С. ЛЕНГ

АЛГЕБРА

Автор книги, видный американский математик, профессор Колумбийского университета С. Ленг, хорошо знаком советскому читателю по двум вышедшим ранее монографиям "Алгебраические числа" и "Введение в теорию дифференцируемых многообразий" (издательство "Мир", 1966 и 1967). В книге рассмотрены все основные разделы современной алгебры (группы, кольца, модули, теория полей, линейная и полилинейная алгебра, представления групп). Читатель найдет здесь также первоначальные сведения по гомологической алгебре и алгебраической геометрии.

Книга отражает изменения, происшедшие в алгебре за последние два десятилетия, и дает читателю возможность основательно познакомиться с областями алгебры, ставшими уже классическими. Язык категорий и функторов связывает воедино разрозненные ранее понятия и результаты.

Книга будет весьма полезной математикам различных специальностей, студентам, аспирантам и научным работникам. Она может служить основой специальных курсов по алгебре.

ОГЛАВЛЕНИЕ

ЧАСТЬ ТРЕТЬЯ

ЛИНЕЙНАЯ АЛГЕБРА И ПРЕДСТАВЛЕНИЯ

УКАЗАТЕЛЬ

От редактора перевода

„Алгебра“ С. Ленга призвана служить в основном тем же целям, что и изданная у нас двадцать лет назад и ставшая теперь библиографической редкостью двухтомная „Современная алгебра“ Ван дер Вардена. Об этой преемственности, как и о содержании всей книги, достаточно подробно говорится в предисловии автора. Читатель, несомненно, почувствует, что умело подобранный свежий материал, а также язык и стиль изложения вполне созвучны алгебре шестидесятых годов — обстоятельство особенно ценное для молодых математиков.

Добросовестная работа переводчика способствовала устранению неточностей и опечаток, помимо тех, список которых был любезно прислан нам автором. Более значительные исправления в соответствии с пожеланиями автора были внесены в гл. XI.

Свободный и местами шутливый тон книги отчасти смягчен подстрочными примечаниями.

А. И. Кострикин

Предисловие

> Я предпочитаю называть ее так [абстрактной алгеброй], а не современной алгеброй, потому что она, несомненно, будет жить долго и в конце концов станет древней алгеброй.
> Ф. Севери (Льеж, 1949)

Эта книга может служить основой годового курса алгебры для аспирантов.

К сожалению, объем материала, который слушатель в идеале должен был бы усвоить за год, чтобы получить надлежащую подготовку по алгебре (независимо от того, по какому предмету он специализируется), превышает физические возможности лектора в течение годового курса. Следовательно, книга должна содержать больше материала, чем в действительности может быть изложено в аудитории.

Порядок изучения различных тем допускает многочисленные вариации. Например, к теории полей и теории Галуа можно приступить сразу же после того, как даны основные определения, относящиеся к группам, кольцам, полям, многочленам от одной переменной и векторным пространствам. Поскольку теория Галуа очень быстро создает впечатление глубины, этот путь весьма привлекателен во многих отношениях.

Можно также после ознакомления с основными определениями начать с линейной алгебры, оставив теорию полей на более позднее время. Главы книги написаны таким образом, чтобы обеспечить наибольшую гибкость в этом отношении, и я часто совершаю преступление против бурбакизма, повторяя короткие рассуждения или определения, чтобы сделать некоторые параграфы или главы логически независимыми друг от друга.

В изложении теории Галуа я следую Артину, но с незначительными модификациями. Чтобы прочувствовать различия, читатель может с пользой для себя обратиться к небольшой книжке Артина. Кроме того, читателю стоило бы ознакомиться с изложением, основанным на теореме Джекобсона — Бурбаки, полезной в несепарабельном случае. Однако стандартный случай достаточно важен в большинстве приложений, чтобы оправдать классическое изложение, которое я здесь выбрал.

Поскольку алгебре научил меня Артин, чувство обязанности по отношению к нему пронизывает всю книгу. В меньшей степени это,

возможно, относится к разделу линейной алгебры и представлений, где влияние Бурбаки является более решающим (в содержании, а не в стиле изложения). Однако в выборе материала я более разборчив, чем Бурбаки, с вытекающими отсюда преимуществами и недостатками меньшей энциклопедичности.

Обеспечив изложение материала, который ни при каких обстоятельствах не может быть опущен в основном курсе, можно затем на выбор развивать его в различных направлениях. Невозможно изложить их все с одинаковой полнотой. Точный момент, когда лектор пожелает остановиться в любом из этих направлений, будет зависеть от времени, места и настроения. Например, главы о вещественных полях и абсолютных значениях могут быть без ущерба опущены или же прочитаны слушателями самостоятельно. То же самое относится к главе о представлениях групп. Теорема Витта о квадратичных формах также может быть опущена. Однако любая книга, преследующая те же цели, что и наша, должна включать набор этих тем, ведущих вглубь, но развиваемых ровно настолько, чтобы избежать полной запутанности и излишнего увеличения числа страниц. По всем этим вопросам не может быть достигнуто даже внутренней удовлетворенности автора, не говоря уж о всеобщем согласии. В конечном счете конкретные решения относительно того, что включать и что не включать, принимаются исходя из соображений общей связности и эстетического равновесия. Например, я умышленно избежал чрезмерного углубления в коммутативную алгебру. Я не мог превращать основной курс алгебры исключительно в тренировочный полигон для будущих алгебраических геометров. Однако всякий преподающий этот курс может наложить на материал отпечаток своей индивидуальности и с большей силой, чем у меня, выделить одни темы за счет других. В предлагаемой книге нет ничего, что воспрепятствовало бы этому.

Структура книги все еще удивительно напоминает ту, которая была придана ей Артином, Нётер и Ван дер Варденом примерно тридцать лет тому назад. Я целиком согласен с Ван дер Варденом в вопросе о включении в учебное пособие такого рода теории представлений конечных групп. Ввиду прогресса, достигнутого Брауэром за истекшие тридцать лет, оказалось возможным дать более полное изложение, чем это мог сделать Ван дер Варден в свое время.

Имеются достаточные основания, чтобы включить в курс больше материала о линейных группах и их представлениях, чем я это сумел сделать, пытаясь сохранить размер книги в разумных пределах. Особенно легко это осуществить с аспирантами, имеющими надлежащую подготовку по линейной алгебре со своих студенческих лет. К счастью, теперь имеется несколько учебников, посвященных алгебрам Ли и группам Ли, так что я не чувствую себя слишком виноватым, опустив эти темы (см., в частности, записки Серра „Алгебры Ли и группы Ли“).

Что касается предварительных сведений, то я предполагаю только, что читатель знаком с основными математическими понятиями (т. е. по существу с множествами и отображениями), а также с целыми и рациональными числами. Более подробное описание того, что предполагается известным, приведено ниже. В нескольких случаях определители используются раньше их формального изложения в тексте. Большинству читателей определители уже будут известны, и мы полагаем, что для улучшения структуры всей книги можно позволить себе такие небольшие отклонения от полного упорядочения логических связей.

Нью-Йорк, 1965 *Серж Ленг*

Предварительные сведения

Мы предполагаем, что читатель знаком с понятием множества и символами $\cap$, $\cup$, $\supset$, $\subset$, $\in$. Если A, B — множества, то запись $A \subset B$ обозначает, что A содержится в B, но может и совпадать с B. То же самое относится к записи $A \supset B$.

Если $f\colon A \to B$ — отображение одного множества в другое, то мы пишем

$$x \longmapsto f(x)$$

для обозначения действия f на элемент x из A. Мы различаем стрелки $\to$ и $\longmapsto$.

Пусть $f\colon A \to B$ — некоторое отображение. Мы говорим, что f *инъективно*, если из $x \neq y$ следует $f(x) \neq f(y)$. Мы говорим, что f *сюръективно*, если для каждого $b \in B$ существует элемент $a \in A$, такой, что $f(a) = b$. Мы говорим, что f *биективно*, если оно одновременно сюръективно и инъективно [1]).

Подмножество A множества B называется *собственным*, если $A \neq B$.

Пусть $f\colon A \to B$ — отображение и A' — подмножество в A.

Ограничение f на A' есть отображение A' в B, обозначаемое символом $f \mid A'$.

Если $f\colon A \to B$ и $g\colon B \to C$ — отображения, то их *композиция* $g \circ f$ определяется соотношением $(g \circ f)(x) = g(f(x))$ для всех $x \in A$.

Пусть $f\colon A \to B$ — отображение и B' — подмножество в B. Через $f^{-1}(B')$ мы обозначаем подмножество в A, состоящее из всех тех $x \in A$, для которых $f(x) \in B'$. Мы называем его *прообразом* множества B'. Соответственно $f(A)$ мы называем *образом* отображения f.

Диаграмма

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & {\scriptstyle h}\searrow \quad \swarrow{\scriptstyle g} & \\ & C & \end{array}$$

---

[1]) В применении к отображениям множеств с заданной системой алгебраических операций в русской литературе наряду с терминами „инъективно", „сюръективно" и „биективно" употребительны также соответственно термины „мономорфно", „эпиморфно" и „изоморфно". — *Прим. ред.*

называется *коммутативной*, если $g \circ f = h$. Аналогично диаграмма

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow[\psi]{} & D \end{array}$$

называется коммутативной, если $g \circ f = \psi \circ \varphi$. Мы будем иногда иметь дело с более сложными диаграммами, состоящими из стрелок между различными объектами. Такие диаграммы называются *коммутативными*, если в любом случае, когда можно пройти от одного объекта к другому по двум различным последовательностям стрелок, скажем

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} A_n$$

и

$$A_1 \xrightarrow{g_1} B_2 \xrightarrow{g_2} \dots \xrightarrow{g_{m-1}} B_m = A_n,$$

соответствующие композиции совпадают:

$$f_{n-1} \circ f_{n-2} \circ \dots \circ f_1 = g_{m-1} \circ g_{m-2} \circ \dots \circ g_1.$$

Большинство наших диаграмм будет состоять из указанных выше треугольников или квадратов, и для проверки коммутативности таких диаграмм достаточно убедиться, что каждый треугольник и квадрат в них коммутативен.

Мы предполагаем, что читатель знаком с целыми и рациональными числами, множества которых обозначаются соответственно через $\mathbf{Z}$ и $\mathbf{Q}$. Во многих примерах мы предполагаем также, что читателю известны вещественные и комплексные числа, множества которых обозначаются через $\mathbf{R}$ и $\mathbf{C}$.

Пусть A и I — два множества. Под *семейством* элементов в A, занумерованных посредством I, понимают отображение $f\colon I \to A$. Таким образом, для каждого $i \in I$ задан элемент $f(i) \in A$. Хотя семейство есть не что иное как отображение, мы часто мыслим его как совокупность объектов из A и записываем его так:

$$\{f(i)\}_{i \in I}$$

или

$$\{a_i\}_{i \in I},$$

употребляя символ a_i вместо $f(i)$. Мы называем I *множеством индексов*.

Мы предполагаем, что читатель знает, что такое отношение эквивалентности. Пусть A — множество с заданным на нем отношением эквивалентности, E — некоторый класс эквивалентности элементов из A. Иногда мы будем определять отображение классов эквивалент-

ности в некоторое множество B. Чтобы определить такое отображение на классе E, мы будем зачастую сначала задавать его значение на некотором элементе $x \in E$ (называемом представителем класса E), а затем показывать, что оно не зависит от выбора представителя $x \in E$. В таком случае говорят, что f *правильно определено.*

Нам будут встречаться произведения множеств, скажем конечные произведения $A \times B$ или $A_1 \times \ldots \times A_n$, и произведения семейств множеств.

Мы будем пользоваться леммой Цорна, которую мы сейчас сформулируем.

Множество A называется (*частично*) *упорядоченным*, если между некоторыми парами элементов задано отношение $x \leqslant y$, удовлетворяющее следующим условиям. Для всех x, y, $z \in A$

имеем $x \leqslant x$;
если $x \leqslant y$ и $y \leqslant z$, то $x \leqslant z$;
если $x \leqslant y$ и $y \leqslant x$, то $x = y$.

Подмножество T в A называется *совершенно* (или *линейно*) упорядоченным, если для всякой пары элементов x, $y \in T$ будет $y \leqslant x$ или $x \leqslant y$.

Пусть S — подмножество в A. Любой элемент $b \in A$, удовлетворяющий условию $x \leqslant b$ для всех $x \in S$, будем называть верхней гранью подмножества S в множестве A.

Упорядоченное множество A называется *индуктивно упорядоченным*, если всякое его совершенно упорядоченное подмножество имеет верхнюю грань в A.

Элемент $a \in A$, для которого из $x \in A$ и $a \leqslant x$ следует $a = x$, называется *максимальным* элементом множества A. (Таким образом, максимальный означает „относительно максимальный“, а не „абсолютно максимальный“.)

Лемма Цорна утверждает: *если A — упорядоченное множество и если оно индуктивно упорядочено и не пусто, то в A существует по крайней мере один максимальный элемент.*

Мы будем также использовать утверждения о мощностях, наподобие следующих.

Пусть A — бесконечное множество. Тогда множество всех конечных подмножеств в A имеет ту же мощность, что и A. Если D счетно, то $A \times D$ имеет ту же мощность, что и A. Мощность мы будем иногда сокращенно обозначать символом card. Имеем

$$(\operatorname{card}(A) \leqslant \operatorname{card}(B) \quad \text{и} \quad \operatorname{card}(B) \leqslant \operatorname{card}(A)) \text{ влечет}$$
$$\operatorname{card}(A) = \operatorname{card}(B).$$

Литература[1])

[1] Artin E., Galois Theory, Notre Dame Mathematical Lectures, № 2, 1946

[2] Artin E., Geometric Algebra, Interscience, New York, 1957.

[3] Bourbaki N., Algèbre commutative, Hermann, Paris, 1962.

[4] Бурбаки Н., Алгебра. Модули, кольца, формы, „Наука", М., 1966.

[5] Бурбаки Н., Алгебра. Многочлены и поля. Упорядоченные группы, „Наука", М., 1965.

[6] Godement R., Cours d'algèbre, Hermann, Paris, 1963.

[7] Jacobson N., Lectures in abstract algebra, Van Nostrand, Princeton, N. J., vol. I, 1951; vol. 2, 1953; vol. 3, 1964.

[8] Ленг С., Алгебраические числа, „Мир", М., 1966.

[9] Lang S., Diophantine geometry, Interscience, New York, 1960.

[10] Ван дер Варден Б. Л., Современная алгебра, т. 1 и 2, Гостехиздат, М. — Л., 1947.

[11] Weber H., Lehrbuch der Algebra, 1898 (reprinted by Chelsea, 1963).

[12] Зарисский О., Самюэль П., Коммутативная алгебра, т. 1 и 2, ИЛ, М., 1963.

[13*] Курош А. Г., Лекции по общей алгебре, Физматгиз, М., 1962.

[14*] Боревич З. И., Шафаревич И. Р., Теория чисел, „Наука", М., 1964.

Выше приведен краткий перечень учебных пособий и монографий по алгебре. Бурбаки всегда наиболее полон и незаменим для ссылок. Джекобсон излагает теорию Галуа с позиций теоремы Джекобсона — Бурбаки, полезной, помимо всего прочего, при рассмотрении чисто несепарабельных расширений. Читателю следует пробежать все эти книги, чтобы ознакомиться с точками зрения, отличными от принятых в настоящей книге.

---

[1]) Звездочкой отмечена литература, добавленная при переводе. — *Прим. ред.*

Часть первая

ГРУППЫ, КОЛЬЦА И МОДУЛИ

В этой части вводятся основные понятия алгебры, и главная трудность для начинающего заключается в овладении разумным словарным запасом за короткое время. Ни одно из новых понятий само по себе не является трудным, но их последовательное накопление может иногда показаться тяжким.

Чтобы понимать последующие части книги, читатель по существу должен знать только основные определения этой первой части. Разумеется, та или иная теорема может в дальнейшем использоваться в отдельных местах, но в целом мы стремились избегать длинных цепочек логических зависимостей.

Глава I

Группы

§ 1. Моноиды

Пусть S — множество. Отображение

$$S \times S \to S$$

называется иногда *законом композиции* (на S в себя). Если x и y — элементы из S, то образ пары (x, y) при этом отображении называется также их *произведением* относительно закона композиции и будет обозначаться через xy. (Иногда мы пишем также $x \cdot y$, а во многих случаях удобно использовать и аддитивное обозначение и писать, таким образом, $x+y$. В этом случае мы называем элемент $x+y$ *суммой* x и y. Обычно обозначение $x+y$ используют только в том случае, когда выполняется соотношение $x+y=y+x$.)

Пусть S — множество, наделенное законом композиции. Произведение элементов x, y, z из S можно составить двумя способами: $(xy)z$ и $x(yz)$. Если $(xy)z=x(yz)$ для всех x, y, z из S, то мы говорим, что закон композиции *ассоциативен*.

Элемент e из S, такой, что $ex=x=xe$ для всех $x \in S$, называется *единичным элементом*. (Когда закон композиции записывается аддитивно, единичный элемент обозначается через 0 и называется *нулевым элементом*.) Единичный элемент единствен, поскольку если e' — другой единичный элемент, то по предположению имеем

$$e=ee'=e'.$$

В большинстве случаев единичный элемент обозначают просто 1 (вместо e). В большей части этой главы, однако, мы будем писать e, чтобы избежать путаницы при доказательствах основных свойств.

Моноид — это множество G с ассоциативным законом композиции, обладающим единичным элементом (так что, в частности, G не пусто).

Пусть G — моноид и $x_1, \ldots, x_n$ — элементы из G (где n — целое число >1). Мы определим их произведение по индукции

$$\prod_{\nu=1}^{n} x_\nu = x_1 \ldots x_n = (x_1 \ldots x_{n-1})\, x_n.$$

Справедливо следующее правило

$$\prod_{\mu=1}^{m} x_\mu \cdot \prod_{\nu=1}^{n} x_{m+\nu} = \prod_{\nu=1}^{m+n} x_\nu,$$

утверждающее по существу, что мы можем любым способом расставлять скобки в нашем произведении, не изменяя его значения. Доказательство легко получается индукцией, и мы предоставляем его читателю в качестве упражнения.

Вместо $\prod_{\nu=1}^{n} x_{m+\nu}$ пишут также $\prod_{m+1}^{m+n} x_\nu$.

Удобно считать, что пустое произведение равно единичному элементу. Таким образом, по определению $\prod_{\nu=1}^{0} x_\nu = e$.

Можно было бы определить более общие законы композиции, т. е. отображения $S_1 \times S_2 \to S_3$ с произвольными множествами; можно, далее, определить ассоциативность и коммутативность в любой ситуации, для которой это имеет смысл. Например, для коммутативности нужен закон композиции

$$f\colon S \times S \to T,$$

где два исходных множества одинаковы. *Коммутативность* тогда означает, что $f(x, y) = f(y, x)$, или $xy = yx$, если опустить в обозначениях f. Что касается ассоциативности, то мы предоставляем читателю найти наиболее общую комбинацию множеств, при которой она работает. Ниже нам встретятся специальные случаи, связанные, например, с отображениями $S \times S \to S$ и $S \times T \to T$. Здесь произведение $(xy)z$ имеет смысл при $x \in S$, $y \in S$ и $z \in T$. Произведение $x(yz)$ также имеет смысл для таких элементов x, y, z, и, следовательно, имеет смысл говорить об ассоциативности нашего закона композиции, коль скоро для всех указанных выше элементов x, y, z выполнено равенство $(xy)z = x(yz)$.

Если закон композиции, определенный на G, коммутативен, то мы также будем говорить, что сам моноид G *коммутативен* (или *абелев*).

Пусть G — коммутативный моноид и $x_1, \ldots, x_n$ — элементы из G. Пусть ψ — биективное отображение множества целых чисел $(1, \ldots, n)$ на себя. Тогда

$$\prod_{\nu=1}^{n} x_{\psi(\nu)} = \prod_{\nu=1}^{n} x_\nu.$$

Мы докажем это утверждение по индукции. Для $n = 1$ оно очевидно. Предположим, что оно верно для $n - 1$. Пусть k — такое целое число, что $\psi(k) = n$. Тогда

$$\prod_{1}^{n} x_{\psi(\nu)} = \prod_{1}^{k-1} x_{\psi(\nu)} \cdot x_{\psi(k)} \cdot \prod_{1}^{n-k} x_{\psi(k+\nu)} = \prod_{1}^{k-1} x_{\psi(\nu)} \cdot \prod_{1}^{n-k} x_{\psi(k+\nu)} \cdot x_{\psi(k)}.$$

Определим отображение φ множества $(1, \ldots, n-1)$ в себя формулами

$$\varphi(\nu) = \psi(\nu), \qquad \text{если} \quad \nu < k,$$
$$\varphi(\nu) = \psi(\nu + 1), \quad \text{если} \quad \nu \geqslant k.$$

Тогда

$$\prod_1^n x_{\psi(\nu)} = \prod_1^{k-1} x_{\varphi(\nu)} \cdot \prod_1^{n-k} x_{\varphi(k-1+\nu)} \cdot x_n = \prod_1^{n-1} x_{\varphi(\nu)} \cdot x_n,$$

что по индукции равно $x_1, \ldots, x_n$, как и требовалось.

Пусть G — коммутативный моноид, I — некоторое множество, и пусть $f\colon I \to G$ — такое отображение, что $f(i) = e$ для почти всех $i \in I$. (Здесь и ниже *почти все* означает *все, кроме конечного числа.*) Пусть I_0 — подмножество в I, состоящее из тех i, для которых $f(i) \neq e$. Под

$$\prod_{i \in I} f(i)$$

мы будем понимать произведение

$$\prod_{i \in I_0} f(i),$$

взятое в любом порядке (его значение не зависит от порядка по предыдущему замечанию). Разумеется, пустое произведение равно e.

Когда G записывается аддитивно, то вместо знака произведения мы пишем знак суммы $\sum$.

Имеется ряд формальных правил обращения с произведениями, которые было бы скучно полностью перечислять. Приведем только один пример. Пусть I, J — два множества и $f\colon I \times J \to G$ — отображение в коммутативный моноид, принимающее значение e для почти всех пар (i, j). Тогда

$$\prod_{i \in I} \Big[\prod_{j \in J} f(i, j) \Big] = \prod_{j \in J} \Big[\prod_{i \in I} f(i, j) \Big].$$

Доказательство предоставляем читателю в качестве упражнения.

Мы будем иногда писать $\prod f(i)$, опуская $i \in I$, если ясно, о каком множестве индексов идет речь.

Пусть x — элемент моноида G. Для всякого целого $n \geqslant 0$ мы определим x^n как

$$\prod_1^n x,$$

так что, в частности, $x^0 = e$, $x^1 = x$, $x^2 = xx$, ... Очевидно, $x^{n+m} = x^n x^m$ и $(x^n)^m = x^{nm}$. Кроме того, в силу ассоциативности для любых двух элементов x и y моноида G, таких, что $xy = yx$,

имеем $(xy)^n = x^n y^n$. Формальное доказательство предоставляем читателю в качестве упражнения.

Пусть S, S' — два подмножества моноида G. Мы понимаем под SS' подмножество, состоящее из всех элементов вида xy, где $x \in S$ и $y \in S'$. По индукции можно определить произведение любого конечного числа подмножеств, причем имеет место ассоциативность. Например, если S, S', S'' — подмножества в G, то $(SS')S'' = S(S'S'')$. Заметим, что $GG = G$ (потому что в G имеется единичный элемент). Для $x \in G$ мы определим xS как $\{x\}S$, где $\{x\}$ — множество, состоящее из одного элемента x. Таким образом, множество xS состоит из всех элементов вида xy, где $y \in S$.

Подмоноидом моноида G называется подмножество H в G, содержащее единичный элемент e и такое, что $xy \in H$, если x, $y \in H$ (мы говорим, что H *замкнуто* относительно закона композиции). Ясно, что подмоноид H сам является моноидом относительно закона композиции, индуцированного законом композиции на G.

Для всякого элемента x моноида G подмножество степеней x^n $(n = 0, 1, \ldots)$ есть подмоноид в G.

Пример моноида. Мы предполагаем, что читатель знаком с терминологией элементарной топологии. Пусть M — множество классов гомеоморфных друг другу компактных (связных) поверхностей. Определим сложение в M. Пусть S, S' — компактные поверхности, D — маленький диск в S и D' — маленький диск в S'. Пусть далее C, C' — окружности, образующие границы D и D', а D_0, D_0' — внутренности дисков D и D' соответственно. Приклеим $S - D_0$ к $S' - D_0'$, отождествив C с C'. Можно показать, что получающаяся поверхность не зависит с точностью до гомеоморфизма от произвола в выборе, имеющегося в предыдущем построении. Если σ, σ' обозначают классы поверхностей, гомеоморфных поверхностям S и S' соответственно, то мы берем в качестве $\sigma + \sigma'$ класс поверхности, полученной указанным процессом склеивания. Можно показать, что так определенное сложение определяет на M структуру моноида, нулевым элементом которого будет класс обычной двумерной сферы. Кроме того, если τ обозначает класс тора, а π — класс проективной плоскости, то всякий элемент σ из M имеет единственное представление в виде

$$\sigma = n\tau + m\pi,$$

где n — целое число $\geqslant 0$, а $m = 0$, 1 или 2. Справедливо равенство $3\pi = \tau + \pi$.

(Предыдущий пример включен по двум причинам: во-первых, чтобы скрасить неизбежную скуку этого параграфа; во-вторых, чтобы показать читателю, что моноиды существуют в природе. Нет нужды говорить, что этот пример никоим образом не будет использоваться в остальной части книги.)

§ 2. Группы

Группа G — это моноид, в котором для каждого элемента $x \in G$ существует элемент $y \in G$, такой, что $xy = yx = e$. Элемент y называется *обратным* к x. Обратный элемент единствен; действительно, если y' — другой обратный к x, то

$$y' = y'e = y'(xy) = (y'x)y = ey = y.$$

Мы обозначаем этот обратный элемент через x^{-1} (или через $-x$, когда закон композиции записывается аддитивно).

Для любого положительного целого числа n мы полагаем $x^{-n} = (x^{-1})^n$. При этом обычные правила оперирования с показателями выполняются для всех целых чисел, а не только для целых чисел $\geqslant 0$ (как это было для моноидов в § 1). Тривиальное доказательство предоставляется читателю.

Мы могли бы также определить левые единицы и левые обратные (очевидным способом). Легко доказать, что они являются на самом деле единицами и обратными соответственно. Именно:

Пусть G — множество с ассоциативным законом композиции, e — левая единица для этого закона. Предположим, что у каждого элемента есть левый обратный. Тогда e — единица и всякий левый обратный является также обратным. В частности, G — группа.

Для доказательства рассмотрим произвольный элемент $a \in G$ и его левый обратный $b \in G$, $ba = e$.

Имеем

$$bab = eb = b.$$

Умножение слева на левый обратный для b дает

$$ab = e,$$

другими словами, b является также правым обратным к a. Кроме того,

$$ae = aba = ea = a,$$

следовательно, e — правая единица.

Пример. Пусть G — группа и S — непустое множество. Множество отображений $M(S, G)$ является группой; именно, для любых двух отображений f, g множества S в G определим отображение fg равенством

$$(fg)(x) = f(x)\,g(x)$$

и отображение f^{-1} равенством $f^{-1}(x) = f(x)^{-1}$. Тривиально проверяется, что $M(S, G)$ — группа. Если G коммутативна, то такова же

и группа $M(S, G)$, и при аддитивной записи закона композиции в G так же записывают и закон композиции в $M(S, G)$, так что пишут $f+g$ вместо fg и $-f$ вместо f^{-1}.

Пример. Пусть S — непустое множество, G — множество биективных отображений S на себя. Тогда G — группа, причем закон композиции — обычная композиция отображений. Единичным элементом G является тождественное отображение множества S, а групповые свойства проверяются тривиально. Элементы группы G называются *перестановками* множества S.

Пример. Множество рациональных чисел образует группу относительно сложения. Множество отличных от нуля рациональных чисел образует группу относительно умножения. Аналогичные утверждения справедливы для вещественных и комплексных чисел.

Пусть G — группа. *Подгруппой* H группы G называется подмножество в G, содержащее единичный элемент и замкнутое относительно закона композиции и взятия обратного элемента (т. е. это подмоноид, такой, что $x^{-1} \in H$, если $x \in H$). Подгруппа называется *тривиальной*, если она состоит из одного единичного элемента. Пересечение любого непустого семейства подгрупп есть подгруппа (тривиальная проверка).

Пусть G, G' — моноиды. *Гомоморфизм* моноидов (или просто гомоморфизм) G в G' — это отображение $f\colon G \to G'$, удовлетворяющее условию $f(xy) = f(x) f(y)$ для всех x, $y \in G$ и переводящее единичный элемент моноида G в единичный элемент G'. Если G и G' — группы, то *гомоморфизм группы* G в G' — это просто моноидный гомоморфизм.

Мы иногда будем говорить: „пусть $f\colon G \to G'$ — гомоморфизм групп“, имея в виду: „пусть G, G' — группы и f — гомоморфизм группы G в G'“.

Пусть $f\colon G \to G'$ — гомоморфизм групп. Тогда

$$f(x^{-1}) = f(x)^{-1};$$

действительно, если e, e' — единичные элементы в G и G' соответственно, то

$$e' = f(e) = f(xx^{-1}) = f(x) f(x^{-1}).$$

Кроме того, если G, G' — группы и $f\colon G \to G'$ — такое отображение, что $f(xy) = f(x) f(y)$ для всех x, y из G, то $f(e) = e'$. Действительно, $f(ee) = f(e)$ и также равно $f(e) f(e)$. Умножение на обратный к $f(e)$ показывает, что $f(e) = e'$.

Пусть G, G' — моноиды. Гомоморфизм $f\colon G \to G'$ называется *изоморфизмом*, если существует гомоморфизм $g\colon G' \to G$, такой, что $f \circ g$ и $g \circ f$ — тождественные отображения (в G' и G соответственно).

Тривиально проверяется, что отображение f является изоморфизмом в том и только в том случае, если оно биективно. Существование изоморфизма между двумя группами G и G' иногда обозначается символом $G \approx G'$. Если $G = G'$, то мы говорим, что изоморфизм есть *автоморфизм*. Гомоморфизм группы G в себя называется также *эндоморфизмом*.

Пример. Пусть G — моноид и x — элемент из G. Пусть $\mathbf{N}$ обозначает (аддитивный) моноид целых чисел $\geqslant 0$. Тогда отображение $f\colon \mathbf{N} \to G$, определяемое формулой $f(n) = x^n$, есть гомоморфизм. Если G — группа, то мы можем продолжить f до гомоморфизма группы $\mathbf{Z}$ в G (как указывалось выше, x^n определено для всех $n \in \mathbf{Z}$). Тривиальные доказательства предоставляются читателю.

Пусть n — фиксированное целое число, и пусть G — *коммутативная* группа. Легко проверяется, что отображение

$$x \longmapsto x^n$$

группы G в себя есть гомоморфизм. То же самое относится к отображению $x \longmapsto x^{-1}$. Отображение $x \longmapsto x^n$ называется *возведением в n-ю степень*.

Пусть G — группа и S — подмножество в G. Мы будем говорить, что S *порождает* G или что S — множество *образующих* для G, если всякий элемент из G может быть представлен как произведение элементов из S или обратных к ним, т. е. как произведение $x_1 \dots x_n$, где каждое x_i или x_i^{-1} лежит в S. Ясно, что множество всех таких произведений будет подгруппой в G (пустое произведение есть единичный элемент) и притом наименьшей подгруппой в G, содержащей S. Таким образом, S порождает G в том и только в том случае, если наименьшая подгруппа в G, содержащая S, совпадает с G.

Пусть G — группа, S — множество ее образующих и G' — другая группа. Пусть $f\colon S \to G'$ — некоторое отображение. Если существует гомоморфизм $\bar{f}$ группы G в G', ограничение которого на S есть f, то такой гомоморфизм единствен, т. е. f допускает самое большее одно продолжение до гомоморфизма G в G'. Это очевидное утверждение будет неоднократно использоваться в дальнейшем.

Пусть $f\colon G \to G'$ и $g\colon G' \to G''$ — гомоморфизмы групп. Тогда композиция $g \circ f$ — тоже гомоморфизм групп. Если f, g — изоморфизмы, то и $g \circ f$ — изоморфизм. Кроме того, $f^{-1}\colon G' \to G$ — тоже изоморфизм. В частности, множество всех автоморфизмов группы G образует группу, обозначаемую символом $\mathrm{Aut}(G)$.

Пусть $f\colon G \to G'$ — гомоморфизм групп, e и e' — единичные элементы групп G, G'. *Ядром* отображения f мы называем подмножество в G, состоящее из всех тех x, для которых $f(x) = e'$. Из определений немедленно вытекает, что ядро H гомоморфизма f —

подгруппа в G. (Докажем, например, что H замкнуто относительно взятия обратного элемента. Пусть $x \in H$. Тогда

$$f(x^{-1})\,f(x) = f(e) = e'.$$

Так как $f(x) = e'$, то $f(x^{-1}) = e'$, откуда $x^{-1} \in H$. Остальные проверки предоставляем читателю.)

Пусть опять $f\colon G \to G'$ — гомоморфизм групп, H' — его *образ*. Тогда H' — подгруппа в G'. Действительно, H' содержит e', и если $f(x)$, $f(y) \in H'$, то $f(xy) = f(x)\,f(y)$ также лежит в H'. Кроме того, $f(x^{-1}) = f(x)^{-1}$ лежит в H', и, следовательно, H' — подгруппа в G'.

Ядро и образ f иногда обозначаются символами $\operatorname{Ker} f$ и $\operatorname{Im} f$.

Гомоморфизм $f\colon G \to G'$, устанавливающий изоморфизм между группой G и ее образом в G', мы будем также называть *вложением*.

Гомоморфизм, ядро которого тривиально, инъективен.

Чтобы доказать это, предположим, что ядро гомоморфизма f тривиально и что $f(x) = f(y)$ для некоторых x, $y \in G$. Умножая на $f(y^{-1})$, получаем

$$f(xy^{-1}) = f(x)\,f(y^{-1}) = e'.$$

Следовательно, xy^{-1} лежит в ядре, т. е. $xy^{-1} = e$ и $x = y$. Если, в частности, гомоморфизм f также и сюръективен, то f — изоморфизм. Таким образом, сюръективный гомоморфизм, ядро которого тривиально, — обязательно изоморфизм. Отметим, что инъективный гомоморфизм является вложением.

Пусть G — группа и H — ее подгруппа. *Левый смежный класс* группы G по H — это подмножество в G вида aH, где a — некоторый элемент из G. Всякий элемент из aH называется *представителем смежного класса* aH. Отображение $x \mapsto ax$ индуцирует биекцию H на aH. Следовательно, любые два левых смежных класса имеют одинаковую мощность.

Заметим, что смежные классы aH и bH, имеющие хотя бы один общий элемент, совпадают. Действительно, пусть $ax = by$, где x, $y \in H$. Тогда $a = byx^{-1}$. Но $yx^{-1} \in H$. Следовательно, $aH = b(yx^{-1})H = bH$, потому что для любого $z \in H$ имеем $zH = H$.

Мы приходим к выводу, что G есть объединение попарно непересекающихся левых смежных классов по H. Аналогичное замечание применимо к *правым смежным классам* (т. е. подмножествам в G вида Ha). Число левых смежных классов группы G по H обозначается через $(G : H)$ и называется (левым) *индексом* подгруппы H в G. Индекс тривиальной подгруппы называется *порядком* группы G и обозначается символом $(G : 1)$. Из предыдущего получаем

Предложение 1. *Пусть G — группа и H — ее подгруппа. Тогда*

$$(G : H)(H : 1) = (G : 1)$$

в том смысле, что если два из этих индексов конечны, то конечен и третий и имеет место написанное равенство. Если порядок $(G:1)$ конечен, то он делится на порядок подгруппы H.

Более общо, пусть H, K — подгруппы в G, причем $H \supset K$. Пусть $\{x_i\}$ — множество представителей (левых) смежных классов H по K и $\{y_j\}$ — множество представителей смежных классов G по H. Тогда мы утверждаем, что $\{y_j x_i\}$ — множество представителей смежных классов группы G по K.

Чтобы доказать это, заметим, что

$$H = \bigcup_i x_i K,$$

$$G = \bigcup_j y_j H,$$

причем в обоих объединениях слагаемые попарно не пересекаются. Следовательно,

$$G = \bigcup_{i,\,j} y_j x_i K.$$

Мы должны показать, что в последнем объединении слагаемые также попарно не пересекаются, т. е. $y_j x_i$ представляют различные смежные классы. Предположим, что

$$y_j x_i K = y_{j'} x_{i'} K$$

для некоторой пары индексов (j, i) и (j', i'). Умножив на H справа и приняв во внимание, что x_i, $x_{i'}$ лежат в H, получим

$$y_j H = y_{j'} H,$$

откуда $y_j = y_{j'}$. Отсюда вытекает, что $x_i K = x_{i'} K$, а потому $x_i = x_{i'}$, что и требовалось показать.

Формула из предложения 1 может быть, следовательно, обобщена:

$$(G:K) = (G:H)(H:K),$$

причем понимать это нужно так: если два из трех индексов, входящих в формулу, конечны, то конечен и третий и имеет место написанное равенство.

§ 3. Циклические группы

Целые числа $\mathbf{Z}$ образуют аддитивную группу. Найдем ее подгруппы. Пусть H — подгруппа в $\mathbf{Z}$. Если H нетривиальна, то пусть a — ее наименьший положительный элемент. Мы утверждаем, что H состоит из всех элементов вида na, где $n \in \mathbf{Z}$. Чтобы доказать это, рассмотрим любой элемент $y \in H$. Существуют целые числа n, r, где $0 \leqslant r < a$, такие, что

$$y = na + r.$$

Так как H — подгруппа и $r = y - na$, то $r \in H$, а потому $r = 0$, и наше утверждение доказано.

Мы будем говорить, что группа G *циклическая*, если существует такой элемент a в G, что всякий элемент x из G может быть записан в виде a^n, где $n \in \mathbf{Z}$ (другими словами, если отображение $f: \mathbf{Z} \to G$, определяемое формулой $f(n) = a^n$, сюръективно). При этом элемент a называется *образующей* группы G.

Пусть G — группа и $a \in G$. Подмножество всех элементов a^n ($n \in \mathbf{Z}$) есть, очевидно, циклическая подгруппа в G. Если m — целое число, для которого $a^m = e$ и $m > 0$, то мы будем называть m *показателем* элемента a. Будем говорить, что $m > 0$ — *показатель* группы G, если $x^m = e$ для всех $x \in G$.

Пусть G — группа и $a \in G$. Пусть f: $\mathbf{Z} \to G$ — гомоморфизм, определенный формулой $f(n) = a^n$, и пусть H — ядро f. Возможны два случая.

(i) Ядро тривиально. Тогда f — изоморфизм $\mathbf{Z}$ на циклическую подгруппу в G, порожденную элементом a, и эта подгруппа бесконечна. (Если a порождает G, то G — циклическая группа.) Мы говорим, что a имеет *бесконечный период*.

(ii) Ядро не тривиально. Пусть d — наименьшее положительное целое число, лежащее в ядре. Это d называется *периодом* (или *порядком*) элемента a. Если m — такое целое число, что $a^m = e$, то $m = ds$ для некоторого целого s. Заметим, что элементы $e, a, \ldots, a^{d-1}$ попарно различны. Действительно, если $a^r = a^s$, где $0 \leqslant r, s \leqslant d - 1$, и, скажем, $r \leqslant s$, то $a^{s-r} = e$. Так как $0 \leqslant s - r < d$, то мы должны иметь $s - r = 0$. Циклическая подгруппа, порожденная элементом a, имеет порядок d. Следовательно, справедливо

Предложение 2. *Пусть G — конечная группа порядка $n > 1$. Тогда период всякого элемента $a \neq e$ из G делит n. Если порядок группы G — простое число p, то G — циклическая группа и любой отличный от e элемент служит образующей для G.*

Далее имеет место

Предложение 3. *Пусть G — циклическая группа. Тогда всякая ее подгруппа — циклическая. Если f — гомоморфизм G, то его образ — циклическая группа.*

Доказательство. Если G — бесконечная циклическая группа, то она изоморфна $\mathbf{Z}$, а мы нашли все подгруппы в $\mathbf{Z}$ и обнаружили, что они циклические. Если G — конечная циклическая группа с образующей a и H — некоторая ее подгруппа, то пусть m — наименьшее положительное целое число, такое, что a^m лежит в H. Легко проверяется, что a^m порождает H. Наконец, если f: $G \to G'$ — гомоморфизм и a — образующая для G, то $f(a)$ есть, очевидно, образующая для $f(G)$ и, следовательно, $f(G)$ — циклическая группа.

Мы предоставляем читателю в качестве упражнений доказательства следующих утверждений о циклических группах:

(i) *Бесконечная циклическая группа имеет в точности две образующие* (если a — образующая, то a^{-1} — единственная другая образующая).

(ii) Пусть G — конечная циклическая группа порядка n и x — ее образующая. *Множество образующих группы G состоит из тех степеней x^{ν} элемента x, в которых показатель ν взаимно прост с n.*

(iii) Пусть G — циклическая группа и a, b — две ее образующие. *Тогда существует автоморфизм группы G, переводящий a в b. Обратно, любой автоморфизм группы G переводит a в некоторую образующую G.*

§ 4. Нормальные подгруппы

Мы уже отмечали, что ядра гомоморфизмов групп являются подгруппами. Теперь мы хотим охарактеризовать такие подгруппы.

Пусть $f\colon G \to G'$ — гомоморфизм групп и H — его ядро. Для всякого элемента x из G выполняется равенство $xH = Hx$, что проверяется непосредственно исходя из определений. Мы можем также переписать это соотношение в виде $xHx^{-1} = H$.

Обратно, пусть G — группа и H — ее подгруппа. Предположим, что для всех элементов x из G имеем $xH \subset Hx$ (или, что эквивалентно, $xHx^{-1} \subset H$). Если мы возьмем x^{-1} вместо x, то получим $H \subset xHx^{-1}$, откуда $xHx^{-1} = H$. Таким образом, наше условие эквивалентно условию $xHx^{-1} = H$ для всех $x \in G$. Подгруппа H, удовлетворяющая этому условию, называется *нормальной* (или *инвариантной*) подгруппой. Мы сейчас увидим, что всякая нормальная подгруппа служит ядром некоторого гомоморфизма.

Пусть G' — множество смежных классов по H (по предположению левые смежные классы совпадают с правыми смежными классами, так что нет нужды делать различие между ними). Если xH и yH — смежные классы, то их произведение $(xH)(yH)$ также будет смежным классом, поскольку

$$xHyH = xyHH = xyH.$$

Это произведение определяет в G' ассоциативный закон композиции. Ясно, что сама подгруппа H как смежный класс служит единичным элементом для этого закона композиции и что $x^{-1}H$ служит обратным для смежного класса xH. Следовательно, G' — группа.

Пусть $f\colon G \to G'$ — отображение, для которого $f(x)$ есть смежный класс xH. Тогда, очевидно, f — гомоморфизм и подгруппа H содержится в его ядре. Если $f(x) = H$, то $xH = H$ и, значит, $x \in H$, так как H содержит единичный элемент. Таким образом, H совпадает с ядром, и мы получили интересовавший нас гомоморфизм.

Группа смежных классов по нормальной подгруппе H обозначается символом G/H (читается G по модулю H или G по H). Отображение f группы G на G/H, построенное выше, называется *каноническим отображением*, а G/H называется *факторгруппой* группы G по H.

Замечания

(1) Пусть $\{H_i\}_{i\in I}$ — семейство нормальных подгрупп группы G. Тогда подгруппа

$$H=\bigcap_{i\in I}H_i$$

также будет нормальной. Действительно, если $y\in H$ и $x\in G$, то xyx^{-1} лежит в каждой подгруппе H_i, а потому и в H.

(2) Пусть S — подмножество в G, и пусть $N=N_S$ — множество всех таких элементов $x\in G$, что $xSx^{-1}=S$. Тогда N, очевидно, — подгруппа в G; она называется *нормализатором* подмножества S. Если S состоит из одного элемента a, то N называют также *централизатором элемента* a. Более общо, пусть Z_S — множество всех таких элементов $x\in G$, что $xyx^{-1}=y$ для любого $y\in S$. Тогда Z_S называется *централизатором подмножества* S. Централизатор самой группы G называется ее *центром*. Это подгруппа в G, состоящая из всех ее элементов, коммутирующих со всеми другими элементами, и, очевидно, инвариантная в G.

Пусть H — подгруппа в G. Тогда она, очевидно, является инвариантной подгруппой своего нормализатора N_H. Следующие утверждения мы предоставляем читателю в качестве упражнений:

Если K — подгруппа в G и H — нормальная подгруппа в K, то $K\subset N_H$.

Если K — подгруппа в N_H, то KH — группа и H — нормальная подгруппа в KH.

Нормализатор подгруппы H — наибольшая подгруппа группы G, для которой H является нормальной подгруппой.

Пусть G — группа, H — ее нормальная подгруппа, x, $y\in G$. Мы будем писать

$$x\equiv y\,(\mathrm{mod}\,H),$$

если x и y лежат в одном и том же смежном классе по H, или, что равносильно, если xy^{-1} (или $y^{-1}x$) лежит в H. Читается это соотношение так: „x и y сравнимы по модулю H“.

Если G — аддитивная группа, то

$$x\equiv 0\,(\mathrm{mod}\,H)$$

означает, что x лежит в H, а

$$x\equiv y\,(\mathrm{mod}\,H)$$

означает, что $x - y$ (или $y - x$) лежит в H. Знак сравнения используется главным образом для аддитивных групп.

Пусть

$$G' \xrightarrow{f} G \xrightarrow{g} G''$$

— последовательность гомоморфизмов. Мы будем говорить, что эта последовательность *точная*, если $\operatorname{Im} f = \operatorname{Ker} g$. Например, если H — нормальная подгруппа в G, то последовательность

$$H \xrightarrow{j} G \xrightarrow{\varphi} G/H$$

точная (здесь j — вложение и φ — каноническое отображение). Последовательность гомоморфизмов с большим числом членов, например

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \to \ \dots \ \xrightarrow{f_{n-1}} G_n,$$

называется *точной*, если она точна в каждом члене, т. е. если

$$\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$$

для всех $i = 1, \dots, n-2$. Например, точность последовательности

$$0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$$

означает, что f инъективно, что $\operatorname{Im} f = \operatorname{Ker} g$ и что g сюръективно. Эта последовательность по существу не что иное, как точная последовательность

$$0 \to H \to G \to G/H \to 0,$$

где $H = \operatorname{Ker} g$.

Далее мы опишем некоторые гомоморфизмы, которые все называются каноническими.

(i) Пусть G, G' — группы и $f\colon G \to G'$ — гомоморфизм, ядром которого служит H. Пусть $\varphi\colon G \to G/H$ — каноническое отображение. Тогда существует единственный гомоморфизм $f_*\colon G/H \to G'$, инъективный и такой, что $f = f_* \circ \varphi$.

Чтобы определить f_*, рассмотрим xH — смежный класс по H. Так как $f(xy) = f(x)$ для всех $y \in H$, положим $f_*(xH)$ равным $f(x)$. Это значение не зависит от выбора представителя x в смежном классе, и тривиально проверяется, что отображение f_* гомоморфно, инъективно и является единственным гомоморфизмом, удовлетворяющим нашим требованиям. Мы будем говорить, что гомоморфизм f_* ***индуцирован*** гомоморфизмом f.

Наш гомоморфизм f_* индуцирует изоморфизм

$$\lambda\colon G/H \to \operatorname{Im} f$$

факторгруппы G/H на образ f, и, таким образом, отображение f может быть разложено в следующую последовательность гомоморфизмов:

$$G \xrightarrow{\varphi} G/H \xrightarrow{\lambda} \operatorname{Im} f \xrightarrow{j} G'.$$

Здесь j — вложение $\operatorname{Im} f$ в G'.

(ii) Пусть G — группа, H — ее подгруппа и N — пересечение всех нормальных подгрупп, содержащих H. Тогда N — нормальная подгруппа и, следовательно, наименьшая нормальная подгруппа, содержащая H. Пусть $f\colon G \to G'$ — гомоморфизм, ядро которого содержит H. Тогда ядро f содержит N и существует единственный гомоморфизм $f_*\colon G/N \to G'$ (о нем говорят, что он индуцирован гомоморфизмом f), для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ & {\scriptstyle\varphi}\searrow \quad \nearrow{\scriptstyle f_*} & \\ & G/N & \end{array}$$

Как и выше, φ — каноническое отображение.

Можно определить f_*, как и в (i), положив

$$f_*(xN) = f(x).$$

Отображение f_* правильно определено; тривиально проверяется, что оно удовлетворяет всем нашим требованиям.

(iii) Пусть G — группа и $H \supset K$ — две ее нормальные подгруппы. Тогда K — нормальная подгруппа в H и можно определить отображение $G/K \to G/H$, сопоставив каждому смежному классу xK смежный класс xH. Немедленно проверяется, что это отображение является гомоморфизмом и что его ядро состоит из всех смежных классов вида xK, где $x \in H$. Таким образом, имеем канонический *изоморфизм*

$$(G/K)/(H/K) \approx G/H.$$

Можно было бы также описать этот изоморфизм, используя (i) и (ii). Мы предоставляем читателю показать, что имеет место коммутативная диаграмма

$$\begin{array}{ccccccc} 0 \to & H & \longrightarrow & G & \to & G/H & \to 0 \\ & \downarrow{\scriptstyle\text{кан}} & & \downarrow{\scriptstyle\text{кан}} & & \downarrow{\scriptstyle\text{id}} & \\ 0 \to & H/K & \to & G/K & \to & G/H & \to 0 \end{array}$$

в которой строки точны.

(iv) Пусть G — группа и H, K — две ее подгруппы. Предположим, что H содержится в нормализаторе подгруппы K. Тогда очевидно, что $H \cap K$ — нормальная подгруппа в H, и столь же очевидно,

что $HK = KH$ есть подгруппа в G. Имеется сюръективный гомоморфизм

$$H \to HK/K,$$

сопоставляющий каждому $x \in H$ смежный класс xK группы HK по K. Читатель тотчас проверит, что ядром этого гомоморфизма служит как раз $H \cap K$. Таким образом, имеет место канонический изоморфизм

$$H/(H \cap K) \approx HK/K.$$

(v) Пусть $f\colon G \to G'$ — гомоморфизм групп, H' — нормальная подгруппа в G' и $H = f^{-1}(H')$:

$$\begin{array}{ccc} G & \longrightarrow & G' \\ \uparrow & & \uparrow \\ f^{-1}(H') & \to & H' \end{array}$$

Тогда H — нормальная подгруппа в G. [Доказательство: если $x \in G$, то $f(xHx^{-1}) = f(x)f(H)f(x)^{-1}$ содержится в H', так что $xHx^{-1} \subset H$.] Компонируя f с каноническим отображением G' на G'/H', получаем гомоморфизм

$$G \to G' \to G'/H',$$

ядром которого служит H. Следовательно, существует инъективный гомоморфизм

$$\bar{f}\colon G/H \to G'/H',$$

называемый снова каноническим и приводящий к коммутативной диаграмме

$$\begin{array}{ccccccc} 0 & \to & H & \to & G & \to & G/H \to 0 \\ & & \downarrow & & \downarrow f & & \downarrow \bar{f} \\ 0 & \to & H' & \to & G' & \to & G'/H' \to 0 \end{array}$$

Если гомоморфизм f сюръективен, то $\bar{f}$ есть изоморфизм.

Укажем теперь некоторые приложения наших утверждений о гомоморфизмах.

Пусть G — группа. Последовательность подгрупп

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_m$$

называется *башней* подгрупп. Башня называется *нормальной*, если каждая G_{i+1} нормальна в G_i ($i = 0, \ldots, m-1$). Башня называется *абелевой* (соответственно *циклической*), если она нормальна и если каждая факторгруппа G_i/G_{i+1} абелева (соответственно циклическая) [1]).

[1]) Здесь вводится терминология, принятая больше в литературе по теории полей. Специалисты по теории групп говорят преимущественно о *рядах* групп с теми или иными свойствами. — *Прим. ред.*

Пусть $f\colon G \to G'$ — гомоморфизм, и пусть

$$G' = G'_0 \supset G'_1 \supset \ldots \supset G'_m$$

— нормальная башня в G'. Положим $G_i = f^{-1}(G'_i)$. Тогда G_i ($i = 0, \ldots, m$) образуют нормальную башню. Если G'_i образуют абелеву башню (соответственно циклическую башню), то и G_i образуют абелеву (соответственно циклическую) башню, поскольку для каждого i имеется инъективный гомоморфизм

$$G_i/G_{i+1} \to G'_i/G'_{i+1}$$

и поскольку подгруппа абелевой группы (соответственно циклической группы) абелева (соответственно циклическая).

Уплотнением башни

$$G = G_0 \supset G_1 \supset \ldots \supset G_m$$

называется башня, которая может быть получена вставлением конечного числа подгрупп в данную башню. Группа называется *разрешимой*, если она обладает абелевой башней, последним элементом которой будет тривиальная подгруппа (т. е. в предыдущих обозначениях $G_m = \{e\}$).

Предложение 4. *Всякая абелева башня конечной группы G допускает циклическое уплотнение. Всякая конечная разрешимая группа G обладает циклической башней, последним элементом которой является $\{e\}$.*

Доказательство. Второе утверждение есть непосредственное следствие первого, и, очевидно, достаточно доказать, что если G — конечная абелева группа, то G обладает циклической башней. Применим индукцию по порядку группы G. Пусть x — элемент из G (можно предполагать, что $x \neq e$) и X — циклическая группа, порожденная x. Положим $G' = G/X$. По индукции мы можем найти циклическую башню в G'; ее прообраз будет циклической башней в G с последним элементом X. Если мы уплотним эту башню, добавив $\{e\}$ в конце, то получим искомую циклическую башню.

§ 5. Действие группы на множестве

Пусть S — множество и G — моноид. Под *действием* G на S (слева) мы понимаем отображение $G \times S \to S$, такое, что если обозначить через xs образ пары (x, s) при этом отображении ($x \in G$ и $s \in S$), то для всех $x, y \in G$ и $s \in S$ будет

$$(xy)s = x(ys) \quad \text{и} \quad es = s.$$

Мы говорим в таком случае, что G действует на множестве S (слева), а также что S есть *G-множество*.

Рассмотрим G-множество S. Всякое $x \in G$ индуцирует отображение T_x: $S \to S$ множества S в себя, задаваемое формулой

$$T_x(s) = xs$$

для всех $s \in S$. Кроме того, по определению имеем

$$T_{xy} = T_x \circ T_y$$

для всех x, $y \in G$.

Если G — группа, то у отображения T_x существует обратное, а именно $T_{x^{-1}}$, и, следовательно, каждое T_x есть перестановка множества S. Отображение $x \mapsto T_x$ является, очевидно, гомоморфизмом группы G в группу перестановок множества S, и мы говорим, что G *представлена* в виде группы перестановок (или что нам дано представление группы G в группу перестановок).

В остальной части этого параграфа мы будем предполагать, что G — группа. Наиболее важными двумя примерами представлений G в виде группы перестановок являются следующие:

(i) *Сопряжение*. Для всякого x из G определим отображение $\sigma_x : G \to G$ формулой $\sigma_x(y) = xyx^{-1}$. Отображение

$$(x, y) \mapsto xyx^{-1}$$

определяет действие G на себе, называемое *сопряжением* (а также *трансформированием*). (Выполнение условий, которым должно удовлетворять действие, проверяется тривиально.) В действительности каждое σ_x является автоморфизмом G, т. е. для всех y, $z \in G$ имеем

$$\sigma_x(yz) = \sigma_x(y)\,\sigma_x(z),$$

и σ_x обладает обратным, а именно $\sigma_{x^{-1}}$. *Мы видим, таким образом, что отображение*

$$x \mapsto \sigma_x$$

есть гомоморфизм группы G в ее группу автоморфизмов. Ядро этого гомоморфизма — нормальная подгруппа в G, состоящая из всех таких $x \in G$, что $xyx^{-1} = y$ для каждого $y \in G$, т. е. из всех $x \in G$, которые коммутируют с каждым элементом из G. Иными словами, это ядро совпадает с центром группы G.

Чтобы избежать путаницы, мы не употребляем записи xy для $\sigma_x(y)$. Иногда пишут

$$\sigma_{x^{-1}}(y) = x^{-1}yx = y^x,$$

т. е. используют экспоненциальное обозначение, так что выполняются правила

$$y^{xz} = (y^x)^z \quad \text{и} \quad y^e = y$$

для всех x, y, $z \in G$.

Отметим, что посредством сопряжений G действует также на множестве своих подмножеств. Действительно, пусть S — множество всех подмножеств в G и пусть $A \in S$ — одно из них. Тогда xAx^{-1} есть также подмножество в G, которое можно обозначить символом $\sigma_x(A)$, и легко проверяется, что отображение

$$(x, A) \longmapsto xAx^{-1}$$

произведения $G \times S$ в S определяет действие G на S. Отметим, кроме того, что если A — подгруппа в G, то xAx^{-1} — тоже подгруппа, так что G действует посредством сопряжений и на множестве всех подгрупп.

Пусть A, B — два подмножества в G. Мы говорим, что они *сопряжены*, если существует такой элемент $x \in G$, что $B = xAx^{-1}$.

(ii) *Сдвиг.* Для каждого $x \in G$ определим сдвиг T_x: $G \to G$, положив $T_x(y) = xy$. Тогда отображение

$$(x, y) \longmapsto xy = T_x(y)$$

определяет действие группы G на себе *Предостережение*: T_x не является групповым гомоморфизмом! Это только перестановка G

Аналогично G действует посредством сдвигов на множестве своих подмножеств, поскольку $xA = T_x(A)$ — подмножество в G вместе с A. Если H — подгруппа в G, то $T_x(H) = xH$ не будет, конечно, подгруппой, но будет левым смежным классом по H и, следовательно, G действует посредством сдвигов на множестве левых смежных классов по H. Мы обозначим это множество через G/H. Таким образом, G/H есть G-множество, даже если подгруппа H и не является нормальной. Множество *правых* смежных классов обычно обозначают символом $H \backslash G$

Указанные два представления группы G в виде группы перестановок будут часто использоваться в дальнейшем В частности, представление посредством сопряжений будет использовано в следующем параграфе при доказательстве теорем Силова.

Пусть S, S' — два G-множества Мы скажем, что отображение f: $S \to S'$ есть *морфизм* G-множеств или G-отображение, если

$$f(xs) = xf(s)$$

для всех $x \in G$ и $s \in S$ (мы вскоре определим категории и увидим, что G-множества образуют категорию).

Возвратимся теперь к общей ситуации и рассмотрим группу, действующую на некотором множестве S. Пусть $s \in S$. Множество элементов $x \in G$, для которых $xs = s$, есть, очевидно, подгруппа в G;

она называется группой *изотропии* элемента s в G и обозначается символом G_s[1]).

Когда G действует на себе посредством сопряжений, группа изотропии элемента есть не что иное, как нормализатор этого элемента. Точно так же, когда G действует посредством сопряжений на множестве своих подгрупп, группа изотропии подгруппы — это снова ее нормализатор.

Пусть G действует на множестве S, s и s' — элементы S и y — такой элемент из G, что $ys = s'$. Тогда

$$G_{s'} = yG_sy^{-1}.$$

Действительно, сразу видно, что yG_sy^{-1} оставляет s' неподвижным и что $y^{-1}G_{s'}y$ оставляет неподвижным s, откуда и вытекает указанное равенство. Другими словами, группы изотропии элементов s и s' сопряжены.

Пусть G действует на множестве S, s — фиксированный элемент из S. Подмножество в S, состоящее из всех элементов вида xs (где $x \in G$), обозначается через Gs и называется *орбитой* элемента s относительно группы G. Если x и y лежат в одном и том же смежном классе по $H = G_s$, то $xs = ys$, и обратно (очевидно). Таким образом, получаем отображение

$$f\colon G/H \to S,$$

задаваемое формулой $f(xH) = xs$; ясно, что это отображение есть морфизм G-множеств. В действительности, как сразу видно, оно индуцирует биекцию множества левых смежных классов G/H на орбиту Gs. Следовательно, *если G — группа, действующая на множестве S и $s \in S$, то порядок* (или *длина*) *орбиты Gs совпадает с индексом $(G : G_s)$.*

В частности, если G действует посредством сопряжений на множестве своих подгрупп и H — одна из них, то *число сопряженных с H подгрупп равно индексу нормализатора N_H в G.*

Пример. Пусть G — группа и H — ее подгруппа индекса 2. Тогда H нормальна в G. Доказательство. Заметим, что H содержится в своем нормализаторе N_H. Поэтому индекс N_H в G равен 1 или 2. Если он равен 1, то все доказано. Предположим, что он равен 2. Пусть G действует посредством сопряжения на множестве своих подгрупп. Тогда орбита подгруппы H содержит 2 элемента и группа G действует на этой орбите. Таким образом, мы получаем гомоморфизм группы G в группу перестановок двух элементов. Так как имеется одна сопряженная с H подгруппа, не равная H, то ядро этого

[1]) В зависимости от контекста подгруппу G_s называют иногда *стабилизатором*, а также *стационарной* или *стабильной* подгруппой элемента (точки) s. — *Прим. ред.*

гомоморфизма есть (нормальная) подгруппа индекса 2 и, следовательно, совпадает с H, т. е. H нормальна вопреки предположению. Это завершает доказательство.

Пусть G действует на множестве S. Тогда две орбиты группы G либо не пересекаются, либо совпадают. Действительно, если Gs_1 и Gs_2 — две орбиты с общим элементом s, то $s = xs_1$ для некоторого $x \in G$ и, следовательно, $Gs = Gxs_1 = Gs_1$. Аналогично $Gs = Gs_2$. Таким образом, S — объединение попарно не пересекающихся различных орбит, и мы можем записать

$$S = \bigcup_{\iota \in I} Gs_\iota \quad (Gs_\iota \text{ попарно не пересекаются}),$$

где I — некоторое множество индексов и s_ι — элементы различных орбит. Если S конечно, это дает разложение порядка множества S в сумму порядков орбит, которое мы назовем *формулой разложения на орбиты*, а именно

$$\operatorname{card}(S) = \sum_{\iota \in I} (G : G_{s_\iota})$$

Пусть x, y — элементы группы (или моноида) G. Они называются коммутирующими, если $xy = yx$. Если G — группа, то множество всех элементов $x \in G$, коммутирующих со всеми элементами G, есть подгруппа в G, которую мы назвали *центром* группы G. Пусть G действует на себе посредством сопряжения. Тогда элемент x лежит в центре в том и только в том случае, если орбита этого элемента совпадает с ним самим и, таким образом, состоит из одного элемента. Вообще, порядок орбиты элемента x равен индексу его нормализатора. Следовательно, в том случае, когда G — конечная группа, предыдущая формула принимает вид

$$(G : 1) = \sum_{x \in C} (G : G_x),$$

где C — множество представителей различных классов сопряженных элементов. Эта формула называется также *формулой классов*.

§ 6. Силовские подгруппы

Пусть p — простое число. Под p-группой мы понимаем конечную группу, порядок которой является степенью p (т. е. равен p^n для некоторого целого $n \geqslant 0$). Пусть G — конечная группа и H — ее подгруппа. Мы называем H *p-подгруппой* в G, если H — p-группа. Мы называем H *силовской* p-подгруппой, если порядок H есть p^n и если p^n — наибольшая степень p, делящая порядок G. Ниже мы

докажем, что такие подгруппы всегда существуют. Для этого нам понадобится лемма.

Лемма. *Пусть G — конечная абелева группа порядка m и p — простое число, делящее m. Тогда G содержит подгруппу порядка p.*

Доказательство. Докажем сначала по индукции, что если G имеет показатель n, то порядок группы G делит некоторую степень n. Пусть $b \in G$, $b \neq 1$, и пусть H — циклическая подгруппа, порожденная b. Тогда порядок H делит n, так как $b^n = 1$. Далее, n есть показатель для G/H. Следовательно, порядок факторгруппы G/H делит, согласно индуктивному предположению, некоторую степень n, а в таком случае это справедливо и для порядка G, потому что

$$(G : 1) = (G : H)(H : 1).$$

Пусть порядок группы G делится на p. В силу только что доказанного в G существует элемент x, период которого делится на p. Пусть этот период равен ps, где s — некоторое целое число. Тогда $x^s \neq 1$ и, очевидно, элемент x^s имеет период p и порождает подгруппу порядка p, что и требовалось доказать.

Теорема 1. *Пусть G — конечная группа и p — простое число, делящее ее порядок. Тогда в G существует силовская p-подгруппа.*

Доказательство проводится индукцией по порядку G. Если порядок простой, то наше утверждение очевидно. Предположим теперь, что теорема доказана для всех групп, порядок которых меньше порядка G. Если в G имеется собственная подгруппа H, индекс которой взаимно прост с p, то силовская p-подгруппа в H будет также силовской p-подгруппой в G и наше утверждение справедливо по индукции. Мы можем поэтому предположить, что у всякой собственной подгруппы индекс делится на p. Пусть теперь G действует на себе посредством сопряжений. Из формулы классов получаем

$$(G : 1) = (Z : 1) + \sum (G : G_x).$$

Здесь Z — центр G и член $(Z : 1)$ соответствует орбитам, состоящим из одного элемента, т. е. как раз элементам из Z. Сумма справа берется по всем другим орбитам, поэтому каждый индекс $(G : G_x) > 1$, и по предположению делится на p. Так как p делит порядок G, отсюда следует, что p должно делить порядок Z; в частности, G имеет нетривиальный центр.

Согласно лемме, в Z существует циклическая подгруппа H, порожденная элементом порядка p. Так как подгруппа H содержится

в Z, то она нормальна. Пусть $f\colon G \to G/H$ — каноническое отображение. Если p^n — наибольшая степень p, делящая $(G:1)$, то p^{n-1} делит порядок G/H. Пусть K' — силовская p-подгруппа в G/H (существующая по предположению индукции), и пусть $K = f^{-1}(K')$. Тогда $K \supset H$ и f отображает K на K'. Следовательно, имеет место изоморфизм $K/H \approx K'$ и K имеет порядок $p^{n-1}p = p^n$, что и требовалось доказать.

Теорема 2. *Для всякой конечной группы G*

(i) *каждая p-подгруппа содержится в некоторой силовской p-подгруппе;*

(ii) *все силовские p-подгруппы сопряжены;*

(iii) *число силовских p-подгрупп* $\equiv 1 \bmod p$.

Доказательство. Все доказательства являются применениями техники, связанной с формулой классов. Пусть S — множество силовских p-подгрупп в G. Тогда G действует на S посредством сопряжения. Пусть P — одна из силовских p-подгрупп. Группа изотропии G_P подгруппы P содержит P, и, следовательно, орбита подгруппы P (обозначим ее через S_0) имеет порядок, взаимно простой с p. Пусть H — p-подгруппа порядка > 1. Тогда H действует посредством сопряжений на S_0 и S_0 распадается в объединение попарно не пересекающихся орбит относительно H. Так как порядок H есть степень p, то индекс любой ее собственной подгруппы делится на p, следовательно, хотя бы одна из H-орбит в S_0 должна состоять только из одного элемента, а именно из некоторой силовской подгруппы P'. Тогда H содержится в нормализаторе P' и, следовательно, HP' есть подгруппа в G. Кроме того, P' нормальна в HP'. Так как

$$HP'/P' \approx H/(H \cap P'),$$

то порядок HP'/P' есть степень p, а потому и порядок HP' есть степень p. Так как P' — максимальная p-подгруппа в G, то мы должны иметь $HP' = P'$ и, следовательно, $H \subset P'$, что доказывает (i).

В частности, рассмотрим случай, когда H — силовская p-подгруппа в G. Как мы показали, H содержится в некоторой подгруппе, сопряженной с P, и, значит, совпадает с ней (так как порядки их одинаковы). Это доказывает (ii). Наконец, возьмем $H = P$. Тогда одна из орбит относительно H содержит ровно один элемент (сама P), *а все другие орбиты имеют более одного элемента*; в действительности порядки этих орбит делятся на p, поскольку они равны индексам собственных подгрупп в P. Это доказывает (iii).

Теорема 3. *Пусть G — конечная p-группа. Тогда G разрешима. Если ее порядок > 1, то G имеет нетривиальный центр.*

Доказательство. Первое утверждение следует из второго, так как если G имеет центр Z и мы по индукции имеем абелеву башню для G/Z, то мы можем поднять эту абелеву башню до G, показав тем самым, что G разрешима. Чтобы доказать второе утверждение, воспользуемся формулой классов

$$(G : 1) = \operatorname{card}(Z) + \sum (G : G_x);$$

здесь сумма берется лишь по тем x, для которых $(G : G_x) \neq 1$. Очевидно, p делит $(G : 1)$, а также делит каждый член в сумме, так что порядок центра делится на p, что и требовалось доказать.

Следствие. *Пусть G — p-группа, порядок которой отличен от* 1. *Тогда существует последовательность подгрупп*

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_n = G,$$

такая, что каждая подгруппа G_i нормальна в G и G_{i+1}/G_i — циклическая группа порядка p.

Доказательство. Так как центр группы G нетривиален, то в нем имеется элемент $a \neq e$ порядка p. Пусть H — циклическая группа, порожденная a. По индукции, если $G \neq H$, то в факторгруппе G/H мы можем найти последовательность подгрупп, удовлетворяющую сформулированным требованиям. Взяв прообраз этой башни в G, получим искомую последовательность.

§ 7. Категории и функторы

Теперь, прежде чем идти дальше, нам будет удобно ввести новую терминологию. Мы уже встречались с объектами разного рода: множествами, моноидами, группами. Со многими другими мы еще встретимся, а для каждого такого рода объектов мы определяем специальный род отображений между ними (например, гомоморфизмы). Некоторые формальные свойства являются общими для всех них, а именно существование тождественных отображений объектов на себя и ассоциативность отображений, выполняемых одно за другим. Мы введем понятие категории, чтобы дать общее абстрактное описание таких ситуаций.

Категория $\mathcal{A}$ включает в себя следующее: класс объектов $\operatorname{Ob}(\mathcal{A})$; для всяких двух объектов A, $B \in \operatorname{Ob}(\mathcal{A})$ множество $\operatorname{Mor}(A, B)$, называемое множеством *морфизмов* объекта A в B; для всяких трех объектов A, B, $C \in \operatorname{Ob}(\mathcal{A})$ закон композиции (т. е. отображение)

$$\operatorname{Mor}(B, C) \times \operatorname{Mor}(A, B) \to \operatorname{Mor}(A, C).$$

При этом должны выполняться аксиомы:

КАТ 1. Два множества $\mathrm{Mor}(A, B)$ и $\mathrm{Mor}(A', B')$ не пересекаются, за исключением случая $A = A'$ и $B = B'$; в этом случае они равны.

КАТ 2. Для каждого объекта A из $\mathcal{A}$ имеется морфизм $\mathrm{id}_A \in \mathrm{Mor}(A, A)$, который для всех объектов $B \in \mathrm{Ob}(\mathcal{A})$ действует тождественно слева и справа на элементы множеств $\mathrm{Mor}(B, A)$ и $\mathrm{Mor}(A, B)$ соответственно.

КАТ 3. Закон композиции ассоциативен (в случае, когда он определен), т. е. если $f \in \mathrm{Mor}(A, B)$, $g \in \mathrm{Mor}(B, C)$ и $h \in \mathrm{Mor}(C, D)$, то

$$(h \circ g) \circ f = h \circ (g \circ f)$$

для любых объектов A, B, C, D из $\mathcal{A}$.

Здесь мы сознательно записываем композицию элемента g из $\mathrm{Mor}(B, C)$ и элемента f из $\mathrm{Mor}(A, B)$ как $g \circ f$, т. е. как композицию отображений. Далее, в этой книге мы увидим, что на практике морфизмы в большинстве случаев действительно являются отображениями или тесно связаны с отображениями.

Класс всех морфизмов категории $\mathcal{A}$ будет обозначаться символом $\mathrm{Ar}(\mathcal{A})$ (от „arrows of $\mathcal{A}$“ — „стрелки из $\mathcal{A}$“). Мы будем иногда использовать запись „$f \in \mathrm{Ar}(\mathcal{A})$“, чтобы выразить, что f — какой-то морфизм из $\mathcal{A}$, т. е. элемент некоторого множества $\mathrm{Mor}(A, B)$, где $A, B \in \mathrm{Ob}(\mathcal{A})$.

Иногда, неточно выражаясь, мы будем называть категорией сам класс объектов — в том случае, когда ясно, что понимается под морфизмами этой категории.

Элемент $f \in \mathrm{Mor}(A, B)$ записывается также в виде $f\colon A \to B$ или

$$A \xrightarrow{f} B.$$

Морфизм f называется *изоморфизмом*, если существует морфизм $g : B \to A$, такой, что $g \circ f$ и $f \circ g$ являются тождественными морфизмами в $\mathrm{Mor}(A, A)$ и $\mathrm{Mor}(B, B)$ соответственно. Если $A = B$, то изоморфизм мы называем также *автоморфизмом*.

Морфизмы объекта A в себя называются *эндоморфизмами*. Множество эндоморфизмов объекта A обозначается символом $\mathrm{End}(A)$. Из наших аксиом немедленно вытекает, что $\mathrm{End}(A)$ — моноид.

Пусть A — объект категории $\mathcal{A}$. Мы обозначаем через $\mathrm{Aut}(A)$ множество его автоморфизмов. Это множество в действительности является группой, поскольку все наши определения так и подобраны, чтобы выполнялись групповые аксиомы (ассоциативность, существование единичного элемента и обратного). Таким образом, мы теперь начинаем улавливать некую обратную связь между абстрактными и более конкретными категориями.

Примеры. Пусть $\mathscr{S}$ — категория, объектами которой служат множества, а морфизмами — отображения множеств. Мы говорим просто, что $\mathscr{S}$ — категория множеств. Три аксиомы КАТ 1, 2, 3 тривиальным образом удовлетворяются.

Пусть Grp — категория групп, т. е. категория, объектами которой служат группы, а морфизмами — гомоморфизмы групп. Снова все три аксиомы тривиально выполняются. Аналогично имеем категорию моноидов, обозначаемую символом Mon.

Ясно также, что G-множества для всякой группы G образуют категорию (с очевидными морфизмами).

Вообще мы можем теперь определить понятие действия группы G на объекте в любой категории. Действительно, пусть $\mathscr{A}$ — некоторая категория и $A \in Ob(\mathscr{A})$. Под *действием* G на A мы будем понимать гомоморфизм G в группу $\mathrm{Aut}(A)$. Обычно объект A является множеством и автоморфизм из $\mathrm{Aut}(A)$ действует на A как на множестве, т. е. индуцирует перестановку на A. Таким образом, если нам задан гомоморфизм

$$\sigma\colon\ G \to \mathrm{Aut}(A),$$

то для каждого $x \in G$ мы имеем автоморфизм σ_x объекта A, являющийся перестановкой на A.

Рассмотрим специальный случай, когда $\mathscr{A}$ — категория абелевых групп, которую можно обозначить символом Ab. Пусть A — абелева группа, G — группа, и пусть задано действие G на группе A, т. е. гомоморфизм

$$\sigma\colon\ G \to \mathrm{Aut}(A).$$

Будем обозначать через $x \cdot a$ элемент $\sigma_x(a)$. Тогда для всех $x, y \in G$, $a, b \in A$ имеем

$$x \cdot (y \cdot a) = (xy) \cdot a,\quad x \cdot (a + b) = x \cdot a + x \cdot b,$$
$$e \cdot a = a,\quad x \cdot 0 = 0.$$

Заметим, что когда группа G действует на себе посредством сопряжений, то G действует на себе не только как на множестве, но и как на объекте в категории групп, т. е. перестановки, индуцированные этим действием, в действительности являются автоморфизмами групп.

Аналогично мы введем позднее другие категории (колец, модулей, полей), и у нас уже есть общее определение того, что следует понимать под действием группы на объекте в любой из этих категорий.

Пусть $\mathscr{A}$ — категория. Мы можем взять в качестве объектов новой категории $\mathscr{C}$ морфизмы из $\mathscr{A}$. Если $f\colon A \to B$ и $f'\colon A' \to B'$ — два морфизма из $\mathscr{A}$ (и, следовательно, объекты из $\mathscr{C}$), то мы

определяем морфизм $f \to f'$ (в $\mathscr{C}$) как пару морфизмов (φ, ψ) из $\mathscr{A}$, для которых следующая диаграмма коммутативна:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ A' & \xrightarrow{f'} & B' \end{array}$$

Ясно, что $\mathscr{C}$ — категория (строго говоря, как и в случае отображений множеств, следовало бы снабжать (φ, ψ) индексами f и f', но на практике такая индексация опускается).

Имеется много вариаций на эту тему. Так, мы можем сосредоточить свое внимание на тех морфизмах из $\mathscr{A}$, у которых фиксирован исходный объект, или на тех, у которых фиксирован конечный объект.

Пусть, например, A — некоторый объект в $\mathscr{A}$, и пусть $\mathscr{A}_A$ — категория, объектами которой служат морфизмы

$$f\colon X \to A$$

из $\mathscr{A}$, для которых A — конечный объект. Морфизм в $\mathscr{A}_A$ из $f\colon X \to A$ в $g\colon Y \to A$ — это просто такой морфизм

$$h\colon X \to Y$$

из $\mathscr{A}$, что диаграмма

$$\begin{array}{ccc} X & \xrightarrow{h} & Y \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle g} & \\ & A & \end{array}$$

коммутативна.

Пусть $\mathscr{A}$, $\mathscr{B}$ — категории. *Ковариантный функтор* F из $\mathscr{A}$ в $\mathscr{B}$ — это правило, сопоставляющее каждому объекту A в $\mathscr{A}$ некоторый объект $F(A)$ в $\mathscr{B}$ и каждому морфизму $f\colon A \to B$ — морфизм $F(f)\colon F(A) \to F(B)$ таким образом, что выполняются следующие условия:

ФУН 1. Для всякого A из $\mathscr{A}$ имеем $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$.

ФУН 2. Если $f\colon A \to B$ и $g\colon B \to C$ — два морфизма из $\mathscr{A}$, то $F(g \circ f) = F(g) \circ F(f)$.

Пример. Сопоставив каждой группе G ее множество (сняв с него групповую структуру) и каждому групповому гомоморфизму сам этот гомоморфизм, рассматриваемый лишь с теоретико-множественной точки зрения, мы получим функтор из категории групп в категорию множеств. Такой функтор называется *стирающим* функтором.

Заметим, что всякий функтор преобразует изоморфизмы в изоморфизмы, так как $f \circ g = \mathrm{id}$ влечет $F(f) \circ F(g) = \mathrm{id}$.

Можно определить понятие *контравариантного функтора* из $\mathscr{A}$ в $\mathscr{B}$, используя то же самое условие ФУН 1 и обращая стрелки в условии ФУН 2, т. е. каждому морфизму $f\colon A \to B$ контравариантный функтор сопоставляет морфизм

$$F(f)\colon F(B) \to F(A)$$

(идущий в противоположном направлении) таким образом, что если

$$f\colon A \to B \text{ и } g\colon B \to C$$

— морфизмы в $\mathscr{A}$, то

$$F(g \circ f) = F(f) \circ F(g).$$

Иногда для обозначения функтора пишут f_* вместо $F(f)$ в случае ковариантного функтора и f^* — в случае контравариантного функтора.

Пример. Пусть $\mathscr{A}$ — некоторая категория и A — фиксированный объект в $\mathscr{A}$. Мы получим ковариантный функтор

$$M_A\colon \mathscr{A} \to \mathscr{S},$$

положив $M_A(X) = \operatorname{Mor}(A, X)$ для любого объекта X из $\mathscr{A}$.

Если $\varphi\colon X \to X'$ — морфизм, то возьмем в качестве

$$M_A(\varphi)\colon \operatorname{Mor}(A, X) \to \operatorname{Mor}(A, X')$$

отображение, задаваемое правилом

$$g \longmapsto \varphi \circ g$$

для любого $g \in \operatorname{Mor}(A, X)$,

$$A \xrightarrow{g} X \xrightarrow{\varphi} X'.$$

Аксиомы ФУН 1 и ФУН 2 проверяются тривиально.

Аналогично для каждого объекта B из $\mathscr{A}$ мы имеем контравариантный функтор

$$M^B\colon \mathscr{A} \to \mathscr{S},$$

такой, что $M^B(Y) = \operatorname{Mor}(Y, B)$. Если $\psi\colon Y' \to Y$ — морфизм, то

$$M^B(\psi)\colon \operatorname{Mor}(Y, B) \to \operatorname{Mor}(Y', B)$$

есть отображение, задаваемое правилом

$$f \longmapsto f \circ \psi$$

для любого $f \in \operatorname{Mor}(Y, B)$,

$$Y' \xrightarrow{\psi} Y \xrightarrow{f} B.$$

Предыдущие два функтора называются *представляющими функторами*.

Рассмотрим важный специальный случай, когда мы имеем дело с категорией групп. Если S — множество и G — группа, то, как мы отмечали в § 2, множество отображений $M(S, G)$ само есть группа. Если G, G' — две группы, то множество морфизмов $\mathrm{Mor}(G, G')$ в категории групп — это просто множество гомоморфизмов G в G'; оно будет обозначаться $\mathrm{Hom}(G, G')$. Заметим, что $\mathrm{Hom}(G, G')$ не будет, вообще говоря, группой, если G' — неабелева группа.

Отметим, кроме того, тот важный факт, что представляющие функторы приводят к гомоморфизмам. Рассмотрим, например, ковариантный представляющий функтор. Пусть S — множество, X, X' — группы и φ: $X \to X'$ — гомоморфизм групп. Имеем индуцированное отображение

$$M_S(\varphi)\colon\ M(S, X) \to M(S, X'),$$

задаваемое правилом $g \mapsto \varphi \circ g$. Если g, $h \in M(S, X)$, то для $x \in X$

$$\varphi \circ (gh)(x) = \varphi((gh)(x)) = \varphi(g(x)\,h(x)) = \varphi(g(x))\,\varphi(h(x)).$$

Следовательно, $M_S(\varphi)$ — гомоморфизм. Аналогичное утверждение справедливо и для контравариантного представляющего функтора.

Тот факт, что $\mathrm{Hom}(G, X)$ есть группа, когда обе группы G, X коммутативны, заслуживает особого внимания. Мы изучим коммутативный случай более детально, когда будем иметь дело с дуальными группами, и позднее, когда будем рассматривать двойственность векторных пространств. Эти разделы дают хорошие дополнительные примеры для обсуждаемых здесь понятий, и читатель может сразу обратиться к ним, если пожелает.

Как отметил Гротендик, представляющие функторы можно использовать, чтобы перенести определения некоторых структур на множествах в произвольные категории. Например, пусть $\mathcal{A}$ — категория и G — объект из $\mathcal{A}$. Мы говорим, что G — *групповой объект* в $\mathcal{A}$, если для каждого объекта X из $\mathcal{A}$ задана групповая структура на множестве $\mathrm{Mor}(X, G)$ таким образом, что сопоставление

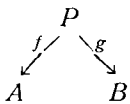
$$X \mapsto \mathrm{Mor}(X, G)$$

функториально (т. е. является функтором из категории $\mathcal{A}$ в категорию групп). Множество $\mathrm{Mor}(X, G)$ иногда обозначают через $G(X)$ и мыслят его как множество точек объекта G в X. За оправданием этой терминологии читатель отсылается к гл. X, § 3.

Другим примером может служить понятие произведения, определенное в категории множеств. Мы распространим это понятие на произвольные категории так, чтобы оно было согласовано с представляющими функторами.

Произведения и копроизведения

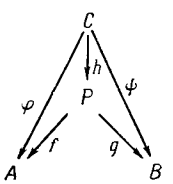
Пусть $\mathcal{A}$ — категория и A, B — объекты из $\mathcal{A}$. Под (*прямым*) *произведением* объектов A, B в $\mathcal{A}$ понимается тройка (P, f, g), состоящая из объекта P в $\mathcal{A}$ и двух морфизмов



и удовлетворяющая следующему условию. Если даны два морфизма в $\mathcal{A}$

$$\varphi\colon C \to A \quad \text{и} \quad \psi\colon C \to B,$$

то существует единственный морфизм $h\colon C \to P$, для которого следующая диаграмма коммутативна:



другими словами, $\varphi = f \circ h$ и $\psi = g \circ h$. Более общо, если дано семейство объектов $\{A_\iota\}_{\iota \in I}$ в $\mathcal{A}$, то (*прямое*) *произведение* этого семейства есть пара $(P, \{f_\iota\}_{\iota \in I})$, где P — объект в $\mathcal{A}$ и $\{f_\iota\}_{\iota \in I}$ — семейство морфизмов

$$f_\iota\colon P \to A_\iota,$$

удовлетворяющая следующему условию Для каждого семейства морфизмов

$$g_\iota\colon C \to A_\iota$$

существует единственный морфизм h. $C \to P$, такой, что $f_\iota \circ h = g_\iota$ для всех ι.

Пример. Пусть $\mathcal{A}$ — категория множеств. Пусть, далее, $\{A_\iota\}_{\iota \in I}$ — некоторое семейство множеств, $P = \prod_{\iota \in I} A_\iota$ — их декартово произведение и $f_\iota\colon P \to A_\iota$ — проекция на ι-множитель. Тогда $(P, \{f_\iota\})$ очевидным образом удовлетворяет требованиям, налагаемым на произведение в категории множеств.

Что касается обозначений, то произведение двух объектов в категории мы будем обычно записывать в виде $A \times B$, а произведение произвольного семейства объектов — в виде $\prod_{\iota \in I} A_\iota$, т. е. используя

те же самые обозначения, что и в категории множеств. В следующем параграфе мы исследуем произведения в категории групп.

Нам придется также встречаться с дуальным понятием. Пусть $\{A_i\}_{i\in I}$ — семейство объектов в категории $\mathcal{A}$. Под их *копроизведением* понимается пара $(S, \{f_i\}_{i\in I})$, состоящая из объекта S и семейства морфизмов

$$\{f_i\colon A_i \to S\},$$

удовлетворяющая следующему условию. Для каждого семейства морфизмов $\{g_i\colon A_i \to C\}$ существует единственный морфизм $h\colon S \to C$, такой, что $h \circ f_i = g_i$ для всех i.

Как в случае произведения, так и в случае копроизведения, морфизм h называется морфизмом, *индуцированным* семейством $\{g_i\}$.

Примеры. Пусть $\mathcal{S}$ — категория множеств. *В этой категории существуют копроизведения.* Например, пусть S, S' — множества, и пусть T — множество, имеющее ту же мощность, что и S', и не пересекающееся с S. Пусть $f_1\colon S \to S$ — тождественное отображение и $f_2\colon S' \to T$ — некоторая биекция. Пусть U — объединение S и T. Тогда (U, f_1, f_2) есть копроизведение для S, S', причем f_1, f_2 рассматриваются как отображения в U.

Пусть $\mathcal{S}_0$ — категория пунктированных множеств. Ее объекты состоят из пар (S, x), где S — множество, а x — некоторый его элемент. Морфизм из (S, x) в (S', x') в этой категории — это такое отображение $g\colon S \to S'$, что $g(x) = x'$. *Копроизведение для (S, x) и (S', x') в этой категории существует* и может быть построено следующим образом. Обозначим через T объединение x и множества той же мощности, что и дополнение к x' в S', такого, что $T \cap S = \{x\}$. Пусть $U = S \cup T$ и

$$f_1\colon (S, x) \to (U, x)$$

— отображение, индуцированное тождественным отображением множества S. Пусть, далее,

$$f_2\colon (S', x') \to (U, x)$$

— отображение, переводящее x' в x и индуцирующее некоторую биекцию $S' - \{x'\}$ на $T - \{x\}$. Тогда тройка

$$((U, x), f_1, f_2)$$

есть копроизведение для (S, x) и (S', x') в категории пунктированных множеств.

Аналогичными конструкциями могут быть получены копроизведения произвольных семейств множеств или пунктированных множеств. Категория пунктированных множеств особенно важна в теории гомотопий.

Пусть $\mathscr{C}$ — некоторая категория. Объект P в $\mathscr{C}$ называется *универсально притягивающим*, если существует единственный морфизм каждого объекта из $\mathscr{C}$ в P, и называется *универсально отталкивающим*, если для каждого объекта из $\mathscr{C}$ существует единственный морфизм P в этот объект.

Когда смысл ясен из контекста, мы будем называть такой объект P просто *универсальным*. Так как универсальный объект обладает тождественным морфизмом в себя, то ясно, что если P, P' — два универсальных объекта в $\mathscr{C}$, то между ними существует однозначно определенный изоморфизм.

Посмотрим теперь, как это применяется, скажем, к копроизведению. Пусть $\mathscr{A}$ — категория и $\{A_\iota\}$ — семейство объектов в $\mathscr{A}$. Определим новую категорию $\mathscr{C}$, взяв в качестве ее объектов семейства морфизмов $\{f_\iota\colon A_\iota \to B\}_{\iota \in I}$. Если даны два таких семейства

$$\{f_\iota\colon A_\iota \to B\} \quad \text{и} \quad \{f'_\iota\colon A_\iota \to B'\},$$

то морфизмом первого объекта во второй будет по определению морфизм $\varphi\colon B \to B'$ в $\mathscr{A}$, такой, что $\varphi \circ f_\iota = f'_\iota$ для всех i. Тогда копроизведение семейства $\{A_\iota\}$ — это просто универсальный объект в $\mathscr{C}$.

Копроизведение семейства $\{A_\iota\}$ будет обозначаться так:

$$\coprod_{\iota \in I} A_\iota.$$

Копроизведение двух объектов A, B будет также обозначаться через

$$A \coprod B.$$

Из предположения единственности вытекает, что копроизведение определено однозначно (с точностью до однозначно определенного изоморфизма). Аналогичное замечание справедливо и для прямого произведения.

§ 8. *Свободные группы*

Пусть I — некоторое множество, и для каждого $i \in I$ пусть G_ι — некоторая группа Пусть $G = \prod G_\iota$ — теоретико-множественное произведение множеств G_ι. Тогда G — это множество всех семейств $(x_\iota)_{\iota \in I}$, где $x_\iota \in G_\iota$. Мы можем определить на G групповую структуру посредством покомпонентного умножения; именно, если $(x_\iota)_{\iota \in I}$ и $(y_\iota)_{\iota \in I}$ — два элемента из G, то их произведением считаем семейство $(x_\iota y_\iota)_{\iota \in I}$. Обратным к $(x_\iota)_{\iota \in I}$ будет $(x_\iota^{-1})_{\iota \in I}$. Ясно, что при этом G — группа и что проекции

$$f_\iota\colon G \to G_\iota$$

являются гомоморфизмами. Поскольку G — теоретико-множественное произведение для G_i, то получаем

Предложение 5. *Группа $\prod G_i$ вместе с гомоморфизмами проектирования образует произведение семейства $\{G_i\}_{i\in I}$ в категории групп.*

Действительно, если $\{g_i\colon G' \to G_i\}_{i\in I}$ — семейство гомоморфизмов, то существует единственный гомоморфизм $g\colon G' \to \prod G_i$, для которого коммутативна требуемая диаграмма. Это — гомоморфизм, определяемый равенством $g(x')_i = g_i(x')$ для $x' \in G'$ и всякого $i \in I$.

Заметим, что каждая группа G_j допускает инъективный гомоморфизм в произведение на его j-ю компоненту, а именно отображение $\lambda_j\colon G_j \to \prod_i G_i$, такое, что i-я компонента элемента $\lambda_j(x)$ для всякого $x \in G_j$ равна единичному элементу группы G_i, если $i \neq j$, и равна самому x, если $i = j$. Это вложение будет называться *каноническим*.

Имеется полезный критерий того, что группа есть прямое произведение своих подгрупп.

Предложение 6. *Пусть G — группа и H, K — две такие ее подгруппы, что $H \cap K = e$, $HK = G$ и $xy = yx$ для всех $x \in H$ и $y \in K$. Тогда отображение*

$$H \times K \to G,$$

при котором $(x, y) \mapsto xy$, есть изоморфизм.

Доказательство. Это отображение, очевидно, гомоморфизм, и притом сюръективный, так как $HK = G$. Если (x, y) принадлежит его ядру, то $x = y^{-1}$, так что x лежит сразу и в H, и в K, а потому $x = e$, следовательно, также $y = e$ и наше отображение — изоморфизм.

Заметим, что предложение 6 обобщается по индукции на любое конечное число подгрупп $H_1, \ldots, H_n$, попарно коммутирующих друг с другом и таких, что $H_1 \ldots H_n = G$ и

$$H_{i+1} \cap (H_1 \ldots H_i) = e.$$

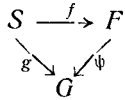
В этом случае группа G изоморфна прямому произведению

$$H_1 \times \ldots \times H_n.$$

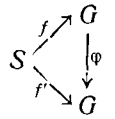
Пусть G — группа и S — подмножество в G. Напомним, что G *порождается* множеством S, если каждый элемент из G может быть записан в виде конечного произведения элементов из S и их обратных (причем пустое произведение всегда представляет единичный элемент G). Элементы из S называются тогда *образующими*. Если в группе G существует конечное множество образующих, то мы на-

зываем ее *конечно порожденной*. Пусть S — некоторое множество. Мы говорим, что отображение $\varphi\colon S \to G$ *порождает* G, если его образ порождает G.

Пусть $f\colon S \to F$ — отображение множества S в некоторую группу, $g\colon S \to G$ — другое такое отображение. Если $f(S)$ (или, как мы условились говорить, f) порождает F, то, очевидно, существует самое большее один гомоморфизм ψ группы F в G, для которого коммутативна следующая диаграмма:



Рассмотрим теперь категорию $\mathscr{C}$, объектами которой являются отображения множества S в группы. Если $f : S \to G$ и $f'\colon S \to G'$ — два объекта в этой категории, то под морфизмом из f в f' мы понимаем гомоморфизм $\varphi\colon G \to G'$, для которого $\varphi \circ f = f'$, т. е. для которого коммутативна диаграмма



Под *свободной группой*, определенной множеством S, мы будем понимать универсальный объект в этой категории.

Предложение 7. *Для всякого множества S существует определенная им свободная группа (F, f). При этом отображение f инъективно и порождает группу F.*

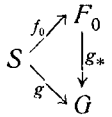
Доказательство (я обязан этим доказательством Ж. Титсу). Ради простоты мы сначала проведем доказательство для случая, когда S конечно. Пусть T — бесконечное счетное множество, Γ — множество всех групповых структур на T и T_γ — соответствующая группа для каждого $\gamma \in \Gamma$. Обозначим через M_γ множество всех отображений множества S в T_γ. Пусть $T_{\gamma,\varphi}$ — теоретико-множественное произведение группы T_γ и множества $\{\varphi\}$, состоящего из одного элемента; таким образом, φ используется как индекс, так что $T_{\gamma,\varphi}$ — это „та же самая“ группа, что и T_γ, но занумерованная посредством φ. Введем декартово произведение

$$F_0 = \prod_{\gamma \in \Gamma} \prod_{\varphi \in M_\gamma} T_{\gamma,\varphi}$$

групп $T_{\gamma,\varphi}$. Определим отображение

$$f_0\colon S \to F_0,$$

переводя S в множитель $T_{\gamma, \varphi}$ посредством φ. Мы утверждаем, что для каждого отображения $g\colon S \to G$ множества S в произвольную группу G существует гомоморфизм $g_*\colon F_0 \to G$, такой, что коммутативна обычная диаграмма



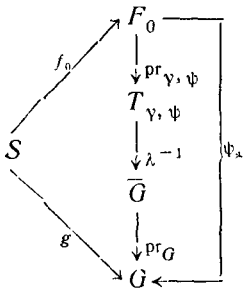
т. е. $g_* \circ f_0 = g$. *Для доказательства заметим сначала, что можно* предполагать, что g порождает G, просто ограничившись рассмотрением подгруппы в G, порожденной образом g. В этом случае $\operatorname{card} G \leqslant \operatorname{card} T$. Пусть $\overline{G}$ — произведение группы G и группы целых чисел $\mathbf{Z}$, так что $\operatorname{card}(\overline{G}) = \operatorname{card}(T)$. Тогда для некоторого $\gamma \in \Gamma$ существует изоморфизм

$$\lambda\colon \overline{G} \to T_\gamma$$

и G естественным образом вкладывается в $\overline{G} = G \times \mathbf{Z}$ как прямой сомножитель. Обозначим это вложение через h, так что $h(G) = G \times \{0\}$. Мы имеем теперь следующую последовательность гомоморфизмов и отображений:

$$S \xrightarrow{g} G \xrightarrow{h} \overline{G} = G \times \mathbf{Z} \xrightarrow{\lambda} T_\gamma.$$

Пусть $\psi = \lambda \circ h \circ g$ — их композиция. Тогда $\psi \in M_\gamma$, и мы можем рассматривать ψ как отображение множества S в $T_{\gamma, \psi}$. Положим $\psi_* = \mathrm{pr}_G \circ \lambda^{-1} \circ \mathrm{pr}_{\gamma, \psi}$, где $\mathrm{pr}_{\gamma, \psi}$ — проекция группы F_0 на множитель $T_{\gamma, \psi}$. Из определений немедленно вытекает, что следующая диаграмма коммутативна:



Обозначим через F подгруппу в F_0, порожденную образом f_0, и через f — отображение f_0, рассматриваемое как отображение множества S в F. Пусть g_* — ограничение ψ_* на F. Непосредственно видно, что g_* — единственное отображение, приводящее к нужной

нам коммутативной диаграмме, следовательно, (F, f) — искомая свободная группа. Кроме того, ясно, что отображение f инъективно.

Предположим теперь, что S не является конечным. Тогда легко так подобрать мощности, чтобы доказательство осталось справедливым. Именно, положим $T = S$ и возьмем за $\bar{G}$ произведение группы G с прямой суммой (см. § 9) достаточного числа экземпляров группы Z, так чтобы было снова $\operatorname{card}(\bar{G}) = \operatorname{card}(T)$. В остальном доказательство проходит, как и прежде.

Отберем для каждого множества S одну свободную группу, определяемую S, и обозначим ее через $(F(S), f_S)$ или, короче, через $F(S)$. Она порождается образом отображения f_S. Множество S можно рассматривать как содержащееся в $F(S)$; тогда элементы из S называются *свободными образующими* группы $F(S)$. Если $g\colon S \to G$ — некоторое отображение, то мы будем обозначать через $g_*\colon F(S) \to G$ гомоморфизм, реализующий универсальность нашей свободной группы $F(S)$.

Пусть $\lambda\colon S \to S'$ — отображение одного множества в другое и $F(\lambda)\colon F(S) \to F(S')$ — отображение $(f_{S'} \circ \lambda)_*$:

$$\begin{array}{ccc} S & \xrightarrow{f_S} & F(S) \\ {\scriptstyle\lambda}\downarrow & \searrow & \downarrow{\scriptstyle F(\lambda)} \\ S' & \xrightarrow[f_{S'}]{} & F(S') \end{array}$$

Мы можем, таким образом, рассматривать F как функтор из категории множеств в категорию групп (функториальные свойства проверяются тривиально, проверка предоставляется читателю).

Если λ сюръективно, то $F(\lambda)$ также сюръективно. Доказательство снова предоставляется читателю.

Если два множества S, S' имеют одинаковую мощность, то они изоморфны в категории множеств (так как изоморфизм в этом случае — биекция!), и, следовательно, группа $F(S)$ изоморфна группе $F(S')$. Если S состоит из n элементов, то мы называем $F(S)$ *свободной группой с n образующими*.

Пусть G — группа и S — то же самое множество, что и G (т. е. G рассматривается как множество без групповой структуры). Имеем тождественное отображение $g\colon S \to G$ и, следовательно, сюръективный гомоморфизм

$$g_*\colon F(S) \to G,$$

который будет называться *каноническим*. Таким образом, всякая группа есть факторгруппа свободной группы.

Группы можно строить также с помощью, как говорят, *образующих* и *соотношений*. Пусть S — множество и $F(S)$ — свободная группа. Будем считать, что $f\colon S \to F(S)$ — вложение. Пусть R —

некоторое множество элементов из $F(S)$. Каждый элемент из R может быть записан в виде конечного произведения

$$\prod_{\nu=1}^{n} x_\nu,$$

где каждое x_ν есть элемент из S или обратный для элемента из S. Пусть N — наименьшая нормальная подгруппа в $F(S)$, содержащая R, т. е. пересечение всех нормальных подгрупп в $F(S)$, содержащих R. Тогда $F(S)/N$ будет называться группой, *определенной образующими S и соотношениями R*.

Пример. Легко показать, что группа, определенная одной образующей a и соотношением $\{a^2\}$, имеет порядок 2. В упражнениях в конце главы предложены менее тривиальные примеры.

Канонический гомоморфизм φ: $F(S) \to F(S)/N$ удовлетворяет (очевидно) свойству универсальности относительно тех гомоморфизмов ψ группы $F(S)$ в группы G, для которых $\psi(x) = 1$ для всех $x \in R$. Ввиду этого группу $F(S)/N$ иногда называют группой, определенной образующими S и соотношениями $x = 1$ (для всех $x \in R$). Например, группа из предыдущего примера могла бы быть названа группой, определенной образующей a и соотношением $a^2 = 1$.

Предложение 8. *Копроизведения в категории групп существуют.*

Доказательство. Пусть $\{G_i\}_{i \in I}$ — семейство групп. Рассмотрим категорию $\mathscr{C}$, объектами которой являются семейства гомоморфизмов групп

$$\{g_i\colon\ G_i \to G\}_{i \in I},$$

с очевидными морфизмами. Нам нужно найти универсальный объект в этой категории. Для каждого индекса i возьмем за S_i то же самое множество, что и G_i, если G_i бесконечно, и произвольное счетное множество, если G_i конечно. Пусть S — множество, имеющее ту же мощность, что и теоретико-множественное объединение попарно не пересекающихся множеств S_i (т. е. их копроизведение в категории множеств). Пусть Γ — множество групповых структур на S и Φ_γ для каждого $\gamma \in \Gamma$ — множество всевозможных семейств гомоморфизмов

$$\varphi = \{\varphi_i\colon\ G_i \to S_\gamma\}.$$

Каждая пара (S_γ, φ), где $\varphi \in \Phi_\gamma$, есть группа (φ использовано только как индекс). Положим

$$F_0 = \prod_{\gamma \in \Gamma} \prod_{\varphi \in \Phi_\gamma} (S_\gamma, \varphi)$$

и для каждого i определим гомоморфизм f_i: $G_i \to F_0$ следующим предписанием: его компонента для каждого множителя (S_γ, φ) совпадает с соответствующей компонентой гомоморфизма φ_i.

Пусть теперь $g = \{g_i\colon G_i \to G\}$ — некоторое семейство гомоморфизмов. Заменяя G, если необходимо, подгруппой, порожденной образами гомоморфизмов g_i, мы видим, что $\operatorname{card}(G) \leqslant \operatorname{card}(S)$, поскольку всякий элемент из G есть *конечное* произведение элементов из этих образов. Вложив G как множитель в произведение с достаточно большим набором экземпляров группы $\mathbf{Z}$, мы можем предполагать, что $\operatorname{card}(G) = \operatorname{card}(S)$. Существует гомоморфизм g_*: $F_0 \to G$, такой, что

$$f_i \circ g_* = g_i$$

для всех i. Действительно, мы можем без потери общности предполагать, что $G = S_\gamma$ для некоторого γ и $g = \psi$ для некоторого $\psi \in \Phi_\gamma$. В качестве g_* возьмем проекцию F_0 на множитель (S_γ, ψ).

Пусть F — подгруппа в F_0, порожденная объединением образов отображений f_i по всем i. Ограничение g_* на F есть единственный гомоморфизм, удовлетворяющий соотношениям $f_i \circ g_* = g_i$ для всех i, и наш универсальный объект, таким образом, построен.

Я обязан Эйленбергу изящным доказательством следующего предложения:

Предложение 9. *Пусть A и B — две группы, теоретико-множественное пересечение которых есть $\{1\}$. Существует группа $A \circ B$, содержащая A и B в качестве подгрупп с тривиальным пересечением $A \cap B = \{1\}$ и обладающая следующим свойством. Всякий элемент $\neq 1$ из $A \circ B$ допускает единственное представление в виде произведения*

$$a_1 \dots a_n \qquad (n \geqslant 1,\ a_i \neq 1 \quad \text{для всех} \quad i),$$

где $a_i \in A$ или $a_i \in B$, причем если $a_i \in A$, то $a_{i+1} \in B$, а если $a_i \in B$, то $a_{i+1} \in A$.

Доказательство. Возьмем в качестве $A \circ B$ множество последовательностей

$$a = (a_1, \dots, a_n) \qquad (n \geqslant 0),$$

таких, что либо $n = 0$, и последовательность пуста, либо $n \geqslant 1$, и тогда элементы последовательности принадлежат A или B и все $\neq 1$, причем никакие два соседних элемента последовательности не принадлежат одновременно ни A, ни B. Пусть $b = (b_1, \dots, b_m)$. Определим произведение ab как последовательность

$(a_1, \dots, a_n, b_1, \dots, b_m)$, если $a_n \in A$, $b_1 \in B$ или $a_n \in B$, $b_1 \in A$,

$(a_1, \dots, a_n b_1, \dots, b_m)$, если a_n, $b_1 \in A$ или a_n, $b_1 \in B$ и $a_n b_1 \neq 1$,

$(a_1, \dots, a_{n-1})(b_2, \dots, b_m)$ (определено по индукции),

если a_n, $b_1 \in A$ или a_n, $b_1 \in B$ и $a_n b_1 = 1$.

Случай, когда $n=0$ или $m=0$, охватывается первым случаем, при этом пустая последовательность служит единичным элементом в $A\circ B$. Ясно, что

$$(a_1, \ldots, a_n)(a_n^{-1}, \ldots, a_1^{-1}) = \text{единичный элемент},$$

так что в проверке нуждается только ассоциативность. Пусть $c = (c_1, \ldots, c_r)$.

Рассмотрим сначала случай, когда $m=0$, т. е. последовательность b пуста. Тогда, очевидно, $(ab)c = a(bc)$. То же самое будет, если $n=0$ или $r=0$. Теперь рассмотрим случай $m=1$. Пусть $b=(x)$, где $x\in A$, $x\neq 1$. Тогда в каждом возможном случае проверяется, что $(ab)c = a(bc)$. Вот эти случаи:

$(a_1, \ldots, a_n, x, c_1, \ldots, c_r)$,	если $a_n\in B$ и $c_1\in B$,
$(a_1, \ldots, a_n x, c_1, \ldots, c_r)$,	если $a_n\in A$, $a_n x\neq 1$, $c_1\in B$,
$(a_1, \ldots, a_n, xc_1, \ldots, c_r)$,	если $a_n\in B$, $c_1\in A$, $xc_1\neq 1$,
$(a_1, \ldots, a_{n-1})(c_1, \ldots, c_r)$,	если $a_n = x^{-1}$ и $c_1\in B$,
$(a_1, \ldots, a_n)(c_2, \ldots, c_r)$,	если $a_n\in B$ и $c_1 = x^{-1}$,
$(a_1, \ldots, a_{n-1}, a_n xc_1, c_2, \ldots, c_r)$,	если $a_n, c_1\in A$, $a_n xc_1\neq 1$,
$(a_1, \ldots, a_{n-1})(c_2, \ldots, c_r)$,	если $a_n, c_1\in A$ и $a_n xc_1 = 1$.

При $m>1$ применяем индукцию. Записав последовательность в виде $b=b'b''$, где b' и b'' — более короткие последовательности, получим

$$(ab)c = (a(b'b''))c = ((ab')b'')c = (ab')(b''c),$$
$$a(bc) = a((b'b'')c) = a(b'(b''c)) = (ab')(b''c),$$

что и требовалось показать.

Мы имеем очевидные вложения групп A и B в $A\circ B$ и, отождествляя A, B с их образами в $A\circ B$, получаем доказательство нашего предложения.

По индукции можно доказать аналогичный результат для нескольких множителей. В частности, для свободной группы получаем

Следствие 1. *Пусть $F(S)$ — свободная группа, определенная множеством S, и $x_1, \ldots, x_n$ — различные элементы из S. Пусть $\nu_1, \ldots, \nu_r$ — целые числа $\neq 0$ и $i_1, \ldots, i_r$ — такие целые числа,*

$$1\leqslant i_1, \ldots, i_r\leqslant n,$$

что $i_j\neq i_{j+1}$ для $j=1, \ldots, r-1$. Тогда

$$x_{i_1}^{\nu_1}, \ldots, x_{i_r}^{\nu_r}\neq 1.$$

Доказательство. Пусть $G_1, \ldots, G_n$ — циклические группы, порожденные элементами $x_1, \ldots, x_n$. Рассмотрим группу $G = G_1\circ \ldots \circ G_n$. Пусть

$$F(S)\to G$$

— гомоморфизм, переводящий каждый элемент x_i в себя, а все другие элементы из S — в единичный элемент группы G. Наше утверждение теперь очевидно.

Следствие 2. *Пусть S — множество из n элементов $x_1, \ldots, x_n$, $n \geqslant 1$, и $G_1, \ldots, G_n$ — бесконечные циклические группы, порожденные этими элементами. Тогда отображение*

$$F(S) \to G_1 \circ \ldots \circ G_n,$$

переводящее каждое x_i в себя, является изоморфизмом.

Доказательство. Это отображение, очевидно, сюръективно и инъективно.

Следствие 3. *Пусть $G_1, \ldots, G_n$ — группы. Гомоморфизм*

$$G_1 \coprod \ldots \coprod G_n \to G_1 \circ \ldots \circ G_n$$

их копроизведения в $G_1 \circ \ldots \circ G_n$, индуцированный естественными вложениями $G_i \to G_1 \circ \ldots \circ G_n$, является изоморфизмом.

Доказательство. Опять-таки очевидно, что этот гомоморфизм инъективен и сюръективен.

§ 9. Прямые суммы и свободные абелевы группы

Абелевы группы образуют категорию, которую можно обозначить символом *Ab*. Заметим, что если $\{A_i\}_{i \in I}$ — семейство абелевых групп, то их произведение в категории групп является также произведением в категории абелевых групп, т. е. если мы образуем теоретико-множественное произведение

$$\prod_{i \in I} A_i$$

и наделим его структурой группы с помощью покомпонентного умножения, то оно станет абелевой группой, обладающей необходимым свойством универсальности.

Копроизведение в категории абелевых групп обычно называется прямой суммой.

Предложение 10. *Прямые суммы в категории абелевых групп существуют.*

Доказательство. Пусть $\{A_i\}_{i \in I}$ — семейство абелевых групп. Рассмотрим подмножество A прямого произведения $\prod A_i$, состоящее из всех семейств $(x_i)_{i \in I}$, $x_i \in A_i$, таких, что $x_i = 0$ для всех, кроме

конечного числа индексов i. Ясно, что A — подгруппа в произведении. Для каждого индекса $j \in I$ мы определим отображение

$$\lambda_j\colon\ A_j \to A,$$

положив $\lambda_j(x)$ равным элементу из A, j-я компонента которого есть x, а все остальные компоненты равны 0. Очевидно, λ_j — инъективный гомоморфизм. Мы утверждаем, что A вместе с семейством отображений $\{\lambda_i\}_{i\in I}$ есть прямая сумма семейства $\{A_i\}$. Пусть $\{f_i\colon\ A_i \to B\}$ — произвольное семейство гомоморфизмов в абелеву группу B. Определим отображение

$$f\colon\ A \to B$$

формулой

$$f\left((x_i)_{i\in I}\right) = \sum_{i\in I} f_i(x_i).$$

Сумма справа в действительности конечная, так как в ней все члены, кроме конечного числа, равны 0. Непосредственно проверяется, что отображение f — гомоморфизм. Кроме того, ясно, что $f \circ \lambda_j(x) = f_j(x)$ для всякого j и всякого $x \in A_j$. Таким образом, f удовлетворяет необходимому условию коммутативности. Ясно также, что отображение f однозначно определено, чем доказательство и завершено.

Заметим, что в случае конечного множества I прямая сумма и прямое произведение совпадают.

Пусть A — абелева группа и B, C — её подгруппы. Если $B + C = A$ и $B \cap C = 0$, то отображение

$$B \times C \to A,$$

задаваемое правилом $(x, y) \mapsto x + y$, является изоморфизмом (мы уже отмечали это в некоммутативном случае). Вместо записи $A = B \times C$ мы будем писать

$$A = B \oplus C$$

и говорить, что A — *прямая сумма* B и C. Аналогичное обозначение используется и для прямой суммы любого конечного числа подгрупп $B_1, \ldots, B_n$, таких, что $B_1 + \ldots + B_n = A$ и

$$B_{i+1} \cap (B_1 + \ldots + B_i) = 0.$$

В этом случае пишем

$$A = B_1 \oplus \ldots \oplus B_n.$$

Пусть теперь S — множество и $\mathscr{C}$ — категория, объектами которой являются отображения $f\colon\ S \to A$ множества S в абелевы группы, с очевидным образом определяемыми морфизмами: если $f\colon\ S \to A$ и $f'\colon\ S \to A'$ — два отображения в абелевы группы, то морфизм из f

в f' — это гомоморфизм (групп) g: $A \to A'$, такой, что коммутативна обычная диаграмма, т. е. $g \circ f = f'$. Универсальный объект этой категории $\mathscr{C}$ называется *свободной абелевой группой*, порожденной множеством S. Мы увидим, что *такой объект всегда существует*.

Действительно, пусть $\mathbf{Z}\langle S\rangle$ — множество всех отображений φ: $S \to \mathbf{Z}$, таких, что $\varphi(x) = 0$ для почти всех $x \in S$. Тогда $\mathbf{Z}\langle S\rangle$ — абелева группа (сложением в которой служит обычное сложение отображений). Пусть k — целое число и x — некоторый элемент из S. Мы обозначаем через $k \cdot x$ отображение φ, для которого $\varphi(x) = k$ и $\varphi(y) = 0$ при $y \neq x$. Очевидно, что всякий элемент φ из $\mathbf{Z}\langle S\rangle$ может быть записан в виде

$$\varphi = k_1 \cdot x_1 + \ldots + k_n \cdot x_n,$$

где k_i — некоторые целые числа и $x_i \in S$ $(i = 1, \ldots, n)$, причем все элементы x_i различны. Кроме того, φ *допускает единственное такое представление*, так как если

$$\varphi = \sum_{x \in S} k_x \cdot x = \sum_{x \in S} k'_x \cdot x,$$

то

$$0 = \sum_{x \in S} (k_x - k'_x) \cdot x,$$

откуда $k'_x = k_x$ для всех $x \in S$.

Вложим S в $\mathbf{Z}\langle S\rangle$ посредством отображения $f_S = f$, для которого $f(x) = 1 \cdot x$. Ясно, что f инъективно и что $f(S)$ порождает $\mathbf{Z}\langle S\rangle$. Для всякого отображения g: $S \to B$ множества S в абелеву группу B определим отображение

$$g_*\colon \mathbf{Z}\langle S\rangle \to B$$

формулой

$$g_*\Big(\sum_{x \in S} k_x \cdot x\Big) = \sum_{x \in S} k_x g(x).$$

Это отображение — гомоморфизм (тривиально), для которого соответствующая диаграмма коммутативна, т. е. $g_* \circ f = g$ (тоже тривиально). Это единственный гомоморфизм, обладающий указанным свойством, так как для всякого такого гомоморфизма g_* должно выполняться условие $g_*(1 \cdot x) = g(x)$. Таким образом, наш универсальный объект построен.

Обычно отождествляют S с его образом в $\mathbf{Z}\langle S\rangle$; иногда мы будем опускать точку и писать просто $k_x x$ или $\sum k_x x$.

Для всякого отображения λ: $S \to S'$ *одного множества в другое существует единственный гомоморфизм* $\bar{\lambda}$, *для которого*

коммутативна следующая диаграмма:

$$\begin{array}{ccc} S & \xrightarrow{f_S} & \mathbf{Z}\langle S\rangle \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\bar{\lambda}} \\ S' & \xrightarrow[f_{S'}]{} & \mathbf{Z}\langle S'\rangle \end{array}$$

Действительно, $\bar{\lambda}$ есть не что иное, как $(f_{S'} \circ \lambda)_*$ в обозначениях предыдущего параграфа. Доказательство этого утверждения предоставляется читателю в качестве тривиального упражнения.

Положим $F_{\mathrm{ab}}(S) = \mathbf{Z}\langle S\rangle$ и $\bar{\lambda} = F_{\mathrm{ab}}(\lambda)$. Очевидно, что F_{ab} есть функтор из категории множеств в категорию абелевых групп.

В качестве упражнения покажите, что всякая абелева группа A есть факторгруппа некоторой свободной абелевой группы F. Если A — конечно порожденная группа, то покажите, что и F можно выбрать конечно порожденной.

Если множество S состоит из n элементов, то мы будем говорить, что свободная абелева группа $F_{\mathrm{ab}}(S)$ есть свободная абелева группа с n образующими. Если S — множество из n символов $x_1, \ldots, x_n$, то мы скажем, что $F_{\mathrm{ab}}(S)$ — свободная абелева группа со свободными образующими $x_1, \ldots, x_n$.

Абелева группа называется *свободной*, если она изоморфна свободной абелевой группе $F_{ab}(S)$ для некоторого множества S. Пусть A — абелева группа, и пусть S — такое подмножество в A, что для любого данного $z \in A$ существует единственный набор целых чисел n_x, по одному для каждого $x \in S$, такой, что почти все $n_x = 0$ и

$$z = \sum_{x \in S} n_x x.$$

Тогда ясно, что группа A изоморфна свободной абелевой группе $F_{\mathrm{ab}}(S)$; мы называем S множеством *свободных образующих* группы A или также ее *базисом*. Аналогичным образом определяется понятие семейства свободных образующих.

Несколько слов об обозначениях. Если A — абелева группа и T — подмножество элементов из A, то мы обозначаем через $\langle T\rangle$ подгруппу, порожденную всеми элементами из T, т. е. наименьшую подгруппу в A, содержащую T.

Пример. *Группа Гротендика. Пусть M — коммутативный моноид, записываемый аддитивно. Существуют коммутативная группа $K(M)$, называемая группой Гротендика моноида M, и гомоморфизм моноидов*

$$\gamma\colon M \to K(M),$$

обладающие свойством универсальности относительно гомоморфизмов моноида M в коммутативные группы.

Доказательство. Пусть $F_{ab}(M)$ — свободная абелева группа, порожденная M. Обозначим через $[x]$ образующую группы $F_{ab}(M)$, соответствующую элементу $x \in M$. Пусть B — подгруппа, порожденная всеми элементами вида

$$[x + y] - [x] - [y],$$

где $x, y \in M$. Положим $K(M) = F_{ab}(M)/B$. Пусть, далее,

$$\gamma\colon M \to K(M)$$

— отображение, являющееся композицией вложения моноида M в $F_{ab}(M)$, задаваемого соответствием $x \longmapsto [x]$, и канонического отображения

$$F_{ab}(M) \to F_{ab}(M)/B.$$

Ясно, что γ — гомоморфизм, удовлетворяющий нужному свойству универсальности.

Будем говорить, что в M выполняется *закон сокращения*, если для любых $x, y, z \in M$, связанных соотношением $x + z = y + z$, имеем $x = y$.

Справедлив следующий важный критерий инъективности построенного выше универсального отображения γ.

Если в M выполняется закон сокращения, то каноническое отображение γ моноида M в его группу Гротендика инъективно.

Доказательство. Доказательство здесь по существу то же самое, что и при построении отрицательных целых чисел, исходя из натуральных. Рассмотрим пары (x, y), где $x, y \in M$, и скажем, что пара (x, y) эквивалентна паре (x', y'), если $y + x' = x + y'$. (Из справедливости закона сокращения вытекает, что это действительно отношение эквивалентности.) Сложение пар определим покомпонентно. Тогда классы эквивалентности пар образуют группу, нулевым элементом которой служит класс пары $(0, 0)$ [или класс пары (x, x) для любого $x \in M$]. Противоположным для элемента (x, y) является (y, x). Имеет место гомоморфизм

$$x \longmapsto \text{класс пары } (0, x).$$

Из закона сокращения сразу следует, что он инъективен. Таким образом, мы построили инъективный гомоморфизм моноида M в некоторую группу. Отсюда вытекает, что универсальный гомоморфизм также должен быть инъективен.

Мы рассмотрим позже несколько примеров универсальных групп $K(M)$.

Для данных абелевой группы A и ее подгруппы B иногда бывает желательно найти подгруппу C, такую, что $A = B \oplus C$. Следующая лемма дает нам условие, при котором это возможно.

Лемма. *Пусть $A \xrightarrow{f} A'$ — сюръективный гомоморфизм абелевых групп и B — ядро f. Тогда, если группа A' свободна, то в A существует подгруппа, такая, что ограничение f на C индуцирует изоморфизм C на A', и $A = B \oplus C$.*

Доказательство. Пусть $\{x'_i\}_{i \in I}$ — базис группы A', и для каждого $i \in I$ пусть x_i — какой-либо элемент из A, для которого $f(x_i) = x'_i$. Пусть C — подгруппа в A, порожденная всеми элементами x_i, $i \in I$. Если

$$\sum_{i \in I} n_i x_i = 0$$

для некоторых целых n_i, из которых почти все равны 0, то, применяя f, получаем

$$0 = \sum_{i \in I} n_i f(x_i) = \sum_{i \in I} n_i x'_i,$$

откуда все $n_i = 0$. Следовательно, наше семейство $\{x_i\}_{i \in I}$ — базис подгруппы C. Аналогичным образом, если $z \in C$ и $f(z) = 0$, то $z = 0$. Следовательно, $B \cap C = 0$. Пусть $x \in A$. Так как $f(x) \in A'$, то существуют целые числа n_i, $i \in I$, такие, что

$$f(x) = \sum_{i \in I} n_i x'_i.$$

Применяя f к $x - \sum_{i \in I} n_i x_i$, находим, что последний элемент лежит в ядре f, скажем

$$x - \sum_{i \in I} n_i x_i = b \in B.$$

Отсюда видно, что $x \in B + C$, и, следовательно, $A = B \oplus C$, что и утверждалось.

Теорема 4. *Пусть A — свободная абелева группа, B — некоторая ее подгруппа. Тогда B — также свободная абелева группа и мощность базиса $B \leqslant$ мощности базиса A. Любые два базиса B имеют одинаковую мощность, называемую рангом B.*

Доказательство. Мы дадим доказательство только для случая, когда A конечно порождена, скажем, базисом $\{x_1, \ldots, x_n\}$ $(n \geqslant 1)$; проводим доказательство индукцией по n. Имеем представление A в виде прямой суммы

$$A = \mathbf{Z}x_1 \oplus \ldots \oplus \mathbf{Z}x_n.$$

Пусть f: $A \to \mathbf{Z}x_1$ — проекция, т. е. гомоморфизм, для которого

$$f(m_1x_1 + \ldots + m_nx_n) = m_1x_1,$$

каковы бы ни были $m_i \in \mathbf{Z}$. Пусть B_1 — ядро ограничения f на B. Тогда B_1 содержится в свободной подгруппе $\langle x_2, \ldots, x_n\rangle$. По индукции B_1 свободна и имеет базис из $\leqslant n-1$ элементов. В силу леммы в B существует подгруппа C_1, изоморфная подгруппе в $\mathbf{Z}x_1$ (а именно, образу $f(B)$), такая, что

$$B = B_1 \oplus C_1.$$

Таким образом, $f(B)$ — либо 0, либо бесконечная циклическая группа, т. е. свободная группа с одной образующей. Это доказывает, что группа B — свободная.

(В случае когда A не является конечно порожденной, можно использовать аналогичное рассуждение с трансфинитной индукцией; мы предоставляем это читателю.)

Заметим, далее, что из предыдущего следует, что существует по меньшей мере один базис подгруппы B, мощность которого $\leqslant n$. Поэтому доказательство будет закончено, если мы покажем, что любые два базиса в B имеют одинаковую мощность. Пусть S — один базис с конечным числом элементов m, T — другой базис, содержащий по крайней мере r элементов. Достаточно доказать, что $r \leqslant m$ (затем можно воспользоваться симметрией). Пусть p — простое число. Тогда факторгруппа B/pB есть прямая сумма циклических групп порядка p, причем в сумме имеется m членов. Значит, порядок этой факторгруппы равен p^m. Используя базис T вместо S, заключаем, что B/pB содержит r-кратное произведение циклических групп порядка p, а потому $p^r \leqslant p^m$ и $r \leqslant m$, что и требовалось показать. (Отметим, что мы не предполагали a priori, что базис T конечен.)

§ 10. Конечно порожденные абелевы группы

Группы, названные в заглавии этого параграфа, встречаются так часто, что стоит установить теорему, полностью описывающую их структуру. В этом параграфе мы записываем наши абелевы группы аддитивно.

Пусть A — абелева группа. Элемент $a \in A$ называется *периодическим*, если он имеет конечный период. Подмножество всех периодических элементов из A является подгруппой в A, называемой *подгруппой кручения* группы A (если a имеет период m и b имеет период n, то $a \pm b$ имеет период, делящий mn).

Конечно порожденная периодическая абелева группа (группа, совпадающая со своей подгруппой кручения), очевидно, конечна. Мы начнем с изучения конечных абелевых групп. Пусть A — абелева группа и p — простое число. Мы обозначаем через $A(p)$ подгруппу

всех элементов $x \in A$, период которых есть степень p. Тогда $A(p)$ — периодическая группа, являющаяся p-группой, если она конечна.

Теорема 5. *Пусть A — конечная абелева группа. Тогда A является прямым произведением своих подгрупп $A(p)$ по всем простым p, таким, что $A(p) \neq 0$.*

Доказательство. Сначала рассмотрим случай абелевой группы A, показатель которой n может быть записан в виде произведения $n = mm'$, где m, m' — взаимно простые целые числа > 1. Существуют целые числа r, s, такие, что

$$rm + sm' = 1.$$

Поэтому

$$A = rmA + sm'A \subset mA + m'A \subset A,$$

откуда следует, что все символы включения нужно заменить на равенства. Если $a \in mA \cap m'A$, то $m'a = 0$ и $ma = 0$, откуда $a = rma + sm'a = 0$. Следовательно, A — прямое произведение подгрупп mA и $m'A$.

Пусть A_m обозначает подгруппу в A, состоящую из всех x, для которых $mx = 0$. Тогда $m'A \subset A_m$, так как $mm'A = 0$. Обратно, если $x \in A_m$, то $x = rmx + sm'x = m'sx$, так что $x \in m'A$. Следовательно, $m'A = A_m$ и аналогично $mA = A_{m'}$, так что окончательно

$$A = A_m \times A_{m'}.$$

По индукции заключаем, что A есть прямое произведение своих подгрупп $A(p)$, что и утверждается в теореме.

Наша следующая задача — описать структуру конечных абелевых p-групп. Пусть $r_1, \ldots, r_s$ — целые числа $\geqslant 1$. Конечная p-группа A называется группой *типа* $(p^{r_1}, \ldots, p^{r_s})$, если она изоморфна прямому произведению циклических групп порядков p^{r_i} $(i = 1, \ldots, s)$.

Теорема 6. *Всякая конечная абелева p-группа изоморфна прямому произведению циклических p-групп. Если она есть группа типа $(p^{r_1}, \ldots, p^{r_s})$, причем*

$$r_1 \geqslant r_2 \geqslant \ldots \geqslant r_s \geqslant 1,$$

то последовательность $(r_1, \ldots, r_s)$ определена однозначно.

Доказательство. Пусть A — конечная абелева p-группа. Нам потребуется следующее замечание. Пусть b — элемент из A, $b \neq 0$, k — целое число $\geqslant 0$, такое, что $p^k b \neq 0$, и пусть p^m — период элемента $p^k b$. Тогда b имеет период p^{k+m}. Доказательство: разумеется,

$p^{k+m}b=0$, а если $p^nb=0$, то, во-первых, $n\geqslant k$, а, во-вторых, $n\geqslant k+m$, так как иначе период элемента p^kb был бы меньше, чем p^m.

Теперь докажем существование искомого прямого произведения по индукции. Пусть $a_1\in A$ — некоторый элемент максимального периода. Не теряя общности, мы можем предполагать, что группа A — не циклическая. Пусть A_1 — циклическая подгруппа, порожденная элементом a_1, периода, скажем, p^{r_1}. Нам нужна лемма.

Лемма. *Пусть $\bar{b}$ — некоторый элемент из A/A_1 периода p^r. Тогда в A существует представитель a класса $\bar{b}$, также имеющий период p^r.*

Доказательство. Пусть b — произвольный представитель класса $\bar{b}$ в A. Тогда p^rb лежит в A_1, скажем, $p^rb=na_1$, где n — некоторое целое число. Заметим, что период $\bar{b}\leqslant$ периода b. Запишем $n=p^k\mu$, где μ взаимно просто с p. Тогда μa_1 также является образующей подгруппы A_1 и, следовательно, имеет период p^{r_1}. Мы можем предполагать, что $k\leqslant r_1$. Тогда $p^k\mu a_1$ имеет период p^{r_1-k}. В силу нашего предыдущего замечания элемент b имеет период

$$p^{r+r_1-k},$$

откуда по предположению $r+r_1-k\leqslant r_1$ и $r\leqslant k$. Это доказывает, что существует элемент $c\in A_1$, такой, что $p^rb=p^rc$. Пусть $a=b-c$. Тогда a есть представитель для $\bar{b}$ в A и $p^ra=0$. Так как период $(a)\geqslant p^r$, то заключаем, что a имеет период, равный p^r.

Возвращаемся к основному доказательству. По индукции факторгруппа A/A_1 допускает представление в виде произведения

$$A/A_1=\bar{A}_2\times\ldots\times\bar{A}_s$$

циклических подгрупп порядков $p^{r_2}, \ldots, p^{r_s}$ соответственно; мы можем предполагать, что $r_2\geqslant\ldots\geqslant r_s$. Пусть $\bar{a}_i$ — образующая для $\bar{A}_i$ $(i=2, \ldots, s)$ и a_i — ее представитель в A, имеющий тот же период, что и $\bar{a}_i$. Пусть A_i — циклическая подгруппа, порожденная элементом a_i. Мы утверждаем, что A есть прямое произведение подгрупп $A_1, \ldots, A_s$.

Для заданного элемента $x\in A$ обозначим через $\bar{x}$ его класс вычетов в A/A_1. Существуют целые числа m_i $(i=2, \ldots, s)$, для которых

$$\bar{x}=m_2\bar{a}_2+\ldots+m_s\bar{a}_s.$$

Следовательно, $x - m_2a_2 - \ldots - m_sa_s$ лежит в A_1 и существует целое число m_1, такое, что

$$x = m_1a_1 + m_2a_2 + \ldots + m_sa_s,$$

откуда $A_1 + \ldots + A_s = A$.

Предположим далее, что $m_1, \ldots, m_s$ — целые числа $\geqslant 0$, такие, что

$$0 = m_1a_1 + m_2a_2 + \ldots + m_sa_s.$$

Так как a_i имеет период p^{r_i} $(i = 1, \ldots, s)$, то мы можем считать, что $m_i < p^{r_i}$. Проводя черту над членами этого уравнения, получаем

$$0 = m_2\bar{a}_2 + \ldots + m_s\bar{a}_s.$$

Так как A/A_1 — прямое произведение подгрупп $\bar{A}_2, \ldots, \bar{A}_s$, то заключаем, что каждое $m_i = 0$ для $i = 2, \ldots, s$. Но тогда также и $m_1 = 0$ и, следовательно, все $m_i = 0$. Отсюда вытекает немедленно, что

$$(A_1 + \ldots + A_i) \cap A_{i+1} = 0$$

для каждого $i \geqslant 1$ и, следовательно, A — прямое произведение подгрупп $A_1, \ldots, A_s$, что и требовалось установить.

Единственность доказываем по индукции. Предположим, что группа A записана двумя способами в виде произведения циклических групп, т. е. имеет одновременно типы, скажем,

$$(p^{r_1}, \ldots, p^{r_s}) \quad \text{и} \quad (p^{m_1}, \ldots, p^{m_k}),$$

где $r_1 \geqslant \ldots \geqslant r_s \geqslant 1$ и $m_1 \geqslant \ldots \geqslant m_k \geqslant 1$. Тогда pA — также p-группа порядка, строго меньшего, чем порядок A, и типов

$$(p^{r_1-1}, \ldots, p^{r_s-1}) \quad \text{и} \quad (p^{m_1-1}, \ldots, p^{m_k-1}),$$

причем подразумевается, что если некоторый показатель r_i или m_j равен 1, то множитель, соответствующий

$$p^{r_i-1} \quad \text{или} \quad p^{m_j-1}$$

в pA, будет просто тривиальной группой 0. По индукции подпоследовательность в

$$(r_1 - 1, \ldots, r_s - 1),$$

состоящая из тех целых чисел, которые $\geqslant 1$, однозначно определена, и то же самое справедливо для соответствующей подпоследовательности в

$$(m_1 - 1, \ldots, m_k - 1).$$

Другими словами, мы имеем $r_i - 1 = m_i - 1$ для всех таких номеров i, что $r_i - 1$ или $m_i - 1 \geqslant 1$. Следовательно, $r_i = m_i$ для всех этих номеров i и две последовательности

$$(p^{r_1}, \ldots, p^{r_s}) \quad \text{и} \quad (p^{m_1}, \ldots, p^{m_k})$$

могут отличаться только своими последними членами, равными p. Эти члены, соответствующие множителям типа $(p, \ldots, p)$, встречаются, скажем, ν раз в первой последовательности и μ раз во второй последовательности. Тогда для некоторого целого n группа A имеет типы

$$(p^{r_1}, \ldots, p^{r_n}, \underbrace{p, \ldots, p}_{\nu \text{ раз}}) \quad \text{и} \quad (p^{r_1}, \ldots, p^{r_n}, \underbrace{p, \ldots, p}_{\mu \text{ раз}}).$$

Таким образом, ее порядок равен

$$p^{r_1 + \cdots + r_n} p^{\nu} = p^{r_1 + \cdots + r_n} p^{\mu},$$

откуда $\nu = \mu$, и наша теорема доказана.

Группа G называется *группой, свободной от кручения*, или *группой без кручения*, если единичный элемент является единственным элементом в G, имеющим конечный период.

Теорема 7. *Пусть A — конечно порожденная абелева группа без кручения. Тогда A — свободная.*

Доказательство. Предположим, что $A \neq 0$. Пусть S — конечное множество образующих и $x_1, \ldots, x_n$ — максимальное подмножество в S, обладающее тем свойством, что, каковы бы ни были целые числа $\nu_1, \ldots, \nu_n$, из

$$\nu_1 x_1 + \ldots + \nu_n x_n = 0$$

вытекают равенства $\nu_j = 0$ для всех j (заметим, что $n \geqslant 1$, так как $A \neq 0$). Пусть B — подгруппа, порожденная элементами $x_1, \ldots, x_n$. Тогда B свободна. В силу предположения о максимальности $x_1, \ldots, x_n$ для заданного $y \in A$ существуют целые числа $m_1, \ldots, m_n, m$, не все равные нулю, такие, что

$$my + m_1 x_1 + \ldots + m_n x_n = 0.$$

При этом $m \neq 0$, иначе все $m_j = 0$. Следовательно, my лежит в B. Это справедливо для каждого элемента y из конечного множества образующих группы A, откуда вытекает, что существует целое число $m \neq 0$, для которого $mA \subset B$. Отображение

$$x \longmapsto mx$$

группы A в себя — гомоморфизм, имеющий тривиальное ядро, поскольку A без кручения. Следовательно, это изоморфизм группы A

на подгруппу в B. В силу теоремы 4 предыдущего параграфа заключаем, что mA свободна, откуда и A свободна.

Теорема 8. *Пусть A — конечно порожденная абелева группа и A_t — ее подгруппа, состоящая из всех элементов, имеющих конечный период. Тогда A_t конечна и A/A_t свободна. При этом в A существует свободная подгруппа B, такая, что A есть прямая сумма A_t и B.*

Доказательство. Напомним, что конечно порожденная периодическая абелева группа очевидным образом конечна. Пусть A порождается n элементами, и пусть F — свободная абелева группа с n образующими. В силу свойства универсальности существует сюръективный гомоморфизм

$$F \xrightarrow{\varphi} A$$

группы F на A. Подгруппа $\varphi^{-1}(A_t)$ в F конечно порождена в силу теоремы 4. Следовательно, A_t сама конечно порождена и потому конечна.

Далее, докажем, что A/A_t не имеет кручения. Пусть $\bar{x}$ — некоторый элемент в A/A_t, такой, что $m\bar{x} = 0$ для некоторого целого $m \neq 0$. Тогда для любого представителя x класса $\bar{x}$ в A имеем $mx \in A_t$, откуда $qmx = 0$ для некоторого целого $q \neq 0$. Следовательно, $x \in A_t$, так что $\bar{x} = 0$ и A/A_t свободна от кручения. Значит, в силу теоремы 7 A/A_t свободна. Для завершения доказательства используем лемму к теореме 4.

Ранг факторгруппы A/A_t называется также *рангом* группы A.

§ 11. Дуальная группа

Пусть A — абелева группа показателя $m \geqslant 1$. Это означает, что $mx = 0$ для каждого элемента $x \in A$. Пусть Z_m — циклическая группа порядка m. Будем обозначать через A^* или через $\mathrm{Hom}(A, Z_m)$ группу гомоморфизмов группы A в Z_m и называть ее *дуальной* к A.

Пусть $f\colon A \to B$ — гомоморфизм абелевых групп, причем обе группы имеют показатель m. Тогда f индуцирует гомоморфизм

$$f^*\colon B^* \to A^*.$$

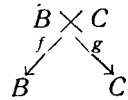
Именно, для каждого $\psi \in B^*$ полагаем $f^*(\psi) = \psi \circ f$. Тривиально проверяется, что f^* — гомоморфизм. Можно рассматривать $\mathrm{Hom}(A, Z_m)$ как контравариантный функтор на категории абелевых групп показателя m. Действительно, свойства

$$\mathrm{id}^* = \mathrm{id} \quad \text{и} \quad (f \circ g)^* = g^* \circ f^*$$

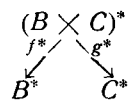
проверяются тривиально.

Теорема 9. *Если A — конечная абелева группа, представимая в виде произведения $A = B \times C$, то A^* изоморфна $B^* \times C^*$ (сам изоморфизм описан ниже). Всякая конечная абелева группа изоморфна своей дуальной.*

Доказательство. Рассмотрим две проекции



произведения $B \times C$ на две его компоненты. Рассмотрим гомоморфизмы



Мы утверждаем, что эти гомоморфизмы индуцируют изоморфизм $B^* \times C^*$ на $(B \times C)^*$.

Действительно, пусть ψ_1, ψ_2 лежат в $\mathrm{Hom}(B, Z_m)$ и $\mathrm{Hom}(C, Z_m)$ соответственно. Тогда пара $(\psi_1, \psi_2) \in B^* \times C^*$, и мы определим соответствующий ей элемент в $(B \times C)^*$, положив

$$(\psi_1, \psi_2)(x, y) = \psi_1(x) + \psi_2(y)$$

для $(x, y) \in B \times C$. Таким образом, получаем гомоморфизм

$$B^* \times C^* \to (B \times C)^*.$$

Обратно, пусть $\psi \in (B \times C)^*$. Тогда

$$\psi(x, y) = \psi(x, 0) + \psi(0, y).$$

Функция ψ_1, определенная на B условием $\psi_1(x) = \psi(x, 0)$, принадлежит B^*, и аналогично функция ψ_2, определенная на C условием $\psi_2(y) = \psi(0, y)$, принадлежит C^*. Таким образом, получаем гомоморфизм

$$(B \times C)^* \to B^* \times C^*,$$

очевидно, обратный гомоморфизму, определенному перед этим. Следовательно, мы получаем изоморфизм, что и доказывает первое утверждение нашей теоремы.

Мы можем записать любую конечную абелеву группу как произведение циклических групп. Таким образом, чтобы доказать второе утверждение, достаточно рассмотреть случай циклических групп.

Пусть A — циклическая группа, порожденная элементом x периода n. Тогда $n \mid m$ и Z_m имеет ровно одну циклическую подгруппу порядка n, Z_n (упражнение 20). Если ψ: $A \to Z_m$ — гомоморфизм и x — образующая для A, то ее период служит показателем для $\psi(x)$, так что

$\psi(x)$, а следовательно и $\psi(A)$, содержится в Z_n. Пусть y — образующая для Z_n. Имеем изоморфизм

$$\psi_1\colon A \to Z_n,$$

для которого $\psi_1(x) = y$. Для каждого целого k, $0 \leqslant k < n$, имеем гомоморфизм $k\psi_1$, для которого

$$(k\psi_1)(x) = k \cdot \psi_1(x) = \psi_1(kx).$$

Таким образом, мы получаем циклическую подгруппу в A^*, состоящую из n элементов $k\psi_1$ $(0 \leqslant k < n)$. Обратно, любой элемент ψ из A^* однозначно определяется своим действием на образующую x и должен переводить x в один из n элементов ky $(0 \leqslant k < n)$ группы Z_n. Следовательно, ψ совпадает с одним из отображений $k\psi_1$. Эти отображения составляют всю группу A^*, которая, таким образом, является циклической группой порядка n с образующей ψ_1. Это доказывает нашу теорему.

При рассмотрении дуальных групп мы используем различные реализации циклических групп Z_m. Такие группы встречаются во многих приложениях, например группа комплексных корней m-й степени из единицы или подгруппа порядка m в $\mathbf{Q}/\mathbf{Z}$ и т. д.

Пусть A и A' — две абелевы группы. *Билинейное* отображение произведения $A \times A'$ в абелеву группу C — это отображение

$$A \times A' \to C,$$

обозначаемое через

$$(x,\ x') \longmapsto \langle x,\ x' \rangle$$

и обладающее следующим свойством: для каждого $x \in A$ функция $x' \longmapsto \langle x,\ x' \rangle$ есть гомоморфизм и аналогично для каждого $x' \in A'$ функция $x \longmapsto \langle x,\ x' \rangle$ есть гомоморфизм.

Частным случаем билинейного отображения является отображение

$$A \times \mathrm{Hom}(A,\ C) \to C,$$

которое каждой паре $(x,\ f)$, где $x \in A$ и $f \in \mathrm{Hom}(A,\ C)$, сопоставляет элемент $f(x)$ из C.

Билинейное отображение называется также *спариванием*.

Элемент $x \in A$ называется *ортогональным* (или *перпендикулярным*) подмножеству S' в A', если $\langle x,\ x' \rangle = 0$ для всех $x' \in S'$. Ясно, что множество элементов $x \in A$, ортогональных к S', образует подгруппу в A. Аналогично определяются элементы из A', ортогональные к подмножествам в A.

Ядро слева нашего билинейного отображения — это подгруппа в A, ортогональная ко всей группе A'. Аналогично определяем ядро справа.

Для заданного билинейного отображения $A \times A' \to C$ обозначим через B, B' его ядра слева и справа. Всякий элемент x' из A' опре-

деляет при помощи соответствия $x \mapsto (x, x')$ некоторый элемент из $\mathrm{Hom}(A, C)$, который мы будем обозначать через $\psi_{x'}$. Так как $\psi_{x'}$ обращается в нуль на B, то мы видим, что, на самом деле, $\psi_{x'}$ будет гомоморфизмом A/B в C. Кроме того, $\psi_{x'} = \psi_{y'}$, если x', y' — такие элементы из A', что

$$x' \equiv y' \pmod{B'}.$$

Следовательно, ψ: $x' \mapsto \psi_{x'}$ есть в действительности гомоморфизм

$$0 \to A'/B' \to \mathrm{Hom}(A/B, C),$$

который инъективен, поскольку мы определили B' как группу, ортогональную к A. Аналогично мы получаем инъективный гомоморфизм

$$0 \to A/B \to \mathrm{Hom}(A'/B', C).$$

Предположим, что группа C — циклическая порядка m. Тогда $m\psi_{x'} = \psi_{mx'} = 0$ для любого $x' \in A'$, откуда A'/B' имеет показатель m. Точно так же и A/B имеет показатель m.

Теорема 10. *Пусть $A \times A' \to C$ — билинейное отображение двух абелевых групп в циклическую группу C порядка m и B, B' — его ядра соответственно слева и справа. Предположим, что факторгруппа A'/B' конечна. Тогда A/B конечна и A'/B' изоморфна дуальной группе группы A/B* (относительно нашего отображения ψ).

Доказательство. Вложение A/B в $\mathrm{Hom}(A'/B', C)$ показывает, что группа A/B конечна. Кроме того, для порядков получаем неравенства

$$(A/B : 1) \leqslant ((A'/B')^* : 1) = (A'/B' : 1)$$

и

$$(A'/B' : 1) \leqslant ((A/B)^* : 1) = (A/B : 1).$$

Отсюда вытекает, что наше отображение ψ биективно и, следовательно, является изоморфизмом.

Следствие. *Пусть A — конечная абелева группа, B — ее подгруппа, A^* — дуальная группа и $B^\perp$ — множество всех $\varphi \in A^*$, таких, что $\varphi(B) = 0$. Тогда существует естественный изоморфизм между $A^*/B^\perp$ и B^*.*

Доказательство. Это частный случай теоремы 10.

УПРАЖНЕНИЯ

1. Показать, что каждая группа порядка $\leqslant 5$ абелева.

2. Показать, что существуют две неизоморфные группы порядка 4, а именно циклическая и произведение двух циклических групп порядка 2.

3. Пусть p — наименьшее простое число, делящее порядок конечной группы G, H — подгруппа индекса p. Показать, что H нормальна в G.

4. Показать, что существуют ровно две неизоморфные неабелевы группы порядка 8. (Одна из них задается образующими σ, τ и соотношениями

$$\sigma^4 = 1, \quad \tau^2 = 1, \quad \tau\sigma\tau = \sigma^3.$$

Другая — группа кватернионов.)

5. Пусть G — группа и A — ее нормальная абелева подгруппа. Показать, что G/A действует на A посредством сопряжений, и таким путем получить гомоморфизм G/A в $\mathrm{Aut}(A)$.

6. Показать, что каждая группа порядка 15 — циклическая.

7. Определить все группы порядка $\leqslant 10$ с точностью до изоморфизма.

8. Группа G называется *периодической*, если для каждого $x \in G$ существует целое число $n \geqslant 1$, для которого $x^n = 1$. Показать, что в категории периодических абелевых групп существуют бесконечные прямые произведения.

9. Пусть σ — перестановка конечного множества I, содержащего n элементов. Определим *знак* $\varepsilon(\sigma)$ перестановки σ, положив его равным $(-1)^m$, где

$$m = n - \text{число орбит } \sigma.$$

Если $I_1, \ldots, I_r$ — орбиты σ, то m также равно сумме

$$m = \sum_{\nu=1}^{r} [\mathrm{card}\,(I_\nu) - 1].$$

Перестановка τ множества I называется *транспозицией*, если в I существуют два таких элемента $i \neq j$, что $\tau(i) = j$, $\tau(j) = i$ и $\tau(x) = x$ для всех $x \in I$, $x \neq i$, j. Пусть τ — транспозиция. Показать, что $\varepsilon(\sigma\tau) = -\varepsilon(\sigma)$, рассмотрев два случая, когда i, j лежат на одной и той же орбите перестановки σ или же на разных орбитах. В первом случае $\sigma\tau$ имеет орбит на одну больше, а во втором случае — на одну меньше. В частности, знак транспозиции равен -1.

10. Доказать по индукции, что транспозиций порождают группу перестановок множества I (называемую *симметрической группой* и обозначаемую часто через S_n). Если $\sigma = \tau_1 \cdots \tau_m$, где τ_i — транспозиции, то $\varepsilon(\sigma) = (-1)^m$. Показать, что $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\,\varepsilon(\sigma')$, где σ, σ' — любые две перестановки.

11. Пусть I — множество целых чисел $(1, \ldots, n)$. Показать, что для любой перестановки σ

$$\prod_{1 \leqslant i < j \leqslant n} [\sigma(j) - \sigma(i)] = \varepsilon(\sigma) \prod_{1 \leqslant i < j \leqslant n} (j - i).$$

12. Пусть G — группа и H — ее подгруппа конечного индекса. Показать, что в G существует нормальная подгруппа N, содержащаяся в H и также имеющая конечный индекс. [*Указание*: если $(G : H) = n$, то найти гомоморфизм G в S_n, ядро которого содержится в H.]

13. Пусть $f\colon A \to A'$ — гомоморфизм абелевых групп, B — подгруппа в A. Обозначим через A^f и A_f соответственно образ и ядро отображения f и аналогично определим B^f и B_f. Показать, что

$$(A : B) = (A^f : B^f)\,(A_f : B_f)$$

в том смысле, что если два из этих трех индексов конечны, то конечен и третий и выполняется написанное равенство.

14. Пусть G — конечная циклическая группа порядка n, порожденная элементом σ. Предположим, что G действует на абелевой группе A, и пусть f, g: $A \to A$ — эндоморфизмы A, определяемые формулами

$$f(x) = \sigma x - x \quad \text{и} \quad g(x) = x + \sigma x + \cdots + \sigma^{n-1}x.$$

Определим *отношение Эрбрана*

$$q(A) = \frac{(A_f : A^g)}{(A_g : A^f)}$$

при условии, что оба индекса конечны. Предположим теперь, что B — подгруппа в A, для которой $GB \subset B$. (а) Определить естественным образом действие G на A/B. (б) Доказать, что

$$q(A) = q(B)\, q(A/B)$$

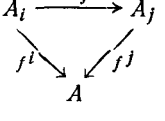
в том смысле, что если два из этих множителей конечны, то конечен и третий и выполняется написанное равенство. (в) Показать, что если A конечна, то $q(A) = 1$.

(Это упражнение — частный случай общей теории эйлеровых характеристик, рассматриваемой в гл. IV. После прочтения этой главы данное упражнение делается тривиальным. Почему?)

15. Пусть I — некоторое множество индексов. Предположим, что на I задано отношение частичного порядка, а именно для некоторых пар (i, j) выполнено соотношение $i \leqslant j$, удовлетворяющее следующим условиям. Для всех i, j, k в I имеем: $i \leqslant i$; если $i \leqslant j$ и $j \leqslant k$, то $i \leqslant k$; если $i \leqslant j$ и $j \leqslant i$, то $i = j$. Мы говорим, что I — *направленное* множество, если для любых $i, j \in I$ существует элемент k, такой, что $i \leqslant k$ и $j \leqslant k$. Пусть I — направленное множество, $\mathcal{A}$ — некоторая категория и $\{A_i\}$ — семейство объектов из $\mathcal{A}$. Предположим, что для каждой пары i, j с условием $i \leqslant j$ задан морфизм

$$f_j^i\colon A_i \to A_j,$$

такой, что $f_k^j \circ f_j^i = f_k^i$ и $f_i^i = \mathrm{id}$, каковы бы ни были $i \leqslant j \leqslant k$. *Прямой предел* семейства $\{f_j^i\}$ — это универсальный объект в следующей категории $\mathcal{C}$. $\mathrm{Ob}(\mathcal{C})$ состоит из пар $(A, (f^i))$, где $A \in \mathrm{Ob}(A)$ и (f^i) — семейство морфизмов f^i: $A_i \to A$, $i \in I$, такое, что для всех $i \leqslant j$ коммутативна следующая диаграмма:



(Универсальный означает, конечно, универсально отталкивающий.)

Показать, что в категории абелевых групп прямые пределы существуют. [*Указание*: профакторизовать прямую сумму по соотношениям, накладываемым отображениями f_j^i.]

16. Обращая стрелки в предыдущем упражнении, ввести понятие *обратного, или проективного, предела*. Доказать, что обратные пределы существуют в категории групп. [*Указание*: получить обратный предел как подгруппу произведения, состоящую из всех векторов (x_i), которые удовлетворяют соотношениям согласования, налагаемым отображениями f_j^i.]

17. Пусть H, G, G' — группы и

$$f\colon H \to G, \quad g\colon H \to G'$$

— два гомоморфизма. Определить понятие копроизведения этих двух гомоморфизмов и показать, что оно существует.

18. Пусть A — периодическая абелева группа. Показать, что A — прямая сумма своих подгрупп $A(p)$ по всем простым p.

19. Рассматривая $\mathbf{Z}$ и $\mathbf{Q}$ как аддитивные группы, показать, что $\mathbf{Q}/\mathbf{Z}$ — периодическая группа, которая имеет одну и только одну подгруппу порядка n для всякого целого $n \geqslant 1$, и что каждая такая подгруппа циклическая.

20. Показать, что если A — циклическая группа порядка n и d — положительное целое число, $d \mid n$, то A содержит ровно одну подгруппу порядка d, причем эта подгруппа циклическая.

21. Показать, что всякая конечная абелева группа, не являющаяся циклической, содержит подгруппу типа (p, p) для некоторого простого p.

22. Пусть G — циклическая группа порядка n и H — циклическая группа порядка m. Показать, что в случае взаимно простых m, n группа $G \times H$ будет циклической (порядка mn).

Глава II

Кольца

§ 1. Кольца и гомоморфизмы

Кольцо A — это множество с двумя законами композиции, называемыми соответственно умножением и сложением, записываемыми соответственно как произведение и как сумма и удовлетворяющими следующим условиям:

КО 1. Относительно сложения A — абелева группа.

КО 2. Умножение ассоциативно и имеет единичный элемент.

КО 3. Для всех x, y, $z \in A$

$$(x+y)z = xz + yz \quad \text{и} \quad z(x+y) = zx + zy.$$

(Эти соотношения называются *дистрибутивностью*.)

Как обычно, мы обозначаем единичный элемент относительно сложения через 0, а единичный элемент относительно умножения — через 1. Мы не предполагаем, что $1 \neq 0$. Заметим, что $0x = 0$ для всех $x \in A$. Доказательство: очевидно, $0x + x = (0+1)x = 1x = x$; следовательно, $0x = 0$. В частности, если $1 = 0$, то A состоит из одного 0.

Для любых x, y имеем $(-x)y = -(xy)$. Доказательство:

$$xy + (-x)y = (x + (-x))y = 0y = 0,$$

так что $(-x)y$ служит обратным для xy относительно сложения.

Легко доказываются и другие стандартные правила, связывающие сложение и умножение, например, $(-x)(-y) = xy$. Мы предоставляем это читателю в качестве упражнений.

Пусть A — кольцо и U — множество всех элементов в A, имеющих одновременно правый и левый обратный. Тогда U — мультипликативная группа. Действительно, если a имеет правый обратный b, так что $ab = 1$, и левый обратный c, так что $ca = 1$, то $c = cab = b$ и мы видим, что c (или b) служит двусторонним обратным для a. Поэтому U удовлетворяет всем аксиомам мультипликативной группы и называется группой делителей единичного элемента 1 или, более кратко, группой *единиц* кольца A. Она иногда обозначается через A^* и называется также группой *обратимых* элементов кольца A. Кольцо A, в котором $1 \neq 0$ и всякий ненулевой элемент обратим, называется *кольцом с делением* или *телом*.

Кольцо A называется *коммутативным*, если $xy = yx$ для всех $x, y \in A$. Коммутативное тело называется *полем*. Отметим, что по определению поле содержит по крайней мере два элемента, а именно 0 и 1.

Подмножество B кольца A называется *подкольцом*, если оно является аддитивной подгруппой, содержит мультипликативную единицу и если $x, y \in B$ влечет $xy \in B$. В этом случае B само есть кольцо, причем операции в B те же самые, что и в A.

Например, рассмотрим *центр* кольца A—подмножество, состоящее из всех элементов $a \in A$, таких, что $ax = xa$ для всех $x \in A$. Непосредственно видно, что центр A является подкольцом.

Точно так же, как мы выводили ассоциативность в общем случае из ассоциативности в случае трех сомножителей, можно доказать дистрибутивность в общем случае. Пусть x, $y_1, \ldots, y_n$ — элементы кольца A. По индукции проверяется, что

$$x(y_1 + \ldots + y_n) = xy_1 + \ldots + xy_n;$$

легко также видеть, что для любых элементов x_i $(i = 1, \ldots, n)$ и y_j $(j = 1, \ldots, m)$ кольца A

$$\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} x_i y_j.$$

Кроме того, дистрибутивность выполняется и для вычитания, например

$$x(y_1 - y_2) = xy_1 - xy_2.$$

Мы предоставляем все эти доказательства читателю.

Примеры. *Пусть S — множество, A—кольцо и $\mathfrak{M}(S, A)$—множество отображений S в A. Тогда $\mathfrak{M}(S, A)$ — кольцо, если для $f, g \in \mathfrak{M}(S, A)$ положить*

$$(fg)(x) = f(x)\,g(x) \quad \text{и} \quad (f+g)(x) = f(x) + g(x)$$

при всех $x \in S$. Мультипликативной единицей служит постоянное отображение, значение которого есть мультипликативная единица кольца A. Аддитивной единицей служит постоянное отображение, значение которого есть аддитивная единица кольца A, т. е. 0. Проверка того, что $\mathfrak{M}(S, A)$ — кольцо относительно введенных выше законов композиции, тривиальна и предоставляется читателю.

Пусть M — аддитивная абелева группа и A — множество $\mathrm{End}(M)$ групповых гомоморфизмов M в себя. Определим сложение в A как сложение отображений и умножение в A как композицию отображений. Тривиально проверяется, что A — кольцо. Его единичным элементом служит, разумеется, тождественное отображение. Вообще говоря, кольцо A не коммутативно.

Левый идеал $\mathfrak{a}$ кольца A — это подмножество в A, являющееся подгруппой аддитивной группы A, и такое, что $A\mathfrak{a} \subset \mathfrak{a}$ (и, следовательно, $A\mathfrak{a} = \mathfrak{a}$, поскольку A содержит 1). При определении правого идеала мы требуем, чтобы $\mathfrak{a}A = \mathfrak{a}$, а *двусторонним идеалом* называем подмножество, которое одновременно является левым и правым идеалом. Двусторонние идеалы в этом параграфе будут называться просто *идеалами*.

Если A — кольцо и $a \in A$, то $\mathfrak{a} = Aa$ есть левый идеал, называемый *главным*. Говорят, что a — образующая для $\mathfrak{a}$ (над A). Аналогично AaA — главный двусторонний идеал. В коммутативном кольце всякий левый или правый идеал является двусторонним.

Коммутативное кольцо, в котором всякий идеал главный и $1 \neq 0$, называется *кольцом главных идеалов*.

Пример. Целые числа $\mathbf{Z}$ образуют коммутативное кольцо. Пусть $\mathfrak{a}$ — идеал $\neq \mathbf{Z}$ и $\neq 0$. Если $n \in \mathfrak{a}$, то $-n \in \mathfrak{a}$. Пусть d — наименьшее целое число > 0, лежащее в $\mathfrak{a}$. Для всякого $n \in \mathfrak{a}$ существуют целые числа q, r, $0 \leqslant r < d$, такие, что

$$n = dq + r.$$

Так как $\mathfrak{a}$ — идеал, то отсюда следует, что r лежит в $\mathfrak{a}$, а потому $r = 0$. Следовательно, $\mathfrak{a}$ состоит из всех кратных qd числа d, где $q \in \mathbf{Z}$, и $\mathbf{Z}$ — кольцо главных идеалов (см. также рассуждение в начале § 3).

Для всякого кольца A подмножество (0) и само A являются идеалами.

Пусть $\mathfrak{a}$, $\mathfrak{b}$ — идеалы в A. Под $\mathfrak{ab}$ мы понимаем множество всех сумм

$$x_1y_1 + \ldots + x_ny_n,$$

где $x_i \in \mathfrak{a}$ и $y_i \in \mathfrak{b}$. Непосредственно проверяется, что $\mathfrak{ab}$ — идеал и что множество идеалов образует мультипликативный моноид, причем единичным элементом в нем служит само кольцо. Этот единичный элемент называется единичным идеалом и часто обозначается через (1). Пусть $\mathfrak{a}$, $\mathfrak{b}$ — левые идеалы; их произведение $\mathfrak{ab}$ определяется так же, как и выше. Оно тоже является левым идеалом, и вновь имеет место ассоциативность: $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$ для любых левых идеалов $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$.

Если $\mathfrak{a}$, $\mathfrak{b}$ — левые идеалы в A, то $\mathfrak{a} + \mathfrak{b}$ (сумма аддитивных подгрупп в A), очевидно, будет левым идеалом. Аналогично для правых и двусторонних идеалов. Таким образом, идеалы образуют также моноид относительно сложения. При этом имеет место и дистрибутивность: если $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, $\mathfrak{b}$ — идеалы в A, то, очевидно,

$$\mathfrak{b}(\mathfrak{a}_1 + \ldots + \mathfrak{a}_n) = \mathfrak{ba}_1 + \ldots + \mathfrak{ba}_n$$

и аналогично для умножения с другой стороны. (Однако множество идеалов не образует кольца!)

Если $\{\mathfrak{a}_i\}_{i\in I}$ — семейство идеалов, то их пересечение

$$\bigcap_{i\in I}\mathfrak{a}_i$$

— также идеал. Аналогично для левых идеалов. Заметим, что если $\mathfrak{a}$, $\mathfrak{b}$ — два идеала кольца A, то $\mathfrak{ab}\subset\mathfrak{a}\cap\mathfrak{b}$.

Пусть $a_1, \ldots, a_n$ — элементы кольца A. Мы обозначаем через $(a_1, \ldots, a_n)$ идеал, являющийся пересечением всех идеалов в A, содержащих эти элементы, или левый идеал, являющийся пересечением всех левых идеалов в A, содержащих эти элементы. Что именно имеется в виду (т. е. двусторонний или левый идеал), всегда будет ясно из контекста. Мы называем $a_1, \ldots, a_n$ *образующими* этого идеала. Главный идеал (или главный левый идеал), таким образом, порождается одним элементом. Сразу видно, что левый идеал, порожденный элементами $a_1, \ldots, a_n$, состоит из всех элементов, которые могут быть записаны в виде

$$x_1a_1+\ldots+x_na_n,$$

где $x_i\in A$.

Под *кольцевым гомоморфизмом* понимают отображение $f\colon A\to B$ одного кольца в другое, являющееся моноидным гомоморфизмом для мультипликативных структур на A и B, а также моноидным гомоморфизмом для аддитивных структур. Другими словами, f должно удовлетворять соотношениям

$$f(a+a')=f(a)+f(a'),\qquad f(aa')=f(a)f(a'),$$
$$f(1)=1,\qquad f(0)=0$$

для всех a, $a'\in A$. (Точнее следовало бы писать $f(1)=\overline{1}$, $f(0)=\overline{0}$, где $\overline{1}$ — единица и $\overline{0}$ — нуль в B.) Его *ядром* служит ядро отображения f, рассматриваемого как аддитивный гомоморфизм.

Как немедленно проверяется, *ядро кольцевого гомоморфизма $f\colon A\to B$ является идеалом в A.*

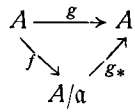
Обратно, пусть $\mathfrak{a}$ — идеал кольца A. Мы можем построить *факторкольцо* $A/\mathfrak{a}$ следующим образом. Рассматривая A и $\mathfrak{a}$ как аддитивные группы, образуем факторгруппу $A/\mathfrak{a}$. Определим теперь в $A/\mathfrak{a}$ мультипликативный закон композиции. Если $x+\mathfrak{a}$ и $y+\mathfrak{a}$ — два смежных класса по $\mathfrak{a}$, то полагаем $(x+\mathfrak{a})(y+\mathfrak{a})$ равным смежному классу $(xy+\mathfrak{a})$. Этот смежный класс правильно определен, так как если x_1, y_1 лежат в тех же самых смежных классах, что и x, y соответственно, то, как немедленно проверяется, x_1y_1 принадлежит тому же смежному классу, что и xy. Наш мультипликативный закон, очевидно, ассоциативен и имеет единичный элемент, а именно смежный класс $1+\mathfrak{a}$. Кроме того, выполняется дистрибутивный закон, поскольку он выполняется для представителей смежных классов.

Таким образом, мы определили структуру кольца на $A/\mathfrak{a}$ и каноническое отображение

$$f\colon A \to A/\mathfrak{a}$$

является, очевидно, гомоморфизмом колец.

Если $g\colon A \to A'$ *— кольцевой гомоморфизм, ядро которого содержит идеал* $\mathfrak{a}$, *то существует однозначно определенный кольцевой гомоморфизм* $g_*\colon A/\mathfrak{a} \to A'$, *для которого коммутативна следующая диаграмма*:



Действительно, если рассматривать f, g как групповые гомоморфизмы (для аддитивных структур), то существует однозначно определенный групповой гомоморфизм g_*, для которого наша диаграмма коммутативна. Мы утверждаем, что на самом деле g_* — кольцевой гомоморфизм. Можно было бы предоставить читателю это тривиальное доказательство, но мы приведем его полностью. Если $x \in A$, то $g(x) = g_* f(x)$. Следовательно, для x, $y \in A$ имеем

$$g_*(f(x)f(y)) = g_*(f(xy)) = g(xy) = g(x)g(y) = g_*(f(x))\,g_*(f(y)).$$

Но для всяких данных ξ, $\eta \in A/\mathfrak{a}$ существуют x, $y \in A$, такие, что $\xi = f(x)$ и $\eta = f(y)$. Далее, так как $f(1) = 1$, то $g_* f(1) = g_*(1) = 1$ и, следовательно, оба условия, необходимые для того, чтобы отображение g_* было гомоморфизмом мультипликативных моноидов, выполняются, что и требовалось показать.

Утверждение, которое мы только что доказали, эквивалентно высказыванию, что каноническое отображение $f\colon A \to A/\mathfrak{a}$ универсально в категории гомоморфизмов, ядра которых содержат $\mathfrak{a}$.

Пусть A — кольцо и B — его подкольцо. Пусть S — подмножество в A. Мы обозначаем через $B[S]$ пересечение всех подколец в A, содержащих B и S. Если всякий элемент из S коммутирует с любым элементом из B, то $B[S]$, очевидно, будет кольцом, состоящим из всех элементов вида

$$\sum b_{i_1, \ldots, i_n} s_1^{i_1} \ldots s_n^{i_n},$$

где сумма пробегает некоторое конечное число наборов $(i_1, \ldots, i_n)$ целых чисел $\geqslant 0$ и $b_{i_1, \ldots, i_n} \in B$, $s_1, \ldots, s_n \in S$.

Если $A = B[S]$, то говорят, что S является множеством образующих (или, точнее, *кольцевых образующих*) для A над B или что A порождается множеством S над B. Если S конечно, то говорят, что A *конечно порождено как кольцо над* B.

Заметим, что, как и в случае групп, гомоморфизм колец однозначно определяется своим действием на образующие. Именно, пусть $f\colon B \to B'$ — гомоморфизм колец, и пусть в предыдущих обозначениях $A = B[S]$. Тогда существует самое большее одно продолжение f до гомоморфизма кольца A, имеющее предписанные значения на S.

Пусть A — кольцо, $\mathfrak{a}$ — идеал и S — подмножество в A. Мы пишем

$$S \equiv 0 \pmod{\mathfrak{a}},$$

если $S \subset \mathfrak{a}$. Пусть $x, y \in A$. Мы пишем

$$x \equiv y \pmod{\mathfrak{a}},$$

коль скоро $x - y \in \mathfrak{a}$. Если $\mathfrak{a}$ — главный идеал, равный (a), то допустима также запись

$$x \equiv y \pmod{a}.$$

Если $f\colon A \to A/\mathfrak{a}$ — канонический гомоморфизм, то $x \equiv y \pmod{\mathfrak{a}}$ означает, что $f(x) = f(y)$. Эти обозначения в форме сравнений бывают удобны, когда хотят избежать явного упоминания канонического отображения f.

Факторкольцо $A/\mathfrak{a}$ называется также *кольцом классов вычетов*. Смежные классы кольца A по $\mathfrak{a}$ называются *классами вычетов* по модулю $\mathfrak{a}$, и для данного $x \in A$ смежный класс $x + \mathfrak{a}$ называется *классом вычетов элемента x по модулю $\mathfrak{a}$*.

Любой биективный гомоморфизм колец $f\colon A \to B$ является изоморфизмом. Действительно, существует обратное в теоретико-множественном смысле отображение $g\colon B \to A$, и тривиально проверяется, что g — гомоморфизм колец.

Мы иногда будем говорить просто „гомоморфизм“ вместо „кольцевой гомоморфизм“, если ясно, что речь идет именно о кольцах. Отметим, что кольца образуют категорию (морфизмами в которой служат гомоморфизмы).

Пусть $f\colon A \to B$ — гомоморфизм колец. Тогда образ $f(A)$ отображения f — подкольцо в B. Доказательство очевидно.

Ясно, что инъективный кольцевой гомоморфизм $f\colon A \to B$ устанавливает изоморфизм между кольцом A и его образом. Такой гомоморфизм будет называться *вложением* (колец).

Пусть $f\colon A \to A'$ — гомоморфизм колец и $\mathfrak{a}'$ — идеал в A'. Тогда $f^{-1}(\mathfrak{a}')$ есть некоторый идеал $\mathfrak{a}$ в A, и мы имеем индуцированный инъективный гомоморфизм

$$A/\mathfrak{a} \to A'/\mathfrak{a}'.$$

Тривиальное доказательство предоставляется читателю.

Предложение 1. *Прямые произведения в категории колец существуют.*

Действительно, пусть $\{A_i\}_{i\in I}$ — семейство колец, и пусть $A=\prod A_i$ — их произведение как аддитивных абелевых групп. Умножение в A определим очевидным способом: если $(x_i)_{i\in I}$ и $(y_i)_{i\in I}$ — два элемента из A, то берем в качестве их произведения $(x_iy_i)_{i\in I}$, т. е. определяем умножение покомпонентно, так же как мы это делали для сложения. Мультипликативная единица — это просто элемент произведения, i-я компонента которого является единичным элементом в A_i. Ясно, что мы получаем на A структуру кольца и что проекция на каждый множитель будет кольцевым гомоморфизмом. Кроме того, A вместе с проекциями, очевидно, удовлетворяет необходимому свойству универсальности.

Отметим, что обычное отображение вложения A_i на i-й множитель *не является* кольцевым гомоморфизмом, поскольку оно не переводит единичный элемент e_i кольца A_i в единичный элемент кольца A. Действительно, оно переводит e_i в элемент кольца A, имеющий e_i в качестве i-й компоненты и $0\,(=0_i)$ — в качестве всех других компонент.

Пусть A — кольцо. Элементы x, y в A называются *делителями нуля*, если $x\neq 0$, $y\neq 0$, а $xy=0$. Большинство колец без делителей нуля, которые мы рассматриваем, будут коммутативными. Ввиду этого мы называем кольцо A *целостным*, если оно коммутативно и если в нем нет делителей нуля и $1\neq 0$ [1]).

Примеры. Кольцо целых чисел $\mathbf{Z}$ — без делителей нуля, т. е. целостное. Если S — множество, содержащее не менее двух элементов, и A — кольцо с $1\neq 0$, то кольцо отображений $M(S, A)$ имеет делитель нуля. (Доказательство?)

Пусть m — положительное целое число $\neq 1$. Кольцо $\mathbf{Z}/m\mathbf{Z}$ содержит делители нуля тогда и только тогда, когда m — не простое. (Доказательство предоставляем читателю в качестве упражнения.)

Часто используется следующий критерий.

Отличные от нуля элементы a, b целостного кольца A порождают один и тот же идеал тогда и только тогда, когда в A существует обратимый элемент u, для которого $b=au$.

Доказательство. Если такой обратимый элемент найдется, то $Ab=Aua=Aa$. Обратно, пусть $Aa=Ab$. Тогда, в частности, $a=bc$ и $b=ad$ для некоторых элементов c, $d\in A$. Следовательно, $a=adc$, откуда $a(1-dc)=0$, а потому $dc=1$. Следовательно, c — обратимый элемент.

---

[1]) Целостное кольцо называют также *кольцом целостности*, *областью целостности* или просто *областью*. — *Прим. ред.*

§ 2. Коммутативные кольца

В этом параграфе слово „кольцо" будет означать „коммутативное кольцо".

Пусть A — кольцо. *Простой* идеал в A — это такой идеал $\mathfrak{p} \neq A$, что кольцо $A/\mathfrak{p}$ — целостное. Эквивалентным образом мы могли бы сказать, что это такой идеал $\mathfrak{p} \neq A$, для которого из условий x, $y \in A$ и $xy \in \mathfrak{p}$ всегда следует, что $x \in \mathfrak{p}$ или $y \in \mathfrak{p}$.

Пусть $\mathfrak{m}$ — идеал. Мы говорим, что $\mathfrak{m}$ — *максимальный* идеал, если $\mathfrak{m} \neq A$ и если не существует идеала $\mathfrak{a} \neq A$, содержащего $\mathfrak{m}$ и $\neq \mathfrak{m}$.

Всякий максимальный идеал — простой. Доказательство. Пусть $\mathfrak{m}$ — максимальный идеал, и пусть x, $y \in A$ таковы, что $xy \in \mathfrak{m}$. Предположим, что $x \notin \mathfrak{m}$. Тогда $\mathfrak{m} + Ax$ — идеал, строго содержащий $\mathfrak{m}$ и, стало быть, равный A. Следовательно, мы можем написать

$$1 = u + ax,$$

где $u \in \mathfrak{m}$ и $a \in A$. Умножая на y, получаем

$$y = yu + axy,$$

откуда $y \in \mathfrak{m}$ и $\mathfrak{m}$, таким образом, простой.

Пусть A — кольцо. Всякий его идеал $\mathfrak{a} \neq A$ содержится в некотором максимальном идеале $\mathfrak{m}$. Доказательство. Множество идеалов, содержащих $\mathfrak{a}$ и $\neq A$, индуктивно упорядочено по включению. Действительно, если $\{\mathfrak{b}_i\}$ — линейно упорядоченное множество таких идеалов, то $1 \notin \mathfrak{b}_i$ ни для какого i и, следовательно, 1 не лежит в идеале $\mathfrak{b} = \bigcup \mathfrak{b}_i$, который и мажорирует все $\mathfrak{b}_i$. Пусть $\mathfrak{m}$ — некоторый максимальный элемент в нашем множестве. Тогда $\mathfrak{m} \neq A$ и $\mathfrak{m}$ является максимальным идеалом, что и требовалось установить.

Пусть A — кольцо. Тогда $\{0\}$ является простым идеалом в том и только в том случае, если A — целостное. (Доказательство очевидно.)

Мы определили *поле* K как такое кольцо, в котором $1 \neq 0$ и мультипликативный моноид отличных от нуля элементов является группой (т. е. если $x \in K$ и $x \neq 0$, то для x существует обратный). Отметим, что единственные идеалы поля K — это само K и нулевой идеал.

Если A — кольцо и $\mathfrak{m}$ — максимальный идеал, то $A/\mathfrak{m}$ — поле. Доказательство. Для $x \in A$ обозначаем через $\bar{x}$ класс вычетов элемента x по модулю $\mathfrak{m}$. Так как $\mathfrak{m} \neq A$, то в $A/\mathfrak{m}$ имеется единичный элемент $\neq 0$. Всякий ненулевой элемент из $A/\mathfrak{m}$ может быть записан

как $\bar{x}$ для некоторого $x \in A$, $x \notin \mathfrak{m}$. Чтобы найти его обратный, заметим, что $\mathfrak{m} + Ax$ есть идеал в A, строго содержащий $\mathfrak{m}$ и, стало быть, равный A. Следовательно, мы можем написать

$$1 = u + yx,$$

где $u \in \mathfrak{m}$ и $y \in A$. Это означает, что $\bar{y}\bar{x} = 1$ (т. е. $\bar{1}$) и, таким образом, $\bar{x}$ имеет обратный, что и требовалось установить.

Мы предоставляем читателю в качестве упражнения доказать, что и обратно, *если A — кольцо и $\mathfrak{m}$ — такой идеал, что $A/\mathfrak{m}$ — поле, то $\mathfrak{m}$ максимален.*

Пусть $f\colon A \to A'$ — гомоморфизм (коммутативных колец, согласно действующему соглашению). Пусть $\mathfrak{p}'$ — простой идеал в A' и $\mathfrak{p} = f^{-1}(\mathfrak{p}')$. Тогда идеал $\mathfrak{p}$ простой.

Для доказательства возьмем x, $y \in A$ с условием $xy \in \mathfrak{p}$. Предположим, что $x \notin \mathfrak{p}$. Тогда $f(x) \notin \mathfrak{p}'$. Но $f(x)f(y) = f(xy) \in \mathfrak{p}'$. Следовательно, $f(y) \in \mathfrak{p}'$, что и требовалось установить.

В качестве упражнения докажите, что если гомоморфизм f сюръективен и $\mathfrak{m}'$ — максимальный идеал в A', то идеал $f^{-1}(\mathfrak{m}')$ максимален в A.

Пример. Пусть $\mathbf{Z}$ — кольцо целых чисел. Мы уже отмечали, что всякий идеал в этом кольце главный и имеет вид $n\mathbf{Z}$ для некоторого целого $n \geqslant 0$ (однозначно определенного идеалом). Пусть $\mathfrak{p}$ — простой идеал (отличный от 0), $\mathfrak{p} = n\mathbf{Z}$. Тогда n должно быть простым числом, что по существу непосредственно вытекает из определения простого идеала. Обратно, если p — простое число, то $p\mathbf{Z}$ — простой идеал (тривиальное упражнение). Кроме того, $p\mathbf{Z}$ — максимальный идеал. Действительно, предположим, что $p\mathbf{Z}$ содержится в некотором идеале $n\mathbf{Z}$. Тогда $p = nm$ для некоторого целого m, откуда $n = p$ или $n = 1$, что и доказывает максимальность $p\mathbf{Z}$.

Пусть n — целое число. Факторкольцо $\mathbf{Z}/n\mathbf{Z}$ называется *кольцом целых чисел по модулю n*. Если n равно простому числу p, то кольцо целых чисел по модулю p является в действительности полем, обозначаемым символом $\mathbf{F}_p$. В частности, мультипликативная группа поля $\mathbf{F}_p$ называется группой отличных от нуля целых чисел по модулю p. Из элементарных свойств групп получаем следующий стандартный факт элементарной теории чисел. Если x — целое число $\not\equiv 0 \pmod{p}$, то $x^{p-1} \equiv 1 \pmod{p}$. (Для простоты обычно пишут $\bmod p$ вместо $\bmod p\mathbf{Z}$ и аналогично пишут $\bmod n$ вместо $\bmod n\mathbf{Z}$ для любого целого n.) Если, далее, дано целое число $n > 1$, то обратимые элементы кольца $\mathbf{Z}/n\mathbf{Z}$ состоят из тех классов вычетов $\bmod n\mathbf{Z}$, которые представляются целыми числами $m \neq 0$, взаимно простыми с n. Порядок группы единиц (обратимых элементов) кольца $\mathbf{Z}/n\mathbf{Z}$

обозначается через $\varphi(n)$ (где φ известна как *эйлерова фи-функция*). Следовательно, если x — целое число, взаимно простое с n, то $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Китайская теорема об остатках. *Пусть A — кольцо и $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ — такие идеалы, что $\mathfrak{a}_i + \mathfrak{a}_j = A$ при всех $i \neq j$. Для любого семейства элементов $x_1, \ldots, x_n$ кольца A существует такой элемент $x \in A$, что $x \equiv x_i \pmod{\mathfrak{a}_i}$ при всех i.*

Доказательство — по индукции. Если $n = 2$, то имеем

$$1 = a_1 + a_2$$

для некоторых элементов $a_i \in \mathfrak{a}_i$ и можно положить $x = x_2 a_1 + x_1 a_2$.

Предположим, что теорема доказана для семейства из $n-1$ идеалов. Для каждого $i \geqslant 2$ мы можем найти элементы $a_i \in \mathfrak{a}_1$ и $b_i \in \mathfrak{a}_i$, такие, что

$$a_i + b_i = 1, \qquad i \geqslant 2.$$

Произведение $\prod_{i=2}^{n} (a_i + b_i)$ равно 1 и лежит в $\mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i$, т. е. в $\mathfrak{a}_1 + \mathfrak{a}_2 \ldots \mathfrak{a}_n$. Следовательно,

$$\mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i = A.$$

В силу справедливости теоремы при $n = 2$ мы можем найти такой элемент $y_1 \in A$, что

$$y_1 \equiv 1 \pmod{\mathfrak{a}_1},$$

$$y_1 \equiv 0 \left(\mathrm{mod} \prod_{i=2}^{n} \mathfrak{a}_i \right).$$

Аналогично найдутся такие элементы $y_2, \ldots, y_n$, что $y_j \equiv 1 \pmod{\mathfrak{a}_j}$ и $y_j \equiv 0 \pmod{\mathfrak{a}_i}$ при $i \neq j$. Тогда элемент $x = x_1 y_1 + \ldots + x_n y_n$ удовлетворяет нашим требованиям.

Еще одно замечание в том же духе: если $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ — такие идеалы в A, что

$$\mathfrak{a}_1 + \ldots + \mathfrak{a}_n = A,$$

и если $\nu_1, \ldots, \nu_n$ — положительные целые числа, то

$$\mathfrak{a}_1^{\nu_1} + \ldots + \mathfrak{a}_n^{\nu_n} = A.$$

Доказательство тривиально и предоставляется читателю в качестве упражнения.

Следствие. *Пусть A — кольцо и $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ — идеалы в A. Предположим, что $\mathfrak{a}_i + \mathfrak{a}_j = A$ при $i \neq j$. Пусть*

$$f\colon A \to \prod_{i=1}^{n} A/\mathfrak{a}_i = (A/\mathfrak{a}_1) \times \ldots \times (A/\mathfrak{a}_n)$$

— отображение кольца A в написанное произведение, индуцированное каноническими отображениями A на $A/\mathfrak{a}_i$ для каждого множителя. Тогда ядро отображения f есть $\bigcap_{i=1}^{n} \mathfrak{a}_i$ и f сюръективно, что приводит, таким образом, к изоморфизму

$$A/\bigcap \mathfrak{a}_i \xrightarrow{\approx} \prod A/\mathfrak{a}_i.$$

Доказательство. Утверждение о ядре очевидно. Сюръективность вытекает из предыдущей теоремы.

Теорема и ее следствие часто применяются к кольцу целых чисел $\mathbf{Z}$ и к попарно различным простым идеалам $(p_1), \ldots, (p_n)$. Они удовлетворяют предпосылкам теоремы, поскольку являются максимальными. Аналогично можно взять целые числа $m_1, \ldots, m_n$, попарно взаимно простые, и применить теорему к главным идеалам $(m_1) = m_1\mathbf{Z}, \ldots, (m_n) = m_n\mathbf{Z}$. Это ультраклассический случай китайской теоремы об остатках.

Пусть, в частности, m — целое число > 1 и

$$m = \prod_i p_i^{r_i}$$

— разложение m на простые сомножители с показателями $r_i \geqslant 1$. Тогда имеем изоморфизм колец

$$\mathbf{Z}/m\mathbf{Z} \approx \prod_i \mathbf{Z}/p_i^{r_i}\mathbf{Z}.$$

Если A — кольцо, то обозначаем, как обычно, через A^* мультипликативную группу обратимых элементов в A. Мы предоставляем следующее утверждение читателю в качестве упражнения.

Предыдущий кольцевой изоморфизм $\mathbf{Z}/m\mathbf{Z}$ на произведение индуцирует изоморфизм групп

$$(\mathbf{Z}/m\mathbf{Z})^* \approx \prod_i \left(\mathbf{Z}/p_i^{r_i}\mathbf{Z}\right)^*.$$

В силу этого изоморфизма имеем

$$\varphi(m) = \prod_i \varphi\left(p_i^{r_i}\right).$$

Если p — простое число и r — целое число $\geqslant 1$, то

$$\varphi(p^r) = (p-1)\,p^{r-1}.$$

Последняя формула доказывается по индукции. Если $r=1$, то $\mathbf{Z}/p\mathbf{Z}$ — поле и мультипликативная группа этого поля имеет порядок $p-1$. При $r \geqslant 1$ рассмотрим канонический гомоморфизм колец

$$\mathbf{Z}/p^{r+1}\mathbf{Z} \to \mathbf{Z}/p^r\mathbf{Z},$$

порожденный включением идеалов $(p^{r+1}) \subset (p^r)$. Индуцированный им гомоморфизм групп

$$\lambda\colon (\mathbf{Z}/p^{r+1}\mathbf{Z})^* \to (\mathbf{Z}/p^r\mathbf{Z})^*$$

сюръективен, потому что любое целое число a, представляющее некоторый элемент из $\mathbf{Z}/p^r\mathbf{Z}$ и взаимно простое с p, будет представлять также некоторый элемент из $(\mathbf{Z}/p^{r+1}\mathbf{Z})^*$. Пусть a — целое число, представляющее такой элемент из $(\mathbf{Z}/p^{r+1}\mathbf{Z})^*$, что $\lambda(a)=1$. Тогда

$$a \equiv 1 \pmod{p^r\mathbf{Z}}$$

и, следовательно, мы можем написать

$$a \equiv 1 + xp^r \pmod{p^{r+1}\mathbf{Z}}$$

для некоторого $x \in \mathbf{Z}$. Значения $x = 0, 1, \ldots, p-1$ приводят к p различным элементам из $(\mathbf{Z}/p^{r+1}\mathbf{Z})^*$, которые все лежат в ядре λ. Но в качестве элемента x в предыдущем сравнении всегда может быть выбрано одно из этих p чисел, поскольку всякое целое число сравнимо с одним из них по модулю p. Следовательно, ядро λ имеет порядок p и наша формула доказана.

Отметим, что ядро λ изоморфно группе $\mathbf{Z}/p\mathbf{Z}$. (Доказательство?)

Пусть A — кольцо. Обозначим на минуту его единичный элемент через e. Отображение

$$\lambda\colon \mathbf{Z} \to A,$$

для которого $\lambda(n) = ne$, будет, очевидно, кольцевым гомоморфизмом с идеалом-ядром (n), порожденным некоторым целым числом $n \geqslant 0$. Канонический инъективный гомоморфизм $\mathbf{Z}/n\mathbf{Z} \to A$ является (кольцевым) изоморфизмом между $\mathbf{Z}/n\mathbf{Z}$ и некоторым подкольцом в A. Если A — целостное, то $n\mathbf{Z}$ — простой идеал и, следовательно, $n=0$ или $n=p$, где p — некоторое простое число. В первом случае A содержит в качестве подкольца кольцо, изоморфное $\mathbf{Z}$ и часто отождествляемое с $\mathbf{Z}$. В этом случае мы говорим, что A имеет *характеристику* 0. Если же $n=p$, то мы говорим, что A имеет *характеристику* p; в этом случае A содержит (изоморфный образ) $\mathbf{F}_p$ в качестве подкольца [1]).

[1]) В дальнейшем употребляется также краткое обозначение $\operatorname{char} A = 0$ или p. — *Прим. ред.*

Всякое поле K имеет характеристику 0 или $p > 0$. В первом случае K содержит в качестве подполя изоморфный образ поля рациональных чисел, а во втором случае оно содержит изоморфный образ поля $\mathbf{F}_p$. В обоих случаях это подполе будет называться *простым полем* (содержащимся в K). Так как это простое поле является наименьшим подполем в K, содержащим 1 и не имеющим автоморфизмов, кроме тождественного, его обычно отождествляют с $\mathbf{Q}$ или $\mathbf{F}_p$, в зависимости от того, какой случай имеет место.

Под *простым кольцом* (в K) мы будем понимать либо кольцо целых чисел $\mathbf{Z}$, если K имеет характеристику 0, либо $\mathbf{F}_p$, если K имеет характеристику p.

§ 3. Локализация

Мы продолжаем предполагать, что „кольцо" означает „коммутативное кольцо".

Пусть A — некоторое кольцо. Под *мультипликативным подмножеством* в A мы будем понимать подмоноид в кольце A (рассматриваемом как мультипликативный моноид согласно КО 2). Другими словами, это есть подмножество S, содержащее 1 и вместе с любыми двумя элементами x, y их произведение xy.

Мы построим сейчас *кольцо частных кольца A по S*, известное также под названием *кольца отношений кольца A по S*.

Рассмотрим пары (a, s), где $a \in A$ и $s \in S$. Определим отношение

$$(a, s) \sim (a', s')$$

между такими парами следующим условием: существует элемент $s_1 \in S$, для которого

$$s_1(s'a - sa') = 0.$$

Тривиально проверяется, что это будет отношение эквивалентности; класс эквивалентности, содержащий пару (a, s), обозначается через a/s. Множество классов эквивалентности обозначается символом $S^{-1}A$.

Отметим, что если $0 \in S$, то $S^{-1}A$ содержит ровно один элемент, а именно $0/1$.

Условием

$$(a/s)(a'/s) = aa'/ss'$$

в $S^{-1}A$ вводится умножение Тривиально проверяется, что это умножение правильно определено. Оно имеет единичный элемент, а именно $1/1$, и, очевидно, ассоциативно.

Сложение в $S^{-1}A$ задается посредством формулы

$$\frac{a}{s}+\frac{a'}{s'}=\frac{s'a+sa'}{ss'}.$$

Тривиально проверяется, что оно правильно определено. Для примера приведем подробное доказательство. Пусть $a_1/s_1=a/s$ и $a_1'/s_1'=a'/s'$. Мы должны показать, что

$$(s_1'a_1'+s_1a_1')/s_1s_1'=(s'a+sa')/ss'.$$

Существуют s_2, $s_3\in S$, для которых

$$s_2(sa_1-s_1a)=0,$$
$$s_3(s'a_1'-s_1'a')=0.$$

Умножим первое равенство на $s_3s's_1'$, а второе — на s_2ss_1, затем сложим их и получим

$$s_2s_3\left[s's_1'(sa_1-s_1a)+ss_1(s'a_1'-s_1'a')\right]=0$$

По определению это и есть то, что мы хотим показать; именно существует элемент из S (например, s_2s_3), который после умножения на

$$ss'(s_1'a_1+s_1a_1')-s_1s_1'(s'a+sa')$$

дает 0.

Заметим, что для данных $a\in A$ и s, $s'\in S$

$$a/s=s'a/s's.$$

Таким образом, это элементарное свойство дробей остается справедливым и в нашей более общей ситуации.

Наконец, так же тривиально проверяется, что два наши закона композиции определяют на $S^{-1}A$ структуру кольца.

Пусть

$$\varphi_S\colon A\to S^{-1}A$$

— *отображение, при котором* $\varphi(a)=a/1$. *Сразу видно, что* φ_S — гомоморфизм колец. Кроме того, всякий элемент из $\varphi_S(S)$ обратим в $S^{-1}A$ (обратным к $s/1$ служит $1/s$).

Пусть $\mathscr{C}$ — категория, объектами которой служат кольцевые гомоморфизмы

$$f\colon A\to B,$$

такие, что для всякого $s\in S$ элемент $f(s)$ обратим в B. Если $f\colon A\to B$ и $f'\colon A\to B'$ — два объекта в $\mathscr{C}$, то морфизм g из f в f' — *это гомоморфизм*

$$g\colon B\to B',$$

для которого коммутативна диаграмма

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & {\scriptstyle f'}\searrow \quad \swarrow{\scriptstyle g} & \\ & B' & \end{array}$$

Мы утверждаем, что φ_S — универсальный объект в этой категории $\mathscr{C}$.

Доказательство. Предположим, что $a/s = a'/s'$, или, другими словами, что пары (a, s) и (a', s') эквивалентны. Найдется $s_1 \in S$, для которого

$$s_1(s'a - sa') = 0.$$

Пусть f: $A \to B$ — объект из $\mathscr{C}$. Тогда

$$f(s_1)[f(s')f(a) - f(s)f(a')] = 0.$$

Умножая на $f(s_1)^{-1}$, а затем на $f(s')^{-1}$ и $f(s)^{-1}$, получаем

$$f(a)f(s)^{-1} = f(a')f(s')^{-1}.$$

Следовательно, мы можем определить отображение

$$h\colon\ S^{-1}A \to B,$$

при котором $h(a/s) = f(a)f(s)^{-1}$ для всех $a/s \in S^{-1}A$. Тривиально проверяется, что h — гомоморфизм, приводящий к нужной коммутативной диаграмме. Тривиально проверяется также, что такой гомоморфизм h единствен и, следовательно, φ_S есть универсальный объект, что и требовалось доказать.

Пусть A — целостное кольцо и S — мультипликативное подмножество, не содержащее 0. Тогда отображение

$$\varphi_S\colon\ A \to S^{-1}A$$

инъективно.

Действительно, по определению равенство $a/1 = 0$ означает, что существует $s \in S$, для которого $sa = 0$ и, следовательно, $a = 0$.

Наиболее важными примерами мультипликативных множеств являются следующие.

(i) Пусть A — кольцо и S — множество обратимых элементов в A (т. е. множество единиц). Тогда S, очевидно, мультипликативно и обозначается, как мы отмечали, через A^*. Если A — поле, то A^* — мультипликативная группа отличных от нуля элементов в A. В этом случае $S^{-1}A$ совпадает просто с A.

(ii) Пусть A — целостное кольцо и S — множество всех его ненулевых элементов. Тогда S — мультипликативное множество и $S^{-1}A$ — поле, называемое *полем частных* или *полем отношений кольца* A.

Обычно A отождествляют с соответствующим подмножеством в $S^{-1}A$ и пишут

$$a/s = s^{-1}a,$$

$a \in A$, $s \in S$.

(iii) Кольцо A называется *локальным кольцом*, если оно имеет единственный максимальный идеал. Если A — локальное кольцо, $\mathfrak{m}$ — его максимальный идеал и $x \in A$, $x \notin \mathfrak{m}$, то элемент x обратим (иначе x порождал бы собственный идеал, не содержащийся в $\mathfrak{m}$, что невозможно). Пусть A — некоторое кольцо и $\mathfrak{p}$ — его простой идеал. Обозначим через S дополнение к $\mathfrak{p}$ в A. Тогда S — мультипликативное подмножество в A и $S^{-1}A$ обозначается символом $A_{\mathfrak{p}}$. Это локальное кольцо (см. упражнение 3); оно называется *локальным кольцом кольца A в $\mathfrak{p}$*.

Пусть A — кольцо и S — некоторое его мультипликативное подмножество. Обозначим через $J(A)$ множество всех идеалов в A. Мы можем определить отображение

$$\psi_S\colon J(A) \to J(S^{-1}A),$$

положив $\psi_S(\mathfrak{a}) = S^{-1}\mathfrak{a}$, где $S^{-1}\mathfrak{a}$ — подмножество в $S^{-1}A$, состоящее из всех дробей a/s с $a \in \mathfrak{a}$ и $s \in S$. Читатель легко проверит, что $S^{-1}\mathfrak{a}$ будет $S^{-1}A$-идеалом и что ψ_S является гомоморфизмом как для аддитивной, так и для мультипликативной структур моноида на множестве $J(A)$. Кроме того, ψ_S сохраняет также пересечения и включения; другими словами, для любых идеалов $\mathfrak{a}$, $\mathfrak{b}$ из A мы имеем

$$S^{-1}(\mathfrak{a}+\mathfrak{b}) = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b}, \quad S^{-1}(\mathfrak{ab}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b}),$$
$$S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}.$$

Для примера докажем последнее соотношение. Пусть $x \in \mathfrak{a} \cap \mathfrak{b}$. Тогда x/s лежит как в $S^{-1}\mathfrak{a}$, так и в $S^{-1}\mathfrak{b}$, так что включение левой части в правую тривиально. Обратно, пусть мы имеем элемент из $S^{-1}A$, который может быть записан в виде $a/s = b/s'$, где $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ и s, $s' \in S$. Тогда найдется элемент $s_1 \in S$, такой, что

$$s_1 s' a = s_1 s b,$$

и этот элемент лежит как в $\mathfrak{a}$, так и в $\mathfrak{b}$. Следовательно, элемент

$$a/s = s_1 s' a / s_1 s' s$$

лежит в $S^{-1}(\mathfrak{a} \cap \mathfrak{b})$, что и требовалось доказать.

§ 4. Кольца главных идеалов

И в этом параграфе „кольцо" означает „коммутативное кольцо".

Пусть A — целостное кольцо. Элемент $a \neq 0$ называется *неприводимым*, если он не является единицей и если из равенства $a = bc$ с $b \in A$ и $c \in A$ следует, что b или c — единица.

Пусть $a \neq 0$ — некоторый элемент в A, и пусть главный идеал (a) простой. Тогда a неприводим. Действительно, если $a = bc$, то один из множителей, скажем b, лежит в (a). Тогда мы можем написать $b = ad$, где d — некоторый элемент из A и, следовательно, $a = acd$. Поскольку A целостное, отсюда следует, что $cd = 1$, другими словами, что c — единица.

Утверждение, обратное предыдущему, верно не всегда. Мы обсудим, при каких условиях оно верно. Говорят, что элемент $a \in A$, $a \neq 0$, обладает *однозначным разложением на неприводимые элементы*, если в A существуют единица u и неприводимые элементы p_i $(i = 1, \ldots, r)$, такие, что

$$a = u \prod_{i=1}^{r} p_i,$$

причем для двух таких разложений на неприводимые элементы

$$a = u \prod_{i=1}^{r} p_i = u' \prod_{j=1}^{s} q_j,$$

мы имеем $r = s$ и после перестановки индексов i $p_i = u_i q_i$, где u_i — некоторые единицы в A, $i = 1, \ldots, r$.

Отметим, что если p — неприводимый элемент и u — единица, то up — тоже неприводимый элемент, так что при разложении на множители мы должны допускать умножение на единицы. В кольце целых чисел $\mathbf{Z}$ отношение порядка позволяет нам выделить один неприводимый элемент (положительное простое число) из двух возможных (а именно, $\pm p$), отличающихся друг от друга на множитель, являющийся единицей. В более общих кольцах это, конечно, невозможно.

Допуская в предыдущем равенстве $r = 0$, мы принимаем соглашение, что всякая единица кольца A имеет разложение на неприводимые элементы.

Кольцо называется *факториальным* (или кольцом с однозначным разложением на множители), если оно целостное и если всякий элемент $\neq 0$ имеет однозначное разложение на неприводимые элементы. Мы докажем ниже, что всякое целостное кольцо главных идеалов факториально.

Пусть A — целостное кольцо и $a, b \in A$, $ab \neq 0$. Мы говорим, что *a делит b*, и пишем $a \mid b$, если существует элемент $c \in A$, для

которого $ac = b$. Мы говорим, что элемент $d \in A$, $d \neq 0$, является *наибольшим общим делителем* (сокращенно н. о. д.) элементов a и b, если $d \mid a$, $d \mid b$ и если любой элемент e из A, $e \neq 0$, делящий и a, и b, делит также d.

Предложение 2. *Пусть A — целостное кольцо главных идеалов и $a, b \in A$, $a, b \neq 0$. Если $(a, b) = (c)$, то c — наибольший общий делитель элементов a и b.*

Доказательство.. Так как b лежит в идеале (c), то $b = xc$ для некоторого $x \in A$, или, что то же самое, $c \mid b$. Аналогично $c \mid a$. Пусть d делит и a, и b, т. е. $a = dy$, $b = dz$, где $y, z \in A$. Так как c лежит в (a, b), то

$$c = wa + tb$$

с некоторыми w, $t \in A$. Тогда $c = w\,dy + t\,dz = d(wy + tz)$, откуда $d \mid c$ и наше предложение доказано.

Теорема 1. *Всякое целостное кольцо A главных идеалов факториально.*

Доказательство. Мы докажем сначала, что всякий ненулевой элемент в A имеет разложение на неприводимые элементы. Обозначим через S — множество главных идеалов $\neq 0$, образующие которых не имеют разложения на неприводимые элементы; предположим, что S не пусто. Пусть (a_1) лежит в S. Рассмотрим произвольную возрастающую цепочку

$$(a_1) \subsetneqq (a_2) \subsetneqq \ldots \subsetneqq (a_n) \subsetneqq \ldots$$

идеалов из S. Мы утверждаем, что она не может быть бесконечной. Действительно, объединение идеалов такой цепочки будет идеалом в A, причем главным, равным, скажем (a). Образующая a должна лежать в некотором элементе цепочки, скажем в (a_n), а тогда

$$(a_n) \subset (a) \subset (a_n),$$

откуда вытекает, что цепочка обрывается на (a_n). Следовательно любой идеал в A, содержащий (a_n) и $\neq (a_n)$, имеет образующую допускающую разложение на неприводимые множители.

Заметим теперь, что элемент a_n не может быть неприводимым (иначе он имел бы разложение) и, следовательно, $a_n = bc$, где ни b, ни c не являются единицей. Но тогда $(b) \neq (a_n)$ и $(c) \neq (a_n)$, а потому и b, и c обладают разложениями на неприводимые множители. Произведение этих разложений будет разложением для a_n вопреки предположению, что S не пусто.

Чтобы доказать единственность, заметим сначала, что если p — неприводимый элемент в A, $a, b \in A$, $p \mid ab$, то $p \mid a$ или $p \mid b$. Дока-

зательство. Если $p \nmid a$, то н. о. д. элементов p и a равен 1 и, следовательно,

$$1 = xp + ya$$

для некоторых $x, y \in A$. Тогда $b = bxp + yab$, а поскольку $p \mid ab$, мы заключаем, что $p \mid b$.

Предположим теперь, что a имеет два разложения

$$a = p_1 \dots p_r = q_1 \dots q_s$$

на неприводимые элементы. Так как p_1 делит произведение, стоящее справа, то p_1 делит один из его сомножителей, причем после их перенумерации мы можем считать, что это q_1. Тогда найдется единица u_1, для которой $q_1 = u_1 p_1$. Сокращая оба разложения на p_1, получаем

$$p_2 \dots p_r = u_1 q_2 \dots q_s.$$

Доказательство завершается по индукции.

Можно было бы называть два элемента a, $b \in A$ эквивалентными, если существует единица u, такая, что $a = bu$. Выберем по одному элементу p из каждого класса эквивалентности, состоящего из неприводимых элементов, и обозначим через P множество таких представителей. Пусть $a \in A$, $a \neq 0$. Тогда существуют единица u и целые числа $\nu(p) \geqslant 0$, равные 0 для почти всех $p \in P$, такие, что

$$a = u \prod_{p \in P} p^{\nu(p)}.$$

При этом единица u и целые числа $\nu(p)$ однозначно определены элементом a. Мы называем $\nu(p)$ *порядком* элемента a в p, обозначая его также символом $\operatorname{ord}_p a$.

Если A — факториальное кольцо, то всякий неприводимый элемент p порождает простой идеал (p). Поэтому в факториальном кольце неприводимые элементы будут также называться *простыми*.

Заметим, что можно обычным способом определить понятие *наименьшего общего кратного* (н. о. к.) конечного числа ненулевых элементов кольца A. Именно, мы полагаем н. о. к. элементов $a_1, \dots, a_n \in A$ равным любому элементу $c \in A$, удовлетворяющему условию

$$\operatorname{ord}_p c = \max_i \operatorname{ord}_p a_i$$

для всех простых элементов p из A. Такой элемент c определен однозначно с точностью до множителя, являющегося единицей.

Мы говорим, что ненулевые элементы a, $b \in A$ *взаимно просты*, если $(a, b) = (1)$. Это означает, что н. о. д. элементов a и b есть единица.

Пример Кольцо целых чисел $\mathbf{Z}$ факториально. Его группа единиц состоит из 1 и -1. Естественно брать в качестве представителя класса

эквивалентности данного простого элемента положительный простой элемент (называемый простым числом) при возможном выборе из двух элементов p и $-p$. Аналогично, как мы покажем позднее, кольцо многочленов от одной переменной над полем факториально, и в качестве представителей простых элементов в этом кольце обычно выбирают неприводимые многочлены со старшим коэффициентом 1.

УПРАЖНЕНИЯ

Все кольца предполагаются коммутативными

1. Пусть A — кольцо с $1 \neq 0$, S — его мультипликативное подмножество, не содержащее 0. Пусть, далее, $\mathfrak{p}$ — максимальный элемент в множестве идеалов кольца A, пересечение которых с S пусто. Показать, что $\mathfrak{p}$ — простой.

2. Пусть $f\colon A \to A'$ — сюръективный гомоморфизм колец. Показать, что если кольцо A — локальное, то и кольцо A' — локальное.

3. Пусть A — кольцо и $\mathfrak{p}$ — простой идеал. Показать, что $A_{\mathfrak{p}}$ имеет единственный максимальный идеал, состоящий из всех элементов вида $a's$, где $a \in \mathfrak{p}$ и $s \notin \mathfrak{p}$.

4. Пусть A — кольцо главных идеалов и S — его мультипликативное подмножество. Показать, что $S^{-1}A$ — кольцо главных идеалов.

5. Пусть A — факториальное кольцо и S — его мультипликативное подмножество. Показать, что $S^{-1}A$ факториально и что простые элементы в $S^{-1}A$ — это те простые p из A, для которых $(p) \cap S$ пусто.

6. Пусть A — кольцо главных идеалов, $a_1, \ldots, a_n$ — ненулевые элементы из A и $(a_1, \ldots, a_n) = (d)$. Показать, что d — наибольший общий делитель для a_i $(i = 1, \ldots, n)$.

7. Пусть p — простое число, A — кольцо $\mathbf{Z}/p^r\mathbf{Z}$ (r — целое число $\geqslant 1$). Пусть $G = A^*$ — группа единиц в A, т. е. группа классов вычетов по модулю p^r, взаимно простых с модулем. Показать, что G — циклическая, за исключением случая, когда

$$p = 2, \quad r \geqslant 3;$$

в этом случае она является группой типа $(2, 2^{r-2})$.

[*Указание*: в общем случае показать, что G — произведение циклической группы, порожденной элементом $1 + p$, на циклическую группу порядка $p - 1$. В исключительном случае показать, что G — произведение группы $\{\pm 1\}$ на циклическую группу, порожденную классом вычетов числа 5 по модулю 2^r.]

8. Пусть i — комплексное число $\sqrt{-1}$. Показать, что $\mathbf{Z}[i]$ — кольцо главных идеалов и, следовательно, факториально. Каковы в нем единицы?

9. Пусть A — кольцо целых функций на комплексной плоскости. Показать, что всякий конечно порожденный идеал в A является главным. Каковы главные простые идеалы в A? Каковы единицы в A? Показать, что A не факториально.

Глава III

Модули

§ 1. Основные определения

Пусть A — кольцо. *Левый модуль* над A, или левый A-модуль M, — это абелева группа, обычно (записываемая аддитивно, вместе с некоторым действием A на M при этом A рассматривается как мультипликативный моноид согласно КО 2), таким, что для всех a, $b \in A$ и x, $y \in M$ выполнены соотношения

$$(a+b)x = ax + bx \quad \text{и} \quad a(x+y) = ax + ay.$$

Мы предоставляем читателю доказать, что $a(-x) = -ax$ и что $0x = 0$. По определению действия $1x = x$.

Аналогичным образом определяют *правый* A-модуль. Мы будем иметь дело только с левыми A-модулями, если не оговорено противное, и поэтому будем называть их просто A-модулями или даже модулями, когда ясно, о каком кольце идет речь.

Примеры.

Отметим, что A есть модуль над собой.

Любая коммутативная группа является $\mathbf{Z}$-модулем.

Аддитивная группа, состоящая из одного 0, является модулем над любым кольцом.

Любой левый идеал в A есть модуль над A.

Пусть S — непустое множество и M — некоторый A-модуль. Множество отображений $\mathfrak{M}(S, M)$ будет $\mathbf{Z}$-модулем. Мы уже отмечали раньше, что это коммутативная группа. Если теперь $f \in \mathfrak{M}(S, M)$, $a \in A$, то считаем af отображением, для которого $(af)(s) = af(s)$. Аксиомы модуля проверяются тривиально.

В остальной части этого параграфа мы будем иметь дело с фиксированным кольцом A и, таким образом, можем опускать приставку A-.

Пусть M — модуль. Под *подмодулем* N в M мы понимаем такую аддитивную подгруппу, что $AN \subset N$. Очевидно, N есть модуль (с действием, индуцированным действием A на M).

Пусть $\mathfrak{a}$ — левый идеал и M — модуль. Множество $\mathfrak{a}M$ всех элементов

$$a_1x_1 + \ldots + a_nx_n,$$

где $a_i \in \mathfrak{a}$ и $x_i \in M$, будет, очевидно, подмодулем в M. Имеет место ассоциативность, а именно для любых левых идеалов $\mathfrak{a}$, $\mathfrak{b}$

$$\mathfrak{a}(\mathfrak{b}M) = (\mathfrak{a}\mathfrak{b})M.$$

Имеют место также некоторые очевидные соотношения дистрибутивности, например $(\mathfrak{a}+\mathfrak{b})M = \mathfrak{a}M + \mathfrak{b}M$. Если N и N' — подмодули в M, то $\mathfrak{a}(N+N') = \mathfrak{a}N + \mathfrak{a}N'$.

Пусть M—A-модуль и N—его подмодуль. Определим структуру модуля на факторгруппе M/N (для уже имеющейся структуры аддитивной группы). Пусть $x+N$ — некоторый смежный класс группы M по N, и пусть $a \in A$. Мы определяем $a(x+N)$ как смежный класс $ax+N$. Тривиально проверяется, что так введенное действие правильно определено (т. е. если y лежит в том же смежном классе, что и x, то ay лежит в том же смежном классе, что и ax) и что оно удовлетворяет всем необходимым условиям, так что M/N превращается в модуль, называемый *фактормодулем* модуля M по N.

Под *гомоморфизмом* модулей понимается отображение

$$f\colon M \to M'$$

одного модуля в другой (над тем же самым кольцом A), которое является гомоморфизмом аддитивных групп и для которого

$$f(ax) = af(x)$$

при всех $a \in A$ и $x \in M$. Ясно, что класс A-модулей образует категорию, морфизмами в которой служат гомоморфизмы модулей, обычно называемые просто гомоморфизмами, если это не приводит к путанице. Когда желают явно указать кольцо A, то говорят, что f является *A-гомоморфизмом*, или также, что f — *A-линейное отображение*.

Тождественное отображение всякого модуля на себя является гомоморфизмом. Для любого модуля M' отображение $\zeta\colon M \to M'$, такое, что $\zeta(x) = 0$ для всех $x \in M$, является гомоморфизмом, называемым *нулевым*.

Пусть M — модуль и N — его подмодуль. Тривиально проверяется, что канонический гомоморфизм аддитивных групп

$$f\colon M \to M/N$$

является также гомоморфизмом модулей. Столь же тривиально проверяется, что он универсален в категории гомоморфизмов модуля M, ядро которых содержит N.

Если $f\colon M \to M'$ — гомоморфизм модулей, то его ядро и образ являются подмодулями в M и M' соответственно (тривиальная проверка). Канонические гомоморфизмы, рассмотренные в гл. 1, § 4, переносятся с необходимыми изменениями и на модули. Для удобства читателя приведем сводку этих гомоморфизмов.

Пусть N, N' — два подмодуля модуля M. Тогда $N+N'$ будет также подмодулем и имеет место изоморфизм

$$N/N\cap N'\approx(N+N')/N'.$$

Если $M\supset M'\supset M''$ — модули, то

$$(M/M'')/(M'/M'')\approx M/M'.$$

Если $f\colon M\to M'$ — гомоморфизм модулей и N' — подмодуль в M', то $f^{-1}(N')$ есть подмодуль в M и имеет место канонический инъективный гомоморфизм

$$\overline{f}\colon M/f^{-1}(N')\to M'/N'.$$

Если гомоморфизм f сюръективен, то $\overline{f}$ — изоморфизм модулей.

Доказательства сводятся к проверке того, что все гомоморфизмы, с которыми мы имели дело, занимаясь абелевыми группами, являются теперь A-гомоморфизмами модулей. Эту проверку мы предоставляем читателю.

Отметим, что, как и в случае групп, гомоморфизм модулей, являющийся биективным отображением, будет изоморфизмом модулей. Здесь вновь доказательство то же, что и для групп (нужно только заметить, что обратное отображение, являющееся, как мы знаем, изоморфизмом групп, есть на самом деле изоморфизм модулей). Проверка снова предоставляется читателю.

Как и в случае абелевых групп, мы называем последовательность гомоморфизмов модулей

$$M'\xrightarrow{f}M\xrightarrow{g}M''$$

точной, если $\operatorname{Im} f=\operatorname{Ker} g$. С подмодулем N модуля M ассоциируется точная последовательность

$$0\to N\to M\to M/N\to 0,$$

где отображение N в M есть включение, а последующее отображение — каноническое. Понятие точности принадлежит Эйленбергу — Стинроду.

§ 2. Группа гомоморфизмов

Пусть A — кольцо и X, X' — A-модули. Мы обозначаем через $\operatorname{Hom}_A(X', X)$ множество A-гомоморфизмов модуля X' в X. Тогда $\operatorname{Hom}_A(X', X)$ есть абелева группа, причем закон сложения — это закон сложения отображений в абелеву группу.

Если кольцо A коммутативно, то мы можем превратить $\operatorname{Hom}_A(X', X)$ в A-модуль, взяв в качестве af с $a\in A$ и $f\in\operatorname{Hom}_A(X', X)$ отображение, для которого

$$(af)(x)=af(x).$$

Проверка аксиом A-модуля тривиальна. Однако если A не коммутативно, то приходится рассматривать $\mathrm{Hom}_A(X', X)$ просто как абелеву группу.

Можно также рассматривать Hom_A как функтор. В действительности это функтор от двух аргументов, контравариантный по первому аргументу и ковариантный по второму. В самом деле, пусть Y — A-модуль и

$$X' \xrightarrow{f} X$$

— A-гомоморфизм. Тогда имеем индуцированный гомоморфизм

$$\mathrm{Hom}_A(f, Y)\colon \mathrm{Hom}_A(X, Y) \to \mathrm{Hom}_A(X', Y)$$

(обращение стрелки!), задаваемый правилом

$$g \longmapsto g \circ f.$$

Это иллюстрируется следующей последовательностью отображений

$$X' \xrightarrow{f} X \xrightarrow{g} Y.$$

Тот факт, что $\mathrm{Hom}_A(f, Y)$ будет гомоморфизмом, представляет собой просто перефразировку свойства $(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$, которое тривиально проверяется. Если $f = \mathrm{id}$, то композиция с f действует на g как тождественное отображение, т. е. $g \circ \mathrm{id} = g$.

Имея последовательность A-гомоморфизмов

$$X' \to X \to X'',$$

мы получаем индуцированную последовательность

$$\mathrm{Hom}_A(X', Y) \leftarrow \mathrm{Hom}_A(X, Y) \leftarrow \mathrm{Hom}_A(X'', Y).$$

Для всякой точной последовательности

$$X' \xrightarrow{\lambda} X \longrightarrow X'' \longrightarrow 0$$

индуцированная последовательность

$$\mathrm{Hom}_A(X', Y) \leftarrow \mathrm{Hom}_A(X, Y) \leftarrow \mathrm{Hom}_A(X'', Y) \leftarrow 0$$

точна.

Это важный факт, доказательство которого тривиально. Например, если $g\colon X'' \to Y$ — A-гомоморфизм, то его образом в $\mathrm{Hom}_A(X, Y)$ будет композиция g с сюръективным отображением X на X''. Если эта композиция равна 0, то $g = 0$, поскольку $X \to X''$ сюръективно. В качестве другого примера рассмотрим гомоморфизм $g\colon X \to Y$, для которого композиция

$$X' \xrightarrow{\lambda} X \xrightarrow{g} Y$$

равна 0. Тогда g обращается в 0 на образе λ. Отображение g, таким образом, можно разложить посредством фактормодуля

$$\begin{array}{ccc} & X/\mathrm{Im}\,\lambda & \\ \nearrow & & \searrow \\ X & \xrightarrow[g]{} & Y \end{array}$$

Так как $X \to X''$ сюръективно, то имеем изоморфизм

$$X/\mathrm{Im}\,\lambda \leftrightarrow X''.$$

Следовательно, мы можем пропустить g через X'', показав тем самым, что ядро гомоморфизма

$$\mathrm{Hom}_A(X',\ Y) \leftarrow \mathrm{Hom}_A(X,\ Y)$$

содержится в образе гомоморфизма

$$\mathrm{Hom}_A(X,\ Y) \leftarrow \mathrm{Hom}_A(X'',\ Y).$$

Проверка других условий, необходимых для точности, предоставляется читателю.

Аналогичную ситуацию мы имеем и по отношению ко второму аргументу, только в этом случае функтор ковариантен. Таким образом, для фиксированного X и последовательности A-гомоморфизмов

$$Y' \to Y \to Y''$$

имеем индуцированную последовательность

$$\mathrm{Hom}_A(X,\ Y') \to \mathrm{Hom}_A(X,\ Y) \to \mathrm{Hom}_A(X,\ Y'').$$

Для всякой точной последовательности

$$0 \to Y' \to Y \to Y''$$

индуцированная последовательность

$$0 \to \mathrm{Hom}_A(X,\ Y') \to \mathrm{Hom}_A(X,\ Y) \to \mathrm{Hom}_A(X,\ Y'')$$

точна.

Доказательство предоставляется читателю. Оно немедленно вытекает из определений.

Отметим, что точность последовательности

$$0 \to Y' \to Y$$

означает, что модуль Y' вкладывается в Y, т. е. изоморфен подмодулю в Y. Если $Y' \subset Y$, то всякий гомоморфизм в Y' может рассматриваться как гомоморфизм в Y. Это соответствует вложению

$$0 \to \mathrm{Hom}_A(X,\ Y') \to \mathrm{Hom}_A(X,\ Y).$$

Пусть M — A-модуль. Из соотношений

$$(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$$

и их правого аналога, а именно

$$g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2,$$

а также из того факта, что существует единичный элемент для композиции, именно id_M, мы заключаем, что $\mathrm{Hom}_A(M, M)$ есть кольцо, умножением в котором служит композиция отображений. Если n—целое число $\geqslant 1$, то мы можем писать f^n для обозначения n-кратной итерации f и можем определить f^0 как id. Согласно общему определению эндоморфизмов в категории, мы можем также писать $\mathrm{End}_A M$ вместо $\mathrm{Hom}_A(M, M)$.

Так как A-модуль M—абелева группа, то $\mathrm{Hom}_{\mathbf{Z}}(M, M)$ (=множеству групповых гомоморфизмов M в себя) есть кольцо и мы могли бы определить действие A на M как кольцевой гомоморфизм $A \to \mathrm{Hom}_{\mathbf{Z}}(M, M)$.

§ 3. *Прямые произведения и суммы модулей*

Пусть A — кольцо. Как и в случае абелевых групп, копроизведение в категории A-модулей называется прямой суммой.

Предложение 1. *Прямые произведения и прямые суммы в категории A-модулей существуют.*

Доказательство. Доказательство в случае произведения мы предоставляем читателю в качестве упражнения. В качестве образца мы рассмотрим случай суммы, следуя конструкции, данной для прямой суммы абелевых групп. Пусть $\{M_i\}_{i \in I}$ — семейство A-модулей и

$$M = \coprod_{i \in I} M_i$$

— их прямая сумма как абелевых групп. Определим на M структуру A-модуля. Если $(x_i)_{i \in I}$ — элемент из M, т. е. такое семейство элементов $x_i \in M_i$, что $x_i = 0$ для почти всех i, и если $a \in A$, то положим

$$a(x_i)_{i \in I} = (ax_i)_{i \in I},$$

задавая тем самым умножение на a покомпонентно. Тривиально проверяется, что это есть действие A на M, превращающее M в A-модуль. Если читатель обратится теперь к данному ранее доказательству существования прямых сумм в категории абелевых групп, то он сразу увидит, что его можно продолжить в том же плане, с тем чтобы показать, что M есть прямая сумма семейства $\{M_i\}_{i \in I}$ как A-модулей (например, отображение

$$\lambda_j \colon M_j \to M,$$

для которого $\lambda_j(x)$ имеет j-ю компоненту, равную x, и i-ю компоненту, равную 0, при $i \neq j$, теперь, как легко видеть, будет A-гомоморфизмом). Для данного семейства A-гомоморфизмов $\{f_i\colon M_i \to N\}$ отображение f, определенное в доказательстве для абелевых групп, является также A-гомоморфизмом и обладает всеми необходимыми свойствами.

В случае когда I—конечное множество, имеется полезный критерий представимости модуля в виде прямого произведения.

Предложение 2. *Пусть M—A-модуль и n—целое число $\geqslant 1$. Для каждого $i = 1, \ldots, n$ пусть $\varphi_i\colon M \to M$ — A-гомоморфизм, такой, что*

$$\sum_{i=1}^{n} \varphi_i = \mathrm{id} \quad \text{и} \quad \varphi_i \circ \varphi_j = 0 \text{ для } i \neq j.$$

Тогда $\varphi_i^2 = \varphi_i$ для всех i. Положим $M_i = \varphi_i(M)$ и возьмем отображение $\varphi\colon M \to \prod M_i$, для которого

$$\varphi(x) = (\varphi_1(x), \ldots, \varphi_n(x)).$$

Тогда φ будет A-изоморфизмом M на прямое произведение $\prod M_i$.

Доказательство. Для каждого j имеем

$$\varphi_j = \varphi_j \circ \mathrm{id} = \varphi_j \circ \sum_{i=1}^{n} \varphi_i = \varphi_j \circ \varphi_j = \varphi_j^2,$$

что доказывает первое утверждение. Ясно, что φ — A-гомоморфизм. Пусть x лежит в его ядре. Так как

$$x = \mathrm{id}(x) = \sum_{i=1}^{n} \varphi_i(x),$$

то мы заключаем, что $x = 0$, так что φ инъективно. Пусть для каждого $i = 1, \ldots, n$ заданы элементы $y_i \in M_i$. Положим $x = y_1 + \ldots + y_n$. Очевидно, $\varphi_j(y_i) = 0$ при $i \neq j$. Следовательно,

$$\varphi_j(x) = y_j$$

для каждого $j = 1, \ldots, n$. Это доказывает, что φ сюръективно, и завершает доказательство нашего предложения.

Заметим, что в том случае, когда I — конечное множество, прямая сумма и прямое произведение совпадают.

Как и в случае абелевых групп, для обозначения прямой суммы мы используем символ $\bigoplus$.

Пусть M — модуль над кольцом A и S — подмножество в M. Под *линейной комбинацией* элементов из S (с коэффициентами в A) понимают сумму

$$\sum_{x \in S} a_x x,$$

где $\{a_x\}$ — некоторое множество элементов из A, почти все из которых равны 0. Эти элементы a_x называются *коэффициентами* линейной комбинации. Пусть N — множество всех линейных комбинаций элементов из S. Тогда N — подмодуль в M, так как если

$$\sum_{x\in S} a_x x \quad \text{и} \quad \sum_{x\in S} b_x x$$

— две линейные комбинации, то их сумма равна

$$\sum_{x\in S} (a_x + b_x)\, x,$$

а если $c \in A$, то

$$c\left(\sum_{x\in S} a_x x\right) = \sum_{x\in S} c a_x x,$$

и эти элементы снова являются линейными комбинациями элементов из S. Мы будем называть N подмодулем, *порожденным* S, а S — множеством *образующих* для N. Иногда мы будем писать $N = A\langle S\rangle$. Если S состоит из одного элемента x, то модуль, порожденный x, записывается также в виде Ax или просто (x), и иногда мы будем говорить, что (x) есть *главный модуль*.

Модуль M называется *конечно порожденным*, или модулем *конечного типа*, если он имеет конечное число образующих.

Подмножество S модуля M называется *линейно независимым* (над A), если из равенства нулю линейной комбинации

$$\sum_{x\in S} a_x x$$

обязательно вытекает, что $a_x = 0$ для всех $x \in S$. Если S линейно независимо и если две линейные комбинации

$$\sum a_x x \quad \text{и} \quad \sum b_x x$$

равны, то $a_x = b_x$ для всех $x \in S$. Действительно, вычитание одной линейной комбинации из другой дает $\sum (a_x - b_x)\, x = 0$, откуда $a_x - b_x = 0$ для всех x. Если подмножество S линейно независимо, то мы будем также говорить, что его элементы линейно независимы. Аналогично *семейство* $\{x_i\}_{i\in I}$ элементов из M называется линейно независимым, если, какова бы ни была линейная комбинация

$$\sum_{i\in I} a_i x_i = 0,$$

$a_i = 0$ для всех i. Подмножество S (соответственно семейство $\{x_i\}$) называется *линейно зависимым*, если оно не является линейно независимым, т. е. если существует соотношение

$$\sum_{x\in S} a_x x = 0 \quad \left(\text{соответственно } \sum_{i\in I} a_i x_i = 0\right),$$

в котором не все a_x (соответственно a_i) $= 0$.

Предостережение. Пусть x — какой-нибудь элемент из M, являющийся линейно независимым. Тогда семейство $\{x_i\}_{i=1, \ldots, n}$, в котором $x_i = x$ для всех i, линейно зависимо, если $n > 1$, но множество, состоящее из самого x, линейно независимо.

Пусть M — A-модуль и $\{M_i\}_{i \in I}$ — некоторое семейство его подмодулей Имея гомоморфизмы включения

$$\lambda_i\colon M_i \to M,$$

получаем индуцированный гомоморфизм

$$\lambda_*\colon \prod M_i \to M,$$

такой, что для любого семейства элементов $(x_i)_{i \in I}$, среди которых все, кроме конечного числа, равны 0,

$$\lambda_*((x_i)) = \sum_{i \in I} x_i.$$

Если λ_* — изоморфизм, то мы говорим, что семейство $\{M_i\}_{i \in I}$ *есть разложение M в прямую сумму*. Это, очевидно, равносильно тому, что всякий элемент из M имеет единственное представление в виде суммы

$$\sum x_i,$$

где $x_i \in M_i$ и почти все $x_i = 0$ Допуская неточность в обозначениях, мы в этом случае будем также писать

$$M = \prod M_i.$$

Если семейство $\{M_i\}$ таково, что всякий элемент из M допускает *какое-то* представление в виде суммы $\sum x_i$ (не обязательно единственное), то мы будем писать $M = \sum M_i$. В общем случае, если $\{M_i\}$ — произвольное семейство подмодулей, то образ определенного выше гомоморфизма λ_* есть подмодуль в M, который будет обозначаться через $\sum M_i$.

Если M — модуль и N, N' — два таких его подмодуля, что $N + N' = M$ и $N \cap N' = 0$, то имеет место изоморфизм модулей

$$M \approx N \oplus N',$$

точно так же как и в случае абелевых групп, и аналогично для конечного числа подмодулей

Отметим, что наше изложение теории абелевых групп есть, разумеется, частный случай теории модулей просто потому, что абелевы группы можно рассматривать как модули над $\mathbf{Z}$ Однако обычно представляется желательным (хотя это и непроизводительно) получать сначала некоторые результаты для абелевых групп, а затем указывать,

что они, вообще говоря, справедливы (очевидным образом) и для модулей.

Пусть M, M', N — модули. Тогда имеет место изоморфизм абелевых групп

$$\boxed{\mathrm{Hom}_A(M \oplus M',\ N) \xleftarrow{\approx} \mathrm{Hom}_A(M,\ N) \times \mathrm{Hom}_A(M',\ N)}$$

и аналогично

$$\boxed{\mathrm{Hom}_A(N,\ M \times M') \xleftarrow{\approx} \mathrm{Hom}_A(N,\ M) \oplus \mathrm{Hom}_A(N,\ M')}.$$

Первый из изоморфизмов получается следующим образом. Если f: $M \oplus M' \to N$ — гомоморфизм, то f индуцирует гомоморфизмы f_1: $M \to N$ и f_2: $M' \to N$ посредством композиции с вложениями соответственно M и M' в их прямую сумму

$$M \to M \oplus \{0\} \subset M \oplus M' \xrightarrow{f} N,$$

$$M' \to \{0\} \oplus \{M'\} \subset M \oplus M' \xrightarrow{f} N.$$

Мы предоставляем читателю проверить, что сопоставление

$$f \longmapsto (f_1,\ f_2)$$

и дает изоморфизм, указанный в первой рамке. Изоморфизм во второй рамке получается аналогичным способом. Если даны гомоморфизмы f_1: $N \to M$ и f_2: $N \to M'$, то имеет место гомоморфизм f: $N \to M \times M'$, определяемый формулой

$$f(x) = (f_1(x),\ f_2(x)).$$

Тривиально проверяется, что сопоставление

$$(f_1,\ f_2) \longmapsto f$$

дает изоморфизм, указанный во второй рамке.

Конечно, прямая сумма и прямое произведение двух модулей изоморфны, но мы различаем их в обозначениях из соображений функториальности.

Предложение 3. *Пусть* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *— точная последовательность модулей. Следующие условия эквивалентны:*

(1) *Существует гомоморфизм* φ: $M'' \to M$, *такой, что* $g \circ \varphi = \mathrm{id}$.

(2) *Существует гомоморфизм* ψ: $M \to M'$, *такой, что* $\psi \circ f = \mathrm{id}$.

При выполнении этих условий имеют место изоморфизмы

$$M = \mathrm{Im}\, f \oplus \mathrm{Ker}\, \psi, \quad M = \mathrm{Ker}\, g \oplus \mathrm{Im}\, \varphi,$$

$$M \approx M' \oplus M''.$$

Доказательство. Выпишем гомоморфизмы из правой части последовательности

$$M \underset{\varphi}{\overset{g}{\rightleftarrows}} M'' \to 0.$$

Пусть $x \in M$. Тогда разность

$$x - \varphi(g(x))$$

лежит в ядре g и, следовательно, $M = \operatorname{Ker} g + \operatorname{Im} \varphi$.

Эта сумма прямая, так как если

$$x = y + z,$$

где $y \in \operatorname{Ker} g$ и $z \in \operatorname{Im} \varphi$, то $z = \varphi(w)$; здесь $w \in M''$, и, применяя g, получаем, что $w = g(x)$. Таким образом, w однозначно определен элементом x, а потому z однозначно определен элементом x. Следовательно, то же справедливо и для y; тем самым доказано, что сумма прямая.

Рассуждения, относящиеся к другой части последовательности, аналогичны, и проведение их предоставляется читателю в качестве упражнения, равно как и доказательство эквивалентности обоих условий. В случае когда эти условия удовлетворяются, говорят, что точная последовательность из предложения 3 *расщепляется*.

§ 4. Свободные модули

Пусть M — модуль над кольцом A и S — подмножество в M. Мы будем говорить, что S — *базис модуля* M, если S не пусто, порождает M и линейно независимо. В частности, если S — базис M, то $M \neq \{0\}$ при условии, что $A \neq \{0\}$, и всякий элемент из M имеет единственное представление в виде линейной комбинации элементов из S. Аналогично мы говорим, что непустое семейство $\{x_i\}_{i \in I}$ элементов из M образует *базис* в M, если оно линейно независимо и порождает M.

Всякое кольцо, рассматриваемое как модуль над собой, обладает базисом, состоящим из единичного элемента 1.

Пусть I — непустое множество, и для каждого $i \in I$ пусть $A_i = A$, причем все A_i рассматриваются как A-модули. Положим

$$F = \coprod_{i \in I} A_i.$$

Модуль F обладает базисом, состоящим из элементов e_i в F, i-й компонентой которых является единичный элемент из A_i, а все другие компоненты равны 0.

Под *свободным* модулем мы будем понимать модуль, обладающий базисом, или же нулевой модуль.

Теорема 1. *Пусть A — кольцо и M — модуль над A с базисом $\{x_\iota\}_{\iota\in I}$, где I — непустое множество. Пусть, далее, N есть A-модуль и $\{y_\iota\}_{\iota\in I}$ — семейство элементов в N. Тогда существует единственный гомоморфизм $f\colon M\to N$, такой, что $f(x_\iota)=y_\iota$ для всех ι.*

Доказательство. Пусть x — некоторый элемент из M. Существует единственное семейство $\{a_\iota\}_{\iota\in I}$ элементов из A, для которого

$$x=\sum_{\iota\in I} a_\iota x_\iota.$$

Положим

$$f(x)=\sum a_\iota y_\iota.$$

Ясно, что f — гомоморфизм, удовлетворяющий нашим требованиям, и что это единственный такой гомоморфизм, так как мы должны иметь

$$f(x)=\sum a_\iota f(x_\iota).$$

Следствие 1. *В обозначениях теоремы предположим, что $\{y_\iota\}_{\iota\in I}$ — базис в N. Тогда гомоморфизм f является изоморфизмом (модулей).*

Доказательство. В силу симметрии существует единственный гомоморфизм

$$g\colon N\to M,$$

такой, что $g(y_\iota)=x_\iota$ для всех ι и $f\circ g$ и $g\circ f$ являются соответствующими тождественными отображениями.

Следствие 2. *Два модуля, имеющие базисы одинаковой мощности, изоморфны.*

Доказательство. Очевидно.

Доказательства следующих утверждений предоставляем читателю в качестве упражнений.

Пусть M — свободный модуль над A с базисом $\{x_\iota\}_{\iota\in I}$, так что

$$M=\coprod_{\iota\in I} Ax_\iota.$$

Пусть $\mathfrak{a}$ — левый идеал в A. Тогда $\mathfrak{a}M$ будет подмодулем в M. Далее, $\mathfrak{a}x_\iota$ — подмодуль в Ax_ι для каждого ι. *Имеет место изоморфизм* (A-модулей)

$$\boxed{M/\mathfrak{a}M\approx\coprod_{\iota\in I} Ax_\iota/\mathfrak{a}x_\iota}.$$

Кроме того, $Ax_\iota/\mathfrak{a}x_\iota$ и $A/\mathfrak{a}$ изоморфны как A-модули.

Предположим дополнительно, что A коммутативно. Тогда $A/\mathfrak{a}$ — кольцо. Кроме того, $M/\mathfrak{a}M$ есть свободный модуль над $A/\mathfrak{a}$ и каждый фактормодуль $Ax_i/\mathfrak{a}x_i$ свободен над $A/\mathfrak{a}$. Если $\bar{x}_i$ — образ x_i при каноническом гомоморфизме

$$Ax_i \to Ax_i/\mathfrak{a}x_i,$$

то $\bar{x}_i$ служит базисом (состоящим из одного элемента) для $Ax_i/\mathfrak{a}x_i$ над $A/\mathfrak{a}$.

§ 5. Векторные пространства

Модуль над полем называется *векторным пространством.*

Теорема 2. *Пусть V — векторное пространство над полем K, причем $V \neq \{0\}$. Пусть Γ — множество образующих для V над K и S — некоторое линейно независимое подмножество в Γ. Тогда в V существует базис $\mathscr{B}$, такой, что $S \subset \mathscr{B} \subset \Gamma$.*

Доказательство. Пусть $\mathfrak{T}$ — множество, элементами которого служат подмножества T из Γ, содержащие S и линейно независимые. Тогда $\mathfrak{T}$ не пусто (оно содержит S). Мы утверждаем, что $\mathfrak{T}$ индуктивно упорядочено. Действительно, если $\{T_i\}$ — совершенно упорядоченное подмножество в T (упорядоченность по включению), то подмножество $\bigcup T_i$ также линейно независимо и содержит S. Пусть $\mathscr{B}$ — максимальный элемент в $\mathfrak{T}$, существующий по лемме Цорна. Тогда $\mathscr{B}$ линейно независимо. Пусть W — подпространство в V, порожденное $\mathscr{B}$. Если $W \neq V$, то существует некоторый элемент $x \in \Gamma$, такой, что $x \notin W$. Тогда $\mathscr{B} \cup \{x\}$ линейно независимо. Действительно, если

$$\sum_{y \in \mathscr{B}} a_y y + bx = 0, \quad a_y,\ b \in K,$$

то мы должны иметь $b = 0$, потому что иначе

$$x = -\sum_{y \in \mathscr{B}} b^{-1} a_y y \in W.$$

Так как в свою очередь $\mathscr{B}$ линейно независимо, то $a_y = 0$ для всех $y \in \mathscr{B}$; это и доказывает, что $\mathscr{B} \cup \{x\}$ линейно независимо вопреки максимальности $\mathscr{B}$. Отсюда следует, что $W = V$ и, кроме того, что $\mathscr{B}$ непусто, так как $V \neq \{0\}$. Теорема доказана.

В частности, мы видим, что если V—векторное пространство $\neq \{0\}$, то всякое множество линейно независимых элементов может быть расширено до базиса, при этом базис может быть выбран из любого данного множества образующих.

Теорема 3. *Пусть V — векторное пространство над полем K. Тогда любые два базиса V над K имеют одинаковую мощность.*

Доказательство. Предположим сначала, что в V существует базис из конечного числа элементов, скажем $\{v_1, \ldots, v_m\}$, $m \geqslant 1$. Докажем, что любой другой базис должен также состоять из m элементов. Для этого достаточно доказать следующее: если $w_1, \ldots, w_n$ — элементы из V, линейно независимые над K, то $n \leqslant m$ (так как затем мы можем использовать симметрию). Доказываем по индукции. В K существуют элементы $c_1, \ldots, c_m$, для которых

$$w_1 = c_1 v_1 + \ldots + c_m v_m, \tag{1}$$

причем хотя бы один из них, скажем c_1, отличен от 0. Тогда v_1 лежит в подпространстве, порожденном над K элементами $w_1, v_2, \ldots, v_m$, и, следовательно, это подпространство совпадает с V. Кроме того, $w_1, v_2, \ldots, v_m$ линейно независимы. Действительно, предположим, что $b_1, \ldots, b_m$ — такие элементы из K, что

$$b_1 w_1 + b_2 v_2 + \ldots + b_m v_m = 0.$$

Если $b_1 \neq 0$, то разделим это равенство на b_1 и выразим w_1 в виде линейной комбинации элементов $v_2, \ldots, v_m$. Вычитание ее из (1) дало бы тогда соотношение линейной зависимости между v_i, что невозможно. Следовательно, $b_1 = 0$, а тогда и все $b_i = 0$, так как v_i линейно независимы.

Предположим по индукции, что после подходящей перенумерации v_i мы нашли $w_1, \ldots, w_r$ ($r < n$), для которых совокупность

$$\{w_1, \ldots, w_r, v_{r+1}, \ldots, v_m\}$$

будет базисом в V. Представим w_{r+1} в виде линейной комбинации

$$w_{r+1} = c_1 w_1 + \ldots + c_r w_r + c_{r+1} v_{r+1} + \ldots + c_m v_m, \tag{2}$$

где $c_i \in K$. Коэффициенты при v_i в этом соотношении не все равны нулю, так как иначе существовала бы линейная зависимость между w_i. Скажем, $c_{r+1} \neq 0$. Применяя рассуждение, аналогичное использованному выше, мы можем заменить v_{r+1} на w_{r+1} и вновь получить базис V. Это означает, что мы можем повторять эту процедуру до тех пор, пока не станет $r = n$, а потому $n \leqslant m$, что и доказывает нашу теорему.

Общий случай бесконечного базиса мы предоставляем в качестве упражнения читателю. [*Указание*: использовать тот факт, что любое конечное число элементов одного базиса содержится в пространстве, порожденном конечным числом элементов другого базиса.]

Если векторное пространство V обладает базисом из конечного числа элементов, скажем из m, то мы будем говорить, что V ко-

нечномерно и что m — его *размерность*. В силу теоремы 3 мы видим, что m есть число элементов *любого* базиса V. Если $V = \{0\}$, то мы полагаем его размерность равной 0 и говорим, что V 0-мерно. Сокращенно размерность обозначается через „dim“ или „$\dim_K$“, если для ясности необходима ссылка на поле K.

Имея дело с векторными пространствами, мы употребляем слова подпространство и факторпространство вместо подмодуль и фактормодуль.

Теорема 4. *Пусть V — векторное пространство над полем K, W — его подпространство. Тогда*

$$\dim_K V = \dim_K W + \dim_K V/W.$$

Если $f\colon V \to U$ — гомоморфизм векторных пространств над K, то

$$\dim V = \dim \operatorname{Ker} f + \dim \operatorname{Im} f.$$

Доказательство. Первое утверждение является частным случаем второго, когда в качестве f взято каноническое отображение. Пусть $\{u_i\}_{i\in I}$ — базис в $\operatorname{Im} f$ и $\{w_j\}_{j\in J}$ — базис в $\operatorname{Ker} f$. Возьмем семейство элементов $\{v_i\}_{i\in I}$ из V, такое, что $f(v_i) = u_i$ для каждого $i \in I$. Мы утверждаем, что

$$\{v_i,\ w_j\}_{i\in I,\ j\in J}$$

будет базисом для V. Этим, очевидно, завершается доказательство нашего утверждения.

Пусть x — элемент из V. Тогда существуют элементы $\{a_i\}_{i\in I}$ в K, почти все равные 0 и такие, что

$$f(x) = \sum_{i\in I} a_i u_i.$$

Следовательно, $f\left(x - \sum a_i v_i\right) = f(x) - \sum a_i f(v_i) = 0$. Значит,

$$x - \sum a_i v_i$$

лежит в ядре f, а потому существуют элементы $\{b_j\}_{j\in J}$ в K, почти все равные 0 и такие, что

$$x - \sum a_i v_i = \sum b_j w_j.$$

Отсюда находим, что $x = \sum a_i v_i + \sum b_j w_j$, т. е. $\{v_i, w_j\}$ порождает V. Остается показать, что семейство $\{v_i, w_j\}$ линейно независимо. Предположим, что существуют элементы c_i, d_j, такие, что

$$0 = \sum c_i v_i + \sum d_j w_j.$$

Применяя f, получаем

$$0 = \sum c_i f(v_i) = \sum c_i u_i,$$

откуда все $c_i = 0$. Отсюда тотчас заключаем, что все $d_j = 0$ и, следовательно, наше семейство $\{v_i, w_j\}$ является базисом для V над K, что и требовалось показать.

Следствие. *Пусть V — векторное пространство и W — его подпространство. Тогда*

$$\dim W \leqslant \dim V.$$

Если V конечномерно и $\dim W = \dim V$, то $W = V$.

Доказательство. Очевидно.

§ 6. Дуальное пространство

Пусть V — векторное пространство над полем K. Будем рассматривать K как 1-мерное пространство над собой. Под *дуальным пространством* V^* к V мы будем понимать пространство $\mathrm{Hom}_K(V, K)$ [1]). Его элементы называются *функционалами*. Таким образом, функционал на V — это K-линейное отображение $f\colon V \to K$. Если $x \in V$ и $f \in V^*$, то $f(x)$ иногда обозначают через $\langle x, f\rangle$. Фиксируя x, мы видим, что выражение $\langle x, f\rangle$, рассматриваемое как функция от $f \in V^*$, K-линейно по своему второму аргументу и, таким образом, x индуцирует линейный функционал на V^*, равный 0 в том и только в том случае, если $x = 0$. Следовательно, мы получаем вложение $V \to V^{**}$, которое не всегда сюръективно.

Пусть $\{x_i\}_{i \in I}$ — базис в V. Для каждого $i \in I$ обозначим через f_i однозначно определенный функционал, для которого $f_i(x_j) = \delta_{ij}$ (другими словами, $f_i(x_j) = 1$, если $i = j$, и $= 0$, если $i \neq j$). Такое линейное отображение существует в силу общих свойств базисов (теорема 1 из § 4).

Теорема 5. *Пусть V — векторное пространство конечной размерности n над полем K. Тогда $\dim V^* = n$. Если $\{x_1, \ldots, x_n\}$ — базис для V и f_i — функционал, для которого $f_i(x_j) = \delta_{ij}$, то $\{f_1, \ldots, f_n\}$ — базис для V^*.*

Доказательство. Пусть $f \in V^*$, и пусть $a_i = f(x_i)$ $(i = 1, \ldots, n)$. Имеем

$$(a_1 f_1 + \ldots + a_n f_n)(x_i) = a_1 f_1(x_i) + \ldots + a_n f_n(x_i) = a_i.$$

[1]) В русской литературе чаще употребляется термин „*сопряженное* пространство". — *Прим. ред.*

Следовательно, $f = a_1 f_1 + \ldots + a_n f_n$, и мы видим, что f_i порождают V^*. Кроме того, они линейно независимы, так как если

$$a_1 f_1 + \ldots + a_n f_n = 0$$

с $a_i \in K$, то, беря значение левой части на x_i, получаем

$$a_i f_i(x_i) = 0,$$

откуда $a_i = 0$ для всех i. Это доказывает нашу теорему.

Следствие. *Если пространство V конечномерно, то отображение $V \to V^{**}$, сопоставляющее каждому $x \in V$ функционал $f \mapsto \langle x, f\rangle$ на V^*, является изоморфизмом V на V^{**}.*

Доказательство. Это отображение — инъективный гомоморфизм. Поэтому его образ будет подпространством в V^{**} размерности n и, следовательно, должен совпадать со всем V^{**}.

Для данного базиса $\{x_i\}$ $(i = 1, \ldots, n)$ базис $\{f_i\}$, определенный в формулировке теоремы, называется *дуальным базисом*. Пользуясь этими базисами, мы можем представить любой элемент A из V посредством координат $(a_1, \ldots, a_n)$ и любой элемент B из V^* посредством координат $(b_1, \ldots, b_n)$, так что

$$A = a_1 x_1 + \ldots + a_n x_n, \qquad B = b_1 f_1 + \ldots + b_n f_n.$$

Отсюда мы видим, что

$$\langle A, B\rangle = a_1 b_1 + \ldots + a_n b_n = A \cdot B$$

есть обычное скалярное произведение наборов из n чисел.

Пусть V — векторное пространство над полем K, и пусть

$$0 \to W \xrightarrow{\lambda} V \xrightarrow{\varphi} U \to 0$$

— точная последовательность K-линейных отображений. Мы утверждаем, что индуцированная последовательность

$$0 \leftarrow \mathrm{Hom}_K(W, K) \leftarrow \mathrm{Hom}_K(V, K) \leftarrow \mathrm{Hom}_K(U, K) \leftarrow 0,$$

т. е. последовательность

$$0 \leftarrow W^* \leftarrow V^* \leftarrow U^* \leftarrow 0$$

также точна.

Точность во всех членах, кроме крайнего левого, есть общий факт, не связанный со спецификой векторных пространств и справедливый для произвольных модулей (см. § 2). Существенным моментом здесь является доказательство сюръективности отображения V^* в W^*. Чтобы установить ее, рассмотрим произвольный функционал g на W. Существует подпространство T в V, такое, что

$$V = \lambda(W) + T$$

есть прямая сумма. Фактически мы можем рассматривать W как подпространство в V, поскольку λ — вложение. Любой элемент из V имеет единственное представление в виде суммы $w+t$, где $w\in W$ и $t\in T$. Определим функционал f на V, положив $f(w+t)=g(w)$ *для всех* $w\in W$ *и* $t\in T$. Тогда ограничение f на $W(=\lambda(W))$ совпадает с g. Это и означает, что левое отображение в индуцированной последовательности сюръективно.

Пусть V и V' — два векторных пространства. Предположим, что нам задано отображение

$$V\times V'\to K,$$

записываемое так:

$$(x,\ x')\longmapsto\langle x,\ x'\rangle,$$

$x\in V$, $x'\in V'$. Мы называем это отображение *билинейным*, если *для каждого* $x\in V$ *функция* $x'\longmapsto\langle x,\ x'\rangle$ *линейна и аналогично для* каждого $x'\in V'$ функция $x\longmapsto\langle x,\ x'\rangle$ линейна. Элемент $x\in V$ называется *ортогональным* (или *перпендикулярным*) подмножеству S' в V', если $\langle x,\ x'\rangle=0$ для всех $x'\in S'$. Аналогично определяется ортогональность элемента из V' подмножеству из V. Очевидно, что множество всех $x\in V$, ортогональных к S', есть подпространство в V.

Определяем *ядро слева* билинейного отображения как подпространство в V, ортогональное к V'; аналогично определяется *ядро справа*.

Пусть W' — ядро справа и W — ядро слева данного билинейного отображения

$$V\times V'\to K,$$

и пусть x' — некоторый элемент из V'. Тогда x' определяет функционал на V по правилу $x\longmapsto\langle x,\ x'\rangle$ и этот функционал, очевидно, зависит только от смежного класса x' по модулю W'; другими словами, если $x'_1\equiv x'_2(\mathrm{mod}\ W')$, то функционалы $x\longmapsto\langle x,\ x'_1\rangle$ и $x\longmapsto\langle x,\ x'_2\rangle$ равны. Следовательно, имеет место гомоморфизм

$$V'\to V^*,$$

ядро которого по определению есть точно W', откуда получаем инъективный гомоморфизм

$$0\to V'/W'\to V^*.$$

Так как все функционалы, соответствующие элементам V', обращаются в нуль на W, то мы можем рассматривать их как функционалы на V/W, т. е. как элементы из $(V/W)^*$. Таким образом, в действительности мы получаем инъективный гомоморфизм

$$0\to V'/W'\to(V/W)^*.$$

Можно было бы дать специальное название гомоморфизму

$$g\colon V' \to V^*,$$

для которого

$$\langle x, x' \rangle = \langle x, g(x') \rangle$$

при всех $x \in V$ и $x' \in V'$. Однако удобнее изображать этот гомоморфизм с помощью стрелок и называть индуцированным отображением, или естественным отображением. Давать ему особое имя — значило бы стремиться к излишнему утяжелению терминологии.

Теорема 6. *Пусть $V \times V' \to K$ — билинейное отображение, W, W' — его ядра слева и справа соответственно, и пусть V'/W' конечномерно. Тогда индуцированный гомоморфизм $V'/W' \to (V/W)^*$ является изоморфизмом.*

Доказательство. В силу симметрии имеет место индуцированный гомоморфизм

$$V/W \to (V'/W')^*,$$

являющийся инъективным. Так как

$$\dim (V'/W')^* = \dim V'/W',$$

то отсюда следует, что V/W конечномерно. Из инъективности предыдущего гомоморфизма и ему аналогичного, а именно

$$0 \to V'/W' \to (V/W)^*,$$

вытекают неравенства

$$\dim V/W \leqslant \dim V'/W'$$

и

$$\dim V'/W' \leqslant \dim V/W,$$

откуда следует, что эти размерности равны. Таким образом, наши гомоморфизмы сюръективны и обратны друг другу, что и доказывает теорему.

УПРАЖНЕНИЯ

1. Показать, что всякий модуль над кольцом A является гомоморфным образом некоторого свободного модуля.

2. Обобщить утверждение теоремы 3 о размерности векторных пространств на свободные модули над произвольным коммутативным кольцом. [*Указание*: вспомнить, как аналогичное утверждение доказывалось для свободных абелевых групп, и воспользоваться максимальными идеалами вместо простых чисел.]

3. Провести подробное доказательство того, что условия расщепимости последовательности, данные в предложении 3, эквивалентны. Показать, что последовательность $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ расщепляется в том и только

в том случае, если существует подмодуль N в M, такой, что модуль M равен прямой сумме $\operatorname{Im} f \oplus N$ и что в этом случае N изоморфен M''. Восстановить все детали в доказательстве предложения 3.

4. Пусть A — коммутативное кольцо, M — A-модуль и S — мультипликативное подмножество в A. Определить $S^{-1}M$ способом, аналогичным тому, который мы использовали при определении $S^{-1}A$, и показать, что $S^{-1}M$ будет $S^{-1}A$-модулем.

5. Пусть A и S обозначают то же, что в упражнении 4. Показать, что если $0 \to M' \to M \to M'' \to 0$—точная последовательность, то и последовательность $0 \to S^{-1}M' \to S^{-1}M \to S^{-1}M'' \to 0$ точна.

6. Пусть V — векторное пространство над полем K и U, W — его подпространства. Показать, что

$$\dim U + \dim W = \dim (U + W) + \dim (U \cap W).$$

7. Пусть E и E_i ($i = 1, \ldots, m$) — модули над некоторым кольцом. Пусть $\varphi_i\colon E_i \to E$ и $\psi_i\colon E \to E_i$—гомоморфизмы, обладающие следующими свойствами:

$$\psi_i \circ \varphi_i = \mathrm{id}, \quad \psi_i \circ \varphi_j = 0, \quad \text{если} \quad i \neq j,$$

$$\sum_{i=1}^{m} \varphi_i \circ \psi_i = \mathrm{id}.$$

Показать, что отображение $x \longmapsto (\psi_1 x, \ldots, \psi_m x)$ является изоморфизмом E на прямое произведение модулей E_i ($i = 1, \ldots, m$), а отображение

$$(x_1, \ldots, x_m) \longmapsto \varphi_1 x_1 + \ldots + \varphi_m x_m$$

— изоморфизмом этого прямого произведения на E.

Обратно, если модуль E равен прямому произведению (или сумме) подмодулей E_i ($i = 1, \ldots, m$) и если обозначить через φ_i вложение E_i в E и через ψ_i — проекцию E на E_i, то эти отображения обладают указанными выше свойствами.

8. *Проективные модули.* Пусть A — кольцо. Модуль P над A называется *проективным*, если для любых заданных гомоморфизма $f\colon P \to M''$ и сюръективного гомоморфизма $g\colon M \to M''$ существует гомоморфизм $h\colon P \to M$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccccc} & & P & & \\ & \swarrow^{h} & \downarrow{\scriptstyle f} & & \\ M & \xrightarrow{g} & M'' & \to & 0. \end{array}$$

Доказать:

(а) Прямая сумма модулей проективна в том и только в том случае, если каждое слагаемое проективно.

(б) Модуль P проективен в том и только в том случае, если существует модуль M, такой, что $P \oplus M$ свободен.

(в) Всякий модуль M может быть включен в точную последовательность $0 \to N \to F \to M \to 0$ с проективным модулем F (ср. упражнение 1).

(г) Модуль P проективен в том и только в том случае, если всякая точная последовательность

$$0 \to M' \to M \to P \to 0$$

расщепляется.

9. *Инъективные модули.* Пусть A — кольцо. Модуль Q называется *инъективным*, если для любых данных модуля N, его подмодуля N' и гомоморфизма $N' \to Q$ существует продолжение этого гомоморфизма на N, т. е. существует гомоморфизм $N \to Q$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccccc} 0 & \to & N' & \to & N \\ & & & \searrow & \downarrow \\ & & & & Q \end{array}$$

Доказать:

(а) Прямое произведение модулей инъективно в том и только в том случае, если каждый сомножитель инъективен.

(б) Абелева группа $\mathbf{Q}/\mathbf{Z}$, рассматриваемая как модуль над кольцом целых чисел $\mathbf{Z}$, инъективна. (Использовать лемму Цорна.) То же утверждение справедливо для $\mathbf{R}/\mathbf{Z}$, где $\mathbf{R}$ — группа вещественных чисел.

(в) Пусть Q — модуль над A. Предположим, что для всякого левого идеала J кольца A любой гомоморфизм $\varphi\colon J \to Q$ может быть продолжен до гомоморфизма A в Q. Тогда Q инъективен. [*Указание*: при заданных $N' \subset N$ и $f\colon N' \to Q$ возьмем $x_0 \in N$, $x_0 \notin N'$. Пусть J — левый идеал, состоящий из элементов $a \in A$, для которых $ax_0 \in N'$. Пусть гомоморфизм $\varphi(a) = f(ax_0)$ продолжен на A; продолжить f по формуле $f(x' + bx_0) = f(x') + \varphi(b)$ для $x' \in N'$ и $b \in A$. Затем использовать лемму Цорна.]

(г) Пусть $A_0 = \mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{R}/\mathbf{Z})$; превратим A_0 в A-модуль, полагая $(af)(x) = f(xa)$ для $a \in A$ и $f \in A_0$. Используя (в), показать, что A_0 инъективен.

(д) Всякий модуль является подмодулем некоторого инъективного модуля. [*Указание*: пусть M — A-модуль и $x \in M$, $x \neq 0$. Показать, что существует гомоморфизм $f_x\colon M \to A_0$, для которого $f_x(x) \neq 0$. Пусть J — идеал в A, аннулирующий x, и $\varphi\colon A \to \mathbf{R}/\mathbf{Z}$ — гомоморфизм, обращающийся в нуль на J и такой, что $\varphi(1) \neq 0$. Построить f_x, для которого $f_x(x) = \varphi$. Затем взять произведение всех f_x.]

(е) Модуль Q инъективен тогда и только тогда, когда всякая точная последовательность

$$0 \to Q \to N \to M \to 0$$

расщепляется.

10. Пусть A — аддитивная подгруппа евклидова пространства $\mathbf{R}^n$; предположим, что во всякой ограниченной области пространства содержится лишь конечное число элементов из A. Показать, что A — свободная абелева группа с числом образующих $\leqslant n$. [*Указание*: провести индукцию по максимальному числу линейно независимых над $\mathbf{R}$ элементов из A. Пусть $v_1, \ldots, v_m$ — максимальное множество таких элементов, и пусть A_0 — подгруппа в A, содержащаяся в $\mathbf{R}$-пространстве, порожденном $v_1, \ldots, v_{m-1}$. По предположению индукции любой элемент в A_0 есть линейная целочисленная комбинация элементов $v_1, \ldots, v_{m-1}$. Пусть S — подмножество элементов $v \in A$ вида $v = a_1v_1 + \ldots + a_mv_m$ с вещественными коэффициентами a_i, удовлетворяющими неравенствам

$$0 \leqslant a_i < 1 \quad \text{при} \quad i = 1, \ldots, m-1;$$
$$0 \leqslant a_m \leqslant 1.$$

Пусть v'_m — элемент из S с наименьшим $a_m \neq 0$; показать, что $\{v_1, \ldots, v_{m-1}, v'_m\}$ будет базисом в A над $\mathbf{Z}$.]

Глава IV

Гомологии

§ 1. Комплексы

Пусть A — кольцо. Под *открытым комплексом* A-модулей понимают последовательность модулей и гомоморфизмов $\{(E_i, d_i)\}$,

$$\to E_{i-1} \xrightarrow{d_{i-1}} E_i \xrightarrow{d_i} E_{i+1} \to,$$

где i пробегает все целые числа и d_i отображает E_i в E_{i+1}, причем

$$d_i \circ d_{i-1} = 0$$

для всех i.

Часто рассматривают конечные последовательности гомоморфизмов, скажем

$$E_1 \to \ \dots \ \to E_r,$$

в которых композиция двух последовательных гомоморфизмов равна 0; такую последовательность можно превратить в комплекс, добавив нули на каждом конце

$$\to 0 \to 0 \to E_1 \to \ \dots \ \to E_r \to 0 \to 0 \to .$$

Замкнутый комплекс A-модулей — это последовательность модулей и гомоморфизмов $\{(E_i, d_i)\}$, где i пробегает множество целых чисел по модулю n для некоторого $n \geqslant 2$, удовлетворяющая тому же свойству, что и выше, для композиций последовательных гомоморфизмов. Таким образом, замкнутый комплекс выглядит так:

$$E_1 \to E_2 \to \ \dots \ \to E_n.$$

Мы называем n *длиной* замкнутого комплекса.

Можно, не опасаясь путаницы, опускать индекс i в d_i и писать просто d. Мы будем также обозначать комплекс $\{(E_i, d_i)\}$ через (E, d) и даже, еще короче, просто через E.

Пусть (E, d) и (E', d') — два комплекса (оба открытые или оба замкнутые), r — целое число. *Морфизм* (комплексов)

$$f\colon (E', d') \to (E, d)$$

степени r — это последовательность гомоморфизмов

$$f_i\colon E'_i \to E_{i+r},$$

таких, что для всякого i коммутативна следующая диаграмма:

$$\begin{array}{ccc} E'_{i-1} & \xrightarrow{f_{i-1}} & E_{i-1+r} \\ {\scriptstyle d'}\downarrow & & \downarrow{\scriptstyle d} \\ E'_i & \xrightarrow[f_i]{} & E_{i+r} \end{array}$$

Точно так же как мы пишем d вместо d_i, мы будем писать f вместо f_i. Если комплексы замкнуты, то мы определяем морфизм одного в другой только в том случае, если они имеют одинаковую длину.

Ясно, что комплексы образуют категорию.

Будет полезно ввести еще одно понятие, относящееся к объектам, *занумерованным посредством моноида*. Пусть G — моноид, который мы предположим коммутативным и аддитивным, имея в виду дальнейшие приложения. Пусть $\{M_i\}_{i\in G}$ — семейство модулей, занумерованных посредством G. Прямая сумма

$$M = \coprod_{i\in G} M_i$$

будет называться *G-градуированным модулем, ассоциированным с семейством* $\{M_i\}_{i\in G}$. Пусть $\{M_i\}_{i\in G}$ и $\{M'_i\}_{i\in G}$ — два семейства, занумерованные посредством G, и M, M' — ассоциированные с ними G-градуированные модули. Пусть $r\in G$. Под *G-градуированным морфизмом* $f\colon M' \to M$ степени r мы будем понимать гомоморфизм f, отображающий M'_i в M_{i+r} для всякого $i\in G$ (при этом M_i отождествляется с соответствующим подмодулем прямой суммы). Таким образом, f есть не что иное, как семейство гомоморфизмов $f_i\colon M'_i \to M_{i+r}$.

Если (E, d) — комплекс, то мы можем рассматривать E как G-градуированный модуль (взяв прямую сумму членов этого комплекса), а d — как G-градуированный морфизм степени 1, полагая G равным $\mathbf{Z}$ или $\mathbf{Z}/n\mathbf{Z}$.

Обратно, если G есть $\mathbf{Z}$ или $\mathbf{Z}/n\mathbf{Z}$, то мы можем рассматривать G-градуированный модуль как комплекс, считая по определению d нулевым отображением.

Для простоты мы будем часто опускать эпитет „G-градуированный“ перед словом „морфизм“, когда речь будет идти о G-градуированных морфизмах.

§ 2. Гомологическая последовательность

Пусть (E, d) — комплекс. Положим

$$Z_i(E) = \operatorname{Ker} d_i$$

и назовем $Z_i(E)$ модулем *i-циклов*. Положим, далее,

$$B_i(E) = \operatorname{Im} d_{i-1}$$

и назовем $B_i(E)$ модулем *i-границ*. Мы часто будем писать Z_i и B_i вместо $Z_i(E)$ и $B_i(E)$ соответственно. Будем называть группу

$$H_i(E) = Z_i/B_i = \operatorname{Ker} d_i/\operatorname{Im} d_{i-1}$$

i-й *группой гомологий* комплекса E. Градуированный модуль, ассоциированный с семейством $\{H_i\}$, будет обозначаться через $H(E)$ и называться *гомологией* комплекса E. Иногда пишут $H_*(E)$ вместо $H(E)$.

Если $f\colon E' \to E$—морфизм комплексов, скажем, степени 0, то имеем индуцированный канонический гомоморфизм степени 0

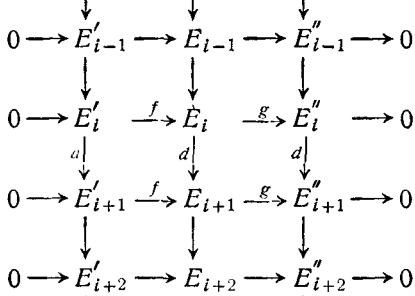
$$f_*\colon H(E') \to H(E)$$

их гомологий. Это непосредственно видно из коммутативных диаграмм, участвующих в определении морфизма комплексов. Действительно, читатель тотчас проверит, что $f_i(Z'_i) \subset Z_i$ и $f_i(B'_i) \subset B_i$, откуда получается индуцированный гомоморфизм $Z'_i/B'_i \to Z_i/B_i$. (Читателю следует один и только один раз в своей жизни проследить все детали до конца.) Таким образом, H есть функтор из категории комплексов в категорию градуированных модулей. Можно было бы писать $H(f)$ вместо f_*, а также $H_i(f)$ или f_{i*} для индуцированного отображения на H'_i.

Рассмотрим короткую точную последовательность комплексов с морфизмами степени 0:

$$0 \to E' \xrightarrow{f} E \xrightarrow{g} E'' \to 0,$$

которая, если ее выписать целиком, выглядит так (пишем d вместо d' и d''):



Можно следующим образом определить морфизм степени 1

$$\delta\colon H(E'') \to H(E'),$$

или, что равносильно, семейство гомоморфизмов

$$\delta_i\colon H_i'' \to H_{i+1}'.$$

Пусть z'' лежит в Z_i''. Так как g сюръективно, то существует элемент $z \in E_i$, для которого $gz = z''$. Сдвинемся теперь вертикально вниз по стрелке d и возьмем dz. Используя коммутативность $gd = dg$, находим, что $gdz = 0$, т. е. dz лежит в $\operatorname{Ker} g \subset E_{i+1}'$. В силу точности существует элемент $z' \in E_{i+1}'$, для которого $fz' = dz$. Кратко мы можем написать

$$z' = f^{-1} dg^{-1} z''.$$

Мы предоставляем читателю в качестве шаблонного упражнения проверить, что z' принадлежит Z_{i+1}', или, другими словами, является циклом, и что его класс по модулю B_{i+1}' не зависит от выбора элемента z, для которого $gz = z''$. Далее, отображение

$$z \longmapsto f^{-1} dg^{-1} z \quad \text{по модулю} \quad B_{i+1}'$$

индуцирует гомоморфизм

$$\delta_i\colon Z_i''/B_i'' \to Z_{i+1}'/B_{i+1}',$$

который и является i-й компонентой искомого морфизма δ.

Теорема 1. *Пусть*

$$0 \to E' \xrightarrow{f} E \xrightarrow{g} E'' \to 0$$

— точная последовательность комплексов с морфизмами f, g степени 0. *Тогда последовательность*

$$H(E') \xrightarrow{f_*} H(E) \xrightarrow{g_*} H(E'') \xrightarrow{\delta} H(E')$$

точна.

Доказательство. Доказательство по существу шаблонно и состоит в петлянии по диаграммам. Однако читателю, желающему приобрести навык в подобного сорта тривиальностях, следует проследить его во всех деталях. В качестве примера докажем, что

$$\operatorname{Ker} \delta \subset \operatorname{Im} g_*.$$

Воспользуемся теми же обозначениями, которые были введены перед формулировкой теоремы при описании морфизма δ. Если z''

представляет класс, образ которого относительно δ равен 0, то это означает, что z' — граница, другими словами, что существует элемент $u' \in E_i'$, для которого $z' = du'$. Тогда, используя обозначения, введенные при определении δ, имеем

$$dz = fz' = f\,du' = d\,fu'$$

в силу коммутативности. Следовательно,

$$d(z - fu') = 0$$

и $z - fu'$ есть цикл в E_i. Но $g(z - fu') = gz = z''$. Это означает, что класс элемента z'' лежит в образе g_*, что и требовалось доказать.

Если фигурирующую в этой теореме гомологическую последовательность выписать полностью, то она выглядит следующим образом:

$$\boxed{\xrightarrow{\delta} H_i' \to H_i \to H_i'' \xrightarrow{\delta} H_{i+1}' \to H_{i+1} \to H_{i+1}'' \xrightarrow{\delta}}.$$

Ясно, что наше отображение δ функториально (в очевидном смысле) и, следовательно, все наше образование (H, δ) является функтором из категории коротких точных последовательностей комплексов в категорию комплексов.

§ 3. Эйлерова характеристика

Мы продолжаем рассматривать A-модули. Пусть Γ — абелева группа, записываемая аддитивно. Пусть φ — правило, сопоставляющее некоторым модулям элементы из Γ и удовлетворяющее следующему условию:

Если $0 \to M' \to M \to M'' \to 0$ — *точная последовательность, то* $\varphi(M)$ *определено тогда и только тогда, когда определены* $\varphi(M')$ *и* $\varphi(M'')$, *и в этом случае*

$$\varphi(M) = \varphi(M') + \varphi(M'').$$

Кроме того, $\varphi(0)$ *определено и равно* 0.

Такое правило φ будет называться *отображением Эйлера — Пуанкаре* на категории A-модулей. В том случае, когда модуль M' изоморфен модулю M, из точности последовательности

$$0 \to M' \to M \to 0 \to 0$$

заключаем, что если $\varphi(M)$ определено, то и $\varphi(M')$ определено и $\varphi(M') = \varphi(M)$. Следовательно, если $\varphi(M)$ определено для модуля M,

то φ определено для всякого подмодуля и фактормодуля M. В частности, если имеется точная последовательность модулей

$$M' \to M \to M''$$

и если $\varphi(M')$ и $\varphi(M'')$ определены, то определено и $\varphi(M)$, что сразу видно, если рассмотреть ядро и образ наших двух отображений и применить определение.

Примеры. В случае $A = \mathbf{Z}$ можно считать φ определенным для всех конечных абелевых групп и равным порядку группы. Значения φ лежат в мультипликативной группе положительных рациональных чисел.

В качестве другого примера рассмотрим категорию векторных пространств над полем k. Можно считать φ определенным для конечномерных пространств и равным размерности. Значения φ лежат тогда в аддитивной группе целых чисел.

Вернемся к общему случаю. Пусть E — открытый комплекс, такой, что почти все H_i равны 0. Пусть φ — отображение Эйлера — Пуанкаре на категории модулей (т. е. A-модулей). Определим *характеристику Эйлера — Пуанкаре* $\chi_\varphi(E)$ (или, короче, эйлерову характеристику) относительно φ формулой

$$\chi_\varphi(E) = \sum (-1)^i \varphi(H_i)$$

при условии, что значения $\varphi(H_i)$ определены для всех H_i; в этом случае мы говорим, что χ_φ *определена* для комплекса E. Той же формулой определим характеристику Эйлера — Пуанкаре и в случае замкнутого комплекса E, длина n которого четна [1]).

За примером читатель может обратиться к упражнению 14 из гл. I.

Можно рассматривать H как комплекс, положив d равным нулевому отображению. При этом мы видим, что $\chi_\varphi(H)$ есть та же знакопеременная сумма, что и выше. Более общо:

Теорема 2. *Пусть F — комплекс, имеющий четную длину, в случае если он замкнут. Предположим, что $\varphi(F_i)$ определено для всех i и что выполнено одно из следующих двух условий*: (i) $F_i = 0$ *для почти всех* i; (ii) $\varphi(F_i) = 0$ *для почти всех* i, *и отображение* φ *таково, что* $\varphi(M) = 0$ *влечет* $\varphi(M') = 0$ *для всякого* $M' \subset M$. *Тогда характеристика* $\chi_\varphi(F)$ *определена и*

$$\chi_\varphi(F) = \sum_i (-1)^i \varphi(F_i).$$

Доказательство. Заметим сначала, что $\varphi(H_i)$ определено для всех i, а из условий (i) или (ii) вытекает, что $\varphi(H_i) = 0$ для

[1]) Здесь и ниже в формулировки автора внесены некоторые уточнения. — *Прим. ред.*

почти всех i. Следовательно, характеристика $\chi_\varphi(F)$ определена. Пусть Z_i и B_i — группы i-циклов и i-границ в F_i соответственно. Имеем точную последовательность

$$0 \to Z_i \to F_i \to B_{i+1} \to 0,$$

из которой получаем

$$\varphi(F_i) = \varphi(Z_i) + \varphi(B_{i+1}),$$

причем для почти всех i каждый из членов этого равенства обращается в нуль. Взяв знакопеременную сумму, немедленно получаем наше утверждение.

Комплекс, гомологии которого тривиальны, называется *ациклическим*.

Следствие. *Пусть F — ациклический комплекс, удовлетворяющий условиям теоремы 2. Тогда*

$$\sum_i (-1)^i \varphi(F_i) = 0.$$

Если открытый комплекс F таков, что $F_i = 0$ для почти всех i, то его можно рассматривать как замкнутый комплекс, определив дополнительное отображение, идущее от дальнего правого нуля к дальнему левому нулю. Таким образом, в этом случае изучение открытого комплекса сводится к изучению замкнутого комплекса.

Теорема 3. *Пусть*

$$0 \to E' \to E \to E'' \to 0$$

— точная последовательность комплексов с морфизмами степени 0. *В случае замкнутых комплексов предполагаем, что их длина четна. Пусть φ — отображение Эйлера — Пуанкаре на категории модулей. Если характеристика χ_φ определена для двух из трех комплексов, то она определена и для третьего и*

$$\chi_\varphi(E) = \chi_\varphi(E') + \chi_\varphi(E'').$$

Доказательство. Имеем точную гомологическую последовательность

$$\to H''_{i-1} \to H'_i \to H_i \to H''_i \to H'_{i+1} \to .$$

Эта гомологическая последовательность есть не что иное, как комплекс, гомологии которого тривиальны. Кроме того, каждая группа гомологий, принадлежащая, скажем E, стоит между группами гомологий E' и E''. Следовательно, если χ_φ определена для E' и E'', то она определена и для E. Аналогично рассуждаем и в двух других случаях. Если наши комплексы — замкнутые четной длины n, то го-

мологическая последовательность имеет четную длину $3n$. Поэтому мы можем применить следствие из теоремы 2 для получения искомого результата.

Для ряда приложений удобно построить универсальное отображение Эйлера. Пусть $\mathcal{A}$ — некоторое множество классов модулей относительно изоморфизма. Если E — модуль, то пусть $[E]$ — его класс относительно изоморфизма. Мы требуем, чтобы $\mathcal{A}$ удовлетворяло условию Эйлера — Пуанкаре, т. е. чтобы для всякой точной последовательности

$$0 \to E' \to E \to E'' \to 0$$

класс $[E]$ тогда и только тогда лежал в $\mathcal{A}$, когда $[E']$ и $[E'']$ лежат в $\mathcal{A}$. Кроме того, нулевой модуль лежит в $\mathcal{A}$. *Мы утверждаем, что существует отображение*

$$\gamma\colon \mathcal{A} \to K(\mathcal{A})$$

множества $\mathcal{A}$ в некоторую абелеву группу $K(\mathcal{A})$, обладающую свойством универсальности по отношению к отображениям Эйлера — Пуанкаре, определенным на $\mathcal{A}$.

Чтобы построить это отображение, рассмотрим свободную абелеву группу $F_{\mathrm{ab}}(\mathcal{A})$, порожденную множеством наших классов $[E]$. Пусть B — ее подгруппа, порожденная всеми элементами вида

$$[E] - [E'] - [E''],$$

где

$$0 \to E' \to E \to E'' \to 0$$

— точная последовательность, члены которой лежат в $\mathcal{A}$. Пусть $K(\mathcal{A})$ — факторгруппа $F_{\mathrm{ab}}(\mathcal{A})/B$, и пусть $\gamma\colon \mathcal{A} \to K(\mathcal{A})$ — естественное отображение. Ясно, что γ обладает свойством универсальности.

Отметим сходство этой конструкции с группой Гротендика моноида. И действительно, группа $K(\mathcal{A})$ известна под названием *группы Эйлера — Гротендика* множества $\mathcal{A}$.

Важное обобщение. Из предыдущего ясно, что бóльшая часть того, что мы сделали, относится к чистой теории стрелок. Действительно, для определения гомологий нам нужны только понятия ядра и коядра (фактормодуля). Тот факт, что модули состоят из элементов, мы использовали лишь для определения δ.

Можно аксиоматизировать понятие категории, в которой все предыдущие рассуждения имеют смысл. Рассмотрим сначала категорию $\mathcal{A}$, такую, что $\mathrm{Mor}(E, F)$ есть абелева группа для каждой пары объектов E, F из $\mathcal{A}$, причем выполняются следующие два условия:

АБ 1. Закон композиции морфизмов билинеен, и существует нулевой объект 0, т. е. такой объект, что $\mathrm{Mor}(0, E)$ и $\mathrm{Mor}(E, 0)$ состоят ровно из одного элемента для любого E.

АБ 2. В этой категории существуют конечные произведения и конечные копроизведения.

Мы говорим тогда, что $\mathcal{A}$ — *аддитивная категория*

Для данного морфизма $E \xrightarrow{f} F$ в категории $\mathcal{A}$ его *ядром* по определению будет такой морфизм $E' \to E$, что для всех объектов X в этой категории точна следующая последовательность:

$$0 \to \mathrm{Mor}(X, E') \to \mathrm{Mor}(X, E) \to \mathrm{Mor}(X, F).$$

Мы определяем *коядро* f как морфизм $F \to F''$, такой, что для всех объектов X в категории точна следующая последовательность:

$$\mathrm{Mor}(E, X) \leftarrow \mathrm{Mor}(F, X) \leftarrow \mathrm{Mor}(F'', X) \leftarrow 0.$$

Непосредственно проверяется, что ядра и коядра универсальны в подходящих категориях и, следовательно, если существуют, то единственны с точностью до однозначно определенного изоморфизма

АБ 3. Ядра и коядра существуют.

АБ 4. Если f: $E \to F$ — морфизм, ядро которого есть 0, то f — ядро своего коядра. Если f: $E \to F$ — морфизм, коядро которого 0, то f — коядро своего ядра. Морфизм, ядро и коядро которого равны 0, есть изоморфизм.

Категория $\mathcal{A}$, удовлетворяющая предыдущим четырем аксиомам, называется *абелевой категорией*.

Например, комплексы модулей образуют абелеву категорию, поскольку ясно, как определить, скажем, ядро морфизма комплексов. В топологии абелеву категорию образуют так называемые векторные пучки.

§ 4. Теорема Жордана — Гёльдера

Мы начнем с некоторых чисто теоретико-групповых результатов. Как и элементарные теоремы об изоморфизмах, они имеют аналоги для модулей, которые будут сформулированы позже.

Лемма о бабочке (Цассенхауз). *Пусть U, V — подгруппы некоторой группы, и пусть u, v — нормальные подгруппы в U и в V соответственно. Тогда*

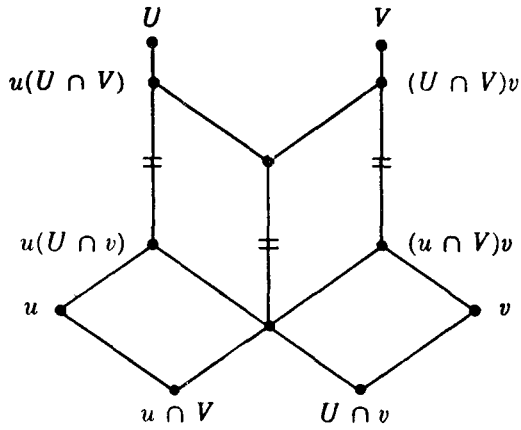
$$u(U \cap v) \text{ нормальна в } u(U \cap V),$$

$$(u \cap V)v \text{ нормальна в } (U \cap V)v$$

и соответствующие факторгруппы изоморфны, т. е.

$$u(U \cap V)/u(U \cap v) \approx (U \cap V)v/(u \cap V)v.$$

Доказательство. Комбинация групп и факторгрупп становится ясной, если посмотреть на следующую диаграмму подгрупп (которая и дала название лемме):



На этой диаграмме нам заданы U, u, V, v. Остальные вершины в диаграмме соответствуют группам, которые определяются следующим образом. Пересечение двух отрезков, идущих вниз, представляет пересечение групп. Два отрезка, идущие вверх, пересекаются в вершине, которая представляет произведение двух подгрупп (т. е. наименьшую подгруппу, содержащую их обеих).

Рассмотрим два параллелограмма, составляющие крылья бабочки, и докажем, что противоположные стороны этих параллелограммов равны.

Действительно, вертикальная сторона, общая обоим параллелограммам, имеет $U \cap V$ в качестве верхнего конца и $(u \cap V)(U \cap v)$ в качестве нижнего конца. Имеем изоморфизм

$$(U \cap V)/(u \cap V)(U \cap v) \approx u(U \cap V)/u(U \cap v).$$

Он получается из теоремы об изоморфизме

$$H/(H \cap N) = HN/N,$$

если положить $H = U \cap V$ и $N = u(U \cap v)$. Таким образом, средняя вертикальная сторона равна вертикальной стороне слева. В силу симметрии она равна также вертикальной стороне справа, и так как две величины, равные порознь третьей, равны между собой, то наша лемма доказана.

Пусть G — группа, и пусть

$$G = G_1 \supset G_2 \supset \ldots \supset G_r = \{e\},$$
$$G = H_1 \supset H_2 \supset \ldots \supset H_s = \{e\}$$

— нормальные башни подгрупп, заканчивающиеся тривиальной группой. Мы будем говорить, что эти башни *эквивалентны*, если $r = s$ и если существует такая перестановка $i \mapsto i'$ индексов $i = 1, \ldots, r-1$, что

$$G_i/G_{i+1} \approx H_{i'}/H_{i'+1}.$$

Другими словами, последовательности факторгрупп в двух наших башнях одинаковы с точностью до изоморфизма и перестановки индексов.

Теорема 4 (Шрейер). *Для всякой группы G две нормальные башни подгрупп, заканчивающиеся тривиальной группой, обладают эквивалентными уплотнениями.*

Доказательство. Рассмотрим две указанные башни. Для каждого $i = 1, \ldots, r-1$ и $j = 1, \ldots, s$ положим

$$G_{ij} = G_{i+1}(H_j \cap G_i).$$

Тогда $G_{is} = G_{i+1}$, и мы получаем уплотнение первой башни

$$G = G_{11} \supset G_{12} \supset \ldots \supset G_{1,\,s-1} \supset G_2 =$$
$$= G_{21} \supset G_{22} \supset \ldots \supset G_{r-1,\,1} \supset \ldots \supset G_{r-1,\,s-1} \supset \{e\}.$$

Аналогично полагаем

$$H_{ji} = H_{j+1}(G_i \cap H_j)$$

для $j = 1, \ldots, s-1$ и $i = 1, \ldots, r$. Это дает уплотнение второй башни. В силу леммы о бабочке для $i = 1, \ldots, r-1$ и $j = 1, \ldots, s-1$ имеем изоморфизмы

$$G_{ij}/G_{i,\,j+1} \approx H_{ji}/H_{j,\,i+1}.$$

Каждая из наших уплотненных башен имеет $(r-1)(s-1)+1$ элементов, а именно G_{ij} ($i = 1, \ldots, r-1$; $j = 1, \ldots, s-1$) и $\{e\}$ в первом случае, H_{ij} и $\{e\}$ во втором случае. Предыдущие изоморфизмы для каждой пары индексов (i, j) показывают, что наши уплотненные башни эквивалентны, что и требовалось доказать.

Группа G называется *простой*, если она не тривиальна и не имеет других нормальных подгрупп, кроме $\{e\}$ и самой себя.

Теорема 5 (Жордан — Гёльдер). *Пусть G — группа и*

$$G = G_1 \supset G_2 \supset \ldots \supset G_r = \{e\}$$

— такая нормальная башня, что каждая группа G_i/G_{i+1} проста для $i = 1, \ldots, r-1$. Тогда любая другая нормальная башня группы G, обладающая теми же свойствами, ей эквивалентна.

Доказательство. Заметим, что при любом уплотнении $\{G_{ij}\}$ нашей башни для каждого i существует в точности один индекс j, для которого $G_i/G_{i+1} = G_{ij}/G_{i,\,j+1}$. Таким образом, последовательность нетривиальных факторов в исходной башне и в уплотненной одинакова. Теорема доказана.

Точно так же как и в случае элементарных теорем об изоморфизме для групп, имеются аналоги теорем 4 и 5 для модулей. Разумеется, в случае модулей нам нет нужды беспокоиться о нормальности подмодулей.

Если M — модуль (над кольцом A), то последовательность подмодулей

$$M = M_1 \supset M_2 \supset \ \dots \ \supset M_r = 0$$

называется также *конечной фильтрацией*, причем r называется *длиной* фильтрации. Говорят, что модуль M *простой*, если он не содержит никаких подмодулей, отличных от $\{0\}$ и самого себя, и если $M \neq 0$. Фильтрация называется *простой*, если каждый фактормодуль M_i/M_{i+1} простой. *Теорема Жордана — Гёльдера утверждает, что всякие две простые фильтрации модуля эквивалентны.*

Модуль M называется модулем *конечной длины*, если он равен 0 или же обладает простой (конечной) фильтрацией. По теореме Жордана — Гёльдера длина такой простой фильтрации однозначно определена; она называется *длиной модуля*. На языке эйлеровых характеристик теорема Жордана — Гёльдера может быть переформулирована так:

Теорема 6. *Пусть* φ *— правило, которое каждому простому модулю сопоставляет элемент некоторой коммутативной группы* Γ, *причем* $\varphi(M) = \varphi(M')$, *если* $M \approx M'$. *Тогда* φ *обладает единственным продолжением до отображения Эйлера — Пуанкаре, определенного на всех модулях конечной длины.*

Доказательство. Для заданной простой фильтрации

$$M = M_1 \supset M_2 \supset \ \dots \ \supset M_r = 0$$

положим

$$\varphi(M) = \sum_{i=1}^{r-1} \varphi(M_i/M_{i+1}).$$

Из теоремы Жордана — Гёльдера непосредственно следует, что эта функция правильно определена и что такое продолжение φ является отображением Эйлера — Пуанкаре.

В частности, мы видим, что длина модуля есть отображение Эйлера — Пуанкаре, принимающее свои значения в аддитивной группе целых чисел и имеющее значение 1 для любого простого модуля.

УПРАЖНЕНИЯ [1])

Взять любую книгу по гомологической алгебре и доказать все теоремы, не заглядывая в доказательства, данные в книге.

Гомологическая алгебра была изобретена Эйленбергом — Маклейном. Общая теория категорий (т. е. теория стрелок) общеизвестна под названием *абстрактной чепухи* (термин принадлежит Стинроду) [2]).

---

[1]) Мы рекомендуем пропустить эти упражнения при первом чтении. — *Прим. ред.*

[2]) Следует отметить, что термин „абстрактная чепуха" носит в книге позитивный характер и используется далее в серьезном смысле. — *Прим. ред.*

Глава V

Многочлены

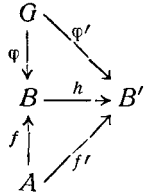
§ 1. Свободные алгебры

Пусть A — коммутативное кольцо. *A-алгебра* (или алгебра над A) — это модуль E вместе с билинейным отображением $E \times E \to E$. *Во всей этой книге мы, если не оговорено противное, будем иметь дело только со следующим специальным типом алгебр.* Пусть $f\colon A \to B$ — гомоморфизм колец, такой, что $f(A)$ содержится в центре B, т. е. $f(a)$ коммутирует с любым элементом из B для всякого $a \in A$. Тогда мы можем рассматривать B как A-модуль, определив действие A на B посредством отображения

$$(a, b) \longmapsto f(a)\,b$$

для всех $a \in A$ и $b \in B$. Аксиомы модуля тривиальным образом удовлетворяются, и мультипликативный закон композиции $B \times B \to B$, очевидно, билинеен (т. е. A-билинеен). Так вот, если не оговорено противное, то под алгеброй над A мы будем всегда понимать указанный выше гомоморфизм колец. Мы говорим, что алгебра является *конечно порожденной*, если B как кольцо над $f(A)$ конечно порождено.

Пусть G — *мультипликативный* моноид и A — коммутативное кольцо. Пусть $\mathscr{C}$ — категория, объектами которой являются тройки (φ, f, B), где $f\colon A \to B$ есть A-алгебра и $\varphi\colon G \to B$ — гомоморфизм мультипликативных моноидов. Если (φ', f', B') — другой объект в $\mathscr{C}$, то морфизм из (φ, f, B) в (φ', f', B') в категории $\mathscr{C}$ — это кольцевой гомоморфизм $h\colon B \to B'$, для которого коммутативна следующая диаграмма:



Универсальный (отталкивающий) объект в $\mathscr{C}$ называется *свободной (A, G)-алгеброй*, или *свободной G-алгеброй над A*. Построим такую алгебру в явном виде.

Пусть $A[G]$ — множество всех отображений $\alpha\colon G \to A$, таких, что $\alpha(x) = 0$ для почти всех $x \in G$. Определяем сложение в $A[G]$ как обычное сложение отображений в абелеву (аддитивную) группу. Если α, $\beta \in A[G]$, то их произведение $\alpha\beta$ определяем формулой

$$(\alpha\beta)(t) = \sum_{xy=t} \alpha(x)\beta(y).$$

Сумма берется по всем таким парам (x, y) с $x, y \in G$, что $xy = t$. Эта сумма в действительности конечна, поскольку имеется лишь конечное число пар элементов $(x, y) \in G \times G$, для которых $\alpha(x)\beta(y) \neq 0$. Мы видим также, что $(\alpha\beta)(t) = 0$ для почти всех t и, следовательно, $\alpha\beta$ принадлежит нашему множеству $A[G]$.

Аксиомы кольца тривиально проверяются. В качестве примера приведем доказательство ассоциативности. Пусть α, β, $\gamma \in A[G]$. Тогда

$$((\alpha\beta)\gamma)(t) = \sum_{xy=t} (\alpha\beta)(x)\gamma(y) = \sum_{xy=t}\left[\sum_{uv=x} \alpha(u)\beta(v)\right]\gamma(y) =$$

$$= \sum_{xy=t}\left[\sum_{uv=x} \alpha(u)\beta(v)\gamma(y)\right] = \sum_{\substack{(u,\,v,\,y)\\ uvy=t}} \alpha(u)\beta(v)\gamma(y),$$

причем последняя сумма берется по всем тройкам (u, v, y), произведение которых равно t. Эта последняя сумма симметрична, и если бы мы вычислили $(\alpha(\beta\gamma))(t)$, то получили бы снова эту сумму. Это доказывает ассоциативность.

Единичным элементом в $A[G]$ служит функция δ, такая, что $\delta(e) = 1$ и $\delta(x) = 0$ для всех $x \in G$, $x \neq e$. Тривиально проверяется, что $\alpha = \delta\alpha = \alpha\delta$ для всех $\alpha \in A[G]$.

Введем теперь другие обозначения, которые сделают структуру $A[G]$ более ясной. Пусть $a \in A$ и $x \in G$. Мы будем обозначать через $a \cdot x$ (а иногда также через ax) функцию, значение которой в x равно a, а в y равно 0, если $y \neq x$. Тогда любой элемент $\alpha \in A[G]$ может быть записан в виде суммы

$$\alpha = \sum_{x \in G} \alpha(x) \cdot x.$$

Действительно, если $\{a_x\}_{x \in G}$ — семейство элементов из A, почти все из которых равны 0, и мы положим

$$\beta = \sum_{x \in G} a_x \cdot x,$$

то для любого $y \in G$ будем иметь $\beta(y) = a_y$ (непосредственно из определений). Это также показывает, что любой данный элемент α допускает единственное представление в виде суммы $\sum a_x \cdot x$.

Имеется естественный способ превратить $A[G]$ в A-модуль. Если $a \in A$ и элемент $\alpha \in A[G]$ записан в виде суммы $\sum a_x \cdot x$, то пола-

гаем $a\alpha$ равным элементу $\sum (aa_x) \cdot x$. Ясно, что все аксиомы модуля удовлетворяются и что множество элементов $\{1 \cdot x\}_{x \in G}$ образует базис $A[G]$ над A.

В наших нынешних обозначениях умножение и сложение могут быть записаны соответственно следующим образом:

$$\left(\sum_{x \in G} a_x \cdot x\right)\left(\sum_{y \in G} b_y \cdot y\right) = \sum_{x, y} a_x b_y \cdot xy,$$

$$\sum_{x \in G} a_x \cdot x + \sum_{x \in G} b_x \cdot x = \sum_{x \in G} (a_x + b_x) \cdot x$$

— именно так, как нам хотелось бы. Отметим, что единичный элемент в $A[G]$ — это просто $1 \cdot e$.

Пусть φ_0: $G \to A[G]$ — отображение, задаваемое формулой $\varphi_0(x) = 1 \cdot x$. Непосредственно проверяется, что отображение φ_0 — гомоморфизм мультипликативных моноидов и что оно на самом деле инъективно, т. е. является вложением.

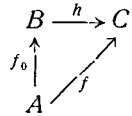
Пусть f_0: $A \to A[G]$ — отображение, задаваемое формулой

$$f_0(a) = a \cdot e.$$

Непосредственно проверяется, что f_0 — гомоморфизм колец, также являющийся вложением. Таким образом, мы превратили $A[G]$ в A-алгебру, и сразу видно, что структура A-модуля на $A[G]$, как на A-алгебре, совпадает с той, которая была описана выше.

Тройка $(\varphi_0, f_0, A[G])$ *есть свободная* (A, G)*-алгебра. Это утверждение является частным случаем следующего предложения.*

Предложение 1. *Пусть* f_0: $A \to B$ — *некоторая* A*-алгебра и* G — *мультипликативный подмоноид в* B. *Предположим, что* G *образует базис для* B *как модуля над* A. *Для всякой* A*-алгебры* f: $A \to C$ *и любого гомоморфизма моноидов* φ: $G \to C$ *существует единственный гомоморфизм колец* h: $B \to C$, *для которого диаграмма*



коммутативна и ограничение h *на* G *равно* φ.

Доказательство. Для каждых $x \in G$ и $a \in A$ пишем $a \cdot x$ вместо $f_0(a)x$. Всякий элемент $\alpha \in A[G]$ имеет единственное представление в виде суммы

$$\alpha = \sum_{x \in G} a_x \cdot x$$

с $a_x \in A$, поскольку G — базис для B над A. Как мы видели при рассмотрении базисов модулей, существует единственный гомоморфизм

модулей $h\colon B \to C$, ограничение которого на G равно φ, а именно такое отображение, для которого

$$h(\alpha) = \sum_{x \in G} f(a_x)\,\varphi(x).$$

Кроме того, если

$$\beta = \sum_{y \in G} b_y \cdot y,$$

то

$$\alpha\beta = \sum_{z \in G} \left(\sum_{xy=z} a_x b_y \right) \cdot z$$

и

$$h(\alpha\beta) = \sum_{z \in G} f\left(\sum_{xy=z} a_x b_y \right) \varphi(z) = \sum_{z \in G} \left(\sum_{xy=z} f(a_x) f(b_y) \right) \varphi(z) = h(\alpha)\, h(\beta).$$

Так как ограничение на G отображения h равно φ, то $h(1) = 1$. Следовательно, h является также гомоморфизмом колец. Отсюда вытекает коммутативность нашей диаграммы. Предложение доказано.

Чтобы вывести из предложения 1, что $(\varphi_0, f_0, A[G])$ — свободная (A, G)-алгебра, надо положить $B = A[G]$ и отождествить G с его образом в $A[G]$ при вложении φ_0.

Начиная с этого момента мы будем, не опасаясь путаницы, писать ax вместо $a \cdot x$. Мы будет называть $A[G]$ *моноидной алгеброй моноида G над A*. Отображения φ_0, f_0 называются *каноническими*.

В следующем параграфе мы в качестве частного случая получим алгебру многочленов. Для случая когда G — группа, групповая алгебра $A[G]$ будет более детально рассмотрена в этой книге позднее.

Наша моноидная алгебра обладает еще одним свойством универсальности.

Предложение 2. *Пусть $\varphi\colon G \to G'$ — гомоморфизм моноидов и $f\colon A \to A'$ — гомоморфизм колец, причем оба кольца A, A' коммутативны. Тогда существует единственный гомоморфизм колец*

$$h\colon A[G] \to A'[G'],$$

для которого коммутативна диаграмма

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow & & \downarrow{\scriptstyle \varphi_0'} \\ A[G] & \xrightarrow{h} & A'[G'] \\ \uparrow & & \uparrow{\scriptstyle f_0'} \\ A & \xrightarrow[f]{} & A' \end{array}$$

(*Вертикальные отображения — канонические.*)

Доказательство. Это прямое следствие предложения 1: положим $C = A'$ [G'], рассмотрим гомоморфизмы

$$\varphi'_0 \circ \varphi \quad \text{и} \quad f'_0 \circ f$$

и применим к ним предложение 1.

§ 2. Определение многочленов

Пусть S — некоторое множество и $\mathbf{N}$ — аддитивный моноид целых чисел $\geqslant 0$ (т. е. моноид натуральных чисел). Обозначим через

$$\mathbf{N}\langle S\rangle$$

множество функций $S \to \mathbf{N}$, которые равны 0 для почти всех элементов из S. (Это по существу та же самая конструкция, которую мы применяли для получения свободных абелевых групп; в настоящем случае мы получаем свободный абелев моноид. Однако мы будем записывать его мультипликативно.) Пусть $x \in S$ и $i \in \mathbf{N}$; мы обозначаем через x^i функцию, которая принимает значение i в x и 0 в $y \neq x$. Если φ, ψ — две функции из $\mathbf{N}\langle S\rangle$, то их произведение $\varphi\psi$ определяется формулой

$$(\varphi\psi)(x) = \varphi(x) + \psi(x).$$

Тогда $\mathbf{N}\langle S\rangle$ будет мультипликативным моноидом, единичным элементом которого служит нулевая функция. Всякий элемент $\varphi \in \mathbf{N}\langle S\rangle$ имеет единственное представление в виде произведения

$$\prod_{x \in S} x^{\nu(x)},$$

где ν: $S \to \mathbf{N}$ — отображение, для которого $\nu(x) = 0$ при почти всех x. Такое произведение будет называться *примитивным одночленом* и будет иногда обозначаться символом $M_{(\nu)}(S)$ или просто $M_{(\nu)}$.

Имеем вложение j_S: $S \to \mathbf{N}\langle S\rangle$ (задаваемое правилом $x \mapsto x^1$), образ которого порождает $\mathbf{N}\langle S\rangle$ как моноид. Отметим, что если n — целое число $\geqslant 0$, то элемент

$$(x^1)^n = x^1 x^1 \ldots x^1$$

равен x^n, т. е. наше обозначение согласуется с обозначением, используемым для произведения функций.

Заметим, что если

$$\prod_{x \in S} x^{\nu(x)} \quad \text{и} \quad \prod_{x \in S} x^{\mu(x)}$$

— примитивные одночлены, то их произведение равно

$$\prod_{x \in S} x^{\nu(x)+\mu(x)}.$$

Как и в случае абелевых групп, имеет место свойство универсальности. Именно, пусть G — коммутативный моноид. Для всякого данного отображения $\lambda\colon S \to G$ существует единственный гомоморфизм моноидов $\mathbf{N}\langle S\rangle \to G$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} S & \xrightarrow{\lambda} & G \\ & {\scriptstyle j_S}\searrow \quad \nearrow & \\ & \mathbf{N}\langle S\rangle & \end{array}$$

В частности, для всякого данного отображения $\lambda\colon S \to S'$ одного множества в другое существует гомоморфизм моноидов $\lambda_*\colon \mathbf{N}\langle S\rangle \to \mathbf{N}\langle S'\rangle$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} S & \xrightarrow{j_S} & \mathbf{N}\langle S\rangle \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\lambda_*} \\ S' & \xrightarrow[j_{S'}]{} & \mathbf{N}\langle S'\rangle, \end{array}$$

иными словами,

$$\lambda_*\Big[\prod_{x\in S} x^{\nu(x)}\Big] = \prod_{x\in S} \lambda(x)^{\nu(x)}.$$

Доказательство этого утверждения тривиально, как и в случае абелевых групп. Можно рассматривать $\mathbf{N}\langle S\rangle$ как функтор из категории множеств в категорию коммутативных моноидов.

Пусть A — коммутативное кольцо. Тогда можно образовать моноидную алгебру $A[\mathbf{N}\langle S\rangle]$ над A, которую мы будем называть *кольцом (или алгеброй) многочленов от S над A*. Для простоты мы будем обозначать это кольцо через $A[S]$. По определению всякий элемент из $A[S]$ имеет единственное представление в виде линейной комбинации

$$\sum_{(\nu)} a_{(\nu)} M_{(\nu)}(S) = \sum_{(\nu)} a_{(\nu)} \prod_{x\in S} x^{\nu(x)},$$

где (ν) пробегает все отображения множества S в $\mathbf{N}$, обращающиеся в 0 для почти всех x, и $a_{(\nu)}$ равно 0 для почти всех (ν). *Примитивные одночлены образуют базис алгебры $A[S]$ над A*, как было отмечено выше для моноидных алгебр. Элементы из $A[S]$ называются *многочленами от S над A*. Элементы $a_{(\nu)}$ называются *коэффициентами* многочлена.

Замечание об обозначениях. Пусть T — подмножество коммутативного кольца B и $\nu\colon T \to \mathbf{N}$ — отображение, для которого $\nu(x) = 0$ при почти всех $x \in T$. Мы будем через $M_{(\nu)}(T)$ обозначать также элемент

$$M_{(\nu)}(T) = \prod_{x\in T} x^{\nu(x)},$$

причем подразумевается, что это произведение берется по тем x, для которых $\nu(x) \neq 0$, и что пустое произведение есть единичный элемент в B. Никакой путаницы с обозначениями для одночленов не возникнет, так как из контекста всегда будет ясно, что мы имеем в виду.

Если S есть множество из n символов $X_1, \ldots, X_n$, то

$$A[S] = A[X_1, \ldots, X_n],$$

и мы будем говорить о кольце (или алгебре) многочленов от $X_1, \ldots, X_n$ над A. Мы иногда будем использовать векторное обозначение и писать $A[X]$ вместо $A[X_1, \ldots, X_n]$.

Всякий многочлен из $A[X]$ может быть однозначно записан в виде

$$\sum a_{(\nu)} M_{(\nu)}(X) = \sum a_{(\nu)} X_1^{\nu_1} \ldots X_n^{\nu_n},$$

где сумма берется по всем наборам из n целых чисел $\nu_1, \ldots, \nu_n \geqslant 0$, причем почти все коэффициенты $a_{(\nu)}$ равны 0.

Пусть снова S — произвольное множество. Отметим, что и S, и A обладают каноническими инъективными отображениями в $A[S]$, задаваемыми соответствиями

$$x \longmapsto 1 \cdot x^1 \text{ и } a \longmapsto a \cdot \prod_{x \in S} x^0.$$

В действительности каноническое отображение A в $A[S]$ является кольцевым гомоморфизмом, именно вложением. Можно безболезненно отождествлять S и A с соответствующими образами в $A[S]$. Одночлен $\prod_{x \in S} x^0$, служащий единичным элементом в моноиде $\mathbf{N}\langle S \rangle$, обозначается также через 1, поскольку это не приводит ни к какой путанице. Таким образом, если S состоит из одного символа X, то всякий многочлен может быть записан в виде

$$a_0 X^0 + a_1 X^1 + \ldots + a_n X^n = a_0 + a_1 X + \ldots + a_n X^n,$$

где $a_\nu \in A$ и n — некоторое целое число $\geqslant 0$.

Пусть A, B — коммутативные кольца и $f_0\colon A \to B$ — некоторая A-алгебра. Пусть S — подмножество в B. Если семейство одночленов

$$M_{(\nu)}(S) = \prod_{x \in S} x^{\nu(x)}$$

линейно независимо над A, то мы будем говорить, что S *алгебраически независимо* над A, или что элементы из S алгебраически независимы над A. Можно было бы также рассмотреть занумерованное множество $S = \{x_i\}_{i \in I}$, образовать одночлены

$$M_{(\nu)}(S) = \prod_{i \in I} x_i^{\nu_i}$$

и назвать семейство $\{x_i\}_{i\in I}$ алгебраически независимым, если одночлены $M_{(\nu)}(S)$ *линейно независимы над* A. *В частности, когда* множество S конечно, скажем $S=\{t_1, \ldots, t_n\}$, одночлены имеют вид

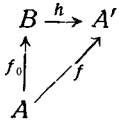
$$M_{(\nu)}(t_1, \ldots, t_n)=t_1^{\nu_1}\ldots t_n^{\nu_n},$$

где $(\nu_1, \ldots, \nu_n)$ пробегает все наборы из n целых чисел $\geqslant 0$.

Наша конструкция алгебры многочленов показывает, как при заданном коммутативном кольце A можно построить A-алгебру, имеющую сколь угодно много алгебраически независимых элементов.

Следующая теорема дает нам важное свойство универсальности для алгебраически независимых элементов.

Теорема 1. *Пусть* A, B *— коммутативные кольца,* f_0: $A\to B$ *— A-алгебра,* S *— подмножество в* B, *порождающее* B. *Предположим, что элементы из* S *алгебраически независимы над* A. *Пусть* A' *— коммутативное кольцо,* f: $A\to A'$ *— гомоморфизм колец и* λ: $S\to A'$ *— некоторое отображение. Тогда существует единственный гомоморфизм колец* h: $B\to A'$, *для которого диаграмма*



коммутативна, и ограничение h *на* S *равно* λ.

Доказательство. Пусть G — мультипликативный моноид, состоящий из всех элементов $M_{(\nu)}(S)$ в B. Если $\nu\neq\mu$, то $M_{(\nu)}(S)\neq M_{(\mu)}(S)$, так как иначе мы имели бы соотношение линейной зависимости

$$M_{(\nu)}(S)-M_{(\mu)}(S)=0.$$

Следовательно, отображение φ: $G\to A'$, для которого

$$\varphi\Big(\prod_{x\in S}x^{\nu(x)}\Big)=\prod_{x\in S}\lambda(x)^{\nu(x)},$$

является гомоморфизмом моноидов. Для завершения доказательства применяем предложение 1.

Мы можем применить теорему 1 к алгебре многочленов $A[S]$, отождествив множество S с его каноническим образом в $A[S]$. Тогда, если $B=A[S]$ и

$$\alpha=\sum_{(\nu)}a_{(\nu)}\cdot\prod_{x\in S}x^{\nu(x)},$$

то гомоморфизм h записывается так:

$$h(\alpha)=\sum_{(\nu)}f(a_{(\nu)})\prod_{x\in S}\lambda(x)^{\nu(x)}.$$

Рассмотрим частный случай, когда S — конечное множество, состоящее из различных элементов $t_1, \ldots, t_n$, алгебраически независимых над A. Пусть $X_1, \ldots, X_n$ суть n различных символов. Тогда имеется гомоморфизм колец

$$A[X_1, \ldots, X_n] \to A[t_1, \ldots, t_n],$$

отображающий X_i в t_i и индуцирующий тождественное отображение на A. Из определений тотчас видно, что его ядро должно быть равно 0 и что поэтому мы имеем изоморфизм. В частности, любые два кольца, порожденные над A n алгебраически независимыми элементами, изоморфны.

Имеется еще несколько частных случаев теоремы 1, которые мы специально отметим.

Пусть сначала A фиксировано, и пусть S, S' — два множества с заданной биекцией λ: $S \to S'$. Рассматривая S' как подмножество в $A[S']$, получаем изоморфизм

$$A[S] \approx A[S'],$$

индуцирующий биекцию S на S'. В случае когда S состоит из n символов $X_1, \ldots, X_n$ и S' состоит из n символов $Y_1, \ldots, Y_n$, мы видим, что кольца многочленов изоморфны, причем этот изоморфизм для каждого i переводит X_i в Y_i.

Предположим, что S содержится в S'. Тогда $A[S]$ канонически вкладывается в $A[S']$. Если S есть множество $\{X_1, \ldots, X_n\}$ и S' есть множество

$$\{X_1, \ldots, X_n, X_{n+1}, \ldots, X_N\},$$

то мы можем считать кольцо многочленов $A[X_1, \ldots, X_n]$ содержащимся в $A[X_1, \ldots, X_N]$. Одночлен

$$X_1^{\nu_1} \ldots X_n^{\nu_n}$$

может рассматриваться как одночлен от $X_1, \ldots, X_N$, если продолжить функцию ν так, чтобы $\nu_i = 0$ для $i > n$.

Пусть теперь A — подкольцо кольца A' и S — некоторое множество. Тогда имеем естественное вложение $A[S]$ в $A'[S]$, а именно многочлен

$$\sum a_{(\nu)} \prod_{x \in S} x^{\nu(x)}$$

с коэффициентами в A может рассматриваться как многочлен, имеющий коэффициенты в A'. Мы будем отождествлять $A[S]$ с соответствующим подкольцом в $A'[S]$.

Более общо, пусть σ: $A \to A'$ — гомоморфизм коммутативных колец. Тогда этот гомоморфизм единственным способом продолжается до гомоморфизма колец

$$\bar{\sigma}\colon A[S] \to A'[S],$$

индуцирующего тождественное отображение на S. Например, пусть S — множество из n символов $X_1, \ldots, X_n$. Тогда

$$\bar{\sigma}\colon A[X_1, \ldots, X_n] \to A'[X_1, \ldots, X_n]$$

есть гомоморфизм колец, задаваемый отображением

$$\sum a_{(\nu)} X_1^{\nu_1} \ldots X_n^{\nu_n} \longmapsto \sum \sigma(a_{(\nu)}) X_1^{\nu_1} \ldots X_n^{\nu_n}.$$

Пусть α обозначает многочлен, стоящий слева от стрелки; мы часто будем обозначать многочлен, стоящий справа, символом α^σ.

Можно сказать, что α^σ получается из α применением σ к коэффициентам α.

Пусть A — целостное кольцо и $\mathfrak{p}$ — его простой идеал. Пусть $\sigma\colon A \to A'$ — канонический гомоморфизм A на $A/\mathfrak{p}$. Если $\alpha(X)$ — многочлен из $A[X]$, то α^σ будет иногда называться *редукцией* α *по модулю* $\mathfrak{p}$.

Например, взяв $A = \mathbf{Z}$ и $\mathfrak{p} = (p)$, где p — простое число, мы можем говорить о многочлене $3X^4 - X + 2$ как о многочлене mod 5, рассматривая коэффициенты 3, -1, 2 как целые числа mod 5, т. е. как элементы из $\mathbf{Z}/5\mathbf{Z}$.

§ 3. *Элементарные свойства многочленов*

Пусть A — коммутативное кольцо и S — множество из n символов $X_1, \ldots, X_n$. Отождествляя $X_1, \ldots, X_n$ с их каноническими образами в кольце многочленов $A[X_1, \ldots, X_n]$, мы называем $X_1, \ldots, X_n$ *независимыми переменными* над A, а $A[X]$—кольцом многочленов от n переменных. Всякий многочлен α из $A[X]$ допускает единственное представление в виде

$$\alpha = \sum a_{(\nu)} X_1^{\nu_1} \ldots X_n^{\nu_n} = \sum a_{(\nu)} M_{(\nu)}(X).$$

Пусть $(b_1, \ldots, b_n)$ — элемент из $\prod_1^n A$ (прямого произведения A самого на себя n раз), которое мы будем обозначать через $A^{(n)}$. В силу теоремы 1 существует однозначно определенный гомоморфизм

$$h\colon A[X_1, \ldots, X_n] \to A,$$

для которого $h(X_i) = b_i$ при $i = 1, \ldots, n$ и который тождествен на A. Имеем

$$h(\alpha) = \sum a_{(\nu)} b_1^{\nu_1} \ldots b_n^{\nu_n}.$$

Мы будем обозначать этот элемент из A через $\alpha(b_1, \ldots, b_n)$ и говорить, что это элемент, полученный *подстановкой* $(b_1, \ldots, b_n)$

вместо $(X_1, \ldots, X_n)$ в α. Таким образом, мы видим, что α определяет функцию на $A^{(n)}$ со значениями в A.

Аналогично, если A — подкольцо (коммутативного) кольца B и $(b) = (b_1, \ldots, b_n)$ — элемент из $B^{(n)}$, то мы можем тем же путем, что и выше, образовать элемент $\alpha(b)$ и получить функцию из $B^{(n)}$ в B, задаваемую соответствием $(b) \longmapsto \alpha(b)$.

Записывая α, как и выше, мы видим, что

$$\alpha(b_1, \ldots, b_n) = \sum a_{(\nu)} M_{(\nu)}(b_1, \ldots, b_n),$$

или в векторных обозначениях

$$\alpha(b) = \sum a_{(\nu)} M_{(\nu)}(b).$$

В этих обозначениях

$$\alpha = \alpha(X) = \alpha(X_1, \ldots, X_n).$$

Мы увидим ниже, что в том случае, когда A — целостное кольцо, $A[X_1, \ldots, X_n]$ также целостное. Если K — поле частных кольца A, то поле частных кольца $A[X_1, \ldots, X_n]$ обозначается через $K(X_1, \ldots, X_n)$. Элементы поля $K(X_1, \ldots, X_n)$ называются *рациональными функциями*. Всякая рациональная функция может быть записана в виде дроби $f(X)/g(X)$, где f, g — многочлены. Если $(b_1, \ldots, b_n)$ — элемент из $K^{(n)}$ и рациональная функция допускает представление в виде такой дроби f/g, что $g(b) \neq 0$, то мы говорим, что эта рациональная функция *определена* в (b). Из общих свойств локализации вытекает, что в этом случае мы можем подставить (b) в рациональную функцию и получить значение $f(b)/g(b)$.

Может случиться, что многочлен не является нулевым многочленом, но определяет нулевую функцию.

Пример. Пусть $A = \mathbf{Z}/p\mathbf{Z}$ для некоторого простого p. Если $a \in A$ и $a = 0$, то $a^p = 0$. Если $a \neq 0$, то a — элемент мультипликативной группы ненулевых элементов из A, имеющей порядок $p - 1$. Значит, $a^{p-1} = 1$, и мы получаем

$$a^p = a.$$

Это справедливо для всех $a \in A$. Поэтому многочлен $X^p - X$ определяет нулевое отображение A в себя, а многочлены X^p и X определяют одну и ту же функцию, а именно тождественное отображение на A.

Вообще пусть F — конечное поле и q — число элементов в F. Тогда как X^q, так и X определяют тождественное отображение F в себя. Можно показать, что любое отображение F в себя задается некоторым многочленом (от одной переменной) и аналогично любая функция на $F^{(n)}$ со значениями в F задается некоторым многочленом от n переменных (см. упражнения).

Пусть снова A — подкольцо в B, и пусть $b_1, \ldots, b_n$ — элементы из B. Напомним, что если гомоморфизм

$$A[X_1, \ldots, X_n] \to B,$$

задаваемый соответствием $\alpha(X) \mapsto \alpha(b)$, имеет тривиальное ядро, т. е. если он является вложением, то $b_1, \ldots, b_n$ *алгебраически независимы над* A. Если $n = 1$ и элемент $b = b_1$ алгебраически независим над A, то мы также говорим, что b *трансцендентен* над A.

Пример. Известно (хотя и не тривиально доказывается), что числа $e = 2{,}71\ldots$ и $\pi = 3{,}14\ldots$ трансцендентны над полем рациональных чисел $\mathbf{Q}$. Не известно, являются ли они алгебраически независимыми (или даже, рационально ли число $e + \pi$). Для конкретных комплексных чисел обычно бывает чрезвычайно трудно выяснить, являются ли они трансцендентными или же алгебраически независимыми над полем рациональных чисел.

Пусть A обозначает, как и прежде, коммутативное кольцо, и пусть $S = \{X_1, \ldots, X_n\}$. Под *степенью* примитивного одночлена

$$X_1^{\nu_1} \ldots X_n^{\nu_n}$$

мы будем понимать целое число $\nu_1 + \ldots + \nu_n$ (которое $\geqslant 0$).

Многочлен

$$aX_1^{\nu_1} \ldots X_n^{\nu_n} \quad (a \in A)$$

будет называться *одночленом* (не обязательно примитивным).

Если $\alpha(X)$ — многочлен из $A[X]$, записываемый в виде

$$\alpha(X) = \sum a_{(\nu)} X_1^{\nu_1} \ldots X_n^{\nu_n},$$

то либо $\alpha = 0$, и в этом случае мы говорим, что его степень равна $-\infty$, либо $\alpha \neq 0$, и тогда мы определяем *степень* α как максимум степеней одночленов $M_{(\nu)}(X)$, для которых $\alpha_{(\nu)} \neq 0$. (О таких одночленах говорят, что они *встречаются* в многочлене.) Отметим, что степень многочлена α равна 0 в том и только в том случае, если

$$\alpha(X) = a_0 X_1^0 \ldots X_n^0$$

для некоторого $a_0 \in A$, $a_0 \neq 0$. Этот многочлен мы также записываем просто как $\alpha(X) = a_0$, т. е. пишем 1 вместо

$$X_1^0 \ldots X_n^0,$$

отождествляя тем самым этот многочлен с константой a_0.

Отметим, что многочлен $\alpha(X_1, \ldots, X_n)$ от n переменных можно рассматривать как многочлен от X_n с коэффициентами в $A[X_1, \ldots, X_{n-1}]$ (если $n \geqslant 2$). Действительно, имеет место гомоморфизм

$$A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_{n-1}][X_n],$$

получаемый подстановкой, и этот гомоморфизм, очевидно, является изоморфизмом. Таким образом,

$$\alpha(X_1, \ldots, X_n) = \sum_{j=0}^{\infty} \alpha_j(X_1, \ldots, X_{n-1}) X_n^j,$$

где α_j — элементы из $A[X_1, \ldots, X_{n-1}]$. Под *степенью многочлена* α *относительно* X_n мы будем понимать его степень как многочлена от X_n с коэффициентами в $A[X_1, \ldots, X_{n-1}]$. Легко видеть, что если эта степень равна d, то d — наибольшее целое число, встречающееся в качестве показателя при X_n в одночленах

$$a_{(\nu)} X_1^{\nu_1} \ldots X_n^{\nu_n}$$

с $a_{(\nu)} \neq 0$. Аналогичным образом определяем степень по каждой переменной X_i $(i = 1, \ldots, n)$.

Степень многочлена α по каждой отдельной переменной, как правило, отличается, конечно, от его степени (которую называют иногда *полной* степенью, если хотят избежать двусмысленности). Например,

$$X_1^3 X_2 + X_2^2$$

имеет полную степень 4, степень 3 по X_1 и 2 по X_2.

Мы будем часто слово „степень" сокращенно обозначать символом deg.

Пусть $f(X)$ — многочлен от одной переменной из $A[X]$

$$f(X) = a_0 + \ldots + a_n X^n,$$

где $a_i \in A$ и n — некоторое целое число $\geqslant 0$. Если $f \neq 0$ и $\deg f = n$, то по определению $a_n \neq 0$; мы называем a_n *старшим коэффициентом* многочлена f, а a_0 — его *постоянным членом*. Заметим, что $a_0 = f(0)$.

Пусть

$$g(X) = b_0 + \ldots + b_m X^m$$

— некоторый многочлен из $A[X]$ степени m, причем $g \neq 0$. Тогда

$$f(X)\, g(X) = a_0 b_0 + \ldots + a_n b_m X^{m+n}.$$

Если предположить, что по крайней мере один из старших коэффициентов a_n *или* b_m *не является делителем* 0 *в* A, *то*

$$\deg(fg) = \deg f + \deg g$$

и старший коэффициент fg *равен* $a_n b_m$. *Это выполняется, в частности, в тех случаях, когда* a_n *или* b_m *есть единица в* A, *или*

когда кольцо A — целостное. Следовательно, если A — целостное кольцо, то $A[X]$ также целостное.

Если f или $g = 0$, то мы по-прежнему имеем

$$\deg(fg) = \deg f + \deg g,$$

если считать, что $-\infty + m = -\infty$ для любого целого m.

Тривиально проверяется, что для любых многочленов f, $g \in A[X]$ имеет место неравенство

$$\deg(f+g) \leqslant \max(\deg f, \deg g),$$

опять-таки при соглашении, что $-\infty < m$ для всякого целого m.

Мы предоставляем читателю в качестве упражнения доказать, что в том случае, когда A — целостное кольцо и f, g — многочлены *от нескольких переменных*, имеют место те же правила:

$$\deg(fg) = \deg f + \deg g,$$

$$\deg(f+g) \leqslant \max(\deg f, \deg g).$$

Здесь степень может пониматься либо как полная степень, либо как степень по одной из переменных. Мы заключаем отсюда, что кольцо $A[X_1 \ldots, X_n]$ — целостное.

Пусть снова A — произвольное коммутативное кольцо и d — целое число $\geqslant 0$. Пусть

$$f(X_1, \ldots, X_n) \neq 0$$

— многочлен от n переменных над A. Мы будем говорить, что f — *однородный* многочлен степени d, или *форма* степени d, если все одночлены, встречающиеся в f, имеют степень d, т. е. если в записи

$$f(X) = \sum a_{(\nu)} X_1^{\nu_1} \ldots X_n^{\nu_n}$$

для всякого $a_{(\nu)} \neq 0$ имеем

$$\nu_1 + \ldots + \nu_n = d.$$

Мы предоставим читателю в качестве упражнения доказать, что *ненулевой многочлен f от n переменных над A является однородным степени d тогда и только тогда, когда для всякого множества из $n+1$ алгебраически независимых элементов $u, t_1, \ldots, t_n$ над A имеет место равенство*

$$f(ut_1, \ldots, ut_n) = u^d f(t_1, \ldots, t_n).$$

Пусть f — однородный многочлен степени d. В силу теоремы 1 аналогичное соотношение выполняется, если подставить вместо u, $t_1, \ldots, t_n$ произвольные элементы $b_0, b_1, \ldots, b_n$ (при этом b_i берутся из некоторого коммутативного кольца B, содержащего A в качестве подкольца).

Отметим, что если f и g — однородные многочлены степеней d и e соответственно и $fg \neq 0$, то fg — однородный многочлен степени de. Если $d = e$ и $f + g \neq 0$, то $f + g$ — однородный многочлен степени d.

Наконец, сделаем одно замечание относительно терминологии. Ввиду изоморфизма

$$A[X_1, \ldots, X_n] \approx A[t_1, \ldots, t_n]$$

между кольцом многочленов от n переменных и кольцом, порожденным над A n алгебраически независимыми элементами, мы можем применять всю терминологию, введенную нами для многочленов, к элементам из $A[t_1, \ldots, t_n]$. Таким образом, мы можем говорить о степени элемента из $A[t]$, и правила для степени произведения и суммы будут выполняться. Фактически мы будем элементы из $A[t]$ называть также многочленами от (t). Алгебраически независимые элементы будут также называться переменными (или независимыми переменными); любое различие, которое мы делаем между $A[X]$ и $A[t]$, является скорее психологическим, чем математическим.

§ 4. Алгоритм Евклида

Теорема 2. *Пусть A — коммутативное кольцо, f, $g \in A[X]$ — многочлены от одной переменной степени $\geqslant 0$. Предположим, что старший коэффициент многочлена g является единицей в A. Тогда существуют однозначно определенные многочлены q, $r \in A[X]$, такие, что*

$$f = gq + r$$

и $\deg r < \deg g$.

Доказательство. Пусть

$$f(X) = a_n X^n + \ldots + a_0,$$
$$g(X) = b_d X^d + \ldots + b_0,$$

где $n = \deg f$, $d = \deg g$, так что a_n, $b_d \neq 0$ и b_d — единица в A. Применим индукцию по n.

Если $n = 0$ и $\deg g > \deg f$, то положим $q = 0$, $r = f$. Если $\deg g = \deg f = 0$, то положим $r = 0$ и $q = a_n b_d^{-1}$.

Предположим, что теорема доказана для многочленов степени $< n$ (где $n > 0$). Мы можем предполагать, что $\deg g \leqslant \deg f$ (иначе возьмем $q = 0$ и $r = f$). Тогда

$$f(X) = a_n b_d^{-1} X^{n-d} g(X) + f_1(X),$$

где $f_1(X)$ имеет степень $< n$. По индукции мы можем найти q_1, r, такие, что

$$f(X) = a_n b_d^{-1} X^{n-d} g(X) + q_1(X) g(X) + r(X)$$

и $\deg r < \deg g$. Положим

$$q(X) = a_n b_d^{-1} X^{n-d} + q_1(X),$$

чем доказательство существования q, r и закончено.

Что касается единственности, то предположим, что

$$f = q_1 g + r_1 = q_2 g + r_2,$$

где $\deg r_1 < \deg g$ и $\deg r_2 < \deg g$. Тогда

$$(q_1 - q_2) g = r_2 - r_1.$$

Так как по предположению старший коэффициент g есть единица, то

$$\deg (q_1 - q_2) g = \deg (q_1 - q_2) + \deg g.$$

Поскольку $\deg (r_2 - r_1) < \deg g$, то предыдущее соотношение может выполняться только при $q_1 - q_2 = 0$, т. е. $q_1 = q_2$ и, следовательно, $r_1 = r_2$, что и требовалось показать.

Теорема 3. *Пусть k — поле. Тогда кольцо многочленов от одной переменной $k[X]$ является целостным кольцом главных идеалов.*

Доказательство. Пусть $\mathfrak{a}$ — идеал в $k[X]$, причем $\mathfrak{a} \neq 0$. Пусть g — элемент из $\mathfrak{a}$ наименьшей степени $\geqslant 0$ и f — любой отличный от нуля элемент из $\mathfrak{a}$. Согласно алгоритму Евклида (т. е. по теореме 2) мы можем найти q, $r \in k[X]$, такие, что

$$f = qg + r$$

и $\deg r < \deg g$. Но $r = f - qg$, следовательно, r лежит в $\mathfrak{a}$. Так как g имеет минимальную степень $\geqslant 0$, то $r = 0$; значит, $\mathfrak{a}$ состоит из всех многочленов вида qg (где $q \in k[X]$). Это доказывает нашу теорему.

Следствие. *Кольцо $k[X]$ факториально.*

Если k — поле, то всякий ненулевой элемент из k будет единицей в k и непосредственно видно, что единицы в $k[X]$ — это просто единицы из k. (Никакой многочлен степени $\geqslant 1$ не может быть единицей ввиду формулы сложения для степени произведения.)

Пусть A — коммутативное кольцо и $f(X)$ — многочлен из $A[X]$. Пусть A — подкольцо в B. Элемент $b \in B$ называется *корнем* или *нулем* f в B, если $f(b) = 0$. Аналогично, если (X) — набор из n переменных, то набор из n элементов (b) называется нулем f, если $f(b) = 0$.

Теорема 4. *Пусть k — поле и f — многочлен степени $n \geqslant 0$ из $k[X]$ от одной переменной X. Тогда f имеет самое большее n корней в k, и если a — корень f в k, то $f(X)$ делится на $X - a$.*

Доказательство. Предположим, что $f(a)=0$. Найдем q, r, такие, что

$$f(X)=q(X)(X-a)+r(X)$$

и $\deg r<1$. Тогда

$$0=f(a)=r(a).$$

Поскольку r либо 0, либо ненулевая константа, то мы должны иметь $r=0$, т. е. $X-a$ делит $f(X)$. Если $a_1, \ldots, a_m$ — различные корни f в k, то по индукции мы находим, что $f(X)$ делится на произведение

$$(X-a_1)\ldots(X-a_m),$$

откуда $m\leqslant n$, как и утверждалось.

Следствие 1. *Пусть k — поле, T — бесконечное подмножество в k и $f(X)\in k[X]$ — многочлен от одной переменной. Если $f(a)=0$ для всех $a\in T$, то $f=0$; иными словами, если f индуцирует нулевую функцию на T, то f — нулевой многочлен.*

Следствие 2. *Пусть k — поле, $T_1, \ldots, T_n$ — бесконечные подмножества в k и $f(X_1, \ldots, X_n)$ — многочлен от n переменных над k. Если $f(a_1, \ldots, a_n)=0$ для всех $a_i\in T_i$ $(i=1, \ldots, n)$, то $f=0$.*

Доказательство. По индукции. Мы только что убедились, что теорема справедлива для одной переменной. Пусть $n\geqslant 2$; запишем

$$f(X_1, \ldots, X_n)=\sum_j f_j(X_1, \ldots, X_{n-1})X_n^j$$

как многочлен от X_n с коэффициентами в $k[X_1, \ldots, X_{n-1}]$. Если существует набор

$$(b_1, \ldots, b_{n-1})\in T_1\times\ldots\times T_{n-1},$$

такой, что $f_j(b_1, \ldots, b_{n-1})\neq 0$ для некоторого j, то

$$f(b_1, \ldots, b_{n-1}, X)$$

— ненулевой многочлен в $k[X_n]$, принимающий значение 0 на бесконечном множестве элементов T_n. Но это невозможно. Следовательно, f_j индуцирует нулевую функцию на $T_1\times\ldots\times T_{n-1}$ для всех j и по индукции мы имеем, что $f_j=0$ для всех j. Следовательно, $f=0$, что и требовалось показать.

Следствие 3. *Пусть k — бесконечное поле и f — многочлен от n переменных над k. Если f индуцирует нулевую функцию на $k^{(n)}$, то $f=0$.*

Рассмотрим теперь случай конечных полей. Пусть k — конечное поле из q элементов и $f(X_1, \ldots, X_n)$ — многочлен от n переменных над k. Запишем

$$f(X_1, \ldots, X_n) = \sum a_{(\nu)} X_1^{\nu_1} \ldots X_n^{\nu_n}.$$

Как мы условились говорить, одночлен $M_{(\nu)}(X)$ *встречается* в f, если $a_{(\nu)} \neq 0$. Предположим, что это имеет место и что в нашем одночлене $M_{(\nu)}(X)$ некоторая переменная X_i встречается с показателем $\nu_i \geqslant q$. Тогда мы можем написать

$$X_i^{\nu_i} = X_i^{q+\mu}, \quad \text{где } \mu \text{ — целое число } \geqslant 0.$$

Если мы теперь заменим в этом одночлене $X_i^{\nu_i}$ на $X_i^{\mu+1}$, то получим новый многочлен, определяющий ту же самую функцию, что и f. Степень этого нового многочлена не больше, чем степень f.

Выполняя предыдущую операцию конечное число раз для всех одночленов, встречающихся в f, и всех переменных $X_1, \ldots, X_n$, мы получим некоторый новый многочлен f^*, который определяет ту же самую функцию, что и f, но степень которого по каждой переменной $< q$.

Теорема 5. *Пусть k — конечное поле из q элементов и f — многочлен от n переменных над k, такой, что степень f по каждой переменной $< q$. Если f индуцирует нулевую функцию на $k^{(n)}$, то $f = 0$.*

Доказательство. По индукции. Если $n = 1$, то $\deg f < q$ и, следовательно, f не может иметь q корней в случае $f \neq 0$. Индуктивный шаг проводится точно так же, как в доказательстве следствия 2.

Пусть f — многочлен от n переменных над конечным полем k. Многочлен g, степень которого по каждой переменной $< q$, будем называть *редуцированным*. Выше мы показали, что существует редуцированный многочлен f^*, который дает ту же самую функцию на $k^{(n)}$, что и f. Теорема 5 теперь показывает, что *этот редуцированный многочлен единствен*. Действительно, если g_1, g_2 — редуцированные многочлены, дающие одну и ту же функцию, то $g_1 - g_2$ редуцирован и дает нулевую функцию. Следовательно, $g_1 - g_2 = 0$ и $g_1 = g_2$.

Дадим еще одно приложение теоремы 4. Пусть k — поле. Под мультипликативной подгруппой в k мы будем понимать подгруппу группы k^* (ненулевых элементов k).

Теорема 6. *Пусть k — поле. Всякая конечная мультипликативная подгруппа U в k циклическая.*

Доказательство. Запишем U в виде произведения подгрупп $U(p)$ для всех простых p, где $U(p)$ есть p-группа. В силу упражнения 22 из гл. I достаточно доказать, что $U(p)$ циклическая для каждого p. Пусть a — элемент из $U(p)$ максимального периода p^r, где r — некоторое целое число. Тогда $x^{p^r}=1$ для всех элементов $x\in U(p)$ и, следовательно, все элементы из $U(p)$ являются корнями многочлена

$$X^{p^r}-1.$$

Циклическая группа, порожденная a, содержит p^r элементов. Если эта циклическая группа не совпадает с $U(p)$, то наш многочлен имеет более чем p^r корней, что невозможно. Следовательно, a порождает $U(p)$, и наша теорема доказана.

Следствие. *Если k — конечное поле, то группа k^* — циклическая.*

Элемент ζ поля k, для которого существует такое целое число $n\geqslant 1$, что $\zeta^n=1$, называется *корнем из единицы* или, более точно, корнем n-й степени из единицы. Таким образом, множество корней n-й степени из единицы — это множество корней многочлена X^n-1. Существует самое большее n таких корней, и они, очевидно, образуют группу, которая, согласно теореме 6, является циклической. Позднее мы изучим корни из единицы более подробно. Образующая группы корней n-й степени из единицы (в том случае, если эта группа имеет порядок n) называется *примитивным* (или *первообразным*) корнем n-й степени из единицы. Например, в поле комплексных чисел $e^{2\pi i/n}$ — примитивный корень n-й степени из единицы, а все корни n-й степени из единицы имеют вид $e^{2\pi i\nu/n}$, где $1\leqslant\nu\leqslant n$.

§ 5. Простейшие дроби

В этом параграфе мы займемся анализом поля частных кольца главных идеалов, используя факториальность такого кольца.

Теорема 7. *Пусть A — целостное кольцо главных идеалов и P — множество представителей для его неприводимых элементов. Пусть K — поле частных кольца A и α — некоторый элемент из K. Тогда для каждого $p\in P$ найдутся элемент $\alpha_p\in A$ и целое число $j(p)\geqslant 0$, такие, что $j(p)=0$ для почти всех $p\in P$, α_p и $p^{j(p)}$ взаимно просты и*

$$\alpha=\sum_{p\in P}\frac{\alpha_p}{p^{j(p)}}.$$

Если имеется другое такое представление

$$\alpha = \sum_{p \in P} \frac{\beta_p}{p^{i(p)}},$$

то $j(p) = i(p)$ *и* $\alpha_p \equiv \beta_p \bmod p^{j(p)}$ *для всех* p.

Доказательство. Докажем сначала существование такого представления. Пусть a, b — взаимно простые ненулевые элементы из A. Тогда существуют x, $y \in A$, для которых $xa + yb = 1$. Следовательно,

$$\frac{1}{ab} = \frac{x}{b} + \frac{y}{a},$$

так что любая дробь c/ab с $c \in A$ может быть разложена в сумму двух дробей (а именно, cx/b и cy/a), знаменатели которых делят b и a соответственно. По индукции отсюда вытекает, что любой элемент $\alpha \in K$ имеет требуемое представление, за тем возможным исключением, что p может делить α_p. Сокращение на наибольший общий делитель приводит к представлению, удовлетворяющему всем нужным условиям.

Что касается единственности, то предположим, что α имеет два представления, указанных в теореме. Пусть q — фиксированный простой элемент из P. Тогда

$$\frac{\alpha_q}{q^{j(q)}} - \frac{\beta_q}{q^{i(q)}} = \sum_{p \neq q} \frac{\beta_p}{p^{i(p)}} - \frac{\alpha_p}{p^{j(p)}}.$$

Если $j(q) = i(q) = 0$, то для q наши условия удовлетворяются. Предположим, что одно из чисел $j(q)$, $i(q)$ отлично от нуля, скажем $j(q) > 0$ и $j(q) \geqslant i(q)$. Пусть d — наименьшее общее кратное для всех степеней $p^{j(p)}$ и $p^{i(p)}$, таких, что $p \neq q$. Умножим предыдущее равенство на $dq^{j(q)}$. Получим

$$d(\alpha_q - q^{j(q)-i(q)}\beta_q) = q^{j(q)}\beta$$

для некоторого $\beta \in A$. Кроме того, d не делится на q. Если $i(q) < j(q)$, то q делит α_q, что невозможно. Следовательно, $i(q) = j(q)$. Но тогда $\alpha_q - \beta_q$ делится на $q^{j(q)}$, что и доказывает теорему.

Применим теорему 7 к кольцу многочленов $k[X]$ над полем k. Пусть P — множество неприводимых многочленов, нормированных так, чтобы старший коэффициент у них был равен 1. Тогда P будет множеством представителей для всех неприводимых элементов из $k[X]$. В представлении для α, указанном в теореме 7, мы можем теперь разделить α_p на $p^{j(p)}$, т. е. применить алгоритм Евклида, если $\deg \alpha_p \geqslant \deg p^{j(p)}$. Мы обозначаем поле частных кольца $k[X]$ через $k(X)$ и называем его элементы рациональными функциями.

Теорема 8. *Пусть $A = k[X]$ — кольцо многочленов от одной переменной над полем k. Пусть P — множество неприводимых многочленов в $k[X]$ со старшим коэффициентом 1. Тогда любой элемент f из $k(X)$ имеет единственное представление в виде*

$$f(X) = \sum_{p \in P} \frac{f_p(X)}{p(X)^{j(p)}} + g(X),$$

где f_p, g — многочлены, $f_p = 0$ при $j(p) = 0$, f_p взаимно прост с p при $j(p) > 0$ и $\deg f_p < \deg p^{j(p)}$ при $j(p) > 0$.

Доказательство. Существование немедленно вытекает из предшествующих замечаний. Единственность следует из того факта, что если имеются два представления с элементами f_p и φ_p соответственно и с многочленами g, h, то $p^{j(p)}$ делит $f_p - \varphi_p$, откуда $f_p - \varphi_p = 0$, а потому $f_p = \varphi_p$, $g = h$.

Можно и дальше разложить член $f_p/p^{j(p)}$, выразив f_p через суммы степеней p. При этом мы добьемся того, что в выражении многочлена f, указанном в теореме 8, будут содержаться лишь так называемые *простейшие дроби* $f_p/p^{j(p)}$, в которых $\deg f_p < \deg p$. В действительности это можно сделать в несколько более общей форме.

Теорема 9. *Пусть k — поле, $k[X]$ — кольцо многочленов от одной переменной, $f, g \in k[X]$. Предположим, что $\deg g \geqslant 1$. Тогда существуют однозначно определенные многочлены*

$$f_0, f_1, \ldots, f_d \in k[X],$$

такие, что $\deg f_i < \deg g$ и

$$f = f_0 + f_1 g + \ldots + f_d g^d.$$

Доказательство. Сначала докажем существование. Если $\deg g > \deg f$, то возьмем $f_0 = f$ и $f_i = 0$ для $i > 0$. Предположим, что $\deg g \leqslant \deg f$. Можно найти многочлены q, r, такие, что

$$f = qg + r, \quad \deg r < \deg g,$$

и так как $\deg g \geqslant 1$, то $\deg q < \deg f$. По индукции существуют многочлены $h_0, h_1, \ldots, h_s$, для которых

$$q = h_0 + h_1 g + \ldots + h_s g^s$$

и, следовательно,

$$f = r + h_0 g + \ldots + h_s g^{s+1},$$

что и доказывает существование.

Что касается единственности, то пусть

$$f = f_0 + f_1 g + \ldots + f_d g^d = \varphi_0 + \varphi_1 g + \ldots + \varphi_m g^m$$

— два разложения, удовлетворяющие условиям теоремы. Добавляя члены, равные 0, к одной из сторон, мы можем считать, что $m = d$. Вычитая, получим

$$0 = (f_0 - \varphi_0) + \ldots + (f_d - \varphi_d)\, g^d.$$

Следовательно, g делит $f_0 - \varphi_0$, а поскольку $\deg(f_0 - \varphi_0) < \deg g$, то $f_0 = \varphi_0$. Возьмем наименьшее i, для которого $f_i \neq \varphi_i$ (если такое i существует). Разделив наше равенство на g^i, мы найдем, что g делит $f_i - \varphi_i$ и что, следовательно, такого i не может существовать. Это доказывает единственность.

Полученное в теореме 9 разложение f по степеням g мы будем называть *g-адическим разложением* многочлена f. Если $g(X) = X$, то g-адическое разложение совпадает с обычной записью f как многочлена.

§ 6. Однозначность разложения на простые множители многочленов от нескольких переменных

Пусть A — факториальное кольцо и K — его поле частных. Пусть $a \in K$, $a \neq 0$. Мы можем представить a в виде отношения элементов из A, не имеющих общих простых множителей. Если p — простой элемент из A, то

$$a = p^r b,$$

где $b \in K$, r — целое число и p не делит ни числитель, ни знаменатель элемента b. Используя однозначность разложения на простые множители в A, мы тотчас убеждаемся, что число r однозначно определено элементом a. Будем называть r *порядком a в p* (и записывать $r = \operatorname{ord}_p a$). Порядок элемента $a = 0$ в p полагаем равным $+\infty$.

Если a, $a' \in K$ и $aa' \neq 0$, то

$$\operatorname{ord}_p(aa') = \operatorname{ord}_p a + \operatorname{ord}_p a'.$$

Это очевидно.

Пусть $f(X) \in K[X]$ — многочлен от одной переменной

$$f(X) = a_0 + a_1 X + \ldots + a_n X^n.$$

Для $f = 0$ полагаем $\operatorname{ord}_p f = +\infty$. Если $f \neq 0$, то считаем по определению

$$\operatorname{ord}_p f = \min \operatorname{ord}_p a_i,$$

где минимум берется по тем i, для которых $a_i \neq 0$.

Будем называть всякий элемент вида up^r, где $r = \operatorname{ord}_p f$ и u — любая единица в A, *p-содержанием* многочлена f. *Содержанием* f будем называть выражение

$$\prod p^{\operatorname{ord}_p f},$$

где произведение берется по всем p, для которых $\operatorname{ord}_p f \neq 0$, а также любое кратное этого выражения на единицу из A. Таким образом, содержание однозначно определено с точностью до умножения на единицу из A. Сокращенно мы обозначаем содержание через cont.

Если $b \in K$, $b \neq 0$, то $\operatorname{cont}(bf) = b \operatorname{cont}(f)$. Это ясно. Следовательно, мы можем записать

$$f(X) = c \cdot f_1(X),$$

где $c = \operatorname{cont}(f)$ и $f_1(X)$ имеет содержание 1. В частности, все коэффициенты многочлена f_1 лежат в A и их н. о. д. равен 1.

Лемма Гаусса. *Пусть A — факториальное кольцо, K — его поле частных, f, $g \in K[X]$ — многочлены от одной переменной. Тогда*

$$\operatorname{cont}(fg) = \operatorname{cont}(f) \operatorname{cont}(g).$$

Доказательство. Записав $f = cf_1$ и $g = dg_1$, где $c = \operatorname{cont}(f)$ и $d = \operatorname{cont}(g)$, мы видим, что достаточно доказать следующее: если f, g имеют содержание 1, то fg также имеет содержание 1, а для этого достаточно доказать, что $\operatorname{ord}_p(fg) = 1$ для всякого простого p. Пусть

$$f(X) = a_n X^n + \ldots + a_0, \quad a_n \neq 0,$$
$$g(X) = b_m X^m + \ldots + b_0, \quad b_m \neq 0,$$

— многочлены с содержанием 1 и p — простой элемент в A. Достаточно доказать, что не все коэффициенты fg делятся на p. Пусть r — наибольшее целое число, такое, что $0 \leqslant r \leqslant n$, а $a_r \neq 0$ и p не делит a_r. Аналогично пусть b_s — самый левый коэффициент в g, $b_s \neq 0$, не делящийся на p. Рассмотрим коэффициент при X^{r+s} в $f(X)g(X)$. Этот коэффициент равен

$$c = a_r b_s + a_{r+1} b_{s-1} + \ldots + a_{r-1} b_{s+1} + \ldots,$$

причем $p \nmid a_r b_s$. Однако p делит все другие ненулевые члены в этой сумме, поскольку в каждом из них содержится либо некоторый коэффициент a_i, стоящий слева от a_r, либо некоторый коэффициент b_j, стоящий слева от b_s. Следовательно, c не делится на p, и наша лемма доказана.

Следствие. *Пусть $f(X) \in A[X]$ имеет в $K[X]$ разложение $f(X) = g(X)h(X)$. Если $c_g = \operatorname{cont}(g)$, $c_h = \operatorname{cont}(h)$ и $g = c_g g_1$, $h = c_h h_1$, то*

$$f(X) = c_g c_h g_1(X) h_1(X)$$

и $c_g c_h$ — элемент из A.

Доказательство. Единственное, что нуждается в доказательстве, — это последнее утверждение, но оно непосредственно вытекает из равенств $\operatorname{cont}(f) = c_g c_h \operatorname{cont}(g_1 h_1) = c_g c_h$.

Теорема 10. *Пусть A — факториальное кольцо. Тогда кольцо многочленов $A[X]$ от одной переменной факториально. Его простыми элементами являются либо простые элементы из A, либо многочлены из $A[X]$, неприводимые в $K[X]$ и имеющие содержание* 1.

Доказательство. Пусть $f \in A[X]$, $f \neq 0$. Используя однозначность разложения на простые множители в $K[X]$ и предыдущее следствие, можно найти разложение

$$f(X) = c \cdot p_1(X) \ldots p_r(X),$$

где $c \in A$ и $p_1, \ldots, p_r$ — многочлены из $A[X]$, неприводимые в $K[X]$. Выделив их содержания, мы можем, не теряя общности, предполагать, что содержание p_i равно 1 для каждого i. Тогда $c = \operatorname{cont}(f)$. Это дает нам существование разложения на простые множители. Очевидно, что каждый многочлен $p_i(X)$ неприводим в $A[X]$. Если мы имеем другое такое разложение, скажем

$$f(X) = d \cdot q_1(X) \ldots q_s(X),$$

то из однозначности разложения на простые множители в $K[X]$ заключаем, что $r = s$ и что после перестановки множителей будет

$$p_i = a_i q_i,$$

где элементы $a_i \in K$. Так как предполагается, что и p_i, и q_i имеют содержание 1, то в действительности a_i лежат в A и являются единицами. Это доказывает теорему.

Следствие. *Пусть A — факториальное кольцо. Тогда кольцо многочленов от n переменных $A[X_1, \ldots, X_n]$ факториально. Его единицами являются в точности единицы из A, а простыми элементами — либо простые элементы из A, либо многочлены, которые неприводимы в $K[X]$ и имеют содержание* 1.

Доказательство. Индукция.

В силу теоремы 10 в тех случаях, когда мы имеем дело с многочленами над факториальным кольцом, содержание которых равно 1, нет необходимости специально указывать, будут ли такие многочлены неприводимыми над A или над полем частных K. Эти два понятия эквивалентны.

Замечание 1. Кольцо многочленов $K[X_1, \ldots, X_n]$ над полем K не является кольцом главных идеалов при $n \geqslant 2$. Например, идеал, порожденный элементами $X_1, \ldots, X_n$, не главный (доказательство тривиально).

Замечание 2. Обычно бывает не слишком просто решить, является ли данный многочлен (скажем, от одной переменной) неприводимым. Например, многочлен X^4+4 приводим над полем рациональных чисел, потому что

$$X^4+4=(X^2-2X+2)(X^2+2X+2).$$

Позже в этой книге мы укажем точный критерий неприводимости многочлена X^n-a. Другие критерии даются в следующем параграфе.

§ 7. Критерии неприводимости

Первый критерий — это критерий Эйзенштейна. *Пусть A — факториальное кольцо, K — его поле частных, $f(X)=a_nX^n+\ldots+a_0$ — многочлен степени $n\geqslant 1$ в $A[X]$ и p — простой элемент в A. Предположим, что*

$$a_n\not\equiv 0 \pmod p,\quad a_i\equiv 0 \pmod p \text{ для всех } i<n,\quad a_0\not\equiv 0 \pmod{p^2}.$$

Тогда $f(X)$ неприводим в $K[X]$.

Доказательство. Выделяя в случае надобности н. о. д. из коэффициентов f, мы можем, не теряя общности, считать, что содержание многочлена f равно 1. Если f разлагается на множители в $K[X]$, то, согласно следствию леммы Гаусса, существует и разложение в $A[X]$, скажем $f(X)=g(X)h(X)$,

$$g(X)=b_dX^d+\ldots+b_0,$$
$$h(X)=c_mX^m+\ldots+c_0,$$

где $d,\ m\geqslant 1$ и $b_dc_m\neq 0$. Пусть σ — канонический гомоморфизм, отображающий A на $A/(p)$. Тогда

$$f^\sigma(X)=g^\sigma(X)h^\sigma(X).$$

Но $f^\sigma(X)=\sigma(a_n)X^n$. Поэтому в силу однозначности разложения на множители в кольце $A/(p)[X]$

$$g^\sigma(X)=\sigma(b_d)X^d \quad\text{и}\quad h^\sigma(X)=\sigma(c_m)X^m,$$

откуда $b_0\equiv 0 \pmod p$ и $c_0\equiv 0 \pmod p$. Следовательно, $a_0=b_0c_0\equiv\equiv 0 \pmod{p^2}$, что противоречит условию.

Пример. Пусть a — отличное от нуля и свободное от квадратов целое число $\neq\pm 1$. Тогда для любого $n\geqslant 1$ многочлен X^n-a неприводим над $\mathbf{Q}$. Многочлены $3X^5-15$, $2X^{10}-21$ неприводимы над $\mathbf{Q}$.

В некоторых случаях многочлен, не удовлетворяющий критерию Эйзенштейна, после простого преобразования начинает ему удовлетворять.

Пример. Пусть p — простое число. Многочлен

$$f(X) = X^{p-1} + \ldots + 1$$

неприводим над $\mathbf{Q}$.

Доказательство. Достаточно доказать, что многочлен $f(X+1)$ неприводим над $\mathbf{Q}$. Заметим, что биномиальные коэффициенты

$$\binom{p}{\nu} = \frac{p!}{\nu!\,(p-\nu)!}, \quad 1 \leqslant \nu \leqslant p-1,$$

делятся на p (потому что числитель делится на p, знаменатель не делится, а сам коэффициент является целым числом). Имеем

$$f(X+1) = \frac{(X+1)^p - 1}{X+1-1} = \frac{X^p + pX^{p-1} + \ldots + pX}{X},$$

откуда видно, что $f(X+1)$ удовлетворяет критерию Эйзенштейна.

Пример. Пусть E — поле и t — элемент некоторого поля, содержащего E, такой, что t трансцендентен над E. Пусть K — поле частных кольца $E[t]$. Для любого целого $n \geqslant 1$ многочлен $X^n - t$ неприводим в $K[X]$. Это вытекает из того факта, что кольцо $A = E[t]$ факториально и t — простой элемент в нем.

Редукционный критерий. *Пусть* A, B — *целостные кольца,*

$$\sigma\colon A \to B$$

— *гомоморфизм и* K, L — *поля частных для* A *и* B *соответственно. Пусть, далее,* $f \in A[X]$ — *такой многочлен, что* $f^\sigma \neq 0$ *и* $\deg f^\sigma = \deg f$. *Если* f^σ *неприводим в* $L[X]$, *то* f *не обладает разложением* $f(X) = g(X)\,h(X)$, *в котором*

$$g,\ h \in A[X] \text{ и } \deg g,\ \deg h \geqslant 1.$$

Доказательство. Предположим, что f имеет такое разложение. Тогда $f^\sigma = g^\sigma h^\sigma$. Так как $\deg g^\sigma \leqslant \deg g$ и $\deg h^\sigma \leqslant \deg h$, то из нашего предположения вытекает, что в этих соотношениях для степеней должно иметь место равенство. Следовательно, в силу неприводимости f^σ в $L[X]$ мы заключаем, что либо g, либо h есть элемент из A, что и требовалось установить.

Предположим в предыдущем критерии, что A — локальное кольцо, т. е. кольцо, имеющее единственный максимальный идеал $\mathfrak{p}$, и что $\mathfrak{p}$ служит ядром σ. Тогда из неприводимости f^σ в $L[X]$ заключаем о неприводимости f в $A[X]$. В действительности любой элемент из A, не лежащий в $\mathfrak{p}$, должен быть единицей в A, так что последнее утверждение критерия можно усилить, добавив, что g или h является единицей в A.

Этот критерий можно применять также в тех случаях, когда A факториально, и в этом случае заключать о неприводимости f в $K[X]$.

Пример. Пусть p — простое число. Ниже будет показано, что многочлен $X^p - X - 1$ неприводим над полем $\mathbf{Z}/p\mathbf{Z}$. Следовательно, $X^p - X - 1$ неприводим над $\mathbf{Q}$. Аналогично многочлен

$$X^5 - 5X^4 - 6X - 1$$

неприводим над $\mathbf{Q}$.

§ 8. Производная и кратные корни

Пусть A — коммутативное кольцо. Определим отображение

$$D\colon\ A[X] \to A[X]$$

кольца многочленов в себя. Если $f(X) = a_n X^n + \ldots + a_0$, где $a_i \in A$, то производная $Df \equiv f'$ определяется соотношением

$$Df(X) = f'(X) = \sum_{\nu=1}^{n} \nu a_\nu X^{\nu-1} = n a_n X^{n-1} + \ldots + a_1.$$

Легко проверяется, что для всяких многочленов f, g из $A[X]$

$$(f+g)' = f' + g', \qquad (fg)' = f'g + fg'$$

и для всякого $a \in A$

$$(af)' = af'.$$

Пусть K — поле, f — многочлен из $K[X]$ и a — его корень в K. Тогда

$$f(X) = (X-a)^m g(X),$$

где $g(X)$ — некоторый многочлен, взаимно простой с $X-a$ (и, следовательно, такой, что $g(a) \neq 0$). Мы называем m *кратностью* a в f и говорим, что a — *кратный корень*, если $m > 1$.

Предложение 1. *Пусть K, f обозначают то же, что и выше. Элемент a поля K является кратным корнем многочлена f тогда и только тогда, когда $f'(a) = 0$.*

Доказательство. Взяв для f указанное выше разложение, получаем

$$f'(X) = (X-a)^m g'(X) + m(X-a)^{m-1} g(X).$$

Если $m > 1$, то, очевидно, $f'(a) = 0$. Обратно, если $m = 1$, то $f'(X) = (X-a)g'(X) + g(X)$, откуда $f'(a) = g(a) \neq 0$. Следовательно, если $f'(a) = 0$, то мы должны иметь $m > 1$, что и требовалось доказать.

Предложение 2. *Пусть* $f \in K[X]$. *Если* K *имеет характеристику* 0 *и* f *имеет степень* $\geqslant 1$, *то* $f' \neq 0$. *Пусть* K *имеет характеристику* $p > 0$ *и* f *имеет степень* $\geqslant 1$. *Тогда* $f' = 0$ *в том и только в том случае, если в выражении для* $f(X)$

$$f(X) = \sum_{\nu=1}^{m} a_\nu X^\nu$$

p *делит каждый индекс* ν, *для которого* $a_\nu \neq 0$.

Доказательство. Если K имеет характеристику 0, то производная одночлена $a_\nu X^\nu$ с $\nu \geqslant 1$ и $a_\nu \neq 0$ отлична от нуля, поскольку она равна $\nu a_\nu X^{\nu-1}$. Если K имеет характеристику $p > 0$, то производная такого одночлена равна 0 тогда и только тогда, когда $p \mid \nu$, что и утверждалось.

Пусть K имеет характеристику $p > 0$, и пусть многочлен f указанного выше вида таков, что $f'(X) = 0$. Тогда мы можем написать

$$f(X) = \sum_{\mu=1}^{d} b_\mu X^{p\mu},$$

где $b_\mu \in K$.

Так как биномиальные коэффициенты $\binom{p}{\nu}$ делятся на p при $1 \leqslant \nu \leqslant p-1$, то для любых элементов a, b из поля K характеристики p мы имеем

$$(a+b)^p = a^p + b^p.$$

Далее, очевидно, $(ab)^p = a^p b^p$, так что отображение

$$x \longmapsto x^p$$

есть гомоморфизм K в себя, имеющий тривиальное ядро и, следовательно, инъективный. Итерируя, мы заключаем, что для всякого целого $r \geqslant 1$ отображение $x \longmapsto x^{p^r}$ есть эндоморфизм поля K, называемый *эндоморфизмом Фробениуса*. По индукции для всяких элементов $c_1, \ldots, c_n$ из K

$$(c_1 + \ldots + c_n)^p = c_1^p + \ldots + c_n^p.$$

Применяя эти замечания к многочленам, мы видим, что для любого элемента $a \in K$ выполняется соотношение

$$(X-a)^{p^r} = X^{p^r} - a^{p^r}.$$

Пусть $c \in K$. Если многочлен

$$X^{p^r} - c$$

имеет корень a в K, то $a^{p^r} = c$ и

$$X^{p^r} - c = (X - a)^{p^r}.$$

Следовательно, наш многочлен имеет ровно один корень кратности p^r. Например, $(X-1)^{p^r} = X^{p^r} - 1$.

§ 9. Симметрические многочлены

Пусть A — коммутативное кольцо и $t_1, \ldots, t_n$ — алгебраически независимые элементы над A. Пусть X — переменная над $A[t_1, \ldots, t_n]$. Образуем многочлен

$$\mathbf{F}(X) = (X - t_1) \ldots (X - t_n) = X^n - s_1 X^{n-1} + \ldots + (-1)^n s_n,$$

где каждый элемент $s_i = s_i(t_1, \ldots, t_n)$ является многочленом от $t_1, \ldots, t_n$. Например,

$$s_1 = t_1 + \ldots + t_n \quad \text{и} \quad s_n = t_1 \ldots t_n.$$

Многочлены $s_1, \ldots, s_n$ называются *элементарными симметрическими многочленами* от $t_1, \ldots, t_n$.

Мы предоставляем читателю в качестве упражнения проверку того, что s_i — однородный многочлен степени i от $t_1, \ldots, t_n$.

Пусть σ — некоторая перестановка целых чисел $(1, \ldots, n)$. Для данного многочлена $f(t) \in A[t] = A[t_1, \ldots, t_n]$ определим f^σ формулой

$$f^\sigma(t_1, \ldots, t_n) = f(t_{\sigma(1)}, \ldots, t_{\sigma(n)})\ ^{1}).$$

Если σ, τ — две перестановки, то $f^{\sigma\tau} = (f^\sigma)^\tau$ и, следовательно, симметрическая группа G на n символах действует на кольце многочленов $A[t]$. Многочлен называется *симметрическим*, если $f^\sigma = f$ для всех $\sigma \in G$. Ясно, что множество симметрических многочленов есть подкольцо в $A[t]$, содержащее постоянные многочлены (т. е. само A), а также элементарные симметрические многочлены $s_1, \ldots, s_n$. Ниже мы увидим, что оно по существу ничего больше и не содержит.

Пусть $X_1, \ldots, X_n$ — переменные. Будем считать *весом* одночлена

$$X_1^{\nu_1} \ldots X_n^{\nu_n}$$

целое число $\nu_1 + 2\nu_2 + \ldots + n\nu_n$. Определим *вес* многочлена $g(X_1, \ldots, X_n)$ как максимум весов одночленов, встречающихся в g.

---

[1]) Имеется лишь внешнее сходство с обозначением f^σ из § 2 и 8. — *Прим. ред.*

Теорема 11. *Пусть* $f(t) \in A[t_1, \ldots, t_n]$ — *симметрический многочлен степени* d. *Тогда существует многочлен* $g(X_1, \ldots, X_n)$ *веса* $\leqslant d$, *такой, что*

$$f(t) = g(s_1, \ldots, s_n).$$

Доказательство. Индукция по n. Если $n = 1$, то теорема очевидна, так как $s_1 = t_1$.

Предположим, что теорема доказана для многочленов от $n-1$ переменной.

Если мы подставим $t_n = 0$ в выражение для $F(X)$, то получим

$$(X - t_1) \ldots (X - t_{n-1}) X = X^n - (s_1)_0 X^{n-1} + \ldots$$
$$\ldots + (-1)^{n-1} (s_{n-1})_0 X,$$

где $(s_i)_0$ — выражение, полученное подстановкой $t_n = 0$ в s_i. Заметим, что $(s_1)_0, \ldots, (s_{n-1})_0$ — это как раз элементарные симметрические многочлены от $t_1, \ldots, t_{n-1}$.

Проведем теперь индукцию по d. Если $d = 0$, то наше утверждение тривиально. Предположим, что $d > 0$ и что наше утверждение доказано для многочленов степени $< d$. Пусть $f(t_1, \ldots, t_n)$ имеет степень $\leqslant d$. Существует многочлен $g_1(X_1, \ldots, X_{n-1})$ веса $\leqslant d$, такой, что

$$f(t_1, \ldots, t_{n-1}, 0) = g_1((s_1)_0, \ldots, (s_{n-1})_0).$$

Отметим, что $g_1(s_1, \ldots, s_{n-1})$ имеет степень $\leqslant d$ по $t_1, \ldots, t_n$. Многочлен

$$f_1(t_1, \ldots, t_n) = f(t_1, \ldots, t_n) - g_1(s_1, \ldots, s_{n-1})$$

имеет степень $\leqslant d$ (по $t_1, \ldots, t_n$) и является симметрическим. Имеем

$$f_1(t_1, \ldots, t_{n-1}, 0) = 0.$$

Следовательно, f_1 делится на t_n, т. е. содержит t_n множителем. Так как f_1 симметрический, то он содержит в качестве множителя $t_1 \ldots t_n$. Следовательно,

$$f_1 = s_n f_2(t_1, \ldots, t_n),$$

где f_2 — некоторый многочлен, который должен быть симметрическим и степень которого $\leqslant d - n < d$. По индукции существует многочлен g_2 от n переменных веса $\leqslant d - n$, для которого

$$f_2(t_1, \ldots, t_n) = g_2(s_1, \ldots, s_n).$$

Получаем

$$f(t) = g_1(s_1, \ldots, s_{n-1}) + s_n g_2(s_1, \ldots, s_n),$$

причем каждый член справа имеет вес $\leqslant d$. Это доказывает нашу теорему.

Покажем теперь, что элементарные симметрические многочлены $s_1, \ldots, s_n$ *алгебраически независимы над* A.

Если они зависимы, то возьмем не равный 0 многочлен $f(X_1, \ldots, X_n) \in A[X]$ наименьшей степени, для которого

$$f(s_1, \ldots, s_n) = 0.$$

Запишем f как многочлен от X_n с коэффициентами в $A[X_1, \ldots, X_{n-1}]$:

$$f(X_1, \ldots, X_n) = f_0(X_1, \ldots, X_{n-1}) + \ldots + f_d(X_1, \ldots, X_{n-1}) X_n^d.$$

Тогда $f_0 \neq 0$. Иначе

$$f(X) = X_n \psi(X),$$

где ψ — некоторый многочлен и, следовательно, $s_n \psi(s_1, \ldots, s_n) = 0$. Отсюда вытекало бы, что $\psi(s_1, \ldots, s_n) = 0$, причем ψ имеет степень, меньшую, чем степень f.

Подставляя s_i вместо X_i в предыдущее тождество, получаем

$$0 = f_0(s_1, \ldots, s_{n-1}) + \ldots + f_d(s_1, \ldots, s_{n-1}) s_n^d.$$

Это — соотношение в $A[t_1, \ldots, t_n]$; если мы подставим 0 вместо t_n в это соотношение, то все члены, кроме первого, обратятся в 0, что дает

$$0 = f_0((s_1)_0, \ldots, (s_{n-1})_0)$$

(мы используем те же обозначения, что и в доказательстве теоремы 1). Мы получили нетривиальное соотношение между элементарными симметрическими многочленами от $t_1, \ldots, t_{n-1}$ — противоречие.

Пример. Рассмотрим произведение

$$\delta(t) = \prod_{i<j} (t_i - t_j).$$

Мы тотчас видим, что какова бы ни была перестановка σ чисел $(1, \ldots, n)$,

$$\delta^\sigma(t) = \pm \delta(t).$$

Следовательно, $\delta(t)^2$ — симметрический многочлен; мы называем его *дискриминантом*

$$D(s_1, \ldots, s_n) = \prod_{i<j} (t_i - t_j)^2.$$

Таким образом, мы рассматриваем дискриминант как многочлен от элементарных симметрических функций.

§ 10. Результант

В этом параграфе мы предполагаем, что читатель знаком с определителями. Теория определителей будет изложена позднее.

Пусть A — коммутативное кольцо, и пусть $v_0, \ldots, v_n, w_0, \ldots, w_m$ алгебраически независимы над A. Образуем два многочлена

$$f_v(X) = v_0X^n + \ldots + v_n,$$
$$g_w(X) = w_0X^m + \ldots + w_m.$$

Назовем *результантом* наборов (v, w), или многочленов f_v, g_w, определитель

$$\begin{vmatrix} v_0 & v_1 & \ldots & v_n & & & \\ & v_0 & v_1 & \ldots & v_n & & \\ & & \ddots & \ddots & & \ddots & \\ & & & v_0 & v_1 & \ldots & v_n \\ w_0 & w_1 & \ldots & w_m & & & \\ & w_0 & w_1 & \ldots & w_m & & \\ & & \ddots & \ddots & & \ddots & \\ & & & w_0 & w_1 & \ldots & w_m \end{vmatrix} \begin{matrix} \\ \\ \\ m \\ \\ \\ \\ n \end{matrix}$$
$$\underbrace{\qquad\qquad\qquad\qquad}_{m+n}$$

Пустые места предполагаются заполненными нулями.

Если подставить вместо (v) и (w) в коэффициенты многочленов f_v и g_w соответственно элементы $(a) = (a_0, \ldots, a_n)$ и $(b) = (b_0, \ldots, b_m)$ из A, то получатся многочлены f_a и g_b с коэффициентами в A, и *мы берем в качестве их результанта определитель, полученный подстановкой* (a) *вместо* (v) *и* (b) *вместо* (w) *в написанный выше определитель*. Результант многочленов f_v, g_w будем обозначать символом

$$R(f_v, g_w) \quad \text{или} \quad R(v, w).$$

Результант $R(f_a, g_b)$ получается подстановкой (a) и (b) вместо соответственно (v) и (w).

Заметим, что $R(v, w)$ — многочлен с целочисленными коэффициентами, т. е. мы можем взять $A = \mathbf{Z}$. Если z — переменная, то

$$R(zv, w) = z^mR(v, w) \quad \text{и} \quad R(v, zw) = z^nR(v, w),$$

что непосредственно видно, если вынести z из первых m строк (соответственно последних n строк) определителя. Таким образом, R однороден степени m по первому набору переменных и однороден степени n по второму набору переменных. Кроме того, будучи пред-

ставлен в виде суммы одночленов, результант $R(v, w)$ содержит одночлен

$$v_0^m w_m^n$$

с коэффициентом 1.

Если подставить в результант 0 вместо v_0 и w_0, то получится 0, поскольку обратится в 0 первый столбец определителя.

Будем теперь действовать над кольцом целых чисел $\mathbf{Z}$. Рассмотрим линейные уравнения

$$\begin{aligned}
X^{m-1}f_v(X) &= v_0X^{n+m-1} + v_1X^{n+m-2} + \ldots + v_nX^{m-1},\\
X^{m-2}f_v(X) &= \qquad v_0X^{n+m-2} + \ldots + v_nX^{m-2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
f_v(X) &= \qquad\qquad v_0X^n + \ldots + v_n,\\
X^{n-1}g_w(X) &= w_0X^{n+m-1} + w_1X^{n+m-2} + \ldots + w_mX^{n-1},\\
X^{n-2}g_w(X) &= \qquad w_0X^{n+m-2} + \ldots + w_mX^{n-2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
g_w(X) &= \qquad\qquad w_0X^m + \ldots + w_m.
\end{aligned}$$

Пусть C — столбец, составленный из левых частей, и пусть

$$C_0, \ldots, C_{m+n-1}$$

— столбцы из коэффициентов. Наши уравнения могут быть записаны так:

$$C = X^{n+m-1}C_0 + \ldots + 1 \cdot C_{m+n}.$$

По правилу Крамера, примененному к последней неизвестной, а именно к 1, получаем

$$R(v, w) = \det(C_0, \ldots, C_{m+n-1}) = \det(C_0, \ldots, C_{m+n-2}, C).$$

Отсюда мы видим, что существуют такие многочлены $\varphi_{v,w}$ и $\psi_{v,w}$ в $\mathbf{Z}[v, w][X]$, для которых

$$\varphi_{v,w}f_v + \psi_{v,w}g_w = R(v, w).$$

Отметим, что $R(v, w) \in \mathbf{Z}[v, w]$, но многочлены в левой части содержат переменную X.

Пусть λ: $\mathbf{Z}[v, w] \to A$ — гомоморфизм в коммутативное кольцо A. Положим $\lambda(v) = (a)$, $\lambda(w) = (b)$; тогда

$$\varphi_{a,b}f_a + \psi_{a,b}g_b = R(a, b) = R(f_a, g_b).$$

Таким образом, из общего соотношения для результанта над $\mathbf{Z}$ мы получаем аналогичное соотношение для всякой пары многочленов над любым коммутативным кольцом A.

Предложение 3. *Пусть K — подполе поля L, и пусть f_a, g_b — многочлены в $K[X]$, имеющие общий корень ξ в L. Тогда $R(a, b) = 0$.*

Доказательство. Если $f_a(\xi) = g_b(\xi) = 0$, то, подставляя ξ вместо X в выражение, полученное для $R(a, b)$, находим, что $R(a, b) = 0$.

Исследуем теперь зависимость между результантом и корнями наших многочленов f_v, g_w. Нам потребуется

Лемма. *Пусть $h(X_1, \ldots, X_n)$ — многочлен от n переменных над кольцом целых чисел $\mathbf{Z}$, обращающийся в 0, если подставить X_1 вместо X_2 и оставить все другие X_i неизменными ($i \neq 2$). Тогда $h(X_1, \ldots, X_n)$ делится на $X_1 - X_2$ в $\mathbf{Z}[X_1, \ldots, X_n]$.*

Доказательство. Упражнение для читателя.

Пусть $v_0, t_1, \ldots, t_n, w_0, u_1, \ldots, u_m$ алгебраически независимы над $\mathbf{Z}$. Образуем многочлены

$$f_v = v_0(X - t_1) \ldots (X - t_n) = v_0X^n + \ldots + v_n,$$
$$g_w = w_0(X - u_1) \ldots (X - u_m) = w_0X^m + \ldots + w_m.$$

Таким образом, мы полагаем

$$v_i = (-1)^i v_0 s_i(t) \quad \text{и} \quad w_j = (-1)^j w_0 s_j(u).$$

Предоставляем читателю легкую проверку того, что

$$v_0, v_1, \ldots, v_n, w_0, w_1, \ldots, w_m$$

алгебраически независимы над $\mathbf{Z}$.

Предложение 4. *В предыдущих обозначениях имеем*

$$R(f_v, g_w) = v_0^m w_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (t_i - u_j).$$

Доказательство. Обозначим через S выражение, стоящее в правой части равенства из формулировки предложения.

Так как $R(v, w)$ однороден степени m по своим первым переменным и однороден степени n по вторым переменным, то

$$R = v_0^m w_0^n h(t, u),$$

где $h(t, u) \in \mathbf{Z}[t, u]$. В силу предложения 3 результант обращается в нуль при подстановке t_i вместо u_j ($i = 1, \ldots, n$ и $j = 1, \ldots, m$), откуда по лемме вытекает, что R, рассматриваемый как элемент из $\mathbf{Z}[v_0, t, w_0, u]$, делится на $t_i - u_j$ для каждой пары (i, j). Следовательно, R делится в $\mathbf{Z}[v_0, t, w_0, u]$ на S, поскольку разность $t_i - u_j$ является, очевидно, простым элементом в этом кольце, и различные пары (i, j) приводят к различным простым элементам.

Из равенства

$$S = v_0^m w_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (t_i - u_j) \tag{1}$$

и из того факта, что

$$\prod_{i=1}^{n} g(t_i) = w_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (t_i - u_j),$$

мы получаем

$$S = v_0^m \cdot \prod_{i=1}^{n} g(t_i). \tag{2}$$

Аналогично

$$S = (-1)^{nm} w_0^n \prod_{j=1}^{m} f(u_j). \tag{3}$$

Из (2) мы видим, что S однородно степени n по (w), а из (3) — что S однородно степени m по (v). Так как R обладает точно теми же свойствами однородности и делится на S, то $R = cS$ для некоторого целого c. Так как и R, и S содержат одночлен $v_0^m w_m^n$, встречающийся в них с коэффициентом 1, то $c = 1$, и наше предложение доказано.

Отметим, что три выражения, найденные выше для S, дают нам разложение на множители результанта R. Мы получаем также обратное утверждение к предложению 3.

Следствие. *Пусть f_a, g_b — многочлены с коэффициентами в некотором поле K, разлагающиеся на множители степени 1 в $K[X]$ и такие, что хотя бы один из старших коэффициентов a_0, $b_0 \neq 0$. Тогда $R(f_a, g_b) = 0$ в том и только в том случае, если f_a и g_b имеют общий корень.*

Доказательство. Пусть результант равен 0, и пусть для определенности $a_0 \neq 0$. Если

$$f_a = a_0 (X - \alpha_1) \ldots (X - \alpha_n),$$

— разложение f_a на множители, то имеет место гомоморфизм

$$\mathbf{Z}[v_0, t, w] \to K,$$

при котором $v_0 \mapsto a_0$, $t_i \mapsto \alpha_i$ и $w_j \mapsto b_j$ для всех i, j. Тогда

$$0 = R(f_a, g_b) = a_0^m \prod_{i=1}^{n} g_b(\alpha_i),$$

откуда следует, что хотя бы один из α_i является корнем многочлена g_b. Обратное уже было доказано.

Выведем еще одно соотношение для результанта в специальном случае. Пусть, как и выше,

$$f_v(X) = v_0X^n + \ldots + v_n = v_0(X - t_1)\ldots(X - t_n).$$

В силу (2) для производной f'_v многочлена f_v

$$R(f_v, f'_v) = v_0^{n-1}\prod_i f'(t_i). \tag{4}$$

Используя правило дифференцирования произведения, находим

$$f'_v(X) = \sum_i v_0(X - t_1)\ldots(\widehat{X - t_i})\ldots(X - t_n),$$

$$f'_v(t_i) = v_0(t_i - t_1)\ldots(\widehat{t_i - t_i})\ldots(t_i - t_n),$$

где крышка над членом указывает, что этот член должен быть опущен.

Мы называем дискриминантом многочлена f_v выражение

$$D(f_v) = D(v) = v_0^{2n-2}\prod_{i<j}(t_i - t_j)^2.$$

Предложение 5. Пусть f_v, как и выше, имеет алгебраически независимые коэффициенты над $\mathbf{Z}$. Тогда

$$R(f_v, f'_v) = v_0^{2n-1}\prod_{i\neq j}(t_i - t_j) = (-1)^{\binom{n}{2}}v_0D(f_v). \tag{5}$$

Доказательство. Подставим выражение, полученное для $f'_v(t_i)$, в произведение (4). Утверждение следует немедленно.

Если мы подставим 1 вместо v_0, то найдем, что дискриминант, как мы его определили в предыдущем параграфе, совпадает с определенным здесь. В частности, получаем явную формулу для дискриминанта. Формулы в случае многочленов степени 2 и 3 приводятся в упражнениях.

УПРАЖНЕНИЯ

1. (а) Сформулировать и доказать аналог теоремы 8 для рациональных чисел.

(б) Сформулировать и доказать аналог теоремы 9 для положительных целых чисел.

2. Пусть f — многочлен от одной переменной над полем k, и пусть X, Y — две переменные. Показать, что в $k[X, Y]$ имеет место разложение в ряд Тейлора

$$f(X + Y) = f(X) + \sum_{i=1}^{n}\varphi_i(X)Y^i,$$

где $\varphi_i(X)$ — некоторые многочлены от X с коэффициентами в k. Если k имеет характеристику 0, то

$$\varphi_i(X) = \frac{D^i f(X)}{i!}.$$

3. Обобщить предыдущее упражнение на многочлены от нескольких переменных (ввести частные производные и показать, что для многочленов от нескольких переменных существует конечное разложение Тейлора).

4. (а) Показать, что многочлены $X^4 + 1$ и $X^6 + X^3 + 1$ неприводимы над полем рациональных чисел.

(б) Показать, что многочлен степени 3 над полем либо неприводим, либо имеет корень в этом поле. Является ли многочлен $X^3 - 5X^2 + 1$ неприводимым над полем рациональных чисел?

(в) Показать, что многочлен от двух переменных $X^2 + Y^2 - 1$ неприводим над полем рациональных чисел. Неприводим ли он над полем комплексных чисел?

5. Пусть $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ — многочлен с целыми коэффициентами, $a_0 \neq 0$. Показать, что если f имеет корень в поле рациональных чисел, то этот корень должен быть целым рациональным числом, делящим a_0. Обобщить это утверждение на любое факториальное кольцо и его поле частных.

6. (а) Пусть k — конечное поле из q элементов. Пусть $f(X_1, \ldots, X_n)$ — многочлен в $k[X]$ степени d, такой, что $f(0, \ldots, 0) = 0$. Элемент $(a_1, \ldots, a_n) \in k^{(n)}$, для которого $f(a) = 0$, называется нулем f. Показать, что если $n > d$, то f имеет по крайней мере еще один нуль в $k^{(n)}$. [*Указание*: предположить противное и сравнить степени редуцированных многочленов

$$1 - f(X)^{q-1}$$

и $\left(1 - X_1^{q-1}\right) \ldots \left(1 - X_n^{q-1}\right)$. Рассуждение принадлежит Шевалле.]

(б) Усилить предыдущий результат, доказав, что число N нулей многочлена f в $k^{(n)}$ сравнимо с нулем по mod q. Рассуждать следующим образом. Пусть i — целое число $\geqslant 0$. Показать, что

$$\sum_{x \in k} x^i = \begin{cases} q - 1 = -1, & \text{если } q - 1 \text{ делит } i, \\ 0 & \text{в противном случае.} \end{cases}$$

Обозначим предыдущую функцию от i через $\psi(i)$. Показать, что

$$N \equiv \sum_{x \in k^{(n)}} (1 - f(x)^{q-1})$$

и что для каждого набора $(i_1, \ldots, i_n)$ целых чисел $\geqslant 0$ будет

$$\sum_{x \in k^{(n)}} x_1^{i_1} \cdots x_n^{i_n} = \psi(i_1) \ldots \psi(i_n).$$

Показать, что оба члена в сумме для N дают 0 mod p. (Приведенное рассуждение принадлежит Варнингу.)

(в) Распространить теорему Шевалле на r многочленов $f_1, \ldots, f_r$ степеней $d_1, \ldots, d_r$ соответственно от n переменных. Показать, что если эти

многочлены не имеют постоянных членов и $n > \sum d_i$, то у них есть нетривиальный общий нуль.

(г) Показать, что произвольная функция $f\colon k^{(n)} \to k$ может быть представлена многочленом. (Как и прежде, k — конечное поле.)

7. Пусть A — коммутативное целостное кольцо и X — переменная над A. Пусть $a, b \in A$, причем a — единица в A. Показать, что отображение $X \mapsto aX + b$ продолжается и притом единственным образом до автоморфизма кольца $A[X]$, индуцирующего тождественное отображение на A. Каков обратный автоморфизм?

8. Показать, что любой автоморфизм кольца $A[X]$ имеет вид, указанный в упражнении 7.

9. Пусть A — коммутативное целостное кольцо, K — его поле частных и $K(X)$ — поле частных кольца $A[X]$ (или, что то же самое, кольца $K[X]$). Показать, что всякий автоморфизм поля $K(X)$, индуцирующий тождественное отображение на K, имеет вид

$$X \mapsto \frac{aX + b}{cX + d},$$

где $a, b, c, d \in K$ таковы, что $(aX + b)/(cX + d)$ не лежит в K, или, что эквивалентно, $ad - bc \neq 0$.

10. Показать, что дискриминант многочлена $aX^2 + bX + c$ равен $b^2 - 4ac$.

11. Показать, что дискриминант многочлена $f(X) = a_0X^3 + a_1X^2 + a_2X + a_3$ равен

$$a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2 + 18a_0a_1a_2a_3.$$

В частности, дискриминантом многочлена $f(X) = X^3 + bX + c$ будет $-4b^3 - 27c^2$.

12. Показать, что дискриминант многочлена обращается в нуль тогда и только тогда, когда многочлен имеет кратный корень. (Вы можете предполагать, что многочлен разлагается на множители степени 1 в некотором поле.)

13. Пусть w — некоторое комплексное число. Показать, что существует постоянная $c = c(w)$, для которой справедливо следующее. Пусть F, G — ненулевые многочлены от одной переменной с комплексными коэффициентами степеней d и d' соответственно и R — их результант. Тогда

$$|R| \leqslant c^{d+d'}\left[\frac{|F(w)|}{|F|} + \frac{|G(w)|}{|G|}\right]|F|^{d'}|G|^{d}(d+d')^{d+d'}.$$

(Мы обозначаем через $|F|$ максимум абсолютных значений коэффициентов многочлена F.)

14. Показать, что можно определить простейшие дроби для положительных рациональных чисел, т. е получить разложение, аналогичное разложению из теоремы 8. Показать, что группа $\mathbf{Q}/\mathbf{Z}$ изоморфна прямой сумме аддитивных групп $\mathbf{Z}[1/p]/\mathbf{Z}$, взятой по всем простым p. Обобщить на произвольное кольцо главных идеалов A. Если K — поле частных кольца A, то что представляет собой K/A?

15. Следующее упражнение несколько труднее предыдущих. Пусть m/n — рациональное число, представленное в виде отношения взаимно простых

целых чисел m, n. Назовем его *высотой* $H(m/n)$ максимум из $|m|$, $|n|$. Пусть

$$\varphi(X) = \frac{f(X)}{g(X)}$$

— элемент из $\mathbf{Q}(X)$, представленный в виде отношения двух взаимно простых многочленов f, g. Назовем *степенью* элемента φ максимум из $\deg f$, $\deg g$. Если число $a \in \mathbf{Q}$ таково, что $g(a) \neq 0$, то мы можем образовать $\varphi(a) = f(a)/g(a)$; в этом случае мы говорим, что функция φ определена в a. Пусть φ имеет степень d. Показать, что существуют две константы $c_1, c_2 > 0$, такие, что для всех рациональных чисел a, в которых φ определена, имеют место неравенства

$$c_1 H(a)^d \leqslant H(\varphi(a)) \leqslant c_2 H(a)^d.$$

[*Указание*: одно из неравенств тривиально. Для получения другого показать, что функция $H(x)^d/H(\varphi(x))$ ограничена.]

Глава VI

Нётеровы кольца и модули

§ 1. Основные критерии

Пусть A — кольцо и M — модуль (т. е. левый A-модуль). Мы будем говорить, что модуль M *нётеров*, если он удовлетворяет одному из следующих трех условий:

(i) Всякий подмодуль в M конечно порожден.

(ii) Всякая возрастающая последовательность подмодулей в M

$$M_1 \subset M_2 \subset M_3 \subset \dots,$$

такая, что $M_i \neq M_{i+1}$, конечна.

(iii) Всякое непустое множество S подмодулей в M содержит максимальный элемент (т. е. такой подмодуль M_0, что для любого элемента N из S, содержащего M_0, имеем $N = M_0$).

Докажем теперь, что три предыдущих условия эквивалентны.

(i) $\Rightarrow$ (ii). Предположим, что имеется возрастающая последовательность подмодулей в M. Пусть N — объединение всех M_i ($i = 1, 2, \dots$). Тогда подмодуль N конечно порожден, скажем, элементами $x_1, \dots, x_r$ и каждая образующая лежит в некотором M_i. Следовательно, существует такой индекс j, что

$$x_1, \dots, x_r \in M_j.$$

Тогда

$$\langle x_1, \dots, x_r \rangle \subset M_j \subset N = \langle x_1, \dots, x_r \rangle,$$

откуда вытекает равенство $M_j = N$, и наше утверждение доказано.

(ii) $\Rightarrow$ (iii). Пусть N_0 — некоторый элемент из S. Если N_0 не максимален, то он содержится собственным образом в некотором подмодуле N_1. Если N_1 не максимален, то он содержится собственным образом в некотором подмодуле N_2. По индукции, если мы нашли подмодуль N_i, который не максимален, то он содержится в качестве собственного подмодуля в некотором подмодуле N_{i+1}. Таким образом, мы смогли бы построить бесконечную цепочку, что невозможно.

(iii) $\Rightarrow$ (i). Пусть N — подмодуль в M, $a_0 \in N$. Если $N \neq \langle a_0 \rangle$, то существует элемент $a_1 \in N$, не лежащий в $\langle a_0 \rangle$. Продолжая по ин-

дукции, мы можем найти возрастающую последовательность подмодулей в N, а именно

$$\langle a_0\rangle\subset\langle a_0, a_1\rangle\subset\langle a_0, a_1, a_2\rangle\subset\dots,$$

включение в которой всякий раз собственное. Множество этих подмодулей содержит максимальный элемент, скажем подмодуль $\langle a_0, a_1, \dots, a_r\rangle$, и этот конечно порожденный подмодуль, очевидно, должен быть равен N, что и требовалось показать.

Предложение 1. *Пусть M—нётеров A-модуль. Тогда всякий подмодуль и всякий фактормодуль модуля M нётеровы.*

Доказательство. Наше утверждение очевидно для подмодулей (скажем, в силу первого условия). Что касается фактормодулей, то пусть N — некоторый подмодуль и f: $M\to M/N$ — канонический гомоморфизм. Пусть $\overline{M}_1\subset\overline{M}_2\subset\dots$ — возрастающая цепочка подмодулей в M/N, и пусть $M_i=f^{-1}(\overline{M}_i)$. Тогда $M_1\subset M_2\subset\dots$ — возрастающая цепочка подмодулей в M, которая должна иметь максимальный элемент, скажем M_r, так что $M_i=M_r$ для $i\geqslant r$. Но $f(M_i)=\overline{M}_i$, что и доказывает наше утверждение.

Предложение 2. *Пусть M — модуль, N — его подмодуль. Предположим, что N и M/N нётеровы. Тогда M нётеров.*

Доказательство. С каждым подмодулем L в M мы можем связать пару модулей:

$$L\mapsto(L\cap N, (L+N)/N).$$

Мы утверждаем: если $E\subset F$—такие два подмодуля в M, что связанные с ними пары совпадают, то $E=F$. Чтобы убедиться в этом, возьмем $x\in F$. В силу предположенного равенства $(E+N)/N=(F+N)/N$ существуют элементы u, $v\in N$ и $y\in E$, такие, что $y+u=x+v$. Тогда

$$x-y=u-v\in F\cap N=E\cap N.$$

Так как $x=y+u-v$, то получаем отсюда, что $x\in E$, и наше утверждение доказано. Если мы имеем возрастающую последовательность

$$E_1\subset E_2\subset\dots,$$

то связанные с ними пары образуют возрастающую последовательность подмодулей в N и M/N соответственно и эти последовательности должны стабилизироваться. Следовательно, наша последовательность $E_1\subset E_2\subset\dots$ также стабилизируется в силу предыдущего утверждения.

Предложения 1 и 2 могут быть суммированы в следующем утверждении: в точной последовательности $0\to M'\to M\to M''\to 0$ модуль M нётеров тогда и только тогда, когда M' и M'' нётеровы.

Следствие. *Пусть M — модуль и N, N' — его подмодули. Если $M = N + N'$ и если оба модуля N, N' нётеровы, то M нётеров. Конечная прямая сумма нётеровых модулей нётерова.*

Доказательство. Заметим сначала, что прямое произведение $N \times N'$ нётерово, так как оно содержит N в качестве подмодуля, фактормодуль по которому изоморфен N', и применимо предложение 2. Имеет место сюръективный гомоморфизм

$$N \times N' \to M,$$

при котором пара (x, x'), где $x \in N$ и $x' \in N'$, переводится в $x + x'$. В силу предложения 1 отсюда вытекает, что M нётеров. Для конечных произведений (или сумм) предложение доказывается по индукции.

Кольцо называется *нётеровым*, если оно нётерово как левый модуль над собой. Это означает, что всякий левый идеал конечно порожден.

Предложение 3. *Пусть A — нётерово кольцо и M — конечно порожденный A-модуль. Тогда M нётеров.*

Доказательство. *Пусть* $x_1, \ldots, x_n$ — образующие M. Тогда существует гомоморфизм

$$f\colon A \times A \times \ldots \times A \to M$$

произведения кольца A на себя n раз, при котором

$$f(a_1, \ldots, a_n) = a_1 x_1 + \ldots + a_n x_n.$$

Этот гомоморфизм сюръективен. В силу следствия из предыдущего предложения произведение нётерово, и, следовательно, в силу предложения 1 модуль M нётеров.

Предложение 4. *Пусть A — нётерово кольцо и $\varphi\colon A \to B$ — сюръективный гомоморфизм колец. Тогда B нётерово.*

Доказательство. Пусть $\mathfrak{b}_1 \subset \ldots \subset \mathfrak{b}_n \subset \ldots$ — возрастающая цепочка левых идеалов в B, и пусть $\mathfrak{a}_i = \varphi^{-1}(\mathfrak{b}_i)$. Тогда $\mathfrak{a}_i$ образуют возрастающую цепочку левых идеалов в A, которая должна стабилизироваться, скажем, на $\mathfrak{a}_r$. Так как $\varphi(\mathfrak{a}_i) = \mathfrak{b}_i$ для всех i, то наше предложение доказано.

Предложение 5. *Пусть A — коммутативное нётерово кольцо, S' — мультипликативное подмножество в A. Тогда кольцо $S^{-1}A$ нётерово.*

Доказательство. Мы предоставляем доказательство читателю в качестве упражнения.

§ 2. Теорема Гильберта

Теорема 1. *Пусть A — коммутативное нётерово кольцо. Тогда кольцо многочленов $A[X]$ также нётерово.*

Доказательство. Пусть $\mathfrak{A}$ — идеал в $A[X]$. Обозначим через $\mathfrak{a}_i$ множество элементов $a \in A$, служащих старшими коэффициентами в многочленах

$$a_0 + a_1 X + \ldots + aX^i,$$

лежащих в $\mathfrak{A}$. Тогда ясно, что $\mathfrak{a}_i$ есть идеал. (Если a, b лежат в $\mathfrak{a}_i$, то $a \pm b$ лежит в $\mathfrak{a}_i$; чтобы это увидеть, достаточно взять сумму и разность соответствующих многочленов. Если $x \in A$, то $xa \in \mathfrak{a}_i$ — это сразу видно, если умножить соответствующий многочлен на x.) Кроме того, имеем

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots,$$

другими словами, наша последовательность идеалов $\{\mathfrak{a}_i\}$ возрастающая. Действительно, умножив упомянутый выше многочлен на X, мы найдем, что $a \in \mathfrak{a}_{i+1}$.

Последовательность идеалов $\{\mathfrak{a}_i\}$ стабилизируется, скажем, на $\mathfrak{a}_r$:

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_r = \mathfrak{a}_{r+1} = \ldots.$$

Пусть

$$a_{01}, \ldots, a_{0n_0} \text{ — образующие для } \mathfrak{a}_0,$$

$$a_{r1}, \ldots, a_{rn_r} \text{ — образующие для } \mathfrak{a}_r.$$

Для каждого $i = 0, \ldots, r$ и $j = 1, \ldots, n_i$ пусть f_{ij} — многочлен из $\mathfrak{A}$ степени i со старшим коэффициентом a_{ij}. Мы утверждаем, что многочлены f_{ij} составляют множество образующих для $\mathfrak{A}$.

Пусть f — многочлен степени d из $\mathfrak{A}$. Индукцией по d мы докажем, что f лежит в идеале, порожденном f_{ij}. Пусть $d \geqslant 0$. Если $d > r$, то заметим, что старшие коэффициенты многочленов

$$X^{d-r} f_{r1}, \ldots, X^{d-r} f_{rn_r}$$

порождают $\mathfrak{a}_d$. Следовательно, существуют элементы $c_1, \ldots, c_{n_r} \in A$, такие, что многочлен

$$f - c_1 X^{d-r} f_{r1} - \ldots - c_{n_r} X^{d-r} f_{rn_r}$$

имеет степень $< d$, причем этот многочлен также лежит в $\mathfrak{a}$. Если $d \leqslant r$, то мы также можем получить многочлен степени $< d$, лежащий в $\mathfrak{a}$, вычтя некоторую линейную комбинацию

$$f - c_1 f_{d1} - \ldots - c_{n_d} f_{dn_d}.$$

Заметим, что многочлен, который мы вычли из f, лежит в идеале, порожденном f_{ij}. По индукции мы можем найти такой многочлен g

в идеале, порожденном f_{ij}, что $f - g = 0$, доказав тем самым нашу теорему.

Следствие. *Пусть A — нётерово коммутативное кольцо, и пусть $B = A[x_1, \ldots, x_m]$ — конечно порожденное коммутативное кольцо, содержащее A в качестве подкольца. Тогда B нётерово.*

Доказательство. Представив B как факторкольцо кольца многочленов, применим теорему 1 и предложение 4.

§ 3. Степенные ряды

Пусть X — некоторый символ, и пусть G — моноид функций на множестве $\{X\}$ со значениями в множестве натуральных чисел. Для всякого $\nu \in \mathbf{N}$ обозначим через X^ν функцию, значение которой в X равно ν. Тогда G — мультипликативный моноид, с которым мы уже сталкивались при рассмотрении многочленов. Его элементами будут $X^0, X^1, X^2, \ldots, X^\nu, \ldots$.

Пусть A — коммутативное кольцо, и пусть $A[[X]]$ — множество функций из G в A, причем на эти функции не накладывается никаких ограничений. Тогда всякий элемент из $A[[X]]$ можно рассматривать как элемент, сопоставляющий каждому одночлену X^ν некоторый коэффициент $a_\nu \in A$. Обозначим этот элемент через

$$\sum_{\nu=0}^{\infty} a_\nu X^\nu.$$

Символ суммирования здесь, разумеется, только символ, но мы будем тем не менее записывать предыдущее выражение также в виде

$$a_0 X^0 + a_1 X^1 + \ldots$$

и называть его *формальным степенным рядом* от одной переменной с коэффициентами в A. Мы называем a_0, a_1, ... коэффициентами этого ряда.

Если даны два элемента из $A[[X]]$, скажем

$$\sum_{\nu=0}^{\infty} a_\nu X^\nu \quad \text{и} \quad \sum_{\mu=0}^{\infty} b_\mu X^\mu,$$

то мы определяем их произведение

$$\sum_{i=0}^{\infty} c_i X^i,$$

полагая

$$c_i = \sum_{\nu+\mu=i} a_\nu b_\mu.$$

Их суммой, как и в случае многочленов, будет по определению

$$\sum_{\nu=0}^{\infty}(a_\nu+b_\nu)X^\nu.$$

Тогда видно, что степенные ряды образуют кольцо, причем доказательство этого факта то же самое, что и для многочленов.

Можно также построить кольцо степенных рядов от нескольких переменных $A[[X_1, \ldots, X_n]]$, в котором каждый элемент может быть представлен в виде

$$\sum_{(\nu)} a_{(\nu)}X_1^{\nu_1}\ldots X_n^{\nu_n}=\sum a_{(\nu)}M_{(\nu)}(X_1, \ldots, X_n).$$

Коэффициенты $a_{(\nu)}$, выбираемые без всяких ограничений, находятся во взаимно однозначном соответствии с наборами из n целых чисел $(\nu_1, \ldots, \nu_n)$, в которых $\nu_i \geqslant 0$ для всех i. Легко показать, что существует изоморфизм между $A[[X_1, \ldots, X_n]]$ и кольцом повторных степенных рядов $A[[X_1]]\ldots[[X_n]]$. Мы предоставляем это в качестве упражнения читателю.

Теорема 2. *Если A нётерово*, то $A[[X]]$ *также нётерово.*

Доказательство. Наше рассуждение будет представлять собой видоизменение рассуждения, использованного при доказательстве теоремы Гильберта для многочленов. Мы будем рассматривать элементы наименьшей степени вместо элементов наибольшей степени.

Пусть $\mathfrak{A}$ — идеал в $A[[X]]$. Обозначим через $\mathfrak{a}_i$ множество элементов $a \in A$, таких, что a служит коэффициентом при X^i в некотором степенном ряде

$$aX^i + \text{члены более высокой степени,}$$

лежащем в $\mathfrak{A}$. Тогда $\mathfrak{a}_i$ — идеал в A и $\mathfrak{a}_i \subset \mathfrak{a}_{i+1}$ (доказательство этого утверждения такое же, как для многочленов). Возрастающая цепочка идеалов стабилизируется:

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_r = \mathfrak{a}_{r+1} = \ldots .$$

Как и прежде, пусть a_{ij} $(i=0, \ldots, r$ и $j=1, \ldots, n_i)$ — образующие для идеалов $\mathfrak{a}_i$, и пусть f_{ij} — степенные ряды, имеющие a_{ij} в качестве начальных коэффициентов. Если дан ряд $f \in \mathfrak{A}$, начинающийся с члена степени d, скажем $d \leqslant r$, то мы можем найти элементы

$$c_1, \ldots, c_{n_d} \in A,$$

такие, что ряд

$$f - c_1 f_{d1} - \ldots - c_{n_d} f_{dn_d}$$

начинается с члена степени $\geqslant d+1$. Действуя по индукции, мы можем предполагать, что $d > r$. Тогда, чтобы получить ряд, начинающийся с члена степени $\geqslant d+1$, используем линейную комбинацию

$$f - c_1^{(d)} X^{d-r} f_{r1} - \ldots - c_{n_r}^{(d)} X^{d-r} f_{rn_r}.$$

Таким образом, если ряд начинается с члена степени $d > r$, то он может быть представлен как линейная комбинация степенных рядов

$$f_{r1}, \ldots, f_{rn_r}$$

с коэффициентами

$$g_1(X) = \sum_{\nu=d}^{\infty} c_1^{(\nu)} X^{\nu-r}, \ldots, g_{n_r}(X) = \sum_{\nu=d}^{\infty} c_{n_r}^{(\nu)} X^{\nu-r},$$

и мы видим, что f_{ij} порождают наш идеал $\mathfrak{A}$, что и требовалось показать.

Следствие. *Если A — поле или нётерово коммутативное кольцо, то кольцо $A[[X_1, \ldots, X_n]]$ нётерово.*

§ 4. Ассоциированные простые идеалы

В этом параграфе мы предполагаем, что A — коммутативное кольцо. Модули и гомоморфизмы, если не оговорено противное, будут A-модулями и A-гомоморфизмами.

Предложение 6. *Пусть S — мультипликативное подмножество в A, причем S не содержит 0. Тогда в A существует идеал, максимальный в множестве идеалов, не пересекающихся с S, и всякий такой идеал является простым.*

Доказательство. Существование такого идеала $\mathfrak{p}$ следует из леммы Цорна (множество идеалов, не пересекающихся с S, не пусто, так как содержит нулевой идеал, и, очевидно, является индуктивно упорядоченным). Пусть $\mathfrak{p}$ — максимальный элемент в этом множестве. Пусть a, $b \in A$, $ab \in \mathfrak{p}$, но $a \notin \mathfrak{p}$ и $b \notin \mathfrak{p}$. По предположению идеалы $(a, \mathfrak{p})$ и $(b, \mathfrak{p})$, порожденные a и $\mathfrak{p}$ (или b и $\mathfrak{p}$ соответственно), пересекаются с S, а потому существуют элементы s, $s' \in S$, c, $c' \in A$, p, $p' \in \mathfrak{p}$, такие, что

$$s = ca + p \quad \text{и} \quad s' = c'b + p'.$$

Перемножив эти два выражения, получим

$$ss' = cc'ab + p'',$$

где p'' — некоторый элемент из $\mathfrak{p}$. Отсюда вытекает, что ss' лежит в $\mathfrak{p}$. Это противоречит тому факту, что $\mathfrak{p}$ не пересекается с S, и тем самым доказывает, что идеал $\mathfrak{p}$ простой.

Элемент a кольца A называется *нильпотентным*, если существует целое число $n \geqslant 1$, такое, что $a^n = 0$.

Следствие 1. *Элемент a кольца A нильпотентен в том и только в том случае, если он лежит во всяком простом идеале кольца A.*

Доказательство. Если $a^n = 0$, то $a^n \in \mathfrak{p}$ для всякого простого идеала $\mathfrak{p}$ и, следовательно, $a \in \mathfrak{p}$. Если $a^n \neq 0$ ни для какого положительного числа n, то обозначим через S мультипликативное подмножество, состоящее из степеней a, а именно $\{1, a, a^2, \ldots\}$, и, согласно предложению, найдем простой идеал, не пересекающийся с S, доказав тем самым обратное предложение.

Нильрадикалом идеала $\mathfrak{a} \subset A$ называется множество всех $a \in A$, таких, что $a^n \in \mathfrak{a}$ для некоторого целого $n \geqslant 1$ (или, что эквивалентно, множество элементов $a \in A$, образ которых в факторкольце $A/\mathfrak{a}$ нильпотентен). Заметим, что нильрадикал идеала $\mathfrak{a}$ является идеалом, поскольку из $a^n = 0$ и $b^m = 0$ следует $(a+b)^k = 0$ для достаточно большого k: в биномиальном разложении либо a, либо b будет появляться в степени, не меньшей, чем n или m.

Следствие 2. *Элемент a кольца A лежит в нильрадикале идеала $\mathfrak{a}$ тогда и только тогда, когда он лежит во всяком простом идеале, содержащем $\mathfrak{a}$.*

Доказательство. Следствие 2 эквивалентно следствию 1, примененному к кольцу $A/\mathfrak{a}$.

Распространим следствие 1 на модули. Сделаем сначала несколько замечаний о локализации. Пусть S — мультипликативное подмножество в A. Для всякого модуля M можно определить $S^{-1}M$ тем же способом, как мы определили $S^{-1}A$. Рассматриваем классы эквивалентности пар (x, s), где $x \in M$ и $s \in S$, причем две пары (x, s) и (x', s') эквивалентны, если существует элемент $s_1 \in S$, такой, что $s_1(s'x - sx') = 0$. Обозначим класс эквивалентности пары (x, s) через x/s. Тотчас проверяется, что множество классов эквивалентности — аддитивная группа (относительно очевидных операций). В действительности она является A-модулем относительно операции

$$(a, x/s) \longmapsto ax/s.$$

Этот модуль классов эквивалентности мы и будем обозначать через $S^{-1}M$. (Отметим, что $S^{-1}M$ можно было бы также рассматривать как $S^{-1}A$-модуль.)

Если $\mathfrak{p}$ — простой идеал в A и S — дополнение к $\mathfrak{p}$ в A, то $S^{-1}M$ обозначается также через $M_{\mathfrak{p}}$.

Из определений тривиально вытекает, что если $N \to M$ — инъективный гомоморфизм, то имеется естественное вложение $S^{-1}N \to S^{-1}M$. Другими словами, если N — подмодуль в M, то $S^{-1}N$ можно рассматривать как подмодуль в $S^{-1}M$.

Если $x \in N$ и $s \in S$, то дробь x/s может рассматриваться как элемент из $S^{-1}N$ или $S^{-1}M$. Если $x/s = 0$ в $S^{-1}M$, то существует элемент $s_1 \in S$, такой, что $s_1 x = 0$, а это означает, что x/s есть 0 также и в $S^{-1}N$. Таким образом, если $\mathfrak{p}$ — простой идеал и N — подмодуль в M, то имеется естественное вложение $N_{\mathfrak{p}}$ в $M_{\mathfrak{p}}$. Фактически мы будем отождествлять $N_{\mathfrak{p}}$ с подмодулем в $M_{\mathfrak{p}}$. В частности, мы видим, что $M_{\mathfrak{p}}$ есть сумма своих подмодулей $(Ax)_{\mathfrak{p}}$, где $x \in M$ (но, разумеется, не прямая сумма).

Пусть $x \in M$. *Аннулятор* $\mathfrak{a}$ элемента x — это идеал, состоящий из всех элементов $a \in A$, таких, что $ax = 0$. Имеет место изоморфизм (модулей)

$$A/\mathfrak{a} \xrightarrow{\approx} Ax$$

относительно отображения

$$a \longmapsto ax.$$

Лемма. *Пусть x — элемент модуля M, $\mathfrak{a}$ — его аннулятор и $\mathfrak{p}$ — простой идеал в A. Тогда $(Ax)_{\mathfrak{p}} \neq 0$ в том и только в том случае, если $\mathfrak{p}$ содержит $\mathfrak{a}$.*

Доказательство. Лемма является непосредственным следствием определений, и ее доказательство предоставляется читателю.

Пусть a — элемент из A. Пусть M — некоторый модуль. Гомоморфизм

$$x \longmapsto ax, \quad x \in M$$

будет называться *главным гомоморфизмом*, ассоциированным с a, и будет обозначаться через a_M. Мы будем говорить, что a_M *локально нильпотентен*, если для каждого $x \in M$ существует такое целое число $n(x) \geqslant 1$, что $a^{n(x)}x = 0$. Из этого условия следует, что для всякого конечно порожденного подмодуля N в M существует такое целое число $n \geqslant 1$, что $a^n N = 0$: достаточно взять в качестве n наибольшую из степеней a, аннулирующих конечное множество образующих N. Поэтому *если модуль M конечно порожден, то гомоморфизм a_M локально нильпотентен в точности тогда, когда он нильпотентен.*

Предложение 7. *Пусть M — модуль, $a \in A$. Тогда a_M локально нильпотентен в том и только в том случае, если a лежит во всяком простом идеале $\mathfrak{p}$, для которого $M_{\mathfrak{p}} \neq 0$.*

Доказательство. Предположим, что a_M локально нильпотентен. Пусть $\mathfrak{p}$ — простой идеал в A, такой, что $M_\mathfrak{p} \neq 0$. Тогда существует $x \in M$, для которого $(Ax)_\mathfrak{p} \neq 0$. Пусть n — такое положительное число, что $a^n x = 0$. Обозначим через $\mathfrak{a}$ аннулятор элемента x. Тогда $a^n \in \mathfrak{a}$ и, следовательно, мы можем, применив лемму и следствие 2 предложения 6, заключить, что a лежит во всяком простом идеале $\mathfrak{p}$, таком, что $M_\mathfrak{p} \neq 0$. Обратно, если дан элемент $x \in M$, $x \neq 0$, то рассмотрим модуль Ax и, обратив предыдущие рассуждения, докажем, что $a^n x = 0$ для некоторого $n \geqslant 1$, установив тем самым локальную нильпотентность гомоморфизма a_M.

Пусть M — модуль. Простой идеал $\mathfrak{p}$ в A будет называться *ассоциированным* с M, если существует элемент $x \in M$, аннулятор которого совпадает с $\mathfrak{p}$. Так как $\mathfrak{p} \neq A$, то, в частности, $x \neq 0$.

Предложение 8. *Пусть M — модуль $\neq 0$ и $\mathfrak{p}$ — максимальный элемент в множестве идеалов, являющихся аннуляторами элементов $x \in M$, $x \neq 0$. Тогда $\mathfrak{p}$ — простой идеал.*

Доказательство. Пусть $\mathfrak{p}$ — аннулятор элемента $x \neq 0$. Тогда $\mathfrak{p} \neq A$. Пусть a, $b \in A$, $ab \in \mathfrak{p}$, $a \notin \mathfrak{p}$. Тогда $ax \neq 0$. Но идеал $(b, \mathfrak{p})$ аннулирует ax и содержит $\mathfrak{p}$. Если $\mathfrak{p}$ максимален, то отсюда вытекает, что $b \in \mathfrak{p}$ и, следовательно, $\mathfrak{p}$ — простой идеал.

Следствие 1. *Если кольцо A нётерово и M — модуль $\neq 0$, то существует простой идеал, ассоциированный с M.*

Доказательство. Множество идеалов, определенное в формулировке предложения 8, не пусто, поскольку $M \neq 0$, и содержит максимальный элемент, поскольку A нётерово.

Следствие 2. *Предположим, что и A, и M нётеровы, $M \neq 0$. Тогда существует последовательность подмодулей*

$$M = M_1 \supset M_2 \supset \ldots \supset M_r = 0,$$

такая, что каждый фактормодуль M_i/M_{i+1} изоморфен $A/\mathfrak{p}_i$, где $\mathfrak{p}_i$ — некоторый простой идеал.

Доказательство. Рассмотрим множество подмодулей, обладающих свойством, описанным в формулировке следствия. Оно не пусто, поскольку существует простой идеал $\mathfrak{p}$, ассоциированный с M, и если $\mathfrak{p}$ — аннулятор x, то $Ax \approx A/\mathfrak{p}$. Пусть N — максимальный элемент в этом множестве. Если $N \neq M$, то в силу предыдущего рассуждения, примененного к M/N, существует подмодуль N' в M, такой, что N'/N изоморфен $A/\mathfrak{p}$ для некоторого $\mathfrak{p}$, а это противоречит максимальности N.

Предложение 9. *Пусть кольцо A нётерово и $a \in A$. Пусть M — модуль. Тогда гомоморфизм a_M инъективен в том и только в том случае, если a не лежит ни в одном из простых идеалов, ассоциированных с M.*

Доказательство. Предположим, что a_M не инъективен, так что $ax = 0$ для некоторого $x \in M$, $x \neq 0$. В силу следствия 1 предложения 8 существует простой идеал $\mathfrak{p}$, ассоциированный с Ax и a есть элемент этого $\mathfrak{p}$. Обратно, если a_M инъективен, то a не может лежать ни в каком ассоциированном простом идеале, потому что a не аннулирует никакого ненулевого элемента из M.

Предложение 10. *Пусть кольцо A нётерово и M — модуль. Пусть $a \in A$. Следующие условия эквивалентны:*

(1) *a_M локально нильпотентен;*

(2) *a лежит в каждом ассоциированном с M простом идеале;*

(3) *a лежит в каждом простом идеале $\mathfrak{p}$, для которого $M_\mathfrak{p} \neq 0$.*

Доказательство. То, что (1) влечет (2), очевидно из определений и не нуждается в предположении, что A нётерово. Не нуждается в этом предположении и то, доказанное в предположении 7, утверждение, что (3) влечет (1). Мы должны, таким образом, показать, что (2) влечет (3). Пусть $\mathfrak{p}$ — простой идеал, для которого $M_\mathfrak{p} \neq 0$. Тогда существует элемент $x \in M$, такой, что $(Ax)_\mathfrak{p} \neq 0$. В силу предложения 8 в A существует простой идеал $\mathfrak{q}$, ассоциированный с $(Ax)_\mathfrak{p}$. Следовательно, существует элемент y/s в $(Ax)_\mathfrak{p}$ с $y \in Ax$, $s \notin \mathfrak{p}$ и $y/s \neq 0$, аннулятор которого совпадает с $\mathfrak{q}$. Отсюда вытекает, что $\mathfrak{q} \subset \mathfrak{p}$, так как иначе существовало бы $b \in \mathfrak{q}$, $b \notin \mathfrak{p}$, причем $0 = by/s$, откуда $y/s = 0$ — противоречие.

Пусть теперь $a_1, \ldots, a_r$ — конечное множество образующих идеала $\mathfrak{q}$. Тогда для каждого $i = 1, \ldots, r$ существует элемент $t_i \notin \mathfrak{p}$, такой, что $t_i a_i y = 0$. Очевидно, $t = t_1 \ldots t_r \notin \mathfrak{p}$. Всякий элемент из $\mathfrak{q}$ аннулирует элемент ty в M, и если $a(ty) = 0$ в M, то $ay/s = 0$ в $M_\mathfrak{p}$, откуда $a \in \mathfrak{q}$. Следовательно, $\mathfrak{q}$ — аннулятор элемента ty в M, являющийся ассоциированным с M простым идеалом. Это как раз и требовалось установить.

Следствие. *Пусть кольцо A нётерово и M — модуль. Следующие условия эквивалентны:*

(1) *существует только один ассоциированный с M простой идеал;*

(2) *$M \neq 0$, и для всякого $a \in A$ гомоморфизм a_M либо инъективен, либо локально нильпотентен. При выполнении этих условий множество тех элементов $a \in A$, для которых a_M локально нильпотентен, совпадает с простым идеалом, ассоциированным с M.*

Доказательство. Это непосредственное следствие предложений 9 и 10.

Приводимое ниже предложение будет использовано в следующем параграфе, чтобы при некоторых условиях охарактеризовать ассоциированные с модулем простые идеалы.

Предложение 11. *Пусть N — подмодуль в M. Всякий простой идеал, ассоциированный с N, ассоциирован также и с M. Любой ассоциированный с модулем M простой идеал ассоциирован также либо с N, либо с M/N.*

Доказательство. Первое утверждение очевидно. Пусть $\mathfrak{p}$ — ассоциированный с M простой идеал, скажем $\mathfrak{p}$ есть аннулятор элемента $x \neq 0$. Если $Ax \cap N = 0$, то Ax изоморфен подмодулю из M/N и, следовательно, $\mathfrak{p}$ ассоциирован с M/N. Если $Ax \cap N \neq 0$, то мы рассматриваем $Ax \cap N$ как модуль над целостным кольцом $A/\mathfrak{p}$ и ясно, что аннулятор любого ненулевого элемента из $Ax \cap N$ в $A/\mathfrak{p}$ есть 0. Следовательно, его аннулятор в A есть $\mathfrak{p}$ и $\mathfrak{p}$ ассоциирован с N, что и требовалось показать.

§ 5. Примарное разложение

Мы продолжаем предполагать, что A — коммутативное кольцо и что модули (соответственно гомоморфизмы) — это A-модули (соответственно A-гомоморфизмы), если не оговорено противное.

Пусть M — модуль. Подмодуль Q в M называется *примарным*, если $Q \neq M$ и если для любого данного $a \in A$ гомоморфизм $a_{M/Q}$ либо инъективен, либо нильпотентен. Рассматривая A как модуль над собой, мы получаем, что идеал $\mathfrak{q}$ примарен тогда и только тогда, когда он удовлетворяет следующему условию:

если $ab \in \mathfrak{q}$ и $a \notin \mathfrak{q}$, то $b^n \in \mathfrak{q}$ для некоторого $n \geqslant 1$.

Пусть Q — примарный подмодуль и $\mathfrak{p}$ — идеал, состоящий из всех элементов $a \in A$, для которых $a_{M/Q}$ нильпотентен. Тогда $\mathfrak{p}$ — простой идеал. Действительно, предположим, что $ab \in \mathfrak{p}$ и $a \notin \mathfrak{p}$. Тогда $a_{M/Q}$ инъективен и, следовательно, $a^n_{M/Q}$ инъективен для всех $n \geqslant 1$. Из нильпотентности $(ab)_{M/Q}$ теперь вытекает, что $b_{M/Q}$ должен быть нильпотентен и, следовательно, что $b \in \mathfrak{p}$. Этим доказано, что идеал $\mathfrak{p}$ простой. Мы будем называть $\mathfrak{p}$ простым идеалом, *соответствующим* Q, а также говорить, что Q $\mathfrak{p}$-примарен [1]).

---

[1]) Говорят также, что Q *принадлежит* простому идеалу $\mathfrak{p}$. — *Прим. ред.*

Предложение 12. *Пусть M — модуль, $Q_1, \ldots, Q_r$ — подмодули, $\mathfrak{p}$-примарные для одного и того же простого идеала $\mathfrak{p}$. Тогда подмодуль $Q_1 \cap \ldots \cap Q_r$ также $\mathfrak{p}$-примарен.*

Доказательство. Положим $N = Q_1 \cap \ldots \cap Q_r$. Пусть $a \in \mathfrak{p}$, и пусть n_i таковы, что $(a_{M/Q_i})^{n_i} = 0$ для каждого $i = 1, \ldots, r$; обозначим через n максимум из $n_1, \ldots, n_r$. Тогда $(a_{M/Q})^n = 0$, так что $a_{M/Q}$ нильпотентен. Обратно, предположим, что $a \notin \mathfrak{p}$. Пусть $x \in M$, $x \notin Q_j$ для некоторого j. Тогда $a^n x \notin Q_j$ для всех положительных n и, следовательно, $a_{M/Q}$ инъективен. Это доказывает наше предложение.

Пусть N — подмодуль в M. Если N представлен в виде конечного пересечения примарных подмодулей, скажем

$$N = Q_1 \cap \ldots \cap Q_r,$$

то мы будем называть это представление *примарным разложением* подмодуля N. Используя предложение 12, мы видим, что, сгруппировав Q_i по их простым идеалам, мы всегда можем получить из данного примарного разложения другое, в котором простые идеалы, соответствующие примарным подмодулям, все различны. Примарное разложение подмодуля N, в котором простые идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, соответствующие $Q_1, \ldots, Q_r$, различны, причем N не может быть представлен в виде пересечения собственного подсемейства примарных подмодулей $\{Q_1, \ldots, Q_r\}$, будет называться *несократимым*. Вычеркивая некоторые из примарных модулей, участвующих в данном разложении, мы находим, что если подмодуль N обладает каким-то примарным разложением, то он обладает и несократимым разложением. Мы докажем сейчас результат, дающий некоторое свойство единственности несократимого примарного разложения.

Пусть $Q_1 \cap \ldots \cap Q_r = N$ — несократимое примарное разложение, причем $\mathfrak{p}_i$ соответствует Q_i. Если $\mathfrak{p}_i$ не содержит никакого $\mathfrak{p}_j (j \neq i)$, то мы говорим, что $\mathfrak{p}_i$ *изолирован*. Изолированные простые идеалы — это, таким образом, те простые идеалы, которые минимальны в множестве простых идеалов, соответствующих примарным модулям Q_i.

Теорема 3. *Пусть N — подмодуль в M, и пусть*

$$N = Q_1 \cap \ldots \cap Q_r = Q'_1 \cap \ldots \cap Q'_s$$

— два его несократимых примарных разложения. Тогда $r = s$. Множество простых идеалов, соответствующих $Q_1, \ldots, Q_r$ и $Q'_1, \ldots, Q'_r$, одно и то же. Если $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ — множество изолированных простых идеалов, соответствующих этим разложениям, то $Q_i = Q'_i$ для $i = 1, \ldots, m$, другими словами, примарные модули, принадлежащие изолированным простым идеалам, однозначно определены.

Доказательство. Предположим, что, после возможной перестановки индексов, $\mathfrak{p}_1$ максимален в множестве простых идеалов, соответствующих примарным модулям Q_i' и Q_i, и что $\mathfrak{p}_1 \neq \mathfrak{p}_j'$ для $j = 1, \ldots, s$. Тогда существует такой элемент $a \in \mathfrak{p}_1$, что $a \notin \mathfrak{p}_i$ $(i = 2, \ldots, r)$ и $a \notin \mathfrak{p}_j'$ $(j = 1, \ldots, s)$. Пусть $n \geqslant 1$ — целое число, для которого $a^n M \subset Q_1$. Обозначим через N^* модуль элементов $x \in M$, таких, что $a^n x \in N$. Мы утверждаем, что $N^* = Q_2 \cap \ldots \cap Q_r$. Ясно, что

$$Q_2 \cap \ldots \cap Q_r \subset N^*.$$

Обратно, если $x \in M$, $x \notin Q_i$ для некоторого $i > 1$, то $a^n x \notin Q_i$, поскольку $a \notin \mathfrak{p}_i$. Следовательно, $N^* \subset Q_2 \cap \ldots \cap Q_r$. Те же рассуждения показывают, что если $\mathfrak{p}_1 \neq \mathfrak{p}_j'$ для $j = 1, \ldots, s$, то

$$Q_2 \cap \ldots \cap Q_r = Q_1' \cap \ldots \cap Q_s',$$

вопреки предположению, что наше представление N в виде пересечения примарных модулей несократимо. Это доказывает, что $\mathfrak{p}_1$ встречается в множестве $\{\mathfrak{p}_1', \ldots, \mathfrak{p}_s'\}$, скажем $\mathfrak{p}_1 = \mathfrak{p}_1'$, а также, что

$$Q_2 \cap \ldots \cap Q_r = Q_2' \cap \ldots \cap Q_s'.$$

Остается доказать единственность примарного модуля, принадлежащего изолированному простому идеалу, скажем $\mathfrak{p}_1$. По определению для каждого $j = 2, \ldots, r$ существует $a_j \in \mathfrak{p}_j$, $a_j \notin \mathfrak{p}_1$. Пусть $a = a_2 \ldots a_r$ — произведение этих элементов. Тогда $a \in \mathfrak{p}_j$ для всех $j > 1$, но $a \notin \mathfrak{p}_1$. Мы можем найти целое число $n \geqslant 1$, такое, что $a^n_{M/Q_j} = 0$ для $j = 2, \ldots, r$. Пусть

$$N_m = \text{множество таких } x \in M, \text{ что } a^m x \in N.$$

Мы утверждаем, что $Q_1 = N_m$ для всех достаточно больших m. Этим будет доказана искомая единственность. Пусть $x \in Q_1$. Тогда $a^m x \in Q_1 \cap \ldots \cap Q_r = N$, так что $x \in N_m$. Обратно, пусть $x \in N_m$, так что $a^m x \in N$ и, в частности, $a^m x \in Q_1$. Так как $a \notin \mathfrak{p}_1$, то по определению a_{M/Q_1} инъективен. Следовательно, $x \in Q_1$ и тем самым наша теорема доказана.

Теорема 4. *Всякий подмодуль N нётерова модуля M обладает примарным разложением.*

Доказательство. Рассмотрим множество подмодулей в M, не обладающих примарным разложением. Если это множество не пусто, то ввиду нётеровости M оно имеет максимальный элемент,

который мы обозначим через N. Подмодуль N не примарен, т. е. существует $a \in A$, такое, что $a_{M/N}$ ни инъективен, ни нильпотентен. Возрастающая последовательность модулей

$$\operatorname{Ker} a_{M/N} \subset \operatorname{Ker} a_{M/N}^2 \subset \operatorname{Ker} a_{M/N}^3 \subset \ldots$$

стабилизируется, скажем, на $a_{M/N}^r$. Обозначим эндоморфизм

$$a_{M/N}^r\colon\ M/N \to M/N$$

через φ. Тогда $\operatorname{Ker} \varphi^2 = \operatorname{Ker} \varphi$. Следовательно, $0 = \operatorname{Ker} \varphi \cap \operatorname{Im} \varphi$ и ни ядро, ни образ φ не равны 0. Беря прообраз в M, мы видим, что N есть пересечение двух подмодулей в M, не равных N. Из максимальности N заключаем, что каждый из этих подмодулей допускает примарное разложение, а потому и N допускает примарное разложение — противоречие.

Мы закончим наше рассмотрение установлением связи между простыми идеалами, принадлежащими примарному разложению, и ассоциированными простыми идеалами, обсуждавшимися в предыдущем параграфе.

Предложение 13. *Пусть A и M нётеровы. Подмодуль Q в M примарен тогда и только тогда, когда с M/Q ассоциируется в точности один простой идеал $\mathfrak{p}$; в этом случае $\mathfrak{p}$ соответствует Q, т. е. Q $\mathfrak{p}$-примарен.*

Доказательство. Это непосредственное следствие определений и следствия предложения 10.

Теорема 5. *Пусть A и M нётеровы. Ассоциированные с модулем M простые идеалы — это в точности простые идеалы, соответствующие примарным модулям в несократимом примарном разложении 0 в M. В частности, множество ассоциированных с модулем M простых идеалов конечно.*

Доказательство. Пусть

$$0 = Q_1 \cap \ldots \cap Q_r$$

— несократимое примарное разложение 0 в M. Имеет место инъективный гомоморфизм

$$M \to \coprod_{i=1}^{r} M/Q_i.$$

В силу предложения 11 из § 4 и предложения 13 мы заключаем, что всякий ассоциированный с M простой идеал соответствует некоторому Q_i. Обратно, пусть $N = Q_2 \cap \ldots \cap Q_r$. Тогда $N \neq 0$, поскольку наше разложение несократимо. Имеем

$$N = N/(N \cap Q_1) \approx (N + Q_1)/Q_1 \subset M/Q_1.$$

Итак, N изоморфен подмодулю в M/Q_1 и, следовательно, обладает ассоциированным простым идеалом, который не может быть ничем иным, как простым идеалом $\mathfrak{p}_1$, соответствующим Q_1. Это доказывает нашу теорему.

УПРАЖНЕНИЯ

Во всех упражнениях „кольцо" означает „коммутативное кольцо".

1. Пусть A — кольцо, $\mathfrak{a}$ — идеал, содержащийся во всяком максимальном идеале, и E — конечно порожденный A-модуль. Если $\mathfrak{a}E = E$, то $E = 0$. [*Указание*: индукция по числу образующих. Выразить одну образующую через другие, используя тот факт, что $1 + a$ есть единица при $a \in \mathfrak{a}$. См. лемму Накаямы в гл. IX.] Это утверждение применимо, в частности, к случаю, когда $A = \mathfrak{o}$ — локальное кольцо и $\mathfrak{a} = \mathfrak{m}$ — его максимальный идеал. Получить следующие два утверждения в качестве следствий:

Пусть E — конечно порожденный $\mathfrak{o}$-модуль и F — его подмодуль. Если $E = F + \mathfrak{m}E$, то $E = F$.

Если $x_1, \ldots, x_n$ — образующие для $\mathfrak{m} \bmod \mathfrak{m}^2$, то они служат образующими для $\mathfrak{m}$ над $\mathfrak{o}$.

2. (Артин — Рис) Пусть A — нётерово кольцо, $\mathfrak{a}$ — идеал, E — конечно порожденный модуль и F — подмодуль. Тогда существует целое число $s \geqslant 0$, такое, что для всех $n \geqslant s$ имеем $\mathfrak{a}^n E \cap F = \mathfrak{a}^{n-s}(\mathfrak{a}^s E \cap F)$. [*Указание*: пусть $A_t = A[t]$ и $A_t' = A[\mathfrak{a}t] = \coprod_{n=0}^{\infty} \mathfrak{a}^n t^n$. Если $a_1, \ldots, a_m$ — образующие идеала $\mathfrak{a}$, то $a_1 t, \ldots, a_m t$ — образующие кольца A_t', которое поэтому нётерово. Определить очевидным способом E_t как A_t-модуль $\coprod t^n E$ и аналогично определить F_t. Пусть $E_t' = A_t' E_t = \coprod \mathfrak{a}^n t^n E$. Тогда E_t' — конечно порожденный A_t'-модуль и $E_t' \cap F_t$ имеет конечное число образующих, включающих лишь конечное число степеней t. Пусть t^s — наибольшая из них; тогда

$$\coprod_{n=0}^{\infty} t^n (\mathfrak{a}^n E \cap F) = E_t' \cap F_t = A_t' \coprod_{\nu=0}^{s} t^\nu (\mathfrak{a}^\nu E \cap F).$$

Сравнение коэффициентов при t^n для $n \geqslant s$ дает

$$\mathfrak{a}^n E \cap F = \coprod_{\nu=0}^{s} \mathfrak{a}^{n-\nu}(\mathfrak{a}^\nu E \cap F),$$

откуда немедленно следует искомый результат.]

3. (Крулль) В условиях предыдущего упражнения предположим, что $\mathfrak{a}$ содержится во всяком максимальном идеале кольца A. Тогда $\bigcap_{n=1}^{\infty} \mathfrak{a}^n E = 0$. [*Указание*: положить $F = \bigcap \mathfrak{a}^n E$ и применить лемму Накаямы.] В частности, пусть $\mathfrak{o}$ — нетерово локальное кольцо и $\mathfrak{m}$ — его максимальный идеал. Тогда

$$\bigcap_{\nu=1}^{\infty} \mathfrak{m}^\nu = 0.$$

4. Пусть A — коммутативное кольцо, M — модуль, N — подмодуль и $N = Q_1 \cap \ldots \cap Q_r$ — его примарное разложение. Положим $\overline{Q}_i = Q_i/N$. Показать, что $0 = \overline{Q}_1 \cap \ldots \cap \overline{Q}_r$ — примарное разложение 0 в M/N. Сформулировать и доказать обратное утверждение.

5. Пусть $\mathfrak{p}$ — простой идеал и $\mathfrak{a}$, $\mathfrak{b}$ — идеалы в A. Показать, что если $\mathfrak{ab} \subset \mathfrak{p}$, то $\mathfrak{a} \subset \mathfrak{p}$ или $\mathfrak{b} \subset \mathfrak{p}$.

6. Пусть $\mathfrak{q}$ — примарный идеал, и пусть $\mathfrak{a}$, $\mathfrak{b}$ — идеалы, удовлетворяющие условию $\mathfrak{ab} \subset \mathfrak{q}$. Предположим, что идеал $\mathfrak{b}$ конечно порожден. Показать, что либо $\mathfrak{a} \subset \mathfrak{q}$, либо существует положительное целое число n, такое, что $\mathfrak{b}^n \subset \mathfrak{q}$.

7. Пусть A — нётерово кольцо и $\mathfrak{q}$ — $\mathfrak{p}$-примарный идеал. Показать, что существует $n \geqslant 1$, такое, что $\mathfrak{p}^n \subset \mathfrak{q}$.

8. Пусть A — произвольное коммутативное кольцо, S — мультипликативное подмножество, $\mathfrak{p}$ — простой идеал и $\mathfrak{q}$ — $\mathfrak{p}$-примарный идеал. Тогда $\mathfrak{p}$ пересекает S в том и только в том случае, если $\mathfrak{q}$ пересекает S. Кроме того, если $\mathfrak{q}$ не пересекает S, то $S^{-1}\mathfrak{q}$ будет $S^{-1}\mathfrak{p}$-примарным идеалом в $S^{-1}A$.

9. Пусть $\mathfrak{a}_S = S^{-1}\mathfrak{a}$, где $\mathfrak{a}$ — идеал в A. Если $\varphi_S\colon A \to S^{-1}A$ — каноническое отображение, то $\varphi_S^{-1}(\mathfrak{a}_S)$ сокращенно обозначаем через $\mathfrak{a}_S \cap A$, хотя бы φ_S и не было инъективным. Показать, что между простыми идеалами из A, не пересекающимися с S, и простыми идеалами из $S^{-1}A$ существует взаимно однозначное соответствие

$$\mathfrak{p} \longmapsto \mathfrak{p}_S \quad \text{и} \quad \mathfrak{p}_S \longmapsto \mathfrak{p}_S \cap A = \mathfrak{p}.$$

Доказать аналогичное утверждение с заменой простых идеалов на примарные.

10. Пусть $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$ — несократимое примарное разложение идеала. Предположим, что $\mathfrak{q}_1, \ldots, \mathfrak{q}_i$ не пересекают S, а $\mathfrak{q}_j$ при $j > i$ пересекают S. Показать, что

$$\mathfrak{a}_S = \mathfrak{q}_{1S} \cap \ldots \cap \mathfrak{q}_{iS}$$

— несократимое примарное разложение идеала $\mathfrak{a}_S$.

11. Предположим, что кольцо A нётерово. Показать, что множество делителей нуля в A является теоретико-множественным объединением всех простых идеалов, соответствующих примарным идеалам в несократимом примарном разложении 0.

Часть вторая

ТЕОРИЯ ПОЛЕЙ

Эта часть связана с решениями алгебраических уравнений с одним или несколькими переменными. Это повторяющаяся тема каждой главы части, и мы закладываем здесь фундамент для любого дальнейшего изучения таких уравнений.

Если даны подкольцо A кольца B и конечное число многочленов $f_1, \ldots, f_n$ из $A[X_1, \ldots, X_n]$, то нас интересуют наборы из n элементов $(b_1, \ldots, b_n) \in B^{(n)}$, такие, что

$$f_i(b_1, \ldots, b_n) = 0$$

для $i = 1, \ldots, r$. При соответствующем выборе A и B это включает в себя основную задачу диофантова анализа, когда A и B имеют „арифметическую“ структуру.

Мы изучим различные случаи сначала для уравнений с одним переменным над произвольным полем, беря в качестве B алгебраические расширения этого поля. Далее мы рассмотрим аспекты этого вопроса, относящиеся к кольцевым структурам (целые расширения). Затем мы перейдем к конечно порожденным кольцевым расширениям и многочленам от нескольких переменных. Наконец, мы введем дополнительные структуры, такие, как вещественность или метрические структуры, задаваемые абсолютными значениями. Каждая из этих структур приводит к некоторым теоремам, описывающим структуру решений указанных выше уравнений.

Глава VII

Алгебраические расширения

§ 1. Конечные и алгебраические расширения

Пусть F — поле. Если F — подполе поля E, то мы говорим также, что E есть *расширение* поля F. Мы можем рассматривать E как векторное пространство над F, и мы говорим, что E — *конечное* или *бесконечное* расширение F, в зависимости от того, конечна или бесконечна размерность этого векторного пространства.

Пусть F — подполе поля E. Элемент α из E называется *алгебраическим* над F, если в F существуют элементы $a_0, \ldots, a_n$ $(n \geqslant 1)$, не все равные 0 и такие, что

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0.$$

Для алгебраического элемента $\alpha \neq 0$ мы всегда можем найти такие элементы a_i в предыдущем равенстве, что $a_0 \neq 0$ (сокращая на подходящую степень α).

Пусть X — переменная над F. Можно также сказать, что элемент α алгебраичен над F, если гомоморфизм

$$F[X] \to E,$$

тождественный на F и переводящий X в α, имеет ненулевое ядро. В таком случае это ядро будет главным идеалом, порожденным одним многочленом $p(X)$, относительно которого мы можем предполагать, что его старший коэффициент равен 1. Имеет место изоморфизм

$$F[X]/(p(X)) \approx F[\alpha],$$

и так как кольцо $F[\alpha]$ целостное, то $p(X)$ неприводим. Если $p(X)$ нормализован условием, что его старший коэффициент равен 1, то $p(X)$ однозначно определяется элементом α и будет называться неприводимым многочленом элемента α над F. Иногда мы будем обозначать его через $\mathrm{Irr}(\alpha, F, X)$.

Расширение E поля F называется *алгебраическим*, если всякий элемент из E алгебраичен над F.

Предложение 1. *Всякое конечное расширение E поля F алгебраично над F.*

Доказательство. Пусть $\alpha \in E$, $\alpha \neq 0$. Степени α

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

не могут быть линейно независимы над F для всех целых положительных n, иначе размерность E над F была бы бесконечна. Линейное соотношение между этими степенями показывает, что элемент α алгебраичен над F.

Заметим, что утверждение, обратное предложению 1, не верно: существуют бесконечные алгебраические расширения. Позднее мы увидим, что подполе поля комплексных чисел, состоящее из всех чисел, алгебраических над $\mathbf{Q}$, является бесконечным расширением $\mathbf{Q}$.

Если E — расширение поля F, то мы обозначаем символом

$$[E : F]$$

размерность E как векторного пространства над F. Будем называть $[E : F]$ *степенью* E над F. Она может быть бесконечной.

Предложение 2. *Пусть k — поле и $F \subset E$ — расширения k. Тогда*

$$[E : k] = [E : F]\,[F : k].$$

Если $\{x_i\}_{i \in I}$ — базис поля F над k и $\{y_j\}_{j \in J}$ — базис поля E над F, то $\{x_i y_j\}_{(i,\, j) \in I \times J}$ будет базисом поля E над k.

Доказательство. Пусть $z \in E$. По предположению существуют элементы $\alpha_j \in F$, почти все равные нулю и такие, что

$$z = \sum_{j \in J} \alpha_j y_j.$$

Для каждого $j \in J$ существуют элементы $b_{ji} \in k$, из которых почти все равны 0, такие, что

$$\alpha_j = \sum_{i \in I} b_{ji} x_i,$$

и, следовательно,

$$z = \sum_j \sum_i b_{ji} x_i y_j.$$

Это означает, что $\{x_i y_j\}$ является семейством образующих для E над k. Мы должны показать, что оно линейно независимо. Пусть $\{c_{ij}\}$ — семейство элементов из k, почти все из которых равны 0, такое, что

$$\sum_j \sum_i c_{ij} x_i y_j = 0.$$

Тогда для каждого j

$$\sum_i c_{ij} x_i = 0,$$

поскольку элементы y_j линейно независимы над F. Наконец, $c_{ij}=0$ для всякого i, так как $\{x_i\}$ — базис поля F над k, что и доказывает наше предложение.

Следствие. *Расширение $E\supset F\supset k$ поля k конечно в том и только в том случае, если E конечно над F и F конечно над k.*

Как и в случае групп, мы называем *башней* полей последовательность расширений

$$F_1\subset F_2\subset \ldots \subset F_n.$$

Для *конечности башни* необходимо и достаточно, чтобы каждый ее этаж был конечен.

Пусть k — поле, E — его расширение и $a\in E$. Мы обозначаем через $k(\alpha)$ наименьшее подполе в E, содержащее k и α. Оно состоит из всех дробей $f(\alpha)/g(\alpha)$, где f, g — многочлены с коэффициентами в k и $g(\alpha)\neq 0$.

Предложение 3. *Пусть элемент α алгебраичен над k. Тогда $k(\alpha)=k[\alpha]$ и поле $k(\alpha)$ конечно над k. Степень $[k(\alpha): k]$ равна степени многочлена* $\operatorname{Irr}(\alpha, k, X)$.

Доказательство. Пусть $p(X)=\operatorname{Irr}(\alpha, k, X)$. Пусть многочлен $f(X)\in k[X]$ таков, что $f(\alpha)\neq 0$. Тогда $f(X)$ не делится на $p(X)$ и, следовательно, существуют многочлены $g(X)$, $h(X)\in k[X]$, такие, что

$$g(X)p(X)+h(X)f(X)=1.$$

Отсюда мы получаем, что $h(\alpha)f(\alpha)=1$ и, значит, $f(\alpha)$ обратим в $k[\alpha]$. Следовательно, $k[\alpha]$ не только кольцо, но и поле, а потому должно быть равно $k(\alpha)$. Пусть $d=\deg p(X)$. Степени

$$1,\ \alpha,\ \ldots,\ \alpha^{d-1}$$

линейно независимы над k; действительно, предположим, что

$$a_0+a_1\alpha+\ \ldots\ +a_{d-1}\alpha^{d-1}=0,$$

где $a_i\in k$, причем не все $a_i=0$. Положим $g(X)=a_0+\ldots+a_{d-1}X^{d-1}$. Тогда $g\neq 0$ и $g(\alpha)=0$. Следовательно, $g(X)$ делится на $p(X)$ — противоречие. Наконец, пусть $f(\alpha)\in k[\alpha]$, где $f(X)\in k[X]$. Существуют многочлены $q(X)$, $r(X)\in k[X]$, такие, что $\deg r<d$ и

$$f(X)=q(X)p(X)+r(X).$$

Тогда $f(\alpha)=r(\alpha)$ и мы видим, что $1, \alpha, \ldots, \alpha^{d-1}$ порождают $k[\alpha]$ как векторное пространство над k. Это доказывает наше предложение.

Пусть E, F — расширения поля k. Если E и F содержатся в некотором поле L, то мы обозначаем через EF наименьшее подполе в L, содержащее и E, и F, и называем его *композитом* E и F в L.

Если не заданы вложения E, F в общее поле L, то мы не можем определить их композит.

Пусть k — подполе в E, $\alpha_1, \ldots, \alpha_n$ — элементы из E. Мы обозначаем через

$$k(\alpha_1, \ldots, \alpha_n)$$

наименьшее подполе в E, содержащее k и $\alpha_1, \ldots, \alpha_n$. Его элементы состоят из всех дробей

$$\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)},$$

где f, g — многочлены от n переменных с коэффициентами в k и $g(\alpha_1, \ldots, \alpha_n) \neq 0$. Действительно, множество таких дробей образует поле, содержащее k и $\alpha_1, \ldots, \alpha_n$. Обратно, любое поле, содержащее k и

$$\alpha_1, \ldots, \alpha_n,$$

должно содержать эти дроби.

Заметим, что E является объединением всех своих подполей $k(\alpha_1, \ldots, \alpha_n)$, когда $(\alpha_1, \ldots, \alpha_n)$ пробегает все конечные подсемейства элементов из E. Можно было бы определить *композит произвольного подсемейства подполей поля* L как наименьшее подполе, содержащее все поля этого семейства. Мы говорим, что E *конечно порождено* над k, если существует конечное семейство элементов $\alpha_1, \ldots, \alpha_n$ из E, такое, что

$$E = k(\alpha_1, \ldots, \alpha_n).$$

Мы видим, что E есть композит всех своих конечно порожденных подполей над k.

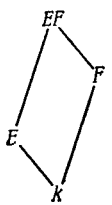
Предложение 4. *Всякое конечное расширение E поля k конечно порождено.*

Доказательство. Пусть $\{\alpha_1, \ldots, \alpha_n\}$ — базис поля E как векторного пространства над k. Тогда, очевидно, $E = k(\alpha_1, \ldots, \alpha_n)$.

Если $E = k(\alpha_1, \ldots, \alpha_n)$ — конечно порожденное поле и F — расширение поля k, причем как F, так и E содержатся в L, то

$$EF = F(\alpha_1, \ldots, \alpha_n)$$

и поле EF конечно порождено над F. Мы часто будем рисовать такую картинку:



Наклонные линии указывают на отношение включения между полями. Мы будем также называть расширение EF поля F *подъемом* E до F.

Пусть элемент α алгебраичен над полем k и F — расширение k. Предположим, что оба поля $k(\alpha)$, F содержатся в некотором поле L. Тогда α алгебраичен над F. Действительно, неприводимый многочлен для α над k a fortiori имеет коэффициенты в F и дает линейную зависимость между степенями α над F.

Пусть нам дана башня полей

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \ldots \subset k(\alpha_1, \ldots, \alpha_n),$$

причем каждое поле порождено над предыдущим одним элементом. Предположим, что каждый элемент α_i алгебраичен над k, $i = 1, \ldots, n$. В качестве частного случая нашего предыдущего замечания получаем, что α_{i+1} алгебраичен над $k(\alpha_1, \ldots, \alpha_i)$. Следовательно, каждый этаж башни — алгебраический.

Предложение 5. *Пусть $E = k(\alpha_1, \ldots, \alpha_n)$ — конечно порожденное расширение поля k, причем α_i алгебраичен над k для каждого $i = 1, \ldots, n$. Тогда E — конечное алгебраическое расширение поля k.*

Доказательство. В силу предыдущих замечаний E можно считать вершиной башни, каждый из этажей которой порождается одним алгебраическим элементом и потому является конечным по предложению 3. Ввиду следствия предложения 2 мы заключаем, что E конечно над k и что оно алгебраично — в силу предложения 1.

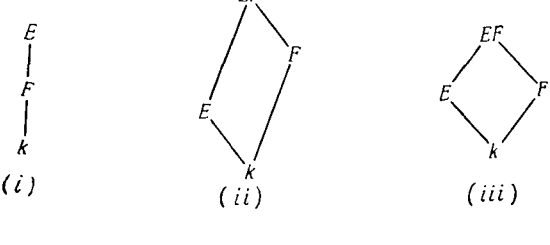
Пусть $\mathscr{C}$ — некоторый класс расширений $F \subset E$. Мы будем называть класс $\mathscr{C}$ *отмеченным*, если он удовлетворяет следующим условиям:

(i) Пусть $k \subset F \subset E$ — башня полей. Расширение $k \subset E$ принадлежит $\mathscr{C}$ тогда и только тогда, когда $k \subset F$ и $F \subset E$ принадлежат $\mathscr{C}$.

(ii) Если $k \subset E$ принадлежит $\mathscr{C}$, а F — любое расширение поля k и если E, F оба содержатся в некотором поле, то $F \subset EF$ принадлежит $\mathscr{C}$.

(iii) Если $k \subset F$ и $k \subset E$ принадлежат $\mathscr{C}$, причем F, E — подполя некоторого общего поля, то $k \subset EF$ принадлежит $\mathscr{C}$.

Указанные свойства иллюстрируются следующими диаграммами:



Эти структурные диаграммы чрезвычайно полезны при обращении с расширениями.

Заметим, что (iii) формально следует из первых двух условий. Действительно, можно рассматривать EF над k как башню с этажами $k \subset F \subset EF$.

Что касается обозначений, то иногда удобнее писать E/F вместо $F \subset E$. Это не может привести к смешению с факторгруппами, так как мы никогда не будем использовать записи E/F для обозначения соответствующей факторгруппы в тех случаях, когда E — расширение поля F.

Предложение 6. *Класс алгебраических расширений является отмеченным, и то же самое относится к классу конечных расширений.*

Доказательство. Рассмотрим сначала класс конечных расширений. Мы уже доказали условие (i). Что касается (ii), то предположим, что E/k конечно, а F — любое расширение поля k. В силу предложения 4 существуют элементы $\alpha_1, \ldots, \alpha_n \in E$, такие, что $E = k(\alpha_1, \ldots, \alpha_n)$. Тогда $EF = F(\alpha_1, \ldots, \alpha_n)$ и, следовательно, EF/F конечно порождено алгебраическими элементами. Используя предложение 5, заключаем, что EF/F конечно.

Рассмотрим теперь класс алгебраических расширений. Пусть

$$k \subset F \subset E$$

— башня. Предположим, что E алгебраично над k. Тогда a fortiori F алгебраично над k и E алгебраично над F. Обратно, предположим, что каждый этаж в башне алгебраический. Пусть $\alpha \in E$. Тогда α удовлетворяет уравнению

$$a_n \alpha^n + \ldots + a_0 = 0,$$

где $a_i \in F$, причем не все $a_i = 0$. Пусть $F_0 = k(a_n, \ldots, a_0)$. Тогда F_0 конечно над k в силу предложения 5 и α алгебраичен над F_0. Из наличия башни

$$k \subset F_0 = k(a_n, \ldots, a_0) \subset F_0(\alpha)$$

и из того факта, что каждый этаж в этой башне конечен, заключаем, что $F_0(\alpha)$ конечно над k, следовательно, α алгебраичен над k. Это доказывает, что E алгебраично над k и что, таким образом, условие (i) выполняется для алгебраических расширений. Выполнение условия (ii) уже отмечалось раньше: при подъеме алгебраический элемент остается алгебраическим и, следовательно, алгебраическое расширение при подъеме также остается алгебраическим.

Замечание. Верно, что конечно порожденные расширения также образуют отмеченный класс, но рассуждение, необходимое для дока-

зательства условия (i), может быть выполнено лишь с применением более сложной техники, чем та, которой мы располагаем сейчас. См. главу о трансцендентных расширениях.

§ 2. *Алгебраическое замыкание*

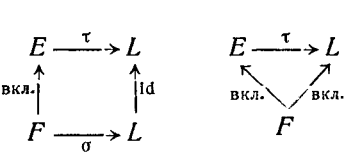
В этом и в следующем параграфе мы будем иметь дело с вложениями одного поля в другое. В связи с этим введем соответствующую терминологию.

Пусть E — расширение поля F, и пусть

$$\sigma\colon F \to L$$

— вложение (т. е. инъективный гомоморфизм) F в L. Тогда σ индуцирует изоморфизм поля F с его образом σF, который мы иногда будем обозначать также через F^σ. Вложение τ поля E в L называется *вложением над* σ, если ограничение τ на F равно σ. Мы говорим также, что τ *продолжает* σ. Если σ — тождественное вложение, то мы говорим, что τ есть *вложение* поля E *над* F.

Эти определения можно было бы дать и в более общих категориях, поскольку все зависит лишь от того, имеют ли смысл диаграммы



Замечание. Пусть $f(X) \in F(X)$ — многочлен, скажем $f(X) = a_0 + \ldots + a_n X^n$, и пусть α — корень f в E. Тогда

$$0 = f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n.$$

Если, как и выше, τ продолжает σ, то мы видим, что $\tau\alpha$ будет корнем многочлена f^σ, поскольку

$$0 = \tau(f(\alpha)) = a_0^\sigma + a_1^\sigma(\tau\alpha) + \ldots + a_n^\sigma(\tau\alpha)^n.$$

Здесь мы пишем a^σ вместо $\sigma(a)$. Это экспоненциальное обозначение часто бывает удобно и будет неоднократно использоваться в дальнейшем. Аналогично мы пишем F^σ вместо $\sigma(F)$ или σF.

При изучении вложений нам будет полезна одна лемма, относящаяся к вложениям алгебраических расширений в себя. Предварительно отметим, что если $\sigma\colon E \to L$ — вложение над k (т. е. индуцирующее тождественное отображение на k), то σ можно рассматривать как k-гомоморфизм векторных пространств, потому что и E, и L могут рассматриваться как векторные пространства над k.

Лемма 1. *Пусть E — алгебраическое расширение поля k, и пусть σ: $E \to E$ — вложение E в себя над k. Тогда σ — автоморфизм.*

Доказательство. Так как гомоморфизм σ инъективен, то достаточно доказать, что он сюръективен. Пусть α — произвольный элемент из E, $p(X)$ — его неприводимый многочлен над k и E' — подполе в E, порожденное всеми корнями многочлена $p(X)$, лежащими в E. Тогда E' — конечно порожденное и, следовательно, будет конечным расширением над k. Кроме того, σ должно переводить всякий корень многочлена $p(X)$ в корень того же самого многочлена и, следовательно, σ отображает E' в себя. Мы можем рассматривать σ как k-гомоморфизм векторных пространств, поскольку σ индуцирует тождественное отображение на k. Так как отображение σ инъективно, то образ $\sigma(E')$ есть подпространство в E', имеющее ту же размерность, что и $[E'\colon k]$. Следовательно, $\sigma(E') = E'$. Так как $\alpha \in E'$, то отсюда вытекает, что α лежит в образе отображения σ, и наша лемма доказана.

Пусть E, F — расширения поля k, содержащиеся в некотором большем поле L. Мы можем образовать кольцо $E[F]$, порожденное элементами F над E. Тогда EF будет полем частных этого кольца, а также полем частных кольца $F[E]$. Ясно, что элементы из $E[F]$ могут быть записаны в виде

$$a_1 b_1 + \ldots + a_n b_n,$$

где $a_i \in E$ и $b_i \in F$. Таким образом, EF есть поле отношений этих элементов.

Лемма 2. *Пусть E_1, E_2 — расширения поля k, содержащиеся в некотором большем поле E, и пусть σ — вложение поля E в поле L. Тогда $\sigma(E_1 E_2) = \sigma(E_1)\,\sigma(E_2)$.*

Доказательство. Применяя σ к отношению элементов указанного выше вида, скажем

$$\sigma\left(\frac{a_1 b_1 + \ldots + a_n b_n}{a_1' b_1' + \ldots + a_m' b_m'}\right) = \frac{a_1^\sigma b_1^\sigma + \ldots + a_n^\sigma b_n^\sigma}{a_1'^\sigma b_1'^\sigma + \ldots + a_m'^\sigma b_m'^\sigma},$$

мы видим, что образом служит элемент из $\sigma(E_1)\,\sigma(E_2)$. Отсюда ясно, что образ $\sigma(E_1 E_2)$ есть $\sigma(E_1)\,\sigma(E_2)$.

Пусть k — поле, $f(X)$ — многочлен степени $\geqslant 1$ из $k[X]$. Рассмотрим задачу отыскания такого расширения E поля k, в котором f имеет корень. Если $p(X)$ — неприводимый многочлен в $k[X]$, делящий $f(X)$, то любой корень $p(X)$ будет также корнем $f(X)$, так что мы можем ограничиться неприводимыми многочленами.

Пусть $p(X)$ — неприводимый многочлен. Канонический гомоморфизм

$$\sigma\colon\ k[X]\to k[X]/(p(X))$$

индуцирует на k гомоморфизм, ядром которого служит 0, поскольку всякий ненулевой элемент из k, будучи обратимым в k, порождает единичный идеал, а 1 не лежит в ядре. Пусть ξ — образ X при гомоморфизме σ, т. е. $\xi=\sigma(X)$ есть класс вычетов $X \bmod p(X)$. Тогда

$$p^{\sigma}(\xi)=p^{\sigma}(X^{\sigma})=(p(X))^{\sigma}=0.$$

Следовательно, элемент ξ есть корень многочлена p^{σ} и как таковой алгебраичен над σk. Таким образом, мы нашли расширение поля σk, а именно $\sigma k(\xi)$, в котором p^{σ} имеет корень.

С помощью несложного теоретико-множественного рассуждения мы сейчас докажем

Предложение 7. *Пусть k — поле и f — многочлен из $k[X]$ степени $\geqslant 1$. Существует расширение E поля k, в котором f имеет корень.*

Доказательство. Можно предполагать, что многочлен $f=p$ неприводим. Мы показали, что существуют поле F и вложение

$$\sigma\colon\ k\to F,$$

такие, что p^{σ} имеет корень ξ в F. Пусть S — множество той же мощности, что и $F-\sigma k$ (дополнение σk в F), и не пересекающееся с k. Положим $E=k\cup S$. Мы можем продолжить $\sigma\colon k\to F$ до биекции E на F. Определим теперь на E структуру поля. Если $x, y\in E$, то полагаем

$$xy=\sigma^{-1}(\sigma(x)\,\sigma(y)),$$

$$x+y=\sigma^{-1}(\sigma(x)+\sigma(y)).$$

При ограничении на k эти операции совпадают с заданными операциями сложения и умножения нашего исходного поля k и ясно, что k есть подполе в E. Положим $\alpha=\sigma^{-1}(\xi)$. Тогда ясно также, что $p(\alpha)=0$, что и требовалось доказать.

Следствие. *Пусть k — поле и $f_1, \ldots, f_n$ — многочлены из $k[X]$ степеней $\geqslant 1$. Тогда существует расширение E поля k, в котором каждый f_i имеет корень, $i=1, \ldots, n$.*

Доказательство. Пусть E_1 — расширение, в котором f_1 имеет корень. Мы можем рассматривать f_2 как многочлен над E_1. Пусть E_2 — расширение E_1, в котором f_2 имеет корень. Продолжая по индукции, немедленно получаем наше следствие.

Поле L называется *алгебраически замкнутым*, если всякий многочлен из $L[X]$ степени $\geqslant 1$ имеет в L корень.

Теорема 1. *Для всякого поля k существует алгебраически замкнутое поле L, содержащее k в качестве подполя.*

Доказательство. Сначала мы построим расширение E_1 поля k, в котором всякий многочлен из $k[X]$ степени $\geqslant 1$ имеет корень. Можно действовать следующим образом (Артин). Каждому многочлену f из $k[X]$ степени $\geqslant 1$ сопоставим символ X_f. Пусть S—множество всех таких символов X_f (так что S находится в биективном соответствии с множеством многочленов из $k[X]$ степени $\geqslant 1$). Образуем кольцо многочленов $k[S]$. Мы утверждаем, что идеал, порожденный всеми многочленами $f(X_f)$ в $k[S]$, не является единичным. Если бы это было не так, то существовала бы конечная комбинация элементов из нашего идеала, равная 1:

$$g_1 f_1(X_{f_1}) + \ \ldots \ + g_n f_n(X_{f_n}) = 1,$$

где $g_i \in k[S]$. Для простоты будем писать X_i вместо X_{f_i}. Многочлены g_i включают в действительности только конечное число переменных, скажем $X_1, \ldots, X_N$ (где $N \geqslant n$). Наше соотношение тогда гласит:

$$\sum_{i=1}^{n} g_i(X_1, \ \ldots, \ X_N) f_i(X_i) = 1.$$

Пусть F — конечное расширение, в котором каждый многочлен $f_1, \ldots, f_n$ имеет корень, скажем α_i есть корень f_i в F при $i = 1, \ldots, n$. Положим $\alpha_i = 0$ при $i > n$. Подставив α_i вместо X_i в наше соотношение, мы получим $0 = 1$ — противоречие.

Пусть $\mathfrak{m}$ — максимальный идеал, содержащий идеал, порожденный всеми многочленами $f(X_f)$ в $k[S]$. Тогда $k[S]/\mathfrak{m}$ — поле и мы имеем каноническое отображение

$$\sigma\colon \ k[S] \to k[S]/\mathfrak{m}.$$

Для всякого многочлена $f \in k[X]$ степени $\geqslant 1$ многочлен f^{σ} имеет корень в поле $k[S]/\mathfrak{m}$, которое является расширением поля σk. Используя теоретико-множественное рассуждение того же типа, что и в предложении 7, мы заключаем, что существует расширение E_1 поля k, в котором каждый многочлен $f \in k[X]$ степени $\geqslant 1$ имеет корень.

По индукции мы можем построить такую последовательность полей

$$E_1 \subset E_2 \subset E_3 \subset \ldots \subset E_n \subset \ldots,$$

что каждый многочлен из $E_n[X]$ степени $\geqslant 1$ имеет корень в E_{n+1}. Пусть E — объединение всех полей E_n, $n=1, 2, \ldots$. Тогда E, естественно, является полем, поскольку для любых $x, y \in E$ найдется номер n, такой, что $x, y \in E_n$, и мы можем взять произведение xy или сумму $x+y$ в E_n. Эти операции, очевидно, не зависят от выбора того n, для которого $x, y \in E_n$, и определяют структуру поля на E. Всякий многочлен из $E[X]$ имеет коэффициенты в некотором подполе E_n и, следовательно, обладает корнем в E_{n+1}, а тем самым и корнем в E, что и требовалось доказать.

Следствие. *Для всякого поля k существует расширение $\bar{k}$, алгебраическое над k и алгебраически замкнутое.*

Доказательство. Пусть E — алгебраически замкнутое расширение поля k, и пусть $\bar{k}$ — объединение всех подрасширений из E, алгебраических над k. Тогда $\bar{k}$ алгебраично над k. Пусть элемент $\alpha \in E$ алгебраичен над $\bar{k}$. Тогда α алгебраичен над k в силу предложения 6. Если f — многочлен степени $\geqslant 1$ из $\bar{k}[X]$, то f имеет корень α в E и алгебраичен над $\bar{k}$. Следовательно, α лежит в $\bar{k}$ и $\bar{k}$ алгебраически замкнуто.

Заметим, что если L — алгебраически замкнутое и $f \in L[X]$ имеет степень $\geqslant 1$, то существует $c \in L$ и $\alpha_1, \ldots, \alpha_n \in L$, такие, что

$$f(X) = c(X-\alpha_1) \ldots (X-\alpha_n).$$

Действительно, f имеет корень α_1 в L, так что $f(X) = (X-\alpha_1)g(X)$, где $g(X) \in L[X]$. Если $\deg g \geqslant 1$, то мы можем повторить это рассуждение и по индукции представить f в виде произведения членов $(X-\alpha_i)$ $(i=1, \ldots, n)$ и некоторого элемента $c \in L$. Отметим, что c совпадает со старшим коэффициентом многочлена f, т. е.

$$f(X) = cX^n + \text{члены меньшей степени.}$$

Следовательно, если коэффициенты f лежат в подполе k поля L, то $c \in k$.

Пусть k — поле и $\sigma\colon k \to L$ — вложение k в алгебраически замкнутое поле L. Мы хотим исследовать продолжения σ на алгебраические расширения E поля k. Начнем с рассмотрения частного случая, когда E порождено одним элементом.

Пусть $E = k(\alpha)$, где α алгебраичен над k,

$$p(X) = \operatorname{Irr}(\alpha, k, X).$$

Пусть β — корень многочлена p^σ в L. Всякий данный элемент из $k(\alpha) = k[\alpha]$ мы можем записать в виде $f(\alpha)$, где $f(X) \in k[X]$ — некоторый многочлен. Определим продолжение σ как отображение

$$f(\alpha) \mapsto f^\sigma(\beta).$$

Это отображение, на самом деле, правильно определено, т. е. не зависит от выбора многочлена $f(X)$, использованного для представления нашего элемента в $k[\alpha]$. Действительно, если многочлен $g(X)$ лежит в $k[X]$ и таков, что $g(\alpha)=f(\alpha)$, то $(g-f)(\alpha)=0$, а потому $p(X)$ делит $g(X)-f(X)$. Следовательно, $p^\sigma(X)$ делит $g^\sigma(X)-f^\sigma(X)$ и, таким образом, $g^\sigma(\beta)=f^\sigma(\beta)$. Далее, очевидно, что наше отображение есть гомоморфизм, индуцирующий σ на k, и что оно служит продолжением σ на $k(\alpha)$. Таким образом, получаем

Предложение 8. *Число возможных продолжений σ на $k(\alpha)$ не превосходит числа корней многочлена p, а именно равно числу различных корней p.*

Это важный факт, который мы позже проанализируем подробнее. А сейчас нас интересуют продолжения σ на произвольные алгебраические расширения k. Мы получим их, используя лемму Цорна.

Теорема 2. *Пусть k — поле, E — его алгебраическое расширение и $\sigma\colon k\to L$ — вложение k в алгебраически замкнутое поле L. Тогда существует продолжение σ до вложения E в L. Если E алгебраически замкнуто и L алгебраично над σk, то любое такое продолжение σ будет изоморфизмом поля E на L.*

Доказательство. Пусть S — множество всех пар (F, τ), где F — подполе в E, содержащее k, и τ — продолжение σ до вложения F в L. Мы пишем $(F, \tau)\leqslant(F', \tau')$ для таких пар (F, τ) и (F', τ'), если $F\subset F'$ и $\tau'\mid F=\tau$. Отметим, что множество S не пусто [оно содержит (k, σ)] и индуктивно упорядочено: если $\{(F_i, \tau_i)\}$ линейно упорядоченное подмножество, то положим $F=\bigcup F_i$ и определим τ на F, положив его равным τ_i на каждом F_i. Тогда (F, τ) служит верхней гранью для этого линейно упорядоченного подмножества. Применяя лемму Цорна, находим (K, λ)—максимальный элемент в S. Тогда λ есть продолжение σ, и мы утверждаем, что $K=E$. В противном случае существует $\alpha\in E$, $\alpha\notin K$; в силу предыдущего вложение λ имеет продолжение на $K(\alpha)$ вопреки максимальности (K, λ). Таким образом, существует продолжение σ на E. Мы обозначаем это продолжение снова через σ.

Если E алгебраически замкнуто и L алгебраично над σk, то σE алгебраически замкнуто и L алгебраично над $\sigma(E)$, следовательно, $L=\sigma E$.

В качестве следствия получаем некую теорему единственности для „алгебраического замыкания“ поля k.

Следствие. *Пусть k — поле и E, E' — алгебраические расширения над k. Предположим, что E, E' алгебраически замкнуты. Тогда существует изоморфизм*

$$\tau\colon E\xrightarrow{\sim}E'$$

поля E на E', индуцирующий тождественное отображение на k.

Доказательство. Продолжим тождественное отображение поля k до вложения E в E' и применим теорему.

Мы видим, что алгебраически замкнутое и алгебраическое расширение поля k определено однозначно с точностью до изоморфизма. Всякое такое расширение будет называться *алгебраическим замыканием* k и будет обозначаться через $\bar{k}$. Фактически, если не оговорено противное, символ $\bar{k}$ мы будем использовать только для обозначения алгебраического замыкания.

Теперь стоит рассмотреть общую ситуацию с изоморфизмами и автоморфизмами в общих категориях.

Пусть $\mathcal{A}$ — категория и A, B — объекты в $\mathcal{A}$. Обозначим через $\mathrm{Iso}(A, B)$ множество изоморфизмов A на B. Предположим, что существует по крайней мере один такой изоморфизм $\sigma\colon A \to B$ с обратным $\sigma^{-1}\colon B \to A$. Если φ — автоморфизм объекта A, то $\sigma \circ \varphi\colon A \to B$ — снова изоморфизм. Аналогично, если ψ — автоморфизм B, то $\psi \circ \sigma\colon A \to B$ — снова изоморфизм. Кроме того, группы автоморфизмов $\mathrm{Aut}(A)$ и $\mathrm{Aut}(B)$ изоморфны относительно взаимно обратных отображений

$$\varphi \longmapsto \sigma \circ \varphi \circ \sigma^{-1},$$
$$\sigma^{-1} \circ \psi \circ \sigma \longleftarrow \psi.$$

Автоморфизм $\sigma \circ \varphi \circ \sigma^{-1}$ определяется тем, что делает коммутативной следующую диаграмму:

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & B \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\sigma\circ\varphi\circ\sigma^{-1}} \\ A & \xrightarrow[\sigma]{} & B \end{array}$$

Аналогичную диаграмму имеем и для $\sigma^{-1} \circ \psi \circ \sigma$.

Пусть $\tau\colon A \to B$ — какой-нибудь другой изоморфизм. Тогда $\tau^{-1} \circ \sigma$ есть автоморфизм объекта A и $\tau \circ \sigma^{-1}$ — автоморфизм B. Таким образом, два изоморфизма отличаются на автоморфизм (объекта A или B). Мы видим, что группа $\mathrm{Aut}(B)$ действует на множестве $\mathrm{Iso}(A, B)$ слева, а $\mathrm{Aut}(A)$ — на множестве $\mathrm{Iso}(A, B)$ справа.

Мы видим также, что группа $\mathrm{Aut}(A)$ определена однозначно с точностью до отображения, аналогичного сопряжению. Это совершенно не похоже на тот тип единственности, который свойствен универсальным объектам в категории. Такие объекты имеют лишь тождественный автоморфизм и, следовательно, определены с точностью до однозначно определенного изоморфизма.

Не так обстоит дело в случае алгебраического замыкания поля, которое обычно имеет большое количество автоморфизмов. Бо́льшая

часть этой главы и вся следующая глава посвящены изучению этих автоморфизмов.

Примеры. Позже в этой книге будет доказано, что поле комплексных чисел алгебраически замкнуто. Комплексное сопряжение является автоморфизмом поля $\mathbf{C}$. Имеется и еще много автоморфизмов, но уже не непрерывных. Мы рассмотрим другие возможные автоморфизмы в главе о трансцендентных расширениях. Подполе поля $\mathbf{C}$, состоящее из всех чисел, алгебраических над $\mathbf{Q}$, есть алгебраическое замыкание $\overline{\mathbf{Q}}$ поля $\mathbf{Q}$. Легко видеть, что $\overline{\mathbf{Q}}$ счетно. Действительно, докажите в качестве упражнения следующее утверждение.

Если k — поле, не являющееся конечным, то любое алгебраическое расширение над k имеет ту же мощность, что и k.

(Если k счетно, то можно сначала перенумеровать все многочлены над k, а затем перенумеровать все элементы произвольного алгебраического расширения.)

В частности, $\overline{\mathbf{Q}} \neq \mathbf{C}$. Для поля $\mathbf{R}$ вещественных чисел $\overline{\mathbf{R}} = \mathbf{C}$.

Если k — конечное поле, то алгебраическое замыкание $\bar{k}$ поля k счетно. Позднее в этой главе мы во всех подробностях опишем природу алгебраических расширений конечных полей.

Не все интересные поля являются подполями поля комплексных чисел. Например, представляет интерес исследовать алгебраические расширения поля $\mathbf{C}(X)$, где X — переменная над $\mathbf{C}$. Изучение этих расширений равносильно изучению разветвленных накрытий сферы (рассматриваемой как риманова поверхность), и фактически имеется точная информация о природе таких расширений, поскольку известна фундаментальная группа сферы, из которой выколото конечное число точек. Мы вернемся к этому примеру позднее, когда будем рассматривать группы Галуа.

§ 3. Поля разложения и нормальные расширения

Пусть k — поле, f — многочлен из $k[X]$ степени $\geqslant 1$. Под *полем разложения* K многочлена f мы будем понимать расширение K поля k, в котором f разлагается на линейные множители, т. е.

$$f(X) = c(X - \alpha_1) \ldots (X - \alpha_n),$$

где $\alpha_i \in K$, $i = 1, \ldots, n$, причем $K = k(\alpha_1, \ldots, \alpha_n)$ порождается всеми корнями f.

Теорема 3. *Пусть K — поле разложения многочлена $f(X) \in k[X]$. Если E — какое-нибудь другое поле разложения f, то существует изоморфизм σ: $E \to K$, индуцирующий тождествен-*

ное отображение на k. Если $k \subset K \subset \bar{k}$, где $\bar{k}$ — алгебраическое замыкание k, то любое вложение поля E в $\bar{k}$, индуцирующее тождественное отображение на k, — обязательно изоморфизм E на K.

Доказательство. Пусть $\bar{K}$—алгебраическое замыкание поля K. Тогда $\bar{K}$ алгебраично над k и, следовательно, является его алгебраическим замыканием. В силу теоремы 2 существует вложение

$$\sigma\colon E \to \bar{K},$$

индуцирующее тождественное отображение на k. Имеем разложение на множители

$$f(X) = c(X - \beta_1) \ldots (X - \beta_n),$$

где $\beta_i \in E$, $i = 1, \ldots, n$. Старший коэффициент c лежит в k. Получаем

$$f(X) = f^{\sigma}(X) = c(X - \sigma\beta_1) \ldots (X - \sigma\beta_n).$$

Но в $\bar{K}[X]$ разложение на множители однозначно. Так как f имеет в $K[X]$ разложение

$$f(X) = c(X - \alpha_1) \ldots (X - \alpha_n),$$

то набор $(\sigma\beta_1, \ldots, \sigma\beta_n)$ отличается от $(\alpha_1, \ldots, \alpha_n)$ только перестановкой. Отсюда заключаем, что $\sigma\beta_i \in K$ для $i = 1, \ldots, n$ и что, следовательно, $\sigma E \subset K$. Но $K = k(\alpha_1, \ldots, \alpha_n) = k(\sigma\beta_1, \ldots, \sigma\beta_n)$ и, значит, $\sigma E = K$, поскольку $E = k(\beta_1, \ldots, \beta_n)$. Это доказывает нашу теорему.

Отметим, что всякий многочлен $f(X) \in k[X]$ имеет поле разложения, а именно поле, порожденное всеми его корнями в данном алгебраическом замыкании $\bar{k}$ поля k.

Пусть I — некоторое множество индексов и $\{f_i\}_{i \in I}$ — семейство многочленов из $k[X]$ степеней $\geqslant 1$. Под *полем разложения* для этого семейства мы будем понимать расширение K поля k, такое, что всякий f_i разлагается в $K[X]$ на линейные множители, причем K порождается всеми корнями всех многочленов f_i, $i \in I$. В большинстве приложений мы будем иметь дело с конечным множеством индексов I, но рассмотрение бесконечных алгебраических расширений приобретает все большее значение, и мы с ними систематически будем сталкиваться. Следует также заметить, что доказательства различных утверждений, которые мы будем приводить, не стали бы проще, если бы мы ограничились конечными расширениями.

Пусть $\bar{k}$ — алгебраическое замыкание поля k, K_i — поле разложения многочлена f_i в $\bar{k}$. Композит полей K_i будет полем разложения для нашего семейства, так как оба условия, определяющие поле

разложения, очевидно, выполняются. Кроме того, теорема 3 немедленно распространяется на бесконечный случай.

Следствие. *Пусть K — поле разложения для семейства $\{f_i\}_{i\in I}$ и E — какое-нибудь другое поле разложения. Любое вложение E в $\bar{K}$, индуцирующее тождественное отображение на k, определяет изоморфизм E на K.*

Доказательство. Мы сохраняем предыдущие обозначения. Заметим, что E содержит однозначно определенное поле разложения E_i многочлена f_i и K содержит однозначно определенное поле разложения K_i многочлена f_i. Любое вложение σ поля E в $\bar{K}$ должно отображать E_i на K_i в силу теоремы 3 и, следовательно, переводить E в K. Так как K есть композит полей K_i, наше отображение σ должно переводить E на K и, следовательно, оно индуцирует изоморфизм E на K.

Замечание. Если I конечно и $f_1, \ldots, f_n$ — наши многочлены, то поле разложения для них — это поле разложения для одного многочлена $f(X) = f_1(X) \ldots f_n(X)$, являющегося их произведением. Однако, даже если ограничиться только конечными расширениями, удобнее иметь дело сразу с множествами многочленов, а не с одним многочленом.

Теорема 4. *Пусть K — алгебраическое расширение поля k, содержащееся в некотором его алгебраическом замыкании $\bar{k}$. Тогда следующие условия эквивалентны:*

НОР 1. *Всякое вложение σ поля K в $\bar{k}$ над k является автоморфизмом поля K.*

НОР 2. *K — поле разложения некоторого семейства многочленов в $k[X]$.*

НОР 3. *Всякий неприводимый в $k[X]$ многочлен, имеющий корень в K, разлагается в K на линейные множители.*

Доказательство. Предположим, что выполняется НОР 1. Пусть α — элемент из K, $p_\alpha(X)$ — его неприводимый многочлен над k и β — корень многочлена p_α в $\bar{k}$. Тогда существует изоморфизм поля $k(\alpha)$ на $k(\beta)$ над k, отображающий α в β. Продолжим этот изоморфизм до вложения K в $\bar{k}$. Это продолжение есть по предположению автоморфизм σ поля K, и, следовательно, $\sigma\alpha = \beta$ лежит в K.

Значит, всякий корень многочлена p_α лежит в K и p_α разлагается на линейные множители в $K[X]$. Следовательно, K есть поле разложения для семейства $\{p_\alpha\}_{\alpha\in K}$, где α пробегает все элементы поля K, и тем самым выполняется НОР 2.

Обратно, предположим, что выполняется НОР 2, и пусть $\{f_i\}_{i\in I}$ — семейство многочленов, для которых K служит полем разложения. Если α — корень некоторого f_i в K, то мы знаем, что $\sigma\alpha$ также будет его корнем для любого вложения σ поля K в $\bar{k}$ над k. Так как K порождается корнями всех многочленов f_i, то σ отображает K в себя. Теперь, чтобы заключить, что σ — автоморфизм, применяем лемму 1.

Доказательство того факта, что НОР 1 влечет НОР 2, показывает также, что при этом выполняется и НОР 3. Обратно, предположим, что выполняется НОР 3. Пусть σ — вложение K в $\bar{k}$ над k. Пусть $\alpha\in K$ и $p(X)$ — неприводимый многочлен элемента α над k. Так как σ — вложение K в $\bar{k}$ над k, то σ отображает α в корень β многочлена $p(X)$, а по предположению β лежит в K. Следовательно, $\sigma\alpha$ лежит в K и σ отображает K в себя. Из леммы 1 вытекает, что σ — автоморфизм.

Расширение K поля k, удовлетворяющее условиям НОР 1, НОР 2, НОР 3, будет называться *нормальным*. Не верно, что класс нормальных расширений является отмеченным. Например, легко показать, что всякое расширение степени 2 нормально, но расширение $\mathbf{Q}\left(\sqrt[4]{2}\right)$ поля рациональных чисел не является нормальным (комплексные корни многочлена X^4-2 в нем не содержатся). Тем не менее это расширение получается последовательными расширениями степени 2, а именно

$$E=\mathbf{Q}\left(\sqrt[4]{2}\right)\supset F\supset\mathbf{Q},$$

где

$$F=\mathbf{Q}(\alpha),\quad \alpha=\sqrt{2}\quad\text{и}\quad E=F\left(\sqrt{\alpha}\right).$$

Таким образом, башня нормальных расширений не обязательно нормальна. Однако некоторые свойства отмеченного класса все же имеют место.

Теорема 5. *Нормальные расширения остаются нормальными при подъеме. Если $K\supset E\supset k$ и K нормально над k, то K нормально над E. Если K_1, K_2 нормальны над k и содержатся в некотором поле L, то K_1K_2 нормально над k и то же самое справедливо для $K_1\cap K_2$.*

Доказательство. Для доказательства нашего первого утверждения предположим, что K нормально над k и F — произвольное расширение поля k. Допустим, что K, F содержатся в некотором большем поле L. Пусть σ — вложение KF над F (в $\bar{L}$). Тогда отображение σ тождественно на F и, следовательно, на k и по предположению его ограничение на K отображает K в себя. Получаем $(KF)^\sigma=K^\sigma F^\sigma=KF$, т. е. KF нормально над F.

Предположим, что $K \supset E \supset k$ и что K нормально над k. Пусть σ — некоторое вложение K над E. Тогда σ есть также вложение K над k, и наше утверждение справедливо по определению.

Наконец, если K_1, K_2 нормальны над k, то для любого вложения σ поля K_1K_2 над k имеем

$$\sigma(K_1K_2) = \sigma(K_1)\,\sigma(K_2),$$

и наше утверждение снова вытекает из сделанных предположений. Утверждение, касающееся пересечения, справедливо потому, что

$$\sigma(K_1 \cap K_2) = \sigma(K_1) \cap \sigma(K_2).$$

Заметим, что если K — конечно порожденное нормальное расширение над k, скажем $K = k(\alpha_1, \ldots, \alpha_n)$, и $p_1, \ldots, p_n$ — соответствующие неприводимые многочлены для $\alpha_1, \ldots, \alpha_n$ над k, то K есть уже поле разложения для конечного семейства $p_1, \ldots, p_n$. Позже мы исследуем, когда K будет полем разложения для одного неприводимого многочлена.

§ 4. Сепарабельные расширения

Пусть E — алгебраическое расширение поля F и

$$\sigma\colon F \to L$$

— вложение F в алгебраически замкнутое поле L. Исследуем более подробно продолжения σ на E. Любое такое продолжение σ отображает E на подполе в L, алгебраическое над σF. Таким образом, для наших целей мы можем предполагать, что L алгебраично над σF и, следовательно, совпадает с алгебраическим замыканием поля σF.

Обозначим через S_σ множество продолжений σ до вложения E в L.

Пусть L' — другое алгебраически замкнутое поле, и пусть $\tau\colon F \to L'$ — вложение. Мы предполагаем, как и выше, что L' есть алгебраическое замыкание поля τF. В силу теоремы 2 существует изоморфизм $\lambda\colon L \to L'$, продолжающий отображение $\tau \circ \sigma^{-1}$, определенное на σF. Это иллюстрируется следующей диаграммой:

$$\begin{array}{ccc} L' & \xleftarrow{\lambda} & L \\ | & \xleftarrow{\quad} E \xrightarrow{\sigma^*} & | \\ | & | & | \\ \tau F & \xleftarrow[\tau]{} F \xrightarrow[\sigma]{} & \sigma F \end{array}$$

Обозначим через S_τ множество вложений E в L', продолжающих τ.

Если $\sigma^* \in S_\sigma$ — продолжение σ до вложения E в L, то $\lambda \circ \sigma^*$ будет продолжением τ до вложения E в L', поскольку при ограничении на F мы имеем

$$\lambda \circ \sigma^* = \tau \circ \sigma^{-1} \circ \sigma = \tau.$$

Таким образом, λ индуцирует отображение S_σ в S_τ. Ясно, что обратное отображение индуцируется изоморфизмом λ^{-1} и, следовательно, S_σ, S_τ приводятся во взаимно однозначное соответствие отображением

$$\sigma^* \to \lambda \circ \sigma^*.$$

В частности, мощность S_σ, S_τ одна и та же. Таким образом, эта мощность зависит только от расширения E/F; мы будем обозначать ее через

$$[E : F]_s$$

и называть *сепарабельной степенью* E над F. Она представляет интерес главным образом в том случае, когда E/F конечно.

Теорема 6. *Для всякой башни* $E \supset F \supset k$

$$[E : k]_s = [E : F]_s [F : k]_s.$$

Если, кроме того, E конечно над k, то $[E: k]_s$ *конечна и*

$$[E : k]_s \leqslant [E : k].$$

Таким образом, сепарабельная степень не превосходит степени.

Доказательство. Пусть σ: $k \to L$ — вложение поля k в алгебраически замкнутое поле L, $\{\sigma_i\}_{i \in I}$ — семейство различных продолжений σ на F, и для каждого i пусть $\{\tau_{ij}\}$ — семейство различных продолжений σ_i на E. В силу доказанного выше каждое σ_i имеет ровно $[E : F]_s$ продолжений до вложения E в L. Множество вложений $\{\tau_{ij}\}$ содержит ровно

$$[E : F]_s [F : k]_s$$

элементов. Всякое вложение E в L над σ должно быть одним из τ_{ij}, и, таким образом, мы видим, что первая формула выполняется, т. е. имеет место мультипликативность сепарабельных степеней в башнях.

Что касается второго утверждения, то предположим, что E/k конечно. Тогда мы можем получить E как башню расширений, каждый этаж которой порождается одним элементом

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \ldots \subset k(\alpha_1, \ldots, \alpha_r) = E.$$

Если мы определим индуктивно $F_{\nu+1} = F_\nu(\alpha_{\nu+1})$, то в силу предложения 8 из § 2 будем иметь

$$[F_\nu(\alpha_{\nu+1}) : F_\nu]_s \leqslant [F_\nu(\alpha_{\nu+1}) : F_\nu].$$

Таким образом, наше неравенство выполняется для каждого этажа башни. В силу мультипликативности отсюда вытекает, что неравенство справедливо для расширения E/k, что и требовалось показать.

Следствие. *Пусть E конечно над k и $E \supset F \supset k$. Равенство* $[E : k]_s = [E : k]$ *выполняется тогда и только тогда, когда соот-*

ветствующее равенство выполняется для каждого этажа башни, т. е. для E/F и F/k.

Доказательство. Очевидно.

Позднее будет показано (это нетрудно показать), что $[E:k]_s$ делит степень $[E:k]$, когда E конечно над k. Определим $[E:k]_i$ как частное, так что

$$[E:k]_s\,[E:k]_i = [E:k].$$

Из мультипликативности в башнях степени и сепарабельной степени вытекает, что символ $[E:k]_i$ также мультипликативен в башнях. Мы будем иметь с ним дело в § 7.

Пусть E — конечное расширение поля k. Мы будем говорить, что E *сепарабельно* над k, если $[E:k]_s = [E:k]$. Алгебраический над k элемент α называется *сепарабельным* над k, если $k(\alpha)$ сепарабельно над k. Мы видим, что это условие эквивалентно тому, что неприводимый многочлен $\mathrm{Irr}(\alpha, k, X)$ не имеет кратных корней.

Многочлен $f(X) \in k[X]$ называется *сепарабельным*, если у него нет кратных корней. Если α — корень сепарабельного многочлена $g(X) \in k[X]$, то неприводимый многочлен элемента α над k делит g и, следовательно, α сепарабелен над k.

Сейчас мы сделаем несколько дополнительных замечаний к предложению 8. Читатель может опустить эти замечания, если он интересуется только полями характеристики 0 или сепарабельными расширениями.

Пусть $f(X) = (X-\alpha)^m g(X)$ — многочлен из $k[X]$, причем $g(X)$ не делится на $X-\alpha$. Напомним, что m называется кратностью α в f. Мы говорим, что α — *кратный* корень f, если $m > 1$. В противном случае мы говорим, что α — *простой* корень.

Предложение 9. *Пусть α — алгебраический элемент над k, $\alpha \in \bar{k}$, и пусть $f(X) = \mathrm{Irr}(\alpha, k, X)$. Если $\mathrm{char}\, k = 0$, то все корни многочлена f имеют кратность 1 (f сепарабелен). Если $\mathrm{char}\, k = p > 0$, то существует целое число $\mu \geqslant 0$, такое, что всякий корень f имеет кратность p^μ. Далее,*

$$[k(\alpha):k] = p^\mu\,[k(\alpha):k]_s$$

и элемент α^{p^μ} сепарабелен над k.

Доказательство. Пусть $\alpha_1, \ldots, \alpha_r$ — различные корни многочлена f в $\bar{k}$ и m — кратность корня $\alpha = \alpha_1$ в f. Для всякого $1 \leqslant i \leqslant r$ существует изоморфизм

$$\sigma\colon\ k(\alpha) \to k(\alpha_i)$$

над k, для которого $\sigma\alpha = \alpha_i$. Продолжим σ до автоморфизма поля $\bar{k}$; будем обозначать это продолжение по-прежнему через σ. Так как

коэффициенты f лежат в k, то $f^{\sigma} = f$. Заметим, что

$$f(X) = \prod_{i=1}^{r} (X - \sigma\alpha_i)^{m_i},$$

где m_i — кратность α_i в f. В силу однозначности разложения на множители заключаем, что $m_i = m_1$ и, следовательно, все m_i равны одному и тому же целому числу m.

Рассмотрим производную $f'(X)$. Если f и f' имеют общий корень, то α будет корнем многочлена меньшей степени, чем $\deg f$. Это невозможно, за исключением случая, когда $\deg f' = -\infty$, другими словами, когда производная f' тождественно равна 0. Если характеристика равна 0, этого не может произойти. Следовательно, если f имеет кратные корни, то мы имеем случай характеристики p и $f(X) = g(X^p)$ для некоторого многочлена $g(X) \in k[X]$. Поэтому α^p — корень многочлена g, степень которого $< \deg f$. Продолжая по индукции, мы получим наименьшее целое число $\mu \geqslant 0$, такое, что α^{p^μ} является корнем сепарабельного многочлена из $k[X]$, а именно такого многочлена h, для которого

$$f(X) = h(X^{p^\mu}).$$

Сравнивая степени f и g, заключаем, что

$$[k(\alpha) : k(\alpha^p)] = p.$$

По индукции находим

$$\left[k(\alpha) : k\left(\alpha^{p^\mu}\right)\right] = p^\mu.$$

Так как h имеет корни кратности 1, то

$$\left[k\left(\alpha^{p^\mu}\right) : k\right]_s = \left[k\left(\alpha^{p^\mu}\right) : k\right]$$

и, сравнивая степени многочленов f и h, мы видим, что число различных корней у f равно числу различных корней у h. Следовательно,

$$[k(\alpha) : k]_s = \left[k\left(\alpha^{p^\mu}\right) : k\right]_s.$$

Отсюда наша формула для степеней вытекает в силу мультипликативности, так что утверждение доказано. Отметим, что корнями многочлена h являются

$$\alpha_1^{p^\mu}, \ldots, \alpha_r^{p^\mu}.$$

Следствие 1. *Для любого конечного расширения E поля k сепарабельная степень $[E : k]_s$ делит степень $[E : k]$. Частное равно 1 в случае поля характеристики 0 и равно некоторой степени p в случае поля характеристики $p > 0$.*

Доказательство. Разложим E/k в башню, каждый этаж которой порождается одним элементом, и применим предложение 9 с учетом мультипликативности наших индексов в башнях.

Если E/k конечно, то мы называем

$$\frac{[E:k]}{[E:k]_s}$$

несепарабельной степенью (или *степенью несепарабельности*) и обозначаем ее через $[E:k]_i$. Таким образом,

$$[E:k]_s\,[E:k]_i = [E:k].$$

Следствие 2. *Конечное расширение сепарабельно тогда и только тогда, когда* $[E:k]_i = 1$.

Доказательство. По определению.

Следствие 3. *Если* $E \supset F \supset k$ *— два конечных расширения, то*

$$[E:k]_i = [E:F]_i\,[F:k]_i.$$

Доказательство. Очевидно.

Отметим, что если элемент α сепарабелен над k и F — произвольное расширение поля k, то α сепарабелен над F. Действительно, если f — сепарабельный многочлен из $k[X]$, для которого $f(\alpha) = 0$, то, поскольку коэффициенты f лежат также и в F, α сепарабелен и над F. (Можно сказать, что сепарабельный элемент остается сепарабельным при подъеме.)

Теорема 7. *Пусть* E *— конечное расширение поля* k. *Тогда для сепарабельности* E *над* k *необходимо и достаточно, чтобы каждый элемент из* E *был сепарабельным над* k.

Доказательство. Пусть E сепарабельно над k и $\alpha \in E$. Рассмотрим башню

$$k \subset k(\alpha) \subset E.$$

В силу теоремы 6 мы должны иметь равенство $[k(\alpha):k] = [k(\alpha):k]_s$, означающее, что α сепарабелен над k. Обратно, предположим, что каждый элемент из E сепарабелен над k. Мы можем записать $E = k(\alpha_1, \ldots, \alpha_n)$, где каждый α_i сепарабелен над k. Рассмотрим башню

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \ldots \subset k(\alpha_1, \ldots, \alpha_n).$$

Будучи сепарабельным над k, каждый элемент α_i сепарабелен над $k(\alpha_1, \ldots, \alpha_{i-1})$ при $i \geqslant 2$. Следовательно, по теореме о башне E сепарабельно над k.

Заметим, что наше последнее рассуждение показывает, что если E порождается конечным числом элементов, каждый из которых сепарабелен над k, то E сепарабельно над k.

Пусть E — произвольное алгебраическое расширение поля k. Будем говорить, что E *сепарабельно* над k, если всякое его конечно

порожденное подрасширение сепарабельно над k, т. е. если всякое расширение $k(\alpha_1, \ldots, \alpha_n)$, где $\alpha_1, \ldots, \alpha_n \in E$, сепарабельно над k.

Теорема 8. *Пусть E — алгебраическое расширение поля k, порожденное семейством $\{\alpha_i\}_{i \in I}$. Если каждый элемент α_i сепарабелен над k, то E сепарабельно над k.*

Доказательство. Всякий элемент из E лежит в некотором конечно порожденном подполе $k(\alpha_{i_1}, \ldots, \alpha_{i_n})$; как мы отметили выше, каждое такое подполе сепарабельно над k. Следовательно, в силу теоремы 7, всякий элемент из E сепарабелен над k, что и завершает доказательство.

Теорема 9. *Сепарабельные расширения образуют отмеченный класс расширений.*

Доказательство. Пусть E сепарабельно над k и $E \supset F \supset k$. Всякий элемент из E сепарабелен над F, и всякий элемент из F, будучи элементом из E, сепарабелен над k. Следовательно, каждый этаж в башне сепарабелен. Обратно, предположим, что $E \supset F \supset k$ — некоторое расширение, для которого E/F сепарабельно и F/k сепарабельно. Если E конечно над k, то мы можем применить теорему 6. А именно мы имеем равенство сепарабельной степени и степени в каждом этаже башни, откуда в силу мультипликативности вытекает равенство степеней для E над k.

Пусть теперь E бесконечно и $\alpha \in E$. Тогда α будет корнем сепарабельного многочлена $f(X)$ с коэффициентами из F. Пусть этими коэффициентами будут $a_n, \ldots, a_0$. Положим $F_0 = k(a_n, \ldots, a_0)$. Тогда F_0 сепарабельно над k и α сепарабелен над F_0. Теперь из рассмотрения конечной башни

$$k \subset F_0 \subset F_0(\alpha)$$

заключаем, что $F_0(\alpha)$ сепарабельно над k и что, следовательно, α сепарабелен над k. Это доказывает условие (i) в определении „отмеченности".

Пусть E сепарабельно над k и F — произвольное расширение поля k, причем оба расширения E, F являются подполями некоторого поля. Всякий элемент из E сепарабелен над k, а потому сепарабелен над F. Так как EF порождается над F всеми элементами из E, то EF сепарабельно над F в силу теоремы 8. Это доказывает условие (ii) в определении „отмеченности" и завершает доказательство нашей теоремы.

Пусть E — конечное расширение над k. Пересечение всех нормальных расширений K поля k (в алгебраическом замыкании $\overline{E}$), содержащих E, есть нормальное расширение над k, которое содержит E и, очевидно, является наименьшим нормальным расширением поля k,

содержащим E. Если $\sigma_1, \ldots, \sigma_n$ — все различные вложения E в $\bar{E}$, то расширение

$$K = (\sigma_1 E)(\sigma_2 E) \ldots (\sigma_n E),$$

композит всех этих вложений, является нормальным расширением k. Действительно, любое его вложение, скажем τ, мы можем применить к каждому расширению $\sigma_i E$; тогда $(\tau\sigma_1, \ldots, \tau\sigma_n)$ будет перестановкой совокупности $(\sigma_1, \ldots, \sigma_n)$ и, следовательно, τ отображает K в себя. Всякое нормальное расширение поля k, содержащее E, должно содержать $\sigma_i E$ для каждого i, и, таким образом, *наименьшее нормальное расширение поля k, содержащее E, в точности равно композиту*

$$(\sigma_1 E) \ldots (\sigma_n E).$$

Если E сепарабельно над k, то из теоремы 9 с помощью индукции заключаем, что наименьшее нормальное расширение поля k, содержащее E, также сепарабельно над k.

Аналогичные результаты будут справедливы и для бесконечного алгебраического расширения E поля k, если взять бесконечный композит. Что касается терминологии, то если E — алгебраическое расширение поля k и σ — произвольное вложение E в $\bar{k}$ над k, то мы называем поле σE сопряженным с E в $\bar{k}$. Мы можем сказать, что *наименьшее нормальное расширение поля k, содержащее E, есть композит всех сопряженных с E подполей в $\bar{E}$.*

Пусть α — алгебраический элемент над k. Если $\sigma_1, \ldots, \sigma_n$ — различные вложения поля $k(\alpha)$ в $\bar{k}$ над k, то мы называем элементы $\sigma_1\alpha, \ldots, \sigma_r\alpha$ *сопряженными* с α в $\bar{k}$. Этими элементами являются попросту различные корни неприводимого многочлена над k, соответствующего элементу α. Наименьшее нормальное расширение поля k, содержащее один из этих сопряженных элементов, совпадает с $k(\sigma_1\alpha, \ldots, \sigma_r\alpha)$.

§ 5. Конечные поля

Мы получили достаточно общих теорем для того, чтобы описать строение конечных полей. Это интересно само по себе, а также дает примеры к общей теории.

Пусть F — конечное поле из q элементов. Как мы уже отмечали раньше, имеется гомоморфизм

$$\mathbf{Z} \to F,$$

переводящий 1 в 1, ядро которого не может быть 0, и, следовательно, является главным идеалом, порожденным простым числом p, по-

скольку $\mathbf{Z}/p\mathbf{Z}$ вкладывается в F, а F не имеет делителей 0. Таким образом, F имеет характеристику p и содержит поле, изоморфное $\mathbf{Z}/p\mathbf{Z}$.

Заметим, что поле $\mathbf{Z}/p\mathbf{Z}$ не имеет других автоморфизмов, кроме тождественного. Действительно, любой автоморфизм должен отображать 1 в 1 и, следовательно, оставляет каждый элемент на месте, так как 1 аддитивно порождает $\mathbf{Z}/p\mathbf{Z}$. Будем отождествлять $\mathbf{Z}/p\mathbf{Z}$ с его образом в F. Тогда F есть векторное пространство над $\mathbf{Z}/p\mathbf{Z}$, причем это векторное пространство должно быть конечномерным, поскольку F конечно. Пусть его размерность будет n, и пусть $\omega_1, \ldots, \omega_n$ — базис для F над $\mathbf{Z}/p\mathbf{Z}$. Всякий элемент из F имеет единственное представление в виде

$$a_1\omega_1 + \ldots + a_n\omega_n,$$

где $a_i \in \mathbf{Z}/p\mathbf{Z}$. Следовательно, $q = p^n$.

Мультипликативная группа F^* поля F имеет порядок $q - 1$. Всякий элемент $\alpha \in F^*$ удовлетворяет уравнению $X^{q-1} = 1$. Следовательно, всякий элемент из F удовлетворяет уравнению

$$f(X) = X^q - X = 0.$$

Это означает, что многочлен $f(X)$ имеет q различных корней в F, а именно все элементы из F. Следовательно, f разлагается в F на множители степени 1, а именно

$$X^q - X = \prod_{\alpha \in F} (X - \alpha).$$

В частности, F есть поле разложения для f. Но поле разложения однозначно определено с точностью до изоморфизма. Следовательно, если конечное поле порядка p^n существует, то оно однозначно определено с точностью до изоморфизма как поле разложения многочлена $X^{p^n} - X$ над $\mathbf{Z}/p\mathbf{Z}$.

Для краткости будем обозначать $\mathbf{Z}/p\mathbf{Z}$ также через $\mathbf{F}_p$. Пусть n — целое число $\geqslant 1$. Рассмотрим поле разложения многочлена

$$X^{p^n} - X = f(X)$$

в алгебраическом замыкании $\bar{\mathbf{F}}_p$. Мы утверждаем, что это поле разложения совпадает с множеством корней многочлена $f(X)$ в $\bar{\mathbf{F}}_p$. Действительно, пусть α, β — корни. Тогда

$$(\alpha + \beta)^{p^n} - (\alpha + \beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0,$$

откуда $\alpha + \beta$ — корень. Точно так же

$$(\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0$$

и, значит, $\alpha\beta$ — корень. Отметим, что 0, 1 — корни $f(X)$. Если $\beta \neq 0$, то

$$(\beta^{-1})^{p^n} - \beta^{-1} = (\beta^{p^n})^{-1} - \beta^{-1} = 0,$$

так что β^{-1} — корень. Наконец,

$$(-\beta)^{p^n} - (-\beta) = (-1)^{p^n}\beta^{p^n} + \beta.$$

Если p нечетно, то $(-1)^{p^n} = -1$, и мы видим, что $-\beta$ — корень. Если p четно, то $-1 = 1$ (в $\mathbf{Z}/2\mathbf{Z}$) и, следовательно, $-\beta = \beta$ — корень. Это доказывает наше утверждение.

Производная многочлена $f(X)$ равна

$$f'(X) = p^n X^{p^n - 1} - 1 = -1.$$

Следовательно, у $f(X)$ нет кратных корней, и, значит, он имеет p^n различных корней в $\mathbf{F}_p$. Таким образом, его поле разложения содержит ровно p^n элементов. Суммируем наши результаты.

Теорема 10. *Для всякого простого числа p и всякого целого числа $n \geqslant 1$ существует поле порядка p^n, обозначаемое символом $\mathbf{F}_{p^n}$, однозначно определенное как подполе в алгебраическом замыкании $\overline{\mathbf{F}}_p$. Это поле разложения многочлена*

$$X^{p^n} - X,$$

и его элементы — корни этого многочлена. Всякое конечное поле изоморфно одному и только одному из полей $\mathbf{F}_{p^n}$.

Мы обычно полагаем $p^n = q$ и пишем $\mathbf{F}_q$ вместо $\mathbf{F}_{p^n}$.

Следствие. *Пусть $\mathbf{F}_q$ — конечное поле и m — целое число $\geqslant 1$. В данном алгебраическом замыкании $\overline{\mathbf{F}}_q$ существует одно и только одно расширение поля $\mathbf{F}_q$ степени m, и этим расширением является поле $\mathbf{F}_{q^m}$.*

Доказательство. Пусть $q = p^n$. Тогда $q^m = p^{mn}$. Поле разложения многочлена $X^{q^m} - X$ есть в точности $\mathbf{F}_{p^{mn}}$ и имеет степень mn над $\mathbf{Z}/p\mathbf{Z}$. Так как $\mathbf{F}_q$ имеет степень n над $\mathbf{Z}/p\mathbf{Z}$, то F_{q^n} имеет степень m над $\mathbf{F}_q$. Обратно, любое расширение степени m над $\mathbf{F}_q$ имеет степень mn над $\mathbf{F}_p$ и, следовательно, должно совпадать с $F_{p^{mn}}$. Это доказывает наше следствие.

Теорема 11. *Мультипликативная группа конечного поля — циклическая.*

Доказательство. Это уже было доказано в гл. V, § 4, теорема 6.

Опишем все автоморфизмы конечного поля.

Пусть $q = p^n$ и $\mathbf{F}_q$ — конечное поле из q элементов. Рассмотрим отображение Фробениуса

$$\varphi\colon \mathbf{F}_q \to \mathbf{F}_q,$$

такое, что $\varphi(x) = x^p$. Очевидно, φ — гомоморфизм и его ядро равно 0, поскольку $\mathbf{F}_q$ — поле. Следовательно, φ инъективно. Так как F_q конечно, то отсюда вытекает, что φ сюръективно и что, следовательно, φ — изоморфизм. Отметим, что он оставляет $\mathbf{F}_p$ неподвижным.

Теорема 12. *Группа автоморфизмов поля $\mathbf{F}_q$ является циклической группой порядка n с образующей φ.*

Доказательство. Пусть G — группа, порожденная φ. Заметим, что $\varphi^n = \mathrm{id}$, поскольку $\varphi^n(x) = x^{p^n} = x$ для всех $x \in \mathbf{F}_q$. Следовательно, n — показатель для φ. Пусть d — период φ, так что $d \geqslant 1$. Имеем $\varphi^d(x) = x^{p^d}$ для всех $x \in \mathbf{F}_q$. Следовательно, всякий элемент $x \in \mathbf{F}_q$ является корнем уравнения

$$X^{p^d} - X = 0.$$

Это уравнение имеет самое большее p^d корней. Следовательно, $d \geqslant n$, откуда $d = n$.

Остается доказать, что G совпадает с группой всех автоморфизмов поля $\mathbf{F}_q$. Любой автоморфизм поля $\mathbf{F}_q$ должен оставлять $\mathbf{F}_p$ на месте, т. е. являться автоморфизмом $\mathbf{F}_q$ над $\mathbf{F}_p$. В силу теоремы 6 из § 4 число таких автоморфизмов $\leqslant n$. Следовательно, $\mathbf{F}_q$ не может иметь никаких других автоморфизмов, кроме тех, что содержатся в G.

Теорема 13. *Пусть m, n — целые числа $\geqslant 1$. Поле $\mathbf{F}_{p^n}$ содержится в $\mathbf{F}_{p^m}$ тогда и только тогда, когда m делится на n. Если это так, то положим $q = p^n$ и $m = nd$. Тогда $\mathbf{F}_{p^m}$ нормально и сепарабельно над $\mathbf{F}_q$ и группа автоморфизмов поля $\mathbf{F}_{p^m}$ над $\mathbf{F}_q$ есть циклическая группа, порожденная отображением φ^n.*

Доказательство. Все утверждения теоремы являются тривиальными следствиями уже доказанного выше, и их проверка предоставляется читателю.

§ 6. Примитивные элементы

Теорема 14. *Пусть E — конечное расширение поля k. Элемент $\alpha \in E$, для которого $E = k(\alpha)$, существует тогда и только тогда, когда имеется лишь конечное число промежуточных по-*

лей F: $k \subset F \subset E$. Если E сепарабельно над k, то такой элемент α существует.

Доказательство. Если k конечно, то, как мы знаем, мультипликативная группа поля E порождается одним элементом, который тем самым порождает и E над k. Поэтому будем предполагать, что k бесконечно.

Предположим, что существует лишь конечное число подполей, промежуточных между k и E. Пусть α, $\beta \in E$. Когда c пробегает элементы из k, мы можем получить лишь конечное число полей типа $k(\alpha + c\beta)$. Следовательно, существуют элементы c_1, $c_2 \in k$, причем $c_1 \neq c_2$, такие, что

$$k(\alpha + c_1\beta) = k(\alpha + c_2\beta).$$

Заметим, что $\alpha + c_1\beta$ и $\alpha + c_2\beta$ лежат в одном и том же поле, и потому там же лежит $(c_1 - c_2)\beta$, а следовательно, и β. Таким образом, α также лежит в этом поле и мы видим, что поле $k(\alpha, \beta)$ может быть порождено одним элементом.

Продолжая по индукции, получаем, что если $E = k(\alpha_1, \ldots, \alpha_n)$, то существуют элементы $c_2, \ldots, c_n \in k$, такие, что

$$E = k(\xi),$$

где $\xi = \alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n$. Это доказывает половину нашей теоремы.

Обратно, предположим, что $E = k(\alpha)$ для некоторого α. Пусть $f(X) = \operatorname{Irr}(\alpha, k, X)$, $k \subset F \subset E$ и $g_F(X) = \operatorname{Irr}(\alpha, F, X)$. Тогда g_F делит f. В $E[X]$ имеет место однозначность разложения на множители, и любой многочлен из $E[X]$, со старшим коэффициентом 1 и делящий $f(X)$, равен произведению некоторого числа сомножителей $(X - \alpha_i)$, где $\alpha_1, \ldots, \alpha_n$ — корни многочлена f. Следовательно, существует лишь конечное число таких многочленов. Таким образом, мы получаем отображение

$$F \longmapsto g_F$$

множества промежуточных полей в конечное множество многочленов. Пусть F_0 — подполе в F, порожденное над k коэффициентами многочлена $g_F(X)$. Тогда g_F имеет коэффициенты в F_0 и неприводим над F_0, поскольку он неприводим над F. Следовательно, степень элемента α над F_0 та же самая, что и над F, т. е. $F = F_0$. Таким образом, поле F однозначно определяется соответствующим ему многочленом g_F, и, значит, наше отображение инъективно. Это доказывает первое утверждение теоремы.

Что касается утверждения, относящегося к сепарабельным расширениям, то, используя индукцию, мы можем без потери общности

предполагать, что $E = k(\alpha, \beta)$, где α, β сепарабельны над k. Пусть $\sigma_1, \ldots, \sigma_n$ — различные вложения поля $k(\alpha, \beta)$ в $\bar{k}$ над k. Положим

$$P(X) = \prod_{i \neq j} (\sigma_i\alpha + X\sigma_i\beta - \sigma_j\alpha - X\sigma_j\beta).$$

Очевидно, $P(X)$ — ненулевой многочлен и, следовательно, существует элемент $c \in k$, для которого $P(c) \neq 0$. Тогда элементы $\sigma_i(\alpha + c\beta)$ $(i = 1, \ldots, n)$ все различны, а потому $k(\alpha + c\beta)$ имеет над k степень не меньше n. Но $n = [k(\alpha, \beta) : k]$ и, следовательно, $k(\alpha, \beta) = k(\alpha + c\beta)$, что и требовалось доказать.

Если $E = k(\alpha)$, то мы будем говорить, что α — *примитивный элемент* поля E (над k).

§ 7. Чисто несепарабельные расширения

Этот параграф имеет чисто технический характер и может быть опущен почти без ущерба для понимания остальной части книги.

Мы всюду предполагаем, что k — поле характеристики $p > 0$.

Элемент α, алгебраический над k, называется *чисто несепарабельным* над k, если существует целое число $n \geqslant 0$, такое, что α^{p^n} лежит в k.

Пусть E — алгебраическое расширение поля k. Мы утверждаем, что следующие условия эквивалентны:

Ч. Нес. 1. $[E : k]_s = 1$.

Ч. Нес. 2. Всякий элемент α из E чисто несепарабелен над k.

Ч. Нес. 3. Неприводимое уравнение для всякого элемента $\alpha \in E$ над k имеет вид $X^{p^n} - a = 0$ при некоторых $n \geqslant 0$ и $a \in k$.

Ч. Нес. 4. Существует такое множество образующих $\{\alpha_i\}_{i \in I}$ поля E над k, что каждый элемент α_i чисто несепарабелен над k.

Чтобы доказать эту эквивалентность, допустим, что выполняется Ч. Нес. 1. В силу теоремы 6 заключаем, что $[k(\alpha) : k]_s = 1$. Пусть $f(X) = \operatorname{Irr}(\alpha, k, X)$. Тогда f имеет только один корень, поскольку

$$[k(\alpha) : k]_s$$

равна числу различных корней многочлена $f(X)$. Положим $m = [k(\alpha) : k]$. Тогда $\deg f = m$ и разложение f над $k(\alpha)$ имеет вид $f(X) = (X - \alpha)^m$. Но $m = p^n r$, где r — целое число, взаимно простое с p. Поэтому

$$f(X) = (X^{p^n} - \alpha^{p^n})^r = X^{p^n r} - r\alpha^{p^n} X^{p^n(r-1)} + \text{младшие члены}.$$

Так как коэффициенты многочлена $f(X)$ лежат в k, то

$$r\alpha^{p^n}$$

лежит в k, и так как $r \neq 0$ (в k), то α^{p^n} лежит в k. Пусть $a = \alpha^{p^n}$. Тогда α есть корень многочлена $X^{p^n} - a$, делящегося на $f(X)$. Отсюда вытекает, что $f(X) = X^{p^n} - a$.

По существу то же самое рассуждение, что и предыдущее, показывает, что Ч. Нес. 2 влечет Ч. Нес. 3. То, что третье условие влечет четвертое, тривиально.

Наконец, предположим, что выполняется Ч. Нес. 4. Пусть E — расширение, порожденное чисто несепарабельными элементами α_i $(i \in I)$. Любое вложение поля E над k отображает α_i в корень многочлена

$$f_i(X) = \operatorname{Irr}(\alpha_i, k, X).$$

Но $f_i(X)$ делит некоторый многочлен $X^{p^n} - a$, имеющий только один (кратный) корень. Следовательно, *любое* вложение поля E над k тождественно на каждом α_i, а потому тождественно на E и мы заключаем, что $[E : k]_s = 1$, что и требовалось доказать.

Расширение, удовлетворяющее четырем предыдущим условиям, будет называться *чисто несепарабельным*.

Предложение 10. *Чисто несепарабельные расширения образуют отмеченный класс расширений.*

Доказательство. Утверждение о башне вытекает из теоремы 6, а свойство подъема — из условия Ч. Нес. 4.

Предложение 11. *Пусть E — алгебраическое расширение поля k, и пусть E_0 — композит всех подполей F поля E, таких, что $F \subset k$ и F сепарабельно над k. Тогда E_0 сепарабельно над k, а E чисто несепарабельно над E_0.*

Доказательство. Поскольку сепарабельные расширения образуют отмеченный класс, то, как мы знаем, E_0 сепарабельно над k. Фактически E_0 состоит из всех элементов E, сепарабельных над k. В силу предложения 9 для заданного элемента $\alpha \in E$, существует такая степень p, скажем p^n, что α^{p^n} сепарабелен над k. Следовательно, E чисто несепарабельно над E_0, что и требовалось показать.

Следствие 1. *Если алгебраическое расширение E поля k одновременно и сепарабельно, и чисто несепарабельно, то $E = k$.*

Доказательство. Очевидно.

Следствие 2. *Пусть расширение K нормально над k, и пусть K_0 — его максимальное сепарабельное подрасширение. Тогда K_0 также нормально над k.*

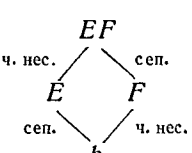
Доказательство. Пусть σ — вложение K_0 в $\bar{K}$ над k. Продолжим σ до вложения поля K. Тогда σ будет автоморфизмом K.

Кроме того, поле σK_0 сепарабельно над k, следовательно, оно содержится в K_0, поскольку K_0 — максимальное сепарабельное подполе. Значит, $\sigma K_0 = K_0$, что и утверждалось.

Следствие 3. *Пусть E, F — два конечных расширения поля k, причем E/k сепарабельно, а F/k чисто несепарабельно. Предположим, что E, F — подполя некоторого общего поля. Тогда*

$$[EF : F] = [E : k] = [EF : k]_s,$$
$$[EF : E] = [F : k] = [EF : k]_i.$$

Доказательство. Картина имеет следующий вид:



Доказательство состоит в тривиальном жонглировании индексами с использованием следствий предложения 9. Мы предоставляем его читателю.

Следствие 4. *Обозначим через E^p поле всех элементов вида x^p, $x \in E$. Пусть E — конечное расширение поля k. Если $E^p k = E$, то E сепарабельно над k. Если E сепарабельно над k, то $E^{p^n} k = E$ для всех $n \geqslant 1$.*

Доказательство. Пусть E_0 — максимальное сепарабельное подполе в E. Допустим, что $E^p k = E$. Положим $E = k(\alpha_1, \ldots, \alpha_n)$. Так как E чисто несепарабельно над E_0, то существует такое m, что $\alpha_i^{p^m} \in E_0$ для всех $i = 1, \ldots, n$. Следовательно, $E^{p^m} \subset E_0$. Но $E^{p^m} k = E$, так что $E = E_0$ сепарабельно над k. Обратно, предположим, что E сепарабельно над k. Но E чисто несепарабельно над $E^p k$. Так как E в то же время сепарабельно над $E^p k$, то заключаем, что $E = E^p k$. Итерируя, получаем $E = E^{p^n} k$ для $n \geqslant 1$, что и требовалось доказать.

Предложение 11 показывает, что любое алгебраическое расширение может быть разложено в башню, состоящую из максимального сепарабельного подрасширения и чисто несепарабельного этажа над ним. Обычно бывает нельзя обратить порядок в этой башне. Однако имеется важный случай, когда это может быть сделано.

Предложение 12. *Пусть K — нормальное расширение поля k, G — его группа автоморфизмов над k и K^G — неподвижное поле группы G. Тогда K^G чисто несепарабельно над k и K*

сепарабельно над K^G. Если K_0 — максимальное сепарабельное подрасширение K, то $K = K^G K_0$ и $K_0 \cap K^G = k$.

Доказательство. Пусть $\alpha \in K^G$ и τ — произвольное вложение поля $k(\alpha)$ над k в $\bar{K}$. Продолжим τ до вложения поля K; будем обозначать это продолжение по-прежнему через τ. Тогда τ — автоморфизм поля K, поскольку K нормально над k. По определению $\tau\alpha = \alpha$ и, следовательно, τ тождественно на $k(\alpha)$. Поэтому $[k(\alpha) : k]_s = 1$ и элемент α чисто несепарабелен. Таким образом, K^G чисто несепарабельно над k. Пересечение K_0 и K^G одновременно и сепарабельно, и чисто несепарабельно над k, и, следовательно, равно k.

Чтобы доказать сепарабельность K над K^G, предположим сначала, что K конечно над k и что, следовательно, группа G конечна в силу теоремы 6. Пусть $\alpha \in K$, и пусть $\sigma_1, \ldots, \sigma_r$ — максимальное подмножество элементов из G, такое, что элементы

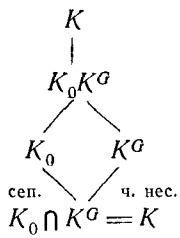
$$\sigma_1\alpha, \ldots, \sigma_r\alpha$$

различны. Тогда некоторое σ_i тождественно на α и α есть корень многочлена

$$f(X) = \prod_{i=1}^{r} (X - \sigma_i\alpha).$$

Заметим, что $f^\tau = f$ для любого $\tau \in G$, поскольку τ переставляет корни. Мы видим, что f сепарабелен и что его коэффициенты лежат в неподвижном поле K^G. Поэтому α сепарабелен над K^G. Редукция бесконечного случая к конечному основывается на том наблюдении, что всякий элемент $\alpha \in K$ содержится в некотором конечном нормальном подрасширении в K. Детали мы предоставляем читателю.

Теперь имеем следующую диаграмму:



В силу предложения 11 K чисто несепарабельно над K_0 и, следовательно, чисто несепарабельно над K_0K^G. С другой стороны, K сепарабельно над K^G и, следовательно, сепарабельно над K_0K^G. Таким образом, $K = K_0K^G$, что и доказывает наше предложение.

Мы видим, что всякое нормальное расширение распадается в композит чисто несепарабельного и сепарабельного расширений. В следующей главе мы определим расширение Галуа как нормальное сепарабельное расширение. Тогда K_0 будет расширением Галуа над k и нормальное расширение распадается на расширение Галуа и чисто несепарабельное расширение. Группа G называется *группой Галуа* расширения K/k.

Поле k называется *совершенным*, если $k^p = k$. (Всякое поле характеристики нуль также называется совершенным.)

Следствие. *Если поле k совершенно, то любое его алгебраическое расширение сепарабельно. Всякое алгебраическое расширение поля k совершенно.*

Доказательство. Всякое конечное алгебраическое расширение содержится в нормальном расширении, поэтому наши утверждения непосредственно следуют из предложения 12.

УПРАЖНЕНИЯ

1. Пусть k — конечное поле из q элементов, $f(X) \in k[X]$ — неприводимый многочлен. Показать, что $f(X)$ делит многочлен $X^{q^n} - X$ тогда и только тогда, когда степень f делит n.

2. Показать, что

$$X^{q^n} - X = \prod_{d \mid n} \prod_{f_d \text{ непр.}} f_d(X),$$

где второе произведение берется по всем неприводимым многочленам степени d со старшим коэффициентом 1. Подсчитав степени, показать, что

$$q^n = \sum_{d \mid n} d\psi(d),$$

где $\psi(d)$ — число неприводимых многочленов степени d. С помощью элементарной теории чисел получить двойственное равенство

$$n\psi(n) = \sum_{d \mid n} \mu(d)\, q^{n/d}.$$

(μ — функция Мёбиуса, см. стр. 236.)

3. Пусть k — поле характеристики p, и пусть t, u алгебраически независимы над k. Доказать следующие утверждения:
(i) $k(t, u)$ имеет степень p^2 над $k(t^p, u^p)$.
(ii) Между $k(t, u)$ и $k(t^p, u^p)$ существует бесконечно много расширений.

4. Пусть E — конечное расширение поля k характеристики $p > 0$, и пусть $p^r = [E : k]_i$. Допустим, что не существует степени p^s с $s < r$, для которой $E^{p^s}k$ сепарабельно над k (т. е. такой, что α^{p^s} сепарабелен над k для всякого α из E). Показать, что E может быть порождено одним элементом над k. [*Указание:* предположить сначала, что E *чисто несепарабельно.*]

5. Пусть k — поле, $f(X)$ — неприводимый многочлен из $k[X]$ и K — конечное нормальное расширение над k. Показать, что если g, h — неприводимые множители $f(X)$ в $K[X]$, то существует автоморфизм σ поля K над k, для которого $g = h^{\sigma}$. Привести пример, показывающий, что это утверждение неверно, если K не нормально над k.

6. Пусть $x_1, \ldots, x_n$ алгебраически независимы над полем k, а y алгебраичен над $k(x) = k(x_1, \ldots, x_n)$. Пусть $P(X_{n+1})$ — неприводимый многочлен элемента y над $k(x)$ и $\varphi(x)$ — наименьшее общее кратное знаменателей коэффициентов многочлена P. Тогда коэффициенты многочлена $\varphi(x)P$ являются элементами из $k[x]$. Показать, что

$$f(X_1, \ldots, X_{n+1}) = \varphi(X_1, \ldots, X_n)\, P(X_{n+1})$$

неприводим над k как многочлен от $n+1$ переменной. Обратно, пусть $f(X_1, \ldots, X_{n+1})$ — неприводимый многочлен над k и $x_1, \ldots, x_n$ алгебраически независимы над k. Показать, что

$$f(x_1, \ldots, x_n, X_{n+1})$$

неприводим над $k(x_1, \ldots x_n)$.

Если f — многочлен от n переменных и $(b) = (b_1, \ldots, b_n)$ такой набор из n элементов, что $f(b) = 0$, то мы говорим, что (b) — *нуль* многочлена f. Мы говорим, что нуль (b) *нетривиален*, если не все координаты b_i равны 0.

7. Пусть $f(X_1, \ldots, X_n)$ — однородный многочлен степени 2 (соответственно 3) над полем k. Показать, что если f имеет нетривиальный нуль в некотором расширении нечетной степени (соответственно, степени 2) над k, то f имеет нетривиальный нуль в k.

8. Пусть $f(X, Y)$ — неприводимый многочлен от двух переменных над полем k, и пусть t трансцендентно над k, причем существуют взаимно простые целые числа m, n и элементы $a, b \in k$, $ab \neq 0$, такие, что $f(at^n, bt^m) = 0$. Показать, что после возможной замены X или Y на обратную величину и с точностью до постоянного множителя многочлен f имеет вид

$$X^m Y^n - c$$

с некоторым $c \in k$.

Ответ к следующему упражнению неизвестен.

9. (Артин) Пусть f — однородный многочлен степени d от n переменных с рациональными коэффициентами. Показать, что если $n > d$, то существуют корень из единицы ζ и элементы $x_1, \ldots, x_n \in \mathbf{Q}[\zeta]$, не все равные нулю, такие, что $f(x_1, \ldots, x_n) = 0$.

Глава VIII

Теория Галуа

§ 1. Расширения Галуа

Пусть K — поле и G — группа автоморфизмов поля K. Мы будем обозначать через K^G подмножество в K, состоящее из всех элементов $x \in K$, таких, что $x^\sigma = x$ для всех $\sigma \in G$. Это подмножество называется *неподвижным полем* группы G[1]). Это действительно поле, поскольку из x, $y \in K^G$ следует

$$(x+y)^\sigma = x^\sigma + y^\sigma = x+y$$

для всех $\sigma \in G$ и аналогичным образом проверяется, что K^G замкнуто относительно умножения, вычитания и деления. Кроме того, K^G содержит 0 и 1 и, следовательно, содержит простое поле.

Алгебраическое расширение K поля k называется *расширением Галуа*, если оно нормально и сепарабельно. Мы будем считать K вложенным в некоторое алгебраическое замыкание. Группа автоморфизмов поля K над k называется *группой Галуа* поля K над k и обозначается символом $G(K/k)$ или просто G. Она совпадает с множеством вложений поля K в $\overline{K}$ над k.

Для удобства читателя мы сформулируем теперь основной результат теории Галуа для конечных расширений Галуа.

Пусть K — конечное расширение Галуа поля k с группой Галуа G. Тогда между множеством подполей E в K, содержащих k, и множеством подгрупп H в G существует биективное соответствие, задаваемое формулой $E = K^H$. Поле E будет расширением Галуа над k тогда и только тогда, когда подгруппа H нормальна в G, и в этом случае отображение $\sigma \mapsto \sigma|E$ индуцирует изоморфизм факторгруппы G/H на группу Галуа поля E над k.

Мы дадим доказательства шаг за шагом, причем, насколько возможно, мы даем их для бесконечных расширений.

Теорема 1. *Пусть K — расширение Галуа поля k, G — его группа Галуа. Тогда $k = K^G$. Если F — промежуточное поле,*

---

[1]) Или, по другой терминологии, *полем инвариантов* группы G.— *Прим. ред.*

$k \subset F \subset G$, то K — расширение Галуа над F. Отображение

$$F \longmapsto G(K/F)$$

множества промежуточных полей в множество подгрупп группы G инъективно.

Доказательство. Пусть $\alpha \in K^G$ и σ — произвольное вложение поля $k(\alpha)$ в $\bar{K}$, индуцирующее тождественное отображение на k. Продолжим σ до вложения K в $\bar{K}$; мы будем обозначать это продолжение по-прежнему через σ. Тогда σ — автоморфизм поля K над k, следовательно, элемент группы G. По предположению σ оставляет α неподвижным. Поэтому

$$[k(\alpha) : k]_s = 1.$$

Так как α сепарабелен над k, то имеем $k(\alpha) = k$ и α есть элемент k. Это доказывает наше первое утверждение.

Пусть F — промежуточное поле. Тогда K нормально над F в силу теоремы 5 и сепарабельно над F в силу теоремы 9 из гл. VII. Следовательно, K — расширение Галуа над F. Если $H = G(K/F)$, то в силу доказанного выше заключаем, что $F = K^H$. Если F, F' — промежуточные поля и $H = G(K/F)$, $H' = G(K/F')$, то

$$F = K^H \quad \text{и} \quad F' = K^{H'}.$$

Если $H = H'$, то $F = F'$, откуда вытекает, что отображение

$$F \longmapsto G(K/F)$$

инъективно, что и доказывает нашу теорему.

Мы будем иногда называть группу $G(K/F)$ над промежуточным полем F группой, *ассоциированной* с F. Мы будем говорить также, что подгруппа H в G *принадлежит* промежуточному полю F, если $H = G(K/F)$.

Следствие 1. *Пусть K/k — расширение Галуа с группой G. Пусть F, F' — два промежуточных поля и H, H' — подгруппы в G, принадлежащие F, F' соответственно. Тогда $H \cap H'$ принадлежит полю FF'.*

Доказательство. Всякий элемент из $H \cap H'$ оставляет FF' неподвижным, и всякий элемент из G, оставляющий FF' неподвижным, оставляет неподвижным также F и F' и, следовательно, лежит в $H \cap H'$. Это доказывает наше утверждение.

Следствие 2. (*Обозначения те же, что и в следствии* 1.) *Неподвижное поле наименьшей подгруппы в G, содержащей H, H', есть $F \cap F'$.*

Доказательство. Очевидно.

Следствие 3. *Пусть обозначения те же, что и в следствии* 1. *Тогда* $F \subset F'$ *в том и только в том случае, если* $H' \subset H$.

Доказательство. Если $F \subset F'$ и $\sigma \in H'$ оставляет F' неподвижным, то σ оставляет неподвижным и F, так что σ лежит в H. Обратно, если $H' \subset H$, то неподвижное поле группы H содержится в неподвижном поле группы H', так что $F \subset F'$.

Следствие 4. *Пусть* E *— конечное сепарабельное расширение поля* k *и* K *— наименьшее нормальное расширение поля* k, *содержащее* E. *Тогда* K *— конечное расширение Галуа над* k. *Существует лишь конечное число промежуточных полей* F, *таких, что* $k \subset F \subset E$.

Доказательство. Мы знаем, что K нормально и сепарабельно. Далее, K конечно над k, поскольку это, как мы видели, конечный композит конечного числа сопряженных с E полей. Группа Галуа расширения K/k имеет лишь конечное число подгрупп. Следовательно, существует лишь конечное число подполей в K, содержащих k, и тем более лишь конечное число подполей в E, содержащих k.

Конечно, следствие 4 было уже доказано в предыдущей главе, но здесь мы получили другое доказательство с иной точки зрения.

Лемма 1. *Пусть* E *— алгебраическое сепарабельное расширение поля* k. *Предположим, что существует целое число* $n \geqslant 1$, *такое, что всякий элемент* α *из* E *имеет степень* $\leqslant n$ *над* k. *Тогда* E *конечно над* k *и* $[E : k] \leqslant n$.

Доказательство. Пусть α — элемент из E, для которого степень $[k(\alpha) : k]$ максимальна, скажем равна $m \leqslant n$. Мы утверждаем, что $k(\alpha) = E$. Если это не так, то существует элемент $\beta \in E$, такой, что $\beta \notin k(\alpha)$, и в силу теоремы о примитивном элементе найдется элемент $\gamma \in k(\alpha, \beta)$, для которого $k(\alpha, \beta) = k(\gamma)$. Но из башни

$$k \subset k(\alpha) \subset k(\alpha, \beta)$$

мы видим, что $[k(\alpha, \beta) : k] > m$, откуда вытекает, что γ имеет степень $> m$ над k, — противоречие.

Теорема 2 (Артин). *Пусть* K *— поле и* G *— конечная группа автоморфизмов поля* K, *имеющая порядок* n. *Пусть* $k = K^G$ *— соответствующее неподвижное поле. Тогда* K *— конечное расширение Галуа над* k *и его группа Галуа есть* G. *Кроме того,* $[K : k] = n$.

Доказательство. Пусть $\alpha \in K$, и пусть $\sigma_1, \ldots, \sigma_r$ — такое максимальное множество элементов из G, что $\sigma_1\alpha, \ldots, \sigma_r\alpha$ различны. Для всякого $\tau \in G$ наборы $\{\tau\sigma_1\alpha, \ldots, \tau\sigma_r\alpha\}$ и $\{\sigma_1\alpha, \ldots, \sigma_r\alpha\}$ отличаются лишь перестановкой, поскольку τ инъективно и каждый элемент $\tau\sigma_i\alpha$ содержится в множестве $\{\sigma_1\alpha, \ldots, \sigma_r\alpha\}$, иначе это множество не было бы максимальным. Следовательно, α — корень многочлена

$$f(X) = \prod_{i=1}^{r} (X - \sigma_i\alpha)$$

и для любого $\tau \in G$ имеем $f^\tau = f$. Таким образом, коэффициенты многочлена f лежат в $K^G = k$. Кроме того, f сепарабелен. Следовательно, всякий элемент α из K есть корень сепарабельного многочлена степени $\leqslant n$ с коэффициентами в k. Далее, этот многочлен разлагается на линейные множители в K. Таким образом, K сепарабельно над k, нормально над k и является поэтому расширением Галуа над k. В силу леммы 1 имеем $[K : k] \leqslant n$. Группа Галуа поля K над k имеет порядок $\leqslant [K : k]$ (в силу теоремы 6 из гл. VII, § 4), и, следовательно, группа G должна быть полной группой Галуа. Этим доказаны все наши утверждения.

Следствие. *Пусть K — конечное расширение Галуа поля k и G — его группа Галуа. Тогда всякая подгруппа в G принадлежит некоторому подполю F, такому, что $k \subset F \subset K$.*

Доказательство. Пусть H — подгруппа в G и $F = K^H$. В силу теоремы Артина K — расширение Галуа над F с группой H.

Замечание. Для бесконечных расширений Галуа K поля k предыдущее следствие уже перестает быть справедливым. Это показывает, что использование того или иного вычислительного соображения действительно необходимо в доказательстве для конечного случая. В настоящем изложении использовано старомодное рассуждение. Читатель может посмотреть собственное доказательство Артина в его книге „Теория Галуа“. В бесконечном случае на группе Галуа G вводится топология Крулля (см. упражнения) и G превращается в компактную вполне несвязную группу. Подгруппы, принадлежащие промежуточным полям,— это *замкнутые* подгруппы. Если читатель желает полностью игнорировать бесконечный случай во всех наших рассмотрениях, он может это сделать без какого-либо ущерба для понимания. Доказательства для бесконечного случая обычно тождественны с доказательствами для конечного случая.

Понятия расширения Галуа и группы Галуа определяются чисто алгебраически. Следовательно, их формальное поведение при изоморфизмах точно такое же, какого можно ожидать от объектов в любой категории. Мы опишем это поведение для рассматриваемого случая в более ясном виде.

Пусть K — расширение Галуа поля k и

$$\lambda\colon K \to K^{\lambda} = \lambda K$$

— изоморфизм. Тогда K^{λ} — расширение Галуа поля k^{λ},

$$\begin{array}{ccc} K & \xrightarrow{\lambda} & K^{\lambda} \\ | & & | \\ k & \xrightarrow[\lambda]{} & k^{\lambda} \end{array}$$

Пусть G — группа Галуа поля K над k. Тогда отображение

$$\sigma \longmapsto \lambda \circ \sigma \circ \lambda^{-1}$$

определяет гомоморфизм G в группу Галуа поля K^{λ} над k^{λ}, обратный к которому задается правилом

$$\lambda^{-1} \circ \tau \circ \lambda \longleftarrow \tau.$$

Следовательно, группа $G\left(K^{\lambda}/k^{\lambda}\right)$ изоморфна $G(K/k)$ относительно предыдущего отображения. Мы можем записать это так:

$$G(\lambda K/\lambda k)^{\lambda} = G(K/k)$$

или

$$G(\lambda K/\lambda k) = \lambda G(K/k)\lambda^{-1},$$

где показатель λ означает „сопряжение“

$$\sigma^{\lambda} = \lambda^{-1} \circ \sigma \circ \lambda.$$

Контравариантности никак нельзя избежать, если мы хотим сохранить правило

$$(\sigma^{\lambda})^{\omega} = \sigma^{\lambda\omega}$$

для композиции отображений λ и ω.

Пусть, в частности, F — промежуточное поле, $k \subset F \subset K$ и $\lambda\colon F \to \lambda F$ — вложение F в K, предполагаемое продолженным до автоморфизма поля K. Тогда $\lambda K = K$. Следовательно,

$$G(K/\lambda F)^{\lambda} = G(K/F)$$

и

$$G(K/\lambda F) = \lambda G(K/F)\lambda^{-1}.$$

Теорема 3. *Пусть K — расширение Галуа поля k с группой G. Пусть F — подполе, $k \subset F \subset K$ и $H = G(K/F)$. Тогда для нормальности F над k необходимо и достаточно, чтобы подгруппа H была нормальной в G. Если F нормально над k, то отображение ограничения $\sigma \longmapsto \sigma|F$ будет гомоморфизмом G на*

группу Галуа поля F над k, ядро которого есть H. Таким образом $G(F/k) \approx G/H$.

Доказательство. Пусть F нормально над k и G' — его группа Галуа. Отображение ограничения $\sigma \mapsto \sigma|F$ переводит G в G', и по определению его ядро есть H. Следовательно, H нормальна в G. Кроме того, любой элемент $\tau \in G'$ продолжается до вложения K в $\overline{K}$, которое должно быть автоморфизмом поля K, так что отображение ограничения сюръективно. Это доказывает последнее утверждение. Наконец, предположим, что F не нормально над k. Тогда существует вложение λ поля F в K над k, которое не является автоморфизмом, т. е. $\lambda F \neq F$. Продолжим λ до автоморфизма поля K над k. Группы Галуа $G(K/\lambda F)$ и $G(K/F)$ сопряжены и, принадлежа разным подполям, не могут совпадать. Следовательно, подгруппа H не нормальна в G.

Расширение Галуа K/k называется *абелевым* (соответственно *циклическим*), если его группа Галуа G абелева (соответственно циклическая).

Следствие. *Пусть K/k — абелево (соответственно циклическое) расширение. Если F — промежуточное поле, $k \subset F \subset K$, то F — расширение Галуа над k и притом абелево (соответственно циклическое).*

Доказательство. Это вытекает немедленно из того факта, что всякая подгруппа абелевой группы нормальна и всякая факторгруппа абелевой (соответственно циклической) группы абелева (соответственно циклическая).

Теорема 4. *Пусть K — расширение Галуа поля k, а F — произвольное расширение, причем K, F — подполя некоторого другого поля. Тогда KF является расширением Галуа над F, а K — расширением Галуа над $K \cap F$. Пусть H — группа Галуа поля KF над F и G — группа Галуа поля K над k. Если $\sigma \in H$, то ограничение σ на K лежит в G и отображение*

$$\sigma \mapsto \sigma|K$$

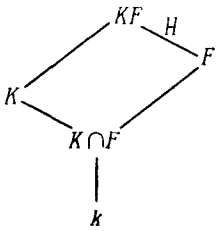
дает изоморфизм H на группу Галуа поля K над $K \cap F$.

Доказательство. Пусть $\sigma \in H$. Ограничение σ на K есть вложение поля K над k, следовательно, элемент группы G, поскольку K нормально над k. Отображение $\sigma \mapsto \sigma|K$, очевидно, является гомоморфизмом. Если $\sigma|K$ тождественно, то σ должно быть тождественно на KF (так как всякий элемент из KF может быть выражен как комбинация сумм, произведений и отношений элементов из K и F). Следовательно, наш гомоморфизм $\sigma \mapsto \sigma|K$ инъективен. Пусть H' —

его образ. Тогда H' оставляет $K \cap F$ неподвижным, и, обратно, если элемент $\alpha \in K$ неподвижен относительно H', то α неподвижен и относительно H, откуда $\alpha \in F$ и $\alpha \in K \cap F$. Поэтому $K \cap F$ — соответствующее неподвижное поле. Если K конечно над k или даже если KF конечно над F, то в силу теоремы 2 H' есть группа Галуа поля K над $K \cap F$, и теорема в этом случае доказана.

(В бесконечном случае нужно еще добавить замечание, что наше отображение $\sigma \mapsto \sigma|K$ непрерывно, откуда вытекает, что его образ замкнут, поскольку H компактна.)

Следующая диаграмма иллюстрирует теорему 4:



Полезно мыслить себе противоположные стороны параллелограмма равными.

Следствие. *Пусть K — конечное расширение Галуа и F — произвольное расширение поля k. Тогда $[KF : F]$ делит $[K : k]$.*

Доказательство. Пусть обозначения те же, что и выше. Как мы знаем, порядок группы H делит порядок группы G, откуда и вытекает наше утверждение.

Предостережение. Утверждение следствия, как правило, неверно, если K не является расширением Галуа над k. Например, пусть $\alpha = \sqrt[3]{2}$ — вещественный кубический корень из 2, ζ — кубический корень из 1, не равный 1, скажем

$$\zeta = \frac{-1+\sqrt{-3}}{2},$$

и пусть $\beta = \zeta\alpha$. Рассмотрим $E = \mathbf{Q}(\beta)$. Так как β — комплексная величина, а α — вещественная, то $\mathbf{Q}(\beta) \neq \mathbf{Q}(\alpha)$. Положим $F = \mathbf{Q}(\alpha)$. Тогда $E \cap F$ будет подполем в E, степень которого над $\mathbf{Q}$ делит число 3. Следовательно, эта степень есть 3 или 1 и, значит, должна быть равна 1, поскольку $E \neq F$. Но

$$EF = \mathbf{Q}(\alpha, \beta) = \mathbf{Q}(\alpha, \zeta) = Q\left(\alpha, \sqrt{-3}\right)$$

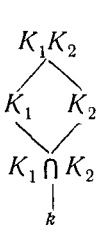
Следовательно, EF имеет степень 2 над F.

Теорема 5. *Пусть K_1 и K_2 — расширения Галуа над полем k с группами Галуа G_1 и G_2 соответственно. Предположим, что K_1, K_2 — подполя некоторого поля. Тогда K_1K_2 — расширение Галуа над k. Пусть G — его группа Галуа. Отобразим $G \to G_1 \times G_2$ посредством ограничений, а именно*

$$\sigma \longmapsto (\sigma|K_1,\ \sigma|K_2).$$

Это отображение инъективно. Если $K_1 \cap K_2 = k$, то это отображение есть изоморфизм.

Доказательство. Нормальность и сепарабельность сохраняются при взятии композита двух полей, так что K_1K_2 есть расширение Галуа над k. Наше отображение, очевидно, является гомоморфизмом G в $G_1 \times G_2$. Если элемент $\sigma \in G$ индуцирует тождественные автоморфизмы на K_1 и K_2, то он индуцирует тождественный автоморфизм и на их композите, так что наше отображение инъективно. Предположим, что $K_1 \cap K_2 = k$. Согласно теореме 4, для заданного элемента $\sigma_1 \in G_1$ найдется элемент σ из группы Галуа поля K_1K_2 над K_2, индуцирующий σ_1 на K_1. Этот элемент σ заведомо лежит в G и индуцирует тождественное отображение на K_2. Следовательно, $G_1 \times \{e_2\}$ содержится в образе нашего гомоморфизма (где e_2 — единичный элемент группы G_2). Аналогично $\{e_1\} \times G_2$ содержится в этом образе. Следовательно, их произведение содержится в образе, а их произведение есть в точности $G_1 \times G_2$. Это доказывает теорему 5.



Следствие 1. *Пусть $K_1, \ldots, K_n$ — расширения Галуа поля k с группами Галуа $G_1, \ldots, G_n$. Предположим, что $K_{i+1} \cap (K_1 \ldots K_i) = k$ для каждого $i = 1, \ldots, n-1$. Тогда группа Галуа композита $K_1 \ldots K_n$ естественным образом изоморфна произведению $G_1 \times \ldots \times G_n$.*

Доказательство. Индукция.

Следствие 2. *Пусть K — конечное расширение Галуа поля k с группой G, причем G может быть представлена в виде прямого произведения $G = G_1 \times \ldots \times G_n$. Пусть K_i — неподвижное поле группы*

$$G_1 \times \ldots \times \{1\} \times \ldots \times G_n,$$

где группа из одного элемента стоит на i-м месте. Тогда K_i — расширение Галуа над k и $K_{i+1} \cap (K_1 \dots K_i) = k$. Кроме того, $K = K_1 \dots K_n$.

Доказательство. В силу следствия 1 теоремы 1 композит всех K_i принадлежит пересечению соответствующих групп, состоящему, очевидно, из единицы. Следовательно, композит равен K. Каждый прямой множитель группы G нормален в G, так что K_i — расширение Галуа над k. В силу следствия 2 теоремы 1 пересечение нормальных расширений принадлежит произведению соответствующих им групп, откуда ясно, что $K_{i+1} \cap (K_1 \dots K_i) = k$.

§ 2. *Примеры и приложения*

Пусть k — поле, $f(X)$ — многочлен степени $\geqslant 1$ из $k[X]$ и

$$f(X) = (X - \alpha_1) \dots (X - \alpha_n)$$

— его разложение на множители в поле разложения K над k. Пусть G — группа Галуа поля K над k. *Мы называем G группой Галуа многочлена $f(X)$* над k. Элементы из G переставляют корни многочлена f. Таким образом, мы имеем инъективный гомоморфизм группы G в симметрическую группу S_n на n элементах. Не всякая перестановка обязательно задается некоторым элементом из G. Ниже мы рассмотрим примеры.

Пример 1. Пусть k — поле и $a \in k$. Если a не является квадратом в k, то многочлен $X^2 - a$ не имеет корня в k и потому неприводим. Предположим, что $\mathrm{char} \neq 2$. Тогда многочлен сепарабелен (поскольку $a \neq 0$), и если α — некоторый его корень, то $k(\alpha)$ — поле разложения, являющееся расширением Галуа. Его группа Галуа — циклическая порядка 2. Выделение полного квадрата показывает, что так описывается всякое квадратичное расширение (для $\mathrm{char} \neq 2$).

Пример 2. Пусть k — поле характеристики $\neq 2$ или 3, $f(X) = X^3 + bX + c$ — многочлен над k. (Любой многочлен степени 3 может быть приведен к такому виду посредством выделения полного куба.) Если f не имеет корней в k, то f неприводим (*любое разложение на множители должно содержать множитель степени 1*). Если α — корень многочлена $f(X)$, то $[k(\alpha) : k] = 3$. Пусть K — поле разложения и G — его группа Галуа. Тогда G имеет порядок 3 или 6, поскольку G есть подгруппа симметрической группы S_3. Во втором случае $k(\alpha)$ не будет нормальным над k.

Имеется простой способ проверить, является ли группа Галуа полной симметрической группой. Рассмотрим дискриминант. Положим

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) \text{ и } \Delta = \delta^2,$$

где α_1, α_2, α_3 — различные корни многочлена $f(X)$. Если G — группа Галуа и $\sigma \in G$, то $\sigma(\delta) = \pm\delta$. Следовательно, σ оставляет Δ неподвижным. Таким образом, Δ лежит в основном поле k, а именно, как мы видели,

$$\Delta = -4b^3 - 27c^2.$$

Множество тех σ в G, которые оставляют δ неподвижным, совпадает в точности с множеством четных перестановок. Таким образом, G будет симметрической группой тогда и только тогда, когда Δ не является квадратом в k.

Например, рассмотрим многочлен

$$f(X) = X^3 - X + 1$$

над полем рациональных чисел. Любой рациональный корень должен быть либо 1, либо -1, так что $f(X)$ неприводим над $\mathbf{Q}$. Дискриминант равен -23 и не является квадратом. Следовательно, группа Галуа — симметрическая группа. Поле разложения содержит подполе степени 2, а именно $K(\delta) = k(\sqrt{\Delta})$.

Пример 3. Рассмотрим многочлен $f(X) = X^4 - 2$ над полем рациональных чисел $\mathbf{Q}$. Он неприводим по критерию Эйзенштейна. Пусть α — вещественный корень и $i = \sqrt{-1}$. Тогда $\pm\alpha$ и $\pm i\alpha$ — четыре корня многочлена $f(X)$ и

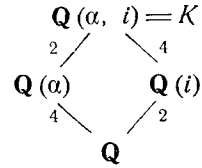
$$[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4.$$

Следовательно, полем разложения многочлена $f(X)$ будет

$$K = \mathbf{Q}(\alpha, i).$$

Поле $\mathbf{Q}(\alpha) \cap \mathbf{Q}(i)$ имеет степень 1 или 2 над $\mathbf{Q}$. Степень не может быть равна 2, иначе $i \in \mathbf{Q}(\alpha)$, что невозможно, поскольку корень α вещественный. Следовательно, степень равна 1, i имеет степень 2 над $\mathbf{Q}(\alpha)$ и поэтому $[K : \mathbf{Q}] = 8$. Группа Галуа многочлена $f(X)$ имеет порядок 8.

Существует автоморфизм τ поля K, оставляющий $\mathbf{Q}(\alpha)$ неподвижным и переводящий i в $-i$, поскольку K — расширение Галуа над $\mathbf{Q}(\alpha)$ степени 2. Имеем $\tau^2 = \mathrm{id}$,

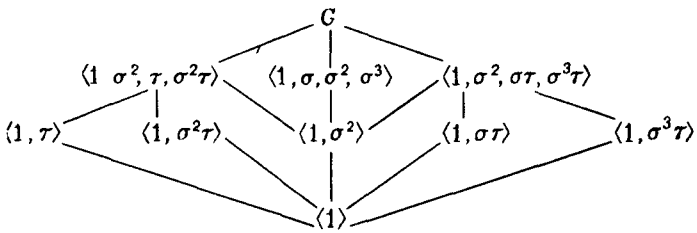


В силу мультипликативности степеней в башнях степени именно таковы, как указано в диаграмме. Таким образом, $X^4 - 2$ неприводим над

$\mathbf{Q}(i)$. Кроме того, K нормально над $\mathbf{Q}(i)$. Существует автоморфизм σ поля K над $\mathbf{Q}(i)$, отображающий корень α многочлена X^4-2 в корень $i\alpha$. Немедленно проверяется, что 1, σ, σ^2, σ^3 различны и что $\sigma^4=\mathrm{id}$. Таким образом, σ порождает циклическую группу порядка 4. Обозначим ее через $\langle\sigma\rangle$. Так как $\tau\notin\langle\sigma\rangle$ и $\langle\sigma\rangle$ имеет индекс 2 в G, то $G=\langle\sigma, \tau\rangle$ порождается элементами σ и τ. Кроме того, непосредственно проверяется, что

$$\tau\sigma=\sigma^3\tau,$$

поскольку это соотношение выполняется при действии на элементы α и i, порождающие K над $\mathbf{Q}$. Это дает нам строение G. Легко проверить, что структура подгрупп следующая:



Пример 4. Пусть k — поле, $t_1, \ldots, t_n$ алгебраически независимы над k и $K=k(t_1, \ldots, t_n)$. Симметрическая группа G на n символах действует на K, переставляя $(t_1, \ldots, t_n)$, и ее неподвижное поле есть поле симметрических функций, т. е. по определению поле, состоящее из тех элементов в K, которые неподвижны относительно G. Пусть $s_1, \ldots, s_n$ — элементарные симметрические многочлены и

$$f(X)=\prod_{i=1}^{n}(X-t_i).$$

С точностью до знака коэффициентами f будут $s_1, \ldots, s_n$. Положим $F=K^G$. Мы утверждаем, что $F=k(s_1, \ldots, s_n)$. Действительно,

$$k(s_1, \ldots, s_n)\subset F.$$

С другой стороны, K является полем разложения многочлена $f(X)$ и его степень над F равна $n!$, а степень над $k(s_1, \ldots, s_n)\leqslant n!$; следовательно, имеет место равенство $F=k(s_1, \ldots, s_n)$.

Многочлен $f(X)$ рассмотренного вида называется общим многочленом степени n. Только что мы построили расширение Галуа, группа Галуа которого есть симметрическая группа.

Используя теорему Гильберта о неприводимости, можно построить расширение Галуа поля $\mathbf{Q}$, группа Галуа которого есть симметрическая группа (см. гл. IX и [9], гл. VIII). Не известно, для всякой ли данной конечной группы G существует расширение Галуа поля $\mathbf{Q}$, группа Галуа которого есть G. Эмма Нётер заметила, что это можно было бы доказать посредством специализации параметров, если бы было известно, что всякое поле E, для которого

$$\mathbf{Q}(s_1, \ldots, s_n) \subset E \subset \mathbf{Q}(t_1, \ldots, t_n),$$

изоморфно полю, порожденному n алгебраически независимыми элементами. Когда писалась эта книга, ответ еще не был известен.

Отметим, что можно задать более общий вопрос. Если $t_1, \ldots, t_n$ алгебраически независимы над полем комплексных чисел $\mathbf{C}$, то всякое ли поле E с условием $\mathbf{C} \subset E \subset \mathbf{C}(t_1, \ldots, t_n)$ изоморфно полю, порожденному r алгебраически независимыми элементами ($r \leqslant n$)? Известно, что ответ утвердителен при $n \leqslant 2$ (Люрот для $n = 1$ и Касательнуово для $n = 2$). Ни в каком другом случае ответ не известен. (Фано думал, что он нашел контрпример, но критическая переоценка в последние годы показала, что вопрос по-прежнему остается открытым.)

Пример 5. Докажем, что *поле комплексных чисел алгебраически замкнуто*. Это послужит иллюстрацией для почти всех ранее доказанных теорем.

Мы используем следующие свойства поля вещественных чисел $\mathbf{R}$: это — упорядоченное поле; всякий положительный элемент является квадратом, и всякий многочлен нечетной степени из $\mathbf{R}[X]$ имеет корень в $\mathbf{R}$. Позднее мы рассмотрим упорядоченные поля в общем случае и наши рассуждения окажутся применимыми к любому упорядоченному полю, обладающему перечисленными выше свойствами.

Пусть $i = \sqrt{-1}$ (другими словами, i — корень многочлена X^2+1). Из всякого элемента в $\mathbf{R}(i)$ извлекается квадратный корень. Если $a + bi \in \mathbf{R}(i)$, $a, b \in \mathbf{R}$, то квадратный корень задается выражением $c + di$, где

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2} \quad \text{и} \quad d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}.$$

Каждая из правых частей этих равенств положительна и, следовательно, имеет квадратный корень в $\mathbf{R}$. Затем тривиальным образом определяется знак у c и у d так, чтобы $(c + di)^2 = a + bi$.

Поскольку $\mathbf{R}$ имеет характеристику 0, всякое его конечное расширение сепарабельно. Всякое конечное расширение поля $\mathbf{R}(i)$ содержится в некотором расширении K, являющемся конечным расши-

рением Галуа над $\mathbf{R}$. Мы должны показать, что $K = \mathbf{R}(i)$. Пусть G — его группа Галуа над $\mathbf{R}$, и пусть H — силовская 2-подгруппа в G и F — неподвижное поле группы H. Подсчитывая степени и порядки, находим, что степень поля F над $\mathbf{R}$ нечетна. В силу теоремы о примитивном элементе существует элемент $\alpha \in F$, такой, что $F = \mathbf{R}(\alpha)$. Тогда α будет корнем неприводимого многочлена нечетной степени из $\mathbf{R}[X]$. Это возможно лишь в том случае, когда эта степень равна 1. Следовательно, $G = H$ — 2-группа.

Далее, мы видим, что K — расширение Галуа над $\mathbf{R}(i)$. Пусть G_1 — его группа Галуа. Так как G_1 — p-группа (с $p = 2$), то, если она нетривиальна, в ней содержится подгруппа G_2 индекса 2. Пусть F — неподвижное поле подгруппы G_2. Тогда F имеет степень 2 над $\mathbf{R}(i)$, т. е. является квадратичным расширением. Но мы видели, что из всякого элемента в $\mathbf{R}(i)$ извлекается квадратный корень и что, следовательно, $\mathbf{R}(i)$ не имеет расширений степени 2. Отсюда вытекает, что G_1 — тривиальная группа и $K = \mathbf{R}(i)$, что нам и требовалось установить.

(Основные идеи предыдущего доказательства были уже у Гаусса. Тот их вариант, который мы выбрали и в котором существенным образом использованы силовские группы, принадлежит Артину.)

Пример 6. Этот пример адресован тем, кто немного знаком с римановыми поверхностями и накрытиями. Пусть t трансцендентно над полем комплексных чисел $\mathbf{C}$. Значения t из $\mathbf{C}$ и ∞ соответствуют точкам гауссовой сферы S, рассматриваемой как риманова поверхность. Пусть $P_1, \ldots, P_{n+1}$, — различные точки сферы S. Конечные накрытия поверхности

$$S - \{P_1, \ldots, P_{n+1}\}$$

находятся в биективном соответствии с некоторыми конечными расширениями поля $\mathbf{C}(t)$, а именно теми, которые не разветвлены вне $P_1, \ldots, P_{n+1}$. Пусть K — объединение всех расширений, соответствующих таким накрытиям, и пусть $\pi_1^{(n)}$ — фундаментальная группа поверхности $S - \{P_1, \ldots, P_{n+1}\}$. Тогда, как известно, $\pi_1^{(n)}$ — свободная группа с n образующими, обладающая таким вложением в группу Галуа поля K над $\mathbf{C}(t)$, что конечные подполя в K над $\mathbf{C}(t)$ находятся в биективном соответствии с подгруппами группы $\pi_1^{(n)}$ конечного индекса. Для данной конечной группы G, порожденной n элементами $\sigma_1, \ldots, \sigma_n$, мы можем найти сюръективный гомоморфизм

$$\pi_1^{(n)} \to G,$$

переводящий образующие $\pi_1^{(n)}$ в $\sigma_1, \ldots, \sigma_n$. Пусть H — его ядро. Тогда H принадлежит подполю K^H поля K, которое нормально

над $\mathbf{C}(t)$ и группа Галуа которого есть G. На языке накрытий это означает, что H принадлежит некоторому конечному накрытию поверхности $S - \{P_1, \ldots, P_{n+1}\}$.

§ 3. Корни из единицы

Пусть k — поле. Под *корнем из единицы* (в k) мы будем понимать всякий элемент $\zeta \in k$, такой, что $\zeta^n = 1$ для некоторого $n \geqslant 1$. Если характеристика поля k равна p, то уравнение

$$X^{p^m} = 1$$

имеет только один корень, а именно 1, и, следовательно, нет никаких корней p^m-й степени из единицы, кроме 1.

Пусть n — целое число > 1, взаимно простое с характеристикой поля k. Многочлен

$$X^n - 1$$

сепарабелен, поскольку его производная nX^{n-1} обращается в нуль лишь при $X = 0$ и, значит, не имеет с $X^n - 1$ общих корней. Следовательно, в $\bar{k}$ многочлен $X^n - 1$ имеет n различных корней, являющихся корнями из единицы. Они, очевидно, образуют группу, а, как мы знаем, всякая конечная мультипликативная группа в поле циклическая (гл. V, теорема 6). Таким образом, группа корней n-й степени из единицы циклическая. Образующие этой группы называются *примитивными*, или *первообразными*, корнями n-й степени из единицы.

Пусть U_n обозначает группу всех корней n-й степени из единицы в $\bar{k}$ и m, n — взаимно простые целые числа; тогда

$$U_{mn} \approx U_m \times U_n.$$

Это следует из того, что U_m, U_n не могут иметь общих элементов, кроме 1, и, значит, $U_m U_n$ содержит ровно mn элементов, каждый из которых есть корень mn-й степени из единицы. Следовательно, $U_m U_n = U_{mn}$ (откуда и получается разложение в прямое произведение).

Теорема 6. *Для всякого примитивного корня n-й степени из единицы ζ*

$$[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n).$$

Доказательство. Пусть $f(X)$ — неприводимый многочлен элемента ζ над $\mathbf{Q}$. Тогда $f(X)$ делит многочлен $X^n - 1$, скажем $X^n - 1 = f(X)h(X)$, где f, h оба имеют старший коэффициент 1. В силу леммы Гаусса f, h имеют целые коэффициенты. Ниже мы покажем, что если p — простое число, не делящее n, то ζ^p также будет корнем многочлена f. Поскольку ζ^p — тоже примитивный корень n-й степени из единицы и поскольку любой примитивный ко-

рень n-й степени из единицы может быть получен последовательным возведением ζ в простые степени с показателями, не делящими n, то отсюда будет следовать, что все примитивные корни n-й степени из единицы являются корнями многочлена f, который поэтому имеет степень $\geqslant \varphi(n)$, и, значит, его степень равна точно $\varphi(n)$.

Предположим, что ζ^p не является корнем f. Тогда ζ^p — корень многочлена h, а сам ζ — корень $h(X^p)$. Следовательно, $f(X)$ делит $h(X^p)$, и мы можем написать

$$h(X^p) = f(X)g(X).$$

Так как f имеет целые коэффициенты и старший коэффициент 1, то и g имеет целые коэффициенты. Поскольку $a^p \equiv a \pmod{p}$ для любого целого числа a, то заключаем, что

$$h(X^p) \equiv h(X)^p \pmod{p}$$

и, следовательно,

$$h(X)^p \equiv f(X)g(X) \pmod{p}.$$

В частности, обозначив через $\bar{f}$ и $\bar{h}$ многочлены над $\mathbf{Z}/p\mathbf{Z}$, получающиеся соответственно из f и h при редукции по модулю p, мы видим, что $\bar{f}$ и $\bar{h}$ не являются взаимно простыми, т. е. имеют общий множитель. Но $X^n - \bar{1} = \bar{f}(X)\bar{h}(X)$ и, следовательно, $X^n - \bar{1}$ имеет кратные корни. Но это, как сразу видно из рассмотрения производной, невозможно, и наша теорема доказана.

Следствие. *Если n, m — взаимно простые целые числа $\geqslant 1$, то*

$$\mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_m) = \mathbf{Q}.$$

Доказательство. Заметим, что ζ_n и ζ_m содержатся оба в $\mathbf{Q}(\zeta_{mn})$, поскольку ζ_{mn}^n — примитивный корень m-й степени из единицы. Кроме того, $\zeta_m\zeta_n$ — примитивный корень степени mn из единицы. Следовательно,

$$\mathbf{Q}(\zeta_n)\,\mathbf{Q}(\zeta_m) = \mathbf{Q}(\zeta_{mn}).$$

Наше утверждение вытекает из мультипликативности $\varphi(mn) = \varphi(m)\varphi(n)$.

Предположим, что $n = p$ — простое число (не имеющее ничего общего с характеристикой). Тогда

$$X^p - 1 = (X-1)(X^{p-1} + \ldots + 1).$$

Любой примитивный корень p-й степени из единицы является корнем второго множителя в правой части этого равенства. Так как

имеется ровно $p-1$ примитивных корней p-й степени из единицы, то мы заключаем, что ими исчерпываются все корни многочлена

$$X^{p-1}+\ldots+1.$$

Мы видели в гл. V, что этот многочлен может быть преобразован в многочлен Эйзенштейна над полем рациональных чисел. Это дает другое доказательство того факта, что $[\mathbf{Q}(\zeta_p):\mathbf{Q}]=p-1$.

Пусть k — произвольное поле, n — целое число, взаимно простое с его характеристикой, $\zeta=\zeta_n$ — примитивный корень n-й степени из единицы в $\bar{k}$ и σ — вложение $k(\zeta)$ в $\bar{k}$ над k. Тогда

$$(\sigma\zeta)^n=\sigma(\zeta^n)=1,$$

так что $\sigma\zeta$ также есть корень n-й степени из единицы. Следовательно, $\sigma\zeta=\zeta^i$ для некоторого целого $i=i(\sigma)$, однозначно определенного по модулю n. Значит, σ отображает $k(\zeta)$ в себя и, таким образом, $k(\zeta)$ нормально над k. Если τ — другой автоморфизм поля $k(\zeta)$ над k, то

$$\sigma\tau\zeta=\zeta^{i(\sigma)\,i(\tau)}.$$

Так как σ и τ — автоморфизмы, то $i(\sigma)$ и $i(\tau)$ взаимно просты с n (иначе $\sigma\zeta$ имел бы период, меньший n). Таким образом, мы получаем гомоморфизм группы Галуа G поля $k(\zeta)$ над k в мультипликативную группу $(\mathbf{Z}/n\mathbf{Z})^*$ целых чисел по модулю n, взаимно простых с n. Этот гомоморфизм, очевидно, инъективен, поскольку $i(\sigma)$ однозначно определяется по модулю n автоморфизмом σ, а действие σ на $k(\zeta)$ определяется действием этого автоморфизма на ζ. Мы заключаем, что $k(\zeta)$ абелево над k.

Пусть φ — функция Эйлера. Как мы знаем, порядок группы $(\mathbf{Z}/n\mathbf{Z})^*$ равен $\varphi(n)$. Следовательно, степень $[k(\zeta):k]$ делит $\varphi(n)$.

Исследуем более подробно разложение на множители многочлена X^n-1; для простоты предположим, что характеристика равна 0. Имеем

$$X^n-1=\prod_{\omega}(X-\omega),$$

где произведение берется по всем корням n-й степени из единицы. Соберем вместе все члены, соответствующие тем корням из единицы, которые имеют одинаковый период. Пусть

$$f_d(X)=\prod_{\text{период }\omega=d}(X-\omega).$$

Тогда

$$X^n-1=\prod_{d\mid n}f_d(X).$$

Мы видим, что $f_1(X) = X - 1$ и что

$$f_n(X) = \frac{X^n - 1}{\prod\limits_{\substack{d \mid n \\ d < n}} f_d(X)}.$$

Следовательно, мы можем вычислять $f_n(X)$ рекуррентно, и видно, что $f_n(X)$ является многочленом из $\mathbf{Q}[X]$, поскольку мы последовательно делим друг на друга многочлены, имеющие коэффициенты в $\mathbf{Q}$. У всех наших многочленов старший коэффициент равен 1, так что в действительности $f_n(X)$ имеет *целочисленные коэффициенты* в силу теоремы 2 из гл. V, § 4. Таким образом, наша конструкция по существу универсальна и годна для любого поля (характеристика которого не делит n).

Мы называем $f_n(X)$ n-м *круговым* многочленом, или многочленом деления круга на n равных частей.

Корнями f_n являются в точности примитивные корни n-й степени из единицы, и, следовательно,

$$\deg f_n = \varphi(n).$$

В силу теоремы 6 мы заключаем, что f_n неприводим над $\mathbf{Q}$ и, значит,

$$f_n(X) = \operatorname{Irr}(\zeta_n, \mathbf{Q}, X).$$

Доказательства следующих рекуррентных формул мы предоставляем читателю в качестве упражнений

1. Если p — простое число, то

$$f_p(X) = X^{p-1} + X^{p-2} + \ldots + 1$$

и для любого целого $r \geqslant 1$

$$f_{p^r}(X) = f_p\left(X^{p^{r-1}}\right).$$

2. Пусть $n = p_1^{r_1} \ldots p_s^{r_s}$ — положительное целое число, разложенное на простые множители. Тогда

$$f_n(X) = f_{p_1 \ldots p_s}\left(X^{p_1^{r_1-1} \ldots p_s^{r_s-1}}\right).$$

3 Если n нечетно, то $f_{2n}(X) = f_n(-X)$.

4 Если p — простое число, не делящее n, то

$$f_{pn}(X) = \frac{f_n(X^p)}{f_n(X)}$$

5. Имеем

$$f_n(X) = \prod_{d \mid n} (X^{n/d} - 1)^{\mu(d)}.$$

Как обычно, μ — это функция Мёбиуса:

$$\mu(n)=\begin{cases} 0, & \text{если } n \text{ делится на } p^2 \text{ для некоторого простого } p; \\ (-1)^r, & \text{если } n=p_1\dots p_r\text{—произведение различных простых чисел;} \\ 1, & \text{если } n=1. \end{cases}$$

В качестве упражнения покажите, что

$$\sum_{d\mid n}\mu(d)=\begin{cases} 1 & \text{при } n=1, \\ 0 & \text{при } n>1. \end{cases}$$

Если ζ — корень n-й степени из единицы и $\zeta\neq 1$, то

$$\frac{1-\zeta^n}{1-\zeta}=1+\zeta+\dots+\zeta^{n-1}=0.$$

Это замечание тривиально, но полезно.

Пусть $\mathbf{F}_q$ — конечное поле из q элементов, где q есть некоторая степень простого числа $p\neq 2$. Тогда $\mathbf{F}_q^*$ содержит $q-1$ элементов и является циклической группой. Следовательно, индекс

$$(\mathbf{F}_q^*:\mathbf{F}_q^{*2})=2.$$

Для целого числа $\nu\not\equiv 0 \pmod p$ положим

$$\left(\frac{\nu}{p}\right)=\begin{cases} 1, & \text{если } \nu\equiv x^2 \pmod p, \\ -1, & \text{если } \nu\not\equiv x^2 \pmod p. \end{cases}$$

Эта функция, известная под названием *квадратичного символа* (или *символа Лежандра*), зависит только от класса вычетов $\nu \bmod p$.

Из нашего предыдущего замечания мы видим, что имеется ровно столько же квадратичных вычетов, сколько и невычетов по модулю p.

Пусть ζ — примитивный корень p-й степени из единицы и

$$S=\sum_{\nu}\left(\frac{\nu}{p}\right)\zeta^{\nu},$$

где сумма берется по всем ненулевым классам вычетов по модулю p. Тогда

$$S^2=\left(\frac{-1}{p}\right)p.$$

Всякое квадратичное расширение поля $\mathbf{Q}$ содержится в некотором расширении, получающемся присоединением к $\mathbf{Q}$ корня из единицы.

Доказательство. Последнее утверждение следует непосредственно из явного выражения $\pm p$ как квадрата в $\mathbf{Q}(\zeta)$, поскольку квадратный корень из любого целого числа содержится в поле, порожденном присоединением квадратных корней из простых множи-

телей, входящих в его разложение, а также $\sqrt{-1}$. Кроме того, для простого числа 2 имеет место соотношение $(1+i)^2=2i$. Докажем утверждение, касающееся S^2. Имеем

$$S^2=\sum_{\nu,\,\mu}\left(\frac{\nu}{p}\right)\left(\frac{\mu}{p}\right)\zeta^{\nu+\mu}=\sum_{\nu,\,\mu}\left(\frac{\nu\mu}{p}\right)\zeta^{\nu+\mu}.$$

Когда ν пробегает все ненулевые классы вычетов, то же самое происходит с $\nu\mu$ при любом фиксированном μ и, следовательно, замена ν на $\nu\mu$ дает

$$S^2=\sum_{\nu,\,\mu}\left(\frac{\nu\mu^2}{p}\right)\zeta^{\mu(\nu+1)}=\sum_{\nu,\,\mu}\left(\frac{\nu}{p}\right)\zeta^{\mu(\nu+1)}=$$

$$=\sum_{\mu}\left(\frac{-1}{p}\right)\zeta^0+\sum_{\nu\neq-1}\left(\frac{\nu}{p}\right)\sum_{\mu}\zeta^{\mu(\nu+1)}.$$

Но $1+\zeta+\ldots+\zeta^{p-1}=0$, так что сумма по μ, стоящая справа, равна -1. Следовательно,

$$S^2=\left(\frac{-1}{p}\right)(p-1)+(-1)\sum_{\nu\neq-1}\left(\frac{\nu}{p}\right)=p\left(\frac{-1}{p}\right)-\sum_{\nu}\left(\frac{\nu}{p}\right)=p\left(\frac{-1}{p}\right),$$

что и требовалось установить.

Мы видим, что $\mathbf{Q}(\sqrt{p})$ содержится в $\mathbf{Q}(\zeta,\sqrt{-1})$ или $\mathbf{Q}(\zeta)$ в зависимости от знака квадратичного символа для -1. Расширение поля называется *круговым*, если оно содержится в поле, полученном присоединением корней из единицы. Выше мы показали, что квадратичные расширения поля $\mathbf{Q}$ являются круговыми. Теорема Кронекера утверждает, что всякое абелево расширение поля $\mathbf{Q}$ является круговым, но ее доказательство требует техники, которая не может быть изложена в этой книге.

§ 4. *Линейная независимость характеров*

Пусть G — моноид и K — поле. Под *характером* G в K мы (в этой главе) будем понимать гомоморфизм

$$\chi\colon G\to K^*$$

моноида G в мультипликативную группу поля K. *Тривиальный* характер — это гомоморфизм, принимающий постоянное значение 1. Функции $f_i\colon G\to K$ называются *линейно независимыми* над K, если из любого соотношения вида

$$a_1f_1+\ldots+a_nf_n=0$$

с $a_i\in K$ следует, что все $a_i=0$.

Теорема 7 (Артин) *Пусть* $\chi_1, \quad , \chi_n$ *— различные характеры* G *в* K *Тогда они линейно независимы над* K

Доказательство Один характер, очевидно, линейно независим. Предположим, что имеется соотношение

$$a_1\chi_1 + \ldots + a_n\chi_n = 0,$$

где коэффициенты $a_i \in K$ не все равны 0 Возьмем такое соотношение с наименьшим возможным n. Тогда $n \geqslant 2$ и ни один a_i не равен 0 Так как χ_1, χ_2 различны, то существует элемент $z \in G$, такой, что $\chi_1(z) \neq \chi_2(z)$. Для всех $x \in G$ имеем

$$a_1\chi_1(xz) + \quad . + a_n\chi_n(xz) = 0,$$

и так как χ_i — характеры, то

$$a_1\chi_1(z)\chi_1 + \ldots + a_n\chi_n(z)\chi_n = 0$$

Разделим на $\chi_1(z)$ и вычтем из нашего первого соотношения Член $a_1\chi_1$ сократится, и мы получим соотношение

$$\left(a_2 - a_2\frac{\chi_2(z)}{\chi_1(z)}\right)\chi_2 + \ . \ = 0$$

Первый коэффициент в этом соотношении отличен от 0, и оно имеет меньшую длину, чем первоначальное соотношение — противоречие.

В качестве приложения теоремы Артина можно рассмотреть случай, когда K — конечное нормальное расширение поля k, а характеры — различные автоморфизмы $\sigma_1, \ldots, \sigma_n$ поля K над k, рассматриваемые как гомоморфизмы группы K^* в K^*. Этот частный случай был исследован уже Дедекиндом, который, однако, сформулировал теорему несколько иным образом, рассматривая определитель, составленный из $\sigma_i\omega_j$, где $\{\omega_j\}$ — подходящее множество элементов из K, и доказывая более сложным путем тот факт, что этот определитель отличен от 0 Формулировка, данная выше, и весьма элегантное доказательство теоремы принадлежат Артину

В качестве другого приложения имеем

Следствие. *Пусть* $\alpha_1, \quad , \alpha_n$ *— различные ненулевые элементы поля* K *Если* $a_1, \ldots, a_n$ *— элементы из* K, *такие, что для всех целых* ν

$$a_1\alpha_1^\nu + \ . \ + a_n\alpha_n^\nu = 0,$$

то $a_i = 0$ *для всех* i

Доказательство Применяем теорему к различным гомоморфизмам

$$\nu \longmapsto \alpha_i^\nu$$

группы $\mathbf{Z}$ в K^*.

Другое интересное приложение будет дано в упражнениях (относительные инварианты).

§ 5. Норма и след

Пусть E — конечное расширение поля k, $[E:k]_s = r$. Положим также

$$p^\mu = [E:k]_i,$$

если характеристика равна $p > 0$, и 1 — в противном случае. Пусть $\sigma_1, \ldots, \sigma_r$ — различные вложения E в алгебраическое замыкание $\bar{k}$ поля k. Для всякого элемента α из E определим его *норму* из E в k формулой

$$N_k^E(\alpha) = \prod_{\nu=1}^{r} \sigma_\nu \alpha^{p^\mu} = \left(\prod_{\nu=1}^{r} \sigma_\nu \alpha\right)^{[E\ k]_i}.$$

Аналогично определяем *след*

$$\mathrm{Tr}_k^E(\alpha) = [E:k]_i \sum_{\nu=1}^{r} \sigma_\nu \alpha.$$

След равен 0, если $[E:k]_i > 1$, другими словами, если E/k не сепарабельно. Таким образом, если E сепарабельно над k, то

$$N_k^E(\alpha) = \prod_{\sigma} \sigma\alpha,$$

где произведение берется по всем различным вложениям E в $\bar{k}$ над k.

Аналогично, если E/k сепарабельно, то

$$\mathrm{Tr}_k^E(\alpha) = \sum_{\sigma} \sigma\alpha.$$

Теорема 8. *Пусть E/k — конечное расширение. Тогда норма N_k^E является мультипликативным гомоморфизмом E^* в k^*, а след — аддитивным гомоморфизмом E в k. Если $E \supset F \supset k$ — башня полей, то оба эти отображения транзитивны, или, что равносильно,*

$$N_k^E = N_k^F \circ N_F^E \quad \text{и} \quad \mathrm{Tr}_k^E = \mathrm{Tr}_k^F \circ \mathrm{Tr}_F^E.$$

Если $E = k(\alpha)$ и $f(X) = \mathrm{Irr}(\alpha, k, X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, то

$$N_k^{k(\alpha)}(\alpha) = (-1)^n a_0 \quad \text{и} \quad \mathrm{Tr}_k^{k(\alpha)}(\alpha) = -a_{n-1}.$$

Доказательство. Для доказательства первого утверждения заметим, что элемент α^{p^μ} сепарабелен над k, если $p^\mu = [E:k]_i$. С другой стороны, произведение

$$\prod_{\nu=1}^{r} \sigma_\nu \alpha^{p^\mu}$$

остается неподвижным при любом изоморфизме в $\bar{k}$, поскольку применение такого изоморфизма просто переставляет множители. Следовательно, это произведение должно лежать в k, так как α^{p^μ} сепарабелен над k. Аналогичное рассуждение применимо и к следу.

Что касается второго утверждения, то пусть $\{\tau_j\}$ — семейство различных вложений F в $\bar{k}$ над k. Продолжим каждое τ_j до изоморфизма $\bar{k}$ на $\bar{k}$ и обозначим это продолжение по-прежнему через τ_j. (Не теряя общности, мы можем предполагать, что $F \subset \bar{k}$.) Пусть $\{\sigma_i\}$ — семейство вложений E в $\bar{k}$ над F. Если σ — некоторое вложение E над k в $\bar{k}$, то $\tau_j^{-1}\sigma$ при каком-то j оставляет F неподвижным и, таким образом, $\tau_j^{-1}\sigma = \sigma_i$ для некоторого i. Следовательно, $\sigma = \tau_j\sigma_i$ и, значит, семейство $\{\tau_j\sigma_i\}$ дает все различные вложения E в $\bar{k}$ над k. В башнях степень несепарабельности мультипликативна, так что наше утверждение о транзитивности нормы и следа очевидно, поскольку, как мы уже показали, N_F^E отображает E в F, и аналогично для следа.

Предположим теперь, что $E = k(\alpha)$. Имеем

$$f(X) = ((X - \alpha_1) \dots (X - \alpha_r))^{[E:k]_i},$$

где $\alpha_1, \dots, \alpha_r$ — различные корни f. Рассмотрение постоянного члена f дает нам выражение для нормы, а рассмотрение второго члена — выражение для следа.

Заметим, что след является k-линейным отображением поля E в k, а именно

$$\mathrm{Tr}_k^E(c\alpha) = c\,\mathrm{Tr}_k^E(\alpha)$$

для всех $\alpha \in E$ и $c \in k$. Это очевидно, поскольку c остается неподвижным при всяком вложении E над k. Таким образом, след есть k-линейный функционал из E в k. Для простоты мы будем писать Tr вместо Tr_k^E.

Теорема 9. *Пусть E — конечное сепарабельное расширение поля k. Тогда функционал* $\mathrm{Tr}\colon E \to k$ *ненулевой. Отображение* $E \times E \to k$, *определяемое правилом*

$$(x, y) \longmapsto \mathrm{Tr}(xy),$$

билинейно и отождествляет E с дуальным ему пространством.

Доказательство. Тот факт, что Tr отличен от нуля, следует из теоремы о линейной независимости характеров. Для всякого $x \in E$ отображение

$$\mathrm{Tr}_x\colon E \to k,$$

для которого $\mathrm{Tr}_x(y) = \mathrm{Tr}(xy)$, будет, очевидно, k-линейным, и отображение

$$x \longmapsto \mathrm{Tr}_x$$

будет k-гомоморфизмом E в дуальное ему пространство $\hat{E}$. (Мы не обозначаем сейчас дуальное пространство через E^*, используя звездочку для обозначения мультипликативной группы поля E.) Если Tr_x — нулевое отображение, то $\mathrm{Tr}(xE) = 0$. Но $xE = E$ при $x \neq 0$. Следовательно, ядро отображения $x \longmapsto \mathrm{Tr}_x$ равно 0 и мы получаем инъективный гомоморфизм E в дуальное пространство $\hat{E}$. Так как эти пространства имеют одинаковую размерность, то, значит, мы получаем изоморфизм. Это доказывает нашу теорему.

Следствие 1. *Пусть* $\omega_1, \ldots, \omega_n$ *— базис* E *над* k. *Тогда существует базис* $\omega_1', \ldots, \omega_n'$ *пространства* E *над* k, *для которого* $\mathrm{Tr}(\omega_i \omega_j') = \delta_{ij}$.

Доказательство. Базис $\omega_1', \ldots, \omega_n'$ есть не что иное, как дуальный базис, который мы определили, когда рассматривали дуальное пространство для произвольного векторного пространства.

Следствие 2. *Пусть* E *— конечное сепарабельное расширение поля* k *и* $\sigma_1, \ldots, \sigma_n$ *— множество различных вложений* E *в* $\bar{k}$ *над* k. *Пусть* $w_1, \ldots, w_n$ *— некоторые элементы из* E. *Тогда векторы*

$$\xi_1 = (\sigma_1 w_1, \ldots, \sigma_1 w_n),$$
$$\ldots\ldots\ldots\ldots$$
$$\xi_n = (\sigma_n w_1, \ldots, \sigma_n w_n)$$

линейно независимы над $\bar{k}$ *в том и только в том случае, если* $w_1, \ldots, w_n$ *образуют базис* E *над* k.

Доказательство. Предположим, что $w_1, \ldots, w_n$ образуют базис расширения E/k. Пусть $\alpha_1, \ldots, \alpha_n$ — элементы из $\bar{k}$, для которых

$$\alpha_1 \xi_1 + \ldots + \alpha_n \xi_n = 0.$$

Тогда отображение

$$\alpha_1 \sigma_1 + \ldots + \alpha_n \sigma_n,$$

примененное к каждому из элементов $w_1, \ldots, w_n$, дает 0. Но $\sigma_1, \ldots, \sigma_n$ линейно независимы как характеры мультипликативной группы E^* в $\bar{k}^*$. Отсюда вытекает, что $\alpha_i = 0$ для $i = 1, \ldots, n$ и наши векторы линейно независимы.

Обратно, предположим, что $w_1, \ldots, w_n$ линейно зависимы над k. Тогда в E найдется элемент $\alpha \neq 0$, для которого $\mathrm{Tr}\,\alpha\omega_i = 0$

при всех i, откуда $\sum_{j=1}^{n} \sigma_j(\alpha)\xi_j=0$. А это и означает, что векторы ξ_j линейно зависимы.

Замечание. В случае характеристики 0 тот факт, что след не равен тождественно 0, совсем тривиален. Действительно, если $c \in k$ и $c \neq 0$, то $\mathrm{Tr}(c)=nc$, где $n=[E:k]$ и $nc \neq 0$. Это соображение сохраняет силу также и в случае характеристики p, взаимно простой с n.

Предложение 1. *Пусть $E=k(\alpha)$—сепарабельное расширение, $f(X)=\mathrm{Irr}(\alpha, k, X)$ и $f'(X)$—производная многочлена $f(X)$. Пусть*

$$\frac{f(X)}{(X-\alpha)}=\beta_0+\beta_1 X+\ldots+\beta_{n-1}X^{n-1},$$

где $\beta_i \in E$. Тогда дуальным базисом для $1, \alpha, \ldots, \alpha^{n-1}$ будет

$$\frac{\beta_0}{f'(\alpha)}, \ \ldots, \ \frac{\beta_{n-1}}{f'(\alpha)}.$$

Доказательство. Пусть $\alpha_1, \ldots, \alpha_n$ — различные корни f. Тогда

$$\sum_{i=1}^{n} \frac{f(X)}{(X-\alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)} = X^r \quad \text{для} \quad 0 \leqslant r \leqslant n-1.$$

Чтобы усмотреть это, обозначим через $g(X)$ разность левой и правой частей этого равенства. Тогда g — многочлен степени не более $n-1$, имеющий n корней $\alpha_1, \ldots, \alpha_n$. Следовательно, g тождественно равен нулю.

Многочлены

$$\frac{f(X)}{(X-\alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)}$$

все сопряжены между собой. Если мы назовем следом многочлена с коэффициентами в E многочлен, полученный применением следа к коэффициентам, то

$$\mathrm{Tr}\left[\frac{f(X)}{(X-\alpha)} \frac{\alpha^r}{f'(\alpha)}\right]=X^r.$$

Рассмотрев коэффициенты при каждой степени X в этом равенстве, мы найдем, что

$$\mathrm{Tr}\left(\alpha^i \frac{\beta_j}{f'(\alpha)}\right)=\delta_{ij},$$

что и доказывает наше предложение.

§ 6. *Циклические расширения*

Напомним, что конечное расширение называется циклическим, если оно является расширением Галуа и его группа Галуа циклическая.

Теорема 90 Гильберта. *Пусть K/k — циклическое расширение с группой Галуа G. Пусть σ — образующая группы G и $\beta \in K$. Норма $N_k^K(\beta) = N(\beta)$ равна 1 в том и только в том случае, когда существует элемент $\alpha \neq 0$ в K, такой, что $\beta = \alpha/\sigma\alpha$.*

Доказательство. Предположим, что такой элемент α существует. Беря норму от β, получаем $N(\alpha)/N(\sigma\alpha)$. Но норма — это произведение по всем автоморфизмам из G. Применение σ лишь переставляет эти автоморфизмы. Следовательно, норма равна 1.

Будет удобно использовать экспоненциальные обозначения. Если τ, $\tau' \in G$ и $\xi \in K$, то пишем

$$\xi^{\tau+\tau'} = \xi^{\tau}\xi^{\tau'}.$$

В силу теоремы Артина о характерах отображение

$$\mathrm{id} + \beta\sigma + \beta^{1+\sigma}\sigma^2 + \ldots + \beta^{1+\sigma+\ldots+\sigma^{n-2}}\sigma^{n-1}$$

не равно тождественно нулю. Следовательно, существует $\theta \in K$, для которого элемент

$$\alpha = \theta + \beta\theta^{\sigma} + \beta^{1+\sigma}\theta^{\sigma^2} + \ldots + \beta^{1+\sigma+\ldots+\sigma^{n-2}}\theta^{\sigma^{n-1}}$$

не равен нулю. Если воспользоваться тем фактом, что $N(\beta) = 1$ и что, следовательно, при применении σ к последнему члену суммы мы получим $\beta^{-1}\theta$, то становится очевидным, что $\beta\alpha^{\sigma} = \alpha$. Чтобы завершить доказательство, разделим на α^{σ}.

Теорема 10. *Пусть k — поле, n — целое число > 0, взаимно простое с характеристикой поля k, причем в k имеется примитивный корень n-й степени из единицы.*

(а) *Если K — циклическое расширение степени n, то существует элемент $\alpha \in K$, такой, что $K = k(\alpha)$ и α удовлетворяет уравнению $X^n - a = 0$ для некоторого $a \in k$.*

(б) *Обратно, пусть $a \in k$ и α — некоторый корень многочлена $X^n - a$. Тогда $k(\alpha)$ — циклическое расширение над k степени d, $d \mid n$ и α^d — элемент из k.*

Доказательство. Пусть ζ — примитивный корень n-й степени из единицы в k, K/k — циклическое расширение с группой G и σ — образующая G. Имеем $N(\zeta^{-1}) = (\zeta^{-1})^n = 1$. В силу теоремы 90 Гильберта существует элемент $\alpha \in K$, такой, что $\sigma\alpha = \zeta\alpha$. Поскольку

ζ лежит в k, то $\sigma^i\alpha = \zeta^i\alpha$ для $i = 1, \ldots, n$. Следовательно, элементы $\zeta^i\alpha$ составляют n различных сопряженных с α над k, откуда вытекает, что $[k(\alpha) : k]$ не меньше, чем n. Так как $[K : k] = n$, то $K = k(\alpha)$. Кроме того,

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = \alpha^n.$$

Неподвижный относительно σ элемент α^n будет неподвижен относительно всякой степени σ и, следовательно, неподвижен относительно G. Поэтому α^n лежит в k и мы полагаем $a = \alpha^n$. Это доказывает первую часть теоремы.

Обратно, пусть $a \in k$ и α — корень многочлена $X^n - a$. Тогда $\zeta^i\alpha$ для всякого $i = 1, \ldots, n$ также является корнем этого многочлена и, следовательно, все его корни лежат в поле $k(\alpha)$, которое тем самым нормально над k. При этом все корни различны, так что $k(\alpha)$ является расширением Галуа над k. Пусть G — его группа Галуа.

Если σ — автоморфизм расширения $k(\alpha)/k$, то $\sigma\alpha$ также будет корнем многочлена $X^n - a$. Следовательно, $\sigma\alpha = \omega_\sigma\alpha$, где ω_σ — некоторый корень n-й степени из единицы, не обязательно примитивный. Отображение $\sigma \mapsto \omega_\sigma$ является, очевидно, гомоморфизмом G в группу корней n-й степени из единицы, причем инъективным. Так как всякая подгруппа циклической группы циклическая, то мы заключаем, что G — циклическая группа, скажем, порядка d и $d \mid n$. Образ G есть циклическая группа порядка d. Если σ — образующая G, то ω_σ — примитивный корень d-й степени из единицы. Далее получаем

$$\sigma(\alpha^d) = (\sigma\alpha)^d = (\omega_\sigma\alpha)^d = \alpha^d.$$

Следовательно, элемент α^d неподвижен относительно G. Это элемент из k, и наша теорема доказана.

Теперь мы переходим к аналогу теоремы 90 Гильберта в характеристике p для циклического расширения степени p.

Теорема 90 Гильберта (аддитивная форма). *Пусть k — поле, K/k — циклическое расширение степени n с группой G и σ — образующая G. Пусть $\beta \in K$. След $\mathrm{Tr}_k^K(\beta)$ равен 0 в том и только в том случае, когда существует элемент $\alpha \in K$, такой, что $\beta = \alpha - \sigma\alpha$.*

Доказательство. Если такой элемент α существует, то след будет 0, поскольку след равен сумме, взятой по всем элементам G, а применение σ лишь переставляют эти элементы.

Обратно, предположим, что $\mathrm{Tr}(\beta) = 0$. Существует элемент $\theta \in K$, для которого $\mathrm{Tr}(\theta) \neq 0$. Положим

$$\alpha = \frac{1}{\mathrm{Tr}(\theta)}\left[\beta\theta^\sigma + (\beta + \sigma\beta)\theta^{\sigma^2} + \ldots + (\beta + \sigma\beta + \ldots + \sigma^{n-2}\beta)\theta^{\sigma^{n-1}}\right].$$

Отсюда сразу вытекает, что $\beta = \alpha - \sigma\alpha$.

Теорема 11 (Артин — Шрейер). *Пусть k — поле характеристики p.*

(а) *Если K — циклическое расширение над k степени p, то существует элемент $\alpha \in K$, такой, что $K = k(\alpha)$, причем α удовлетворяет уравнению $X^p - X - a = 0$ для некоторого $a \in k$.*

(б) *Обратно, для данного элемента $a \in k$ многочлен $f(X) = X^p - X - a$ либо имеет корень в k, и тогда все его корни лежат в k, либо неприводим. В последнем случае, если α — некоторый его корень, то $k(\alpha)$ — циклическое расширение степени p над k.*

Доказательство. Пусть K/k — циклическое расширение степени p. Тогда $\mathrm{Tr}_k^K(-1) = 0$ (это просто результат сложения -1 с собой p раз). Пусть σ — образующая группы Галуа. В силу аддитивной формы теоремы 90 Гильберта имеется элемент $\alpha \in K$, для которого $\sigma\alpha - \alpha = 1$, или, что то же самое, $\sigma\alpha = \alpha + 1$. Следовательно, $\sigma^i\alpha = \alpha + i$ для всех целых чисел $i = 1, \ldots, p$ и α имеет p различных сопряженных, так что $[k(\alpha) : k] \geqslant p$. Отсюда вытекает, что $K = k(\alpha)$. Заметим, что

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha.$$

Следовательно, элемент $\alpha^p - \alpha$, неподвижный относительно σ, будет неподвижен относительно степеней σ, а потому и относительно G. Таким образом, он лежит в неподвижном поле k. Полагая $a = \alpha^p - \alpha$, видим, что наше первое утверждение доказано.

Обратно, пусть $a \in k$. Если α — корень многочлена $X^p - X - a$, то $\alpha + i$ при $i = 1, \ldots, p$ также служит его корнем. Таким образом, $f(X)$ имеет p различных корней. Если один корень лежит в k, то и все корни лежат в k. Допустим, что ни один из корней не лежит в k. Мы утверждаем, что многочлен неприводим. Предположим, что

$$f(X) = g(X)\,h(X),$$

где $g, h \in k[X]$ и $1 \leqslant \deg g < p$. Так как

$$f(X) = \prod_{i=1}^{p} (X - \alpha - i),$$

то $g(X)$ совпадает с произведением по некоторым целым числам i. Пусть $d = \deg g$. Коэффициент при X^{d-1} будет суммой членов $-(\alpha + i)$, взятой точно по d целым числам i. Следовательно, он равен $-d\alpha + j$, где j — некоторое целое число. Но $d \neq 0$ в k и, значит, α лежит в k, поскольку коэффициенты g лежат в k — противоречие. Таким образом, $f(X)$ неприводим. Все его корни лежат в поле $k(\alpha)$, которое по этой причине нормально над k. Так как $f(X)$ не имеет кратных корней, то $k(\alpha)$ будет расширением Галуа

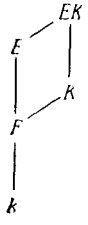
над k. Имеется автоморфизм σ поля $k(\alpha)$ над k, такой, что $\sigma\alpha = \alpha + 1$ (поскольку $\alpha + 1$ также корень). Степени σ^i автоморфизма σ дают $\sigma^i(\alpha) = \alpha + i$ для $i = 1, \ldots, p$ и поэтому все различны. Следовательно, группа Галуа состоит из этих степеней, а потому является циклической, что и доказывает теорему.

§ 7. Разрешимые и радикальные расширения

Конечное расширение E/k (которое мы для удобства будем предполагать сепарабельным) называется *разрешимым*, если группа Галуа наименьшего расширения Галуа K над k, содержащего E, является разрешимой группой. Это эквивалентно тому, что существует разрешимое расширение Галуа L поля k, такое, что $k \subset E \subset L$. Действительно, имеем $k \subset E \subset K \subset L$ и $G(K/k)$ есть гомоморфный образ группы $G(L/k)$.

Предложение 2. *Разрешимые расширения образуют отмеченный класс расширений.*

Доказательство. Пусть E/k разрешимо и F — поле, содержащее k, причем E, F — подполя некоторого алгебраически замкнутого поля. Пусть K — разрешимое расширение Галуа над k и $E \subset K$. Тогда KF будет расширением Галуа над F и $G(KF/F)$ — подгруппой в $G(K/k)$ в силу теоремы 4 из § 1. Следовательно, EF/F разрешимо. Ясно, что подрасширение разрешимого расширения разрешимо. Пусть $E \supset F \supset k$ — башня с разрешимыми расширениями E/F и F/k. Пусть K — конечное разрешимое расширение Галуа поля k, содержащее F. Как мы только что видели, EK/K разрешимо. Пусть L — разрешимое расширение Галуа поля K, содержащее EK. Если σ — *произвольное вложение L над k в заданное алгебраическое замыкание*, то $\sigma K = K$ и, следовательно, σL — разрешимое расширение поля K. Пусть M — композит всех расширений σL для всех вложений σ поля L над k. Тогда M — расширение Галуа над k, а следовательно, и над K. Группа Галуа поля M над K является подгруппой произведения $\prod_{\sigma} G(\sigma L/K)$,



в силу теоремы 5 из § 1. Следовательно, она разрешима. По теореме 3 из § 1 имеет место сюръективный гомоморфизм $G(M/k) \to G(K/k)$. Значит, группа Галуа расширения M/k имеет разрешимую нормальную подгруппу, факторгруппа по которой разрешима. Поэтому она сама разрешима. Так как $E \subset M$, то наше доказательство закончено.

Конечное расширение F поля k называется *разрешимым в радикалах*, если оно сепарабельно и если существует конечное расширение E поля k, содержащее F и обладающее разложением в башню

$$k \subset E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_m = E,$$

таким, что каждый этаж E_{i+1}/E_i принадлежит к одному из следующих типов:

(1) получается присоединением корня из единицы;

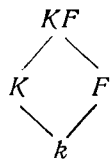
(2) получается присоединением корня многочлена $X^n - a$, где $a \in E_i$ и n взаимно просто с характеристикой;

(3) получается присоединением корня уравнения $X^p - X - a$, где $a \in E_i$ и p — характеристика > 0.

Сразу же видно, что класс расширений, разрешимых в радикалах, является отмеченным классом.

Теорема 12. *Пусть E — сепарабельное расширение поля k. Тогда E разрешимо в радикалах в том и только в том случае, если E/k разрешимо.*

Доказательство. Предположим, что E/k разрешимо. Пусть K — конечное разрешимое расширение Галуа поля k, содержащее E; m — произведение всех степеней простых чисел, не равных характеристике и делящих степень $[K : k]$; $F = k(\zeta)$, где ζ — примитивный корень m-й степени из единицы. Тогда F/k абелево. Поднимем K над F. Тогда KF разрешимо над F. Между F и KF имеется башня подполей



такая, что каждый ее этаж — циклический простого порядка, поскольку всякая разрешимая группа обладает башней подгрупп такого типа, и мы можем применить теорему 3 из § 1. В силу теорем 10 и 11 заключаем, что KF разрешимо в радикалах над F и, следовательно, разрешимо в радикалах над k. Это доказывает, что E/k разрешимо в радикалах.

Обратно, предположим, что E/k разрешимо в радикалах. Для любого вложения σ поля E в $\bar{E}$ над k расширение $\sigma E/k$ также

разрешимо в радикалах. Следовательно, наименьшее содержащее E расширение Галуа K поля k, которое является композитом E и его сопряженных, разрешимо в радикалах. Пусть m — произведение всех степеней простых чисел, не равных характеристике и делящих степень $[K:k]$. Положим снова $F=k(\zeta)$, где ζ — примитивный корень m-й степени из единицы. Достаточно доказать, что KF разрешимо над F, поскольку отсюда будет вытекать, что KF разрешимо над k и, следовательно, группа $G(K/k)$, являющаяся гомоморфным образом группы $G(KF/k)$, разрешима. Но KF/F может быть разложено в башню расширений, каждый этаж которой имеет простую степень и принадлежит к типу, описанному в теоремах 10 и 11, причем соответствующие корни из единицы лежат в поле F. Следовательно, KF/F разрешимо, и наша теорема доказана.

Замечание. Можно было бы так видоизменить предыдущее изложение, чтобы не предполагать сепарабельности. Тогда нужно было бы иметь дело с нормальными расширениями вместо расширений Галуа и считать уравнения $X^p-a=0$ разрешимыми в радикалах, когда p равно характеристике. При этом будет иметь место теорема, соответствующая теореме 12. Доказательства очевидны ввиду § 7 из гл. VII.

§ 8. Теория Куммера

В этом параграфе мы дадим обобщение теоремы, касающейся циклических расширений, на тот случай, когда основное поле содержит достаточно много корней из единицы.

Пусть k — поле и m — положительное целое число. Расширение Галуа K поля k с группой G называется расширением *показателя* m, если $\sigma^m=1$ для всех $\sigma\in G$.

Мы будем исследовать абелевы расширения показателя m. Сначала предположим, что m взаимно просто с характеристикой поля k и что k содержит примитивный корень m-й степени из единицы. Обозначим через Z_m группу корней m-й степени из 1. Будем предполагать в этом параграфе, что все наши алгебраические расширения содержатся в некотором фиксированном алгебраическом замыкании $\bar{k}$.

Пусть $a\in k$. Выражение $a^{1/m}$ $\left(\text{или } \sqrt[m]{a}\right)$ не определено однозначно. Если $\alpha^m=a$ и ζ — корень m-й степени из единицы, то также и $(\zeta\alpha)^m=a$. Мы будем использовать символ $a^{1/m}$ для обозначения любого такого элемента α и все такие элементы α будем называть корнями m-й степени из a. Заметим, что, поскольку корни m-й степени из единицы лежат в основном поле, поле $k(\alpha)$ будет одним и тем же независимо от того, какой корень m-й степени α из a мы выберем. Мы будем обозначать это поле символом $k(a^{1/m})$.

Обозначим через k^{*m} подгруппу в k^*, состоящую из всех m-х степеней ненулевых элементов из k. Это образ группы k^* при гомоморфизме $x \longmapsto x^m$.

Пусть B — подгруппа k^*, содержащая k^{*m}. Мы будем обозначать символом $k(B^{1/m})$, или K_B, композит всех полей $k(a^{1/m})$ с $a \in B$. Он однозначно определен подгруппой B как подполе в $\bar{k}$.

Пусть $a \in B$ и α — корень m-й степени из a. Многочлен $X^m - a$ разлагается на линейные множители в K_B, и, таким образом, K_B — расширение Галуа над k, поскольку это выполняется для всех $a \in B$. Пусть G — его группа Галуа. Если $\sigma \in G$, то $\sigma\alpha = \omega_\sigma \alpha$, где $\omega_\sigma \in Z_m \subset k^*$ — некоторый корень m-й степени из единицы. Отображение

$$\sigma \longmapsto \omega_\sigma$$

является, очевидно, гомоморфизмом G в Z_m, т. е. для τ, $\sigma \in G$ имеем $\tau\sigma\alpha = \omega_\tau \omega_\sigma \alpha = \omega_\sigma \omega_\tau \alpha$. Мы можем написать $\omega_\sigma = \sigma\alpha/\alpha$. Этот корень из единицы ω_σ не зависит от выбора корня m-й степени из a, поскольку если α' — другой корень m-й степени, то $\alpha' = \zeta\alpha$ для некоторого $\zeta \in Z_m$, откуда

$$\sigma\alpha'/\alpha' = \zeta\sigma\alpha/\zeta\alpha = \sigma\alpha/\alpha.$$

Обозначим ω_σ символом $\langle \sigma, a \rangle$. Соответствие

$$(\sigma, a) \longmapsto \langle \sigma, a \rangle$$

дает нам отображение

$$G \times B \to Z_m.$$

Если $a, b \in B$ и $\alpha^m = a$, $\beta^m = b$, то $(\alpha\beta)^m = ab$ и, следовательно,

$$\sigma(\alpha\beta)/\alpha\beta = (\sigma\alpha/\alpha)(\sigma\beta/\beta).$$

Отсюда, заключаем, что предыдущее отображение билинейно. Кроме того, если $a \in k^{*m}$, то $\langle \sigma, a \rangle = 1$.

Теорема 13. *Пусть k — поле и m — целое число > 0, взаимно простое с характеристикой поля k, причем примитивный корень m-й степени из единицы лежит в k. Пусть B — подгруппа в k^*, содержащая k^{*m}, и $K_B = k(B^{1/m})$. Тогда K_B — абелево расширение Галуа показателя m. Пусть G — его группа Галуа. Имеет место билинейное отображение*

$$G \times B \to Z_m, \quad \textit{задаваемое соответствием} \quad (\sigma, a) \longmapsto \langle \sigma, a \rangle.$$

Если $\sigma \in G$, $a \in B$ и $\alpha^m = a$, то $\langle \sigma, a \rangle = \sigma\alpha/\alpha$. Ядро слева равно 1, а ядро справа есть k^{*m}. Расширение K_B/k конечно тогда и только тогда, когда индекс $(B : k^{*m})$ конечен, и в этом случае

$$[K_B : k] = (B : k^{*m}).$$

Доказательство. Пусть $\sigma \in G$, причем $\langle \sigma, a \rangle = 1$ для всех $a \in B$. Тогда $\sigma\alpha = \alpha$ для всякого примитивного элемента α поля K_B, такого, что $\alpha^m = a \in B$. Следовательно, σ индуцирует тождественное отображение на K_B и ядро слева равно 1. Пусть $a \in B$, причем $\langle \sigma, a \rangle = 1$ для всех $\sigma \in G$. Рассмотрим подполе $k(a^{1/m})$ в K_B. Если $a^{1/m}$ не лежит в k, то существует автоморфизм поля $k(a^{1/m})$ над k, не являющийся тождественным. Продолжим этот автоморфизм на K_B и обозначим продолжение снова через σ. Тогда ясно, что $\langle \sigma, a \rangle \neq 1$. Это доказывает наше утверждение.

В силу теоремы двойственности из гл. I, § 11 мы видим, что группа G конечна тогда и только тогда, когда конечна группа B/k^{*m}, и в этом случае порядок G равен индексу $(B : k^{*m})$.

Теорема 14. *В обозначениях теоремы* 13 *отображение* $B \longmapsto K_B$ *дает биективное соответствие между множеством подгрупп в* k^*, *содержащих* k^{*m}, *и множеством абелевых расширений над* k *показателя* m.

Доказательство. Пусть B_1, B_2 — подгруппы в k^*, содержащие k^{*m}. Если $B_1 \subset B_2$, то $k(B_1^{1/m}) \subset k(B_2^{1/m})$. Обратно, предположим, что $k(B_1^{1/m}) \subset k(B_2^{1/m})$. Мы хотим доказать, что $B_1 \subset B_2$. Пусть $b \in B_1$. Тогда $k(b^{1/m}) \subset k(B_2^{1/m})$, причем $k(b^{1/m})$ содержится в конечно порожденном подрасширении в $k(B_2^{1/m})$. Таким образом, не теряя общности, мы можем предполагать, что группа B_2/k^{*m} — конечно порожденная и, следовательно, конечная. Пусть B_3 — подгруппа в k^*, порожденная B_2 и b. Тогда $k(B_2^{1/m}) = k(B_3^{1/m})$, а из того, что мы видели выше, вытекает, что степень этого поля над k есть

$$(B_2 : k^{*m}) \quad \text{или} \quad (B_3 : k^{*m}).$$

Таким образом, эти два индекса равны и $B_2 = B_3$. Это доказывает, что $B_1 \subset B_2$.

Итак, мы получили вложение нашего множества групп B в множество абелевых расширений поля k, имеющих показатель m. Предположим теперь, что K — некоторое абелево расширение над k показателя m. Любое конечное подрасширение есть композит циклических расширений показателя m, поскольку всякая конечная абелева группа является произведением циклических групп, и мы можем применить следствие 2 теоремы 5, § 1. В силу теоремы 10 всякое циклическое расширение может быть получено присоединением корня m-й степени. Следовательно, K может быть получено присоединением семейства корней m-й степени, скажем корней m-й степени из элементов $\{b_j\}_{j \in J}$, где $b_j \in k^*$. Пусть B — подгруппа в k^*, порожденная всеми b и k^{*m}.

Если $b' = ba^m$, где $a,\ b \in k$, то, очевидно,

$$k\left(b'^{1/m}\right) = k\left(b^{1/m}\right).$$

Следовательно, $k\left(B^{1/m}\right) = K$, что и требовалось доказать.

В случае когда мы имеем дело с абелевыми расширениями показателя p, равного характеристике, мы должны развить аддитивную теорию, находящуюся к теоремам 13 и 14 в таком же отношении, как теорема 11 к теореме 10.

Пусть k — поле характеристики p. Определим оператор $\wp$, положив

$$\wp(x) = x^p - x$$

для $x \in k$. Тогда $\wp$ есть аддитивный гомоморфизм поля k в себя. Подгруппа $\wp(k)$ играет ту же роль, что и подгруппа k^{*m} в мультипликативной теории для случая, когда m — простое число. Теория, касающаяся степеней p, несколько сложнее и принадлежит Витту. Читателя, желающего посмотреть, как она выглядит, мы отсылаем к упражнениям.

Корень многочлена $X^p - X - a$ с $a \in k$ будем обозначать через $\wp^{-1}a$. Для всякой подгруппы B в k, содержащей $\wp k$, положим $K_B = k\left(\wp^{-1}B\right)$. Это поле, полученное присоединением $\wp^{-1}a$ к k для всех $a \in B$. Подчеркнем тот факт, что B — *аддитивная* подгруппа в k.

Теорема 15. *Пусть k — поле характеристики p. Отображение $B \longmapsto k\left(\wp^{-1}B\right)$ является биективным соответствием между подгруппами в k, содержащими $\wp k$, и абелевыми расширениями поля k, имеющими показатель p. Пусть $K = K_B = k\left(\wp^{-1}B\right)$ и G — группа Галуа этого расширения. Имеет место билинейное отображение*

$$G \times B \to \mathbf{Z}/p\mathbf{Z}, \text{ задаваемое правилом } (\sigma,\ a) \longmapsto \langle \sigma,\ a \rangle.$$

Если $\sigma \in G$, $a \in B$ и $\wp\alpha = a$, то $\langle \sigma,\ a \rangle = \sigma\alpha - \alpha$. Ядро слева равно 1, а ядро справа есть $\wp k$. Расширение K_B/k конечно тогда и только тогда, когда индекс $(B : \wp k)$ конечен, и в этом случае

$$[K_B : k] = (B : \wp k).$$

Доказательство. Доказательство полностью аналогично доказательствам теорем 13 и 14. Оно может быть получено заменой умножения сложением и использованием „$\wp$-х корней“ вместо корней m-й степени. Никаких других изменений в доказательстве не требуется.

Аналогичная теорема для абелевых расширений показателя p^n требует векторов Витта и будет изложена в упражнениях.

§ 9. Уравнение $X^n - a = 0$

Когда корни из единицы не содержатся в основном поле, уравнение $X^n - a = 0$ по-прежнему представляет интерес, но требует более деликатного обращения.

Теорема 16. *Пусть k — поле, n — целое число $\geqslant 2$ и $a \in k$, $a \neq 0$, причем $a \notin k^p$ для всех простых чисел p, делящих n, и $a \notin -4k^4$, если $4 \mid n$. Тогда многочлен $X^n - a$ неприводим в $k[X]$.*

Доказательство. Наше первое предположение означает, что a не является p-й степенью в k. По индукции мы сведем нашу теорему к случаю, когда n — степень простого числа.

Запишем $n = p^r m$, где p взаимно просто с m и нечетно. Пусть

$$X^m - a = \prod_{\nu=1}^{m} (X - \alpha_\nu)$$

— разложение $X^m - a$ на линейные множители и, скажем, $\alpha = \alpha_1$. Подставляя X^{p^r} вместо X, получаем

$$X^n - a = X^{p^r m} - a = \prod_{\nu=1}^{m} (X^{p^r} - \alpha_\nu).$$

По индукции можно считать, что $X^m - a$ неприводим в $k[X]$. Мы утверждаем, что α не является p-й степенью в $k(\alpha)$. Действительно, пусть $\alpha = \beta^p$, $\beta \in k(\alpha)$ и N — норма из $k(\alpha)$ в k. Тогда

$$-a = (-1)^m N(\alpha) = (-1)^m N(\beta^p) = (-1)^m N(\beta)^p.$$

Если m нечетно, то a будет p-й степенью, что невозможно. Аналогично, если m четно (а p нечетно), мы также получаем противоречие. Это доказывает наше утверждение, поскольку m взаимно просто с p. Считая теорему известной для степеней простых чисел, заключаем, что многочлен $X^{p^r} - \alpha$ неприводим над $k(\alpha)$. Если A — корень многочлена $X^{p^r} - \alpha$, то $k \subset k(\alpha) \subset k(A)$ — башня, нижний этаж которой имеет степень m, а верхний — степень p^r. Отсюда вытекает, что A имеет степень n над k и что, следовательно, многочлен $X^n - a$ неприводим.

Пусть теперь $n = p^r$ — степень простого числа.

Предположим, что p совпадает с характеристикой. Пусть α — корень p-й степени из a. Тогда $X^p - a = (X - \alpha)^p$ и, следовательно, $X^{p^r} - a = (X^{p^{r-1}} - \alpha)^p$ при $r \geqslant 2$. По соображениям, еще более тривиальным, чем вышеприведенные, мы видим, что α не является p-й степенью в $k(\alpha)$ и, значит, $X^{p^{r-1}} - \alpha$ неприводим над $k(\alpha)$. Следовательно, $X^{p^r} - a$ неприводим над k.

Предположим, что p не совпадает с характеристикой. Снова рассуждаем по индукции. Пусть α — некоторый корень многочлена $X^p - a$. Сначала рассмотрим случай $r = 1$. Пусть ζ — примитивный корень p-й степени из единицы. Многочлен $X^p - a$ над $k(\zeta)$ либо неприводим, либо разлагается на линейные множители. Во втором случае $k(\alpha) \subset k(\zeta)$. Поскольку $k(\zeta)/k$ абелево, то $k(\alpha)$ есть расширение Галуа над k. Так как всякий сопряженный с α элемент имеет вид $\zeta'\alpha$, где ζ' — некоторый примитивный корень p-й степени из единицы, то $k(\alpha) = k(\zeta)$. Следовательно, все корни $X^p - a$, не лежащие в k, имеют одинаковую степень над k, делящую $p - 1$. Но это невозможно и, следовательно, многочлен $X^p - a$ неприводим. Пусть теперь $r \geqslant 2$. Положим $\alpha = \alpha_1$. Имеем

$$X^p - a = \prod_{\nu=1}^{p} (X - \alpha_\nu),$$

$$X^{p^r} - a = \prod_{\nu=1}^{p} (X^{p^{r-1}} - \alpha_\nu).$$

Предположим, что α не является p-й степенью в $k(\alpha)$. Пусть A — корень $X^{p^{r-1}} - \alpha$. Если p нечетно, то по индукции A имеет степень p^{r-1} над $k(\alpha)$, следовательно, степень p^r над k, и все готово. Если же $p = 2$, то предположим, что $\alpha = -4\beta^4$, где $\beta \in k(\alpha)$. Пусть N — норма из $k(\alpha)$ в k. Тогда $-a = N(\alpha) = 16N(\beta)^4$, т. е. $-a = b^2$, где $b \in k$. Ниже будет показано, что в этом случае из наших предположений относительно a вытекает неприводимость многочлена $X^{2^r} - a = X^{2^r} + b^2$. Предположим, что $\alpha = \beta^p$ для некоторого $\beta \in k(\alpha)$, и выведем из этого следствия.

Взяв норму из $k(\alpha)$ в k, находим

$$-a = (-1)^p N(\alpha) = (-1)^p N(\beta^p) = (-1)^p N(\beta)^p.$$

Если p нечетно, то a будет p-й степенью в k — противоречие. Следовательно, $p = 2$ и $-a = N(\beta)^2$ — квадрат в k. Запишем $-a = b^2$, где $b \in k$. Так как a не является квадратом в k, то заключаем, что и -1 не является квадратом в k. Пусть $i^2 = -1$. Над $k(i)$ справедливо разложение

$$X^{2^r} - a = X^{2^r} + b^2 = (X^{2^{r-1}} + ib)(X^{2^{r-1}} - ib).$$

Каждый множитель имеет степень 2^{r-1}, и мы рассуждаем по индукции. Если $X^{2^{r-1}} \pm ib$ приводим над $k(i)$, то $\pm ib$ либо есть квадрат в $k(i)$, либо лежит в $-4(k(i))^4$. В любом случае $\pm ib$ будет квадратом в $k(i)$, скажем

$$\pm ib = (c + di)^2 = c^2 + 2c\,di - d^2,$$

где c, $d \in k$. Отсюда получаем $c^2 = d^2$, т. е. $c = \pm d$, и $\pm ib = 2cdi = \pm 2c^2 i$. Возведение в квадрат дает противоречие, а именно

$$a = -b^2 = -4c^4.$$

Из однозначности разложения на множители мы теперь заключаем, что $X^{2^r} + b^2$ не может разлагаться в $k[X]$ на множители, что и доказывает теорему.

Условия нашей теоремы необходимы, поскольку

$$X^4 + 4b^4 = (X^2 + 2bX + 2b^2)(X^2 - 2bX + 2b^2).$$

При $n = 4m$ и $a \in -4k^4$ многочлен $X^n - a$ приводим.

Следствие 1. *Пусть k — поле и для некоторого простого числа p элемент $a \in k$, $a \neq 0$, не является p-й степенью. Если p совпадает с характеристикой или же нечетно, то для всякого $r \geqslant 1$ многочлен $X^{p^r} - a$ неприводим.*

Доказательство. *Это утверждение логически слабее, чем* утверждение теоремы.

Следствие 2. *Пусть k — поле, причем алгебраическое замыкание $\bar{k}$ поля k имеет конечную степень > 1 над k. Тогда $\bar{k} = k(i)$, где $i^2 = -1$, и k имеет характеристику* 0.

Доказательство. Заметим, что $\bar{k}$ нормально над k. Если $\bar{k}$ несепарабельно над k, то $\bar{k}$ — чисто несепарабельно над некоторым подполем и имеет над ним степень > 1 (в силу гл. VII, § 7), следовательно, существуют подполе E, содержащее k, и элемент $a \in E$, такие, что $X^p - a$ неприводим над E. В силу следствия 1, $\bar{k}$ не может быть конечной степени над E. (Если читатель опустил § 7 гл. VII, то он может ограничиться рассмотрением случая характеристики 0.)

Итак, мы можем предполагать, что $\bar{k}$ является расширением Галуа над k. Пусть $k_1 = k(i)$. Тогда $\bar{k}$ будет расширением Галуа также и над k_1. Пусть G — группа Галуа $\bar{k}/k_1$. Предположим, что имеется простое число p, делящее порядок G. Пусть H — подгруппа порядка p и F — соответствующее неподвижное поле. Тогда $[\bar{k} : F] = p$. Если p равно характеристике, то упражнение 5 в конце главы дает противоречие. Поэтому мы можем предполагать, что p не равно характеристике. Тогда корни p-й степени из единицы, отличные от 1, являются корнями многочлена степени $\leqslant p - 1$ (а именно, $X^{p-1} + \ldots + 1$) и, следовательно, должны лежать в F. В силу теоремы 10 из § 6 отсюда вытекает, что $\bar{k}$ есть поле разложения некоторого многочлена $X^p - a$ с $a \in F$. Многочлен $X^{p^2} - a$ должен быть приводим. В силу

нашей теоремы имеем $p=2$ и $a=-4b^4$, где $b\in F$, откуда

$$\bar{k}=F(a^{1/2})=F(i).$$

Но мы предполагали, что $i\in k_1$ — противоречие.

Остается доказать, что k имеет характеристику 0. Предположим, что k имеет характеристику >0 (но никакой буквы для обозначения характеристики мы не используем, поскольку p уже занято). Поле, получаемое присоединением примитивного корня из единицы ζ_{2^r} к простому полю $\mathbf{F}$, является циклическим над этим простым полем. В силу теоремы 4 из § 1 группа Галуа поля $\bar{k}$ над k, являющаяся циклической порядка 2 и порождаемая, скажем, элементом σ, соответствует некоторой подгруппе группы Галуа расширения $\mathbf{F}(\zeta_{2^r})$ над $\mathbf{F}$. Однако расширение $\mathbf{F}(\zeta_{2^r})$, будучи циклическим над $\mathbf{F}$, обладает только одним подполем степени 2 над $\mathbf{F}$, и это подполе должно содержать i, поскольку i имеет степень 1 или 2 над $\mathbf{F}$. Так как $\sigma i\neq i$, то неподвижное подполе в $\mathbf{F}(\zeta_{2^r})$ относительно σ должно совпадать с $\mathbf{F}$. Это означает, что $\mathbf{F}(\zeta_{2^r})$ имеет степень 2 над $\mathbf{F}$, что дает противоречие, если взять r достаточно большим.

Следствие 2 принадлежит Артину.

§ 10. Когомологии Галуа

Пусть G — группа и A — абелева группа, которую мы в наших общих замечаниях, предшествующих теореме, будем записывать аддитивно. Предположим, что G действует на A посредством гомоморфизма $G\to \mathrm{Aut}(A)$. Под 1-*коциклом* группы G в A понимают семейство элементов $\{\alpha_\sigma\}_{\sigma\in G}$, где $\alpha_\sigma\in A$, удовлетворяющее соотношениям

$$\alpha_\sigma+\sigma\alpha_\tau=\alpha_{\sigma\tau}$$

для всех σ, $\tau\in G$. Если $\{\alpha_\sigma\}_{\sigma\in G}$ и $\{\beta_\sigma\}_{\sigma\in G}$ — 1-коциклы, то мы можем сложить их и получить 1-коцикл $\{\alpha_\sigma+\beta_\sigma\}_{\sigma\in G}$. Ясно, что 1-коциклы образуют группу; ее обозначают символом $Z^1(G, A)$. Семейство элементов $\{\alpha_\sigma\}_{\sigma\in G}$ называется 1-*кограницей* группы G в A, если существует элемент $\beta\in A$, для которого $\alpha_\sigma=\sigma\beta-\beta$ при всех $\sigma\in G$. Ясно, что всякая 1-кограница является 1-коциклом и что 1-кограницы образуют группу, обозначаемую $B^1(G, A)$. Факторгруппа $Z^1(G, A)/B^1(G, A)$ называется первой группой когомологий группы G в A и обозначается символом $H^1(G, A)$.

Теорема 17. *Пусть K/k — конечное расширение Галуа с группой Галуа G. Тогда $H^1(G, K^*)=1$ для действия G на K^* и $H^1(G, K)=0$ для действия G на аддитивной группе поля K.*

Другими словами, первая группа когомологий тривиальна в обоих случаях.

Доказательство. Пусть $\{\alpha_\sigma\}_{\sigma\in G}$ — 1-коцикл группы G в K^*. Соотношение, которому должен удовлетворять коцикл, в мультипликативной записи выглядит так:

$$\alpha_\sigma\alpha_\tau^\sigma = \alpha_{\sigma\tau}.$$

В силу линейной независимости характеров существует $\theta\in K$, для которого элемент

$$\beta = \sum_{\tau\in G}\alpha_\tau\tau(\theta)$$

отличен от нуля. Тогда

$$\sigma\beta = \sum_{\tau\in G}\alpha_\tau^\sigma\sigma\tau(\theta) = \sum_{\tau\in G}\alpha_{\sigma\tau}\alpha_\sigma^{-1}\sigma\tau(\theta) = \alpha_\sigma^{-1}\sum_{\tau\in G}\alpha_{\sigma\tau}\sigma\tau(\theta) = \alpha_\sigma^{-1}\beta.$$

Мы получаем, что $\alpha_\sigma = \beta/\sigma\beta$, и использование β^{-1} вместо β дает нам то, что нужно.

Что касается аддитивной части теоремы, то найдем элемент $\theta\in K$, для которого след $\mathrm{Tr}(\theta)$ не равен 0. Для заданного 1-коцикла $\{\alpha_\sigma\}$ в аддитивной группе поля K положим

$$\beta = \frac{1}{\mathrm{Tr}(\theta)}\sum_{\tau\in G}\alpha_\tau\tau(\theta).$$

Сразу же получаем $\alpha_\sigma = \beta - \sigma\beta$, что и требовалось.

§ 11. Алгебраическая независимость гомоморфизмов

Пусть A — аддитивная группа, K — поле и $\lambda_1, \ldots, \lambda_n$: $A\to K$ — аддитивные гомоморфизмы. Мы будем говорить, что $\lambda_1, \ldots, \lambda_n$ *алгебраически зависимы* (над K), если существует многочлен $f(X_1, \ldots, X_n)$ в $K[X_1, \ldots, X_n]$, такой, что

$$f(\lambda_1(x), \ldots, \lambda_n(x)) = 0$$

для всех $x\in A$, но при этом f не индуцирует нулевую функцию на $K^{(n)}$, т. е. на прямом произведении K с собой n раз. Мы знаем, что с каждым многочленом f можно сопоставить однозначно определенный редуцированный многочлен, дающий ту же самую функцию. Если K бесконечно, то редуцированный многочлен совпадает с f. В нашем определении зависимости мы могли бы предполагать f редуцированным.

Многочлен $f(X_1, \ldots, X_n)$ будет называться *аддитивным*, если он индуцирует аддитивный гомоморфизм $K^{(n)}$ в K. Пусть $(Y) = (Y_1, \ldots, Y_n)$ — переменные, независимые от (X). Положим

$$g(X, Y) = f(X + Y) - f(X) - f(Y),$$

где $X + Y$ обозначает результат покомпонентного сложения векторов. Тогда полная степень g, рассматриваемого как многочлен от (X) с коэффициентами в $K[Y]$, строго меньше, чем полная степень f, и аналогично его степень по каждому X_i не больше, чем степень f по этому X_i. Это сразу видно из рассмотрения разности одночленов

$$M_{(\nu)}(X + Y) - M_{(\nu)}(X) - M_{(\nu)}(Y) = \\ = (X_1 + Y_1)^{\nu_1} \ldots (X_n + Y_n)^{\nu_n} - X_1^{\nu_1} \ldots X_n^{\nu_n} - Y_1^{\nu_1} \ldots Y_n^{\nu_n}.$$

Аналогичное утверждение справедливо и для g, рассматриваемого как многочлен от (Y) с коэффициентами в $K[X]$. Отсюда вытекает, что если f редуцированный, то g также редуцированный. Следовательно, если f аддитивный, то g — нулевой многочлен.

Пример. Пусть K имеет характеристику p. Тогда в случае одной переменной отображение

$$\xi \mapsto a\xi^{p^m},$$

где $a \in K$ и $m \geqslant 1$, аддитивно и задается аддитивным многочленом aX^{p^m}. Ниже мы увидим, что это типичный пример.

Теорема 18 (Артин). *Пусть* $\lambda_1, \ldots, \lambda_n$: $A \to K$ — *аддитивные гомоморфизмы аддитивной группы в поле. Если эти гомоморфизмы алгебраически зависимы над* K, *то в* $K[X]$ *имеется аддитивный многочлен* $f(X_1, \ldots, X_n) \neq 0$, *такой, что*

$$f(\lambda_1(x), \ldots, \lambda_n(x)) = 0$$

для всех $x \in A$.

Доказательство. Пусть $f(X) = f(X_1, \ldots, X_n) \in K[X]$ — редуцированный многочлен наименьшей возможной степени, такой, что $f \neq 0$, но $f(\Lambda(x)) = 0$ для всех $x \in A$, где $\Lambda(x)$ — вектор $(\lambda_1(x), \ldots, \lambda_n(x))$. Докажем, что f аддитивен.

Пусть $g(X, Y) = f(X + Y) - f(X) - f(Y)$. Тогда

$$g(\Lambda(x), \Lambda(y)) = f(\Lambda(x + y)) - f(\Lambda(x)) - f(\Lambda(y)) = 0$$

для всех $x, y \in A$. Мы утверждаем, что g индуцирует нулевую функцию на $K^{(n)} \times K^{(n)}$. Предположим противное. Возможны два случая.

Случай 1. Имеем $g(\xi, \Lambda(y)) = 0$ для всех $\xi \in K^{(n)}$ и для всех $y \in A$. По предположению существует вектор $\xi' \in K^{(n)}$, для которого $g(\xi', Y)$ не равен тождественно 0. Положим $P(Y) = g(\xi', Y)$. Так

как степень g по (Y) строго меньше степени f, то получаем противоречие.

Случай 2. Существуют $\xi' \in K^{(n)}$ и $y' \in A$, такие, что $g(\xi', \Lambda(y')) \neq 0$. Положим $P(X) = g(X, \Lambda(y'))$. Тогда $P(X)$ — ненулевой многочлен, но $P(\Lambda(x)) = 0$ для всех $x \in A$ — снова противоречие.

Таким образом, g индуцирует нулевую функцию на $K^{(n)} \times K^{(n)}$, чем и доказано нужное нам утверждение, а именно, что f аддитивен.

Рассмотрим теперь аддитивные многочлены более подробно.

Пусть f — аддитивный многочлен от n переменных над K и притом редуцированный. Положим

$$f_i(X_i) = f(0, \ldots, X_i, \ldots, 0),$$

где X_i стоит на i-м месте, а остальные компоненты равны 0. В силу аддитивности

$$f(X_1, \ldots, X_n) = f_1(X_1) + \ldots + f_n(X_n),$$

поскольку разность между правой и левой частями есть редуцированный многочлен, принимающий на $K^{(n)}$ значение 0. Кроме того, f_i для каждого i — аддитивный многочлен от одной переменной. Сейчас мы изучим такие многочлены.

Пусть $f(X)$ — редуцированный многочлен от одной переменной, индуцирующий линейное отображение K в себя. Предположим, что в f встречается одночлен $a_r X^r$ с коэффициентом $a_r \neq 0$. Тогда одночлены степени r в

$$g(X, Y) = f(X + Y) - f(X) - f(Y)$$

задаются выражениями

$$a_r(X + Y)^r - a_r X^r - a_r Y^r.$$

Но, как мы уже видели, g тождественно равен 0. Следовательно, предыдущее выражение есть тождественный 0, так что многочлен

$$(X + Y)^r - X^r - Y^r$$

является нулевым. Но он содержит член $rX^{r-1}Y$. Следовательно, при $r > 1$ наше поле должно иметь характеристику p, а r должно делиться на p. Запишем $r = p^m s$, где s взаимно просто с p. Тогда

$$0 = (X + Y)^r - X^r - Y^r = \left(X^{p^m} + Y^{p^m}\right)^s - \left(X^{p^m}\right)^s - \left(Y^{p^m}\right)^s.$$

Рассуждая, как и выше, заключаем, что $s = 1$.

Итак, если f — аддитивный многочлен от одной переменной, то

$$f(X) = \sum_{\nu=0}^{m} a_\nu X^{p^\nu},$$

где $a_\nu \in K$. В случае характеристики 0 единственными аддитивными многочленами от одной переменной являются многочлены вида aX, где $a \in K$.

Как и следовало ожидать, мы называем $\lambda_1, \ldots, \lambda_n$ *алгебраически независимыми*, если любой редуцированный многочлен f, такой, что $f(\Lambda(x)) = 0$ для всех $x \in A$, является нулевым многочленом.

Применим теорему 18 к тому случаю, когда $\lambda_1, \ldots, \lambda_n$ — автоморфизмы поля, и скомбинируем ее с теоремой о линейной независимости характеров.

Теорема 19. *Пусть K — бесконечное поле и $\sigma_1, \ldots, \sigma_n$ — различные элементы конечной группы автоморфизмов K. Тогда $\sigma_1, \ldots, \sigma_n$ алгебраически независимы над K.*

Доказательство (Артин). В случае характеристики 0 теорема 18 и линейная независимость характеров показывают, что наше утверждение верно. Пусть характеристика $p > 0$, и пусть $\sigma_1, \ldots, \sigma_n$ алгебраически зависимы.

Существует аддитивный многочлен $f(X_1, \ldots, X_n)$ в $K[X_1, \ldots, X_n]$, такой, что $f \neq 0$, но

$$f(\sigma_1(x), \ldots, \sigma_n(x)) = 0$$

для всех $x \in K$. В силу предыдущего мы можем записать это соотношение в виде

$$\sum_{i=1}^{n} \sum_{r=1}^{m} a_{ir} \sigma_i(x)^{p^r} = 0$$

для всех $x \in K$, причем не все коэффициенты a_{ir} равны 0. Поэтому в силу теоремы о линейной независимости характеров эндоморфизмы

$$\{x \longmapsto \sigma_i(x)^{p^r}\} \quad \text{для} \quad i = 1, \ldots, n \quad \text{и} \quad r = 1, \ldots, m$$

не могут быть все различны. Следовательно, для всех $x \in K$ мы имеем

$$\sigma_i(x)^{p^r} = \sigma_j(x)^{p^s},$$

где либо $i \neq j$, либо $r \neq s$. Пусть, скажем, $r \leqslant s$. Извлечение корня p-й степени в характеристике p однозначно. Значит,

$$\sigma_i(x) = \sigma_j(x)^{p^{s-r}} = \sigma_j\left(x^{p^{s-r}}\right)$$

для всех $x \in K$. Положим $\sigma = \sigma_j^{-1}\sigma_i$. Тогда

$$\sigma(x) = x^{p^{s-r}}$$

для всех $x \in K$. Если $\sigma^n = \mathrm{id}$, то

$$x = x^{p^{n(s-r)}}$$

для всех $x \in K$. Поскольку K бесконечно, это возможно только при $s = r$. Но тогда $\sigma_i = \sigma_j$ вопреки тому факту, что мы начинали с различных автоморфизмов.

§ 12. Теорема о нормальном базисе

Теорема 20. *Пусть K/k — конечное расширение Галуа степени n и $\sigma_1, \ldots, \sigma_n$ — элементы его группы Галуа G. Тогда существует элемент $w \in K$, такой, что $\sigma_1 w, \ldots, \sigma_n w$ образуют базис K над k.*

Доказательство. Здесь мы докажем это только для случая, когда k бесконечно. В случае конечного поля k доказательство можно будет провести позднее методами линейной алгебры как упражнение.

Для всякого $\sigma \in G$ пусть X_σ — переменная и $t_{\sigma,\tau} = X_{\sigma^{-1}\tau}$. Положим $X_i = X_{\sigma_i}$. Пусть

$$f(X_1, \ldots, X_n) = \det(t_{\sigma_i, \sigma_j}).$$

Тогда f не является тождественным нулем, что видно, если подставить 1 вместо X_{id} и 0 вместо X_σ для $\sigma \neq \mathrm{id}$. Так как k бесконечно, то по теореме 19 определитель не может быть равным нулю при всех $x \in K$, если мы в f подставим $\sigma_i(x)$ вместо X_i. Следовательно, существует элемент $w \in K$, для которого

$$\det(\sigma_i^{-1}\sigma_j(w)) \neq 0.$$

Предположим, что элементы $a_1, \ldots, a_n \in k$ таковы, что

$$a_1\sigma_1(w) + \cdots + a_n\sigma_n(w) = 0.$$

Применим σ_i^{-1} к этому соотношению для каждого $i = 1, \ldots, n$. Поскольку $a_j \in k$, мы получим систему линейных уравнений относительно неизвестных a_j. Так как определитель из коэффициентов $\neq 0$, то

$$a_j = 0 \quad \text{для} \quad j = 1, \ldots, n$$

и, следовательно, w будет искомым элементом.

УПРАЖНЕНИЯ

1. Пусть k — поле, X — переменная над k и

$$\varphi(X) = \frac{f(X)}{g(X)}$$

— рациональная функция из $k(X)$, представленная в виде отношения двух взаимно простых многочленов f, g. Определим степень φ как $\max(\deg f,$

deg g) и положим $Y = \varphi(X)$. (а) Показать, что степень φ равна степени расширения $k(X)$ над $k(Y)$ (в предположении, что $Y \notin k$). (б) Показать, что всякий автоморфизм поля $k(X)$ над k может быть представлен рациональной функцией φ степени 1 и, обратно, что всякая такая функция φ определяет некоторый автоморфизм. (в) Показать, что эта группа автоморфизмов порождается следующими отображениями ($a,\ b \in k$):

$$X \longmapsto aX, \quad a \neq 0; \quad X \longmapsto X + b; \quad X \longmapsto \frac{1}{X}.$$

2. Пусть k — поле из q элементов и $K = k(X)$ — поле рациональных функций от одной переменной над k. Пусть G — группа автоморфизмов поля K, задаваемых отображениями

$$X \longmapsto \frac{aX + b}{cX + d},$$

где a, b, c, d лежат в k и $ad - bc \neq 0$. Доказать следующие утверждения:

(i) Порядок G равен $q^3 - q$.

(ii) Неподвижное поле группы G равно $k(Y)$, где

$$Y = \frac{(X^{q^2} - X)^{q+1}}{(X^q - X)^{q^2+1}}.$$

(iii) Пусть H_1 — подгруппа в G, состоящая из отображений $X \longmapsto aX + b$ с $a \neq 0$. Неподвижное поле группы H_1 совпадает с $k(T)$, где $T = (X^q - X)^{q-1}$.

(iv) Пусть H_2 — подгруппа в H_1, состоящая из отображений $X \longmapsto X + b$ с $b \in k$. Неподвижное поле группы H_2 равно $k(Z)$, где $Z = X^q - X$.

3. Пусть $\overline{\mathbf{Q}}$ — фиксированное алгебраическое замыкание поля $\mathbf{Q}$, E — максимальное подполе в $\overline{\mathbf{Q}}$, не содержащее $\sqrt{2}$ (такое подполе существует в силу леммы Цорна). Показать, что всякое конечное расширение поля E — циклическое. (Ваше доказательство должно остаться пригодным, если вместо $\sqrt{2}$ взять любое алгебраическое иррациональное число.)

4. Пусть k — поле, $\overline{k}$ — его алгебраическое замыкание, σ — автоморфизм $\overline{k}$, оставляющий k неподвижным, и F — неподвижное поле относительно σ. Показать, что всякое конечное расширение поля F — циклическое.

(Две предыдущие задачи — это примеры Артина, показывающие, как выкапывать ямы в алгебраически замкнутом поле.)

5. (i) Пусть K — циклическое расширение поля F с группой Галуа G, порожденной σ. Предположим, что характеристика равна p и что $[K:F] = p^{m-1}$, где m — некоторое целое число $\geqslant 2$. Пусть β — элемент поля K, для которого $\mathrm{Tr}_F^K(\beta) = 1$. Показать, что в K существует элемент α, такой, что

$$\sigma\alpha - \alpha = \beta^p - \beta.$$

(ii) Доказать, что многочлен $X^p - X - \alpha$ неприводим в $K[X]$.

(iii) Доказать, что если θ — корень этого многочлена, то $F(\theta)$ — расширение Галуа поля F, циклическое и имеющее степень p^m, и что его группа Галуа порождается продолжением σ^* автоморфизма σ, для которого

$$\sigma^*(\theta) = \theta + \beta.$$

6. Пусть E — алгебраическое расширение поля k, такое, что всякий многочлен $f(X)$ из $k[X]$ степени $\geqslant 1$ имеет хотя бы один корень в E. Доказать, что E алгебраически замкнуто. [*Указание*: рассмотреть отдельно

сепарабельный и чисто несепарабельный случай и воспользоваться теоремой о примитивном элементе.]

7. *Относительные инварианты* (Сато). Пусть k — поле, K — его расширение и G — группа автоморфизмов K над k, причем k совпадает с неподвижным полем группы G. (Мы не предполагаем, что K алгебраично над k.) Под *относительным инвариантом* группы G в K мы будем понимать элемент $P \in K$, $P \neq 0$, такой, что для всякого $\sigma \in G$ существует элемент $\chi(\sigma) \in k$, для которого $P^\sigma = \chi(\sigma) P$. Так как σ — автоморфизм, то $\chi(\sigma) \in k^*$. Мы будем говорить, что отображение χ: $G \to k^*$ *принадлежит* P, и будем называть его *характером*. Доказать следующие утверждения:

(а) Определенное выше отображение χ — гомоморфизм.

(б) Если один и тот же характер χ принадлежит относительным инвариантам P и Q, то существует такой элемент $c \in k^*$, что $P = cQ$.

(в) Относительные инварианты образуют мультипликативную группу, которую мы обозначаем через I.

Элементы $P_1, \ldots, P_m$ из I называются *мультипликативно независимыми* по модулю k^*, если их образы в факторгруппе I/k^* мультипликативно независимы, т. е. если из соотношения

$$P_1^{\nu_1} \ldots P_m^{\nu_m} = c \in k^*,$$

где $\nu_1, \ldots, \nu_m$ — целые числа, следует, что $\nu_1 = \ldots = \nu_m = 0$.

(г) Доказать, что если $P_1, \ldots, P_m$ мультипликативно независимы по модулю k^*, то они алгебраически независимы над k. [*Указание*: воспользоваться теоремой Артина о характерах.]

(д) Пусть $K = k(X_1, \ldots, X_n)$ — поле частных кольца многочленов $k[X_1, \ldots, X_n] = k[X]$, причем G индуцирует автоморфизмы этого кольца многочленов. Доказать: если $F_1(X)$ и $F_2(X)$ — относительно инвариантные многочлены, то их н. о. д. является относительным инвариантом; если $P(X) = F_1(X)/F_2(X)$ — относительный инвариант, являющийся отношением двух взаимно простых многочленов, то $F_1(X)$ и $F_2(X)$ — относительные инварианты. Доказать, что относительно инвариантные многочлены порождают I/k^*. Пусть S — множество относительно инвариантных многочленов, которые не могут быть разложены в произведение двух относительно инвариантных многочленов степени $\geqslant 1$. Показать, что элементы из S/k^* мультипликативно независимы и что, следовательно, I/k^* — свободная абелева группа. [Если вы знакомы с понятием степени трансцендентности, то, используя (г), вы сможете заключить, что эта группа — конечно порожденная.]

8. Пусть E — конечное сепарабельное расширение над k степени n, $W = (w_1, \ldots, w_n)$ — система элементов из E и $\sigma_1, \ldots, \sigma_n$ — различные вложения E в $\bar{k}$ над k. Определим дискриминант системы W, положив

$$D_{E/k}(W) = \det(\sigma_i w_j)^2.$$

Доказать: (а) Если $V = (v_1, \ldots, v_n)$ — какая-нибудь другая система (столбец) элементов из E и $X = (x_{ij})$ — матрица из элементов поля k, такая, что $W = XV$, то

$$D_{E/k}(W) = \det(X)^2 D_{E/k}(V).$$

(б) Дискриминант является элементом из k.

(в) Пусть $E = k(\alpha)$ и $f(X) = \operatorname{Irr}(\alpha, k, X)$. Пусть $\alpha_1, \ldots, \alpha_n$ — корни f и, скажем, $\alpha = \alpha_1$. Тогда

$$f'(\alpha) = \prod_{j=2}^{n} (\alpha - \alpha_j).$$

Показать, что

$$D_{E/k}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_k^E (f'(\alpha)).$$

(г) Пусть обозначения те же, что и в (а). Показать, что

$$\det(\mathrm{Tr}(w_i w_j)) = (\det(\sigma_i w_j))^2.$$

[*Указание*: пусть A — матрица $(\sigma_i w_j)$. Показать, что ${}^tAA$ есть матрица $(\mathrm{Tr}(w_i w_j))$.]

9. Пусть F — конечное поле и K — его конечное расширение. Показать, что норма N_F^K и след Tr_F^K сюръективны (как отображения K в F).

10. Пусть $a \neq 0, \neq \pm 1$ — целое число, свободное от квадратов. Для каждого простого числа p пусть K_p — поле разложения многочлена $X^p - a$ над $\mathbf{Q}$. Показать, что $[K_p : \mathbf{Q}] = p(p-1)$. Для всякого целого числа $m > 0$, свободного от квадратов, пусть

$$K_m = \prod_{p \mid m} K_p$$

— композит всех полей K_p с $p \mid m$, и пусть $d_m = [K_m : \mathbf{Q}]$ — степень K_m над $\mathbf{Q}$. Показать, что если m нечетно, то $d_m = \prod_{p \mid m} d_p$, а если m четно, $m = 2n$, то $d_{2n} = d_n$ или $2d_n$, в зависимости от того, содержится или нет $\sqrt{a}$ в поле корней m-й степени из единицы $\mathbf{Q}(\zeta_m)$.

11. Пусть A — абелева группа и G — конечная циклическая группа с образующей σ, действующая на A [посредством гомоморфизма $G \to \mathrm{Aut}(A)$]. Определим след $\mathrm{Tr}_G = \mathrm{Tr}$ на A, положив $\mathrm{Tr}(x) = \sum_{\tau \in G} \tau x$. Обозначим через A_{Tr} ядро следа и рассмотрим $(1-\sigma)A$ — подгруппу в A, состоящую из всех элементов вида $y - \sigma y$. Показать, что $H^1(G, A) \approx A_{\mathrm{Tr}}/(1-\sigma)A$.

12. Какова группа Галуа следующих многочленов: (а) $X^3 - X - 1$ над $\mathbf{Q}$. (б) $X^3 - 10$ над $\mathbf{Q}$. (в) $X^3 - 10$ над $\mathbf{Q}(\sqrt{2})$. (г) $X^3 - 10$ над $\mathbf{Q}(\sqrt{-3})$. (д) $X^3 - X - 1$ над $\mathbf{Q}(\sqrt{-23})$. (е) $X^4 - 5$ над $\mathbf{Q}$, $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{-5})$, $\mathbf{Q}(i)$. (ж) $X^4 - a$ над $\mathbf{Q}$, где a — любое целое число $\neq 0, \neq \pm 1$ и свободное от квадратов. (з) $X^n - a$ над $\mathbf{Q}$, где n нечетное > 1, a — любое свободное от квадратов целое положительное число. (и) $X^4 + 2$ над $\mathbf{Q}$, $\mathbf{Q}(i)$. (к) $(X^2-2)(X^3-3)(X^2-5)(X^2-7)$ над $\mathbf{Q}$. (л) $(X^2 - p_1) \ldots (X^2 - p_n)$ над $\mathbf{Q}$ ($p_1, \ldots, p_n$ — различные простые числа). (м) $(X^3-2)(X^3-3)(X^2-2)$ над $\mathbf{Q}(\sqrt{-3})$. (н) $X^n - t$ над $\mathbf{C}(t)$, где t трансцендентно над полем комплексных чисел $\mathbf{C}$, а n — целое положительное число. (о) $X^4 - t$ над $\mathbf{R}(t)$, где t такое же, как и выше.

13. Пусть k — поле, n — нечетное целое число $\geqslant 1$ и ζ — примитивный корень n-й степени из единицы, лежащий в k. Показать, что k содержит также примитивный корень $2n$-й степени из единицы.

14. Пусть k — конечное расширение поля рациональных чисел. Показать, что в k имеется только конечное число корней из единицы.

15. Определить, какие корни из единицы имеются в следующих полях: $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{-5})$.

16. Для каких целых чисел m примитивный корень m-й степени из единицы имеет степень 2 над $\mathbf{Q}$?

17. Пусть k — поле характеристики 0, причем для всякого конечного расширения E поля k индекс $(E^*: E^{*n})$ конечен, каково бы ни было целое положительное n. Доказать, что для всякого такого n существует только конечное число абелевых расширений над k степени n.

18. Пусть $f(z)$ — рациональная функция с коэффициентами в конечном расширении поля рациональных чисел, причем существует бесконечно много корней из единицы ζ, для которых $f(\zeta)$ есть корень из единицы. Показать, что существует такое целое число n, что $f(z) = cz^n$, где c — некоторая константа (являющаяся на самом деле корнем из единицы).

Это упражнение может быть обобщено следующим образом. Пусть Γ_0 — конечно порожденная мультипликативная группа комплексных чисел и Γ — группа всех комплексных чисел γ, таких, что γ^m лежит в Γ_0 для некоторого целого $m \neq 0$. Пусть $f(z)$ — рациональная функция с комплексными коэффициентами, такая, что существует бесконечно много $\gamma \in \Gamma$, для которых $f(\gamma)$ лежит в Γ. Тогда снова $f(z) = cz^n$ для некоторых c и n.

Мною дано доказательство соответствующего утверждения для случая, когда значения γ и f берутся в Γ_0, а не в Γ (см. „Diophantine Geometry", гл. VII, теорема 7).

19. Пусть K/k — расширение Галуа. На группе $G(K/k) = G$ определяем топологию Крулля, беря в качестве фундаментальной системы открытых окрестностей единицы множество подгрупп, которые принадлежат конечным расширениям E поля k, содержащимся в K. Используя представление на левых смежных классах, находим, что нормальные подгруппы кофинальны в этом семействе и что, следовательно, семейство нормальных подгрупп, принадлежащих конечным нормальным расширениям, определяет ту же самую топологию. Показать, что группа G алгебраически и топологически изоморфна проективному пределу конечных факторгрупп G/U, где U пробегает все такие нормальные подгруппы. Вывести отсюда, что G компактна и вполне несвязна. Такие группы называются *проконечными*. Показать, что всякая замкнутая подгруппа конечного индекса открыта. Показать, что замкнутые подгруппы — это в точности те подгруппы, которые принадлежат промежуточным подполям $k \subset F \subset K$. Показать, что если H — произвольная подгруппа в G и F — ее неподвижное поле, то подгруппа в G, принадлежащая F, совпадает с замыканием H в G.

20. Пусть k — такое поле, что всякое его конечное расширение — циклическое и что для всякого целого n оно имеет одно расширение степени n. Показать, что группа Галуа $G = G(\bar{k}/k)$ есть обратный предел $\varprojlim \mathbf{Z}/m\mathbf{Z}$, где $m\mathbf{Z}$ пробегает все подгруппы в $\mathbf{Z}$, упорядоченные по включению. Показать, что этот предел изоморфен прямому произведению пределов

$$\varinjlim_{n \to \infty} \mathbf{Z}/p^n\mathbf{Z},$$

взятому по всем простым числам p, другими словами, он изоморфен произведению всех аддитивных групп целых p-адических чисел.

21. *Векторы Витта.* Пусть $x_1, x_2, \ldots$ — последовательность алгебраически независимых элементов над кольцом целых чисел $\mathbf{Z}$. Для всякого $n \geqslant 1$ положим

$$x^{(n)} = \sum_{d \mid n} d x_d^{n/d}.$$

Показать, что x_n может быть выражено через $x^{(d)}$, где $d \mid n$, с рациональными коэффициентами.

Используя векторную терминологию, мы называем $(x_1, x_2, \ldots)$ компонентами Витта вектора x, а $(x^{(1)}, x^{(2)}, \ldots)$ — его *призрачными* компонентами. Сам x мы называем *вектором Витта*.

Рассмотрим степенной ряд

$$f_x(t) = \prod_{n \geqslant 1} (1 - x_n t^n).$$

Показать, что

$$-t \frac{d}{dt} \log f_x(t) = \sum_{n \geqslant 1} x^{(n)} t^n.$$

[Под $\frac{d}{dt} \log f(t)$ мы понимаем $f'(t)/f(t)$, где $f(t)$ — степенной ряд, производная которого $f'(t)$ берется формально.]

Если x, y — два вектора Витта, то их сумму и произведение определяем покомпонентно *относительно призрачных компонент*, т. е. полагаем

$$(x \dotplus y)^{(n)} = x^{(n)} \dotplus y^{(n)}.$$

Каковы $(x \dotplus y)_n$? Показать, что

$$f_x(t)\, f_y(t) = f_{x+y}(t).$$

Стало быть, $(x \dotplus y)_n$ — многочлен с целочисленными коэффициентами от $x_1, y_1, \ldots, x_n, y_n$. Показать также, что

$$f_{xy}(t) = \prod_{d,\, e \geqslant 1} \left(1 - x_d^{m/d} y_e^{m/e} t^m\right)^{de/m},$$

где m — наименьшее общее кратное d, e и d, e пробегают все целые числа $\geqslant 1$. Таким образом, $(xy)_n$ также есть многочлен от $x_1, y_1, \ldots, x_n, y_n$ с целочисленными коэффициентами.

Предыдущие соображения принадлежат Витту (устное сообщение) и отличаются от приведенных в его первоначальной работе.

Проверить, что формулы, выражающие компоненты $(x \dotplus y)_{p^n}$ и $(xy)_{p^n}$, зависят только от компонент x_{p^k} и y_{p^k}, где $k = 0, 1, \ldots, n$.

Если A — коммутативное кольцо, то, взяв гомоморфный образ кольца многочленов над $\mathbf{Z}$ в A, мы увидим, что можно определить сложение и умножение векторов Витта с компонентами в A и что эти векторы Витта образуют кольцо $W(A)$. Показать, что W есть функтор, т. е. что любой гомоморфизм φ кольца A в коммутативное кольцо A' индуцирует гомоморфизм $W(\varphi)$: $W(A) \to W(A')$.

22. Пусть p — простое число. Рассмотрим векторы Витта с компонентами, равными 0, за исключением тех, которые занумерованы степенями p. Применим log по основанию p к номерам этих компонент, — так что мы будем писать x_n вместо x_{p^n}. Например, x_0 теперь обозначает то, что раньше было x_1. Если k — поле характеристики p, то тем же символом $W(k)$ обозначается совокупность векторов Витта только что указанного вида. В силу упражнения 21 $W(k)$ является кольцом. Для вектора Витта $x = (x_0, x_1, \ldots, x_n, \ldots)$ положим

$$Vx = (0, x_0, x_1, \ldots) \quad \text{и} \quad Fx = (x_0^p, x_1^p, \ldots).$$

Таким образом, V есть оператор сдвига. Очевидно, $V \circ F = F \circ V$. Показать, что

$$(Vx)^{(n)} = px^{(n-1)} \quad \text{и} \quad x^{(n)} = (Fx)^{(n-1)} + p^n x_n.$$

Кроме того, по определению имеем

$$x^{(n)} = x_0^{p^n} + px_1^{p^{n-1}} + \ldots + p^n x_n.$$

23. Рассмотрим снова $W(k)$, где k — поле характеристики p. Тогда V — аддитивный эндоморфизм кольца $W(k)$ и F — кольцевой гомоморфизм $W(k)$ в себя. Кроме того, для всякого $x \in W(k)$ имеем

$$px = VFx.$$

Если $x,\ y \in W(k)$, то $(V^i x)(V^j y) = V^{i+j}\left(F^j x,\ F^i x\right)$. Обозначая для $a \in k$ через $\{a\}$ вектор Витта $(a, 0, 0, \ldots)$, мы можем символически записать

$$x = \sum_{i=0}^{\infty} V^i \{x_i\}.$$

Показать, что если $x \in W(k)$ и $x_0 \neq 0$, то x есть единица в $W(k)$. [*Указание*: имеем $1 - x\left\{x_0^{-1}\right\} = Vy$ и затем

$$x\left\{x_0^{-1}\right\} \sum_0^{\infty} (Vy)^i = (1 - Vy) \sum_0^{\infty} (Vy)^i = 1.\Big]$$

24. Пусть n — целое число $\geqslant 1$, p, как обычно, — простое число и k — поле характеристики p. Обозначим символом $W_n(k)$ кольцо усеченных векторов Витта $(x_0, \ldots, x_{n-1})$ с компонентами в k. Мы рассматриваем $W_n(k)$ как аддитивную группу. Для $x \in W_n(k)$ положим $\wp(x) = Fx - x$. Очевидно, $\wp$ — гомоморфизм. Если K — расширение Галуа поля k, $\sigma \in G(K/k)$ и $x \in W_n(K)$, то мы можем определить σx как вектор с компонентами $(\sigma x_0, \ldots, \sigma x_{n-1})$. Доказать аналог теоремы 90 Гильберта для векторов Витта и показать, что первая группа когомологий тривиальна. [Берем вектор, след которого является единицей в $W_n(k)$, и тем же путем, что и в доказательстве теоремы 17, § 10, устанавливаем, что цикл является кограницей.]

25. Показать, что если $x \in W_n(k)$, то существует вектор $\xi \in W_n(\bar{k})$, для которого $\wp(\xi) = x$. Сделать это по индукции сначала для первой компоненты, а затем показать, что вектор $(0, \alpha_1, \ldots, \alpha_{n-1})$ лежит в образе $\wp$ тогда и только тогда, когда $(\alpha_1, \ldots, \alpha_{n-1})$ лежит в образе $\wp$. Доказать по индукции, что если $\xi,\ \xi' \in W_n(k')$ для некоторого расширения k' поля k и если $\wp\xi = \wp\xi'$, то $\xi - \xi'$ — вектор, компоненты которого лежат в простом поле. Следовательно, решения уравнения $\wp\xi = x$ для заданного $x \in W_n(k)$ отличаются все между собой на векторы с компонентами из простого поля, а таких векторов имеется p^n штук. Полагаем

$$k(\xi) = k(\xi_0, \ldots, \xi_{n-1})$$

или символически

$$k(\wp^{-1}x).$$

Доказать, что это расширение Галуа поля k, и показать, что циклические расширения поля k, имеющие степень p^n, — это в точности расширения типа $k(\wp^{-1}x)$, где вектор x таков, что $x_0 \notin \wp k$.

26. Развить теорию Куммера для абелевых расширений показателя p^n поля k, используя $W_n(k)$. Другими словами, показать, что между подгруп-

пами B в $W_n(k)$, содержащими $\wp W_n(k)$, и абелевыми расширениями указанного выше типа имеется биективное соответствие

$$B \longmapsto K_B,$$

где $K_B = k(\wp^{-1}B)$. Все это принадлежит Витту (см. Witt E., Journal für die reine und angewandte Mathematik, 1935 и 1936 гг.). Доказательства, с небольшими изменениями, те же самые, что и данные в тексте для теории Куммера.

27. Дать пример поля K, имеющего степень 2 над двумя различными подполями E и F соответственно, но такого, что K не алгебраично над $E \cap F$.

28. Пусть $F = \mathbf{F}_p$ — простое поле характеристики p, K — поле, полученное из F присоединением всех примитивных корней l-й степени из единицы для всех простых чисел $l \neq p$. Показать, что K алгебраически замкнуто. [*Указание*: показать, что если q — простое число и r — целое число $\geqslant 1$, то существует простое число l, такое, что период $p \bmod l$ равен q^r. Для этого используется старый прием Ван дер Вардена. Пусть l — простое число, делящее целое число

$$b = \frac{p^{q^r}-1}{p^{q^{r-1}}-1} = (p^{q^{r-1}}-1)^{q-1} + q\,(p^{q^{r-1}}-1)^{q-2} + \ldots + q.$$

Если l не делит $p^{q^{r-1}}-1$, то все готово. В противном случае $l = q$. Но при этом q^2 не делит b и, следовательно, существует простое число $l \neq q$, делящее b. Тогда степень $F(\zeta_l)$ над F есть q^r, так что K содержит подполя произвольной степени над F.]

Глава IX

Расширения колец

В этой главе слово „кольцо" будет обозначать „коммутативное кольцо".

§ 1. Целые расширения колец

В гл. VII и VIII мы изучали алгебраические расширения полей. По целому ряду причин желательно исследовать также алгебраические расширения колец. Например, данный многочлен с целыми коэффициентами, скажем $X^5 - X - 1$, можно привести по модулю любого простого числа p и получить таким образом многочлен с коэффициентами в конечном поле. В качестве другого примера рассмотрим многочлен

$$X^n + s_{n-1}X^{n-1} + \ldots + s_0,$$

где $s_{n-1}, \ldots, s_0$ алгебраически независимы над полем k. Этот многочлен имеет коэффициенты в $k[s_0, \ldots, s_{n-1}]$, а после подстановки вместо $s_0, \ldots, s_{n-1}$ элементов из k получается многочлен с коэффициентами в k. В общем можно получать информацию о многочленах, беря гомоморфизм кольца, в котором лежат их коэффициенты. Эта глава посвящена краткому описанию основных фактов, касающихся многочленов над кольцами.

Пусть A — кольцо и M — A-модуль. Мы будем говорить, что модуль M *точный*, если равенство $aM = 0$, $a \in A$, возможно только при $a = 0$. Отметим, что A является точным модулем над собой, поскольку A содержит единичный элемент. Кроме того, если $A \neq 0$, то точный модуль над A не может быть модулем, состоящим только из нуля.

Пусть A — подкольцо кольца B и $\alpha \in B$. Следующие условия эквивалентны:

ЦЕЛ 1. Элемент α есть корень многочлена

$$X^n + a_{n-1}X^{n-1} + \ldots + a_0$$

степени $n \geqslant 1$ с коэффициентами $a_i \in A$. (Существенным моментом здесь является то, что старший коэффициент равен 1.)

ЦЕЛ 2. Подкольцо $A[\alpha]$ — конечно порожденный A-модуль.

ЦЕЛ 3. Существует точный модуль над $A[\alpha]$, являющийся конечно порожденным A-модулем.

Докажем их эквивалентность. Предположим, что выполняется ЦЕЛ 1. Пусть $g(X)$ — многочлен из $A[X]$ степени $\geqslant 1$ со старшим коэффициентом 1, для которого $g(\alpha)=0$. Если $f(X)\in A[X]$, то

$$f(X)=q(X)g(X)+r(X),$$

где $q,\ r\in A[X]$ и $\deg r<\deg g$. Следовательно, $f(\alpha)=r(\alpha)$ и мы видим, что если $\deg g=n$, то $1,\ \alpha,\ \ldots,\ \alpha^{n-1}$ являются образующими $A[\alpha]$ как модуля над A.

Уравнение $g(X)=0$, где g — многочлен описанного выше вида, для которого $g(\alpha)=0$, называется *целым уравнением* для α над A.

Предположим, что выполняется ЦЕЛ 2. Тогда в качестве точного модуля мы можем взять само кольцо $A[\alpha]$.

Предположим, что выполняется ЦЕЛ 3, и пусть M — точный модуль над $A[\alpha]$, конечно порожденный над A, скажем, элементами $w_1,\ \ldots,\ w_n$. Так как $\alpha M\subset M$, то существуют элементы $a_{ij}\in A$, такие, что

$$\begin{aligned}\alpha w_1&=a_{11}w_1+\ \ldots\ +a_{1n}w_n,\\ &\ldots\ldots\ldots\ldots\ldots\\ \alpha w_n&=a_{n1}w_1+\ \ldots\ +a_{nn}w_n.\end{aligned}$$

Перенося $\alpha w_1,\ \ldots,\ \alpha w_n$ в правые части этих уравнений, мы приходим к заключению, что определитель

$$d=\begin{vmatrix}\alpha-a_{11} & & & \\ & \alpha-a_{22} & -a_{ij} & \\ & & \ddots & \\ -a_{ij} & & & \alpha-a_{nn}\end{vmatrix}$$

аннулирует M: $dM=0$. (Это будет доказано в главе, в которой мы рассматриваем определители.) Так как модуль M точный, то должно выполняться равенство $d=0$. Следовательно, α есть корень многочлена

$$\det|X\delta_{ij}-a_{ij}|,$$

дающего целое уравнение для α над A.

Элемент α, удовлетворяющий трем предыдущим условиям ЦЕЛ 1, 2, 3, называется *целым* над A.

Предложение 1. *Пусть A — целое кольцо, K — его поле частных и α — алгебраический элемент над K. Тогда в A существует элемент $c\neq 0$, такой, что $c\alpha$ — целый элемент над A.*

Доказательство. Имеем уравнение

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0,$$

где $a_i \in A$ и $a_n \neq 0$. Умножим его на a_n^{n-1}. Тогда

$$(a_n\alpha)^n + \ldots + a_0 a_n^{n-1} = 0$$

будет целым уравнением для $a_n\alpha$ над A.

Пусть A, B — подкольца кольца C, и пусть $\alpha \in C$. Если α — целый элемент над A и $A \subset B$, то тем более α — целый элемент над B. Таким образом, целость элемента сохраняется при подъеме.

Пусть B — кольцо, содержащее A в качестве подкольца. Мы будем говорить, что B — *целое* над A, если всякий элемент из B является целым над A.

Предложение 2. *Если B — целое кольцо над A, конечно порожденное как A-алгебра, то B конечно порождено и как A-модуль.*

Доказательство. Это предложение можно доказывать индукцией по числу кольцевых образующих и, таким образом, учитывая наличие башни

$$A \subset A[\alpha_1] \subset A[\alpha_1, \alpha_2] \subset \ldots \subset A[\alpha_1, \ldots, \alpha_n] = B,$$

предполагать, что $B = A[\alpha]$ для некоторого элемента α, целого над A. Но, как мы уже видели, в этом случае наше утверждение верно (это составляет часть определения целости).

Так же как для расширений полей, мы можем говорить, что класс $\mathscr{C}$ расширений колец $A \subset B$ является *отмеченным*, если он удовлетворяет аналогичным свойствам, а именно:

(i) Пусть $A \subset B \subset C$ — башня колец. Расширение $A \subset C$ тогда и только тогда принадлежит $\mathscr{C}$, когда $A \subset B$ принадлежит $\mathscr{C}$ и $B \subset C$ принадлежит $\mathscr{C}$.

(ii) Если $A \subset B$ принадлежит $\mathscr{C}$ и C — любое расширение кольца A, причем B, C оба являются подкольцами некоторого кольца, то $C \subset B[C]$ принадлежит $\mathscr{C}$. (Отметим, что $B[C] = C[B]$ есть наименьшее кольцо, содержащее и B, и C.)

Как и для полей, мы в качестве формального следствия из (i) и (ii) получаем, что выполняется также и свойство

(iii) Если $A \subset B$ и $A \subset C$ принадлежат $\mathscr{C}$, причем B, C — подкольца некоторого кольца, то $A \subset B[C]$ принадлежит $\mathscr{C}$.

Предложение 3. *Целые расширения колец образуют отмеченный класс.*

Доказательство. Пусть $A \subset B \subset C$ — башня колец. Если C — целое над A, то ясно, что B — целое над A и C — целое над B.

Обратно, предположим, что каждый этаж в башне целый. Пусть $\alpha \in C$. Тогда α удовлетворяет целому уравнению

$$\alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_0 = 0,$$

где $b_i \in B$. Положим $B_1 = A[b_0, \ldots, b_{n-1}]$. Тогда B_1, согласно предложению 2, будет конечно порожденным A-модулем и $B_1[\alpha]$ — конечно порожденным B_1-модулем. Так как $A[\alpha] \subset B_1[\alpha]$, то $B_1[\alpha]$ — точный $A[\alpha]$-модуль. Наконец, $B_1[\alpha]$ есть конечно порожденный A-модуль. Действительно, если $v_1, \ldots, v_r$ — образующие B_1 над A и $w_1, \ldots, w_s$ — образующие $B_1[\alpha]$ над B_1, то $v_i w_j$, $i = 1, \ldots, r$, $j = 1, \ldots, s$, порождают $B_1[\alpha]$ над A. Следовательно, кольцо C — целое над A. Наконец, пусть B, C — кольца, являющиеся расширениями A, причем B — целое над A. Предположим, что B, C — подкольца некоторого кольца. Тогда $C[B]$ порождается над C элементами из B, а каждый элемент из B является целым над C. То, что $C[B]$ является целым над C, непосредственно вытекает теперь из следующего предложения.

Предложение 4. *Пусть A — подкольцо кольца C. Тогда элементы из C, целые над A, образуют подкольцо в C.*

Доказательство. Если α — целый элемент над A, то $A[\alpha]$ — целое расширение A, поскольку для любого $\alpha' \in A[\alpha]$ конечно порожденный A-модуль $A[\alpha]$ является точным $A[\alpha']$-модулем. Пусть теперь α, $\beta \in C$ — целые элементы над A. Рассмотрим башню $A \subset A[\alpha] \subset A[\alpha, \beta]$. Каждый этаж в этой башне является целым, а потому, согласно первой части доказательства предложения 3, $A[\alpha, \beta]$ — целое расширение A. Следовательно, $\alpha \pm \beta$ и $\alpha\beta$ — целые элементы над A, что и доказывает наше предложение.

В условиях предложения 4 множество элементов из C, целых над A, называется *целым замыканием* кольца A в C.

Предложение 5. *Пусть B — целое кольцо над A и σ — его гомоморфизм. Тогда кольцо $\sigma(B)$ — целое над $\sigma(A)$.*

Доказательство. Пусть $\alpha \in B$ и

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

— целое уравнение для α над A. Применение σ дает

$$\sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha)^{n-1} + \cdots + \sigma(a_0) = 0,$$

что и доказывает наше утверждение.

Следствие. *Пусть A — целостное кольцо, k — его поле частных, E — конечное расширение над k и $\alpha \in E$ — целый элемент над A. Тогда норма и след элемента α (из E в k) являются*

целыми над A и таковы же коэффициенты неприводимого многочлена над k, соответствующего α.

Доказательство. Для всякого вложения σ поля E над k элемент $\sigma\alpha$ является целым над A. Так как норма — это произведение элементов $\sigma\alpha$ по всем таким σ (возведенное в степень, равную некоторой степени характеристики), то норма — целый элемент над A. Аналогичное верно для следа и для коэффициентов многочлена $\mathrm{Irr}(\alpha, k, X)$, которые являются элементарными симметрическими функциями от его корней.

Пусть A — целостное кольцо и k — его поле частных. Мы будем говорить, что A *целозамкнуто*, если оно совпадает со своим целым замыканием в k.

Предложение 6. *Всякое факториальное кольцо A целозамкнуто.*

Доказательство. Предположим, что имеется дробь a/b с $a, b \in A$, целая над A, и простой элемент p в A, делящий b, но не делящий a. Тогда для некоторого целого числа $n \geqslant 1$ и $a_i \in A$

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_0 = 0,$$

откуда

$$a^n + a_{n-1}ba^{n-1} + \cdots + a_0 b^n = 0.$$

Так как элемент p делит b, то он должен делить a^n, а следовательно, и a — противоречие.

Пусть $f\colon A \to B$ — гомоморфизм колец (A, B — коммутативные кольца). Напомним, что такой гомоморфизм называется также A-алгеброй. Мы можем рассматривать B как A-модуль. Будем говорить, что B — целое над A (относительно этого кольцевого гомоморфизма f), если B — целое над $f(A)$. Это расширение нашего определения целости полезно, так как в некоторых приложениях имеют место отклонения от обычной ситуации, а мы тем не менее хотим говорить о целости. Более точно, нам следовало бы говорить, что не B является целым над A, а что f есть *целый гомоморфизм колец* или, просто, f — *целый*. Мы будем часто использовать эту терминологию.

Некоторые из наших предыдущих предложений непосредственно дают следствия для целых гомоморфизмов колец; например, если $f\colon A \to B$ и $g\colon B \to C$ целые, то $g \circ f\colon A \to C$ целый. Однако, вообще говоря, не верно, что если $g \circ f$ целый, то целый и f.

Пусть $f\colon A \to B$ — целый гомоморфизм и S — мультипликативное подмножество в A. Тогда имеет место гомоморфизм

$$S^{-1}f\colon S^{-1}A \to S^{-1}B,$$

где, строго говоря, $S^{-1}B = (f(S))^{-1}B$ и $S^{-1}f$ определяется по формуле

$$(S^{-1}f)(x/s) = f(x)/f(s).$$

Проверка того, что это гомоморфизм, тривиальна. Имеет место коммутативная диаграмма

$$\begin{array}{ccc} B & \to & S^{-1}B \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle S^{-1}f} \\ A & \to & S^{-1}A \end{array}$$

горизонтальными отображениями в которой служат канонические отображения $x \longmapsto x/1$.

Предложение 7. *Пусть $f\colon A \to B$ — целый гомоморфизм и S — мультипликативное подмножество в A. Тогда гомоморфизм $S^{-1}f\colon S^{-1}A \to S^{-1}B$ — целый.*

Доказательство. Для $\alpha \in B$, $a \in A$ и $s \in S$ будем писать $a\alpha$ и α/s вместо $f(a)\alpha$ и $\alpha/f(s)$ соответственно. Так как всякий элемент $\alpha \in B$ — целый над $f(A)$, то имеем

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0,$$

где $a_i \in A$. Беря канонический образ в $S^{-1}B$ и деля почленно на s^n, получаем

$$(\alpha/s)^n + (a_{n-1}/s)(\alpha/s)^{n-1} + \cdots + a_0/s^n = 0;$$

это доказывает, что элемент α/s является целым над $(S^{-1}f)(S^{-1}A)$.

Предложение 8. *Пусть A — целостное и целозамкнутое кольцо, S — мультипликативное подмножество в A, $0 \notin S$. Тогда $S^{-1}A$ целозамкнуто.*

Доказательство. Пусть α — элемент поля частных, целый над $S^{-1}A$. Имеем уравнение

$$\alpha^n + \frac{a_{n-1}}{s_{n-1}}\alpha^{n-1} + \cdots + \frac{a_0}{s_0} = 0,$$

$a_i \in A$ и $s_i \in S$. Пусть s равно произведению $s_{n-1} \ldots s_0$. Тогда ясно, что элемент $s\alpha$ — целый над A и, следовательно, лежит в A. Значит, α лежит в $S^{-1}A$ и кольцо $S^{-1}A$ целозамкнуто.

Лемма Накаямы. *Пусть A — кольцо, $\mathfrak{a}$ — идеал, содержащийся во всех максимальных идеалах кольца A, и M — конечно порожденный A-модуль. Если $\mathfrak{a}M = M$, то $M = 0$.*

Доказательство. Индукция по числу образующих M. Пусть, скажем, M порождается элементами $w_1, \ldots, w_n$. Существует представление

$$w_1 = a_1 w_1 + \cdots + a_n w_n,$$

где $a_i \in \mathfrak{a}$. Следовательно,

$$(1 - a_1) w_1 = a_2 w_2 + \cdots + a_n w_n.$$

Если элемент $1 - a_1$ не является единицей в A, то он содержится в некотором максимальном идеале $\mathfrak{p}$. Так как $a_1 \in \mathfrak{p}$ по предположению, то мы получаем противоречие: $1 \in \mathfrak{p}$. Следовательно, $1 - a_1$ — единица, и предыдущее равенство, разделенное на этот элемент, показывает, что модуль M может быть порожден $n - 1$ элементами, чем и завершается доказательство.

Пусть $\mathfrak{p}$ — простой идеал кольца A и S — дополнение к $\mathfrak{p}$ в A. Мы пишем в этом случае $S = A - \mathfrak{p}$. Если $f\colon A \to B$ есть A-алгебра (т. е. гомоморфизм колец), то будем писать $B_\mathfrak{p}$ вместо $S^{-1}B$. Мы можем рассматривать $B_\mathfrak{p}$ как $A_\mathfrak{p} = S^{-1}A$-модуль.

Пусть A — подкольцо в B, $\mathfrak{p}$ — простой идеал в A и $\mathfrak{P}$ — простой идеал в B. Мы будем говорить, что $\mathfrak{P}$ *лежит над* $\mathfrak{p}$, если $\mathfrak{P} \cap A = \mathfrak{p}$. В этом случае вложение $A \to B$ индуцирует вложение факторколец

$$A/\mathfrak{p} \to B/\mathfrak{P},$$

и по существу мы имеем коммутативную диаграмму

$$\begin{array}{ccc} B & \to & B/\mathfrak{P} \\ \uparrow & & \uparrow \\ A & \to & A/\mathfrak{p} \end{array}$$

в которой горизонтальные стрелки обозначают канонические гомоморфизмы, а вертикальные — вложения.

Если кольцо B — целое над A, то $B/\mathfrak{P}$ — целое над $A/\mathfrak{p}$, согласно предложению 5.

Предложение 9. *Пусть A — подкольцо в B и $\mathfrak{p}$ — простой идеал в A, причем кольцо B — целое над A. Тогда $\mathfrak{p}B \neq B$ и существует простой идеал $\mathfrak{P}$ в B, лежащий над $\mathfrak{p}$.*

Доказательство. Мы знаем, что $B_\mathfrak{p}$ — целое над $A_\mathfrak{p}$ и что $A_\mathfrak{p}$ — локальное кольцо с максимальным идеалом $\mathfrak{m}_\mathfrak{p} = S^{-1}\mathfrak{p}$, где $S = A - \mathfrak{p}$. Так как, очевидно,

$$\mathfrak{p}B_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}B_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}B_\mathfrak{p},$$

наше первое утверждение достаточно доказать для случая, когда A — локальное кольцо. (Отметим, что существование простого идеала $\mathfrak{p}$

влечет, что $1 \neq 0$ и $\mathfrak{p}B = B$ тогда и только тогда, когда $1 \in \mathfrak{p}B$.) Если $\mathfrak{p}B = B$, то 1 представляется в виде линейной комбинации элементов из B с коэффициентами в $\mathfrak{p}$

$$1 = a_1 b_1 + \cdots + a_n b_n,$$

где $a_i \in \mathfrak{p}$ и $b_i \in B$. Пусть $B_0 = A[b_1, \ldots, b_n]$. Тогда $\mathfrak{p}B_0 = B_0$ и B_0 — конечный A-модуль в силу предложения 2. Следовательно, $B_0 = 0$ в силу леммы Накаямы, — противоречие.

Чтобы доказать наше второе утверждение, рассмотрим следующую коммутативную диаграмму:

$$\begin{array}{ccc} B & \longrightarrow & B_{\mathfrak{p}} \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_{\mathfrak{p}} \end{array}$$

Мы только что доказали, что $\mathfrak{m}_{\mathfrak{p}} B_{\mathfrak{p}} \neq B_{\mathfrak{p}}$. Следовательно, $\mathfrak{m}_{\mathfrak{p}} B_{\mathfrak{p}}$ содержится в некотором максимальном идеале $\mathfrak{M}$ кольца $B_{\mathfrak{p}}$. Переходя к прообразам, мы видим, что прообраз $\mathfrak{M}$ в $A_{\mathfrak{p}}$ есть идеал, содержащий $\mathfrak{m}_{\mathfrak{p}}$. Так как идеал $\mathfrak{m}_{\mathfrak{p}}$ максимальный, то $\mathfrak{M} \cap A_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}$. Пусть $\mathfrak{P}$ — прообраз $\mathfrak{M}$ в B. Тогда $\mathfrak{P}$ — простой идеал в B. Прообраз $\mathfrak{m}_{\mathfrak{p}}$ в A есть просто $\mathfrak{p}$. Беря полный прообраз $\mathfrak{M}$ по обоим путям в диаграмме, находим

$$\mathfrak{P} \cap A = \mathfrak{p},$$

что и требовалось показать.

Предложение 10. *Пусть A — подкольцо в B, причем кольцо B — целое над A. Простой идеал $\mathfrak{P}$ в B, лежащий над простым идеалом $\mathfrak{p}$ кольца A, максимален в том и только в том случае, если $\mathfrak{p}$ максимален.*

Доказательство. Предположим, что $\mathfrak{p}$ максимален в A. Тогда $A/\mathfrak{p}$ — поле и $B/\mathfrak{P}$ — целостное кольцо, целое над $A/\mathfrak{p}$. Если $\alpha \in B/\mathfrak{P}$, то элемент α алгебраичен над $A/\mathfrak{p}$, а мы знаем, что тогда $A/\mathfrak{p}[\alpha]$ — поле. Следовательно, всякий ненулевой элемент из $B/\mathfrak{P}$ обратим в кольце $B/\mathfrak{P}$, которое поэтому является полем. Обратно, предположим, что $\mathfrak{P}$ — максимальный идеал в B. Тогда $B/\mathfrak{P}$ — поле, целое над целостным кольцом $A/\mathfrak{p}$. Если $A/\mathfrak{p}$ — не поле, то оно содержит ненулевой максимальный идеал $\mathfrak{m}$. В силу предложения 9 в $B/\mathfrak{P}$ существует простой идеал $\mathfrak{M}$, лежащий над $\mathfrak{m}$, $\mathfrak{M} \neq 0$, — противоречие.

§ 2. Целые расширения Галуа

Мы исследуем здесь взаимоотношение между теорией Галуа многочлена и теорией Галуа того же самого многочлена, приведенного по модулю простого идеала.

Предложение 11. *Пусть A — целостное кольцо, целозамкнутое в своем поле частных K; L — конечное нормальное расши-*

рение поля K с группой Галуа G; $\mathfrak{p}$ — максимальный идеал в A и $\mathfrak{P}$, $\mathfrak{Q}$ — простые идеалы целого замыкания B кольца A в L, лежащие над $\mathfrak{p}$. Тогда существует элемент $\sigma \in G$, такой, что $\sigma\mathfrak{P} = \mathfrak{Q}$.

Доказательство. Предположим, что $\mathfrak{Q} \neq \sigma\mathfrak{P}$ ни для одного $\sigma \in G$. Тогда $\tau\mathfrak{Q} \neq \sigma\mathfrak{P}$ ни для какой пары элементов σ, $\tau \in G$. Существует элемент $x \in B$, такой, что

$$x \equiv 0 \pmod{\sigma\mathfrak{P}} \quad \text{для всех} \quad \sigma \in G,$$
$$x \equiv 1 \pmod{\sigma\mathfrak{Q}} \quad \text{для всех} \quad \sigma \in G$$

(использовать китайскую теорему об остатках). Норма

$$N_K^L(x) = \left(\prod_{\sigma \in G} \sigma x\right)^{[L:K]_i}$$

лежит в $B \cap K = A$ (так как A целозамкнуто) и, значит, в $\mathfrak{P} \cap A = \mathfrak{p}$. Но $x \notin \sigma\mathfrak{Q}$ ни при каком $\sigma \in G$, так что $\sigma x \notin \mathfrak{Q}$ ни при каком $\sigma \in G$. Это противоречит тому факту, что норма элемента x лежит в $\mathfrak{p} = \mathfrak{Q} \cap A$.

Локализацией можно снять предположение о максимальности $\mathfrak{p}$; достаточно предполагать, что $\mathfrak{p}$ простой.

Следствие. *Пусть A — кольцо, целозамкнутое в своем поле частных K; E — конечное алгебраическое расширение поля K; B — целое замыкание A в E и $\mathfrak{p}$ — максимальный идеал в A. Тогда существует лишь конечное число простых идеалов в B, лежащих над $\mathfrak{p}$* [1]).

Доказательство. Пусть L — наименьшее нормальное расширение поля K, содержащее E. Если $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ — два различных простых идеала в B, лежащих над $\mathfrak{p}$, и $\mathfrak{P}_1$, $\mathfrak{P}_2$ — два простых идеала из целого замыкания A в L, лежащих над $\mathfrak{Q}_1$ и $\mathfrak{Q}_2$ соответственно, то $\mathfrak{P}_1 \neq \mathfrak{P}_2$. Это соображение сводит наше утверждение к случаю, когда E — нормальное расширение над K, а тогда оно становится непосредственным следствием предложения 11.

Пусть кольцо A целозамкнуто в своем поле частных K и B — его целое замыкание в конечном расширении Галуа L с группой G. Тогда $\sigma B = B$ для всякого $\sigma \in G$. Пусть $\mathfrak{p}$ — некоторый максимальный идеал в A и $\mathfrak{P}$ — максимальный идеал в B, лежащий над $\mathfrak{p}$. Обозначим через $G_{\mathfrak{P}}$ подгруппу в G, состоящую из всех автоморфизмов σ, для которых $\sigma\mathfrak{P} = \mathfrak{P}$. Тогда группа $G_{\mathfrak{P}}$ естественным образом действует на поле классов вычетов $B/\mathfrak{P}$ и оставляет неподвижным поле $A/\mathfrak{p}$. Каждому $\sigma \in G_{\mathfrak{P}}$ мы можем сопоставить автоморфизм σ' поля $B/\mathfrak{P}$ над $A/\mathfrak{p}$, и отображение, задаваемое правилом

$$\sigma \mapsto \sigma',$$

[1]) Именно в таком виде следствие используется в § 4 гл. XII. В формулировке автора на E налагается условие сепарабельности. — *Прим. ред.*

индуцирует гомоморфизм $G_{\mathfrak{P}}$ в группу автоморфизмов поля $B/\mathfrak{P}$ над $A/\mathfrak{p}$.

Группа $G_{\mathfrak{P}}$ будет называться *группой разложения* идеала $\mathfrak{P}$. Ее неподвижное поле будет обозначаться через L^d и будет называться *полем разложения* идеала $\mathfrak{P}$. Пусть B^d — целое замыкание A в L^d и $\mathfrak{Q} = \mathfrak{P} \cap B^d$. В силу предложения 11 $\mathfrak{P}$ — единственный простой идеал в B, лежащий над $\mathfrak{Q}$.

Пусть $G = \bigcup \sigma_j G_{\mathfrak{P}}$ — разложение на смежные классы группы G по $G_{\mathfrak{P}}$. Тогда простые идеалы $\sigma_j\mathfrak{P}$ — это в точности все различные простые идеалы в B, лежащие над $\mathfrak{p}$. Действительно, для двух элементов σ, $\tau \in G$ тогда и только тогда $\sigma\mathfrak{P} = \tau\mathfrak{P}$, когда $\tau^{-1}\sigma\mathfrak{P} = \mathfrak{P}$, т. е. $\tau^{-1}\sigma$ лежит в $G_{\mathfrak{P}}$. Таким образом, τ, σ лежат в одном и том же смежном классе $\bmod G_{\mathfrak{P}}$.

Непосредственно ясно, что группой разложения простого идеала $\sigma\mathfrak{P}$ будет $\sigma G_{\mathfrak{P}}\sigma^{-1}$.

Предложение 12. *Поле L^d — это наименьшее подполе E в L, содержащее K и такое, что $\mathfrak{P}$ — единственный простой идеал в B, лежащий над идеалом $\mathfrak{P} \cap E$ (который является простым в $B \cap E$).*

Доказательство. Пусть E обладает указанными свойствами, и пусть H — группа Галуа расширения L над E. Положим $\mathfrak{q} = \mathfrak{P} \cap E$. В силу предложения 11 все простые идеалы в B, лежащие над $\mathfrak{q}$, сопряжены посредством элементов из H. Так как имеется только один такой простой идеал, а именно $\mathfrak{P}$, то это означает, что H оставляет $\mathfrak{P}$ инвариантным. Следовательно, $H \subset G_{\mathfrak{P}}$ и $E \supset L^d$. Но, как мы уже отмечали, само L^d обладает требуемыми свойствами.

Предложение 13. *В тех же обозначениях имеем $A/\mathfrak{p} = B^d/\mathfrak{Q}$ (относительно канонического вложения $A/\mathfrak{p} \to B^d/\mathfrak{Q}$).*

Доказательство. Если σ — элемент из G, не лежащий в $G_{\mathfrak{P}}$, то $\sigma\mathfrak{P} \neq \mathfrak{P}$ и $\sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$. Положим

$$\mathfrak{Q}_\sigma = \sigma^{-1}\mathfrak{P} \cap B^d.$$

Тогда $\mathfrak{Q}_\sigma \neq \mathfrak{Q}$. Пусть x — произвольный элемент из B^d. В B^d существует элемент y, такой, что

$$y \equiv x \pmod{\mathfrak{Q}},$$
$$y \equiv 1 \pmod{\mathfrak{Q}_\sigma}$$

для всякого σ из G, не лежащего в $G_{\mathfrak{P}}$. В частности,

$$y \equiv x \pmod{\mathfrak{P}},$$
$$y \equiv 1 \pmod{\sigma^{-1}\mathfrak{P}}$$

для всякого σ вне $G_{\mathfrak{P}}$. Второе сравнение переписывается в виде

$$\sigma y \equiv 1 \pmod{\mathfrak{P}}$$

для всех $\sigma \notin G_{\mathfrak{P}}$. Норма элемента y из L^d в K есть произведение y на множители вида σy с $\sigma \notin G_{\mathfrak{P}}$. Следовательно,

$$N_K^{L^d}(y) \equiv x \pmod{\mathfrak{P}}.$$

Но норма лежит в K и даже в A, поскольку она является произведением элементов, целых над A. Так как и x, и норма лежат в B^d, то последнее сравнение выполняется по модулю $\mathfrak{Q}$. Но именно это и утверждается нашим предложением.

Пусть x — элемент из B. Мы будем обозначать через x' его образ относительно гомоморфизма $B \to B/\mathfrak{P}$. Тогда σ' есть автоморфизм поля $B/\mathfrak{P}$, удовлетворяющий соотношению

$$\sigma' x' = (\sigma x)'.$$

Пусть $f(X)$ — многочлен с коэффициентами в B. Мы будем обозначать через $f'(X)$ его естественный образ при предыдущем гомоморфизме. Таким образом, если

$$f(X) = b_n X^n + \cdots + b_0,$$

то

$$f'(X) = b_n' X^n + \cdots + b_0'.$$

Предложение 14. *Пусть кольцо A целозамкнуто в своем поле частных K; B — его целое замыкание в конечном расширении Галуа L поля K с группой G; $\mathfrak{p}$ — максимальный идеал в A и $\mathfrak{P}$ — максимальный идеал в B, лежащий над $\mathfrak{p}$. Тогда $B/\mathfrak{P}$ — нормальное расширение поля $A/\mathfrak{p}$ и отображение $\sigma \mapsto \sigma'$ индуцирует гомоморфизм $G_{\mathfrak{P}}$ на группу Галуа $G'_{\mathfrak{P}}$ расширения $B/\mathfrak{P}$ над $A/\mathfrak{p}$.*

Доказательство. Пусть $B' = B/\mathfrak{P}$ и $A' = A/\mathfrak{p}$. Любой элемент из B' может быть записан как x' для некоторого $x \in B$. Элемент x' порождает некоторое сепарабельное подрасширение в B' над A'. Пусть f — неприводимый многочлен для x над K. Коэффициенты f лежат в A, поскольку сам x — целый над A и все корни f — целые над A. Таким образом,

$$f(X) = \prod_{i=1}^{m} (X - x_i)$$

разлагается на линейные множители в B. Так как

$$f'(X) = \prod_{i=1}^{m} (X - x_i')$$

и все x'_i лежат в B', то f' разлагается на линейные множители в B'. Заметим, что $f(x)=0$ влечет $f'(x')=0$. Следовательно, B' нормально над A' и

$$[A'(x'):A'] \leqslant [K(x):K] \leqslant [L:K].$$

Это означает, что максимальное сепарабельное подрасширение поля A' в B' имеет конечную степень над A' (использовать теорему о примитивном элементе из элементарной теории полей). Эта степень в действительности ограничена числом $[L:K]$.

Остается доказать, что отображение $\sigma \longmapsto \sigma'$ дает сюръективный гомоморфизм группы $G_{\mathfrak{P}}$ на группу Галуа расширения B' над A'. Чтобы сделать это, мы сначала приведем соображение, сводящее задачу к случаю, когда $\mathfrak{P}$ — единственный простой идеал в B, лежащий над $\mathfrak{p}$. Именно, *в силу предложения 13 поля вычетов основного кольца и кольца* B^d в поле разложения одинаковы. Значит, для доказательства сюръективности мы можем взять в качестве основного поля L^d. Это и есть желаемая редукция, так что мы можем считать, что $K=L^d$, $G=G_{\mathfrak{P}}$.

Так и считая, выберем образующую максимального сепарабельного подрасширения в B' над A'; пусть это будет x' для некоторого элемента x из B. Пусть f — неприводимый многочлен элемента x над K. Всякий автоморфизм поля B' определяется его действием на x', а x' он переводит в некоторый корень многочлена f'. Положим $x=x_1$. Для любого данного корня x_i многочлена f существует элемент σ группы $G=G_{\mathfrak{P}}$, такой, что $\sigma x = x_i$. Следовательно, $\sigma' x' = x'_i$, так что автоморфизмы B' над A', индуцированные элементами из G, действуют транзитивно на корнях f'. Значит, они дают нам все автоморфизмы поля вычетов, что и требовалось показать.

Следствие 1. *Пусть* A *— кольцо, целозамкнутое в своем поле частных* K; L *— конечное расширение Галуа поля* K; B *— целое замыкание* A *в* L; $\mathfrak{p}$ *— некоторый максимальный идеал в* A; $\varphi\colon A \to A/\mathfrak{p}$ *— канонический гомоморфизм и* ψ_1, ψ_2 *— два гомоморфизма кольца* B *в заданное алгебраическое замыкание поля* $A/\mathfrak{p}$, *продолжающие* φ. *Тогда существует такой автоморфизм* σ *поля* L *над* K, *что*

$$\psi_1 = \psi_2 \circ \sigma.$$

Доказательство. Ядра ψ_1, ψ_2 — это простые идеалы в B, сопряженные между собой согласно предложению 11. Следовательно, существует такой элемент τ группы Галуа G, что ψ_1, $\psi_2 \circ \tau$ имеют одно и то же ядро. Не теряя общности, мы можем поэтому считать, что ψ_1, ψ_2 имеют одно и то же ядро $\mathfrak{P}$. Следовательно, существует автоморфизм ω поля $\psi_1(B)$ на $\psi_2(B)$, такой, что $\omega \circ \psi_1 = \psi_2$. В силу

предыдущего предложения существует элемент σ группы $G_{\mathfrak{P}}$, для которого $\omega \circ \psi_1 = \psi_1 \circ \sigma$. Это доказывает нужное нам утверждение.

Замечание. Во всех предыдущих предложениях можно было бы предполагать, что $\mathfrak{p}$ — произвольный простой, а не обязательно максимальный идеал. В этом случае, чтобы иметь возможность применить наши доказательства, достаточно произвести локализацию в $\mathfrak{p}$.

Ядро отображения

$$G_{\mathfrak{P}} \to G'_{\mathfrak{P}},$$

с которым мы имели дело выше, называется *группой инерции* идеала $\mathfrak{P}$. Она состоит из тех автоморфизмов в $G_{\mathfrak{P}}$, которые индуцируют тривиальный автоморфизм на поле вычетов. Неподвижное поле этой группы называется *полем инерции* и обозначается через L^t.

Следствие 2. *Сохраняя предпосылки следствия* 1, *предположим еще, что* $\mathfrak{P}$ — *единственный простой идеал в* B, *лежащий над* $\mathfrak{p}$. *Пусть* $f(X)$ — *многочлен из* $A[X]$ *со старшим коэффициентом* 1, *неприводимый в* $K[X]$ *и имеющий корень* α *в* B. *Тогда многочлен* f' *является степенью неприводимого многочлена из* $A'[X]$.

Доказательство. Как следует из доказательства предложения 14, любые два корня f' сопряжены относительно некоторого изоморфизма B' над A' и, следовательно, f' не может разлагаться на взаимно простые множители. Поэтому f' есть степень неприводимого многочлена.

Предложение 15. *Пусть* A — *целостное кольцо, целозамкнутое в своем поле частных* K, *и* L — *конечное расширение Галуа поля* K, *причем* $L = K(\alpha)$, *где* α — *целый элемент над* A, *являющийся корнем неприводимого многочлена*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0, \qquad a_i \in A.$$

Пусть $f'(X)$ — *соответствующий многочлен с коэффициентами из* $A/\mathfrak{p}$, *где* $\mathfrak{p}$ — *некоторый максимальный идеал в* A. *Пусть, наконец,* $\mathfrak{P}$ — *лежащий над* $\mathfrak{p}$ *простой идеал из целого замыкания* B *кольца* A *в* L *и* $G_{\mathfrak{P}}$ — *его группа разложения. Если у* f' *нет кратных корней, то отображение* $\sigma \mapsto \sigma'$ *имеет тривиальное ядро и является изоморфизмом группы* $G_{\mathfrak{P}}$ *на группу Галуа многочлена* f' *над* $A/\mathfrak{p}$.

Доказательство. Пусть

$$f(X) = \prod (X - x_i)$$

— разложение f в L. Как мы знаем, $x_i \in B$. Если $\sigma \in G_{\mathfrak{P}}$, то, как и прежде, обозначим через σ' гомоморфный образ σ в группе $G'_{\mathfrak{P}}$.

Имеем

$$f'(X) = \prod (X - x_i').$$

Предположим, что $\sigma' x_i' = x_i'$ для всех i. Так как $(\sigma x_i)' = \sigma' x_i'$ и так как f' не имеет кратных корней, то автоморфизм σ также тождественный. Следовательно, наше отображение инъективно, а группа инерции тривиальна. Поле $A'[x_1', \ldots, x_n']$ есть подполе в B', и любой автоморфизм B' над A', ограничение которого на это подполе тождественно, должен быть тождественным, поскольку $G_{\mathfrak{B}} \to G'_{\mathfrak{B}}$ — сюръективное отображение на группу Галуа B' над A'. Следовательно, B' чисто несепарабельно над $A'[x_1', \ldots, x_n']$, а потому группа $G_{\mathfrak{B}}$ изоморфна группе Галуа многочлена f' над A'.

Предложение 15 дает очень эффективный инструмент для исследования многочленов над кольцом. Например, рассмотрим „общий" многочлен

$$f_w(X) = X^n + w_{n-1}X^{n-1} + \ldots + w_0,$$

где $w_0, \ldots, w_{n-1}$ алгебраически независимы над полем k. Как мы знаем, группой Галуа этого многочлена над $k(w_0, \ldots, w_n)$ является симметрическая группа. Пусть $t_1, \ldots, t_n$ — его корни, и пусть α — образующая поля разложения. Не теряя общности, мы можем считать элемент α целым над кольцом $k[w_0, \ldots, w_{n-1}]$ (умножая любую заданную образующую на подходяще выбранный многочлен и используя предложение 1). Пусть $g_w(X)$ — неприводимый многочлен элемента α над $k(w_0, \ldots, w_{n-1})$. Коэффициентами g служат многочлены от (w). Если мы сможем подставить вместо (w) значения (a) с такими $a_0, \ldots, a_{n-1} \in k$, что g_a останется неприводимым, то, согласно предложению 15, мы тотчас получим заключение, что группа Галуа многочлена g_a также будет симметрической. Аналогично, если всякое поле между $k(w_0, \ldots, w_{n-1})$ и $k(t_1, \ldots, t_n)$ порождается n алгебраически независимыми элементами, то мы можем применить подобную конструкцию для получения расширений с заданными группами Галуа. Может ли это быть сделано, является одной из основных нерешенных задач теории Галуа. Это по существу есть параметризация всех расширений Галуа независимыми элементами.

В качестве другого примера рассмотрим многочлен $X^5 - X - 1$ над $\mathbf{Z}$.

Редукция по модулю 5 показывает, что этот многочлен неприводим. Редукция по модулю 2 дает неприводимые множители

$$(X^2 + X + 1)(X^3 + X^2 + 1) \pmod 2.$$

Следовательно, группа Галуа над полем рациональных чисел (как группа перестановок корней многочлена) содержит 5-цикл и произведение 2-цикла и 3-цикла. Отсюда легко вытекает, что она должна быть полной симметрической группой.

§ 3. Продолжение гомоморфизмов

Когда мы рассматривали процесс локализации, мы очень коротко остановились на вопросе о продолжении гомоморфизма на локальное кольцо. При изучении теории полей мы также привели одну теорему продолжения для вложений одного поля в другое. Теперь мы разберем вопрос о продолжении в полной общности.

Напомним сначала случай локального кольца. Пусть A — кольцо и $\mathfrak{p}$ — некоторый простой идеал. Как мы знаем, локальное кольцо $A_{\mathfrak{p}}$ — это множество всех дробей x/y, где x, $y \in A$ и $y \notin \mathfrak{p}$. Его максимальный идеал состоит из дробей, у которых $x \in \mathfrak{p}$. Пусть L — поле и φ: $A \to L$ — гомоморфизм, ядром которого служит $\mathfrak{p}$. Тогда мы можем продолжить φ до гомоморфизма $A_{\mathfrak{p}}$ в L, положив

$$\varphi(x/y) = \varphi(x)/\varphi(y),$$

где, как и выше, x/y — элемент из $A_{\mathfrak{p}}$.

Далее, мы имеем целые расширения колец. Пусть $\mathfrak{o}$ — локальное кольцо с максимальным идеалом $\mathfrak{m}$, B — целое расширение над $\mathfrak{o}$ и φ: $\mathfrak{o} \to L$ — гомоморфизм $\mathfrak{o}$ в некоторое алгебраически замкнутое поле L. Предположим, что ядром φ служит $\mathfrak{m}$. В силу предложения 9 из § 1 в B существует максимальный идеал $\mathfrak{M}$, лежащий над $\mathfrak{m}$, т. е. такой, что $\mathfrak{M} \cap \mathfrak{o} = \mathfrak{m}$. Тогда $B/\mathfrak{M}$ есть поле, являющееся алгебраическим расширением поля $\mathfrak{o}/\mathfrak{m}$, а $\mathfrak{o}/\mathfrak{m}$ изоморфно подполю $\varphi(\mathfrak{o})$ в L, поскольку ядро φ совпадает с $\mathfrak{m}$.

Мы можем выбрать такой изоморфизм поля $\mathfrak{o}/\mathfrak{m}$ на $\varphi(\mathfrak{o})$, что композиция гомоморфизмов

$$\mathfrak{o} \to \mathfrak{o}/\mathfrak{m} \to L$$

будет равна φ. Вложим теперь $B/\mathfrak{M}$ в L так, чтобы сделать коммутативной диаграмму

$$\begin{array}{ccc} B & \to & B/\mathfrak{M} \\ \uparrow & & \uparrow \searrow \\ \mathfrak{o} & \to & \mathfrak{o}/\mathfrak{m} \to L \end{array}$$

и получить таким образом гомоморфизм B в L, продолжающий φ.

Предложение 16. *Пусть A — подкольцо в B, причем B — целое над A. Пусть φ: $A \to L$ — гомоморфизм в некоторое алгебраически замкнутое поле L. Тогда φ обладает продолжением до гомоморфизма B в L.*

Доказательство. Пусть $\mathfrak{p}$ — ядро φ и S — дополнение к $\mathfrak{p}$ в A. Мы имеем коммутативную диаграмму

$$\begin{array}{ccc} B & \to & S^{-1}B \\ \uparrow & & \uparrow \\ A & \to & S^{-1}A = A_{\mathfrak{p}} \end{array}$$

и φ может быть пропущен через канонический гомоморфизм кольца A в $S^{-1}A$. Кроме того, кольцо $S^{-1}B$ — целое над $S^{-1}A$. Это сводит вопрос к уже рассмотренному выше случаю с локальным кольцом.

Теорема 1. *Пусть A — подкольцо поля K и $x \in K$, $x \neq 0$. Пусть φ: $A \to L$ — гомоморфизм A в алгебраически замкнутое поле L. Тогда φ допускает продолжение до гомоморфизма в L либо кольца $A[x]$, либо кольца $A[x^{-1}]$.*

Доказательство. Мы можем продолжить φ до гомоморфизма локального кольца $A_{\mathfrak{p}}$, где $\mathfrak{p}$ — ядро φ. Таким образом, не теряя общности, мы можем считать, что A — локальное кольцо с максимальным идеалом $\mathfrak{m}$. Предположим, что

$$\mathfrak{m}A[x^{-1}] = A[x^{-1}].$$

Тогда

$$1 = a_0 + a_1 x^{-1} + \cdots + a_n x^{-n},$$

где $a_i \in \mathfrak{m}$. Умножив на x^n, получим

$$(1 - a_0)\, x^n + b_{n-1} x^{n-1} + \cdots + b_0 = 0$$

с надлежащими элементами $b_i \in A$. У нас $a_0 \in \mathfrak{m}$, так что $1 - a_0 \notin \mathfrak{m}$, и, следовательно, $1 - a_0$ есть единица в A, поскольку предполагается, что A — локальное кольцо. Разделив на $1 - a_0$, мы видим, что элемент x — целый над A и что, следовательно, наш гомоморфизм обладает продолжением на $A[x]$.

Если, напротив, мы имеем, что

$$\mathfrak{m}A[x^{-1}] \neq A[x^{-1}],$$

то $\mathfrak{m}A[x^{-1}]$ содержится в некотором максимальном идеале $\mathfrak{P}$ кольца $A[x^{-1}]$ и идеал $\mathfrak{P} \cap A$ содержит $\mathfrak{m}$. Поскольку $\mathfrak{m}$ максимальный, мы должны иметь $\mathfrak{P} \cap A = \mathfrak{m}$. Так как φ и каноническое отображение $A \to A/\mathfrak{m}$ имеют одно и то же ядро, а именно $\mathfrak{m}$, то мы можем найти вложение ψ поля $A/\mathfrak{m}$ в L, такое, что композиция

$$A \to A/\mathfrak{m} \xrightarrow{\psi} L$$

равна φ. Отметим, что $A/\mathfrak{m}$ канонически вкладывается в $B/\mathfrak{P}$, где $B = A[x^{-1}]$. Продолжим ψ до гомоморфизма $B/\mathfrak{P}$ в L, что мы можем сделать независимо от того, будет ли образ x^{-1} в $B/\mathfrak{P}$ трансцендентным или алгебраическим над $A/\mathfrak{m}$. Композиция

$$B \to B/\mathfrak{P} \to L$$

и дает нам искомое продолжение φ.

Следствие. *Пусть A — подкольцо поля K, L — некоторое алгебраически замкнутое поле, φ: $A \to L$ — гомоморфизм и B —*

максимальное подкольцо в K, на которое φ может быть продолжен в качестве гомоморфизма в L. Тогда B — локальное кольцо, и если $x \in K$, $x \neq 0$, то либо $x \in B$, либо $x^{-1} \in B$.

Доказательство. Пусть S — множество пар (C, ψ), где C — подкольцо в K, содержащее A, и ψ: $C \to L$ — гомоморфизм, продолжающий φ. Тогда S не пусто [оно содержит (A, φ)] и частично упорядочено по отношению к возрастающему включению и ограничению. Другими словами, $(C, \psi) \leqslant (C', \psi')$, если $C \subset C'$, и ограничение ψ' на C равно ψ. Ясно, что S индуктивно упорядочено, поэтому в силу леммы Цорна существует максимальный элемент, скажем (B, ψ_0). Тогда, во-первых, B — локальное кольцо, иначе ψ_0 продолжается до локального кольца, определяемого его ядром, и во-вторых, B обладает требуемым свойством в соответствии с теоремой 1.

УПРАЖНЕНИЯ

1. Какова группа Галуа над полем рациональных чисел уравнения

$$X^4 + 2X^2 + X + 3 = 0?$$

2. Указать многочлен степени 6, группа Галуа которого была бы симметрической группой на 6 элементах.

3. Пусть K — расширение Галуа поля рациональных чисел $\mathbf{Q}$ с группой G, B — целое замыкание кольца $\mathbf{Z}$ в K, и пусть элемент $\alpha \in B$ таков, что $K = Q(\alpha)$. Положим $f(X) = \operatorname{Irr}(\alpha, Q, X)$ и предположим, что f остается неприводимым над $\mathbf{Z}/p\mathbf{Z}$, где p — некоторое простое число. Что вы можете сказать о группе Галуа G?

4. Пусть A — целостное кольцо, K — его поле частных и t — трансцендентный элемент над K. Показать, что если A целозамкнуто, то $A[t]$ также целозамкнуто.

5. Пусть A — целостное кольцо, целозамкнутое в своем поле частных K, L — конечное сепарабельное расширение поля K и B — целое замыкание A в L. Показать, что если A нетерево, то B — конечный A-модуль. [*Указание*: пусть $\{\omega_1, \ldots, \omega_n\}$ — базис поля L над K. Умножив все элементы этого базиса на подходящий элемент из A, мы можем, не теряя общности, считать, что все ω_i — целые над A. Пусть $\{\omega_1', \ldots, \omega_n'\}$ — дуальный базис относительно следа, так что $\operatorname{Tr}(\omega_i \omega_j') = \delta_{ij}$. Запишем α из L, целый над A, в виде

$$\alpha = b_1\omega_1' + \ldots + b_n\omega_n',$$

где $b_j \in K$. Взяв след $\operatorname{Tr}(\alpha\omega_i)$ для $i = 1, \ldots, n$, заключаем, что B содержится в конечном модуле $A\omega_1' + \cdots + A\omega_n'$.]

6. Предыдущее упражнение применимо к случаю, когда $A = \mathbf{Z}$ и $K = \mathbf{Q}$. Всякое конечное расширение поля $\mathbf{Q}$ называется *числовым полем*, а целое замыкание кольца $\mathbf{Z}$ в таком расширении L называется кольцом *целых алгебраических чисел* поля L. Обозначим его через I_L. Пусть $\sigma_1, \ldots, \sigma_n$ — раз-

личные вложения L в поле комплексных чисел. Вложим I_L в евклидово пространство посредством отображения

$$\alpha \longmapsto (\sigma_1\alpha, \ldots, \sigma_n\alpha).$$

Показать, что в любой ограниченной области пространства имеется лишь конечное число элементов из I_L. [*Указание*: коэффициенты в целом уравнении для α являются элементарными симметрическими функциями от сопряженных с α элементов и, таким образом, являются ограниченными целыми числами.] Использовать упражнение 10 из гл. III для вывода, что I_L есть свободный $\mathbf{Z}$-модуль размерности $\leqslant n$. Показать, что в действительности его размерность равна n, причем базис I_L над $\mathbf{Z}$ служит также базисом L над $\mathbf{Q}$.

7. Пусть E — конечное расширение над $\mathbf{Q}$; I_E — кольцо целых алгебраических чисел поля E; U — группа единиц кольца I_E; $\sigma_1, \ldots, \sigma_n$ — различные вложения E в $\mathbf{C}$. Отобразим U в евклидово пространство посредством отображения

$$l\colon \alpha \longmapsto (\log|\sigma_1\alpha|, \ldots, \log|\sigma_n\alpha|).$$

Показать, что $l(U)$ — *конечно порожденная свободная абелева группа*, установив, что в любой конечной области пространства имеется лишь конечное число элементов из $l(U)$. Показать, что ядро отображения l — конечная группа, являющаяся поэтому группой корней из единицы в E. Таким образом, сама группа U — *конечно порожденная абелева группа*.

8. Используя лемму Цорна, обобщить результаты § 2, особенно предложения 11 и 14, на бесконечные расширения Галуа.

Глава X

Трансцендентные расширения

В этой главе слово „кольцо" означает „коммутативное кольцо".

§ 1. Базисы трансцендентности

Пусть K — расширение поля k и S — некоторое подмножество в K. Напомним, что S называется алгебраически независимым над k, если из соотношения

$$0 = \sum a_{(\nu)} M_\nu(S) = \sum a_{(\nu)} \prod_{x \in S} x^{\nu(x)}$$

с коэффициентами $a_{(\nu)} \in k$, почти все из которых равны 0, с необходимостью следует, что все $a_{(\nu)} = 0$.

Мы можем ввести отношение порядка среди алгебраически независимых подмножеств в K по возрастающему включению. Эти подмножества тогда, очевидно, оказываются индуктивно упорядоченными, и, таким образом, существуют максимальные элементы. Если S — алгебраически независимое подмножество в K и если мощность S является наибольшей среди мощностей всех таких подмножеств, то мы будем называть эту мощность *степенью трансцендентности* или *размерностью* расширения K над k. В действительности нам будет необходимо различать только конечные степени трансцендентности и бесконечные степени трансцендентности. Заметим, что понятие степени трансцендентности находится в таком же отношении к понятию алгебраической независимости, как понятие размерности к понятию линейной независимости.

Мы часто будем иметь дело с семействами элементов из K, скажем с семейством $\{x_i\}_{i \in I}$; мы будем говорить, что такое семейство алгебраически независимо над k, если его элементы различны (другими словами, $x_i \neq x_j$ при $i \neq j$), и множество, состоящее из элементов этого семейства, алгебраически независимо над k.

Подмножество S в K, алгебраически независимое над k и максимальное относительно упорядоченности по включению, будет называться *базисом трансцендентности* поля K над k. Из максималь-

ности ясно, что если S — базис трансцендентности K над k, то поле K алгебраично над $k(S)$.

Теорема 1. *Пусть K — расширение поля k. Любые два базиса трансцендентности K над k имеют одинаковую мощность. Если Γ — множество образующих K над k (т. е. $K=k(\Gamma)$) и S — подмножество в Γ, алгебраически независимое над k, то существует базис трансцендентности $\mathscr{B}$ поля K над k, такой, что $S\subset\mathscr{B}\subset\Gamma$.*

Доказательство. Мы докажем, что если существует один конечный базис трансцендентности, скажем $\{x_1, \ldots, x_m\}$, $m\geqslant 1$, то любой другой базис трансцендентности также должен содержать m элементов. Для этого достаточно будет доказать следующее: если $w_1, \ldots, w_n$ — элементы из K, алгебраически независимые над k, то $n\leqslant m$ (так как затем мы сможем использовать симметрию). По предположению существует ненулевой многочлен f_1 от $m+1$ переменных с коэффициентами в k, такой, что

$$f_1(w_1, x_1, \ldots, x_m)=0.$$

Кроме того, по предположению w_1 встречается в f_1 и некоторое x_i, скажем x_1, также встречается в f_1. Тогда элемент x_1 алгебраичен над $k(w_1, x_2, \ldots, x_m)$. Предположим по индукции, что после подходящей перенумерации $x_2, \ldots, x_m$ мы можем найти $w_1, \ldots, w_r$ $(r<n)$, такие, что K алгебраично над

$$k(w_1, \ldots, w_r, x_{r+1}, \ldots, x_m).$$

Тогда существует ненулевой многочлен f от $m+1$ переменных с коэффициентами в k, для которого

$$f(w_{r+1}, w_1, \ldots, w_r, x_{r+1}, \ldots, x_m)=0,$$

причем w_{r+1} действительно встречается в f. Так как все w алгебраически независимы над k, то некоторый элемент x_j $(j=r+1, \ldots, m)$ также встречается в f. После перенумерации мы можем считать, что $j=r+1$. Тогда x_{r+1} алгебраичен над

$$k(w_1, \ldots, w_{r+1}, x_{r+2}, \ldots, x_m).$$

Поскольку башня алгебраических расширений является алгебраическим расширением, то K алгебраично над $k(w_1, \ldots, w_{r+1}, x_{r+2}, \ldots, x_m)$. Мы можем повторять эту процедуру, и если $n\geqslant m$, то, заменив все x элементами w, мы обнаружим, что K алгебраично над $k(w_1, \ldots, w_m)$. Это показывает, что из $n\geqslant m$ следует равенство $n=m$, что и требовалось.

Мы, таким образом, доказали следующее: либо степень трансцендентности конечна и равна мощности любого другого базиса трансцендентности, либо она бесконечна, и тогда всякий базис трансцендент-

ности бесконечен. Утверждение о мощности в бесконечном случае предоставляется читателю в качестве упражнения. Мы также оставляем в качестве упражнения утверждение о том, что всякое множество алгебраически независимых элементов может быть дополнено до базиса трансцендентности, выбранного из данного множества образующих. (Читатель отметит полную аналогию этих утверждений с соответствующими утверждениями о линейных базисах.)

§ 2. *Теорема Гильберта о нулях*

Теорема о нулях является специальным случаем теоремы о продолжении гомоморфизмов, относящимся к конечно порожденным кольцам над полями.

Теорема 2. *Пусть* k *— поле,* $k[x] = k[x_1, \ldots, x_n]$ *— конечно порожденное кольцо над* k *и* $\varphi\colon k \to L$ *— вложение* k *в некоторое алгебраически замкнутое поле* L. *Тогда существует продолжение* φ *до гомоморфизма* $k[x]$ *в* L.

Доказательство. Пусть $\mathfrak{M}$ — некоторый максимальный идеал в $k[x]$, σ — канонический гомоморфизм $\sigma\colon k[x] \to k[x]/\mathfrak{M}$. Тогда $\sigma k[\sigma x_1, \ldots, \sigma x_n]$ — поле, являющееся расширением поля σk. Если мы сможем доказать нашу теорему для случая, когда конечно порожденное кольцо является в действительности полем, то мы рассмотрим тогда ограничение $\varphi \circ \sigma^{-1}$ на σk и продолжим его до гомоморфизма $\sigma k[\sigma x_1, \ldots, \sigma x_n]$ в L, что и даст нам искомое продолжение для φ.

Не теряя поэтому общности, мы предполагаем, что $k[x]$ — поле. Если оно алгебраично над k, то все доказано (в силу известного результата для алгебраических расширений). В противном случае пусть $t_1, \ldots, t_r$ — некоторый базис трансцендентности, $r \geqslant 1$. Не теряя общности, мы можем считать, что φ тождественно на k. Каждый элемент $x_1, \ldots, x_n$ алгебраичен над $k(t_1, \ldots, t_r)$. Умножив неприводимый многочлен $\operatorname{Irr}(x_i, k(t), X)$ на подходящий ненулевой элемент из $k[t]$, мы получим многочлен, все коэффициенты которого лежат в $k[t]$. Пусть $a_1(t), \ldots, a_n(t)$ — множество старших коэффициентов этих многочленов и $a(t)$ — их произведение

$$a(t) = a_1(t) \ldots a_n(t).$$

Так как $a(t) \neq 0$, то существуют такие элементы $t_1', \ldots, t_r' \in \bar{k}$, что $a(t') \neq 0$ и, следовательно, $a_i(t') \neq 0$ ни для какого i.

Каждый элемент x_i является целым над кольцом

$$k\left[t_1, \ldots, t_r, \frac{1}{a_1(t)}, \ldots, \frac{1}{a_r(t)}\right].$$

Рассмотрим гомоморфизм

$$\varphi\colon k[t_1, \ldots, t_r] \to \bar{k},$$

который тождествен на k и для которого $\varphi(t_j) = t'_j$. Пусть $\mathfrak{p}$ — его ядро. Тогда $a(t) \notin \mathfrak{p}$. Наш гомоморфизм φ однозначно продолжается на локальное кольцо $k[t]_{\mathfrak{p}}$, а в силу предыдущих замечаний он продолжается до гомоморфизма

$$k[t]_{\mathfrak{p}}[x_1, \ldots, x_n]$$

в $\bar{k}$, согласно предложению 16 из гл. IX, § 2. Это доказывает требуемое утверждение.

Следствие 1. *Пусть k — поле и $k[x_1, \ldots, x_n] = k[x]$ — конечно порожденное кольцо над k. Если $k[x]$ — поле, то $k[x]$ алгебраично над k.*

Доказательство. Все гомоморфизмы поля являются изоморфизмами (на образ), и существует гомоморфизм $k[x]$ над k в алгебраическое замыкание поля k.

Следствие 2. *Пусть $k[x_1, \ldots, x_n]$ — конечно порожденное целостное кольцо над полем k, и пусть $y_1, \ldots, y_m$ — ненулевые элементы этого кольца. Тогда существует такой гомоморфизм*

$$\psi\colon k[x] \to \bar{k}$$

над k, что $\psi(y_j) \neq 0$ ни для одного $j = 1, \ldots, m$.

Доказательство. Рассмотрим кольцо $k\left[x_1, \ldots, x_n, y_1^{-1}, \ldots, y_m^{-1}\right]$ и применим к нему теорему.

Пусть S — некоторое множество многочленов в кольце многочленов $k[X_1, \ldots, X_n]$ от n переменных, L — некоторое расширение поля k. Под *нулем* множества S в L понимают любой набор из n элементов $(c_1, \ldots, c_n)$, лежащих в L, такой, что

$$f(c_1, \ldots, c_n) = 0$$

для всех $f \in S$. Если S состоит из одного многочлена f, то мы будем также говорить, что (c) есть нуль f. Множество всех нулей семейства S называется *алгебраическим множеством* в L (или, точнее, в $L^{(n)}$). Пусть $\mathfrak{a}$ — идеал, порожденный всеми элементами из S. Поскольку $S \subset \mathfrak{a}$, ясно, что всякий нуль $\mathfrak{a}$ служит также нулем S. Однако, очевидно, справедливо и обратное, а именно всякий нуль S является также нулем $\mathfrak{a}$, поскольку всякий элемент из $\mathfrak{a}$ имеет вид

$$g_1(X) f_1(X) + \ldots + g_m(X) f_m(X),$$

где $f_j \in S$, а $g_i \in k[X]$. Таким образом, рассматривая нули какого-либо множества S, мы всегда можем считать их нулями некоторого идеала. Отметим кстати, что любое алгебраическое множество будет множеством нулей некоторого конечного числа многочленов, так как всякий идеал в $k[X]$ конечно порожден (гл. VI). Еще одним следствием теоремы 2 является

Теорема Гильберта о нулях. *Пусть* $\mathfrak{a}$ — *идеал в* $k[X] = k[X_1, \ldots, X_n]$, *и пусть всякий его нуль* $(c) = (c_1, \ldots, c_n)$ *в* $\bar{k}^{(n)}$ *будет также нулем многочлена* $f \in k[X]$: $f(c) = 0$ *Тогда существует целое число* $m \geqslant 0$, *для которого* $f^m \in \mathfrak{a}$.

Доказательство. Если $\mathfrak{a}$ — само кольцо многочленов, то наше утверждение очевидно. Пусть $\mathfrak{a} \neq k[X]$. Предположим, что никакая степень f^m многочлена f не лежит в $\mathfrak{a}$ $(m = 0, 1, \ldots)$. Обозначим через S мультипликативное множество всех степеней f и через $\mathfrak{p}$ — максимальный элемент в множестве идеалов, содержащих $\mathfrak{a}$, пересечение которых с S пусто. Тогда $\mathfrak{p}$ — простой идеал, согласно предложению 6 из гл. VI, § 4. Имеет место изоморфизм

$$k[X_1, \ldots, X_n]/\mathfrak{p} \approx k[x_1, \ldots, x_n],$$

и так как $f \notin \mathfrak{p}$, то $f(x_1, \ldots, x_n) \neq 0$. Пусть

$$\varphi\colon k[x] \to \bar{k}$$

— гомоморфизм над k, для которого $\varphi(f(x)) \neq 0$. Тогда $\varphi(f(x)) = f(\varphi(x))$, где $\varphi(x) = (\varphi(x_1), \ldots, \varphi(x_n))$. Это противоречит предположению, что f обращается в нуль на всех алгебраических нулях идеала $\mathfrak{a}$.

§ 3. Алгебраические множества

Мы ограничимся несколькими самыми элементарными замечаниями об алгебраических множествах. Пусть k — поле, A — алгебраическое множество нулей в некотором фиксированном алгебраически замкнутом расширении этого поля. Множество всех многочленов $f \in k[X_1, \ldots, X_n]$, таких, что $f(x) = 0$ для всех $(x) \in A$, является, очевидно, идеалом $\mathfrak{a}$ в $k[X]$, и этот идеал определяется множеством A Мы будем называть его идеалом, *принадлежащим* A, или же говорить, что он *ассоциирован* с A. Если A — множество нулей множества многочленов S, то $S \subset \mathfrak{a}$, причем $\mathfrak{a}$ может быть больше, чем S. С другой стороны, заметим, что A есть также множество нулей идеала $\mathfrak{a}$.

Пусть A, B — алгебраические множества, $\mathfrak{a}$, $\mathfrak{b}$ — их ассоциированные идеалы. Тогда ясно, что $A \subset B$ в том и только в том случае, если $\mathfrak{a} \supset \mathfrak{b}$. Следовательно, $A = B$ в точности тогда, когда $\mathfrak{a} = \mathfrak{b}$. Это приводит к важному следствию. Поскольку кольцо многочленов

$k[X]$ нётерово, то алгебраические множества удовлетворяют дуальному свойству, а именно во всякой убывающей последовательности алгебраических множеств

$$A_1 \supset A_2 \supset \ldots$$

обязательно $A_m = A_{m+1} = \ldots$ для некоторого целого m, т. е. все A_ν равны при $\nu \geqslant m$. Кроме того, по двойственности к другому свойству, характеризующему условие нётеровости, заключаем, что всякое непустое множество алгебраических множеств содержит минимальный элемент.

Теорема 3. *Конечное объединение и конечное пересечение алгебраических множеств являются алгебраическими множествами. Если A, B — алгебраические множества нулей идеалов $\mathfrak{a}$, $\mathfrak{b}$ соответственно, то $A \cup B$ будет множеством нулей идеала $\mathfrak{a} \cap \mathfrak{b}$, а $A \cap B$ — множеством нулей идеала* $(\mathfrak{a}, \mathfrak{b})$.

Доказательство. Рассмотрим сначала $A \cup B$. Пусть $(x) \in A \cup B$. Тогда (x) есть нуль идеала $\mathfrak{a} \cap \mathfrak{b}$. Обратно, пусть (x) — нуль идеала $\mathfrak{a} \cap \mathfrak{b}$, причем $(x) \notin A$. Тогда существует многочлен $f \in \mathfrak{a}$, такой, что $f(x) \neq 0$. Но $(f)\mathfrak{b} \subset \mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ и, следовательно, $(fg)(x) = 0$ для всех $g \in \mathfrak{b}$, откуда $g(x) = 0$ для всех $g \in \mathfrak{b}$. Следовательно, (x) лежит в B и $A \cup B$ есть алгебраическое множество нулей идеала $\mathfrak{a} \cap \mathfrak{b}$.

Чтобы доказать, что $A \cap B$ — алгебраическое множество, возьмем $(x) \in A \cap B$. Тогда (x) будет нулем идеала $(\mathfrak{a}, \mathfrak{b})$. Обратно, пусть (x) — нуль идеала $(\mathfrak{a}, \mathfrak{b})$. Тогда, очевидно, $(x) \in A \cap B$, что и требовалось. Это доказывает нашу теорему.

Алгебраическое множество V называется *k-неприводимым*, если оно не может быть представлено в виде объединения $V = A \cup B$ алгебраических множеств A, B, где A, B отличны от V. Мы будем иногда говорить „неприводимое“ вместо „k-неприводимое“.

Теорема 4. *Всякое алгебраическое множество A может быть представлено в виде конечного объединения неприводимых алгебраических множеств*

$$A = V_1 \cup \ldots \cup V_r.$$

Если между V_i нет включений, т. е. если $V_i \not\subset V_j$ при $i \neq j$, то это представление единственно.

Доказательство. Сначала докажем существование. Предположим, что множество алгебраических множеств, которые не могут быть представлены в виде конечного объединения неприводимых алгебраических множеств, не пусто. Пусть V — минимальный элемент в нем. Тогда V не может быть неприводимым, и мы можем записать

$V = A \cup B$, где A, B — алгебраические множества, причем $A \neq V$ и $B \neq V$. Так как каждое из A, B строго меньше, чем V, то мы можем представить A, B в виде конечных объединений неприводимых алгебраических множеств, получив, таким образом, представление и для V, — противоречие.

Что касается единственности, то пусть

$$A = V_1 \cup \ldots \cup V_r = W_1 \cup \ldots \cup W_s$$

— два представления A в виде объединения неприводимых алгебраических множеств без включений. Каждое W_j мы можем записать в виде

$$W_j = (W_j \cap V_1) \cup \ldots \cup (W_j \cap V_r).$$

Так как множество $W_j \cap V_i$ — алгебраическое, то $W_j = W_j \cap V_i$ для некоторого i. Следовательно, $W_j \subset V_i$ для некоторого i. Аналогично V_i содержится в некотором W_v. Поскольку между W_j нет включений, мы должны иметь $W_j = V_i = W_v$. Наше рассуждение может быть проведено для каждого W_j и каждого V_i. Это доказывает, что каждое W_j встречается среди V_i и каждое V_i — среди W_j, откуда и вытекает единственность представления.

В качестве упражнения докажите, что тогда и только тогда алгебраическое множество неприводимо, когда его ассоциированный идеал простой. Неприводимое алгебраическое множество обычно называют *многообразием*.

Понятие алгебраического множества может быть следующим образом обобщено на произвольные (коммутативные) кольца.

Пусть A—коммутативное кольцо. Под *спектром* $\operatorname{spec}(A)$ мы будем понимать множество простых идеалов в A. Подмножество C в $\operatorname{spec}(A)$ называется *замкнутым*, если существует идеал $\mathfrak{a}$ кольца A, такой, что C состоит из всех простых идеалов $\mathfrak{p}$, для которых $\mathfrak{a} \subset \mathfrak{p}$. Дополнение к замкнутому подмножеству в $\operatorname{spec}(A)$ называется *открытым* подмножеством в $\operatorname{spec}(A)$. Следующие утверждения легко проверяются, и их проверка предоставляется читателю.

Объединение конечного числа замкнутых множеств замкнуто. Пересечение произвольного семейства замкнутых множеств замкнуто.

Пересечение конечного числа открытых множеств открыто. Объединение произвольного семейства открытых множеств открыто.

Пустое множество и все множество $\operatorname{spec}(A)$ *одновременно и открыты, и замкнуты.*

Для всякого подмножества S в A множество простых идеалов $\mathfrak{p} \in \operatorname{spec}(A)$, таких, что $S \subset \mathfrak{p}$, совпадает с множеством простых идеалов $\mathfrak{p}$, содержащих идеал, порожденный S.

Пусть $f \in A$. Мы можем рассматривать множество простых идеалов из $\operatorname{spec}(A)$, содержащих f, как множество нулей элемента f. Действительно, это есть множество таких $\mathfrak{p}$, для которых образом f при каноническом гомоморфизме

$$A \to A/\mathfrak{p}$$

служит 0.

Пусть A, B — кольца и φ: $A \to B$ — гомоморфизм. Тогда φ индуцирует отображение

$$\operatorname{spec}(\varphi) = \varphi^{-1}\colon \operatorname{spec}(B) \to \operatorname{spec}(A)$$

по правилу

$$\mathfrak{p} \longmapsto \varphi^{-1}(\mathfrak{p}).$$

Читатель тотчас проверит, что отображение $\operatorname{spec}(\varphi)$ непрерывно в том смысле, что если U — открытое множество в $\operatorname{spec}(B)$, то $\varphi^{-1}(U)$ открыто в $\operatorname{spec}(A)$.

Мы можем рассматривать spec как функтор из категории коммутативных колец в категорию топологических пространств. Топология, которую мы определили выше на множества $\operatorname{spec}(A)$, называется *топологией Зарисского*.

Под *точкой* из $\operatorname{spec}(A)$ в поле L понимается отображение

$$\operatorname{spec}(\varphi)\colon \operatorname{spec}(L) \to \operatorname{spec}(A),$$

индуцированное некоторым гомоморфизмом φ: $A \to L$ кольца A в L.

Например, каждому простому числу p соответствует точка из $\operatorname{spec}(\mathbf{Z})$, а именно точка, определяемая отображением редукции

$$\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}.$$

Соответствующая точка задается обращенной стрелкой

$$\operatorname{spec}(\mathbf{Z}) \leftarrow \operatorname{spec}(\mathbf{Z}/p\mathbf{Z}).$$

В качестве другого примера рассмотрим кольцо многочленов $k[X_1, \ldots, X_n]$ над полем k. Для всякого n-набора $(c_1, \ldots, c_n)$ из $\overline{k}^{(n)}$ имеем гомоморфизм

$$\varphi\colon k[X_1, \ldots, X_n] \to \overline{k},$$

такой, что φ тождествен на k и $\varphi(X_i) = c_i$ для всех i. Соответствующая точка задается обращенной стрелкой

$$\operatorname{spec}(k[X]) \leftarrow \operatorname{spec}(\overline{k}).$$

Таким образом, мы можем отождествлять точки из n-пространства $\overline{k}^{(n)}$ с точками из $\operatorname{spec}(k[X])$ (над k) в $\overline{k}$.

Обобщением понятия алгебраического множества, определенного нами выше, служит понятие замкнутого множества. В качестве упражнения предлагается доказать следующее утверждение.

Теорема 5. *Пусть A — нётерово кольцо. Тогда всякое замкнутое множество C в* $\operatorname{spec}(A)$ *может быть представлено как конечное объединение неприводимых замкнутых множеств, причем это представление единственно, если в объединении*

$$C = V_1 \cup \ldots \cup V_r$$

неприводимых замкнутых множеств включений $V_i \subset V_j$ при $i \neq j$ нет.

Разумеется, под неприводимым замкнутым множеством мы понимаем такое замкнутое множество, которое не может быть представлено в виде собственного объединения двух замкнутых множеств.

§ 4. Теорема Нётера о нормализации

Теорема 6. *Пусть $k[x_1, \ldots, x_n] = k[x]$ — конечно порожденное целостное кольцо над полем k, причем $k(x)$ имеет степень трансцендентности r. Тогда в $k[x]$ существуют элементы $y_1, \ldots, y_r$, такие, что кольцо $k[x]$ — целое над*

$$k[y] = k[y_1, \ldots, y_r].$$

Доказательство. Если $(x_1, \ldots, x_n)$ уже алгебраически независимы над k, то все доказано. Если нет, то имеется нетривиальное соотношение

$$\sum a_{(j)} x_1^{j_1} \ldots x_n^{j_n} = 0,$$

в котором каждый коэффициент $a_{(j)} \in k$ и $a_{(j)} \neq 0$. Сумма берется по конечному числу различных n-наборов целых чисел $(j_1, \ldots, j_n)$, $j_\nu \geqslant 0$. Пусть $m_2, \ldots, m_n$ — целые положительные числа. Положим

$$y_2 = x_2 - x_1^{m_2}, \ldots, y_n = x_n - x_1^{m_n}$$

и подставим $x_i = y_i + x_1^{m_i}$ $(i = 2, \ldots, n)$ в предыдущее уравнение. Используя векторные обозначения, положим $(m) = (1, m_2, \ldots, m_n)$ и введем скалярное произведение $(j) \cdot (m) = j_1 + m_2 j_2 + \ldots + m_n j_n$. Развернув соотношение после указанной подстановки, получим

$$\sum a_{(j)} x_1^{(j)\cdot(m)} + f(x_1, y_2, \ldots, y_n) = 0,$$

где f — многочлен, в котором не встречаются чистые степени x_1. Выберем теперь целое число d достаточно большим [скажем, большим, чем любая компонента вектора (j), для которого $a_{(j)} \neq 0$] и возьмем

$$m = (1, d, d^2, \ldots, d^{n-1}).$$

Тогда все $(j) \cdot (m)$ различны для тех (j), для которых $a_{(j)} \neq 0$. Тем самым мы получаем целое уравнение для x_1 над $k[y_2, \ldots, y_n]$.

Так как каждый из $x_i (i > 1)$ содержится в $k[x_1, y_2, \ldots, y_n]$, то кольцо $k[x]$ — целое над $k[y_2, \ldots, y_n]$. Мы можем теперь продолжать по индукции и, используя транзитивность целых расширений, уменьшать число игреков до тех пор, пока не дойдем до алгебраически независимого множества игреков.

§ 5. *Линейно свободные расширения*

В этом параграфе мы обсудим вопрос о том, каким образом два расширения K и L поля k ведут себя по отношению друг к другу. Мы будем считать, что все рассматриваемые поля содержатся в одном алгебраически замкнутом поле Ω.

Расширение K называется *линейно свободным*[1]) *от* L *над* k, если всякое конечное множество элементов из K, линейно независимое над k, линейно независимо и над L.

Это определение несимметрично, но на самом деле, как мы сейчас докажем, свойство быть линейно свободным симметрично относительно K и L. Предположим, что K линейно свободно от L над k. Пусть $y_1, \ldots, y_n$ — элементы из L, линейно независимые над k. Допустим, что имеется нетривиальное соотношение линейной зависимости над K

$$x_1y_1 + x_2y_2 + \ldots + x_ny_n = 0. \tag{1}$$

Пусть, скажем, $x_1, \ldots, x_r$ линейно независимы над k, а $x_{r+1}, \ldots, x_n$ являются их линейными комбинациями $x_i = \sum_{\mu=1}^{r} a_{i\mu}x_\mu$, $i=r+1, \ldots, n$. Перепишем соотношение (1) в виде

$$\sum_{\mu=1}^{r} x_\mu y_\mu + \sum_{i=r+1}^{n} \left(\sum_{\mu=1}^{r} a_{i\mu}x_\mu \right) y_i = 0$$

и, собрав члены после раскрытия скобок во второй сумме, получим

$$\sum_{\mu=1}^{r} \left(y_\mu + \sum_{i=r+1}^{n} (a_{i\mu}y_i) \right) x_\mu = 0.$$

Поскольку игреки линейно независимы над k, коэффициенты при x_μ не равны 0. Это противоречит линейной свободе K от L над k.

Дадим теперь два критерия линейной свободы.

Критерий 1. Пусть K — поле частных кольца R и L — поле частных кольца S, $k \subset K \cap L$. Чтобы убедиться в том, что L и K линейно свободны над k, достаточно показать, что если элементы

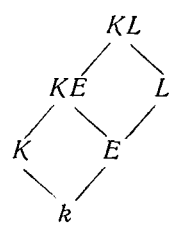
[1]) Или *линейно разделенным*. Алгебраически свободные поля (см. ниже) в равной мере называют также алгебраически разделенными. — *Прим. ред.*

$y_1, \ldots, y_n$ из S линейно независимы над k, то между ними нет линейных соотношений и над R. Действительно, если элементы $y_1, \ldots, y_n$ из L линейно независимы над k и если имеется соотношение $x_1y_1 + \ldots + x_ny_n = 0$ с $x_i \in K$, то мы можем выбрать y в S и x в R, такие, что $xy \neq 0$, $yy_i \in S$ для всех i и $xx_i \in R$ для всех i. Умножение нашего соотношения на xy дает линейную зависимость между элементами из R и S. Однако элементы yy_i, очевидно, линейно независимы над k, что и доказывает критерий.

Критерий 2. Пусть снова R — подкольцо в K, такое, что K есть его поле частных, и пусть R — векторное пространство над k с базисом $\{u_\alpha\}$. Чтобы доказать, что K и L линейно свободны над k, достаточно показать, что элементы $\{u_\alpha\}$ этого базиса линейно независимы и над L. Действительно, предположим, что это так. Пусть $x_1, \ldots, x_m$ — элементы из R, линейно независимые над k. Они лежат в конечномерном векторном пространстве, порожденном некоторыми из u_α, скажем $u_1, \ldots, u_n$, и могут быть дополнены до базиса этого пространства над k. При подъеме это n-мерное векторное пространство над L должно сохранить свою размерность, поскольку элементы u остаются по предположению линейно независимыми, а, следовательно, иксы также должны остаться линейно независимыми.

Следующее предложение дает полезный критерий, позволяющий устанавливать линейную свободу в башне полей:

Предложение 1. *Пусть K — поле, содержащее некоторое другое поле k, и $L \supset E$ — еще два расширения поля k. Тогда K и L линейно свободны над k в том и только в том случае, если K и E линейно свободны над k, а KE, L линейно свободны над E.*



Доказательство. Предположим сначала, что K, E линейно свободны над k и KE, L линейно свободны над E. Пусть $\{\varkappa\}$ — базис K как векторного пространства над k (мы используем сами элементы этого базиса в качестве их индексирующего множества), и пусть $\{\alpha\}$ — базис E над k, а $\{\lambda\}$ — базис L над E. Тогда $\{\alpha\lambda\}$ будет базисом L над k. Если K и L не являются линейно свободными над k, то существует соотношение

$$\sum_{\lambda,\,\alpha}\left(\sum_{\varkappa} c_{\varkappa\lambda\alpha}\varkappa\right)\lambda\alpha = 0 \quad \text{с какими-то} \quad c_{\varkappa\lambda\alpha} \neq 0, \quad c_{\varkappa\lambda\alpha} \in k.$$

Изменение порядка суммирования дает

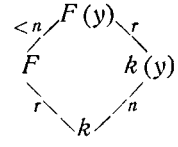
$$\sum_{\lambda}\left(\sum_{\varkappa,\,\alpha} c_{\varkappa\lambda\alpha}\varkappa\alpha\right)\lambda = 0$$

вопреки линейной свободе L и KE над E.

Обратно, предположим, что K и L линейно свободны над k. Тогда тем более K и E линейно свободны над k. Поле KE есть поле частных кольца $E[K]$, порожденного над E всеми элементами из K. Это кольцо является векторным пространством над E, и базис K над k служит также базисом для кольца $E[K]$ над E. Из этого замечания и из критериев линейной свободы мы видим, что достаточно доказать, что элементы такого базиса остаются линейно независимыми над L. Но это вытекает из предположения, что K и L линейно свободны над k.

Введем еще одно понятие, касающееся двух расширений K и L поля k. Мы будем говорить, что K *алгебраически свободно от* L *над* k, если всякое конечное множество элементов из K, алгебраически независимое над k, алгебраически независимо и над L. Пусть (x) и (y) — два множества элементов из Ω. Мы будем говорить, что они *свободны над* k (или *алгебраически независимы над* k), если поля $k(x)$ и $k(y)$ алгебраически свободны над k.

Так же как и в случае линейной свободы, наше определение несимметрично; докажем, что в действительности выражаемое им отношение симметрично. Именно, предположим, что K алгебраически свободно от L над k. Пусть $y_1, \ldots, y_n$ — элементы из L, алгебраически независимые над k. Допустим, что они становятся зависимыми над K. Тогда они являются алгебраически зависимыми уже над некоторым подполем F в K, конечно порожденным над k и, скажем, имеющим степень трансцендентности r над k. Подсчет степени трансцендентности поля $F(y)$ над k двумя способами приводит к противоречию (см. упражнение 5):



Предложение 2. *Если* K *и* L *линейно свободны над* k, *то они алгебраически свободны над* k.

Доказательство. Пусть $x_1, \ldots, x_n$ — элементы из K, алгебраически независимые над k. Предположим, что они становятся алгебраически зависимыми над L. Имеем соотношение

$$\sum y_\alpha M_\alpha(x) = 0$$

между одночленами $M_\alpha(x)$ с коэффициентами y_α из L. Это—линейное соотношение между $M_\alpha(x)$. Но последние линейно независимы над k, так как иксы предполагаются алгебраически независимыми над k, — противоречие.

Предложение 3. *Пусть L — расширение поля k и $(u) = (u_1, \ldots, u_r)$ — множество алгебраически независимых величин над L. Тогда поле $k(u)$ линейно свободно от L над k.*

Доказательство. Согласно критериям линейной свободы, достаточно доказать, что элементы базиса кольца $k[u]$, которые линейно независимы над k, остаются линейно независимыми и над L. Но одночлены $M(u)$ дают базис $k[u]$ над k. Они должны остаться линейно независимыми над L, поскольку, как мы уже видели, линейное соотношение дает алгебраическое соотношение. Предложение доказано.

Отметим в заключение, что свойство двух расширений K и L поля k быть линейно свободными или алгебраически свободными является свойством конечного типа. Для доказательства того, что они обладают каким-либо из этих свойств, достаточно доказать это для всех подполей K_0 и L_0 в K и L соответственно, конечно порожденных над k. Это следует из того факта, что в определениях фигурирует только конечное число величин.

§ 6. Сепарабельные расширения

Пусть K — конечно порожденное расширение поля k, $K = k(x)$. Мы будем говорить, что оно *сепарабельно порождено*, если можно найти базис трансцендентности $(t_1, \ldots, t_r)$ поля K/k, такой, что K — сепарабельное алгебраическое расширение поля $k(t)$. Такой базис трансцендентности называется *сепарирующим базисом трансцендентности* для K над k.

Через p мы всегда будем обозначать характеристику поля, если она отлична от 0. Поле, получаемое из k присоединением корней p^m-й степени из всех элементов k, будет обозначаться через k^{1/p^m}. Композит всех этих полей по $m = 1, 2, \ldots$ обозначается символом k^{1/p^∞}.

Предложение 4. *Следующие условия, относящиеся к расширению K поля k, эквивалентны:*

(1) *K линейно свободно от k^{1/p^∞}.*

(2) *K линейно свободно от k^{1/p^m} для некоторого m.*

(3) *Всякое подполе поля K, содержащее k и конечно порожденное над k, сепарабельно порождено.*

Доказательство. Ясно, что (1) влечет (2). Чтобы доказать, что (2) влечет (3), мы можем, очевидно, предполагать, что K конечно порождено над k, скажем $K = k(x) = k(x_1, \ldots, x_n)$. Пусть степень трансцендентности этого расширения равна r. Если $r = n$, то доказательство закончено. В противном случае пусть $x_1, \ldots, x_r$ — базис трансцендентности. Тогда элемент x_{r+1} алгебраичен над $k(x_1, \ldots, x_r)$. Пусть $f(X_1, \ldots, X_{r+1})$ — многочлен наименьшей степени, для которого

$$f(x_1, \ldots, x_{r+1}) = 0.$$

Тогда f неприводим. Мы утверждаем, что не все x_i $(i = 1, \ldots, r+1)$ встречаются в нем обязательно в степени, кратной p. Если бы это было так, то мы могли бы написать $f(X) = \sum c_\alpha M_\alpha(X)^p$, где $M_\alpha(X)$ — одночлены от $X_1, \ldots, X_{r+1}$ и $c_\alpha \in k$. Это означало бы, что $M_\alpha(x)$ линейно зависимы над $k^{1/p}$ (извлечем корень p-й степени из уравнения $\sum c_\alpha M_\alpha(x)^p = 0$). Однако $M_\alpha(x)$ линейно независимы над k (иначе уравнение для $x_1, \ldots, x_{r+1}$ было бы меньшей степени) и мы, таким образом, получаем противоречие с линейной свободой $k(x)$ и $k^{1/p}$. Итак, скажем, X_1 встречается не только в степени, кратной p, в многочлене $f(X)$. Далее, $f(X)$ неприводим в $k[X_1, \ldots, X_{r+1}]$ и, следовательно, $f(X) = 0$ есть неприводимое уравнение для x_1 над $k(x_2, \ldots, x_{r+1})$. Так как X_1 встречается не только в степени, кратной p, то это уравнение есть сепарабельное уравнение для x_1 над $k(x_2, \ldots, x_{r+1})$, иными словами, x_1 — сепарабельный алгебраический элемент над $k(x_2, \ldots, x_n)$. Если $(x_2, \ldots, x_n)$ — базис трансцендентности, то доказательство закончено. Если нет, то, скажем x_2 сепарабелен над $k(x_3, \ldots, x_n)$. Тогда $k(x)$ сепарабельно над $k(x_3, \ldots, x_n)$. Рассуждая по индукции, мы видим, что этот процесс может быть продолжен до тех пор, пока не получится базис трансцендентности. Это доказывает, что (2) влечет (3). Это также доказывает, что сепарирующий базис трансцендентности для $k(x)$ над k может быть выбран из любого данного множества образующих. Для завершения доказательства достаточно, предполагая K конечно порожденным над k, убедиться в том, что (3) влечет (1). Пусть (u) — сепарирующий базис трансцендентности для K над k. Тогда K — сепарабельное алгебраическое расширение $k(u)$. В силу предложения 3 $k(u)$ и k^{1/p^∞} линейно свободны. Положим $L = k^{1/p^\infty}$. Тогда $k(u)L$ чисто несепарабельно над $k(u)$ в соответствии с элементарной теорией конечных алгебраических расширений и, следовательно, линейно свободно от K над $k(u)$. Используя предложение 1, заключаем, что K линейно свободно от L над k, что и доказывает наше предложение.

Расширение K поля k, удовлетворяющее условиям предложения 4, называется *сепарабельным*, что согласуется с использованием этого слова для алгебраических расширений.

Утверждение об эквивалентности первых двух условий нашего предложения известно как *критерий Маклейна*. Оно имеет следующие непосредственные следствия:

Следствие 1. *Если K сепарабельно над k и E — подполе в K, содержащее k, то E сепарабельно над k.*

Следствие 2. *Пусть E — сепарабельное расширение над k и K — сепарабельное расширение над E. Тогда K — сепарабельное расширение над k.*

Доказательство. Применить предложение 1 и определение сепарабельности.

Следствие 3. *Если поле k совершенно, то всякое расширение над k сепарабельно.*

Следствие 4. *Пусть K — сепарабельное расширение над k, алгебраически свободное от расширения L поля k. Тогда KL — сепарабельное расширение поля L.*

Доказательство. Всякий элемент из KL допускает представление в виде комбинации конечного числа элементов из K и L. Следовательно, любое конечно порожденное подполе в KL, содержащее L, содержится в композите FL, где F — некоторое подполе в K, конечно порожденное над k. В силу следствия 1 мы можем предполагать, что K конечно порождено над k. Пусть (t) — базис трансцендентности K над k, такой, что K — сепарабельное алгебраическое расширение поля $k(t)$. По предположению (t) есть базис трансцендентности KL над L, и так как всякий элемент из K является сепарабельным алгебраическим над $k(t)$, то он также сепарабелен над $L(t)$. Следовательно, KL сепарабельно порождено над L. Следствие доказано.

Следствие 5. *Пусть K и L — два сепарабельных расширения поля k, алгебраически свободные друг от друга над k. Тогда KL сепарабельно над k.*

Доказательство. Применить следствия 4 и 2.

Следствие 6. *Пусть K, L — два расширения поля k, линейно свободные над k. Тогда K сепарабельно над k в том и только в том случае, если KL сепарабельно над L.*

Доказательство. Если поле K не сепарабельно над k, то оно не линейно свободно от $k^{1/p}$ над k и тем более не линейно сво-

бодно от $Lk^{1/p}$ над k. Отсюда в силу предложения 1 вытекает, что KL не линейно свободно от $Lk^{1/p}$ над L и, следовательно, KL не сепарабельно над L. Обратное есть частный случай следствия 4, поскольку линейно свободные поля алгебраически свободны.

Мы завершим наше рассмотрение сепарабельности двумя результатами. Первый из них уже был получен в ходе доказательства первой части предложения 4, но мы сформулируем его здесь в явном виде.

Предложение 5. *Для конечно порожденного сепарабельного расширения K поля k сепарирующий базис трансцендентности может быть выбран из любого заданного множества образующих.*

Чтобы сформулировать второй результат, обозначим через K^{p^m} поле, получаемое возведением всех элементов поля K в p^m-ю степень.

Предложение 6. *Пусть K — конечно порожденное расширение поля k. Если $K^{p^m}k = K$ для некоторого m, то K — сепарабельное алгебраическое расширение поля k. Обратно, если K — сепарабельное алгебраическое расширение над k, то $K^{p^m}k = K$ для всех m.*

Доказательство. В случае когда K/k — конечное алгебраическое расширение, утверждение уже было доказано в элементарной теории конечных алгебраических расширений (гл. VII, § 7, следствие 4). Пусть K трансцендентно над k и $t_1, \ldots, t_r$ — базис трансцендентности. Тогда K есть конечное алгебраическое, но не сепарабельное расширение поля $k(t_1^p, \ldots, t_r^p)$, а потому $K \neq K^{p^m}k \times \times (t_1^p, \ldots, t_r^p) \supseteq K^{p^m}k$. Это доказывает наше предложение.

§ 7. Дифференцирования

Дифференцированием D кольца R называется отображение D: $R \to R$ кольца R в себя, линейное и удовлетворяющее обычным правилам для производных, т. е. $D(x+y) = Dx + Dy$ и $D(xy) = = xDy + yDx$. В качестве примера рассмотрим кольцо многочленов $k[X]$ над полем k. Для каждой переменной X_i взятие обычной частной производной $\partial/\partial X_i$ является дифференцированием в $k[X]$. Мы можем также очевидным образом получить дифференцирование в поле частных, а именно положив

$$D(u/v) = (v\,Du - u\,Dv)/v^2.$$

Мы будем работать с дифференцированиями поля K. Дифференцирование в K называется *тривиальным*, если $Dx = 0$ для всех $x \in K$. Оно называется *тривиальным на подполе* k в K, если $Dx = 0$ для всех $x \in k$. В этом случае говорят также, что D есть *дифференцирование поля K над k*. На простом поле дифференцирование всегда тривиально: имеем

$$D(1) = D(1 \cdot 1) = 2D(1), \text{ откуда } D(1) = 0.$$

Рассмотрим теперь задачу о продолжении дифференцирований. Пусть $L = K(x) = K(x_1, \ldots, x_n)$ — конечно порожденное расширение. Для $f \in K[X]$ обозначаем через $\partial f/\partial x_i$ многочлены $\partial f/\partial X_i$, вычисленные в (x). Когда существует дифференцирование D^* на L, совпадающее с заданным дифференцированием D на K? Если $f(X) \in K[X]$ — многочлен, обращающийся в нуль на множестве (x), то любое такое дифференцирование D^* должно удовлетворять соотношению

$$0 = D^* f(x) = f^D(x) + \sum (\partial f/\partial x_i) D^* x_i, \tag{1}$$

где f^D обозначает многочлен, получаемый применением D ко всем коэффициентам f. *Отметим, что если соотношение (1) выполняется* для всякого обращающегося в нуль на (x) элемента из конечного множества образующих идеала в $K[X]$, то (1) выполняется для всякого многочлена из этого идеала. Это непосредственное следствие из правил дифференцирования. Упомянутый идеал будет иногда называться идеалом в $K[X]$, определенным множеством (x).

Предыдущее необходимое условие для существования D^* оказывается также и достаточным.

Теорема 7. *Пусть D — дифференцирование поля K, (x) — произвольное множество величин и $\{f_\alpha(X)\}$ — множество образующих для идеала в $K[X]$, определенного множеством (x). Если тогда (u) — любое множество элементов из $K(x)$, удовлетворяющих уравнениям*

$$0 = f_\alpha^D(x) + \sum (\partial f_\alpha/\partial x_i) u_i,$$

то существует одно и только одно дифференцирование D^* поля $K(x)$, совпадающее с D на K и такое, что $D^* x_i = u_i$ для всякого i.

Доказательство. Необходимость была показана выше. Обратно, если $g(x)$, $h(x)$ лежат в $K[x]$ и $h(x) \neq 0$, то непосредственно проверяется, что отображение D^*, определенное формулами

$$D^* g(x) = g^D(x) + \sum \frac{\partial g}{\partial x_i} u_i,$$

$$D^*(g/h) = \frac{hD^* g - gD^* h}{h^2},$$

правильно определено и является дифференцированием поля $K(x)$.

Рассмотрим частный случай, когда (x) состоит из одного элемента x. Пусть D — заданное дифференцирование на K.

Случай 1. Элемент x — сепарабельный алгебраический над K. Пусть $f(X)$ — неприводимый многочлен, которому удовлетворяет x над K. Тогда $f'(x) \neq 0$. Имеем

$$0 = f^D(x) + f'(x)\,u,$$

откуда $u = -f^D(x)/f'(x)$. Следовательно, D продолжается на $K(x)$ однозначно Если D тривиально на K, то D тривиально и на $K(x)$.

Случай 2. Элемент x трансцендентен над K. Тогда D продолжается, причем элемент u может быть выбран в $K(x)$ произвольным образом.

Случай 3. Элемент x чисто несепарабелен над K, так что $x^{p^m} - a = 0$, где $a \in K$. Тогда D продолжается на $K(x)$ в том и только в том случае, если $D(a) = 0$. В частности, если D тривиально на K, то элемент u может быть выбран произвольным образом

Предложение 7. *Конечно порожденное расширение $K(x)$ над K тогда и только тогда является сепарабельным алгебраическим, когда всякое дифференцирование D поля $K(x)$, тривиальное на K, тривиально и на $K(x)$.*

Доказательство. Если $K(x)$ — сепарабельное алгебраическое расширение поля K, то это случай 1. Наоборот, если оно не является сепарабельным алгебраическим, то мы можем соорудить башню расширений между K и $K(x)$, каждый этаж которой относится к одному из трех рассмотренных выше случаев. По крайней мере один этаж будет относиться к случаю 2 или 3. Рассмотрев самый верхний этаж этого типа, мы тотчас увидим, как построить дифференцирование, тривиальное на основании и нетривиальное на вершине башни.

Предложение 8. *Пусть даны поле K и элементы $(x) = (x_1, \ldots, x_n)$ из некоторого его расширения, причем существуют n многочленов $f_i \in K[X]$, таких, что*

1) $f_i(x) = 0$ *и*

2) $\det(\partial f_i/\partial x_j) \neq 0$.

Тогда $K(x)$ — сепарабельное алгебраическое над K.

Доказательство. Пусть D — дифференцирование на $K(x)$, тривиальное на K. Поскольку $f_i(x) = 0$, мы должны иметь $Df_i(x) = 0$, откуда вытекает, что Dx_i удовлетворяют n линейным уравнениям, матрица из коэффициентов которых имеет ненулевой определитель. Следовательно, $Dx_i = 0$, так что D тривиально на $K(x)$. Поэтому $K(x)$ — сепарабельное алгебраическое над K.

Следующее предложение непосредственно вытекает из рассмотренного выше случая 3.

Предложение 9. *Пусть $K = k(x)$ — конечно порожденное расширение поля k. Элемент z из K тогда и только тогда лежит в $K^p k$, когда $Dz = 0$ для всякого дифференцирования D поля K над k.*

Доказательство. Если z лежит в $K^p k$, то, очевидно, всякое дифференцирование D поля K над k обращается в нуль на z. Обратно, если $z \notin K^p k$, то z чисто несепарабелен над $K^p k$ и, согласно рассмотренному выше случаю 3, мы можем найти дифференцирование D, тривиальное на $K^p k$ и такое, что $Dz = 1$. Это дифференцирование определено сначала только на поле $K^p k(z)$. Его можно продолжить на K следующим образом. Предположим, что имеется элемент $w \in K$, такой, что $w \notin K^p k(z)$. Тогда $w^p \in K^p k$ и D обращается в нуль на w^p. Мы можем снова применить случай 3, чтобы продолжить D с $K^p k(z)$ на $K^p k(z, w)$. Продвигаясь так шаг за шагом, мы в конце концов достигнем K и тем докажем наше предложение.

Дифференцирования поля K образуют векторное пространство над K, если определить zD для $z \in K$ формулой $(zD)(x) = zDx$.

Пусть K — конечно порожденное расширение поля k размерности r над k. Обозначим через $\mathfrak{D}$ K-векторное пространство дифференцирований поля K над k. Для всякого $z \in K$ имеем спаривание

$$(D, z) \longmapsto Dz$$

пространств $\mathfrak{D}$, K в K. Всякий элемент z поля K определяет, таким образом, K-линейный функционал на $\mathfrak{D}$. Этот функционал обозначается через dz. Имеем

$$d(yz) = y\,dz + z\,dy,$$
$$d(y + z) = dy + dz.$$

Эти линейные функционалы порождают дуальное к $\mathfrak{D}$ пространство $\mathfrak{F}$, если определить $y\,dz$ условием $(D, y dz) \longmapsto y\,Dz$.

Предложение 10. *Предположим, что K — конечно порожденное сепарабельное расширение поля k, имеющее степень трансцендентности r. Тогда векторное пространство $\mathfrak{D}$ (над K) дифференцирований поля K над k имеет размерность r. Элементы $t_1, \ldots, t_r$ поля K образуют сепарирующий базис трансцендентности для K над k в том и только в том случае, если $dt_1, \ldots, dt_r$ образуют базис дуального к $\mathfrak{D}$ пространства $\mathfrak{F}$ над K.*

Доказательство. Если $t_1, \ldots, t_r$ — сепарирующий базис трансцендентности для K над k, то, согласно случаям 1 и 2 теоремы

о продолжении, мы можем найти дифференцирования $D_1, \ldots, D_r$ поля K над k, для которых $D_i t_j = \delta_{ij}$. Для заданного $D \in \mathscr{D}$ положим $w_i = Dt_i$. Тогда ясно, что $D = \sum w_i D_i$, так что D_i образуют базис пространства $\mathscr{D}$ над K, а dt_i образуют дуальный базис. Обратно, если $dt_1, \ldots, dt_r$ образуют базис для $\mathscr{F}$ над K, а K не является сепарабельным алгебраическим над $k(t)$, то, согласно предложению 7, мы можем найти дифференцирование D, которое тривиально на $k(t)$, но нетривиально на K. Тогда $(D, dt_i) \mapsto Dt_i = 0$ для всех i, что противоречит тому факту, что $dt_1, \ldots, dt_r$ есть базис дуального пространства. Следовательно, K является сепарабельным алгебраическим над $k(t)$. Элементы $t_1, \ldots, t_r$ алгебраически независимы, так как в противном случае степень трансцендентности K над k была бы меньше r. Итак, $t_1, \ldots, t_r$ образуют сепарирующий базис для K над k.

Следствие. *Пусть K — конечно порожденное сепарабельное расширение поля k и z — элемент из K, трансцендентный над k. Тогда K сепарабельно над $k(z)$ в том и только в том случае, если существует дифференцирование D поля K над k, такое, что $Dz \neq 0$*

Доказательство. Если K сепарабельно над $k(z)$, то z допускает включение в сепарирующий базис для K над k, и мы можем применить предложение Если $Dz \neq 0$, то $dz \neq 0$ и мы можем включить dz в базис пространства $\mathscr{F}$ над K. Опять-таки из предложения вытекает, что K сепарабельно над $k(z)$.

УПРАЖНЕНИЯ

1. Доказать, что поле комплексных чисел имеет бесконечно много автоморфизмов [*Указание*: использовать базисы трансцендентности.]

2. Подполе k поля K называется алгебраически замкнутым в K, если всякий элемент из K, алгебраический над k, содержится в k Доказать: если k алгебраически замкнуто в K и K, L алгебраически свободны над k, причем либо L сепарабельно над k, либо K сепарабельно над k, то L алгебраически замкнуто в KL

3. Доказать эквивалентность следующих условий (они определяют понятие *регулярного расширения*):
(i) k алгебраически замкнуто в K и K сепарабельно над k.
(ii) K линейно свободно от $\overline{k}$ над k.

4. Доказать для регулярных расширений результаты, аналогичные тем, которые были доказаны выше для сепарабельных расширений.

5. Пусть $k \subset E \subset K$ — расширения полей. Показать, что

$$\text{Ст трансц } (K/k) = \text{Ст. трансц } (K/E) + \text{Ст трансц. } (E/k).$$

Если $\{x_i\}$ — базис трансцендентности для E/k и $\{y_i\}$ — базис трансцендентности для K/E, то $\{x_i, y_j\}$ будет базисом трансцендентности для K/k.

6. Пусть K/k — конечно порожденное расширение и E — подрасширение, $K \supset E \supset k$. Показать, что E/k конечно порождено.

7. Пусть k — поле характеристики 0, $z_1, \ldots, z_r$ — алгебраически независимые над k величины и (e_{ij}), $i = 1, \ldots, m$, $j = 1, \ldots, r$, $r \geqslant m$, — целочисленная матрица ранга m. Пусть, далее,

$$w_i = z_1^{e_{i1}} \ldots z_r^{e_{ir}} \text{ для } i = 1, \ldots, m$$

Показать, что $w_1, \ldots, w_m$ алгебраически независимы над k. [*Указание*: рассмотреть K-гомоморфизм

$$D \longmapsto (Dz_1/z_1, \ldots, Dz_r/z_r),$$

отображающий K-пространство дифференцирований поля K/k в $K^{(r)}$, и получить линейные условия на те дифференцирования D, которые обращаются в нуль на $k(w_1, \ldots, w_m)$.]

8. Пусть k, (z) обозначают то же, что в упражнении 7. Показать, что для всякой рациональной функции P

$$d(P(z)) = \operatorname{grad} P(z) \cdot dz,$$

здесь использованы векторные обозначения, т. е. $dz = (dz_1, \ldots, dz_r)$ и $\operatorname{grad} P = (\partial P/\partial z_1, \ldots, \partial P/\partial z_r)$. Определить $d \log P$ и выразить его в терминах координат. Показать, что для любых двух рациональных функций P, Q из $k(z)$

$$d \log (PQ) = d \log P + d \log Q.$$

Глава XI

Вещественные поля

§ 1. Упорядоченные поля

Пусть K — поле. *Упорядочение* поля K — это подмножество P в K, обладающее следующими свойствами:

ПОР 1. Для всякого данного элемента $x \in K$ либо $x \in P$, либо $x = 0$, либо $-x \in P$, и эти три возможности взаимно исключают друг друга. Иными словами, K есть объединение попарно не пересекающихся множеств P, $\{0\}$ и $-P$.

ПОР 2. Если x, $y \in P$, то $x + y \in P$ и $xy \in P$.

Мы будем также говорить, что K *упорядочено* посредством P, и называть P множеством *положительных* элементов.

Пусть K упорядочено посредством P. Так как $1 \neq 0$ и $1 = 1^2 = (-1)^2$, то $1 \in P$. В силу ПОР 2 имеем $1 + \ldots + 1 \in P$, откуда вытекает, что K имеет характеристику 0. Если $x \in P$, то из $xx^{-1} = 1 \in P$ вытекает, что $x^{-1} \in P$.

Пусть x, $y \in K$. По определению $x < y$ (или $y > x$) означает, что $y - x \in P$. Если $x < 0$, т. е. элемент $-x$ положительный, то мы говорим, что элемент x *отрицательный*. Тривиально проверяется, что имеют место обычные соотношения для неравенств, например,

$$x < y \text{ и } y < z \text{ влечет } x < z,$$
$$x < y \text{ и } z > 0 \text{ влечет } xz < yz,$$
$$x < y \text{ и } x, y > 0 \text{ влечет } 1/y < 1/x.$$

По определению $x \leqslant y$ означает, что $x < y$ или $x = y$. Если $x \leqslant y$ и $y \leqslant x$, то $x = y$.

Пусть K упорядочено. Для всякого $x \in K$, $x \neq 0$, элемент x^2 положителен, поскольку $x^2 = (-x)^2$ и либо $x \in P$, либо $-x \in P$. Таким образом, сумма квадратов положительна или равна 0.

Пусть E — поле. Тогда произведение сумм квадратов в E также будет суммой квадратов. Если a, $b \in E$ — суммы квадратов и $b \neq 0$, то a/b — сумма квадратов.

Первое утверждение очевидно, и второе — тоже, если принять во внимание равенство $a/b = ab\,(b^{-1})^2$.

Если E имеет характеристику $\neq 2$ и если -1 есть сумма квадратов, то всякий элемент $a \in E$ будет суммой квадратов, поскольку $4a = (1 + a)^2 - (1 - a)^2$.

Если K — поле с упорядочением P и F — подполе, то, очевидно, $P \cap F$ определяет упорядочение на F, называемое *индуцированным* упорядочением.

Отметим, что обе наши аксиомы ПОР 1 и ПОР 2 применимы и к кольцу. Если A — упорядоченное кольцо с $1 \neq 0$, то ясно, что A не может иметь делителей нуля и упорядочение кольца A можно очевидным образом продолжить на поле частных: дробь называется положительной, если она допускает запись в виде a/b, где a, $b \in A$ и a, $b > 0$. Тривиально проверяется, что тем самым действительно определено упорядочение на поле частных.

Пример. Определим упорядочение в кольце многочленов $\mathbf{R}[t]$ над полем вещественных чисел. Многочлен

$$f(t) = a_n t^n + \ldots + a_0$$

с $a_n \neq 0$ будем считать положительным, если $a_n > 0$. Обе аксиомы тривиально проверяются. Отметим, что $t > a$ для всех $a \in \mathbf{R}$. Таким образом, элемент t является бесконечно большим по отношению к $\mathbf{R}$. Существование бесконечно больших (или бесконечно малых) элементов в упорядоченном поле — это основная черта, которой такое поле может отличаться от подполя поля вещественных чисел.

Сделаем несколько замечаний относительно этого явления, т. е. существования бесконечно больших элементов.

Пусть K — упорядоченное поле и F — его подполе с индуцированным упорядочением. Как обычно, полагаем $|x| = x$, если $x > 0$, и $|x| = -x$, если $x < 0$. Мы будем говорить, что элемент α из K *бесконечно большой* над F, если $|\alpha| > x$ для всех $x \in F$. Мы будем говорить, что этот элемент *бесконечно малый* над F, если $0 \leqslant |\alpha| < |x|$ для всех $x \in F$, $x \neq 0$. Мы видим, что элемент α является бесконечно большим тогда и только тогда, когда элемент α^{-1} бесконечно малый. Мы будем говорить, что K *архимедово* над F, если в K нет элементов, бесконечно больших над F. Промежуточное поле F_1, $K \supset F_1 \supset F$, называется *максимальным архимедовым полем над* F, если оно архимедово над F и никакое другое промежуточное поле, содержащее F_1, не является архимедовым над F. Если F_1 архимедово над F и F_2 архимедово над F_1, то F_2 архимедово над F. Следовательно, по лемме Цорна всегда существует максимальное архимедово подполе F_1 в K над F. Мы будем говорить, что F — *максимальное архимедово подполе* в K, если оно является максимальным архимедовым полем над собой в K.

Пусть K — упорядоченное поле и F — его подполе. Обозначим через $\mathfrak{o}$ множество элементов из K, не являющихся бесконечно большими над F. Ясно, что $\mathfrak{o}$ — кольцо, причем для любого $\alpha \in K$ будет либо $\alpha \in \mathfrak{o}$, либо $\alpha^{-1} \in \mathfrak{o}$. Следовательно, $\mathfrak{o}$ является так называемым *кольцом нормирования*, содержащим F. Обозначим через $\mathfrak{m}$ идеал,

состоящий из всех $\alpha \in K$, бесконечно малых над F. Тогда $\mathfrak{m}$ — единственный максимальный идеал в $\mathfrak{o}$, поскольку любой элемент из $\mathfrak{o}$, не лежащий в $\mathfrak{m}$, имеет обратный в $\mathfrak{o}$. Мы будем называть $\mathfrak{o}$ *кольцом нормирования, определенным упорядочением расширения* K/F.

Предложение 1. *Пусть* K *— упорядоченное поле,* F *— его подполе,* $\mathfrak{o}$ *— кольцо нормирования, определенное упорядочением расширения* K/F, *и* $\mathfrak{m}$ *— его максимальный идеал. Тогда* $\mathfrak{o}/\mathfrak{m}$ *— вещественное поле* (см. § 2).

Доказательство. В противном случае мы имели бы равенство

$$-1 = \sum \alpha_i^2 + a,$$

где $\alpha_i \in \mathfrak{o}$ и $a \in \mathfrak{m}$. Но поскольку сумма $\sum \alpha_i^2$ положительна, а элемент a бесконечно мал, это равенство, очевидно, невозможно.

§ 2. Вещественные поля

Поле K называется *вещественным*, если -1 не является суммой квадратов в K [1]). Поле K называется *вещественно замкнутым*, если оно вещественное и любое его вещественное алгебраическое расширение совпадает с K. Другими словами, K является максимальным по отношению к свойству вещественности алгебраических замыканий.

Предложение 2. *Пусть* K *— вещественное поле.*

(i) *Если* $a \in K$, *то либо* $K(\sqrt{a})$, *либо* $K(\sqrt{-a})$ *— вещественное поле. Если* a *— сумма квадратов в* K, *то поле* $K(\sqrt{a})$ *вещественное. Если поле* $K(\sqrt{a})$ *не является вещественным, то* $-a$ *есть сумма квадратов в* K.

(ii) *Если* f *— неприводимый многочлен нечетной степени* n *из* $K[X]$ и α *— корень* f, *то поле* $K(\alpha)$ *вещественное.*

Доказательство. Пусть $a \in K$. Если a — квадрат в K, то поле $K(\sqrt{a}) = K$ и, следовательно, является вещественным по условию. Предположим, что a не есть квадрат в K. Если поле $K(\sqrt{a})$ не вещественное, то существуют b_i, $c_i \in K$, такие, что

$$-1 = \sum (b_i + c_i\sqrt{a})^2 = \sum (b_i^2 + 2c_ib_i\sqrt{a} + c_i^2 a).$$

---

[1]) Принято говорить в таком случае о *формально вещественном* поле, но мы сохраним краткую терминологию автора, поскольку из контекста ясно, когда речь идет об обычном поле вещественных чисел. — *Прим. ред.*

Так как $1, \sqrt{a}$ линейно независимы над K, то отсюда вытекает, что

$$-1 = \sum b_i^2 + a \sum c_i^2.$$

Если a — сумма квадратов в K, то получаем противоречие. Во всяком случае,

$$-a = \frac{1 + \sum b_i^2}{\sum c_i^2}$$

есть частное сумм квадратов и, значит, в силу сделанного выше замечания $-a$ является суммой квадратов. Следовательно, поле $K(\sqrt{-a})$ вещественное, что доказывает наше первое утверждение.

Что касается второго, то предположим, что $K(\alpha)$ не вещественное. Тогда мы можем записать

$$-1 = \sum g_i(\alpha)^2,$$

где многочлены g_i из $K[X]$ имеют степени $\leqslant n-1$. В $K[X]$ существует многочлен h, такой, что

$$-1 = \sum g_i(X)^2 + h(X) f(X).$$

Сумма $\sum g_i(X)^2$ имеет четную степень, и эта степень должна быть > 0, так как иначе -1 была бы суммой квадратов в K. Степень эта $\leqslant 2n-2$ Поскольку f имеет нечетную степень n, h имеет нечетную степень $\leqslant n-2$. Мы видим, что если β — корень h, то -1 есть сумма квадратов в $K(\beta)$. Так как $\deg h < \deg f$, то доказательство завершается по индукции.

Пусть K — вещественное поле. Под *вещественным замыканием* поля K мы будем понимать вещественно замкнутое поле L, алгебраическое над K.

Теорема 1. *Всякое вещественное поле K обладает вещественным замыканием. Вещественно замкнутое поле R имеет единственное упорядочение (а именно, положительные элементы в R — это суммы квадратов). Всякий положительный элемент в R является квадратом, и всякий многочлен нечетной степени из $R[X]$ имеет корень в R. Имеет место равенство $\overline{R} = R(\sqrt{-1})$*

Доказательство. В силу леммы Цорна наше поле K содержится в некотором вещественно замкнутом поле, алгебраическом над K. Пусть теперь R — вещественно замкнутое поле и P — множество ненулевых элементов из R, являющихся суммами квадратов. Тогда P замкнуто относительно сложения и умножения. В силу предложения 2 всякий элемент из P есть квадрат в R и для данного элемента $a \in R$, $a \neq 0$, будет либо $a \in P$, либо $-a \in P$. Таким образом, P определяет упорядочение. Опять-таки в силу предложения 2 всякий многочлен нечетной степени над R имеет корень в R. Наше последнее утверждение вытекает из примера 5 гл VIII, § 2.

Следствие. *Пусть K — вещественное поле и a — элемент из K, не являющийся суммой квадратов. Тогда существует упорядочение поля K, при котором элемент a отрицателен.*

Доказательство. В силу предложения 2 поле $K(\sqrt{-a})$ вещественно и, следовательно, имеет упорядочение как подполе своего вещественного замыкания. Относительно этого упорядочения $-a > 0$ и, значит, a отрицателен.

Предложение 3. *Пусть R — поле, такое, что $R \neq \bar{R}$ и $\bar{R} = R(\sqrt{-1})$. Тогда R вещественно и, следовательно, вещественно замкнуто.*

Доказательство. Пусть P — множество элементов из R, которые являются квадратами и $\neq 0$. Мы утверждаем, что P есть упорядочение поля R. Действительно, пусть $a \in R$, $a \neq 0$. Предположим, что a не является квадратом в R. Пусть α — корень уравнения $X^2 - a = 0$. Тогда $R(\alpha) = R(\sqrt{-1})$ и, следовательно, существуют c, $d \in R$, для которых $\alpha = c + d\sqrt{-1}$. В таком случае

$$\alpha^2 = c^2 + 2cd\sqrt{-1} - d^2.$$

Так как 1, $\sqrt{-1}$ линейно независимы над R, то $c = 0$ (поскольку $a \notin R^2$) и, следовательно, $-a$ есть квадрат.

Теперь докажем, что сумма квадратов будет квадратом. Для простоты положим $i = \sqrt{-1}$. Поскольку поле $R(i)$ алгебраически замкнуто, для данных a, $b \in R$ мы можем найти c, $d \in R$, такие, что $(c + di)^2 = a + bi$. Тогда $a = c^2 - d^2$ и $b = 2cd$. Следовательно, $a^2 + b^2 = (c^2 + d^2)^2$.

Если $a \in R$, $a \neq 0$, то одновременно a и $-a$ не могут быть квадратами в R. Таким образом, P — упорядочение, и наше предложение доказано.

Теорема 2. *Пусть R — вещественно замкнутое поле, a, $b \in R$ и $f(X)$ — многочлен из $R[X]$, причем $f(a) < 0$ и $f(b) > 0$. Тогда существует элемент c между a и b, для которого $f(c) = 0$.*

Доказательство. Так как поле $R(\sqrt{-1})$ алгебраически замкнуто, то f разлагается над R в произведение неприводимых множителей степеней 1 и 2. Если многочлен $X^2 + \alpha X + \beta$ неприводим (α, $\beta \in R$), то он является суммой квадратов, а именно

$$\left(X + \frac{\alpha}{2}\right)^2 + \left(\beta - \frac{\alpha^2}{4}\right),$$

так что $4\beta > \alpha^2$. Следовательно, изменение знака f происходит за счет изменения знака какого-то линейного множителя, который, как тривиально проверяется, должен иметь корень, лежащий между a и b.

Лемма. *Пусть K — подполе упорядоченного поля E и $\alpha \in E$ — алгебраический элемент над K, являющийся корнем многочлена*

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$$

с коэффициентами в K. Тогда $|\alpha| \leqslant 1 + |a_{n-1}| + \ldots + |a_0|$.

Доказательство. Если $|\alpha| \leqslant 1$, то утверждение очевидно. Если $|\alpha| > 1$, то выражаем $|\alpha|^n$ через члены меньшей степени, делим на $|\alpha|^{n-1}$ и получаем доказательство нашей леммы.

Отметим, что из этой леммы вытекает, что элемент, алгебраический над некоторым упорядоченным полем, не может быть бесконечно большим относительно этого поля.

Пусть $f(X)$ — многочлен с коэффициентами в вещественно замкнутом поле R, не имеющий кратных корней, и $u < v$ — элементы из R. Под *последовательностью Штурма* для f на интервале $[u, v]$ мы будем понимать упорядоченную систему многочленов

$$S = \{f = f_0, f' = f_1, \ldots, f_m\},$$

обладающую следующими свойствами:

ШТ 1. Последний многочлен f_m является отличной от нуля константой.

ШТ 2. Ни для какого $0 \leqslant j \leqslant m-1$ не существует точки $x \in [u, v]$, такой, что $f_j(x) = f_{j+1}(x) = 0$.

ШТ 3. Если $x \in [u, v]$ и $f_j(x) = 0$ для некоторого $j = 1, \ldots, m-1$, то $f_{j-1}(x)$ и $f_{j+1}(x)$ имеют противоположные знаки.

ШТ 4. Имеем $f_j(u) \neq 0$ и $f_j(v) \neq 0$ для всех $j = 0, \ldots, m$ [1].

Для любого элемента $x \in [u, v]$, не являющегося корнем ни для какого из многочленов f_j, мы будем обозначать через $W_S(x)$ число перемен знаков в последовательности

$$\{f(x), f_1(x), \ldots, f_m(x)\}$$

и будем называть $W_S(x)$ вариацией знаков в этой последовательности.

Теорема Штурма. *Число корней многочлена f, заключенных между u и v, равно разности $W_S(u) - W_S(v)$ для любой последовательности Штурма S.*

Доказательство. Заметим, что если $\alpha_1 < \alpha_2 < \ldots < \alpha_r$ — упорядоченная последовательность корней многочленов f_j в $[u, v]$

[1] Читатель заметит, что без специального выбора интервала $[u, v]$ выполнение этого условия при $j \neq 0$ не обеспечивается конструкцией системы. На самом деле его можно заменить условием возрастания произведения $f_0(x) f_1(x)$ при возрастании x в малой окрестности (относительно интервальной топологии) нуля α многочлена $f = f_0$. В определении вариации $W_S(\beta)$ нужно тогда потребовать $f(\beta) \neq 0$ и выбросить из последовательности $\{f_0(\beta), \ldots, f_m(\beta)\}$ нулевые члены. — *Прим. ред.*

($j = 0, \ldots, m-1$), то вариация $W_S(x)$ постоянна в открытых интервалах между этими корнями (в силу теоремы 2). Следовательно, достаточно доказать, что если имеется точно один элемент α, такой, что $u < \alpha < v$ и α есть корень некоторого f_j, то разность $W_S(u) - W_S(v)$ равна 1, когда α — корень f, и 0 в противном случае. Предположим сначала, что α — корень некоторого f_j для $1 \leqslant j \leqslant m-1$. Тогда согласно ШТ 3 элементы $f_{j-1}(\alpha)$, $f_{j+1}(\alpha)$ имеют противоположные знаки и эти знаки не изменяются при замене α на u или v. Следовательно, вариация знаков в последовательностях

$$\{f_{j-1}(u),\ f_j(u),\ f_{j+1}(u)\} \text{ и } \{f_{j-1}(v),\ f_j(v),\ f_{j+1}(v)\}$$

одна и та же, а именно равна 1. Таким образом, если α не является корнем f, то $W_S(u) = W_S(v)$. Если теперь α — корень f, то $f(u)$ и $f(v)$ имеют противоположные знаки, но $f'(u)$ и $f'(v)$ имеют один и тот же знак, а именно знак, совпадающий со знаком $f(v)$. Следовательно, в этом случае $W_S(u) = W_S(v) + 1$. Это доказывает нашу теорему.

Для многочлена без кратных корней последовательность Штурма строится без труда. Применяя алгоритм Евклида, получаем

$$\begin{aligned} f &= g_1 f' - f_2, \\ f_1 &= g_2 f_2 - f_3, \\ &\cdots\cdots\cdots \\ f_{m-2} &= g_{m-1} f_{m-1} - f_m, \end{aligned}$$

где $f' = f_1$. Так как f, f' не имеют общих множителей, то последний член в этой последовательности будет отличной от нуля константой. Тривиально проверяются и другие свойства последовательности Штурма. Если бы, например, два последовательных многочлена в этой последовательности имели общий нуль, то он был бы нулем и для всех остальных многочленов, вопреки тому факту, что последний из них в 0 не обращается.

Следствие. *Пусть K — упорядоченное поле, f — неприводимый многочлен над K степени $\geqslant 1$. Число корней f в двух вещественных замыканиях поля K, индуцирующих заданное упорядочение на K, одинаково.*

Доказательство. Используя лемму, мы можем взять в качестве v достаточно большой положительный и в качестве u достаточно большой отрицательный элементы в K, так чтобы все корни f и все корни многочленов в последовательности Штурма лежали между u и v. Тогда $W_S(u) - W_S(v)$ будет равно общему числу корней f в любом вещественном замыкании поля K, индуцирующем заданное упорядочение.

Теорема 3. *Пусть K — упорядоченное поле и R, R' — его вещественные замыкания, индуцирующие заданное упорядочение на K. Тогда существует однозначно определенный изоморфизм σ: $R \to R'$ над K, и этот изоморфизм сохраняет порядок.*

Доказательство. Мы покажем сперва, что для данного конечного подрасширения E в R над K существует вложение E в R' над K. Пусть $E = K(\alpha)$, и пусть $f(X) = \operatorname{Irr}(\alpha, K, X)$. Тогда $f(\alpha) = 0$ и следствие теоремы Штурма показывает, что f имеет некоторый корень β в R'. Таким образом, существует изоморфизм $K(\alpha)$ на $K(\beta)$ над K, отображающий α в β.

Пусть $\alpha_1, \ldots, \alpha_n$ — различные корни f в R и $\beta_1, \ldots, \beta_n$ — различные корни f в R', причем

$$\alpha_1 < \ldots < \alpha_n \text{ в упорядочении поля } R,$$
$$\beta_1 < \ldots < \beta_n \text{ в упорядочении поля } R'.$$

Мы утверждаем, что можно выбрать вложение σ поля $K(\alpha_1, \ldots, \alpha_n)$ в R' таким образом, что $\sigma\alpha_i = \beta_i$ для $i = 1, \ldots, n$. Действительно, пусть γ_i — такой элемент из R, что

$$\gamma_i^2 = \alpha_{i+1} - \alpha_i \text{ при } i = 1, \ldots, n-1,$$

и пусть $E_1 = K(\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{n-1})$. В силу только что доказанного существует вложение σ поля E_1 в R', а тогда $\sigma\alpha_{i+1} - \sigma\alpha_i$ есть квадрат в R'. Следовательно,

$$\sigma\alpha_1 < \ldots < \sigma\alpha_n.$$

Это доказывает, что $\sigma\alpha_i = \beta_i$ для $i = 1, \ldots, n$. Кроме того, последнее условие полностью определяет действие σ на $K(\alpha_1, \ldots, \alpha_n)$. Мы утверждаем, что σ сохраняет порядок. Действительно, пусть $y \in K(\alpha_1, \ldots, \alpha_n)$, $0 < y$ и элемент $\gamma \in R$ таков, что $\gamma^2 = y$. Тогда существует вложение поля $K(\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{n-1}, \gamma)$ в R' над K, которое индуцирует σ на $K(\alpha_1, \ldots, \alpha_n)$ и для которого σy есть квадрат, а, значит, как и утверждалось, $\sigma y > 0$.

Используя теперь лемму Цорна, мы, очевидно, получим изоморфизм R на R' над K. Этот изоморфизм сохраняет порядок, поскольку он отображает квадраты на квадраты. Тем самым теорема доказана.

Предложение 4. *Пусть K — упорядоченное поле, K' — его расширение, в котором нет соотношений вида*

$$-1 = \sum_{i=1}^{n} a_i \alpha_i^2$$

с $a_i \in K$, $a_i > 0$, и $\alpha_i \in K'$. Пусть L — поле, получаемое из K' присоединением квадратных корней из всех положительных элементов поля K. Тогда L вещественно.

Доказательство. Если—нет, то существует соотношение типа

$$-1=\sum_{i=1}^{n} a_i\alpha_i^2$$

с $a_i\in K$, $a_i>0$, и $\alpha_i\in L$. (Мы можем взять $a_i=1$.) Пусть r — наименьшее целое число, для которого мы можем записать указанное выше соотношение с α_i, лежащими в подполе поля L, имеющем вид

$$K'(\sqrt{b_1},\ \ldots,\ \sqrt{b_r}),$$

где $b_j\in K$, $b_j>0$. Если

$$\alpha_i=x_i+y_i\sqrt{b_r},$$

где

$$x_i,\ y_i\in K'(\sqrt{b_1},\ \ldots,\ \sqrt{b_{r-1}}),$$

то

$$-1=\sum a_i(x_i+y_i\sqrt{b_r})^2=\sum a_i\left(x_i^2+2x_iy_i\sqrt{b_r}+y_i^2b_r\right).$$

По предположению $\sqrt{b_r}$ не лежит в $K'(\sqrt{b_1},\ \ldots,\ \sqrt{b_{r-1}})$. Следовательно,

$$-1=\sum a_ix_i^2+\sum a_ib_ry_i^2,$$

вопреки минимальности r.

Теорема 4. *У всякого упорядоченного поля K существует вещественное замыкание R, индуцирующее заданное упорядочение на K.*

Доказательство. Возьмем $K'=K$ в предложении 4. Тогда L вещественно и содержится в некотором вещественном замыкании. Наше утверждение теперь очевидно.

Следствие. *Пусть K — упорядоченное поле и K' — его расширение. Для того чтобы существовало упорядочение на K', индуцирующее заданное упорядочение поля K, необходимо и достаточно, чтобы отсутствовали соотношения типа*

$$-1=\sum_{i=1}^{n} a_i\alpha_i^2,$$

где $a_i\in K$, $a_i>0$ и $\alpha_i\in K'$.

Доказательство. Если нет таких соотношений, то, согласно предложению 4, L вещественно и, значит, содержится в некотором вещественном замыкании, упорядочение которого индуцирует некоторое упорядочение на K' и заданное упорядочение на K, что и требовалось. Обратное очевидно.

Пример. Пусть $\overline{\mathbf{Q}}$ — поле алгебраических чисел. Непосредственно видно, что $\mathbf{Q}$ допускает только одно упорядочение, а именно обычное. Следовательно, любые два вещественных замыкания поля $\mathbf{Q}$ в $\overline{\mathbf{Q}}$ изоморфны, причем соответствующий изоморфизм однозначно определен. Вещественные замыкания поля $\mathbf{Q}$ в $\overline{\mathbf{Q}}$ исчерпываются в точности подполями в $\overline{\mathbf{Q}}$, над которыми $\overline{\mathbf{Q}}$ имеет конечную степень. Пусть K — конечное вещественное расширение поля $\mathbf{Q}$, содержащееся в $\overline{\mathbf{Q}}$, Элемент α из K тогда и только тогда будет суммой квадратов в K, когда положителен всякий элемент, сопряженный с α в поле вещественных чисел, или, что эквивалентно, в одном из вещественных замыканий поля $\mathbf{Q}$ в $\overline{\mathbf{Q}}$.

Замечание. Теория, развитая в этом и предыдущем параграфах, принадлежит Артину — Шрейеру.

§ 3. Вещественные нули и гомоморфизмы

Подобно тому как мы развили теорию продолжения гомоморфизмов в алгебраически замкнутое поле и получили теорему Гильберта о нулях в алгебраически замкнутом поле, мы хотим теперь развить теорию для случая, когда принимаемые значения лежат в вещественно замкнутом поле. Одной из основных теорем будет следующая:

Теорема 5. *Пусть k — поле, $K = k(x_1, \ldots, x_n)$ — конечно порожденное расширение. Предположим, что k упорядочено. Пусть R_k — вещественное замыкание поля k, индуцирующее то же самое упорядочение на k, что и K. Тогда существует гомоморфизм*

$$\varphi\colon k[x_1, \ldots, x_n] \to R_k$$

над k.

В качестве приложений теоремы 5 получаем

Следствие 1. *Пусть обозначения те же, что и в теореме, и пусть $y_1, \ldots, y_m \in k[x]$, причем*

$$y_1 < y_2 < \ldots < y_m$$

в заданном упорядочении поля K. Тогда гомоморфизм φ можно выбрать таким образом, что

$$\varphi y_1 < \ldots < \varphi y_m.$$

Доказательство. Пусть $\gamma_i^2 = y_{i+1} - y_i$, где $\gamma_i \in \overline{K}$. Тогда поле $K(\gamma_1, \ldots, \gamma_{m-1})$ обладает упорядочением, индуцирующим заданное упорядочение на K. Применяем теорему к кольцу

$$k\left[x_1, \ldots, x_n, \gamma_1^{-1}, \ldots, \gamma_{m-1}^{-1}, \gamma_1, \ldots, \gamma_{m-1}\right].$$

Следствие 2 (Артин). *Пусть k — вещественное поле, допускающее только одно упорядочение, и это упорядочение архимедово. Пусть $f(X_1, \ldots, X_n) \in k(X)$ — рациональная функция, не принимающая отрицательных значений: $f(a) \geqslant 0$ для всех $(a) = (a_1, \ldots, a_n) \in k^{(n)}$, в которых $f(a)$ определено. Тогда $f(X)$ есть сумма квадратов в $k(X)$.*

Доказательство. Предположим, что утверждение не верно. В силу следствия теоремы 1 § 2 существует упорядочение $k(X)$, при котором f отрицательна. Применим следствие 1 к кольцу

$$k\left[X_1, \ldots, X_n, h(X)^{-1}\right],$$

где $h(X)$ — знаменатель $f(X)$. Мы можем найти гомоморфизм φ этого кольца в R_k (тождественный на k), такой, что $\varphi(f) < 0$. Но $\varphi(f) = f(\varphi X_1, \ldots, \varphi X_n)$. Так как в R_k нет бесконечно малых элементов относительно k, то найдутся элементы $a_i \in k$ $(i = 1, \ldots, n)$, близкие к φX_i, и в силу непрерывности $f(a_1, \ldots, a_n) < 0$, — противоречие.

Следствие 2 было проблемой Гильберта. Доказательство теоремы 5, которое мы приведем, отличается от артиновского доказательства этого следствия рядом технических моментов.

Сначала мы покажем, как можно свести теорему 5 к случаю, когда K имеет степень трансцендентности 1 над k, причем k вещественно замкнуто.

Лемма 1. *Пусть R — вещественно замкнутое поле и R_0 — подполе, алгебраически замкнутое в R (т. е. такое, что всякий элемент из R, не лежащий в R_0, трансцендентен над R_0). Тогда R_0 вещественно замкнуто.*

Доказательство. Пусть $f(X)$ — неприводимый многочлен над R_0. Он разлагается в R на линейные и квадратные множители. Их коэффициенты лежат в R, алгебраичны над R_0 и, следовательно, лежат в R_0. Таким образом, сам $f(X)$ либо линеен, либо является неприводимым квадратным трехчленом над R_0. В силу теоремы о промежуточном значении мы можем во втором случае предполагать, что f положительно определен, т. е. $f(a) > 0$ для всех $a \in R_0$. Не теряя общности, мы можем считать, что $f(X) = X^2 + b^2$ для некоторого $b \in R_0$. Любой корень этого многочлена приносит с собой $\sqrt{-1}$, а потому единственным алгебраическим расширением R_0 является $R_0(\sqrt{-1})$. Это доказывает, что R_0 вещественно замкнуто.

Обозначим через R_K вещественное замыкание поля K, индуцирующее заданный порядок на K, и через R_0—алгебраическое замыкание k в R_K. В силу леммы 1 R_0 вещественно замкнуто.

Рассмотрим поле $R_0(x_1, \ldots, x_n)$. Если мы сможем доказать нашу теорему для кольца $R_0[x_1, \ldots, x_n]$ и найдем гомоморфизм

$$\psi\colon R_0[x_1, \ldots, x_n] \to R_0,$$

то, рассмотрев изоморфизм $\sigma\colon R_0 \to R_K$ над k (существующий согласно теореме 3) и положив $\varphi = \sigma \circ \psi$, мы получим решение нашей задачи над k. Тем самым теорема сводится к случаю, когда k вещественно замкнуто.

Пусть теперь F — промежуточное поле, $K \supset F \supset k$, над которым K имеет степень трансцендентности 1. Обозначим через R_F вещественное замыкание F, содержащееся в R_K. Если наша теорема верна для расширений размерности 1, то мы можем найти гомоморфизм

$$\psi\colon R_F[x_1, \ldots, x_n] \to R_F.$$

Заметим, что поле $k(\psi x_1, \ldots, \psi x_n)$ имеет степень трансцендентности $\leqslant n-1$ и вещественно, так как содержится в R_F. Таким образом, по индукции теорема сводится к случаю, когда K имеет размерность 1 и k, как мы видели выше, вещественно замкнуто.

Наше утверждение геометрически интерпретируется следующим образом. Можно считать, что $K = R(x, y)$, где x трансцендентен над R и (x, y) — корень некоторого неприводимого многочлена $f(X, Y)$ из $R[X, Y]$, и мы хотим по существу доказать, что имеется бесконечно много точек на кривой $f(X, Y) = 0$ с координатами, лежащими в R, т. е. бесконечно много вещественных точек.

Основная идея состоит в том, чтобы найти некоторую точку $(a, b) \in R^{(2)}$, такую, что $f(a, b) = 0$, но $D_2 f(a, b) \neq 0$. Тогда мы сможем применить теорему о промежуточном значении. Очевидно, $f(a, b+h)$ меняет знак, когда малое положительное h заменяется на малый отрицательный элемент из R. Если взять элемент $a' \in R$, близкий к a, то $f(a', b+h)$ также будет менять знак для малых h и, следовательно, $f(a', Y)$ имеет нуль в R для всех a', достаточно близких к a. Этим путем мы получим бесконечно много нулей.

Чтобы найти нашу точку, рассмотрим $f(x, Y)$ как многочлен от одной переменной Y с коэффициентами в $R(x)$. При этом, не теряя общности, мы можем считать, что старший коэффициент равен 1. Построим последовательность Штурма для этого многочлена, скажем

$$\{f(x, Y), f_1(x, Y), \ldots, f_m(x, Y)\}.$$

Положим $d = \deg f$ и обозначим через $A(x) = (a_{d-1}(x), \ldots, a_0(x))$ коэффициенты $f(x, Y)$. Из алгоритма Евклида видно, что коэффи-

циенты многочленов в последовательности Штурма могут быть выражены в виде рациональных функций

$$\{G_v(A(x))\}$$

от $a_{d-1}(x), \ldots, a_0(x)$.

Пусть

$$v(x) = 1 \pm a_{d-1}(x) \pm \ldots \pm a_0(x) + s,$$

где s — некоторое положительное целое число, а знаки выбраны таким образом, чтобы каждый член в этой сумме давал положительный вклад. Положим $u(x) = -v(x)$ и выберем s так, чтобы ни u, ни v не были корнями никакого многочлена в последовательности Штурма для f. Для дальнейшего нам потребуется лемма.

Лемма 2. *Пусть R — вещественно замкнутое поле и $\{h_i(x)\}$ — конечное множество рациональных функций от одной переменной с коэффициентами в R. Предположим, что поле рациональных функций $R(x)$ каким-то образом упорядочено, так что каждой функции $h_i(x)$ приписан некоторый знак. Тогда имеется бесконечно много таких значений a переменной x в R, что при любом i величина $h_i(a)$ определена и имеет тот же знак, что и $h_i(x)$.*

Доказательство. Рассматривая по отдельности числители и знаменатели наших рациональных функций, мы можем без потери общности предполагать, что h_i — многочлены. Тогда

$$h_i(x) = c \prod (x - \lambda) \prod p(x),$$

где первое произведение берется по всем корням λ многочлена h_i, а второе — по положительно определенным квадратичным множителям над R. Для любого $\xi \in R$ величина $p(\xi)$ положительна. Достаточно поэтому показать, что для всех λ могут быть сохранены знаки $(x-\lambda)$ при подстановке вместо x бесконечного множества значений a. Упорядочив все значения λ и x, получим

$$\ldots < \lambda_1 < x < \lambda_2 < \ldots,$$

где, возможно, λ_1 или λ_2 должно быть опущено, если x меньше или больше, чем любое λ. Произвольное значение a для x в R, выбранное между λ_1 и λ_2, будет удовлетворять требованиям нашей леммы.

Чтобы применить лемму к доказательству существования нашей точки, возьмем множество рациональных функций $\{h_i(x)\}$, состоящее из всех коэффициентов $a_{d-1}(x), \ldots, a_0(x)$, всех рациональных функций $G_v(A(x))$ и всех функций $f_j(x, u(x))$, $f_j(x, v(x))$, вариация знаков которых удовлетворяет теореме Штурма. Мы найдем бесконечно много значений a переменной x в R, которые сохраняют знаки этих рациональных функций. Тогда многочлены $f(a, Y)$ имеют корни

в R и для всех, кроме конечного числа, значений a эти корни будут кратности 1.

Теперь уже дело простой техники показать, что для всех, кроме конечного числа, точек на кривой элементы $x_1, \ldots, x_n$ лежат в локальном кольце гомоморфизма $R[x, y] \to R$, переводящего (x, y) в точку (a, b), для которой $f(a, b) = 0$, но $D_2 f(a, b) \neq 0$ (см. пример в конце § 4 гл. XII и упражнение 12 той же главы). Можно было бы дать здесь и непосредственное доказательство. Таким образом, мы получаем гомоморфизм

$$R[x_1, \ldots, x_n] \to R,$$

что и доказывает теорему 5.

Теорема 5 допускает обращение.

Теорема 6. *Пусть k — вещественное поле, $K = k(x_1, \ldots, x_n, y) = k(x, y)$ — его конечно порожденное расширение, такое, что элементы $x_1, \ldots, x_n$ алгебраически независимы над k, а y алгебраичен над $k(x)$. Пусть $f(X, Y)$ — неприводимый многочлен из $k[X, Y]$, для которого $f(x, y) = 0$. Пусть, далее, R — вещественно замкнутое поле, содержащее k, причем существует набор $(a, b) \in R^{(n+1)}$, такой, что $f(a, b) = 0$, но $D_{n+1} f(a, b) \neq 0$. Тогда поле K вещественное.*

Доказательство. Пусть $t_1, \ldots, t_n$ алгебраически независимы над R. По индукции мы можем упорядочить $R(t_1, \ldots, t_n)$ таким образом, чтобы каждый t_i был бесконечно малым относительно R (см. пример из § 1). Пусть R' — вещественное замыкание поля $R(t_1, \ldots, t_n)$, сохраняющее упорядочение. Положим $u_i = a_i + t_i$ для $i = 1, \ldots, n$. Тогда $f(u, b + h)$ при малых положительных и отрицательных значениях h из R имеет разные знаки и, следовательно, $f(u, Y)$ имеет в R' корень, скажем v. Так как многочлен f неприводим, то изоморфизм $k(x)$ на $k(u)$, переводящий x_i в u_i, продолжается до вложения $k(x, y)$ в R' и, следовательно, поле K вещественно, что и требовалось показать.

На языке алгебраической геометрии теоремы 5 и 6 утверждают, что поле функций многообразия над вещественным полем k тогда и только тогда вещественно, когда многообразие имеет простую точку в некотором вещественном замыкании поля k.

На тех же идеях основано доказательство следующей теоремы.

Теорема 7. *Пусть k — поле и K — его конечно порожденное расширение, причем K упорядочено. Пусть R — вещественно замкнутое поле, содержащее k и индуцирующее то же самое упорядочение на k, что и K. Предположим, что степень трансцендентности R над k не меньше, чем степень трансцендентности K над k. Тогда существует вложение K в R над k.*

Мы предоставим доказательство читателю в качестве упражнения. Используя прием с извлечением квадратных корней, можно всегда выбрать указанное вложение так, чтобы сохранить конечное число неравенств в заданном упорядочении поля K.

УПРАЖНЕНИЯ

1. Показать на примере, что следствие 2 § 3 перестает быть верным, если упорядочение поля k не предполагать архимедовым (в чем дело?). [*Указание* (Dubois D. W., *Notices Amer. Math. Soc.*, 1967. 14, № 3, 67T — 288). Пусть $\mathbf{Q}$ — поле рациональных чисел, t — переменная; на $\mathbf{Q}(t)$ вводится упорядочение, относительно которого $0 < t$ — бесконечно малая величина. Пусть K — вещественное замыкание поля $\mathbf{Q}(t)$ и $k = \bigcap k_i$, где каждое k_i — промежуточное поле, $Q(t) \subseteq k_i \subseteq K$, не допускающее квадратичного расширения в K. Положить $f(X) = (X^3 - t)^2 - t^3$]. [1])

2. Пусть α алгебраично над $\mathbf{Q}$ и $\mathbf{Q}(\alpha)$ — вещественное поле. Доказать, что α будет суммой квадратов в $\mathbf{Q}(\alpha)$ тогда и только тогда, когда $\sigma\alpha > 0$ для всякого вложения σ поля $\mathbf{Q}(\alpha)$ в $\mathbf{R}$.

3. Пусть F — конечное расширение поля $\mathbf{Q}$ и φ: $F \to \mathbf{Q}$ — $\mathbf{Q}$-линейный функционал, такой, что $\varphi(x^2) > 0$ для всех $x \in F$, $x \neq 0$. Пусть $\alpha \in F$, $\alpha \neq 0$. Показать, что если $\varphi(\alpha x^2) \geqslant 0$ для всех $x \in F$, то α является суммой квадратов в F и F чисто вещественно, т. е. всякое вложение F в поле комплексных чисел содержится в поле вещественных чисел. [*Указание*: использовать тот факт, что след дает отождествление F с его дуальным пространством над $\mathbf{Q}$, и применить аппроксимационную теорему из гл. XII, § 1.]

4. Прочитать формулировки результатов в статье „Теория вещественных точек“ (Lang S., The theory of real places, *Ann. Math.*, 1953, 378—391) и доказать эти результаты, не заглядывая в доказательства, данные в статье.

5. Пусть $\alpha \leqslant t \leqslant \beta$ — вещественный интервал и $f(t)$ — вещественный многочлен, положительный на этом интервале. Показать, что $f(t)$ может быть записан в виде

$$\sum Q_\nu^2 + \sum (t - \alpha) Q_\mu^2 + \sum (\beta - t) Q_\lambda^2,$$

где Q^2 обозначает квадрат. [*Указание*: разложить многочлен и использовать тождество

$$(t - \alpha)(\beta - t) = \frac{(t - \alpha)^2 (\beta - t) + (t - \alpha)(\beta - t)^2}{\beta - \alpha}.]$$

6. Показать, что поле вещественных чисел имеет только тождественный автоморфизм. [*Указание*: показать, что автоморфизм сохраняет упорядочение.]

---

[1]) Добавлено при переводе. Место этого упражнения было занято утверждением, совпадающим с леммой из § 2 и не исключенным лишь по недосмотру. — *Прим. ред.*

Глава XII

Абсолютные значения

§ 1. Определения, зависимость и независимость

Пусть K — поле. *Абсолютное значение* v на K — это вещественнозначная функция $x \mapsto |x|_v$ на K, удовлетворяющая следующим трем условиям:

АЗ 1. $|x|_v \geqslant 0$ для всех $x \in K$, и $|x|_v = 0$ тогда и только тогда, когда $x = 0$.

АЗ 2. $|xy|_v = |x|_v |y|_v$ для всех $x, y \in K$.

АЗ 3. $|x+y|_v \leqslant |x|_v + |y|_v$ для всех $x, y \in K$.

Если вместо АЗ 3 абсолютное значение удовлетворяет более сильному условию

АЗ 4. $|x+y|_v \leqslant \max(|x|_v, |y|_v)$,

то мы будем говорить, что оно является *нормированием* или что оно *неархимедово*. Абсолютное значение, для которого $|x|_v = 1$ при всех $x \neq 0$, называется *тривиальным*.

Имея дело с одним фиксированным абсолютным значением, мы будем писать $|x|$ вместо $|x|_v$ и говорить о $|\ |$ как об абсолютном значении.

Абсолютное значение на K определяет метрику. Расстояние между двумя элементами x, y из K в этой метрике равно $|x-y|$. Таким образом, абсолютное значение определяет топологию на K. Два абсолютных значения называются *зависимыми*, если они определяют одну и ту же топологию. В противном случае они называются *независимыми*.

Отметим, что $|1| = |1|^2 = |(-1)^2| = |1|^2$, откуда

$$|1| = |-1| = 1.$$

Кроме того, $|-x| = |x|$ для всех $x \in K$ и $|x^{-1}| = |x|^{-1}$ для $x \neq 0$.

Предложение 1. *Пусть* $|\ |_1$ *и* $|\ |_2$ *— нетривиальные абсолютные значения на поле* K. *Тогда для их зависимости необходимо и достаточно, чтобы из соотношения*

$$|x|_1 < 1$$

следовало $|x|_2 < 1$. *Если они зависимы, то существует число* $\lambda > 0$, *такое, что* $|x|_1 = |x|_2^{\lambda}$ *для всех* $x \in K$.

Доказательство. Если два абсолютных значения зависимы, то наше условие выполняется, поскольку множество тех $x \in K$, для которых $|x|_1 < 1$, совпадает с множеством тех x, для которых $\lim x^n = 0$ при $n \to \infty$. Обратно, предположим, что условие теоремы выполняется. Тогда из $|x|_1 > 1$ следует $|x|_2 > 1$, поскольку $|x^{-1}|_1 < 1$. По предположению существует элемент $x_0 \in K$, для которого $|x_0|_1 > 1$. Пусть $a = |x_0|_1$ и $b = |x_0|_2$. Положим

$$\lambda = \frac{\log b}{\log a}.$$

Пусть $x \in K$, $x \neq 0$. Тогда $|x|_1 = |x_0|_1^{\alpha}$ для некоторого числа α. Если m, n — такие целые числа, что $m/n > \alpha$, причем $n > 0$, то

$$|x|_1 < |x_0|_1^{m/n},$$

откуда

$$|x^n/x_0^m|_1 < 1$$

и, значит,

$$|x^n/x_0^m|_1 < 1.$$

Отсюда вытекает, что $|x|_2 < |x_0|_2^{m/n}$. Следовательно,

$$|x|_2 \leqslant |x_0|_2^{\alpha}.$$

Аналогично доказывается обратное неравенство и, таким образом, получаем

$$|x|_2 = |x_0|_2^{\alpha}$$

для всех $x \in K$, $x \neq 0$. Утверждение, что $|x|_2 = |x|_1^{\lambda}$, теперь очевидно.

Дадим несколько примеров абсолютных значений.

Рассмотрим сначала поле рациональных чисел. Имеем прежде всего обычное абсолютное значение, а именно $|m| = m$ для любого положительного целого числа m.

Для всякого простого числа p имеем *p-адическое абсолютное значение* v_p, определяемое формулой

$$|p^r m/n|_p = 1/p^r,$$

где r — целое число, а m, n — целые числа $\neq 0$, не делящиеся на p. Непосредственно видно, что p-адическое абсолютное значение неархимедово.

Аналогичное определение нормирования можно дать для любого поля K, являющегося полем частных кольца главных идеалов. Пусть, например, $K = k(t)$, где k — некоторое поле и t — переменная над k. Для всякого неприводимого многочлена $p(t)$ из $k[t]$ имеем нормирование v_p, определяемое так же, как в поле рациональных чисел, но

с тем отличием, что здесь нет естественного способа его нормализовать. Поэтому выбираем число c, такое, что $0 < c < 1$, и для любой рациональной функции $p^r f/g$, где f, g — многочлены, не делящиеся на p, полагаем

$$|p^r f/g|_p = c^r.$$

Разные значения постоянной c приводят к зависимым нормированиям.

Всякое подполе поля комплексных чисел (или вещественных чисел) обладает абсолютным значением, индуцированным обычным абсолютным значением в поле комплексных чисел. Позднее мы увидим, как можно получать абсолютные значения на некоторых полях, вкладывая их в другие поля, которые уже снабжены естественными абсолютными значениями.

Предположим, что определенное на некотором поле абсолютное значение ограничено на простом кольце (т. е. кольце целых чисел $\mathbf{Z}$, *если характеристика равна* 0, *и кольце целых чисел* $\bmod p$, *если характеристика равна* p). *Тогда это абсолютное значение непременно неархимедово.*

Доказательство. Для любых элементов x, y и любого положительного целого числа n имеем

$$|(x+y)^n| \leqslant \sum \left| \binom{n}{\nu} x^\nu y^{n-\nu} \right| \leqslant (n+1)\, C\, (\max(|x|, |y|))^n.$$

Извлекая из обеих частей корни n-й степени и устремляя n к бесконечности, получаем доказательство нашего утверждения. Отметим, что предпосылка утверждения всегда выполнена в случае характеристики > 0, поскольку в этом случае простое кольцо конечно!

Мы отсылаем читателя к любой другой книге, где рассматриваются абсолютные значения, за доказательством того факта, что всякое архимедово абсолютное значение на поле рациональных чисел зависит от обычного абсолютного значения. Этот факт по существу бесполезен (и нигде не используется в дальнейшем), так как мы всегда исходим из конкретно заданного множества абсолютных значений на интересующем нас поле.

В предложении 1 мы получили сильное условие, которому должны удовлетворять зависимые абсолютные значения. Теперь мы получим условие, которому удовлетворяют независимые абсолютные значения.

Аппроксимационная теорема (Артин—Уэплз). *Пусть* K — *поле и* $|\ |_1, \ldots, |\ |_s$ — *нетривиальные попарно независимые абсолютные значения на* K. *Пусть* $x_1, \ldots, x_s$ — *элементы из* K *и* $\varepsilon > 0$. *Тогда существует элемент* $x \in K$, *такой, что*

$$|x - x_i|_i < \varepsilon$$

для всех i.

Доказательство. Рассмотрим сначала два из наших абсолютных значений, скажем v_1 и v_s. По условию мы можем найти элемент $\alpha \in K$, такой, что $|\alpha|_1 < 1$ и $|\alpha|_s \geqslant 1$. Аналогично мы можем найти элемент $\beta \in K$, такой, что $|\beta|_1 \geqslant 1$ и $|\beta|_s < 1$. Положим $y = \beta/\alpha$. Тогда $|y|_1 > 1$ и $|y|_s < 1$.

Теперь докажем, что существует элемент $z \in K$, такой, что $|z|_1 > 1$ и $|z|_j < 1$ для $j = 2, \ldots, s$. Доказываем это по индукции. Случай $s = 2$ был только что рассмотрен. Предположим, что мы нашли элемент $z \in K$, удовлетворяющий условиям

$$|z|_1 > 1 \text{ и } |z|_j < 1 \quad \text{для} \quad j = 2, \ldots, s-1.$$

Если $|z|_s \leqslant 1$, то элемент $z^n y$ для достаточно большого n будет удовлетворять нашим требованиям.

Если $|z|_s > 1$, то последовательность

$$t_n = \frac{z^n}{1+z^n}$$

стремится к 1 относительно v_1 и v_s и стремится к 0 относительно v_j $(j = 2, \ldots, s-1)$. Ясно, что при достаточно большом n элемент $t_n y$ удовлетворяет нашим требованиям.

Используя только что построенный элемент z, мы видим, что последовательность $z^n/(1+z^n)$ стремится к 1 относительно v_1 и к 0 относительно v_j для $j = 2, \ldots, s$. Поэтому для всякого i мы можем построить элемент z_i, который очень близок к 1 относительно v_i и очень близок к 0 относительно v_j $(j \neq i)$. Тогда элемент

$$x = z_1 x_1 + \ldots + z_s x_s$$

удовлетворяет требованиям теоремы.

§ 2. Пополнения

Пусть K — поле с нетривиальным абсолютным значением v, которое во всем этом параграфе будет оставаться фиксированным. Обычным способом можно определить понятие *последовательности Коши*. Это такая последовательность $\{x_n\}$ элементов из K, что для заданного $\varepsilon > 0$ существует целое число N, такое, что для всех n, $m > N$ имеем

$$|x_n - x_m| < \varepsilon.$$

Мы будем говорить, что поле K *полное*, если всякая последовательность Коши сходится.

Предложение 2. *Существует пара* (K_v, i), *состоящая из поля* K_v, *полного относительно некоторого абсолютного значения*,

и вложения $i\colon K \to K_v$, *такого, что абсолютное значение на* K *индуцируется абсолютным значением на* K_v (*т. е.* $|x|_v = |ix|$ *для* $x \in K$). *При этом* iK *плотно в* K_v. *Если* (K'_v, i') — *другая такая пара, то существует однозначно определенный изоморфизм* $\varphi\colon K_v \to K'_v$, *сохраняющий абсолютные значения, для которого коммутативна следующая диаграмма*:

$$\begin{array}{ccc} K_v & \xrightarrow{\varphi} & K'_v \\ & {\scriptstyle i}\nwarrow \quad \nearrow{\scriptstyle i'} & \\ & K & \end{array}$$

Доказательство. Единственность очевидна. Существование доказывается хорошо известным способом, который мы сейчас кратко напомним, предоставив детали читателю.

Последовательности Коши образуют кольцо, сложение и умножение в котором производятся покомпонентно.

Определяется нуль-последовательность как последовательность $\{x_n\}$, для которой $\lim\limits_{n\to\infty} x_n = 0$. Нуль-последовательности образуют идеал в кольце последовательностей Коши, который на самом деле является максимальным идеалом. (Если последовательность Коши не является нуль-последовательностью, то для всех достаточно больших n ее члены отличны от 0 и для почти всех ее членов можно взять обратные элементы. С точностью до конечного числа членов снова получаем последовательность Коши.)

Поле классов вычетов кольца последовательностей Коши по модулю нуль-последовательностей и есть поле K_v. Мы вкладываем K в K_v „по диагонали“, т. е. сопоставляем элементу $x \in K$ последовательность $(x, x, x, \ldots)$.

Абсолютное значение на K продолжаем на K_v по непрерывности. Если $\{x_n\}$ — последовательность Коши, представляющая элемент ξ из K_v, то полагаем $|\xi| = \lim |x_n|$. Легко доказывается, что так определенное абсолютное значение не зависит от выбора представляющей последовательности $\{x_n\}$ для ξ и индуцирует заданное абсолютное значение на K.

Наконец, доказывается, что поле K_v — полное. Это делается обычным диагональным процессом. Если $\xi_1, \xi_2, \ldots$ — последовательность Коши в K_v и ξ_j представляется последовательностью Коши $\{x_{jn}\}$ из K, то без всякого труда доказывается, что

$$x_{11}, \; x_{22}, \; x_{33}, \; \ldots$$

будет последовательностью Коши в K, представляющей элемент ξ из K_v, для которого

$$\lim_{j\to\infty} \xi_j = \xi.$$

Пара (K_v, i), фигурирующая в предложении 2, может быть названа *некоторым пополнением* K. Стандартная пара, полученная с помощью предыдущей конструкции, могла бы быть названа (просто) *пополнением* K.

Пусть поле K снабжено некоторым нетривиальным архимедовым абсолютным значением v. Если известно, что ограничение v на подполе рациональных чисел зависимо от обычного абсолютного значения, то пополнение K_v является полным полем, содержащим пополнение поля $\mathbf{Q}$ в качестве замкнутого подполя, т. е. содержащим в качестве замкнутого подполя поле $\mathbf{R}$ вещественных чисел. Стоит привести теорему Гельфанда — Мазура, касающуюся структуры таких полей. Но сначала введем понятие нормированного векторного пространства.

Пусть K — *поле с нетривиальным абсолютным значением* и E — векторное пространство над K. Под *нормой* на E (согласованной с абсолютным значением на K) мы будем понимать функцию $\xi \longmapsto |\xi|$, отображающую E в поле вещественных чисел, такую, что

НО 1. $|\xi| \geqslant 0$ для всех $\xi \in E$, и $|\xi| = 0$ тогда и только тогда, когда $\xi = 0$.

НО 2. $|x\xi| \leqslant |x|\,|\xi|$ для всех $x \in K$ и $\xi \in E$.

НО 3. Если $\xi, \xi' \in E$, то $|\xi + \xi'| \leqslant |\xi| + |\xi'|$. Две нормы $|\ |_1$ и $|\ |_2$ называются *эквивалентными*, если существуют числа C_1, $C_2 > 0$, такие, что для всех $\xi \in E$ имеют место неравенства

$$C_1 |\xi|_1 \leqslant |\xi|_2 \leqslant C_2 |\xi|_1.$$

Предположим, что пространство E конечномерно с базисом $\omega_1, \ldots, \omega_n$ над K. Имея выражения

$$\xi = x_1\omega_1 + \ldots + x_n\omega_n, \qquad x_i \in K$$

элементов $\xi \in E$ через этот базис, мы можем определить норму, положив

$$|\xi| = \max_i |x_i|.$$

Три свойства, определяющих норму, тривиально проверяются.

Предложение 3. *Пусть K — поле, полное относительно некоторого нетривиального абсолютного значения, E — конечномерное пространство над K. Любые две нормы на E (согласованные с заданным абсолютным значением на K) эквивалентны.*

Доказательство. Докажем сначала, что топология на E является топологией прямого произведения, т. е. что если $\omega_1, \ldots, \omega_n$ — базис E над K, то последовательность

$$\xi^{(\nu)} = x_1^{(\nu)}\omega_1 + \ldots + x_n^{(\nu)}\omega_n, \qquad x_i^{(\nu)} \in K,$$

является последовательностью Коши в E в точности тогда, когда каждая из n последовательностей $x_i^{(\nu)}$ является последовательностью Коши в K. Доказывать будем индукцией по n. Утверждение очевидно для $n=1$. Предположим, что $n \geqslant 2$. Рассмотрим указанную выше последовательность. Не теряя общности, мы можем считать, что она сходится к 0. (Если необходимо, рассмотрим последовательность $\xi^{(\nu)} - \xi^{(\mu)}$ при $\nu, \mu \to \infty$.) Мы должны показать, что последовательности коэффициентов также сходятся к 0. Если это не имеет места, то существует число $a > 0$, такое, что при некотором j, скажем $j=1$,

$$|x_1^{(\nu)}| > a$$

для сколь угодно больших ν. Таким образом, для некоторой подпоследовательности значений ν последовательность $\xi^{(\nu)}/x_1^{(\nu)}$ сходится к 0 и, следовательно,

$$\frac{\xi^{(\nu)}}{x_1^{(\nu)}} - \omega_1 = \frac{x_2^{(\nu)}}{x_1^{(\nu)}}\omega_2 + \ \dots\ + \frac{x_n^{(\nu)}}{x_1^{(\nu)}}\omega_n.$$

Пусть $\eta^{(\nu)}$ обозначает правую часть этого равенства. Тогда подпоследовательность $\eta^{(\nu)}$ сходится (поскольку сходится левая часть равенства). По индукции заключаем, что коэффициенты при $\omega_2, \dots, \omega_n$ также сходятся в K, скажем, к $y_2, \dots, y_n$. Беря предел, получаем, что

$$-\omega_1 = y_2\omega_2 + \ \dots\ + y_n\omega_n$$

вопреки линейной независимости ω_i.

В заключение мы должны убедиться, что нормы, индуцирующие одинаковую топологию, эквивалентны. Пусть этими нормами будут $|\ |_1$ и $|\ |_2$. Существует число $C > 0$, такое, что для любого $\xi \in E$

$$|\xi|_1 \leqslant C \quad \text{влечет} \quad |\xi|_2 \leqslant 1.$$

Возьмем элемент $a \in K$ с условием $0 < |a| < 1$. Для всякого $\xi \in E$ существует однозначно определенное целое число s, такое, что

$$C|a| < |a^s\xi|_1 \leqslant C.$$

Значит, $|a^s\xi|_2 \leqslant 1$, откуда тотчас получаем

$$|\xi|_2 \leqslant C^{-1}|a|^{-1}|\xi|_1.$$

Второе неравенство следует из симметрии с аналогичной константой

Теорема 1. *Пусть A — коммутативная алгебра над полем вещественных чисел, содержащая некоторый элемент j, такой, что $j^2 = -1$. Положим $\mathbf{C} = \mathbf{R} + \mathbf{R}j$. Допустим, что A нормирована (как векторное пространство над $\mathbf{R}$) и что $|xy| \leqslant |x|\,|y|$*

для всех x, $y \in A$. *Тогда для заданного элемента* $x_0 \in A$, $x_0 \neq 0$, *найдется элемент* $c \in \mathbf{C}$, *такой, что* $x_0 - c$ *необратим в* A.

Доказательство (Торнхейм). Предположим, что элемент $x_0 - z$ обратим для всех $z \in \mathbf{C}$. Рассмотрим отображение f: $\mathbf{C} \to A$, определяемое формулой

$$f(z) = (x_0 - z)^{-1}.$$

Легко проверяется (как обычно), что взятие обратных является непрерывной операцией. Следовательно, f непрерывно и для $z \neq 0$ имеем

$$f(z) = z^{-1}(x_0 z^{-1} - 1)^{-1} = \frac{1}{z}\left(\frac{1}{\frac{x_0}{z} - 1}\right).$$

Отсюда мы видим, что $f(z)$ стремится к нулю, когда z уходит в бесконечность (в $\mathbf{C}$). Следовательно, $z \mapsto |f(z)|$ является непрерывным отображением $\mathbf{C}$ в множество вещественных чисел $\geqslant 0$, ограниченным и принимающим малые значения вне некоторого большого круга. Значит, оно имеет максимум, скажем M. Пусть D — множество элементов $z \in \mathbf{C}$, для которых $|f(z)| = M$. Тогда D непусто; D ограничено и замкнуто. Докажем, что D открыто, и тем самым получим противоречие.

Пусть c_0 — некоторая точка из D, которую после сдвига мы можем предполагать совпадающей с нулем. Мы утверждаем, что если r, вещественное и > 0, мало, то все точки окружности радиуса r с центром в c_0 лежат в D. Действительно, рассмотрим сумму

$$S(n) = \frac{1}{n}\sum_{k=1}^{n} \frac{1}{x_0 - \omega^k r},$$

где ω — примитивный корень n-й степени из единицы. Формальное взятие логарифмической производной от $X^n - r^n = \prod_{k=1}^{n}(X - \omega^k r)$ показывает, что

$$\frac{nX^{n-1}}{X^n - r^n} = \sum_{k=1}^{n} \frac{1}{X - \omega^k r},$$

откуда, деля на n и подставляя x_0 вместо X, получаем

$$S(n) = \frac{1}{x_0 - r\,(r/x_0)^{n-1}}.$$

Если r мало (скажем, $|r/x_0| < 1$), то

$$\lim_{n \to \infty} |S(n)| = \left|\frac{1}{x_0}\right| = M.$$

Предположим, что существует комплексное число λ с абсолютным значением 1, такое, что

$$\left|\frac{1}{x_0-\lambda r}\right|<M.$$

Тогда около λ найдется на единичной окружности интервал и найдется такое число $\varepsilon>0$, что для всех корней из единицы ζ, лежащих в этом интервале,

$$\left|\frac{1}{x_0-\zeta r}\right|<M-\varepsilon.$$

(Это вытекает из непрерывности.) Возьмем n достаточно большим. Пусть b_n — число корней n-й степени из единицы, лежащих в нашем интервале. Тогда b_n/n приблизительно равно длине этого интервала (деленной на 2π). Мы можем представить $S(n)$ в виде суммы

$$S(n)=\frac{1}{n}\left[\sum\nolimits_{\mathrm{I}}\frac{1}{x_0-\omega^k r}+\sum\nolimits_{\mathrm{II}}\frac{1}{x_0-\omega^k r}\right],$$

где первая сумма $\sum_{\mathrm{I}}$ берется по тем корням из единицы ω^k, которые лежат в нашем интервале, а вторая сумма берется по всем остальным корням. Каждый член второй суммы имеет норму $\leqslant M$, так как M — максимум. Следовательно, получаем оценку

$$|S(n)|\leqslant\frac{1}{n}\left[\left|\sum\nolimits_{\mathrm{I}}\right|+\left|\sum\nolimits_{\mathrm{II}}\right|\right]\leqslant$$
$$\leqslant\frac{1}{n}\left(b_n(M-\varepsilon)+(n-b_n)M\right)\leqslant M-\frac{b_n}{n}\varepsilon.$$

Это противоречит тому факту, что предел $|S(n)|$ равен M.

Следствие. *Пусть поле K является расширением поля* $\mathbf{R}$ *и обладает абсолютным значением, продолжающим обычное абсолютное значение на* $\mathbf{R}$. *Тогда либо* $K=\mathbf{R}$, *либо* $K=\mathbf{C}$.

Доказательство. Допустим сначала, что K содержит $\mathbf{C}$. Тогда из предположения, что K — поле, и из теоремы 1 следует, что $K=\mathbf{C}$.

Если K не содержит $\mathbf{C}$, другими словами, не содержит квадратного корня из -1, то мы введем $L=K(j)$, где $j^2=-1$. Определим норму на L (как $\mathbf{R}$-пространстве), положив

$$|x+yj|=|x|+|y|$$

для $x, y\in K$. Это, очевидно, превращает L в нормированное $\mathbf{R}$-пространство. Кроме того, если $z=x+yj$ и $z'=x'+y'j$, то

$$\begin{aligned}|zz'|&=|xx'-yy'|+|xy'+x'y|\leqslant\\&\leqslant|xx'|+|yy'|+|xy'|+|x'y|=\\&=|x||x'|+|y||y'|+|x||y'|+|x'||y|=\\&=(|x|+|y|)(|x'|+|y'|)=|z||z'|,\end{aligned}$$

и мы можем снова применить теорему 1, что и завершает доказательство.

При помощи предложения 3 получается следующее важное утверждение:

Предложение 4. *Пусть K — поле, полное относительно нетривиального абсолютного значения v, и E — произвольное алгебраическое расширение K. Тогда v имеет единственное продолжение на E. Если E конечно над K, то E полное.*

Доказательство. В архимедовом случае существование продолжения очевидно, поскольку мы имеем дело с вещественными или комплексными числами. В неархимедовом случае мы отложим доказательство существования до одного из следующих параграфов. Оно использует идеи, совершенно отличные от рассматриваемых здесь. Что касается единственности, то мы можем предполагать, что E конечно над K. В силу предложения 3 всякое продолжение v на E определяет ту же топологию, что и норма, задаваемая как максимум абсолютных значений коэффициентов в разложении по базису. Если в E задана последовательность Коши $\xi^{(\nu)}$

$$\xi^{(\nu)} = x_{\nu 1}\omega_1 + \ \ldots \ + x_{\nu n}\omega_n,$$

то n последовательностей $\{x_{\nu i}\}$ $(i = 1, \ldots, n)$ должны быть последовательностями Коши в K по определению нормы как максимума норм коэффициентов. Если $\{x_{\nu i}\}$ сходится в K к элементу z_i, то очевидно, что последовательность $\xi^{(\nu)}$ сходится к $z_1\omega_1 + \ \ldots \ + z_n\omega_n$. Следовательно, E — полное. Кроме того, поскольку любые два продолжения v на E эквивалентны, мы можем применить предложение 1, причем обязательно $\lambda = 1$, так как оба продолжения индуцируют одно и то же абсолютное значение v на K. Это доказывает то, что нужно.

Из единственности мы можем получить явное выражение для абсолютного значения на алгебраическом расширении K. Заметим сначала, что если E — нормальное расширение K и σ — автоморфизм E над K, то функция

$$x \longmapsto |\sigma x|$$

является абсолютным значением на E, продолжающим заданное абсолютное значение на K.

Следовательно, мы должны иметь

$$|\sigma x| = |x|$$

для всех $x \in E$. Если E алгебраично над K и σ — вложение E в $\bar{K}$ над K, то остается справедливым то же заключение. В частности, если α — алгебраический элемент степени n над K и $\alpha_1 \ \ldots, \alpha_n$ —

его сопряженные (с учетом кратностей, равных степени несепарабельности), то все абсолютные значения $|\alpha_i|$ равны. Обозначив через N норму из $K(\alpha)$ в K, мы видим, что

$$|N(\alpha)| = |\alpha|^n,$$

и извлекая корень n-й степени, получаем

Предложение 5. *Пусть K — поле, полное относительно некоторого нетривиального абсолютного значения. Пусть элемент α алгебраичен над K и N — норма из $K(\alpha)$ в K. Если $n = [K(\alpha) : K]$, то*

$$|\alpha| = |N(\alpha)|^{1/n}.$$

В частном случае поля комплексных чисел над полем вещественных чисел можно записать $\alpha = a + bi$, где $a, b \in \mathbf{R}$, и мы видим, что формула из предложения 5 является обобщением формулы для абсолютного значения комплексного числа

$$\alpha = (a^2 + b^2)^{1/2},$$

поскольку $a^2 + b^2$ есть не что иное, как норма числа α из $\mathbf{C}$ в $\mathbf{R}$.

§ 3. Конечные расширения

В этом параграфе мы будем иметь дело с полем K, снабженным нетривиальным абсолютным значением v.

Мы хотим описать, как это абсолютное значение продолжается на конечные расширения поля K. Если E — расширение над K и w — некоторое абсолютное значение на E, продолжающее v, то будем писать $w \mid v$.

Мы знаем, что v может быть продолжено на пополнение K_v, а затем однозначно продолжено на его алгебраическое замыкание $\overline{K}_v$. Если E — конечное расширение K или даже произвольное алгебраическое расширение, то мы можем продолжить v на E, вложив E в $\overline{K}_v$ посредством изоморфизма над K и взяв индуцированное абсолютное значение на E. Мы докажем теперь, что всякое продолжение v может быть получено этим способом.

Предложение 6. *Пусть E — конечное расширение поля K, w — некоторое абсолютное значение на E, продолжающее v, E_w — соответствующее пополнение и K_w — замыкание K в E_w, причем E отождествлено с подполем в E_w. Тогда $E_w = EK_w$ (композит).*

Доказательство. Заметим, что K_w является пополнением K и что композит EK_w конечен над K_w, а потому, согласно предложению 4, § 2, является полным полем. Так как он содержит E, то E плотно в нем и, следовательно, $E_w = EK_w$.

Если мы начинаем с вложения $\sigma\colon E \to \bar{K}_v$ (относительно которого всегда предполагается, что оно берется над K), то снова в силу предложения 4 § 2 поле $\sigma E \cdot K_v$ — полное. Таким образом, эта конструкция и конструкция из предложения 6 по существу совпадают с точностью до изоморфизма. В дальнейшем мы примем точку зрения вложений. Теперь мы должны определить, когда два вложения дают нам одно и то же абсолютное значение на E.

Пусть даны два вложения σ, $\tau\colon E \to \bar{K}_v$; мы будем говорить, что они *сопряжены над* K_v, если существует автоморфизм λ поля $\bar{K}_v$ над K_v, для которого $\sigma = \lambda\tau$. Мы видим, что в действительности нам достаточно знать действие λ на τE или $\tau E \cdot K_v$.

Предложение 7. *Пусть E — алгебраическое расширение K. Два вложения σ, $\tau\colon E \to \bar{K}_v$ тогда и только тогда приводят к одному и тому же абсолютному значению на E, когда они сопряжены над K_v.*

Доказательство. Предположим, что они сопряжены над K_v. Тогда единственность продолжения абсолютного значения с K_v на $\bar{K}_v$ гарантирует, что индуцированные абсолютные значения на E равны. Обратно, предположим, что они равны. Пусть $\lambda\colon \tau E \to \sigma E$ — изоморфизм над K. Покажем, что λ продолжается до изоморфизма $\tau E \cdot K_v$ на $\sigma E \cdot K_v$ над K_v. Так как τE плотно в $\tau E \cdot K_v$, то всякий элемент $x \in \tau E \cdot K_v$ может быть записан в виде

$$x = \lim \tau x_n,$$

где $x_n \in E$. Поскольку абсолютные значения, индуцированные вложениями σ и τ на E, совпадают, последовательность $\lambda\tau x_n = \sigma x_n$ сходится к некоторому элементу из $\sigma E \cdot K_v$, который мы обозначим через λx. Непосредственно проверяется, что λx не зависит от специального выбора последовательности τx_n и что $\lambda\colon \tau E \cdot K_v \to \sigma E \cdot K_v$ есть изоморфизм, который, очевидно, оставляет поле K_v неподвижным. Это доказывает наше предложение.

Ввиду двух предыдущих предложений при заданном продолжении w абсолютного значения v на конечное расширение E поля K мы можем отождествлять E_w с композитом EK_v полей E и K_v. Если степень $N = [E : K]$ конечна, то мы будем называть

$$N_w = [E_w : K_v]$$

локальной степенью.

Предложение 8. *Пусть E — конечное сепарабельное расширение над K степени N. Тогда*

$$N = \sum_{w \mid v} N_w.$$

Доказательство. Как известно, $E = K(\alpha)$ для какого-то элемента α. Пусть $f(X)$ — его неприводимый многочлен над K. Тогда над K_v мы имеем разложение

$$f(X) = f_1(X) \dots f_r(X)$$

на неприводимые множители $f_i(X)$. В силу нашего предположения о сепарабельности все они встречаются с кратностью 1. Вложения E в $\overline{K}_v$ соответствуют отображениям α в корни многочленов f_i. Два вложения сопряжены тогда и только тогда, когда они отображают α в корни одного и того же многочлена f_i. С другой стороны, ясно, что локальная степень в каждом случае есть в точности степень f_i. Это доказывает наше предложение.

Предложение 9. *Пусть E — конечное расширение над K. Тогда*

$$\sum_{w \mid v} [E_w : K_v] \leqslant [E : K].$$

Если E чисто несепарабельно над K, то существует только одно абсолютное значение w на E, продолжающее v.

Доказательство. Сначала докажем второе утверждение. Если E чисто несепарабельно над K и p^r — его несепарабельная степень, то $\alpha^{p^r} \in K$ для всякого α из E. Следовательно, v имеет единственное продолжение на E. Рассмотрим теперь общий случай конечного расширения и положим $F = E^{p^r}K$. Тогда F сепарабельно над K и E чисто несепарабельно над F. В силу предыдущего предложения

$$\sum_{w \mid v} [F_w : K_v] = [F : K]$$

и для каждого w будет $[E_w : F_w] \leqslant [E : F]$. После этого неравенство, фигурирующее в формулировке предложения, становится очевидным.

Если v — такое абсолютное значение на K, что для всякого конечного расширения E поля K имеет место равенство $[E : K] = \sum_{w \mid v} [E_w : K_v]$, то мы будем говорить, что v *хорошо себя ведет*.

Рассмотрим башню конечных расширений $L \supset E \supset K$. Пусть w пробегает все абсолютные значения на E, продолжающие v, а u — все

абсолютные значения на L, продолжающие v. Если $u \mid w$, то L_u содержит E_w. Таким образом,

$$\sum_{u \mid v} [L_u : K_v] = \sum_{w \mid v} \sum_{u \mid w} [L_u : E_w]\,[E_w : K_v] =$$
$$= \sum_{w \mid v} [E_w : K_v] \sum_{u \mid w} [L_u : E_w] \leqslant$$
$$\leqslant \sum_{w \mid v} [E_w : K_v]\,[L : E] \leqslant$$
$$\leqslant [E : K]\,[L : E].$$

Отсюда мы непосредственно видим, что если v хорошо себя ведет, E — конечное расширение над K и w продолжает v на E, то w также хорошо себя ведет (мы должны всюду иметь равенство).

Пусть E — конечное расширение K и p^r — его несепарабельная степень. Напомним, что норма элемента $\alpha \in E$ задается формулой

$$N_K^E(\alpha) = \prod_{\sigma} \sigma\alpha^{p^r},$$

где σ пробегает все различные изоморфизмы E над K (в заданное алгебраическое замыкание).

Если w — абсолютное значение, продолжающее v на E, то норма из E_w в K_v будет называться *локальной нормой*.

Заменив выше произведение на сумму, получим *след* и *локальный след*. Мы обозначаем след сокращенно символом Tr.

Предложение 10. *Пусть E — конечное расширение K, и пусть v хорошо себя ведет. Тогда*

$$N_K^E(\alpha) = \prod_{w \mid v} N_{K_v}^{E_w}(\alpha),$$

$$\mathrm{Tr}_K^E(\alpha) = \sum_{w \mid v} \mathrm{Tr}_{K_v}^{E_w}(\alpha)$$

для любого $\alpha \in E$.

Доказательство. Предположим сначала, что $E = K(\alpha)$, и пусть $f(X)$ — неприводимый многочлен элемента α над K. Разложив $f(X)$ на неприводимые множители над K_v, получим

$$f(X) = f_1(X) \ldots f_r(X),$$

где каждый $f_i(X)$ неприводим и все f_i различны ввиду нашего предположения, что v хорошо себя ведет. Норма $N_K^E(\alpha)$ равна свободному члену f, умноженному на $(-1)^{\deg f}$, и аналогично для каждого f_i. Поскольку свободный член f равен произведению свободных членов f_i, получаем первую часть предложения. Утверждение для следа вытекает из рассмотрения предпоследнего коэффициента у f и каждого f_i.

Если E не равно $K(\alpha)$, то мы просто используем транзитивность нормы и следа. Детали предоставляются читателю.

Можно оперировать и непосредственно с вложениями. Пусть $\sigma_1, \ldots, \sigma_m$ — различные вложения E в $\bar{K}_v$ над K и p^r — несепарабельная степень E над K. Несепарабельная степень композита $\sigma E \cdot K_v$ над K_v для всякого σ не превосходит p^r. Если мы разобьем $\sigma_1, \ldots, \sigma_m$ на различные классы сопряженности над K_v, то из предположения, что v хорошо себя ведет, немедленно следует, что несепарабельная степень $\sigma_i E \cdot K_v$ над K_v для каждого i должна быть также равна p^r. Таким образом, формула, выражающая норму в виде произведения сопряженных с кратностью p^r, распадается в произведение множителей, соответствующих классам сопряженности над K_v.

Принимая во внимание предложение 5 из § 2, мы получаем

Предложение 11. *Пусть K снабжено хорошо себя ведущим абсолютным значением v. Пусть, далее, E — конечное расширение над K и*

$$N_w = [E_w\colon K_v]$$

для всякого абсолютного значения w на E, продолжающего v. Тогда

$$\prod_{w \mid v} |\alpha|_w^{N_w} = \left| N_K^E(\alpha) \right|_v$$

для любого $\alpha \in E$.

§ 4. Нормирования

В этом параграфе мы получим среди других результатов теорему о существовании продолжения неархимедовых абсолютных значений на алгебраические расширения. Введем сначала одно обобщение понятия *неархимедова абсолютного значения.*

Пусть Γ — мультипликативная коммутативная группа. Мы будем говорить, что на Γ определено *упорядочение*, если задано подмножество S в Γ, замкнутое относительно умножения и такое, что Γ есть объединение следующих попарно непересекающихся подмножеств: S, единичного элемента 1 и множества S^{-1}, состоящего из всех обратных к элементам из S.

По определению неравенство $\alpha < \beta$ для $\alpha, \beta \in \Gamma$ означает, что $\alpha\beta^{-1} \in S$. В частности, $\alpha < 1$ тогда и только тогда, когда $\alpha \in S$. Легко проверяются следующие свойства отношения $<$:

1. Каковы бы ни были $\alpha, \beta \in \Gamma$, либо $\alpha < \beta$, либо $\alpha = \beta$, либо $\beta < \alpha$, причем эти возможности взаимно исключают друг друга.

2. $\alpha < \beta$ влечет $\alpha\gamma < \beta\gamma$ для всякого $\gamma \in \Gamma$.

3. $\alpha < \beta$ и $\beta < \gamma$ влечет $\alpha < \gamma$.

(Обратно, отношение, удовлетворяющее указанным трем свой-

ствам, определяет подмножество S, состоящее из всех элементов < 1. Однако этот факт нам в дальнейшем не потребуется.)

Удобно присоединить формально к упорядоченной группе дополнительный элемент 0, такой, что $0\alpha = 0$ и $0 < \alpha$ для всех $\alpha \in \Gamma$. Упорядоченная группа тогда является аналогом мультипликативной группы положительных вещественных чисел, за исключением того, что упорядочение, возможно, неархимедово.

Если $\alpha \in \Gamma$ и n — целое число $\neq 0$, для которого $\alpha^n = 1$, то $\alpha = 1$. Это тотчас следует из предположения о том, что S замкнуто относительно умножения и не содержит 1. В частности, отображение $\alpha \mapsto \alpha^n$ инъективно.

Пусть K — поле. Под *нормированием* K мы будем понимать отображение $x \mapsto |x|$ поля K в упорядоченную группу Γ, к которой присоединен дополнительный элемент 0, такое, что

НОР 1. $|x| = 0$ тогда и только тогда, когда $x = 0$.

НОР 2. $|xy| = |x||y|$ для всех $x, y \in K$.

НОР 3. $|x + y| \leqslant \max(|x|, |y|)$.

Мы видим, что нормирование определяет гомоморфизм мультипликативной группы K^* в Γ. Нормирование называется *тривиальным*, если оно отображает K^* в 1. Если отображение, задаваемое нормированием, не сюръективно, то его образ будет упорядоченной подгруппой в Γ и, беря ограничение на этот образ, мы получим нормирование, отображающее K^* на упорядоченную группу, называемую *группой значений*.

Мы будем обозначать нормирования также через v. Пусть v_1, v_2 — два нормирования на K. Мы будем говорить, что они эквивалентны, если существует сохраняющий порядок изоморфизм λ образа v_1 на образ v_2, такой, что

$$|x|_2 = \lambda |x|_1$$

для всех $x \in K$. (Мы принимаем соглашение, что $\lambda(0) = 0$.)

Нормирования, как и абсолютные значения, обладают дополнительными свойствами. Например, $|1| = 1$, поскольку $|1| = |1|^2$. Кроме того,

$$|\pm x| = |x|$$

для всех $x \in K$. Доказательство очевидно. Далее, если $|x| < |y|$, то

$$|x + y| = |y|.$$

Чтобы убедиться в этом, заметим, что при наших предположениях

$$|y| = |y + x - x| \leqslant \max(|y + x|, |x|) \leqslant \max(|x|, |y|) = |y|.$$

Наконец, в сумме

$$x_1 + \ldots + x_n = 0$$

по крайней мере два элемента суммы имеют одинаковые значения

при нормировании. Это непосредственно вытекает из предыдущего замечания.

Пусть K — поле. Подкольцо $\mathfrak{o}$ в K называется *кольцом нормирования*, если оно обладает тем свойством, что для всякого $x \in K$ либо $x \in \mathfrak{o}$, либо $x^{-1} \in \mathfrak{o}$.

Мы увидим сейчас, как кольца нормирования приводят к нормированиям. Пусть $\mathfrak{o}$ — кольцо нормирования в K и U — группа единиц кольца $\mathfrak{o}$. Мы утверждаем, что $\mathfrak{o}$ — локальное кольцо. Действительно, предположим, что x, $y \in \mathfrak{o}$ не являются единицами. Пусть, скажем, $x/y \in \mathfrak{o}$. Тогда $1 + x/y = (x+y)/y \in \mathfrak{o}$ Если бы элемент $x+y$ был единицей, то $1/y \in \mathfrak{o}$, вопреки предположению, что y — не единица. Следовательно, $x+y$ — не единица. Тривиально проверяется, что для $z \in \mathfrak{o}$ элемент zx не является единицей. Следовательно, не единицы образуют идеал, являющийся, таким образом, единственным максимальным идеалом в $\mathfrak{o}$.

Пусть $\mathfrak{m}$ — максимальный идеал в $\mathfrak{o}$ и $\mathfrak{m}^*$ — мультипликативная система ненулевых элементов из $\mathfrak{m}$. Тогда

$$K^* = \mathfrak{m}^* \cup U \cup \mathfrak{m}^{*-1}$$

есть объединение попарно не пересекающихся множеств $\mathfrak{m}^*$, U и $\mathfrak{m}^{*-1}$. Факторгруппе K^*/U может быть придано упорядочение. Если $x \in K^*$, то обозначаем смежный класс xU символом $|x|$, полагая $|0| = 0$. Считаем по определению, что $|x| < 1$ (т. е $|x| \in S$) тогда и только тогда, когда $x \in \mathfrak{m}^*$. Наше множество S, очевидно, замкнуто относительно умножения, и если положить $\Gamma = K^*/U$, то Γ окажется объединением попарно не пересекающихся множеств S, 1, S^{-1}. Таким образом, мы получаем нормирование поля K.

Отметим, что если x, $y \in K$ и $y \neq 0$, то

$$|x| < |y| \Longleftrightarrow |x/y| < 1 \Longleftrightarrow x/y \in \mathfrak{m}^*.$$

Обратно, если задано нормирование поля K в некоторую упорядоченную группу, то пусть $\mathfrak{o}$ — подмножество в K, состоящее из всех таких x, что $|x| \leqslant 1$. Из аксиом нормирования тотчас вытекает, что $\mathfrak{o}$ — кольцо Если $|x| < 1$, то $|x^{-1}| > 1$, так что x^{-1} не лежит в $\mathfrak{o}$. Если $|x| = 1$, то $|x^{-1}| = 1$. Мы видим, что $\mathfrak{o}$ есть кольцо нормирования, максимальный идеал которого состоит из элементов x с $|x| < 1$ и единицами которого служат элементы x с $|x| = 1$. Читатель тотчас проверит, что имеется биективное соответствие между кольцами нормирования в K и классами эквивалентности нормирований.

Пусть F — поле и пусть символ ∞ удовлетворяет обычным алгебраическим правилам. Для $a \in F$ по определению

$$a \pm \infty = \infty; \quad a \cdot \infty = \infty, \quad \text{когда} \quad a \neq 0;$$

$$\infty \cdot \infty = \infty; \qquad 1/0 = \infty \quad \text{и} \quad 1/\infty = 0$$

Выражения $\infty \pm \infty$, $0 \cdot \infty$, $0/0$, ∞/∞ не определены.

Точкой φ поля K в поле F называется отображение

$$\varphi\colon K \to \{F, \infty\}$$

поля K в множество, состоящее из F и ∞, удовлетворяющее обычным правилам для гомоморфизмов

$$\varphi(a+b) = \varphi(a) + \varphi(b),$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

(если только выражения, стоящие в правых частях этих формул, определены) и такое, что $\varphi(1) = 1$. Мы будем говорить также, это эта точка является *F-значной*. Элементы из K, которые не переводятся в ∞, будут называться *конечными* в этой точке, а остальные элементы будут называться *бесконечными*.

Читатель тотчас проверит, что множество $\mathfrak{o}$ элементов из K, конечных в некоторой точке, является кольцом нормирования в K. Его максимальный идеал состоит из тех элементов x, для которых $\varphi(x) = 0$. Обратно, если $\mathfrak{o}$ — кольцо нормирования в K с максимальным идеалом $\mathfrak{m}$, то обозначим через $\varphi\colon \mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$ канонический гомоморфизм и положим $\varphi(x) = \infty$ для $x \in K$, $x \notin \mathfrak{o}$. Тривиально проверяется, что φ — точка.

Пусть $\varphi_1\colon K \to \{F_1, \infty\}$ и $\varphi_2\colon K \to \{F_2, \infty\}$ — две точки поля K. Беря их ограничения на образы, мы можем считать, что они сюръективны. Будем говорить, что они *эквивалентны*, если существует изоморфизм $\lambda\colon F_1 \to F_2$, для которого $\varphi_2 = \lambda \circ \varphi_1$. (Мы полагаем $\lambda(\infty) = \infty$.) Легко видеть, что две точки эквивалентны в том и только в том случае, если они имеют одно и то же кольцо нормирования. Ясно, что имеется биективное соответствие между классами эквивалентности точек поля K и кольцами нормирования в K. Точка называется *тривиальной*, если она инъективна. Кольцом нормирования тривиальной точки служит просто само поле K.

Заметим, что, как и в случае гомоморфизмов, композиция двух точек снова является точкой (тривиальная проверка).

Часто удобнее иметь дело с точками, а не с кольцами нормирования, так же как иногда удобнее иметь дело с гомоморфизмами, а не с каноническими гомоморфизмами или кольцами по модулю идеала. Однако во всем дальнейшем мы используем язык колец нормирования и предоставляем читателю перевод на язык точек.

Общая теория нормирований и колец нормирования принадлежит Круллю (1932). Однако теория продолжения гомоморфизмов из гл. IX, § 3, была развита лишь около 1945 г. Она дает нам теорему продолжения для нормирований.

Теорема 1. *Пусть K — подполе поля L. Тогда всякое нормирование на K имеет продолжение до нормирования на L.*

Доказательство. Пусть $\mathfrak{o}$ — кольцо нормирования в K, соответствующее данному нормированию. Пусть $\varphi: \mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$ — канонический гомоморфизм на поле вычетов. Продолжим его до гомоморфизма некоторого кольца нормирования $\mathfrak{O}$ в L, согласно § 3 из гл. IX. Пусть $\mathfrak{M}$ — максимальный идеал в $\mathfrak{O}$. Так как $\mathfrak{M} \cap \mathfrak{o}$ содержит $\mathfrak{m}$, но не содержит 1, то $\mathfrak{M} \cap \mathfrak{o} = \mathfrak{m}$. Пусть U' — группа единиц кольца $\mathfrak{O}$. Тогда $U' \cap K = U$ будет группой единиц кольца $\mathfrak{o}$. Таким образом, имеем каноническое вложение

$$K^*/U \to L^*/U',$$

которое, как непосредственно проверяется, сохраняет порядок. Отождествляя K^*/U с подгруппой в L^*/U', мы получаем продолжение нашего нормирования поля K до нормирования L.

Разумеется, когда мы имеем дело с абсолютными значениями, мы требуем, чтобы группа значений была подгруппой мультипликативной группы положительных чисел. Следовательно, мы должны еще кое-что доказать о природе группы значений L^*/U' в случае, когда L алгебраично над K.

Предложение 12. *Пусть L — конечное расширение степени n поля K, и пусть w — нормирование L с группой значений Γ', а Γ — группа значений нормирования поля K. Тогда* $(\Gamma' : \Gamma) \leqslant n$.

Доказательство. Пусть $|y_1|, \ldots, |y_r|$ — элементы из Γ', представляющие различные смежные классы Γ' по Γ. Докажем, что y_j линейно независимы над K. В соотношении $a_1y_1 + \ldots + a_ry_r = 0$ с $a_j \in K$, $a_j \neq 0$, два члена должны иметь одно и то же значение, скажем $|a_iy_i| = |a_jy_j|$, где $i \neq j$ и, значит,

$$|y_i| = |a_i^{-1}a_j||y_j|.$$

Это противоречит предположению, что $|y_i|, |y_j|$ $(i \neq j)$ представляют разные смежные классы Γ' по Γ, и тем самым доказывает наше предложение.

Следствие 1. *Существует целое число $e \geqslant 1$, такое, что отображение $\gamma \mapsto \gamma^e$ индуцирует инъективный гомоморфизм Γ' в Γ.*

Доказательство. Возьмем e равное индексу $(\Gamma' : \Gamma)$.

Следствие 2. *Если K — поле с нормированием v, группа значений которого есть упорядоченная подгруппа упорядоченной группы положительных вещественных чисел, и если L — алгебраическое расширение поля K, то существует продолжение нормирования v на L, группой значений которого также служит некоторая упорядоченная подгруппа положительных вещественных чисел.*

Доказательство. Мы знаем, что можно продолжить v до нормирования w поля L с некоторой группой значений Γ', а группа

значений Γ нормирования v может быть отождествлена с подгруппой в $\mathbf{R}^+$. В силу следствия 1 всякий элемент из Γ' имеет конечный период по модулю Γ. Так как каждый элемент из $\mathbf{R}^+$ имеет единственный корень e-й степени для всякого целого числа $e \geqslant 1$, то мы очевидным образом можем найти сохраняющее порядок вложение Γ' в $\mathbf{R}^+$, тождественное на Γ. Таким образом, мы получаем наше продолжение v до абсолютного значения на L.

Следствие 3. *Если L конечно над K и Γ — бесконечная циклическая группа, то группа Γ' также бесконечная циклическая.*

Доказательство. Использовать следствие 1 и тот факт, что всякая подгруппа циклической группы циклическая.

Придадим теперь нашему предыдущему предложе ию несколько более сильную форму. Будем называть $(\Gamma' : \Gamma)$ *индексом ветвления.*

Предложение 13. *Пусть L — конечное расширение степени n поля K, $\mathfrak{O}$ — кольцо нормирования в L, $\mathfrak{M}$ — его максимальный идеал, $\mathfrak{o} = \mathfrak{O} \cap K$ и $\mathfrak{m}$ — максимальный идеал кольца $\mathfrak{o}$, т. е. $\mathfrak{m} = \mathfrak{M} \cap \mathfrak{o}$. Тогда степень поля вычетов $[\mathfrak{O}/\mathfrak{M} : \mathfrak{o}/\mathfrak{m}]$ конечна. Если мы обозначим ее через f и через e — индекс ветвления, то $ef \leqslant n$.*

Доказательство. Пусть $y_1, \ldots, y_e$ — представители в L^* различных смежных классов Γ'/Γ и $z_1, \ldots, z_s$ — элементы из $\mathfrak{O}$, классы вычетов которых $\bmod \mathfrak{M}$ линейно независимы над $\mathfrak{o}/\mathfrak{m}$. Рассмотрим соотношение

$$\sum_{i,\,j} a_{ij} z_j y_i = 0,$$

где $a_{ij} \in K$ и не все $a_{ij} = 0$. Во внутренней сумме

$$\sum_{j=1}^{s} a_{ij} z_j$$

поделим все члены на коэффициент a_{iv}, имеющий наибольшее значение относительно нормирования. Мы получим линейную комбинацию элементов $z_1, \ldots, z_s$ с коэффициентами в $\mathfrak{o}$, причем по крайней мере один коэффициент является единицей. Так как $z_1, \ldots, z_s$ линейно независимы по модулю $\mathfrak{M}$ над $\mathfrak{o}/\mathfrak{m}$, то наша линейная комбинация является единицей. Следовательно,

$$\left| \sum_{j=1}^{s} a_{ij} z_j \right| = |a_{iv}|$$

для некоторого индекса v. В сумме

$$\sum_{i=1}^{e} \left(\sum_{j=1}^{s} a_{ij} z_j \right) y_i = 0,$$

рассматриваемой как сумма по i, по крайней мере два члена имеют одинаковое значение. Это противоречит независимости элементов $|y_1|, \ldots, |y_e| \bmod \Gamma$, как и в доказательстве предложения 12.

Замечание. Наше доказательство показывает также, что элементы $\{z_j y_i\}$ линейно независимы над K. Позднее это будет использовано.

Если w — продолжение нормирования v, то индекс ветвления будет обозначаться через $e(w|v)$, а степень поля вычетов — через $f(w|v)$.

Предложение 14. *Пусть K — поле с нормированием v и $K \subset E \subset L$ — конечные расширения K. Пусть w — продолжение v на E и u — продолжение w на L. Тогда*

$$e(u|w)\,e(w|v) = e(u|v),$$
$$f(u|w)\,f(w|v) = f(u|v).$$

Доказательство. Очевидно.

Словами предыдущее предложение можно выразить так: индекс ветвления и степень поля вычетов мультипликативны в башнях.

С помощью нормирований (или колец нормирования) можно получить характеристику целых элементов. Будем пользоваться следующей терминологией. Пусть $\mathfrak{o}$, $\mathfrak{O}$ — локальные кольца с максимальными идеалами $\mathfrak{m}$, $\mathfrak{M}$ соответственно. Будем говорить, что $\mathfrak{O}$ *лежит над* $\mathfrak{o}$, если $\mathfrak{o} \subset \mathfrak{O}$ и $\mathfrak{M} \cap \mathfrak{o} = \mathfrak{m}$. В этом случае имеется каноническое вложение $\mathfrak{o}/\mathfrak{m} \subset \mathfrak{O}/\mathfrak{M}$.

Предложение 15. *Пусть $\mathfrak{o}$ — локальное кольцо, содержащееся в поле L. Элемент x из L тогда и только тогда является целым над $\mathfrak{o}$, когда x принадлежит всякому кольцу нормирования $\mathfrak{O}$ поля L, лежащему над $\mathfrak{o}$.*

Доказательство. Предположим, что x не является целым над $\mathfrak{o}$. Пусть $\mathfrak{m}$ — максимальный идеал в $\mathfrak{o}$. Тогда идеал $(\mathfrak{m}, 1/x)$ в $\mathfrak{o}[1/x]$ не может совпадать со всем кольцом, поскольку в противном случае мы имели бы

$$-1 = a_n (1/x)^n + \ldots + a_1 (1/x) + y,$$

где $y \in \mathfrak{m}$ и $a_i \in \mathfrak{o}$, откуда

$$(1+y)\,x^n + \ldots + a_n = 0.$$

Но $1+y$ не лежит в $\mathfrak{m}$, следовательно, является единицей в $\mathfrak{o}$. Разделив уравнение на $1+y$, видим, что x — целый над $\mathfrak{o}$, вопреки нашему предположению. Таким образом, идеал $(\mathfrak{m}, 1/x)$ не совпадает со всем кольцом и, следовательно, содержится в некотором максимальном идеале $\mathfrak{P}$, пересечение которого с $\mathfrak{o}$ содержит $\mathfrak{m}$, т. е. должно быть равно $\mathfrak{m}$. Продолжая канонический гомоморфизм $\mathfrak{o}[1/x] \to \mathfrak{o}[1/x]/\mathfrak{P}$ до гомоморфизма некоторого кольца нормирования $\mathfrak{O}$

поля L, мы видим, что образ $1/x$ есть 0 и, следовательно, x не может лежать в этом кольце нормирования.

Обратно, предположим, что элемент x является целым над $\mathfrak{o}$, и пусть

$$x^n + \ldots + a_0 = 0$$

— целое уравнение для x с коэффициентами в $\mathfrak{o}$. Пусть $\mathfrak{O}$ — произвольное кольцо нормирования поля L, лежащее над $\mathfrak{o}$, и $|\ |$ — соответствующее нормирование. Разделим уравнение на x^n. Если $|x| > 1$, то $|1/x| < 1$, и мы получаем выражение для 1 в виде суммы членов, каждый из которых имеет нормирование < 1, что невозможно. Следовательно, $|x| \leqslant 1$, т. е. $x \in \mathfrak{O}$, что и требовалось установить.

Предложение 16. *Пусть A — кольцо, содержащееся в поле L. Элемент x поля L тогда и только тогда является целым над A, когда x лежит во всяком кольце нормирования $\mathfrak{O}$ поля L, содержащем A.*

Доказательство. Доказательство аналогично доказательству предыдущего предложения и предоставляется читателю в качестве упражнения.

Мы закончим этот параграф установлением связи между кольцами нормирования в конечном расширении и целыми замыканиями.

Предложение 17. *Пусть $\mathfrak{o}$ — кольцо нормирования поля K, L — конечное расширение K, $\mathfrak{O}$ — кольцо нормирования поля L, лежащее над $\mathfrak{o}$, и $\mathfrak{M}$ — его максимальный идеал. Пусть, далее, B — целое замыкание кольца $\mathfrak{o}$ в L и $\mathfrak{P} = \mathfrak{M} \cap B$. Тогда $\mathfrak{O}$ равно локальному кольцу $B_{\mathfrak{P}}$.*

Доказательство. Ясно, что $B_{\mathfrak{P}}$ содержится в $\mathfrak{O}$. Обратно, пусть x — элемент из $\mathfrak{O}$. Тогда x удовлетворяет уравнению с коэффициентами в K, среди которых не все равны 0, скажем

$$a_n x^n + \ldots + a_0 = 0, \qquad a_i \in K.$$

Пусть a_s — коэффициент, имеющий наибольшее значение среди a_i относительно нормирования, ассоциированного с кольцом нормирования $\mathfrak{o}$, и притом самый старший из коэффициентов, имеющих это значение. Положим $b_i = a_i/a_s$. Тогда все $b_i \in \mathfrak{o}$ и $b_n, \ldots, b_{s+1} \in \mathfrak{M}$. Разделим уравнение на x^s. Получим

$$(b_n x^{n-s} + \ldots + b_{s+1}x + 1) + \frac{1}{x}\left(b_{s-1} + \ldots + b_0 \frac{1}{x^{s-1}}\right) = 0.$$

Обозначим через y и z два выражения, стоящие в скобках в предыдущем уравнении, так что

$$-y = z/x \quad \text{и} \quad -xy = z.$$

Чтобы доказать наше предложение, достаточно показать, что y и z лежат в B и что y не лежит в $\mathfrak{P}$.

Воспользуемся предложением 15. Если некоторое кольцо нормирования из L, лежащее над $\mathfrak{o}$, содержит x, то оно содержит и y, поскольку y есть многочлен от x с коэффициентами в $\mathfrak{o}$. Следовательно, оно содержит также и $z = -xy$. Если, с другой стороны, кольцо нормирования поля L, лежащее над $\mathfrak{o}$, содержит $1/x$, то оно содержит z, поскольку z есть многочлен от $1/x$ с коэффициентами в $\mathfrak{o}$. Следовательно, это кольцо нормирования содержит также и y. Отсюда в силу предложения 15 заключаем, что y, z лежат в B.

Кроме того, так как $x \in \mathfrak{O}$, а $b_n, \ldots, b_{s+1}$ лежат по построению в $\mathfrak{M}$, то y не может лежать в $\mathfrak{M}$ и, следовательно, не может лежать в $\mathfrak{P}$. Это завершает доказательство.

Следствие 1. *Пусть обозначения те же, что и в предложении. Тогда существует лишь конечное число колец нормирования в L, лежащих над $\mathfrak{o}$.*

Доказательство. Это вытекает из того факта, что существует лишь конечное число максимальных идеалов $\mathfrak{P}$ кольца B, лежащих над максимальным идеалом кольца $\mathfrak{o}$ (следствие к предложению 11, гл. IX, § 2).

Следствие 2. *Пусть обозначения те же, что и в предложении. Предположим дополнительно, что L является расширением Галуа над K. Если $\mathfrak{O}$ и $\mathfrak{O}'$ — два кольца нормирования в L, лежащие над $\mathfrak{o}$, с максимальными идеалами $\mathfrak{M}$, $\mathfrak{M}'$ соответственно, то существует автоморфизм σ поля L над K, такой, что $\sigma\mathfrak{O} = \mathfrak{O}'$ и $\sigma\mathfrak{M} = \mathfrak{M}'$.*

Доказательство. Пусть $\mathfrak{P} = \mathfrak{O} \cap B$ и $\mathfrak{P}' = \mathfrak{O}' \cap B$. В силу предложения 11 из гл. IX, § 2, мы знаем, что существует автоморфизм σ поля L над K, для которого $\sigma\mathfrak{P} = \mathfrak{P}'$. После этого наше утверждение очевидно.

Пример. Пусть k — поле и K — его конечно порожденное расширение степени трансцендентности 1. Если t — базис трансцендентности K над k, то K будет конечным алгебраическим расширением над $k(t)$. Пусть $\mathfrak{O}$ — кольцо нормирования поля K, содержащее k, причем $\mathfrak{O} \neq K$. Положим $\mathfrak{o} = \mathfrak{O} \cap k(t)$. Тогда, очевидно, $\mathfrak{o}$ является кольцом нормирования поля $k(t)$ (условие об обратных заведомо удовлетворяется) и соответствующее нормирование поля $k(t)$ не может быть тривиальным: либо t, либо $t^{-1} \in \mathfrak{o}$. Скажем, $t \in \mathfrak{o}$. Пусть $\mathfrak{m}$ — максимальный идеал в $\mathfrak{o}$. Тогда $\mathfrak{m} \cap k[t]$ не может быть нулевым идеалом, иначе канонический гомоморфизм $\mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$ индуцировал бы изоморфизм на $k[t]$ и, значит, изоморфизм на $k(t)$ вопреки предположению. Следовательно, $\mathfrak{m} \cap k[t]$ есть простой идеал $\mathfrak{p}$, порожден-

ный каким-то неприводимым многочленом $p(t)$. Локальное кольцо $k[t]_{\mathfrak{p}}$ является, очевидно, кольцом нормирования, которое должно совпадать с $\mathfrak{o}$, поскольку всякий элемент из $k(t)$ имеет представление вида $p^r u$, где u — единица в $k[t]_{\mathfrak{p}}$. Таким образом, мы определили все кольца нормирования поля $k(t)$, содержащие k, и мы видим, что группа значений—циклическая. Такие нормирования будут называться *дискретными*. Они изучаются более подробно ниже. Ввиду следствия 3 предложения 12 кольцо нормирования $\mathfrak{O}$ в K также дискретно.

Поле вычетов $\mathfrak{o}/\mathfrak{m}$ равно $k[t]/\mathfrak{p}$, а потому является конечным расширением k. В силу предложения 13 отсюда следует, что $\mathfrak{O}/\mathfrak{M}$ конечно над k (здесь $\mathfrak{M}$ обозначает максимальный идеал в $\mathfrak{O}$).

Наконец, отметим, что существует лишь конечное число колец нормирования $\mathfrak{O}$ поля K, содержащих k и таких, что t лежит в максимальном идеале кольца $\mathfrak{O}$. Действительно, такое кольцо нормирования должно лежать над $k[t]_{\mathfrak{p}}$, где $\mathfrak{p}=(t)$ — простой идеал, порожденный t, и мы можем применить доказанное выше следствие 1.

§ 5. *Пополнения и нормирования*

В этом параграфе мы рассматриваем неархимедово абсолютное значение v на поле K. Это абсолютное значение является нормированием, группа значений которого Γ_K есть подгруппа группы положительных вещественных чисел. Пусть $\mathfrak{o}$ — его кольцо нормирования, $\mathfrak{m}$ — максимальный идеал.

Обозначим через $\hat{K}$ пополнение K относительно v и через $\hat{\mathfrak{o}}$ (соответственно $\hat{\mathfrak{m}}$) — замыкание $\mathfrak{o}$ (соответственно $\mathfrak{m}$) в $\hat{K}$. По непрерывности всякий элемент из $\hat{\mathfrak{o}}$ имеет значение $\leqslant 1$, а всякий элемент из $\hat{K}$, не лежащий в $\hat{\mathfrak{o}}$, имеет значение >1. Если $x\in\hat{K}$, то существует элемент $y\in K$, для которого $|x-y|$ очень мало и, значит, $|x|=|y|$ для такого элемента y (в силу неархимедовости). Следовательно, $\hat{\mathfrak{o}}$ — кольцо нормирования в $\hat{K}$ и $\hat{\mathfrak{m}}$ — его максимальный идеал. Кроме того,

$$\hat{\mathfrak{o}}\cap K=\mathfrak{o},\quad \hat{\mathfrak{m}}\cap K=\mathfrak{m},$$

и мы имеем изоморфизм

$$\mathfrak{o}/\mathfrak{m}\xrightarrow{\approx}\hat{\mathfrak{o}}/\hat{\mathfrak{m}}.$$

Таким образом, поле вычетов $\mathfrak{o}/\mathfrak{m}$ не изменяется при пополнении.

Пусть E — расширение поля K, $\mathfrak{o}_E$ — его кольцо нормирования, лежащее над $\mathfrak{o}$, и $\mathfrak{m}_E$ — максимальный идеал в $\mathfrak{o}_E$. Предположим, что нормирование, соответствующее $\mathfrak{o}_E$, является в действительности

абсолютным значением, так что мы можем образовать пополнение $\hat{E}$. Тогда имеет место коммутативная диаграмма

$$\begin{array}{ccc} \mathfrak{o}_E/\mathfrak{m}_E & \xrightarrow{\approx} & \hat{\mathfrak{o}}_E/\hat{\mathfrak{m}}_E \\ \uparrow & & \uparrow \\ \mathfrak{o}/\mathfrak{m} & \xrightarrow{\approx} & \hat{\mathfrak{o}}/\hat{\mathfrak{m}} \end{array}$$

в которой вертикальные стрелки являются вложениями, а горизонтальные — изоморфизмами. Таким образом, расширение поля вычетов нашего нормирования можно изучать для пополнений E и K.

Аналогичное замечание применимо и к индексу ветвления. Пусть $\Gamma_v(K)$ и $\Gamma_v(\hat{K})$ обозначают группы значений наших нормирований на K и $\hat{K}$ соответственно (т. е. образ при отображении $x \longmapsto |x|$ для $x \in K^*$ и $x \in \hat{K}^*$ соответственно). Мы видели выше, что $\Gamma_v(K) = \Gamma_v(\hat{K})$; другими словами, ввиду свойства неархимедовости группа значений при пополнении остается той же самой. (Это, разумеется, уже не так в архимедовом случае.) Пусть снова E — расширение поля K и w — абсолютное значение на E, продолжающее v. Имеет место коммутативная диаграмма

$$\begin{array}{ccc} \Gamma_w(E) & \xrightarrow{=} & \Gamma_w(\hat{E}) \\ \uparrow & & \uparrow \\ \Gamma_v(K) & \xrightarrow{=} & \Gamma_v(\hat{K}) \end{array}$$

из которой видно, что индекс ветвления $(\Gamma_w(E) : \Gamma_v(K))$ также не изменяется при пополнении.

§ 6. *Дискретные нормирования*

Нормирование называется *дискретным*, если его группа значений циклическая. В этом случае нормирование является абсолютным значением (если мы рассматриваем группу значений как подгруппу в группе положительных вещественных чисел). Для всякого простого числа p p-адическое нормирование поля рациональных чисел дискретно. В силу следствия 3 предложения 12 § 4 продолжение дискретного нормирования на конечное расширение также дискретно. Если не считать абсолютные значения, получаемые вложением поля в поле вещественных или комплексных чисел, дискретные нормирования являются практически наиболее важными абсолютными значениями. Мы посвятим им несколько замечаний.

Пусть v — дискретное нормирование поля K и $\mathfrak{o}$ — его кольцо нормирования, $\mathfrak{m}$ — максимальный идеал. В $\mathfrak{m}$ имеется элемент π,

значение которого $|\pi|$ порождает всю группу значений. (Другой образующей группы значений служит элемент $|\pi^{-1}|$.) Такой элемент π называется *локальным параметром* для v (или для $\mathfrak{m}$). Всякий элемент x из K может быть записан в форме

$$x = u\pi^r,$$

где u — единица из $\mathfrak{o}$ и r — некоторое целое число. Действительно, $|x| = |\pi|^r = |\pi^r|$ для некоторого $z \in \mathbf{Z}$, откуда вытекает, что x/π^r — единица в $\mathfrak{o}$. Мы называем r *порядком* x относительно v. Он, очевидно, не зависит от выбора параметра. Мы будем также говорить, что x имеет *нуль порядка* r. (Если r отрицательно, то мы говорим, что x имеет *полюс порядка* $-r$.)

В частности, мы видим, что $\mathfrak{m}$ — главный идеал, порожденный π. В качестве упражнения проверьте, что всякий идеал в $\mathfrak{o}$ главный и является степенью $\mathfrak{m}$. Заметим, кроме того, что $\mathfrak{o}$ — факториальное кольцо с единственным простым элементом (с точностью до единиц), а именно π.

Для элементов x, $y \in K$ будем использовать запись $x \sim y$, если $|x| = |y|$. Пусть π_i $(i = 1, 2, \ldots)$ — последовательность элементов из $\mathfrak{o}$, таких, что $\pi_i \sim \pi^i$. Пусть R — множество представителей $\mathfrak{o}/\mathfrak{m}$ в $\mathfrak{o}$. Это означает, что каноническое отображение $\mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$ индуцирует биекцию R на $\mathfrak{o}/\mathfrak{m}$. *Всякий элемент x из $\mathfrak{o}$ может быть записан в виде сходящегося ряда*

$$x = a_0 + a_1\pi_1 + a_2\pi_2 + \ldots,$$

где коэффициенты $a_i \in R$ однозначно определяются элементом x. Это легко доказывается посредством индуктивного рассуждения. Предположим, что

$$x \equiv a_0 + \ldots + a_n\pi_n \pmod{\mathfrak{m}^{n+1}}.$$

Тогда $x - (a_0 + \ldots + a_n\pi_n) = \pi_{n+1}y$ для некоторого $y \in \mathfrak{o}$. По предположению $y = a_{n+1} + \pi z$ для некоторого $a_{n+1} \in R$. Отсюда получаем

$$x \equiv a_0 + \ldots + a_{n+1}\pi_{n+1} \pmod{\mathfrak{m}^{n+2}},$$

и ясно, что n-й член нашего ряда стремится к 0. Очевидно, что построенный таким образом ряд сходится к x. Если поле K — полное относительно нашего нормирования, то всякий такой ряд сходится к некоторому элементу из K (в силу неархимедовости!). Из того факта, что R содержит точно по одному представителю для каждого класса вычетов $\bmod \mathfrak{m}$, вытекает, что a_i однозначно определены

Примеры. Рассмотрим сначала случай поля рациональных чисел с p-адическим нормированием v_p. Пополнение обозначим символом $\mathbf{Q}_p$. Это поле *p-адических чисел*. Замыкание $\mathbf{Z}$ в $\mathbf{Q}_p$ называется кольцом *целых p-адических чисел* $\mathbf{Z}_p$. Отметим, что простое число p является простым элементом и в кольце $\mathbf{Z}$, и в его замыкании $\mathbf{Z}_p$. Мы можем выбрать в качестве нашего множества представителей R множество целых чисел $(0, 1, \ldots, p-1)$. Таким образом, всякое целое p-адическое число может быть записано в виде сходящейся суммы $\sum a_i p^i$, где a_i — целые числа, $0 \leqslant a_i \leqslant p-1$. Эта сумма называется *$p$-адическим разложением*. Такие суммы складываются и умножаются обычным способом как сходящиеся ряды.

Например, справедлив обычный формализм для геометрической прогрессии, и, скажем, для $p=3$

$$-1 = \frac{2}{1-3} = 2(1+3+3^2+\ldots).$$

Отметим, что представители $(0, 1, \ldots, p-1)$ ни в коей мере не являются единственными, могущими быть использованными. В действительности можно доказать, что $\mathbf{Z}_p$ содержит корни $(p-1)$-й степени из единицы, и часто удобнее выбирать эти корни из единицы в качестве представителей для ненулевых элементов поля вычетов.

Теперь рассмотрим случай поля рациональных функций $k(t)$, где k — произвольное поле и t трансцендентно над k. Возьмем нормирование, определяемое простым элементом t кольца $k[t]$. Это нормирование дискретно, а пополнением $k[t]$ относительно него служит кольцо степенных рядов $k[[t]]$. Мы можем взять элементы из k в качестве представителей поля вычетов, которое канонически изоморфно k. Максимальным идеалом в $k[[t]]$ является идеал, порожденный t.

Все это представляет собой алгебраизацию обычной ситуации, возникающей в теории функций комплексного переменного. Например, пусть z_0 — точка на комплексной плоскости и $\mathfrak{o}$ — кольцо функций, голоморфных в некотором круге с центром z_0. Тогда $\mathfrak{o}$ — кольцо дискретного нормирования, максимальный идеал которого состоит из тех функций, которые имеют нуль в z_0. Всякий элемент из $\mathfrak{o}$ обладает разложением в степенной ряд

$$f(z) = \sum_{\nu=m}^{\infty} a_\nu (z-z_0)^\nu.$$

В качестве представителей поля вычетов могут быть взяты комплексные числа a_ν. Если $a_m \neq 0$, то говорят, что $f(z)$ имеет нуль порядка m. Порядок будет один и тот же, иметь ли в виду порядок относительно дискретного нормирования в алгебраическом смысле,

или порядок в смысле теории функций комплексного переменного. Мы можем выбрать канонический униформизирующий параметр, а именно $z - z_0$ и

$$f(z) = (z - z_0)^m g(z),$$

где $g(z)$ — степенной ряд, начинающийся с ненулевой константы. Таким образом, $g(z)$ обратим.

Пусть снова K — поле, полное относительно некоторого дискретного нормирования, и E — конечное расширение K. Пусть $\mathfrak{o}_E$, $\mathfrak{m}_E$ — кольцо нормирования в E и его максимальный идеал, лежащие над $\mathfrak{o}$, $\mathfrak{m}$ в K. Пусть Π — простой элемент в E. Если Γ_E и Γ_K — группы значений нормирований в E и K соответственно и

$$e = (\Gamma_E : \Gamma_K)$$

— индекс ветвления, то

$$|\Pi^e| = |\pi|,$$

а элементы

$$\Pi^i \pi^j, \quad 0 \leqslant i \leqslant e-1, \quad j = 0, 1, 2, \ldots,$$

имеют порядок $je + i$ в E.

Пусть $\omega_1, \ldots, \omega_f$ — элементы из $\mathfrak{o}_E$, классы вычетов которых $\bmod \mathfrak{m}_E$ образуют базис в $\mathfrak{o}_E/\mathfrak{m}_E$. Если R, как и выше, обозначает множество представителей поля $\mathfrak{o}/\mathfrak{m}$ в $\mathfrak{o}$, то множество, состоящее из всех элементов вида

$$a_1\omega_1 + \ldots + a_f\omega_f,$$

где $a_i \in R$, будет множеством представителей для $\mathfrak{o}_E/\mathfrak{m}_E$ в $\mathfrak{o}_E$. Отсюда видно, что всякий элемент из $\mathfrak{o}_E$ обладает сходящимся разложением

$$\sum_{i=0}^{e-1} \sum_{\nu=1}^{f} \sum_{j=0}^{\infty} a_{\nu, i, j} \pi^j \omega_\nu \Pi^i.$$

Таким образом, элементы $\{\omega_\nu \Pi^i\}$ образуют множество образующих $\mathfrak{o}_E$ как модуля над $\mathfrak{o}$. С другой стороны, мы видели в доказательстве предложения 13 из § 4, что эти элементы линейно независимы над K. Следовательно, получаем

Предложение 18. *Пусть K — поле, полное относительно дискретного нормирования, E — конечное расширение K и e, f — соответственно индекс ветвления и степень поля вычетов. Тогда*

$$ef = [E : K].$$

Следствие 1. *Пусть $\alpha \in E$, $\alpha \neq 0$, v — нормирование на K и w — его продолжение на E. Тогда*

$$\operatorname{ord}_v N_K^E(\alpha) = f(w \mid v) \operatorname{ord}_w \alpha.$$

Доказательство. Это вытекает непосредственно из формулы

$$|N_K^E(\alpha)| = |\alpha|^{ef}$$

и из определений.

Следствие 2. *Пусть K — произвольное поле и v — дискретное нормирование на K. Пусть E — конечное расширение поля K. Если v хорошо себя ведет в E (например, если E сепарабельно над K), то*

$$\sum_{w|v} e(w|v) f(w|v) = [E : K].$$

Если E — расширение Галуа над K, то все e_w равны одному и тому же числу e, а все f_w — одному и тому же числу f, так что

$$efr = [E : K],$$

где r — число продолжений v на E.

Доказательство. Первое утверждение вытекает из нашего предположения и из предложения 8 § 3. Если E — расширение Галуа над K, то, как мы знаем из следствия 2 предложения 17 § 4, любые два нормирования поля E, лежащие над v, сопряжены. Следовательно, все индексы ветвления равны и то же самое верно для степеней полей вычетов. Наше соотношение $efr = [E : K]$ теперь очевидно.

§ 7. Нули многочленов в полных полях

Пусть K — поле, полное относительно некоторого нетривиального абсолютного значения.

Пусть

$$f(X) = \prod (X - \alpha_i)^{r_i}$$

— многочлен из $K[X]$ со старшим коэффициентом 1 и с различными корнями α_i кратностей r_i. Обозначим через d степень f. Пусть g — другой многочлен с коэффициентами из $\overline{K}$ также степени d и со старшим коэффициентом 1. Обозначим через $|g|$ — максимум абсолютных значений коэффициентов g. Легко видеть, что если величина $|g|$ ограничена, то абсолютные значения корней g также ограничены.

Предположим, что g близок к f в том смысле, что величина $|f - g|$ мала. Если β — корень g, то величина

$$|f(\beta) - g(\beta)| = |f(\beta)| = \prod |\alpha_i - \beta|^{r_i}$$

мала и, следовательно, β должен быть близок к некоторому корню f. Если β близок, скажем, к $\alpha = \alpha_1$, то его расстояние до других корней f близко к расстоянию от α_1 до других корней, а потому ограничено снизу. В этом случае мы будем говорить, что β *принадлежит* α.

Предложение 19. *Если многочлен g достаточно близок к f и $\beta_1, \ldots, \beta_s$ — корни g, принадлежащие α (с учетом кратностей), то $s = r_1$ есть кратность α в f.*

Доказательство. Предположим противное. Тогда можно найти последовательность многочленов g_ν, стремящихся к f, у которых имеется точно s корней $\beta_1^{(\nu)}, \ldots, \beta_s^{(\nu)}$, принадлежащих β, причем $s \neq r_1$. (Мы можем брать многочлены с одним и тем же s, так как имеется лишь конечное число возможных значений для s.) Кроме того, остальные корни g_ν также принадлежат корням f, и мы можем предполагать, что эти корни сгруппированы в соответствии с тем, какому корню f они принадлежат. Так как $\lim g_\nu = f$, то заключаем, что α должен иметь кратность s в f — противоречие.

Исследуем теперь условия, при которых многочлен имеет корень в полном поле.

Предположим, что K — поле, полное относительно некоторого дискретного нормирования с кольцом нормирования $\mathfrak{o}$ и максимальным идеалом $\mathfrak{p}$. Пусть π — фиксированный простой элемент в $\mathfrak{p}$.

Мы будем иметь дело с n-мерным пространством над $\mathfrak{o}$. Вектор $(a_1, \ldots, a_n)$, где $a_i \in \mathfrak{o}$, будем обозначать через A. Будем говорить, что A — *нуль* многочлена $f(X_1, \ldots, X_n) \in \mathfrak{o}[X]$ от n переменных, если $f(A) = 0$, и что A *нуль* f по модулю $\mathfrak{p}^m$, если $f(A) \equiv 0 \pmod{\mathfrak{p}^m}$.

Пусть $C = (c_0, \ldots, c_n)$ — вектор из $\mathfrak{o}^{(n+1)}$ и m — целое число $\geqslant 1$. Исследуем природу решений сравнения вида

$$\pi^m (c_0 + c_1 x_1 + \ldots + c_n x_n) \equiv 0 \pmod{\mathfrak{p}^{m+1}}. \qquad (*)$$

Это сравнение эквивалентно линейному сравнению

$$c_0 + c_1 x_1 + \ldots + c_n x_n \equiv 0 \pmod{\mathfrak{p}}. \qquad (**)$$

Если хоть один коэффициент c_i $(i = 1, \ldots, n)$ не сравним с 0 $(\mathrm{mod}\ \mathfrak{p})$, то множество решений не пусто и имеет обычную структуру решения одного неоднородного линейного уравнения над полем $\mathfrak{o}/\mathfrak{p}$. В частности, оно имеет размерность $n - 1$. Сравнение (*) или (**), где хотя бы одно $c_i \not\equiv 0 \pmod{\mathfrak{p}}$, будет называться *собственным сравнением*.

Обозначим через $D_i f$ формальную частную производную от f по X_i и введем запись

$$\operatorname{grad} f(X) = (D_1 f(X), \ldots, D_n f(X)).$$

Предложение 20. *Пусть* $f(X) \in \mathfrak{o}[X]$ *и* r *— целое число* $\geqslant 1$. *Пусть* $A \in \mathfrak{o}^{(n)}$ *— вектор, такой, что*

$$f(A) \equiv 0 \pmod{\mathfrak{p}^{2r-1}},$$
$$D_i f(A) \equiv 0 \pmod{\mathfrak{p}^{r-1}} \quad \text{для всех} \quad i = 1, \ldots, n,$$
$$D_i f(A) \not\equiv 0 \pmod{\mathfrak{p}^{r}} \quad \text{для некоторого} \quad i = 1, \ldots, n.$$

Пусть v *— целое число* $\geqslant 0$ *и* $B \in \mathfrak{o}^{(n)}$ *— вектор, для которого*

$$B \equiv A \pmod{\mathfrak{p}^{r}} \quad \text{и} \quad f(B) \equiv 0 \pmod{\mathfrak{p}^{2r-1+v}}.$$

Вектор $Y \in \mathfrak{o}^{(n)}$ *тогда и только тогда удовлетворяет сравнениям*

$$Y \equiv B \pmod{\mathfrak{p}^{r+v}} \quad \text{и} \quad f(Y) \equiv 0 \pmod{\mathfrak{p}^{2r+v}},$$

когда он может быть записан в виде $Y = B + \pi^{r+v}C$, *где* $C \in \mathfrak{o}^{(n)}$ *— некоторый вектор, удовлетворяющий собственному сравнению*

$$f(B) + \pi^{r+v} \operatorname{grad} f(B) \cdot C \equiv 0 \pmod{\mathfrak{p}^{2r+v}}.$$

Доказательство. Доказательство короче, чем формулировка предложения. Пусть $Y = B + \pi^{r+v}C$. Запишем разложение Тейлора

$$f(B + \pi^{r+v}C) = f(B) + \pi^{r+v} \operatorname{grad} f(B) \cdot C \pmod{\mathfrak{p}^{2r+2v}}.$$

Решая это сравнение по модулю $\mathfrak{p}^{2r+v}$, получаем, согласно предположению, собственное сравнение, поскольку

$$\operatorname{grad} f(B) \equiv \operatorname{grad} f(A) \equiv 0 \pmod{\mathfrak{p}^{r-1}}.$$

Следствие 1. *В предпосылках предложения* 20 *существует нуль многочлена* f *в* $\mathfrak{o}^{(n)}$, *сравнимый с* $A \bmod \mathfrak{p}^r$.

Доказательство. Мы можем записать этот нуль в виде сходящегося ряда

$$A + \pi^r C_0 + \pi^{r+1} C_1 + \ldots,$$

вычисляя $C_0, C_1, \ldots$ индуктивно, как в предложении.

Следствие 2. *Пусть* f *— многочлен от одной переменной из* $\mathfrak{o}[X]$, *и пусть элемент* $a \in \mathfrak{o}$ *удовлетворяет условиям* $f(a) \equiv 0 \pmod{\mathfrak{p}}$, *но* $f'(a) \not\equiv 0 \pmod{\mathfrak{p}}$. *Тогда существует элемент* $b \in \mathfrak{o}$, $b \equiv a \pmod{\mathfrak{p}}$, *такой, что* $f(b) = 0$.

Доказательство. Возьмем в предложении $n = 1$ и $r = 1$ и применим следствие 1.

Следствие 3. *Пусть* m *— положительное целое число, не делящееся на характеристику поля* K. *Тогда существует целое число* r, *такое, что для всякого* $a \in \mathfrak{o}$, $a \equiv 1 \pmod{\mathfrak{p}^r}$, *уравнение* $X^m - a = 0$ *имеет корень в* K.

Доказательство. Применить предложение.

Пример. В 2-адическом поле $\mathbf{Q}_2$ существует квадратный корень из -7, т. е. $\sqrt{-7} \in \mathbf{Q}_2$, так как $-7 = 1 - 8$.

(Об уточнениях предыдущего предложения см. N. Bourbaki, Algèbre Commutative, Ch. III, § 4, 5.) В тех случаях, когда абсолютное значение недискретно, также можно сформулировать критерий существования нуля у многочлена.

Предложение 21. *Пусть K — поле, полное относительно неархимедова абсолютного значения (нетривиального). Пусть $\mathfrak{o}$ — его кольцо нормирования, $f(X) \in \mathfrak{o}[X]$ — многочлен от одной переменной, и пусть элемент $\alpha_0 \in \mathfrak{o}$ таков, что*

$$|f(\alpha_0)| < |f'(\alpha_0)^2|$$

(здесь f' обозначает формальную производную многочлена f). Тогда последовательность

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

сходится к некоторому корню α многочлена f, лежащему в $\mathfrak{o}$, и имеет место неравенство

$$|\alpha - \alpha_0| \leqslant \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1.$$

Доказательство. Это легкое упражнение. Мы предоставляем детали читателю. Отметим, что здесь снова показатель 2 дает точное условие того, что приближенный корень можно поднять до настоящего корня. В тех случаях, когда абсолютное значение дискретно, предложение 21 превращается в частный случай предложения 20.

Техника, используемая в этом предложении, полезна также при рассмотрении некоторых колец, скажем локального кольца с максимальным идеалом $\mathfrak{m}$, таким, что $\mathfrak{m}^r = 0$ для некоторого целого r. Если имеется многочлен f из $\mathfrak{o}[X]$ и приближенный корень α_0, для которого $f'(\alpha_0) \not\equiv 0 \bmod \mathfrak{m}$, то аппроксимационная последовательность Ньютона показывает, как поднять α_0 до корня f.

УПРАЖНЕНИЯ

1. (а) Пусть K — поле с нормированием. Для всякого многочлена

$$f(X) = a_0 + a_1X + \ldots + a_nX^n$$

из $K[X]$ определим $|f|$ как максимум значений $|a_i|$ $(i = 0, \ldots, n)$. Показать, что этим определяется нормирование в $K[X]$, а также что это нормирование может быть продолжено на поле рациональных функций $K(X)$. Почему лемма Гаусса является частным случаем предыдущего утверждения? Обобщить на многочлены от нескольких переменных.

(б) Пусть f — многочлен с комплексными коэффициентами. Определим $|f|$ как максимум абсолютных значений коэффициентов. Пусть d — целое число $\geqslant 1$.

Показать, что существуют константы C_1, C_2 (зависящие только от d), такие, что если f, g — многочлены из $\mathbf{C}[X]$ степени $\leqslant d$, то

$$C_1 |f||g| \leqslant |fg| \leqslant C_2 |f||g|.$$

[*Указание*: индукция по числу множителей степени 1. Отметим, что правое неравенство *тривиально*.]

2. Пусть $M_{\mathbf{Q}}$ — множество абсолютных значений, состоящее из обычного абсолютного значения и всех p-адических абсолютных значений v_p на поле рациональных чисел $\mathbf{Q}$. Показать, что для любого рационального числа $a \in \mathbf{Q}$, $a \neq 0$, имеет место равенство

$$\prod_{v \in M_{\mathbf{Q}}} |a|_v = 1.$$

Пусть K — конечное расширение $\mathbf{Q}$ и M_K обозначает множество абсолютных значений на K, продолжающих абсолютные значения из $M_{\mathbf{Q}}$, и для всякого $w \in M_K$ пусть N_w — локальная степень $[K_w : \mathbf{Q}_v]$. Показать, что для $\alpha \in K$, $\alpha \neq 0$, имеет место равенство

$$\prod_{w \in M_K} |\alpha|_w^{N_w} = 1.$$

3. Показать, что поле p-адических чисел $\mathbf{Q}_p$ не имеет других автоморфизмов, кроме тождественного. [*Указание*: показать, что такие автоморфизмы непрерывны в p-адической топологии. Использовать следствие 3 предложения 20 в качестве *алгебраической характеристики элементов, близких к* 1.]

4. Пусть A — целостное кольцо главных идеалов, K — его поле частных и $\mathfrak{o}$ — кольцо нормирования в K, содержащее A, причем $\mathfrak{o} \neq K$. Показать, что $\mathfrak{o}$ есть локальное кольцо $A_{(p)}$ для некоторого простого элемента p. [Это применимо и к кольцу $\mathbf{Z}$, и к кольцу многочленов $k[X]$ над полем k.]

5. Пусть A — целостное кольцо, K — его поле частных. Предположим, что всякий конечно порожденный идеал в A — главный. Пусть $\mathfrak{o}$ — дискретное кольцо нормирования в K, содержащее A. Показать, что $\mathfrak{o} = A_{(p)}$ для некоторого элемента p из A и что p — образующая максимального идеала в $\mathfrak{o}$.

6. (Иссса) Пусть K — поле мероморфных функций на комплексной плоскости $\mathbf{C}$ и $\mathfrak{o}$ — кольцо дискретного нормирования в K (содержащее поле констант $\mathbf{C}$). Показать, что функция z лежит в $\mathfrak{o}$ [*Указание*: пусть a_1, a_2, ... — дискретная последовательность комплексных чисел, сходящихся к бесконечности, например последовательность целых положительных чисел, p — некоторое простое число и ν_1, ν_2, ... — последовательность целых чисел, $0 \leqslant \nu_i \leqslant p-1$, для которой $\sum \nu_i p^i$ не является p-адическим разложением рационального числа. Пусть f — целая функция, имеющая нуль порядка $\nu_i p^i$ в a_i для всякого i и не имеющая никаких других нулей. Если z не содержится в $\mathfrak{o}$, то рассмотреть дробь

$$g(z) = \frac{f(z)}{\prod_{i=1}^{n} (z - a_i)^{\nu_i p^i}}.$$

Пользуясь вейерштрассовским разложением целой функции, показать, что $g(z) = h(z)^{p^n+1}$ для некоторой целой функции $h(z)$.

Вычисляя теперь порядок нуля g относительно дискретного нормирования, определенного кольцом $\mathfrak{o}$, через порядки нуля f и $\prod (z-\alpha_i)^{\nu_i p^t}$, получить противоречие]

Показать, что если U — некомпактная риманова поверхность, L — поле мероморфных функций на U и $\mathfrak{o}$ — кольцо дискретного нормирования в L, содержащее константы, то всякая голоморфная функция φ на U лежит в $\mathfrak{o}$ [*Указание* рассмотреть отображение $\varphi\ U \to \mathbf{C}$ и получить дискретное нормирование на K, компонируя φ с мероморфными функциями на $\mathbf{C}$ Затем применить первую часть упражнения] Показать, что кольцо нормирования — это кольцо, ассоциированное с точкой на римановой поверхности [*Дальнейшее указание* если вы не знакомы с римановыми поверхностями, то сделайте это для комплексной плоскости Для всякого $z \in U$ пусть f_z — функция, голоморфная на U и имеющая только нуль порядка 1 в z Показать что если для некоторого z_0 функция f_{z0} имеет порядок $\geqslant 1$ в $\mathfrak{o}$, то $\mathfrak{o}$ — кольцо нормирования, ассоциированное с z_0 Иными словами, всякая другая функция f_z имеет порядок 0 в $\mathfrak{o}$ Убедиться посредством приема аналогичного использованному в первой части упражнения, что нормирование, определяемое кольцом $\mathfrak{o}$, тривиально на любой голоморфной функции]

7. *Снова векторы Витта* Пусть k — совершенное поле характеристики p Мы будем использовать векторы Витта в той форме, в какой они описаны в упражнениях из гл VIII На $W(k)$ можно определить абсолютное значение, а именно $|x| = p^{-r}$, если x_r — первая ненулевая компонента x Показать, что это действительно абсолютное значение, очевидно, дискретное, определенное на кольце и допускающее продолжение на поле частных Показать, что последнее поле — полное, и заметить, что $W(k)$ — кольцо нормирования Максимальный идеал состоит из тех x, у которых $x_0 = 0$, т е равен $pW(k)$

8. Пусть F — поле, полное относительно некоторого дискретного нормирования, $\mathfrak{o}$ — соответствующее кольцо нормирования и π — простой элемент, причем поле $\mathfrak{o}/(\pi) = k$ имеет характеристику p Доказать, что если $a, b \in \mathfrak{o}$ и $a \equiv b \pmod{\pi^r}$, где $r > 0$, то $a^{p^n} \equiv b^{p^n} \pmod{\pi^{r+n}}$ для всех целых $n \geqslant 0$

9. Пусть F обозначает то же, что и выше Показать, что в $\mathfrak{o}$ существует система представителей R для $\mathfrak{o}/(\pi)$, такая, что $R^p = R$ и что такая система единственна (Тейхмюллер) [*Указание* пусть α — некоторый класс вычетов из k Для всякого $\nu \geqslant 0$ пусть a_ν — представитель в $\mathfrak{o}$ класса $\alpha^{p^{-\nu}}$, показать, что последовательность $a_\nu^{p^\nu}$ сходится при $\nu \to \infty$ и притом к представителю a класса α, не зависящему от выбора a_ν] Показать, что полученная таким образом система представителей R замкнута относительно умножения и что если F имеет характеристику p, то система R замкнута также относительно сложения, а значит, изоморфна k

10. Предположим, что F имеет характеристику 0. Сопоставим каждому вектору $x \in W(k)$ элемент

$$\sum \xi_t^{p^{-t}} p^t,$$

где ξ_t — представитель x_t в специальной системе из предыдущего упражнения Показать, что это отображение дает вложение $W(k)$ в $\mathfrak{o}$

11. (*Локальная униформизация*) Пусть k — поле, K — конечно порожденное расширение степени трансцендентности 1 и $\mathfrak{o}$ — кольцо дискретного нормирования поля K над k с максимальным идеалом $\mathfrak{m}$ Предположим, что $\mathfrak{o}/\mathfrak{m} = k$ и что K сепарабельно над $k(x)$, где x — некоторая образующая $\mathfrak{m}$.

Показать, что существует элемент $y \in \mathfrak{o}$, такой, что $K = k(x, y)$, и обладающий также следующим свойством.

Если φ — точка поля K, определенная кольцом $\mathfrak{o}$, $a = \varphi(x)$, $b = \varphi(y)$ (разумеется, $a = 0$) и $f(X, Y)$ — неприводимый многочлен из $k[X, Y]$, для которого $f(x, y) = 0$, то $D_2 f(a, b) \neq 0$. [*Указание*: записать сначала $K = k(x, z)$, где элемент z — целый над $k[x]$. Пусть $z = z_1, \ldots, z_n$ $(n \geqslant 2)$ — элементы, сопряженные с z над $k(x)$. Продолжить $\mathfrak{o}$ до кольца нормирования $\mathfrak{O}$ поля $k(z_1, \ldots, z_n)$. Рассмотреть

$$z = a_0 + a_1 x + \ldots + a_r x^r + \ldots$$

— разложение z в степенной ряд с $a_i \in k$ и ввести $P_r(x) = a_0 + \ldots + a_r x^r$. Для $i = 1, \ldots, n$ положить

$$y_i = \frac{z_i - P_r(x)}{x^r}.$$

Взяв r достаточно большим, показать, что y_1 не имеет полюса в $\mathfrak{O}$, но $y_2, \ldots, y_n$ имеют полюса в $\mathfrak{O}$. Элементы $y_1, \ldots, y_n$ сопряжены над $k(x)$. Пусть $f(X, Y)$ — неприводимый многочлен пары (x, y) над k. Тогда $f(x, Y) = \psi_n(x) Y^n + \ldots + \psi_0(x)$, где $\psi_i(x) \in k[x]$. Можно также предполагать, что $\psi_i(0) \neq 0$ (так как f неприводим). Записать $f(x, Y)$ в виде

$$f(x, Y) = \psi_n(x)\, y_2 \ldots y_n (Y - y_1)\left(y_2^{-1} Y - 1\right) \ldots \left(y_n^{-1} Y - 1\right).$$

Показать, что $\psi_n(x)\, y_2 \ldots y_n = u$ не имеет полюса в $\mathfrak{O}$. Пусть $\overline{w}$ обозначает класс вычета элемента $w \in \mathfrak{O}$ по модулю максимального идеала в $\mathfrak{O}$. Тогда

$$0 \neq f(\overline{x}, Y) = (-1)^{n-1}\, \overline{u}\, (Y - \overline{y}_1).$$

Положив $y = y_1$, $\overline{y} = b$, найти, что $D_2 f(a, b) = (-1)^{n-1}\, \overline{u} \neq 0$.]

12. Доказать обращение упражнения 11: если $K = k(x, y)$, $f(X, Y)$ — неприводимый многочлен пары (x, y) над k и если элементы $a, b \in k$ таковы, что $f(a, b) = 0$, но $D_2 f(a, b) \neq 0$, то существует однозначно определенное кольцо нормирования $\mathfrak{o}$ поля K с максимальным идеалом $\mathfrak{m}$, такое, что $x \equiv a \pmod{\mathfrak{m}}$ и $y \equiv b \pmod{\mathfrak{m}}$. Кроме того, $\mathfrak{o}/\mathfrak{m} = k$ и $x - a$ — образующая $\mathfrak{m}$. [*Указание*: показать, что если $g(x, y) \in k[x, y]$ — элемент, для которого $g(a, b) = 0$, то $g(x, y) = (x - a) A(x, y)/B(x, y)$, где A, B — такие многочлены, что $B(a, b) \neq 0$. Если $A(a, b) = 0$, то повторить процесс. Показать, что процесс не может повторяться бесконечно и приводит к доказательству требуемого утверждения.]

13. Пусть K — поле характеристики 0, полное относительно некоторого неархимедова абсолютного значения. Показать, что ряды

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots,$$

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$$

сходятся в некоторой окрестности 0. (Основная трудность возникает в случае, когда характеристика поля вычетов равна $p > 0$, так как p делит знаменатели $n!$ и n. Получить выражение для показателя степени, в которой p встречается в $n!$) Доказать, что exp и log дают отображения, обратные друг другу, из окрестности 0 в окрестность 1.

14. Пусть поле K, так же как в предыдущем упражнении, имеет характеристику 0 и является полным относительно некоторого неархимедова абсолютного значения. Показать, что при любом целом $n > 0$ обычное биномиальное разложение для $(1 + x)^{1/n}$ сходится в некоторой окрестности 0. Сделать

это сначала в предположении, что характеристика поля вычетов не делит n; в этом случае доказательство утверждения намного проще.

15. Пусть $\mathbf{Q}_p$ — p-адическое поле. Показать, что $\mathbf{Q}_p$ содержит бесконечно много квадратичных полей вида $\mathbf{Q}(\sqrt{-m})$, где m — целое положительное число.

16. Показать, что кольцо целых p-адических чисел $\mathbf{Z}_p$ компактно. Показать, что группа единиц в $\mathbf{Z}_p$ компактна.

17. Пусть K — поле, полное относительно некоторого дискретного нормирования с конечным полем вычетов и $\mathfrak{o}$ — кольцо элементов поля K, порядки которых $\geqslant 0$. Показать, что $\mathfrak{o}$ компактно. Показать, что группа единиц кольца $\mathfrak{o}$ замкнута в $\mathfrak{o}$ и компактна.

18. Пусть K — поле, полное относительно некоторого дискретного нормирования, и $\mathfrak{o}$ — кольцо целых элементов поля K, причем $\mathfrak{o}$ компактно. Пусть $f_1, f_2, \ldots$ — последовательность многочленов от n переменных с коэффициентами в $\mathfrak{o}$. Предположим, что все эти многочлены имеют степень $\leqslant d$ и что они сходятся к многочлену f (т. е. $|f - f_i| \to 0$ при $i \to \infty$). Показать, что если каждый f_i имеет нуль в $\mathfrak{o}$, то f также имеет нуль в $\mathfrak{o}$. Показать, что если многочлены f_i однородны степени d и каждый f_i имеет нетривиальный нуль в $\mathfrak{o}$, то f имеет нетривиальный нуль в $\mathfrak{o}$. [*Указание*: использовать компактность кольца $\mathfrak{o}$ и для однородного случая — компактность группы единиц в $\mathfrak{o}$.] (О приложениях этого упражнения, а также предложения 21 см статью Lang S., On quasi-algebraic closure, *Ann. Math.*, 1951.)

19. Показать, что если p, p' — два различных простых числа, то поля $\mathbf{Q}_p$ и $\mathbf{Q}_{p'}$ неизоморфны.

20. Доказать, что поле $\mathbf{Q}_p$ содержит все корни $(p-1)$-й степени из единицы. [*Указание*: использовать предложение 21, применив его к многочлену $X^{p-1} - 1$, который разлагается в поле вычетов на множители степени 1.] Показать, что два различных корня $(p-1)$-й степени из единицы не могут быть сравнимы по модулю p.

Часть третья

ЛИНЕЙНАЯ АЛГЕБРА И ПРЕДСТАВЛЕНИЯ

Мы будем заниматься модулями и векторными пространствами, исследуя их структуру с различных точек зрения. Основной темой здесь будет изучение пары, состоящей из модуля и эндоморфизма или кольца эндоморфизмов, и попытки разложить такую пару в прямую сумму компонент, структура которых может быть явно описана. Тема прямой суммы повторяется в каждой главе. Иногда для получения разложения в прямую сумму мы используем двойственность относительно спаривания, а иногда получаем наше разложение непосредственно. Если модуль никак не разлагается в прямую сумму простых компонент, у нас не остается другого выбора, как применить конструкцию Гротендика и посмотреть, что из этого может получиться.

Тема продолжения встречается лишь однажды, в теореме Витта, кратким контрапунктом к теме разложения.

Глава XIII

Матрицы и линейные отображения

На протяжении этой главы R обозначает коммутативное кольцо и E, F — R-модули. Приставку R- перед линейными отображениями и модулями мы будем опускать.

§ 1. Матрицы

Под *матрицей размера* $m \times n$ над R понимается снабженное двумя индексами семейство (a_{ij}) элементов из R ($i = 1, \ldots, m$ и $j = 1, \ldots, n$), обычно записываемое в виде

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & \cdot & \cdot \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}.$$

Мы будем называть a_{ij} *коэффициентами* или *компонентами матрицы*. Матрица размера $1 \times n$ называется *строкой* (размерности, или длины, n), а матрица размера $m \times 1$ — *столбцом* (размерности, или высоты, m).

Сложение для матриц одинакового размера определяется покомпонентно. Если $A = (a_{ij})$ и $B = (b_{ij})$ — матрицы одного и того же размера, то под $A + B$ понимается матрица, у которой ij-компонента равна $a_{ij} + b_{ij}$. Сложение, очевидно, ассоциативно. Произведение матрицы A на элемент $c \in R$ мы определяем как матрицу (ca_{ij}), у которой ij-компонента равна ca_{ij}. Таким образом, множество матриц размера $m \times n$ над R является модулем (т. е. R-модулем).

Произведение AB двух матриц определено лишь при определенных условиях, а именно когда A имеет размер $m \times n$, а B имеет размер $n \times r$, т. е. только в том случае, когда длина строк в A такая же, как и высота столбцов в B. Пусть это имеет место, и пусть $A = (a_{ij})$ и $B = (b_{jk})$. Мы понимаем под AB матрицу размера $m \times r$, у которой ik-компонента равна

$$\sum_{j=1}^{n} a_{ij} b_{jk}.$$

Если для матриц A, B, C произведения AB и BC определены, то определены также произведения $(AB)C$ и $A(BC)$ и выполняется равенство

$$(AB)C = A(BC).$$

Доказывается это тривиально. Пусть $C = (c_{kl})$. Читатель тотчас обнаружит, что il-компонента каждого из предыдущих произведений равна

$$\sum_j \sum_k a_{ij} b_{jk} c_{kl}.$$

Матрица размера $m \times n$ называется *квадратной матрицей*, если $m = n$[1]). Например, матрица размера 1×1 — квадратная матрица; она иногда будет отождествляться с элементом из R, являющимся ее единственной компонентой.

Для данного целого числа $n \geqslant 1$ квадратные матрицы размера $n \times n$ образуют кольцо.

Это опять-таки тривиально проверяется, и проверка предоставляется читателю.

Единичным элементом кольца матриц размера $n \times n$ является матрица

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & & & 0 \\ \cdot & & \cdot & & \cdot \\ \cdot & & & \cdot & \cdot \\ \cdot & & & & \cdot \\ 0 & & & & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

все компоненты которой равны 0, за исключением стоящих на диагонали, которые равны 1. Мы иногда будем писать I вместо I_n. Вообще если $A = (a_{ij})$ — квадратная матрица, то мы будем называть элементы a_{ii} ее *диагональными компонентами*.

Имеется естественный гомоморфизм кольца R в кольцо матриц размера $n \times n$, задаваемый правилом

$$c \longmapsto cI_n.$$

Здесь cI_n — это квадратная матрица размера $n \times n$, у которой все компоненты равны 0, за исключением диагональных компонент, которые равны c. Будем обозначать кольцо матриц размера $n \times n$ над R через $\mathrm{Mat}_n(R)$. Тогда $\mathrm{Mat}_n(R)$ есть алгебра над R (относительно введенного выше гомоморфизма).

Пусть $A = (a_{ij})$ — матрица размера $m \times n$. Назовем *транспонированной* (по отношению) к ней матрицей ${}^tA$ матрицу (a_{ji}) ($j = 1, \dots, n$ и $i = 1, \dots, m$). Тогда ${}^tA$ — матрица размера $n \times m$.

[1]) Ее называют также квадратной матрицей *порядка* n. — *Прим. ред.*

Читатель тотчас проверит, что если A, B — матрицы одинакового размера, то

$$^t(A+B) = {}^tA + {}^tB.$$

Если $c \in R$, то $^t(cA) = c\,{}^tA$. Если матрицы A, B можно перемножить, то произведение $^tB\,{}^tA$ определено и

$$^t(AB) = {}^tB\,{}^tA.$$

Отметим, что операции над матрицами коммутируют с гомоморфизмами. Более точно, пусть $\varphi : R \to R'$ — гомоморфизм колец, и пусть A, B — матрицы над R. Определим φA как матрицу, получаемую применением φ ко всем компонентам A. Тогда

$$\varphi(A+B) = \varphi A + \varphi B, \quad \varphi(AB) = (\varphi A)(\varphi B),$$

$$\varphi(cA) = \varphi(c)\,\varphi A, \quad \varphi({}^tA) = {}^t\varphi(A)$$

Аналогичные замечания будут применимы ко всем нашим дальнейшим рассмотрениям (например, в следующем параграфе).

Пусть $A = (a_{ij})$ — квадратная матрица размера $n \times n$ над коммутативным кольцом R. Определим *след* A формулой

$$\operatorname{tr}(A) = \sum_{i=1}^{n} a_{ii};$$

другими словами, след есть сумма диагональных элементов. *Для любых двух матриц A, B размера $n \times n$*

$$\operatorname{tr}(AB) = \operatorname{tr}(BA).$$

Действительно, если $A = (a_{ij})$ и $B = (b_{ij})$, то

$$\operatorname{tr}(AB) = \sum_{i}\sum_{\nu} a_{i\nu} b_{\nu i} = \operatorname{tr}(BA).$$

В качестве приложения заметим, что *если B — обратимая матрица размера $n \times n$* (т. е. является единицей в кольце матриц), *то*

$$\operatorname{tr}(B^{-1}AB) = \operatorname{tr}(A).$$

Действительно, $\operatorname{tr}(B^{-1}AB) = \operatorname{tr}(ABB^{-1}) = \operatorname{tr}(A)$.

§ 2. Ранг матрицы

Пусть k — поле и A — матрица размера $m \times n$ над k. Под *строчным рангом* A мы будем понимать максимальное число линейно независимых строк матрицы A, а под *столбцовым рангом* A — максимальное число линейно независимых столбцов A. Таким образом, эти ранги представляют собой размерности векторных пространств, порожденных соответственно строками A и столбцами A. Мы утверждаем, что эти ранги равны одному и тому же числу, и это число мы назовем *рангом* A.

Действительно, пусть $A^1, \ldots, A^n$ — столбцы A и $A_1, \ldots, A_m$ — строки A. Пусть ${}^tX = (x_1, \ldots, x_m)$ — строки с компонентами $x_i \in k$. Имеем линейное отображение

$$X \longmapsto x_1A_1 + \ldots + x_mA_m$$

пространства $k^{(m)}$ на пространство, порожденное строками. Обозначим через W его ядро. Тогда W будет подпространством в $k^{(m)}$ и

$$\dim W + \text{строчный ранг} = m.$$

Пусть Y — столбец размерности m. Тогда отображение

$$(X, Y) \longmapsto {}^tXY \equiv X \cdot Y$$

является билинейным отображением в k, если матрицу ${}^tXY$ размера 1×1 рассматривать как элемент из k. Заметим, что W ортогонально пространству столбцов $A^1, \ldots, A^n$, т. е. это есть пространство всех X, для которых $X \cdot A^j = 0$ при $j = 1, \ldots, n$. В силу теоремы двойственности из гл. III мы знаем, что пространство $k^{(m)}$ дуально самому себе относительно спаривания

$$(X, Y) \longmapsto X \cdot Y$$

и что $k^{(m)}/W$ дуально пространству, порожденному столбцами $A^1, \ldots, A^n$. Следовательно,

$$\dim k^{(m)}/W = \text{столбцовый ранг},$$

или

$$\dim W + \text{столбцовый ранг} = m.$$

Отсюда заключаем, что

$$\text{столбцовый ранг} = \text{строчный ранг},$$

что и требовалось установить.

Отметим, что W можно рассматривать как пространство решений системы из n линейных уравнений

$$x_1A_1 + \ldots + x_mA_m = 0$$

с m неизвестными $x_1, \ldots, x_m$. Действительно, если мы запишем предыдущее векторное уравнение через координаты, то получим обычную систему из n линейных уравнений. Предоставляем читателю проделать это, если он пожелает.

§ 3. Матрицы и линейные отображения

Пусть E — модуль, и пусть существует базис $\mathscr{B} = \{\xi_1, \ldots, \xi_n\}$ для E над R. Это означает, что всякий элемент из E имеет однозначное представление в виде линейной комбинации

$$x = x_1\xi_1 + \ldots + x_n\xi_n,$$

где $x_i \in R$. Мы будем называть $(x_1, \ldots, x_n)$ *компонентами* x относительно этого базиса. Упорядоченный набор из n элементов можно

рассматривать как строку. Будем обозначать через X столбец, полученный транспонированием строки $(x_1, \ldots, x_n)$, называя также X *столбцом элемента x относительно заданного базиса.*

Заметим, что если $\{\xi_1', \ldots, \xi_m'\}$ — другой базис E над R, то $m = n$. Действительно, пусть $\mathfrak{p}$ — некоторый максимальный идеал в R. Тогда $E/\mathfrak{p}E$ — векторное пространство над полем $R/\mathfrak{p}R$ и непосредственно ясно, что если обозначить через $\overline{\xi}_i$ класс вычетов элемента $\xi_i \bmod \mathfrak{p}E$, то $\{\overline{\xi}_1, \ldots, \overline{\xi}_n\}$ будет базисом для $E/\mathfrak{p}E$ над $R/\mathfrak{p}R$. Следовательно, n равно также размерности этого векторного пространства, а инвариантность мощности базисов векторных пространств над полями нам известна. Таким образом, $m = n$. Мы будем называть n *размерностью* модуля E над R.

Будем рассматривать $R^{(n)}$ как модуль столбцов высоты n. Это свободный модуль размерности n над R. Он имеет базис, состоящий из единичных векторов $e^1, \ldots, e^n$, для которых в строке

$$^t e^i = (0, \ldots, 0, 1, 0, \ldots, 0)$$

все компоненты равны 0, за исключением i-й компоненты, равной 1.

Матрица A размера $m \times n$ задает линейное отображение

$$L_A : R^{(n)} \to R^{(m)}$$

по правилу

$$X \longmapsto AX.$$

Действительно, $A(X + Y) = AX + AY$ и $A(cX) = cAX$ для столбцов X, Y и $c \in R$.

Предыдущие рассмотрения могут быть распространены на несколько более общую ситуацию, которая может оказаться очень полезной. Пусть E — абелева группа, причем R — коммутативное подкольцо в

$$\mathrm{End}_{\mathbf{Z}}(E) = \mathrm{Hom}_{\mathbf{Z}}(E, E).$$

Тогда E есть R-модуль. Кроме того, если A — матрица размера $m \times n$ над R, то получаем линейное отображение

$$L_A : E^{(n)} \to E^{(m)},$$

определяемое по правилу, аналогичному указанному выше, а именно $X \longmapsto AX$. Это интерпретируется очевидным образом как обычное умножение матриц. Если $A = (a_{ij})$ и X — столбец элементов из E, то

$$AX = \begin{pmatrix} a_{11} \ldots a_{1n} \\ \ldots \\ a_{m1} \ldots a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \cdot \\ \cdot \\ \cdot \\ y_n \end{pmatrix},$$

где $y_i = \sum_{j=1}^{n} a_{ij} x_j$.

Если A, B — матрицы над R, для которых определено произведение, то для любого $c \in R$ имеем

$$L_{AB} = L_A L_B \text{ и } L_{cA} = cL_A.$$

Таким образом,

$$A(BX) = (AB)X.$$

Произвольное коммутативное кольцо R можно рассматривать как модуль над собой. Тем самым мы снова приходим к частному случаю отображения $R^{(n)}$ в $R^{(m)}$. Кроме того, если E — модуль над R, то R можно рассматривать как кольцо эндоморфизмов E.

Предложение 1. *Пусть E — свободный модуль над R с базисом $\{x_1, \ldots, x_n\}$, $y_1, \ldots, y_n$ — некоторые элементы из E и A — такая матрица над R, что*

$$A\begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \cdot \\ \cdot \\ \cdot \\ y_n \end{pmatrix}.$$

Тогда $\{y_1, \ldots, y_n\}$ является базисом в E в том и только в том случае, если матрица A обратима.

Доказательство. Пусть X, Y — столбцы из наших элементов, т. е. $AX = Y$. Предположим, что Y — базис. Тогда существует матрица C над R, для которой $CY = X$, так что $CAX = X$, откуда $CA = I$ и аналогично $AC = I$; следовательно, A обратима. Обратно, предположим, что A обратима. Если бы $y_1, \ldots, y_n$ были связаны соотношением

$$b_1 y_1 + \ldots + b_n y_n = 0$$

с $b_i \in R$, то, придав этому соотношению матричную форму

$$BY = 0,$$

где B — строка $(b_1, \ldots, b_n)$, и подставив вместо Y его выражение $Y = AX$, мы получили бы, что $B(AX) = (BA)X = 0$. Но $\{x_1, \ldots, x_n\}$ — базис. Следовательно, $BA = 0$, а значит, и $B = (BA)A^{-1} = B(AA^{-1}) = 0$. Таким образом, $b_1 = \ldots = b_n = 0$ и компоненты Y линейно независимы, что доказывает наше предложение.

Отметим, что в доказательстве второй половины предложения 1 использовалось лишь существование такой матрицы C, что $CA = I$. Таким образом получаем

Следствие. *Если для матрицы A существует матрица C, такая, что $CA = I$ или $AC = I$, то матрица A обратима и $C = A^{-1}$.*

Возвратимся к нашей ситуации модулей над произвольным коммутативным кольцом R.

Пусть E, F — модули. Мы увидим, как можно линейному отображению сопоставить матрицу, если только заданы базисы в E и F. Предположим, что модули E, F — свободные с базисами $\mathscr{B} = \{\xi_1, \ldots, \xi_n\}$ и $\mathscr{B}' = \{\xi_1', \ldots, \xi_n'\}$ соответственно. Пусть

$$f\colon E \to F$$

— линейное отображение. Существуют однозначно определенные элементы $a_{ij} \in R$, такие, что

$$f(\xi_1) = a_{11}\xi_1' + \ldots + a_{m1}\xi_m',$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$f(\xi_n) = a_{1n}\xi_1' + \ldots + a_{mn}\xi_m^1,$$

или, иначе,

$$f(\xi_j) = \sum_{i=1}^{m} a_{ij}\xi_i'.$$

(Отметим, что сумма берется по первому индексу.)
Полагаем

$$M_{\mathscr{B}'}^{\mathscr{B}}(f) = (a_{ij}).$$

Если элемент $x = x_1\xi_1 + \ldots + x_n\xi_n$ выражен через базис, то мы обозначаем столбец X компонент элемента x через $M_{\mathscr{B}}(x)$. Имеем

$$M_{\mathscr{B}'}(f(x)) = M_{\mathscr{B}'}^{\mathscr{B}}(f)\, M_{\mathscr{B}}(x).$$

Другими словами, если X' — столбец компонент $f(x)$ и M — матрица, ассоциированная с f, то $X' = MX$. Таким образом, действие линейного отображения выражается произведением матриц и мы имеем $f = L_M$.

Предложение 2. *Пусть E, F, D — модули и $\mathscr{B}$, $\mathscr{B}'$, $\mathscr{B}''$ — конечные базисы в E, F, D соответственно. Пусть*

$$E \xrightarrow{f} F \xrightarrow{g} D$$

— линейные отображения. Тогда

$$M_{\mathscr{B}''}^{\mathscr{B}}(g \circ f) = M_{\mathscr{B}''}^{\mathscr{B}'}(g)\, M_{\mathscr{B}'}^{\mathscr{B}}(f).$$

Доказательство. Пусть A и B — матрицы, ассоциированные относительно заданных базисов с отображениями f, g соответственно. Если X — столбец, ассоциированный с $x \in E$, то столбец, ассоциированный с $g(f(x))$, равен $B(AX) = (BA)X$. Следовательно, BA есть матрица, ассоциированная с $g \circ f$. Это доказывает то, что нужно.

Следствие 1. *Пусть* $E = F$. *Тогда*

$$M_{\mathscr{B}'}^{\mathscr{B}}(\mathrm{id})\, M_{\mathscr{B}}^{\mathscr{B}'}(\mathrm{id}) = M_{\mathscr{B}'}^{\mathscr{B}'}(\mathrm{id}) = I.$$

Всякая матрица $M_{\mathscr{B}'}^{\mathscr{B}}(\mathrm{id})$ обратима.

Доказательство. Очевидно.

Следствие 2. *Пусть* $N = M^{\mathscr{B}}(\mathrm{id})$. *Тогда*

$$M_{\mathscr{B}'}^{\mathscr{B}'}(f) = M_{\mathscr{B}'}^{\mathscr{B}}(\mathrm{id}) M_{\mathscr{B}}^{\mathscr{B}}(f)\, M_{\mathscr{B}}^{\mathscr{B}'}(\mathrm{id}) = N M_{\mathscr{B}}^{\mathscr{B}}(f)\, N^{-1}.$$

Доказательство. Очевидно.

Следствие 3. *Пусть* E *— свободный модуль размерности* n *над* R *и* $\mathscr{B}$ *— некоторый его базис. Отображение*

$$f \longmapsto M_{\mathscr{B}}^{\mathscr{B}}(f)$$

является изоморфизмом кольца всех эндоморфизмов модуля E *на кольцо матриц размера* $n \times n$ *над* R. *Фактически это отображение является изоморфизмом алгебр над* R.

Мы будем называть $M_{\mathscr{B}}^{\mathscr{B}}(f)$ *матрицей, ассоциированной с* f *относительно базиса* $\mathscr{B}$.

Пусть E — свободный модуль размерности n над R. Под $GL(E)$, или $\mathrm{Aut}_R(E)$ понимается группа линейных автоморфизмов модуля E. Это—группа единиц в $\mathrm{End}_R(E)$. Под $GL_n(R)$ понимают группу обратимых матриц размера $n \times n$ над R. Как только выбран базис для E над R, мы получаем изоморфизм групп

$$GL(E) \longleftrightarrow GL_n(R)$$

относительно этого базиса.

Пусть

$$f\colon E \to E$$

— некоторое линейное отображение. Выберем какой-нибудь базис $\mathscr{B}$ и рассмотрим матрицу M, ассоциированную с f относительно $\mathscr{B}$. *След* f полагаем по определению равным следу M, т. е.

$$\mathrm{tr}(f) = \mathrm{tr}(M).$$

Если M' — матрица f относительно какого-то другого базиса, то существует *обратимая матрица* N, такая, что $M' = N^{-1}MN$, и, следовательно, след не зависит от выбора базиса.

§ 4. Определители

Пусть $E_1, \ldots, E_n$, F — модули. Отображение

$$f\colon E_1 \times \ldots \times E_n \to F$$

называется *R-полилинейным* (или просто полилинейным), если оно линейно по каждой переменной, т. е. если для всякого индекса i и элементов $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n, x_j \in E_j$, отображение

$$x \longmapsto f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n)$$

является линейным отображением E_i в F.

Полилинейное отображение, определенное на n-кратном произведении, называется также *n-линейным*. Если $E_1 = \ldots = E_n = E$, то мы будем говорить, что f — *полилинейное отображение на* E, вместо того, чтобы говорить, что оно полилинейно на $E^{(n)}$.

Пусть f—n-линейное отображение. Выбрав два индекса i, j, $i \neq j$, а потом зафиксировав все переменные, кроме i-й и j-й, мы можем рассматривать f как билинейное отображение на $E_i \times E_j$.

Предположим, что $E_1 = \ldots = E_n = E$. Говорят, что полилинейное отображение f является *знакопеременным*, если $f(x_1, \ldots, x_n) = 0$, всякий раз как существует такой индекс i, $1 \leqslant i \leqslant n-1$, что $x_i = x_{i+1}$ (другими словами, когда два соседних элемента равны).

Предложение 3. *Пусть f — n-линейное знакопеременное отображение на E и $x_1, \ldots, x_n \in E$. Тогда*

$$f(\ldots, x_i, x_{i+1}, \ldots) = -f(\ldots, x_{i+1}, x_i, \ldots).$$

Другими словами, когда мы переставляем два соседних аргумента, значение f меняет знак. Если $x_i = x_j$ для $i \neq j$, то $f(x_1, \ldots, \ldots, x_n) = 0$.

Доказательство. Сосредотачивая свое внимание на множителях, стоящих на i-м и j-м месте, мы можем считать, что f в нашем первом утверждении билинейно. Тогда для всех x, $y \in E$ имеем

$$0 = f(x+y, x+y) = f(x, y) + f(y, x).$$

Этим и доказано то, что нужно, а именно что $f(y, x) = -f(x, y)$. Что касается второго утверждения, то мы можем последовательно переставлять соседние аргументы f до тех пор, пока имеющиеся по условию два равных аргумента не станут рядом. Это показывает, что $f(x_1, \ldots, x_n) = 0$, когда $x_i = x_j$, $i \neq j$.

Следствие. *Пусть f—n-линейное знакопеременное отображение на E. Пусть $x_1, \ldots, x_n \in E$, $i \neq j$ и $a \in R$. Тогда значение f на $(x_1, \ldots, x_n)$ не изменится, если мы заменим x_i на $x_i + ax_j$, а все другие компоненты оставим неизменными.*

Доказательство. Очевидно.

Полилинейное знакопеременное отображение, принимающее свои значения в R, называется полилинейной *знакопеременной формой*.

Нам неоднократно придется вычислять значения полилинейного знакопеременного отображения на линейных комбинациях элементов из E.

Положим

$$w_1 = a_{11}v_1 + \ldots + a_{1n}v_n,$$
$$\ldots\ldots\ldots\ldots$$
$$w_n = a_{n1}v_1 + \ldots + a_{nn}v_n.$$

Пусть f — n-линейное знакопеременное отображение на E. Разлагая правую часть равенства

$$f(w_1, \ldots, w_n) = f(a_{11}v_1 + \ldots + a_{1n}v_n, \ldots, a_{n-1}v_1 + \ldots + a_{nn}v_n),$$

мы получим сумму членов вида

$$a_{1,\,\sigma(1)} \ldots a_{n,\,\sigma(n)} f(v_{\sigma(1)}, \ldots, v_{\sigma(n)}),$$

где σ пробегает множество произвольных отображений набора $\{1, \ldots, n\}$ в себя. Если σ не биективно (т. е. не является перестановкой), то два аргумента $v_{\sigma(i)}$ и $v_{\sigma(j)}$ совпадут при $i \neq j$ и соответствующий член будет равен 0. Следовательно, мы можем брать нашу сумму лишь по перестановкам σ. Перемещая элементы $(v_{\sigma(1)}, \ldots, v_{\sigma(n)})$ обратно, к их стандартному порядку, и используя предложение 3, мы приходим к следующему разложению.

Лемма. *Пусть $w_1, \ldots, w_n$ обозначают то же, что и выше. Тогда*

$$f(w_1, \ldots, w_n) = \sum_{\sigma} \varepsilon(\sigma)\, a_{1,\,\sigma(1)} \ldots a_{n,\,\sigma(n)} f(v_1, \ldots, v_n),$$

где сумма берется по всем перестановкам σ множества $\{1, \ldots, n\}$ и $\varepsilon(\sigma)$ есть знак перестановки.

При рассмотрении определителей я буду следовать изложению Артина в его книге „Galois Theory".

Под *определителем* размера $n \times n$ мы будем понимать отображение

$$\det\colon \operatorname{Mat}_n(R) \to R,$$

обозначаемое также через

$$D\colon \operatorname{Mat}_n(R) \to R,$$

которое обладает свойством $D(I) = 1$ и является, если рассматривать его как функцию от столбцов $A^1, \ldots, A^n$ матрицы A, полилинейным знакопеременным отображением. В этой главе для обозначения определителей мы будем использовать главным образом букву D.

Позднее мы докажем, что определители существуют. А сейчас мы выведем их свойства.

Правило Крамера. *Пусть $A^1, \ldots, A^n$ — столбцы размерности n, и пусть элементы $x_1, \ldots, x_n \in R$ таковы, что*

$$x_1A^1 + \ldots + x_nA^n = B$$

для некоторого столбца B. Тогда для всякого i имеем

$$x_i D(A^1, \ldots, A^n) = D(A^1, \ldots, B, \ldots, A^n),$$

где в правой части равенства B стоит на i-м месте.

Доказательство. Пусть, скажем, $i=1$. Напишем разложение

$$D(B, A^2, \ldots, A^n) = \sum_{j=1}^{n} x_j D(A^j, A^2, \ldots, A^n)$$

и применим предложение 3 (все члены в правой части равны 0, за исключением одного, содержащего x_1).

Следствие. *Предположим, что R — поле. Тогда $A^1, \ldots, A^n$ линейно зависимы в том и только в том случае, если $D(A^1, \ldots, A^n) = 0$*

Доказательство. Пусть мы имеем соотношение

$$x_1 A_1 + \ldots + x_n A^n = 0,$$

где $x_i \in R$. Тогда $x_i D(A) = 0$ для всех i. Если некоторый коэффициент $x_i \neq 0$, то $D(A) = 0$. Обратно, предположим, что $A^1, \ldots, A^n$ линейно независимы. Тогда мы можем представить единичные векторы $e^1, \ldots, e^n$ (см. § 3) в виде линейных комбинаций

$$e^1 = b_{11} A^1 + \ldots + b_{1n} A^n,$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$e^n = b_{n1} A^1 + \ldots + b_{nn} A^n,$$

где $b_{ij} \in R$. Но

$$1 = D(e^1, \ldots, e^n).$$

Ввиду предыдущей леммы последнее выражение может быть разложено в сумму членов, содержащих $D(A^1, \ldots, A^n)$, и следовательно, $D(A)$ не может быть равно 0.

Предложение 4. *Если определители существуют, то они определены однозначно. Если, далее, $A^1, \ldots, A^n$ — столбцы размерности n матрицы $A = (a_{ij})$,* то

$$D(A^1, \ldots, A^n) = \sum_{\sigma} \varepsilon(\sigma)\, a_{\sigma(1),1} \ldots a_{\sigma(n),n},$$

где сумма берется по всем перестановкам σ множества $\{1, \ldots, n\}$ и $\varepsilon(\sigma)$ — знак перестановки.

Доказательство. Пусть $e^1, \ldots, e^n$, — как обычно, единичные векторы. Мы можем записать

$$A^1 = a_{11} e^1 + \ldots + a_{n1} e^n,$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$A^n = a_{1n} e^1 + \ldots + a_{nn} e^n.$$

Поэтому

$$D(A^1, \ldots, A^n) = \sum_{\sigma} \varepsilon(\sigma)\, a_{\sigma(1),1} \ldots a_{\sigma(n),n}$$

в силу леммы. Это доказывает, что значение определителя однозначно определено и задается указанной формулой.

Следствие. *Пусть* φ: $R \to R'$ *— гомоморфизм в коммутативное кольцо. Если* A *— квадратная матрица над* R *и* φA *— матрица, полученная применением* φ *к каждой компоненте* A, *то*

$$\varphi(D(A)) = D(\varphi A).$$

Доказательство. Применим φ к выражению из предложения 4.

Предложение 5. *Для всякой квадратной матрицы* A *над* R

$$D(A) = D({}^tA).$$

Доказательство. В произведении

$$a_{\sigma(1),1} \ldots a_{\sigma(n),n}$$

каждое целое число k от 1 до n встречается среди чисел $\sigma(1), \ldots, \sigma(n)$ точно один раз. Следовательно, мы можем переписать это произведение в виде

$$a_{1,\sigma^{-1}(1)} \ldots a_{n,\sigma^{-1}(n)},$$

а так как $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$, то сумма из предложения 4 запишется в виде

$$\sum_{\sigma} \varepsilon(\sigma^{-1})\, a_{1,\sigma^{-1}(1)} \ldots a_{n,\sigma^{-1}(n)}.$$

В этой сумме каждый член соответствует перестановке σ. Однако, когда σ пробегает все перестановки, то же самое происходит и с σ^{-1}. Следовательно, наша сумма равна

$$\sum_{\sigma} \varepsilon(\sigma)\, a_{1,\sigma(1)} \ldots a_{n,\sigma(n)},$$

а это есть не что иное, как $D({}^tA)$, что и требовалось показать.

Следствие, *Определитель является полилинейным и знакопеременным по отношению к строкам матрицы*

Теперь мы докажем существование и одновременно одно дополнительное важное свойство определителей.

При $n = 1$ полагаем $D(a) = a$ для любых $a \in R$.

Предположим, что мы уже доказали существование определителей размера $m \times m$ для всех целых чисел $m < n$ $(n \geqslant 2)$. Пусть

A — матрица размера $n \times n$ над R, $A = (a_{ij})$. Обозначим через A_{ij} матрицу размера $(n-1) \times (n-1)$, полученную из A вычеркиванием i-й строки и j-го столбца. Пусть i — фиксированное целое число $1 \leqslant i \leqslant n$. Определяем индуктивно

$$D(A) = (-1)^{i+1} a_{i1} D(A_{i1}) + \ldots + (-1)^{i+n} a_{in} D(A_{in}).$$

(Это выражение известно как *разложение определителя D по i-й строке*.) Докажем, что D удовлетворяет определению определителя.

Рассмотрим D как функцию k-го столбца. Возьмем произвольный член

$$(-1)^{i+j} a_{ij} D(A_{ij}).$$

Если $j \neq k$, то a_{ij} не зависит от k-го столбца, а $D(A_{ij})$ зависит от k-го столбца линейно. Если $j = k$, то a_{ij} зависит линейно от k-го столбца, а $D(A_{ij})$ от k-го столбца не зависит. Так как определитель $D(A)$ есть сумма таких членов, то он зависит от k-го столбца линейно и, таким образом, $D(A)$ полилинеен.

Далее, предположим, что два соседних столбца равны, скажем, $A^k = A^{k+1}$. Пусть индекс $j \neq k$ и $\neq k+1$. Тогда матрица A_{ij} имеет два соседних равных столбца и, следовательно, ее определитель равен 0. Таким образом, члены, соответствующие индексу $j \neq k$ или $k+1$, дают нулевой вклад в $D(A)$. Остальные два члена могут быть записаны так:

$$(-1)^{i+k} a_{ik} D(A_{ik}) + (-1)^{i+k+1} a_{i,\,k+1} D(A_{i,\,k+1}).$$

Матрицы A_{ik} и $A_{i,\,k+1}$ равны ввиду предположения, что k-й столбец A равен $(k+1)$-му столбцу. Аналогично $a_{ik} = a_{i,\,k+1}$. Следовательно, эти два члена сокращаются, поскольку они имеют противоположные знаки. Это доказывает, что наша форма — знакопеременная, и дает

Предложение 6. *Определители существуют и удовлетворяют правилу разложения по строкам и столбцам.*

[Для разложения по столбцам мы используем тот факт, что $D(A) = D^t(A)$.]

Теорема 1. *Пусть E — модуль над R, $v_1, \ldots, v_n$ — элементы из E и $A = (a_{ij})$ — матрица над R. Положим*

$$A \begin{pmatrix} v_1 \\ \cdot \\ \cdot \\ \cdot \\ v_n \end{pmatrix} = \begin{pmatrix} w_1 \\ \cdot \\ \cdot \\ \cdot \\ w_n \end{pmatrix}.$$

Пусть, далее, Δ — некоторое n-линейное знакопеременное отображение на E. Тогда

$$\Delta(w_1, \ldots, w_n) = D(A)\Delta(v_1, \ldots, v_n).$$

Доказательство. Разложим

$$\Delta(a_{11}v_1 + \ldots + a_{1n}v_n, \ldots, a_{n1}v_1 + \ldots + a_{nn}v_n)$$

и, приняв во внимание, что $D(A) = D({}^tA)$, получим в точности то, что требовалось.

Пусть E, F — модули, и пусть $L_a^n(E, F)$ обозначает множество всех n-линейных знакопеременных отображений E в F. Если $F = R$, то мы также будем писать $L_a^n(E, R) = L_a^n(E)$. Ясно, что $L_a^n(E, F)$ — модуль над R, т. е. это множество замкнуто относительно сложения и умножения на элементы из R.

Следствие 1. *Пусть E — свободный модуль над R, $\{v_1, \ldots, v_n\}$ — некоторый его базис. Пусть, далее, F — произвольный модуль и $w \in F$. Тогда существует единственное n-линейное знакопеременное отображение*

$$\Delta_w : E \times \ldots \times E \to F,$$

такое, что $\Delta_w(v_1, \ldots, v_n) = w$.

Доказательство. Не теряя общности, мы можем предполагать, что $E = R^n$, и если $A^1, \ldots, A^n$ — столбцы, то мы полагаем $\Delta_w(A^1, \ldots, A^n) = D(A)w$. Тогда Δ_w, очевидно, обладает требуемыми свойствами.

Следствие 2. *Если модуль E свободен над R и обладает базисом, состоящим из n элементов, то модуль $L_a^n(E)$ свободен над R и обладает базисом, состоящим из одного элемента.*

Доказательство. Пусть Δ_1 — полилинейное знакопеременное отображение, принимающее значение 1 на базисе $\{v_1, \ldots, v_n\}$. Любой элемент $\varphi \in L_a^n(E)$ может быть записан единственным образом в виде $c\Delta_1$ для некоторого $c \in R$, а именно для $c = \varphi(v_1, \ldots, v_n)$. Это доказывает то, что нужно.

Любые два базиса для $L_a^n(E)$ в предыдущем следствии отличаются множителем, являющимся единицей в R. Другими словами, если Δ — базис $L_a^n(E)$, то $\Delta = c\Delta_1 = \Delta_c$ для некоторого $c \in R$, и c должно быть единицей. Базис Δ_1 зависит, конечно, от выбора базиса для E. Когда мы рассматриваем $R^{(n)}$, наш определитель D есть в точности Δ_1 по отношению к стандартному базису, состоящему из единичных векторов $e^1, \ldots, e^n$.

Иногда бывает удобно говорить, что любой базис в $L_a^n(E)$ является *определителем* на E. В этом случае следствие из правила Крамера может быть сформулировано несколько иначе.

Следствие 3. *Пусть R — поле, E — векторное пространство размерности n и Δ — произвольный определитель на E. Пусть $v_1, \ldots, v_n \in E$. Для того чтобы $\{v_1, \ldots, v_n\}$ было базисом E, необходимо и достаточно, чтобы*

$$\Delta(v_1, \ldots, v_n) \neq 0.$$

Предложение 7. Для любых матриц A, B размера $n \times n$ над R

$$D(AB) = D(A)\,D(B).$$

Доказательство. Это предложение является в действительности следствием теоремы 1. Возьмем в качестве $v_1, \ldots, v_n$ единичные векторы $e^1, \ldots, e^n$ и рассмотрим

$$AB \begin{pmatrix} e^1 \\ \cdot \\ \cdot \\ \cdot \\ e^n \end{pmatrix} = \begin{pmatrix} w_1 \\ \cdot \\ \cdot \\ \cdot \\ w_n \end{pmatrix}.$$

Получим

$$D(w_1, \ldots, w_n) = D(AB)\,D(e^1, \ldots, e^n).$$

С другой стороны, пользуясь ассоциативностью и применяя теорему 1 дважды, имеем

$$D(w_1, \ldots, w_n) = D(A)\,D(B)\,D(e^1, \ldots, e^n).$$

Так как $D(e^1, \ldots, e^n) = 1$, то получаем наше предложение.

Пусть $A = (a_{ij})$ — матрица размера $n \times n$ над R. Введем матрицу

$$\tilde{A} = (b_{ij}),$$

в которой

$$b_{ij} = (-1)^{i+j} D(A_{ji}).$$

(Обратите внимание, что индексы переставлены!)

Предложение 8. *Пусть $d = D(A)$. Тогда $A\tilde{A} = \tilde{A}A = dI$. Определитель $D(A)$ обратим в R в том и только в том случае, если матрица A обратима, и в этом случае*

$$A^{-1} = \frac{1}{d}\,\tilde{A}.$$

Доказательство. Для любой пары индексов i, k ik-компонента матрицы $A\tilde{A}$ равна

$$a_{i1}b_{1k} + a_{i2}b_{2k} + \ldots + a_{in}b_{nk} =$$
$$= a_{i1}(-1)^{k+1}D(A_{k1}) + \ldots + a_{in}(-1)^{k+n}D(A_{kn}).$$

Если $i = k$, то сумма является просто разложением определителя по i-й строке и, следовательно, равна d. Если $i \neq k$, то обозначим через $\bar{A}$ матрицу, полученную из A заменой k-й строки на i-ю строку с сохранением всех остальных элементов неизменными. Если мы вычеркнем из $\bar{A}$ k-ю строку и j-й столбец, то получим ту же самую матрицу, что и вычеркивая k-ю строку и j-й столбец из матрицы A. Таким образом,

$$\bar{A}_{kj} = A_{kj}$$

и наша предыдущая сумма может быть записана в виде

$$a_{i1}(-1)^{k+1}D(\bar{A}_{k1}) + \ldots + a_{in}(-1)^{k+n}D(\bar{A}_{kn}).$$

Это есть разложение определителя $\bar{A}$ по i-й строке. Так как $D(\bar{A}) = 0$, то наша сумма равна 0. Мы таким образом доказали, что ik-компонента матрицы $A\tilde{A}$ равна d, если $i = k$ (т. е. если это диагональная компонента), и равна 0 в противном случае. Это доказывает, что $A\tilde{A} = dI$. С другой стороны, из определений мы тотчас заключаем, что ${}^t\tilde{A} = \widetilde{{}^tA}$. Поэтому

$${}^t(\tilde{A}A) = {}^tA\,{}^t\tilde{A} = {}^tA\widetilde{{}^tA} = dI,$$

т. е. и $\tilde{A}A = dI$, поскольку ${}^t(dI) = dI$. Когда d — единица в R, матрица A обратима и обратной для нее служит матрица $D^{-1}\tilde{A}$. Обратно, если A обратима и $AA^{-1} = I$, то $d(A)D(A^{-1}) = 1$ и, следовательно, элемент $D(A)$ обратим, что и требовалось показать.

Следствие. *Пусть F — произвольный R-модуль, $w_1, \ldots, w_n$ — элементы из F и $A = (a_{ij})$ — матрица размера $n \times n$ над R. Предположим, что*

$$a_{11}w_1 + \ldots + a_{1n}w_n = 0,$$
$$\ldots\ldots\ldots\ldots$$
$$a_{n1}w_1 + \ldots + a_{nn}w_n = 0.$$

Тогда $D(A)w_i = 0$ для всех i. В частности, если F порождается элементами $w_1, \ldots, w_n$, то $D(A)F = 0$.

Доказательство. Это вытекает из замечаний § 3. Умножая на $\tilde{A}$, находим

$$\tilde{A}A\begin{pmatrix} w_1 \\ \cdot \\ \cdot \\ \cdot \\ w_n \end{pmatrix} = d\begin{pmatrix} w_1 \\ \cdot \\ \cdot \\ \cdot \\ w_n \end{pmatrix},$$

где $d = D(A)$.

Предложение 9. *Пусть E, F — свободные модули размерности n над R с базисами $\mathscr{B}$ и $\mathscr{B}'$ соответственно. Линейное отображение $f: E \to F$ тогда и только тогда является изоморфизмом, когда определитель ассоциированной с ним матрицы $M_{\mathscr{B}'}^{\mathscr{B}}(f)$ есть единица в R.*

Доказательство. Пусть $A = M_{\mathscr{B}'}^{\mathscr{B}}(f)$. По определению f будет изоморфизмом в том и только в том случае, если существует линейное отображение $g: F \to E$, такое, что $g \circ f = \mathrm{id}$ и $f \circ g = \mathrm{id}$. Если f — изоморфизм и $B = M_{\mathscr{B}}^{\mathscr{B}'}(g)$, то $AB = BA = I$. Беря определитель произведения, заключаем, что элемент $D(A)$ обратим в R. Обратно, если $D(A)$ — единица, то в силу предложения 7 мы можем определить матрицу A^{-1}. Эта матрица ассоциирована с некоторым линейным отображением $g: F \to E$, обратным к f, что и требовалось установить.

Наконец, введем понятие определителя эндоморфизма.

Пусть E — свободный модуль над R и $\mathscr{B}$ — его базис. Пусть $f: E \to E$ — эндоморфизм модуля E. Положим

$$M = M_{\mathscr{B}}^{\mathscr{B}}(f).$$

Если $\mathscr{B}'$ — другой базис для E и $M' = M_{\mathscr{B}'}^{\mathscr{B}'}(f)$, то существует обратимая матрица N, такая, что

$$M' = NMN^{-1}.$$

Беря определитель, мы видим, что $D(M') = D(M)$. Следовательно, этот определитель не зависит от выбора базиса; он будет называться *определителем линейного отображения f*. Ниже мы дадим характеризацию этого определителя, не зависящую от выбора базиса.

Пусть E — произвольный модуль. Мы можем рассматривать $L_a^n(E)$ как функтор от переменной E (контравариантный). Далее, мы можем рассматривать $L_a^n(E, F)$ как функтор от двух переменных, контравариантный по первой и ковариантный по второй переменной. Действительно, пусть

$$E' \xrightarrow{f} E$$

— линейное отображение. Всякому полилинейному отображению $\varphi\colon E^{(n)} \to F$ можно сопоставить композицию $\varphi \circ f^{(n)}$,

$$E' \times \ldots \times E' \xrightarrow{f^{(n)}} E \times \ldots \times E \xrightarrow{\varphi} F,$$

где $f^{(n)}$ есть произведение f на себя n раз. Отображение

$$L_a^n(f)\colon L_a^n(E, F) \to L_a^n(E', F),$$

задаваемое правилом

$$\varphi \mapsto \varphi \circ f^{(n)},$$

очевидно, линейно, и оно определяет наш функтор. Мы будем иногда писать f^* вместо $L_a^n(f)$.

Рассматривая, в частности, случай, когда $E = E'$ и $F = R$, получим индуцированное отображение

$$f^*\colon L_a^n(E) \to L_a^n(E).$$

Предложение 10. *Пусть E — свободный модуль размерности n над R и Δ — базис в $L_a^n(E)$. Пусть $f\colon E \to E$ — эндоморфизм модуля E. Тогда*

$$f^*\Delta = D(f)\Delta.$$

Доказательство. Это непосредственное следствие теоремы 1. А именно пусть A (или ${}^tA$) — матрица эндоморфизма f относительно некоторого базиса $\{v_1, \ldots, v_n\}$ модуля E. По определению

$$f^*\Delta(v_1, \ldots, v_n) = \Delta(f(v_1), \ldots, f(v_n));$$

в силу теоремы 1 правая часть равна

$$D(A)\Delta(v_1, \ldots, v_n).$$

Согласно следствию 1 теоремы 1, заключаем, что $f^*\Delta = D(A)\Delta$, поскольку обе эти формы принимают одинаковое значение на $v_1, \ldots, v_n)$.

§ 5. Двойственность

Пусть R — коммутативное кольцо и E, F — модули над R. Тогда *R-билинейная форма* на $E \times F$ — это отображение

$$f\colon E \times F \to R,$$

обладающее следующими свойствами: для всякого $x \in E$ отображение

$$y \mapsto f(x, y)$$

R-линейно, и для всякого $y \in F$ отображение

$$x \mapsto f(x, y)$$

R-линейно. В остальной части этого параграфа мы будем опускать приставку R и будем писать $\langle x, y\rangle_f$ или $\langle x, y\rangle$ вместо $f(x, y)$. Для $x \in E$ и $y \in F$ пишем $x \perp y$, если $\langle x, y\rangle = 0$. Аналогично, в случае, когда S — подмножество в F, пишем $x \perp S$, если $x \perp y$ для всех $y \in S$. В этом случае мы говорим, что элемент x *перпендикулярен* к S. Пусть $S^\perp$ состоит из всех элементов в E, перпендикулярных к S. Это, очевидно, подмодуль в E. Аналогичным образом определяется перпендикулярность с другой стороны. Мы считаем по определению *ядром f слева* $F^\perp$ и *ядром f справа* $E^\perp$. Мы будем говорить, что форма f *невырождена слева* (*справа*), если ее ядро слева (соответственно справа) равно 0. Пусть E_0 — ядро f слева; имеем индуцированное билинейное отображение

$$E/E_0 \times F \to R,$$

которое, как тривиально вытекает из определений, невырождено слева. Аналогично, если F_0 — ядро f справа, то имеем индуцированное билинейное отображение

$$E/E_0 \times F/F_0 \to R,$$

которое невырождено с обеих сторон. Это отображение определено, поскольку значение $\langle x, y\rangle$ зависит только от смежного класса x по модулю E_0 и смежного класса y по модулю F_0.

Мы будем обозначать через $L^2(E, F; R)$ множество всех билинейных отображений $E \times F$ в R. Ясно, что это множество является модулем (т. е. R-модулем) с обычными сложением отображений и умножением отображений на элементы из R.

Форма f порождает гомоморфизм

$$\varphi_f\colon E \to \mathrm{Hom}_R(F, R),$$

такой, что

$$\varphi_f(x)(y) = f(x, y) = \langle x, y\rangle$$

для всех $x \in E$ и $y \in F$. Мы будем называть $\mathrm{Hom}_R(F, R)$ *дуальным модулем* модуля F и обозначать его через F^*. Имеем изоморфизм

$$\boxed{L^2(E, F; R) \leftrightarrow \mathrm{Hom}_R(E, \mathrm{Hom}_R(F, R))},$$

задаваемый отображением $f \mapsto \varphi_f$, обратное к которому определяется очевидным образом: если $\varphi\colon E \to \mathrm{Hom}_R(F, R)$ — гомоморфизм, то определяем f по формуле

$$f(x, y) = \varphi(x)(y).$$

Мы будем называть форму f *неособой слева*, если φ_f — изоморфизм, другими словами, если наша форма может быть использована

для отождествления E с модулем, дуальным к F. Форма, *неособая справа*, определяется аналогичным образом, и мы будем говорить, что форма f *неособая*, если она неособая слева и справа.

Предостережение: невырожденная форма не обязательно должна быть неособой.

Получим теперь изоморфизм

$$\boxed{\operatorname{End}_R(E) \leftrightarrow L^2(E,\ F;\ R)},$$

зависящий от фиксированного неособого билинейного отображения f: $E \times F \to R$.

Пусть $A \in \operatorname{End}_R(E)$ — линейное отображение E в себя. Тогда отображение

$$(x,\ y) \longmapsto \langle Ax,\ y\rangle = \langle Ax,\ y\rangle_f$$

билинейно, и этим путем всякому $A \in \operatorname{End}_R(E)$ мы сопоставляем линейным образом некоторую билинейную форму из $L^2(E, F; R)$.

Обратно, пусть отображение h: $E \times F \to R$ билинейно. При заданном $x \in E$ отображение h_x: $F \to R$, для которого $h_x(y) = h(x, y)$, линейно и лежит в дуальном модуле F^*. По предположению существует единственный элемент $x' \in E$, такой, что для всех $y \in F$

$$h(x,\ y) = \langle x',\ y\rangle.$$

Очевидно, что сопоставление $x \longmapsto x'$ является линейным отображением E в себя. Таким образом, всякому билинейному отображению $E \times F \to R$ мы сопоставили линейное отображение $E \to E$.

Непосредственно видно, что отображения, описанные в последних двух абзацах, являются взаимно обратными изоморфизмами между $\operatorname{End}_R(E)$ и $L^2(E, F; R)$. Подчеркнем еще раз, что они зависят от нашей формы f.

Разумеется, мы могли бы все то же самое проделать справа и получить аналогичный *изоморфизм*

$$\boxed{L^2(E,\ F;\ R) \leftrightarrow \operatorname{End}_R(F)},$$

также зависящий от нашей фиксированной неособой формы f.

В качестве приложения рассмотрим линейное отображение A: $E \to E$. Пусть $(x,\ y) \longmapsto \langle Ax,\ y\rangle$ — соответствующее ему билинейное отображение. Тогда существует однозначно определенное линейное отображение

$${}^tA\colon\ F \to F,$$

такое, что

$$\langle Ax,\ y\rangle = \langle x,\ {}^tAy\rangle$$

для всех $x \in E$ и $y \in F$. Мы будем называть ${}^tA$ отображением, *сопряженным к A относительно f*[1].

Непосредственно ясно, что если A, B — линейные отображения E в себя, то для $c \in R$ имеем

$$ {}^t(cA) = c\,{}^tA, \quad {}^t(A+B) = {}^tA + {}^tB \text{ и } {}^t(AB) = {}^tB\,{}^tA. $$

Предположим, что $E = F$. Пусть отображение $f\colon E \times E \to R$ билинейно. Под *автоморфизмом пары* (E, f) или просто под автоморфизмом формы f мы будем понимать линейный автоморфизм $A\colon E \to E$, такой, что

$$ \langle Ax, Ay\rangle = \langle x, y\rangle $$

для всех $x, y \in E$. Группа автоморфизмов формы f обозначается через $\mathrm{Aut}(f)$.

Предложение 11. *Пусть $f\colon E \times E \to R$ — неособая билинейная форма, $A\colon E \to E$ — линейное отображение. Тогда A является автоморфизмом f в том и только в том случае, если ${}^tAA = \mathrm{id}$ и A обратимо.*

Доказательство. Из равенства

$$ \langle x, y\rangle = \langle Ax, Ay\rangle = \langle x, {}^tAAy\rangle, $$

выполняющегося для всех $x, y \in E$, заключаем, что ${}^tAA = \mathrm{id}$, если A — автоморфизм формы f. Обратное столь же очевидно.

Замечание. Если модуль E свободен и конечномерен, то условие ${}^tAA = \mathrm{id}$ влечет обратимость A.

Пусть $f\colon E \times E \to R$ — билинейная форма. Мы будем говорить, что f — *симметрическая*, если $f(x, y) = f(y, x)$ для всех $x, y \in E$. Множество симметрических билинейных форм на E будет обозначаться символом $L_s^2(E)$. Возьмем фиксированную симметрическую неособую билинейную форму f на E, записав ее в виде $(x, y) \mapsto \langle x, y\rangle$. Эндоморфизм $A : E \to E$ называется *симметрическим относительно f*, если ${}^tA = A$. Ясно, что множество симметрических эндоморфизмов модуля E является модулем, который мы будем обозначать через $\mathrm{Sym}(E)$. Имеем *изоморфизм, зависящий от нашей фиксированной симметрической неособой формы f*,

$$ \boxed{L_s^2(E) \longleftrightarrow \mathrm{Sym}(E)}. $$

---

[1] Точнее, сопряженным к A слева. Об этом достаточно выразительно свидетельствует обозначение ${}^tA$. В английском тексте для ${}^tA$ использовано название transpose в отличие от adjoint в эрмитовом случае. При переводе было сохранено лишь различие в обозначениях: ${}^tA$ и A^*. — *Прим. ред.*

Этот изоморфизм описывается следующим образом. Если g — симметрическая билинейная форма на E, то существует однозначно определенное линейное отображение A, такое, что

$$g(x, y) = \langle Ax, y\rangle$$

для всех $x, y \in E$. Используя тот факт, что обе формы f, g симметрические, получаем

$$\langle Ax, y\rangle = \langle Ay, x\rangle = \langle y, {}^tAx\rangle = \langle {}^tAx, y\rangle.$$

Следовательно, $A = {}^tA$. Сопоставление $g \longmapsto A$ дает гомоморфизм $L_s^2(E)$ в $\mathrm{Sym}(E)$. Обратно, для заданного симметрического эндоморфизма A модуля E мы можем определить симметрическую форму правилом $(x, y) \longmapsto \langle Ax, y\rangle$, и сопоставление этой формы эндоморфизму A, очевидно, дает гомоморфизм $\mathrm{Sym}(E)$ в $L_s^2(E)$, обратный к предыдущему гомоморфизму. Следовательно, $\mathrm{Sym}(E)$ и $L_s^2(E)$ изоморфны.

Напомним, что билинейная форма $g : E \times E \to R$ называется знакопеременной, если $g(x, x) = 0$ для всех $x \in E$ и, следовательно, $g(x, y) = -g(y, x)$ для всех $x, y \in E$. Множество билинейных знакопеременных форм на E является модулем, обозначаемым символом $L_a^2(E)$.

Пусть $f : (x, y) \longmapsto \langle x, y\rangle$ — фиксированная *симметрическая* неособая билинейная форма на E. Эндоморфизм $A : E \to E$ будет называться *кососимметрическим* или *знакопеременным* относительно f, если ${}^tA = -A$ и, кроме того, $\langle Ax, x\rangle = 0$ для всех $x \in E$. Если для всякого $a \in R$ соотношение $2a = 0$ возможно лишь при $a = 0$, то второе условие $\langle Ax, x\rangle = 0$ излишне, так как $\langle Ax, x\rangle = -\langle Ax, x\rangle$ влечет $\langle Ax, x\rangle = 0$. Ясно, что множество знакопеременных эндоморфизмов модуля E образует модуль, обозначаемый через $\mathrm{Alt}(E)$. *Имеет место изоморфизм, зависящий от нашей фиксированной симметрической неособой формы* f,

$$\boxed{L_a^2(E) \longleftrightarrow \mathrm{Alt}(E)}.$$

Этот изоморфизм описывается следующим образом. Если g — знакопеременная билинейная форма на E, то соответствующее ей линейное отображение A — это такое отображение, для которого

$$g(x, y) = \langle Ax, y\rangle$$

при всех $x, y \in E$. Аналогично симметрическому случаю тривиально проверяется, что соответствие $g \longleftrightarrow A$ дает нам искомый изоморфизм.

Примеры. Пусть k — поле, E — конечномерное векторное пространство над k и $f : E \times E \to E$ — билинейное отображение, записы-

ваемое в виде $(x, y) \longmapsto xy$. Каждому $x \in E$ сопоставим линейное отображение λ_x: $E \to E$, для которого

$$\lambda_x(y) = xy.$$

Тогда отображение, получаемое взятием следа, а именно

$$(x, y) \longmapsto \operatorname{tr}(\lambda_{xy}),$$

есть билинейная форма на E. Если $xy = yx$, то эта билинейная форма симметрическая.

Далее, пусть E — пространство непрерывных функций на отрезке $[0,1]$, $K(s, t)$ — непрерывная функция от двух вещественных переменных, определенная на квадрате $0 \leqslant s \leqslant 1$ и $0 \leqslant t \leqslant 1$. Для $\varphi, \psi \in E$ положим

$$\langle \varphi, \psi \rangle = \int \int \varphi(s) K(s, t) \psi(t)\, ds\, dt,$$

где двойной интеграл берется по квадрату. Получаем билинейную форму на E. Если $K(s, t) = K(t, s)$, то эта билинейная форма симметрическая. Когда мы в следующем параграфе будем рассматривать матрицы и билинейные формы, читатель увидит аналогию между предыдущей формулой и билинейной формой, определяемой матрицей.

Наконец, пусть U — открытое подмножество вещественного банахова пространства E (или конечномерного евклидова пространства, если читатель на этом настаивает), и пусть f: $U \to \mathbf{R}$ — дважды непрерывно дифференцируемое отображение. Для всякого $x \in U$ производная $Df(x)$: $E \to \mathbf{R}$ есть непрерывное линейное отображение, а вторая производная $D^2 f(x)$ может рассматриваться как непрерывное симметрическое билинейное отображение $E \times E$ в $\mathbf{R}$.

§ 6. Матрицы и билинейные формы

Мы исследуем связь между понятиями, введенными выше, и матрицами. Пусть $f: E \times F \to R$ — билинейное отображение, где E, F — свободные модули над R с базисами $\mathscr{B} = \{v_1, \ldots, v_m\}$, $\mathscr{B}' = \{w_1, \ldots, w_n\}$ соответственно. Положим $g_{ij} = \langle v_i, w_j \rangle$. Если

$$x = x_1 v_1 + \ldots + x_m v_m$$

и

$$y = y_1 w_1 + \ldots + y_n w_n$$

— элементы из E и F соответственно с координатами x_i, $y_j \in R$, то

$$\langle x, y \rangle = \sum_{i=1}^{m} \sum_{j=1}^{n} g_{ij} x_i y_j.$$

Пусть X, Y — столбцы координат для x и y относительно наших базисов. Тогда

$$\langle x, y\rangle = {}^tXGY,$$

где G — матрица (g_{ij}). Мы могли бы записать $G = M^{\mathscr{B}}_{\mathscr{B}'}(f)$. Будем называть G *матрицей, ассоциированной с формой f относительно базисов $\mathscr{B}, \mathscr{B}'$.*

Обратно, если дана матрица G (размера $m \times n$), то из отображения

$$(X, Y) \mapsto {}^tXGY$$

мы получаем билинейную форму. Таким образом, мы приходим к соответствию между билинейными формами и матрицами и ясно, что это соответствие индуцирует изоморфизм (R-модулей)

$$\boxed{L^2(E, F; R) \leftrightarrow \mathrm{Mat}_{m\times n}(R)},$$

задаваемый правилом

$$f \mapsto M^{\mathscr{B}}_{\mathscr{B}'}(f).$$

Два отображения между этими двумя модулями, описанные нами выше, очевидно, обратны друг другу.

Если базисы $\mathscr{B} = \{v_1, \ldots, v_n\}$ и $\mathscr{B}' = \{w_1, \ldots, w_n\}$ таковы, что $\langle v_i, w_j\rangle = \delta_{ij}$, то будем говорить, что эти базисы *дуальны* друг другу. В этом случае билинейное отображение имеет на (X, Y) значение

$$X \cdot Y = x_1y_1 + \ldots + x_ny_n,$$

задаваемое обычным скалярным произведением.

Легко найти общее правило, по которому изменяется матрица G, когда мы меняем базисы в E и F. Однако мы выпишем явную формулу только в том случае, когда $E = F$ и $\mathscr{B} = \mathscr{B}'$. Итак, имеем билинейную форму $f: E \times E \to R$. Пусть $\mathscr{C}$ — другой базис в E. Будем писать $X_{\mathscr{B}}$ и $X_{\mathscr{C}}$ для столбцов, соответствующих элементу x из E относительно этих двух базисов. Обозначим через C обратимую матрицу $M^{\mathscr{C}}_{\mathscr{B}}(\mathrm{id})$, для которой

$$X_{\mathscr{B}} = CX_{\mathscr{C}}.$$

Тогда наша форма задается формулой

$$\langle x, y\rangle = {}^tX_{\mathscr{C}}{}^tCGCY_{\mathscr{C}}.$$

Мы видим, что

$$M^{\mathscr{C}}_{\mathscr{C}}(f) = {}^tCM^{\mathscr{B}}_{\mathscr{B}}(f)C. \tag{1}$$

Другими словами, матрица билинейной формы преобразуется при помощи матрицы C перехода от одного базиса к другому и транспонированной к ней матрицы ${}^tC$.

Если F — свободный модуль над R с базисом $\{\eta_1, \ldots, \eta_n\}$, то $\mathrm{Hom}_R(F, R)$ — также свободный модуль и имеется дуальный базис $\{\eta_1^*, \ldots, \eta_n^*\}$

$$\eta_i^*(\eta_j) = \delta_{ij}.$$

Это проверяется точно так же, как для векторных пространств над полями.

Предложение 12. *Пусть E, F — свободные модули размерности n над R и $f: E \times F \to R$ — некоторая билинейная форма. Следующие условия эквивалентны:*

Форма f — неособая слева.

Форма f — неособая справа.

Форма f — неособая.

Определитель матрицы f относительно любых базисов обратим в R.

Доказательство. Предположим, что f — неособая слева. Фиксируем некоторый базис в E, относительно которого будем записывать элементы из E в виде столбцов и рассмотрим матрицу G для f. Тогда наша форма будет задаваться отображением

$$(X, Y) \longmapsto {}^tXGY,$$

где X, Y — столбцы с коэффициентами в R. По предположению отображение

$$X \longmapsto {}^tXG$$

задает изоморфизм между модулем столбцов и модулем строк длины n над R. Следовательно, матрица G обратима, так что ее определитель есть единица в R. Обратное столь же очевидно, и мы видим, что если $\det(G)$ есть единица, то отображение

$$Y \longmapsto GY$$

должно быть изоморфизмом модуля столбцов на себя. Это доказывает наше утверждение.

Исследуем теперь, как ведет себя в терминах матриц отображение, сопряженное к данному. Пусть E, F — свободные модули над R размерности n.

Пусть $f: E \times F \longmapsto R$ — неособая билинейная форма, и предположим, что заданы базисы $\mathscr{B}$ в E и $\mathscr{B}'$ в F. Пусть G — матрица f относительно этих базисов и $A: E \to E$ — линейное отображение с матрицей M относительно $\mathscr{B}$. Если $x \in E$, $y \in F$ и X, Y — их столбцы относительно $\mathscr{B}$, $\mathscr{B}'$, то

$$(Ax, y) = {}^t(MX)GY = {}^tX{}^tMGY.$$

Пусть N — матрица отображения ${}^tA$ относительно базиса $\mathscr{B}'$. Тогда NY есть столбец элемента ${}^tAy$ относительно $\mathscr{B}'$. Следовательно,

$$\langle x, {}^tAy\rangle = {}^tXGNY.$$

Отсюда заключаем, что ${}^tMG = GN$, и так как матрица G обратима, то мы можем выразить N через M. Получаем

Предложение 13. *Пусть E, F — свободные модули размерности n над R, $f: E \times E \to R$ — неособая билинейная форма, $\mathscr{B}, \mathscr{B}'$ — базисы над R в E и F соответственно и G — матрица f относительно этих базисов. Пусть $A: E \to E$ — линейное отображение и M — его матрица относительно $\mathscr{B}$. Тогда матрицей относительно $\mathscr{B}'$ сопряженного к A отображения ${}^tA$ будет*

$$(G^{-1})^t MG.$$

Следствие 1. *Если G — единичная матрица, то матрица сопряженного отображения ${}^tA$ получается из матрицы отображения A переходом к транспонированной матрице.*

В терминах матриц и базисов мы получаем следующую характеризацию того факта, что матрица индуцирует автоморфизм формы:

Следствие 2. *Сохраняя обозначения предложения* 13, *положим $E = F$ и $\mathscr{B} = \mathscr{B}'$. Матрица M размера $n \times n$ тогда и только тогда является матрицей автоморфизма формы f (относительно нашего базиса), когда*

$${}^tMGM = G.$$

В частности, если это условие удовлетворяется, то матрица M обратима.

Доказательство. Используем определения и формулу, доказанную в предложении 13. Отметим, что M обратима хотя бы потому, что ее определитель есть единица в R.

Матрица M над R называется *симметрической* (соответственно *кососимметрической* [1])), если ${}^tM = M$ (соответственно если ${}^tM = -M$ и диагональные элементы в M равны 0).

Предложение 14. *Пусть E — свободный модуль размерности n над R и $\mathscr{B}$ — фиксированный базис. Отображение*

$$f \to M_{\mathscr{B}}^{\mathscr{B}}(f)$$

индуцирует изоморфизм между модулем симметрических билинейных форм на $E \times E$ (соответственно модулем знакоперемен-

[1]) В тексте — *знакопеременной* что, понятно, одно и то же, когда 2 не является делителем нуля в R. — *Прим. ред.*

ных форм на $E \times E$) и модулем симметрических матриц размера $n \times n$ над R (соответственно модулем кососимметрических матриц размера $n \times n$ над R).

Доказательство. Рассмотрим сначала симметрический случай. Предположим, что форма f симметрическая. Пусть в терминах координат $G = M_{\mathscr{B}}^{\mathscr{B}}(f)$. Наша форма задается произведением ${}^tXGY$, которое должно быть равно ${}^tYGX$ в силу симметричности. Однако ${}^tXGY$ можно рассматривать как матрицу размера 1×1, совпадающую со своей транспонированной матрицей, а именно с ${}^tY{}^tGX$. Таким образом,

$$ {}^tYGX = {}^tY{}^tGX $$

для всех векторов X, Y. Отсюда следует, что $G = {}^tG$. Обратно, очевидно, что любая симметрическая матрица определяет симметрическую форму.

Что касается знакопеременных форм, то, заменяя x на $x + y$ в соотношении $\langle x, x\rangle = 0$, получим

$$ \langle x, y\rangle + \langle y, x\rangle = 0. $$

В терминах координатных векторов X, Y и матрицы G это дает

$$ {}^tXGY + {}^tYGX = 0. $$

Перейдя, скажем, от второй из матриц размера 1×1, входящих в это соотношение, к транспонированной, получим (для всех X, Y)

$$ {}^tXGY + {}^tX{}^tGY = 0. $$

Следовательно, $G + {}^tG = 0$. Кроме того, беря в качестве X любой из единичных векторов

$$ {}^t(0, \ldots, 0, 1, 0, \ldots, 0) $$

и используя соотношение ${}^tXGX = 0$, находим, что диагональные элементы в G должны быть равны 0. Обратно, если матрица G размера $n \times n$ такова, что ${}^tG + G = 0$ и $g_{ii} = 0$ для $i = 1, \ldots, n$, то непосредственно проверяется, что отображение

$$ (X, Y) \longmapsto {}^tXGY $$

определяет знакопеременную форму. Это доказывает наше предложение.

Разумеется, если, как это обычно бывает, элемент 2 не является делителем нуля в R, то из условия ${}^tM = -M$ следует, что диагональные элементы в M должны быть равны 0. Таким образом, в этом случае прямо из $G + {}^tG = 0$ вытекает, что форма знакопеременная.

§ 7. Полуторалинейная двойственность

Существуют формы „почти" билинейные, для которых описанные выше результаты остаются верными почти без изменений; их нужно рассмотреть отдельно для сохранения ясности в используемых обозначениях.

Пусть R имеет автоморфизм периода 2. Мы будем записывать этот автоморфизм так: $a \mapsto \bar{a}$ (имея в виду аналогию с комплексным сопряжением).

Следуя Бурбаки, будем говорить, что отображение

$$f\colon E \times F \to R$$

является *полуторалинейной формой*, если оно $\mathbf{Z}$-билинейно и если для $x \in E$, $y \in F$ и $a \in R$ мы имеем

$$f(ax, y) = af(x, y)$$

и

$$f(x, ay) = \bar{a}f(x, y).$$

Пусть E, E' — модули. Отображение $\varphi\colon E \to E'$ называется *антилинейным* (или *полулинейным*), если оно $\mathbf{Z}$-линейно и $\varphi(ax) = \bar{a}\varphi(x)$ для всех $x \in E$. Таким образом, мы можем сказать, что полуторалинейная форма линейна по своему первому аргументу и антилинейна по второму аргументу. Пусть $\overline{\mathrm{Hom}}_R(E, E')$ обозначает модуль антилинейных отображений E в E'.

Теперь мы последовательно повторим все те замечания, которые раньше были сделаны для билинейных форм.

Для полуторалинейной формы f определяем, как и прежде, перпендикулярность, а также ядра справа и слева. Эти ядра являются подмодулями, скажем, E_0 и F_0, и мы получаем индуцированную полуторалинейную форму

$$E/E_0 \times F/F_0 \to R,$$

которая невырождена с обеих сторон.

Пусть F — R-модуль. Назовем его *антимодулем* модуль E, аддитивная группа которого та же, что и у F, а операция $R \times \bar{F} \to \bar{F}$ задается отображением

$$(a, y) \mapsto \bar{a}y.$$

Имеем естественный изоморфизм R-модулей

$$\mathrm{Hom}_R(\bar{F}, R) \leftrightarrow \overline{\mathrm{Hom}}_R(F, R).$$

Полуторалинейная форма $f\colon E \times F \to R$ индуцирует линейное отображение

$$\varphi_f\colon E \to \mathrm{Hom}_R(\bar{F}, R).$$

Мы говорим, что f — *неособая слева*, если φ_f — изоморфизм. Аналогично имеем соответствующее линейное отображение

$$\varphi'_f\colon \bar{F} \to \mathrm{Hom}_R(E, R)$$

модуля $\bar{F}$ в модуль, дуальный к E, и мы говорим, что f — *неособая справа*, если φ'_f — изоморфизм. Мы говорим, что форма f *неособая*, если она неособая слева и справа.

Заметим, что наша полуторалинейная форма f может рассматриваться как билинейная форма

$$f\colon E \times \bar{F} \to R$$

и наши понятия неособости совместимы с соответствующими понятиями, определенными раньше для билинейных форм.

Имея фиксированную неособую полуторалинейную форму на $E \times F$, мы получаем зависящий от этой формы изоморфизм между модулем полуторалинейных форм на $E \times F$ и модулем эндоморфизмов модуля E. Мы также получаем антиизоморфизм между этими модулями и модулем эндоморфизмов модуля F. В частности, мы можем ввести понятие *сопряженного эндоморфизма*, обозначаемого в случае полуторалинейных форм звездочкой. Именно, пусть $f\colon E \times F \to R$ — неособая полуторалинейная форма, $A\colon E \to E$ — некоторое линейное отображение. Существует однозначно определенное линейное отображение

$$A^*\colon F \to F,$$

такое, что

$$\langle Ax, y\rangle = \langle x, A^*y\rangle$$

для всех $x \in E$ и $y \in F$. Отметим, что A^* линейно, а не антилинейно. Мы называем A^* *сопряженным* с A относительно нашей формы f. Имеют место правила

$$(cA)^* = \bar{c}A^*, \quad (A+B)^* = A^* + B^*, \quad (AB)^* = B^*A^*$$

для линейных отображений A, B модуля E в себя и $c \in R$.

Предположим, что $E = F$. Пусть $f\colon E \times E \to R$ — полуторалинейная форма. Под *автоморфизмом* формы f мы будем понимать линейное отображение $A\colon E \to E$, для которого

$$\langle Ax, Ay\rangle = \langle x, y\rangle,$$

в полной аналогии с автоморфизмами для билинейных форм.

Предложение 11 П. *Пусть $f\colon E \times E \to R$ — неособая полуторалинейная форма, $A\colon E \to E$ — некоторое линейное отображение. Тогда A является автоморфизмом f в том и только в том случае, если $A^*A = \mathrm{id}$ и A обратимо.*

Доказательства этого, а также всех последующих предложений, полностью аналогичные соответствующим доказательствам из билинейного случая, опускаются.

Полуторалинейная форма $g\colon E \times E \to R$ называется *эрмитовой*, если

$$g(x, y) = \overline{g(y, x)}$$

для всех $x, y \in E$. Множество эрмитовых форм на E будет обозначаться через $L_h^2(E)$. Пусть R_0 — подкольцо в R, состоящее из всех элементов, неподвижных относительно нашего автоморфизма $a \mapsto \bar{a}$ (т. е. состоящее из всех элементов $a \in R$, таких, что $a = \bar{a}$). Тогда $L_h^2(E)$ есть R_0-модуль.

Фиксируем некоторую эрмитову неособую форму $f\colon (x, y) \mapsto \langle x, y\rangle$ на E. Эндоморфизм $A\colon E \to E$ называется *эрмитовым* относительно f, если $A^* = A$. Ясно, что множество эрмитовых эндоморфизмов является R_0-модулем, который мы будем обозначать символом $\mathrm{Herm}(E)$. *Имеет место R_0-изоморфизм, зависящий от нашей фиксированной эрмитовой неособой формы f,*

$$\boxed{L_h^2(E) \leftrightarrow \mathrm{Herm}(E)}.$$

Этот изоморфизм описывается следующим образом. Эрмитова форма g тогда и только тогда соответствует эрмитову отображению A, когда

$$g(x, y) = \langle Ax, y\rangle$$

для всех $x, y \in E$.

Опишем теперь связи между нашими понятиями и матрицами, так же как это мы сделали для билинейных форм.

Начнем с полуторалинейной формы $f\colon E \times F \to R$.

Если E, F — свободные модули и мы, как и прежде, выбрали в них базисы, то снова можно сопоставить нашей форме матрицу G, и в терминах координатных векторов X, Y эта полуторалинейная форма будет задаваться отображением

$$(X, Y) \mapsto {}^tX G \bar{Y},$$

где $\bar{Y}$ — вектор, полученный из Y применением нашего автоморфизма к каждой компоненте Y.

Если $E = F$ и мы используем один и тот же базис и справа, и слева, то в тех же обозначениях, которые использованы в формуле (1), последняя для полуторалинейных форм f принимает вид

$$M_{\mathscr{C}}^{\mathscr{C}}(f) = {}^tC M_{\mathscr{B}}^{\mathscr{B}}(f)\, \bar{C}. \qquad (1\text{ П})$$

Таким образом, в формуле *появляется автоморфизм сопряжения.*

Предложение 12П. *Пусть E, F — свободные модули размерности n над R и $f\colon E \times F \to R$ — полуторалинейная форма. Тогда следующие условия эквивалентны:*

Форма f — неособая слева.

Форма f — неособая справа.

Форма f — неособая.

Определитель матрицы f относительно любых базисов обратим в R.

Предложение 13П. *Пусть E, F — свободные модули размерности n над R, $f\colon E \times F \to R$ — полуторалинейная форма. Пусть $\mathscr{B}$, $\mathscr{B}'$ — базисы над R для E и F соответственно и G — матрица f относительно этих базисов. Пусть, наконец, $A\colon E \to E$ — линейное отображение и M — его матрица относительно $\mathscr{B}$. Тогда матрицей относительно $\mathscr{B}'$ сопряженного к A отображения A^* будет*

$$(\overline{G}^{-1})^t\, \overline{M} G.$$

Следствие 1. *Если G — единичная матрица, то матрица отображения A^* равна ${}^t\overline{M}$.*

Следствие 2. *Сохраняя обозначения предложения, положим $E = F$ и $\mathscr{B} = \mathscr{B}'$. Матрица M размера $n \times n$ тогда и только тогда является матрицей автоморфизма формы f (относительно нашего базиса), когда*

$${}^t M G \overline{M} = G.$$

Матрица M называется *эрмитовой*, если ${}^t M = \overline{M}$.

Пусть, как и прежде, R_0 — подкольцо в R, состоящее из всех элементов, неподвижных относительно нашего автоморфизма $a \mapsto \overline{a}$ (т. е. состоящее из всех элементов $a \in R$, таких, что $a = \overline{a}$).

Предложение 14П. *Пусть E — свободный модуль размерности n над R и $\mathscr{B}$ — его базис. Отображение*

$$f \mapsto M_{\mathscr{B}}^{\mathscr{B}}(f)$$

индуцирует R_0-изоморфизм между R_0-модулем эрмитовых форм на E и R_0-модулем эрмитовых матриц размера $n \times n$ над R.

Замечание. Если бы мы предположили с самого начала, что наш автоморфизм $a \mapsto \overline{a}$ имеет период 2 или 1 (т. е. если бы мы позволили ему быть тождественным), то результаты о билинейных и симметрических формах стали бы частными случаями результатов этого параграфа. Однако неудобства, которые причинила бы путаница в обозначениях, вполне оправдывают сделанное нами повторение.

Терминология

По некоторой странной причине группа автоморфизмов симметрической (соответственно знакопеременной или эрмитовой) формы на векторном пространстве называется *ортогональной* (соответственно *симплектической* или *унитарной*) группой этой формы. Слово „ортогональный" особенно неудачно, так как ортогональное отображение сохраняет не только ортогональность — оно сохраняет также скалярное произведение, т. е. длину. Далее, слово „симплектический" также неудачно. Дело в том, что часто рассматривают эрмитовы формы над некоторыми телами (обладающими автоморфизмами порядка 2), и их группы автоморфизмов также были названы симплектическими, что создает настоящую путаницу с использованием этого слова применительно к знакопеременным формам.

Я обсуждал с несколькими лицами вопрос, как унифицировать и улучшить терминологию, и нам кажется, что можно было бы принять следующие соглашения.

Как сказано в тексте, группа автоморфизмов любой формы f обозначается символом $\mathrm{Aut}(f)$.

С другой стороны, имеется стандартная форма, которая над полем вещественных чисел выражается через координаты в виде

$$f(x, x) = x_1^2 + \ldots + x_n^2,$$

над полем комплексных чисел

$$f(x, x) = x_1\bar{x}_1 + \ldots + x_n\bar{x}_n$$

и над телом кватернионов — посредством той же формулы, что и в комплексном случае. Группу автоморфизмов этой формы следовало бы называть *унитарной группой* и обозначать через U_n. Группы точек из U_n в поле вещественных чисел (соответственно в поле комплексных чисел или в теле кватернионов) тогда обозначались бы через

$$U_n(\mathbf{R}), \quad U_n(\mathbf{C}), \quad U_n(\mathbf{K}),$$

и эти три группы назывались бы *вещественной унитарной группой* (соответственно *комплексной унитарной группой* или *кватернионной унитарной группой*). Аналогично группа точек из U_n в любом подполе или подкольце k тела кватернионов обозначалась бы через $U_n(k)$.

Наконец, если f — стандартная знакопеременная форма, задаваемая матрицей

$$\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix},$$

то ее группу автоморфизмов можно было бы обозначать через A_{2n} и называть *группой знакопеременной формы* или просто *знакопере-*

менной группой, если нет опасности спутать ее со знакопеременной группой перестановок. Группа точек группы знакопеременной формы в поле k обозначалась бы тогда через $A_{2n}(k)$.

Как обычно, подгруппа в $\mathrm{Aut}(f)$, состоящая из тех элементов, определитель которых равен 1, обозначалась бы добавлением впереди буквы S и называлась бы по-прежнему *специальной группой*. В четырех стандартных случаях это дает $SU_n(\mathbf{R})$, $SU_n(\mathbf{C})$, $SU_n(\mathbf{K})$, $SA_{2n}(k)$.

УПРАЖНЕНИЯ

1. Интерпретировать ранг матрицы A в терминах размерности образа и ядра линейного отображения L_A.

2. Пусть $\mathfrak{g}$ — модуль над коммутативным кольцом R. Говоря, что билинейное отображение $\mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$, записываемое в виде $(x, y) \longmapsto [x, y]$, наделяет $\mathfrak{g}$ структурой *алгебры Ли*, если $[x, x] = 0$ и

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$$

для всех $x, y, z \in \mathfrak{g}$.

(а) Пусть $M_n(R)$ — кольцо матриц над R. Показать, что если $x, y \in M_n(R)$, то произведение

$$(x, y) \longmapsto [x, y] = xy - yx$$

превращает $M_n(R)$ в алгебру Ли.

(б) Пусть $\mathfrak{g}$ — алгебра Ли. Сопоставим всякому элементу $x \in \mathfrak{g}$ линейное отображение $\mathrm{ad}x$, задаваемое формулой $(\mathrm{ad}x)(y) = [x, y]$. Показать, что $\mathrm{ad}x$ — дифференцирование $\mathfrak{g}$ в себя (т. е. удовлетворяет правилу $D([x, y]) = [Dx, y] + [x, Dy]$).

(в) Показать, что отображение $x \longmapsto \mathrm{ad}\, x$ является гомоморфизмом алгебры Ли $\mathfrak{g}$ в модуль дифференцирований $\mathfrak{g}$ в себя [1]).

3. Если задано некоторое множество многочленов $\{P_\nu(X_{ij})\}$ в кольце многочленов $R[X_{ij}]$ $(1 \leqslant i, j \leqslant n)$, то нуль этого множества в R — это всякая матрица $x = (x_{ij})$, такая, что $x_{ij} \in R$ и $P_\nu(x_{ij}) = 0$ для всех ν. Используя векторные обозначения, пишем $(X) = (X_{ij})$. Пусть $G(R)$ обозначает множество нулей нашего множества многочленов $\{P_\nu\}$. Таким образом, $G(R) \subset M_n(R)$, и если R' — произвольная коммутативная ассоциативная R-алгебра, то $G(R') \subset M_n(R')$. Мы будем говорить, что множество $\{P_\nu\}$ определяет *алгебраическую группу* над R, если $G(R')$ есть подгруппа группы $GL_n(R')$ для всех R' (где $GL_n(R')$ — мультипликативная группа обратимых матриц в R').

Например, группа матриц, удовлетворяющих уравнению ${}^tXX = I_n$, является алгебраической группой.

Пусть $R' = R[t]$ — R-алгебра, которая свободна как R-модуль с базисом $\{1, t\}$, где $t^2 = 0$. Обозначим через $\mathfrak{g}$ множество матриц $x \in M_n(R)$, таких, что $I_n + tx \in G(R[t])$. Показать, что $\mathfrak{g}$ — алгебра Ли. [*Указание*: заметить, что

$$P_\nu(I_n + tX) = P_\nu(I_n) + \mathrm{grad}\, P_\nu(I_n)\, tX.$$

---

[1]) Дифференцирования образуют алгебру Ли относительно операции $[D_1, D_2] = D_1D_2 - D_2D_1$. — *Прим. ред.*

Использовать алгебру $R[t, u]$, где $t^2 = u^2 = 0$, чтобы показать, что если $I_n + tx \in G(R[t])$ и $I_n + uy \in G(R[u])$, то $[x, y] \in g$.]

(Я взял предыдущее из первых четырех страниц записок Серра по группам и алгебрам Ли (Serre J.-P., Lie algebras and Lie groups, New York — Amsterdam, 1965 (готовится русский перевод в изд-ве „Мир")). За дальнейшей информацией, помимо записок Серра, можно обращаться к книгам Джекобсона, Бурбаки и др.)

4. Пусть E — конечное расширение поля k. Возьмем элемент $\alpha \in E$ и рассмотрим k-линейное отображение $f_\alpha: E \to E$, для которого $f_\alpha(x) = \alpha x$. Показать, что след этого линейного отображения совпадает со следом $\mathrm{Tr}_k^E(\alpha)$, определенным в теории полей. [*Указание*: сначала предположить, что $E = k(\alpha)$, взять в качестве базиса степени α и вычислить след f_α относительно этого базиса. Какова будет матрица f_α относительно этого базиса?]

5. Пусть E — конечное расширение поля k. Показать, что норма $N_k^E(\alpha)$ равна определителю $\det(f_\alpha)$ (обозначения из предыдущего упражнения).

6. Пусть A — обратимая матрица над коммутативным кольцом R. Показать, что $({}^tA)^{-1} = {}^t(A^{-1})$.

7. Пусть f — неособая билинейная форма на модуле E над R. Пусть A — R-автоморфизм модуля E. Показать, что $({}^tA)^{-1} = {}^t(A^{-1})$. Доказать то же самое в эрмитовом случае, т. е. что $(A^*)^{-1} = (A^{-1})^*$.

8. Пусть $A_1, \ldots, A_r$ — строки размерности n над полем k. Пусть $X = (x_1, \ldots, x_n)$ и $b_1, \ldots, b_r \in k$. Под системой линейных уравнений над k понимают систему типа

$$A_1 \cdot X = b_1, \ \ldots, \ A_r \cdot X = b_r.$$

Если $b_1 = \ldots = b_r = 0$, то говорят, что система *однородная*. Мы называем n числом неизвестных, а r — числом уравнений. Решение X однородной системы называется *тривиальным*, если $x_i = 0$, $i = 1, \ldots, n$.

(а) Показать, что однородная система из r линейных уравнений с n неизвестными при $n > r$ всегда имеет нетривиальное решение.

(б) Пусть L — система однородных линейных уравнений над полем k, причем k — подполе в k'. Показать, что если L имеет нетривиальное решение в k', то она имеет нетривиальное решение также в k.

9. Пусть M — матрица размера $n \times n$ над полем k. Предположим, что $\mathrm{tr}(MX) = 0$ для всех матриц X размера $n \times n$ над k. Показать, что $M = 0$.

10. Пусть S — некоторое множество матриц размера $n \times n$ над полем k. Показать, что столбец $X \neq 0$ размерности n над k такой, что $MX = X$ для всех $M \in S$ существует в том и только в том случае, если такой столбец существует над некоторым расширением k' поля k.

11. Пусть $\mathbf{K}$ — тело над полем вещественных чисел, порожденное элементами i, j, k, такими, что $i^2 = j^2 = k^2 = -1$ и

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Тогда $\mathbf{K}$ обладает антиавтоморфизмом порядка 2, задаваемым отображением

$$a_0 + a_1 i + a_2 j + a_3 k \longmapsto a_0 - a_1 i - a_2 j - a_3 k.$$

Обозначим этот антиавтоморфизм так: $\alpha \longmapsto \bar{\alpha}$. Чему равно $\alpha\bar{\alpha}$? Показать, что теория эрмитовых форм может быть построена над телом $\mathbf{K}$, которое называется телом *кватернионов*.

12. Пусть $f_{11}, \ldots, f_{1n}$ — многочлены от n переменных над полем k, которое можно считать алгебраически замкнутым. Предположим, что эти многочлены порождают единичный идеал в кольце многочленов $k[X_1, \ldots, X_n]$. Выяснить, существуют ли многочлены f_{ij}, такие, что определитель

$$\begin{vmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ f_{n1} & f_{2n2} & \cdots & f_{nn} \end{vmatrix}$$

равен 1. (Это очень интересная проблема, которая впервые возникла, когда Серр пытался узнать, является ли всякий конечно порожденный проективный модуль над кольцом многочленов свободным. Ответ на нее до сих пор неизвестен (при $n \geqslant 3$). Однако если $f_{11}, \ldots, f_{1n}$ берутся из целостного кольца главных идеалов, то аналогичная задача является легким упражнением.)

13. Пусть A, B — квадратные матрицы одного и того же размера над полем k. Предположим, что B неособая (т. е. обратимая). Показать, что если t — переменная, то $\det(A + tB)$ является многочленом от t, старший коэффициент которого есть $\det(B)$, а свободный член равен $\det(A)$.

Глава XIV

Структура билинейных форм

§ 1. Предварительные сведения, ортогональные суммы

Цель этой главы — проникнуть несколько глубже в структурную теорию наших трех типов форм. При этом мы будем большей частью предполагать, что основное кольцо является полем и даже полем характеристики $\neq 2$ в симметрическом случае.

Напомним наши три определения. Пусть E — модуль над коммутативным кольцом R, $g\colon E \times E \to R$ — некоторое отображение. Билинейное отображение g мы называем *симметрической* формой, если $g(x, y) = g(y, x)$ для всех $x, y \in E$. Мы называем форму g *знакопеременной*, если $g(x, x) = 0$ и, следовательно, $g(x, y) = -g(y, x)$ для всех $x, y \in E$. В том случае, когда R имеет автоморфизм $a \mapsto \bar{a}$ порядка 2, мы говорим, что g — *эрмитова* форма, если отображение g линейно по своему первому аргументу, антилинейно по второму и

$$g(x, y) = \overline{g(y, x)}.$$

Мы будем писать $g(x, y) = \langle x, y\rangle$, если ясно, о какой форме g идет речь. Мы также иногда будем писать $g(x, y) = x \cdot y$ или $g(x, x) = x^2$, называя g *скалярным произведением*.

Если $v_1, \ldots, v_m \in E$, то будем обозначать через $(v_1, \ldots, v_m)$ подмодуль в E, порожденный элементами $v_1, \ldots, v_m$.

Пусть форма g симметрическая, знакопеременная или эрмитова. Тогда ясно, что левое ядро g равно ее правому ядру; оно будет называться просто *ядром* g.

В любом из этих случаев мы будем говорить, что форма g *невырожденная*, если ее ядро равно 0. Предположим, что E конечномерно над некоторым полем k. Тогда форма невырождена в том и только в том случае, если она неособая, т. е. индуцирует изоморфизм E с его дуальным пространством (антидуальным в случае эрмитовых форм).

За исключением нескольких замечаний об антилинейности из предыдущей главы, в этой главе мы не будем использовать результатов о двойственности. Нам потребуется только двойственность над полями, рассмотренная в гл. III. Кроме того, нам по существу не при-

дется здесь встречаться с матрицами, за исключением замечаний о пфаффиане в § 10.

Введем еще одно обозначение. При изучении форм на векторных пространствах мы будем часто разлагать векторное пространство в прямые суммы ортогональных подпространств. Если E — векторное пространство с формой g и F, F' — его подпространства, то мы будем писать

$$E = F \perp F'$$

для обозначения того факта, что E есть прямая сумма F и F' и что F ортогонально (или перпендикулярно) F', т. е., другими словами, $x \perp y$ (или $\langle x, y\rangle = 0$) для всех $x \in F$ и $y \in F'$. Мы в этом случае будем говорить, что E является *ортогональной суммой* F и F'. Это не будет приводить к путанице с использованием символа $\perp$ в тех случаях, когда мы пишем $F \perp F'$ лишь для обозначения того, что F перпендикулярно F'. Из контекста всегда будет ясно, что мы имеем в виду.

Бо́льшая часть этой главы посвящена получению определенных ортогональных разложений векторного пространства с одним из наших трех типов форм, таких, что каждое слагаемое в сумме имеет некоторый легко распознаваемый тип.

В симметрическом и эрмитовом случаях особенно интересны прямые разложения, слагаемые в которых одномерны. Так, в случае симметрической или эрмитовой формы $\langle\ ,\ \rangle$ мы говорим, что $\{v_1, \ldots, v_n\}$ — *ортогональный базис* (относительно этой формы), если $\langle v_i, v_j\rangle = 0$ для всех $i \neq j$. Очевидно, что всякий ортогональный базис дает такое разложение. Если форма невырожденная и если $\{v_1, \ldots, v_n\}$ — ортогональный базис, то непосредственно видно, что $\langle v_i, v_i\rangle \neq 0$ ни для какого i.

Предложение 1. *Пусть E — векторное пространство над полем k и g — форма одного из трех указанных выше типов. Предположим, что E представляется в виде ортогональной суммы*

$$E = E_1 \perp \cdots \perp E_m.$$

Тогда g невырождена на E в том и только в том случае, если она невырождена на каждом E_i. Если E_i^0 — ядро ограничения g на E_i, то ядром g на E будет ортогональная сумма

$$E^0 = E_1^0 \perp \cdots \perp E_m^0.$$

Доказательство. Элементы v, w из E однозначно записываются в виде

$$v = \sum_{i=1}^{m} v_i, \quad w = \sum_{i=1}^{m} w_i,$$

где $v_i,\ w_i \in E_i$. Тогда

$$v \cdot w = \sum_{i=1}^{m} v_i \cdot w_i$$

и $v \cdot w = 0$ для всех $w \in E$ в том и только в том случае, если $v_i \cdot w_i = 0$ для всякого $i = 1, \ldots, m$. Теперь наше утверждение очевидно.

Заметим, что если $E_1, \ldots, E_m$ — векторные пространства над k и $g_1, \ldots, g_m$ — формы на этих пространствах, то мы можем определить форму $g = g_1 \oplus \ldots \oplus g_m$ на прямой сумме $E = E_1 \oplus \ldots \oplus E_m$; а именно, если v, w записаны как выше, то полагаем

$$g(v,\ w) = \sum_{i=1}^{m} g_i(v_i,\ w_i).$$

Ясно, что при этом фактически $E = E_1 \perp \ldots \perp E_m$. Мы могли бы также писать $g = g_1 \perp \ldots \perp g_m$.

Предложение 2. *Пусть E — конечномерное пространство над полем k и g — форма на E одного из упомянутых выше типов. Предположим, что g невырождена. Пусть F — подпространство в E. Форма g тогда и только тогда невырождена на F, когда $F + F^{\perp} = E$, причем невырожденность на F эквивалентна невырожденности на $F^{\perp}$.*

Доказательство. Имеем (как тривиальное следствие из гл. III, § 5)

$$\dim F + \dim F^{\perp} = \dim E = \dim\left(F + F^{\perp}\right) + \dim\left(F \cap F^{\perp}\right).$$

Следовательно, $F + F^{\perp} = E$ тогда и только тогда, когда $\dim\left(F \cap F^{\perp}\right) = 0$. Отсюда тотчас вытекает наше первое утверждение. Так как F, $F^{\perp}$ входят в размерностное условие симметрично, то отсюда вытекает также наше второе утверждение.

Вместо того чтобы говорить, что форма невырождена на E, мы будем иногда, допуская вольность, говорить, что само E невырождено.

Пусть E — конечномерное пространство над полем k, g — форма одного из упомянутых выше типов и E_0 — ядро этой формы. Мы получаем индуцированную форму того же самого типа

$$g_0\colon\ E/E_0 \times E/E_0 \to k,$$

поскольку $g(x, y)$ зависит только от смежного класса x и смежного класса y по модулю E_0. При этом g_0 — невырожденная, так как ее ядро с обеих сторон равно 0.

Пусть E, E' — конечномерные векторные пространства с формами g, g' соответственно. Линейное отображение $\sigma\colon E \to E'$ называется *метрическим*, если

$$g'(\sigma x, \sigma y) = g(x, y)$$

или, в других обозначениях, $\sigma x \cdot \sigma y = x \cdot y$ для всех $x, y \in E$. Если отображение σ — линейный метрический изоморфизм, то мы будем говорить, что σ — *изометрия*. Формы g', g при этом называются *изометричными* (или *эквивалентными*).

Пусть E, E_0 обозначают то же, что и выше. Тогда мы имеем индуцированную форму на факторпространстве E/E_0. Если W — дополнительное подпространство к E_0, т. е. $E = E_0 \oplus W$, то каноническое отображение $\sigma\colon E \to E/E_0$ — метрическое и индуцирует изометрию W на E/E_0. Это утверждение очевидно. Оно показывает, что если $E = E_0 \oplus W'$ — другое разложение E в прямую сумму, то W' изометрично W. Мы знаем, что пространство $W \approx E/E_0$ невырождено. Следовательно, наша форма определяет однозначно с точностью до изометрии невырожденную форму на подпространстве, дополнительном к ядру.

§ 2. Квадратичные отображения

Пусть R — коммутативное кольцо и E, F — R-модули. Как обычно, будем опускать приставку R. Напомним, что билинейное отображение $f\colon E \times E \to F$ называется симметрическим, если $f(x, y) = f(y, x)$ для всех $x, y \in E$.

Будем говорить, что F *не имеет 2-кручения*, если для всякого $y \in F$, такого, что $2y = 0$, мы имеем $y = 0$. (Это выполняется, если элемент 2 обратим в R.)

Пусть $f\colon E \to F$ — некоторое отображение. Мы будем говорить, что f *квадратично* (т. е. R-квадратично), если существуют симметрическое билинейное отображение $g\colon E \times E \to F$ и линейное отображение $h\colon E \to F$, такие, что для всех $x \in E$ имеем

$$f(x) = g(x, x) + h(x).$$

Предложение 3. *Предположим, что F не имеет 2-кручения. Пусть $f\colon E \to F$ — квадратичное отображение, выраженное, как выше, через симметрическое билинейное отображение g и линейное отображение h. Тогда g, h однозначно определяются отображением f. Для всех $x, y \in E$ имеем*

$$2g(x, y) = f(x + y) - f(x) - f(y).$$

Доказательство. Если мы вычислим $f(x+y) - f(x) - f(y)$, то получим $2g(x, y)$. Если g_1 — симметрическое билинейное отобра-

жение, h_1 — линейное отображение и $f(x) = g_1(x, x) + h_1(x)$, то $2g(x, y) = 2g_1(x, y)$. Так как по предположению F не имеет 2-кручения, то отсюда вытекает, что $g(x, y) = g_1(x, y)$ для всех $x, y \in E$ и, следовательно, g однозначно определено. Но тогда h определяется из соотношения

$$h(x) = f(x) - g(x, x).$$

Мы будем называть g, h билинейным и линейным отображениями, *ассоциированными* с f.

Для отображения $f\colon E \to F$ определим

$$\Delta f\colon E \times E \to F,$$

положив

$$\Delta f(x, y) = f(x + y) - f(x) - f(y).$$

Мы будем говорить, что f — *однородное квадратичное* отображение, если оно квадратичное и если ассоциированное с ним линейное отображение равно 0. Мы будем говорить, что модуль F *однозначно делим* на 2, если для всякого $z \in F$ существует единственный элемент $u \in F$, такой, что $2u = z$. (Это снова выполняется, если элемент 2 обратим в R.)

Предложение 4. *Пусть $f\colon E \to F$ — такое отображение, что Δf билинейно, причем модуль F однозначно делим на 2. Тогда отображение $x \mapsto f(x) - \frac{1}{2}\Delta f(x, x)$ $\mathbf{Z}$-линейно. Если f удовлетворяет условию $f(2x) = 4f(x)$, то f — однородное квадратичное.*

Доказательство. Очевидно.

Под *квадратичной формой* на E понимают однородное квадратичное отображение $f\colon E \to R$ со значениями в R.

В дальнейшем мы в основном будем интересоваться симметрическими билинейными формами. Квадратичные формы будут играть второстепенную роль.

Рассматривая квадратичные формы в § 3—8, *мы будем предполагать, что k — поле характеристики $\neq 2$. В оставшейся части главы мы будем также предполагать, что все модули и векторные пространства конечномерны.*

§ 3. Симметрические формы, ортогональные базисы

Теорема 1. *Пусть E — векторное пространство над k и g — симметрическая форма на E. Если* $\dim E \geqslant 1$, *то в E существует ортогональный базис.*

Доказательство. Предположим сначала, что форма g невырожденная, и докажем в этом случае наше утверждение по индукции. Если размерность n равна 1, то утверждение очевидно.

Предположим, что $n > 1$. Пусть $v_1 \in E$ — элемент, для которого $v_1^2 \neq 0$ (такой элемент существует, поскольку по предположению характеристика $\neq 2$ и форма g ненулевая). Пусть $F = (v_1)$ — подпространство, порожденное v_1. Тогда F невырождено и в силу предложения 2

$$E = F + F^{\perp}.$$

Кроме того, $\dim F^{\perp} = n - 1$. Пусть $\{v_2, \ldots, v_n\}$ — ортогональный базис в $F^{\perp}$. Тогда элементы $\{v_1, \ldots, v_n\}$ попарно ортогональны. Кроме того, они линейно независимы, так как если

$$a_1 v_1 + \ldots + a_n v_n = 0,$$

где $a_i \in k$, то, взяв скалярное произведение на v_i, получим $a_i v_i^2 = 0$, откуда $a_i = 0$ для всех i.

Замечание. Фактически мы показали, что если g невырожденная и элемент $v \in F$ таков, что $v^2 \neq 0$, то можно дополнить v до ортогонального базиса в E.

Предположим теперь, что форма g вырожденная. Пусть E_0 — ее ядро. Мы можем записать E в виде прямой суммы

$$E = E_0 \oplus W$$

для некоторого подпространства W. Ограничение g на W невырождено, иначе существовал бы элемент $\neq 0$ в W, лежащий в ядре E. Следовательно, если $\{v_1, \ldots, v_r\}$ — произвольный базис E_0 и $\{w_1, \ldots, w_{n-r}\}$ — ортогональный базис W, то

$$\{v_1, \ldots, v_r, w_1, \ldots, w_{n-r}\}$$

— ортогональный базис в E, что и требовалось показать.

Следствие. *Пусть* $\{v_1, \ldots, v_n\}$ — *ортогональный базис в* E. *Предположим, что* $v_i^2 \neq 0$ *для* $i \leqslant r$ *и* $v_i^2 = 0$ *для* $i > r$. *Тогда ядро в* E *равно* $(v_{r+1}, \ldots, v_n)$.

Доказательство. Очевидно.

Если $\{v_1, \ldots, v_n\}$ — ортогональный базис пространства E и если

$$X = x_1 v_1 + \ldots + x_n v_n, \qquad x_i \in k,$$

то

$$X^2 = a_1 x_1^2 + \ldots + a_n x_n^2,$$

где $a_i = \langle v_i, v_i \rangle$. Об этом представлении формы мы скажем, что она *приведена к диагональному виду*. Непосредственно видно, что по

отношению к ортогональному базису ассоциированная матрица формы является диагональной матрицей, а именно

$$\begin{pmatrix} a_1 & & & & & & \\ & a_2 & & & 0 & & \\ & & \ddots & & & & \\ & & & a_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & 0 & & & & & 0 \end{pmatrix}.$$

§ 4. Гиперболические пространства

Пусть E — векторное пространство над k с симметрической формой. Мы будем говорить, что E — *гиперболическая плоскость*, если форма невырождена, E имеет размерность 2 и в E существует элемент $w \neq 0$, такой, что $w^2 = 0$. Мы будем говорить, что E — *гиперболическое пространство*, если оно является ортогональной суммой гиперболических плоскостей. В этом случае мы также будем говорить, что форма на E гиперболическая.

Пусть E — гиперболическая плоскость с элементом $w \neq 0$, для которого $w^2 = 0$. Если $E = (w, u)$, где u — некоторый элемент из E, то $u \cdot w \neq 0$, иначе w был бы ненулевым элементом из ядра. Пусть $w \cdot bu = bw \cdot u = 1$, где $b \in k$. Выберем $a \in k$ таким образом, чтобы

$$(aw + bu)^2 = 2abw \cdot u + b^2u^2 = 0.$$

(Это можно сделать, поскольку для a мы получили линейное уравнение.) Положим $v = aw + bu$. Тем самым мы нашли базис для E, а именно $E = (w, v)$, такой, что

$$w^2 = v^2 = 0 \quad \text{и} \quad w \cdot v = 1.$$

Относительно этого базиса матрица нашей формы имеет вид

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Заметим, что, обратно, пространство E, имеющее базис $\{w, v\}$, удовлетворяющий условиям $w^2 = v^2 = 0$ и $w \cdot v = 1$, невырождено и, следовательно, является гиперболической плоскостью. Базис $\{w, v\}$, удовлетворяющий этим соотношениям, будем называть *гиперболической парой*.

Ортогональная сумма невырожденных пространств невырождена, и, следовательно, гиперболическое пространство невырождено. Отметим, что гиперболическое пространство всегда имеет четную размерность.

Лемма. *Пусть E — векторное пространство над k с невырожденной симметрической формой g, F — его некоторое подпространство и F_0 — ядро g в F, причем имеет место ортогональное разложение*

$$F = F_0 \perp U.$$

Пусть $\{w_1, \ldots, w_s\}$ — базис в F_0. Тогда в E существуют элементы $v_1, \ldots, v_s$, перпендикулярные к U, такие, что всякая пара $\{w_i, v_i\}$ является гиперболической парой, порождающей некоторую гиперболическую плоскость P_i, причем имеет место ортогональное разложение

$$U \perp P_1 \perp P_2 \perp \ldots \perp P_s.$$

Доказательство. Пусть

$$U_1 = (w_2, \ldots, w_s) \oplus U.$$

Тогда U_1 содержится в $F_0 \oplus U$ собственным образом, так что $(F_0 \oplus U)^\perp$ содержится в $U_1^\perp$ собственным образом. Следовательно, существует элемент u_1, такой, что $u_1 \in U_1^\perp$, но $u_1 \notin (F_0 \oplus U)^\perp$. Имеем $w_1 \cdot u_1 \neq 0$, и значит, (w_1, u_1) — гиперболическая плоскость P_1. Выше мы уже видели, что можно найти элемент $v_1 \in P_1$, такой, что $\{w_1, v_1\}$ — гиперболическая пара. Кроме того, получаем разложение в ортогональную сумму

$$F_1 = (w_2, \ldots, w_s) \perp P_1 \perp U.$$

Ясно, что $(w_2, \ldots, w_s)$ будет ядром g в F_1, и мы можем закончить доказательство по индукции.

§ 5. Теорема Витта

Теорема 2. *Пусть E — векторное пространство над k, g — невырожденная симметрическая форма на E. Пусть, далее, F, F' — подпространства в E и σ: $F \to F'$ — изометрия. Тогда σ может быть продолжено до изометрии E на себя.*

Доказательство. Сначала сведем доказательство к случаю, когда F невырождено.

Мы можем записать $F = F_0 \perp U$, как в лемме из предыдущего параграфа. Тогда $\sigma F = F' = \sigma F_0 \perp \sigma U$. Кроме того, $\sigma F_0 = F_0'$ будет

ядром g в F'. Теперь мы можем расширить и F, и F', как в лемме, до ортогональных сумм

$$U \perp P_1 \perp \ldots \perp P_s \quad \text{и} \quad \sigma U \perp P_1' \perp \ldots \perp P_s',$$

соответствующих выбору некоторого базиса в F_0 и образу этого базиса в F_0'. Таким образом, мы можем продолжить σ до изометрии этих расширенных пространств, являющихся уже невырожденными.

Итак, предположим, что F, F' невырождены, и будем действовать шаг за шагом.

Допустим сначала, что $F' = F$, т. е. что σ — изометрия F на себя. Тогда мы можем продолжить σ на E, просто оставляя каждый элемент из $F^\perp$ неподвижным.

Далее, предположим, что $\dim F = \dim F' = 1$ и что $F \neq F'$. Пусть, скажем, $F = (v)$ и $F' = (v')$, где $v' = \sigma v$. Тогда $v^2 = v'^2$. Кроме того, (v, v') имеет размерность 2.

Подпространство (v, v') обладает изометрией, продолжающей σ, которая переводит v в v' и v' в v. Если (v, v') невырождено, то мы можем применить предыдущий шаг и завершить доказательство.

Если (v, v') вырождено, то ядро g на нем имеет размерность 1. Пусть w — базис этого ядра. Существуют элементы a, $b \in k$, такие, что $v' = av + bw$. Тогда $v'^2 = a^2 v^2$ и, следовательно, $a = \pm 1$. Заменив w на bw, мы можем считать, что $v' = av + w$. Пусть $z = v + av'$. Применим лемму к пространству

$$(w, z) = (w) \perp (z).$$

Мы найдем элемент $y \in E$, для которого

$$y \cdot z = 0, \quad y^2 = 0 \quad \text{и} \quad w \cdot y = 1.$$

Пространство $(z, w, y) = (z) \perp (w, y)$ невырождено как ортогональная сумма (z) и гиперболической плоскости (w, y). Оно обладает изометрией, при которой

$$z \leftrightarrow az, \quad w \leftrightarrow -aw, \quad y \leftrightarrow -ay.$$

Но $v = \frac{1}{2}(z - aw)$ отображается при этой изометрии на $v' = \frac{1}{2}(az + w)$. Таким образом, с этим случаем мы разделались.

Заканчиваем доказательство по индукции. В силу существования ортогонального базиса (теорема 1) всякое подпространство F размерности > 1 имеет ортогональное разложение в сумму подпространств меньшей размерности. Пусть $F = F_1 \perp F_2$, где $\dim F_1$ и $\dim F_2 \geqslant 1$. Тогда

$$\sigma F = \sigma F_1 \perp \sigma F_2.$$

Пусть $\sigma_1 = \sigma \mid E_1$ — ограничение σ на F_1. По индукции мы можем продолжить σ_1 до изометрии

$$\bar{\sigma}_1\colon E \to E.$$

Тогда $\bar{\sigma}_1(F_1^\perp) = (\sigma_1 F_1)^\perp$. Так как σF_2 перпендикулярно к $\sigma F_1 = \sigma_1 F_1$, то σF_2 содержится в $\bar{\sigma}_1(F_1^\perp)$. Пусть $\sigma_2 = \sigma \mid F_2$. Тогда изометрия

$$\sigma_2\colon F_2 \to \sigma_2 F_2 = \sigma F_2$$

продолжается по индукции до изометрии

$$\bar{\sigma}_2\colon F_1^\perp \to \bar{\sigma}_1(F_1^\perp).$$

Пара $(\sigma_1, \bar{\sigma}_2)$ и дает нам искомую изометрию пространства $F_1 \perp F_1^\perp = E$ на себя.

Следствие 1. *Пусть E, E' — векторные пространства с невырожденными симметрическими формами. Предположим, что они изометричны. Пусть F, F' — их подпространства и $\sigma'\colon F \to F'$ — изометрия. Тогда σ может быть продолжено до изометрии E на E'.*

Доказательство. Очевидно.

Пусть E — векторное пространство над k с симметрической формой g. Мы будем говорить, что g — *нулевая* форма или что E — *нуль-пространство*, если $\langle x, y\rangle = 0$ для всех x, $y \in E$. Поскольку мы предположили, что характеристика k не равна 2, то условие $x^2 = 0$ для всех $x \in E$ влечет, что g — нулевая форма. Действительно,

$$4x \cdot y = (x+y)^2 - (x-y)^2.$$

В качестве приложений теоремы 2 мы получаем еще несколько следствий.

Следствие 2. *Пусть E — векторное пространство с невырожденной симметрической формой, W — его максимальное нуль-подпространство и W' — некоторое нуль-подпространство. Тогда $\dim W' \leqslant \dim W$ и W' содержится в каком-то максимальном нуль-подпространстве, размерность которого совпадает с $\dim W$.*

Доказательство. Тот факт, что W' содержится в максимальном нуль-подпространстве, следует из леммы Цорна. Предположим, что $\dim W' \geqslant \dim W$. Имеем изометрию W на подпространство в W', которая может быть продолжена до изометрии E на себя. Тогда $\sigma^{-1}(W')$ есть нуль-подпространство, содержащее W и, следовательно, равное W, откуда $\dim W = \dim W'$. Наши утверждения следуют из симметрии.

Пусть E — векторное пространство с невырожденной симметрической формой и W — нуль-подпространство. Согласно лемме § 4, мы можем вложить W в некоторое гиперболическое подпространство H в E, размерность которого равна $2\dim W$, причем W является максимальным нуль-подпространством в H. Любое такое H будет называться *гиперболическим расширением* W.

Следствие 3. *Пусть E — векторное пространство с невырожденной симметрической формой, W и W' — максимальные нуль-подпространства, а H, H' — гиперболические расширения W, W' соответственно. Тогда H и H' изометричны, равно как и $H^{\perp}$ и $H'^{\perp}$.*

Доказательство. Имеем очевидную изометрию H на H', которая может быть продолжена до изометрии E на себя. Эта изометрия отображает $H^{\perp}$ на $H'^{\perp}$, что и требовалось.

Следствие 4. *Пусть g_1, g_2, h — симметрические формы на векторных пространствах над полем k. Если форма $g_1 \oplus h$ изометрична форме $g_2 \oplus h$ и если g_1, g_2 невырождены, то g_1 изометрична g_2.*

Доказательство. Пусть g_1 — форма на E_1, g_2 — форма на E_2 и h — форма на F. Тогда имеем изометрию $F \oplus E_1$ на $F \oplus E_2$. Продолжим тождественную изометрию id: $F \to F$ до изометрии σ пространства $F \oplus E_1$ на $F \oplus E_2$, согласно следствию 1. Так как E_1 и E_2 — соответствующие ортогональные дополнения к F в этих двух пространствах, то мы должны иметь $\sigma(E_1) = E_2$, что и доказывает требуемое утверждение.

Пусть g — симметрическая форма на векторном пространстве E. Мы будем говорить, что g *определенная*, если $g(x, x) \neq 0$ для любого $x \in E$, $x \neq 0$ (т. е. $x^2 \neq 0$, если $x \neq 0$).

Следствие 5. *Пусть g — симметрическая форма на векторном пространстве. Тогда g обладает разложением в ортогональную сумму*

$$g = g_0 \oplus g_{\text{hyp}} \oplus g_{\text{def}},$$

где g_0 — нулевая форма, g_{hyp} — гиперболическая и g_{def} — определенная. Форма $g_{\text{hyp}} \oplus g_{\text{def}}$ невырожденная. Формы g_0, g_{hyp} и g_{def} однозначно определены с точностью до изометрии.

Доказательство. Разложение $g = g_0 \oplus g_1$, где g_0 — нулевая форма, а g_1 — невырожденная, единственно с точностью до изометрии, поскольку g_0 соответствует ядру g.

Мы можем поэтому предполагать, что g — невырожденная. Если

$$g = g_h \oplus g_d,$$

где g_h — гиперболическая, g_d — определенная, то g_h соответствует гиперболическому расширению максимального нуль-подпространства и, согласно следствию 3, g_h определена однозначно. Следовательно, g_d однозначно определена как ортогональное дополнение к g_h. (Под однозначной определенностью мы, разумеется, понимаем однозначную определенность с точностью до изометрии.)

Мы сокращаем g_{hyp} до g_h и g_{def} до g_d.

§ 6. Группа Витта

Пусть g, φ — симметрические формы на векторных пространствах над k. Мы будем говорить, что они *эквивалентны*, если g_d изометрична φ_d. Читатель тотчас проверит, что это действительно отношение эквивалентности. Далее, (ортогональная) сумма двух нулевых форм есть нулевая форма, а сумма двух гиперболических форм — гиперболическая форма. Однако сумма двух определенных форм, разумеется, не обязательно является определенной формой. Мы будем записывать наше отношение эквивалентности так: $g \sim \varphi$. Эквивалентность сохраняется при ортогональных суммах и, следовательно, классы эквивалентности симметрических форм образуют коммутативный моноид.

Теорема 3. *Моноид классов эквивалентности симметрических форм (над полем k) является группой.*

Доказательство. Мы должны показать, что всякий элемент обладает аддитивным обратным. Пусть g — симметрическая форма; мы можем считать ее определенной. Обозначим через $-g$ форму на E, для которой $(-g)(x, y) = -g(x, y)$. Мы утверждаем, что форма $g \oplus (-g)$ эквивалентна 0. Пусть E — пространство, на котором определена форма g. Тогда форма $g \oplus -g$ определена на $E \oplus E$. Пусть W — подпространство, состоящее из всех пар (x, x), где $x \in E$. Тогда W — нуль-пространство для $g \oplus -g$. Так как $\dim(E \oplus E) = 2 \dim W$, то W — максимальное нуль-пространство и форма $g \oplus -g$ — гиперболическая, что и требовалось показать.

Группа из теоремы 3 называется *группой Витта* поля k и обозначается через $W(k)$. Она важна при изучении представлений элементов поля k квадратичной формой f, порожденной g [т. е. $f(x) = g(x, x)$], например, когда хотят классифицировать определенные формы f.

Определим теперь другую группу, которая важна при более функториальном изучении симметрических форм, например, при

изучении квадратичных форм, возникающих при исследовании многообразий в топологии.

Заметим, что классы изометрии невырожденных симметрических форм (над k) образуют моноид $M(k)$, законом композиции в котором служит взятие ортогональной суммы. Кроме того, в нем выполняется закон сокращения (следствие 4 теоремы 2). Пусть

$$\gamma\colon M(k) \to WG(k)$$

— каноническое отображение $M(k)$ в группу Гротендика этого моноида, которую мы будем называть *группой Витта — Гротендика* над k. Как мы знаем, из выполнимости закона сокращения следует, что γ инъективно.

Пусть g — симметрическая невырожденная форма над k. Мы *определяем ее размерность* $\dim g$ как размерность того пространства E, на котором она определена. Ясно, что

$$\dim(g \oplus g') = \dim g + \dim g'.$$

Следовательно, можно продолжить dim до гомоморфизма

$$\dim\colon WG(k) \to \mathbf{Z}.$$

Этот гомоморфизм расщепляется, так как существует невырожденная симметрическая форма размерности 1.

Пусть $WG_0(k)$ — ядро гомоморфизма dim. Если g — невырожденная симметрическая форма, то ее определителем $\det(g)$ мы будем считать взятый по модулю квадратов в k^* определитель матрицы G, представляющей g относительно некоторого базиса. Как элемент из k^*/k^{*2} он однозначно определен. Положим det 0-формы равным 1. Тогда det есть гомоморфизм

$$\det\colon M(k) \to k^*/k^{*2}$$

и может поэтому быть продолжен до гомоморфизма, обозначаемого по-прежнему через det, группы Витта — Гротендика:

$$\det\colon WG(k) \to k^*/k^{*2}.$$

Некоторые другие свойства группы Витта — Гротендика приведены в упражнениях.

§ 7. Симметрические формы над упорядоченными полями

Теорема 4 (Сильвестр). *Пусть k — упорядоченное поле и E — векторное пространство над k с невырожденной симметрической формой g. Существует целое число $r \geqslant 0$, такое, что каков бы ни был ортогональный базис $\{v_1, \ldots, v_n\}$ для E, среди*

n элементов $v_1^2, \ldots, v_n^2$ *в точности* r *будут* >0 *и в точности* $n-r$ *будут* <0.

Доказательство. Пусть $a_i = v_i^2$ для $i = 1, \ldots, n$. После изменения нумерации базисных элементов мы можем считать, что, скажем, $a_1, \ldots, a_r > 0$ и $a_i < 0$ для $i > r$. Пусть $\{w_1, \ldots, w_n\}$ — любой ортогональный базис и $b_i = w_i^2$. Допустим, $b_1, \ldots, b_s > 0$ и $b_j < 0$ для $j > s$. Докажем, что $r = s$. Действительно, достаточно доказать, что

$$v_1, \ldots, v_r, w_{s+1}, \ldots, w_n$$

линейно независимы, так как тогда $r + n - s \leqslant n$, откуда $r \leqslant s$ и $r = s$ в силу симметрии. Предположим, что

$$x_1 v_1 + \ldots + x_r v_r + y_{s+1} w_{s+1} + \ldots + y_n w_n = 0.$$

Тогда

$$x_1 v_1 + \ldots + x_r v_r = -y_{s+1} w_{s+1} - \ldots - y_n w_n.$$

Возведение в квадрат обеих частей равенства дает

$$a_1 x_1^2 + \ldots + a_r b_r^2 = b_{s+1} y_{s+1}^2 + \ldots + b_n y_n^2.$$

Левая сторона $\geqslant 0$, а правая сторона $\leqslant 0$. Следовательно, обе стороны равны 0, откуда вытекает, что $x_i = y_j = 0$, другими словами, что наши векторы линейно независимы.

Следствие 1. *Предположим, что всякий положительный элемент в* k *является квадратом. Тогда существует ортогональный базис* $\{v_1, \ldots, v_n\}$ *пространства* E, *такой, что* $v_i^2 = 1$ *для* $i \leqslant r$ *и* $v_i^2 = -1$ *для* $i > r$, *причем число* r *однозначно определено.*

Доказательство. Разделим каждый вектор произвольного ортогонального базиса на квадратный корень из абсолютной величины его квадрата.

Базис, обладающий свойством, описанным в следствии, называется *ортонормальным*. Если X — элемент из E, имеющий относительно такого базиса координаты $(x_1, \ldots, x_n)$, то

$$X^2 = x_1^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_n^2.$$

Будем говорить, что симметрическая форма g *положительно определенная*, если $X^2 > 0$ для всех $X \in E$, $X \neq 0$. Это имеет место тогда и только тогда, когда в теореме 4 $r = n$. Мы будем говорить, что g *отрицательно определенная*, если $X^2 < 0$ для всех $X \in E$, $X \neq 0$.

Следствие 2. *Векторное пространство E обладает ортогональным разложением $E = E^+ \perp E^-$, таким, что g будет положительно определенной на E^+ и отрицательно определенной на E^-. Размерность E^+ (или E^-) одна и та же во всех таких разложениях.*

Предположим теперь, что форма g положительно определенная и что всякий положительный элемент в k является квадратом.

Определим *норму* элемента $v \in E$, положив

$$|v| = \sqrt{v \cdot v}.$$

Тогда $|v| > 0$, если $v \neq 0$. Имеем также *неравенство Шварца*

$$|v \cdot w| \leqslant |v| \cdot |w|$$

для всех v, $w \in E$. Оно доказывается обычным способом. Разложим

$$0 \leqslant (av \pm bw)^2 = (av \pm bw) \cdot (av \pm bw)$$

по билинейности и положим $a = |w|$ и $b = |v|$. Получим

$$\mp 2abv \cdot w \leqslant 2|v|^2|w|^2.$$

Если $|v|$ или $|w| = 0$, то наше неравенство тривиально. Если ни один из этих элементов $\neq 0$, то разделим на $|v||w|$ и получим то, что требуется.

Из неравенства Шварца выводится неравенство треугольника

$$|v + w| \leqslant |v| + |w|.$$

Мы предоставляем вывод читателю в качестве шаблонного упражнения.

В случае когда мы имеем положительно определенную форму, существует канонический путь получения ортонормального базиса посредством индуктивного процесса, начинающегося с произвольного базиса $\{v_1, \ldots, v_n\}$. Пусть

$$v_1' = \frac{1}{|v_1|} v_1.$$

Тогда v_1' имеет норму 1. Положим

$$w_2 = v_2 - (v_2 \cdot v_1') v_1',$$

а затем

$$v_2' = \frac{1}{|w_2|} w_2.$$

По индукции полагаем

$$w_r = v_r - (v_r \cdot v_1') v_1' - \ldots - (v_r \cdot v_{r-1}') v_{r-1}'$$

и

$$v_r' = \frac{1}{|w_r|} w_r.$$

Тогда $\{v_1', \ldots, v_n'\}$ — ортонормальный базис. Только что описанный индуктивный процесс известен под названием *ортогонализации Грама — Шмидта*.

§ 8. Алгебра Клиффорда

Пусть E — векторное пространство над полем k и g — симметрическая форма на E. Было бы желательно найти универсальную алгебру над k, в которую можно вложить E, и такую, что квадрат в этой алгебре соответствует значению квадратичной формы на E. Более точно, под *алгеброй Клиффорда* формы g мы будем понимать пару $(C(g), \rho)$ — алгебру $C(g)$ и линейное отображение $\rho\colon E \to C(g)$, — обладающую следующими свойствами: (1) для всех $X \in E$ имеем $\rho(X)^2 = g(X, X)\cdot 1$; (2) если $\psi\colon E \to L$ — линейное отображение E в k-алгебру L, такое, что

$$\psi(X)^2 = g(X, X)\cdot 1$$

(1 — единичный элемент в L) для всех $X \in E$, то существует однозначно определенный гомоморфизм алгебр

$$C(\psi) = \psi_*\colon C(g) \to L,$$

для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} E & \xrightarrow{\rho} & C(g) \\ & {\scriptstyle\psi}\searrow \quad \swarrow{\scriptstyle\psi_*} & \\ & L & \end{array}$$

Согласно абстрактной чепухе [1]), алгебра Клиффорда формы g однозначно определена с точностью до единственного изоморфизма. Кроме того, ясно, что если $(C(g), \rho)$ существует, то $C(g)$ как алгебра над k порождается образом $\rho(E)$ отображения ρ.

Мы будем писать $\rho = \rho_g$, если необходимо явно указать, о какой форме g идет речь.

Заменяя в соотношении

$$\rho(X)^2 = g(X, X)\cdot 1$$

X на $X + Y$, находим

$$\rho(X)\rho(Y) + \rho(Y)\rho(X) = 2g(X, Y)\cdot 1.$$

Теорема 5. *Пусть g — симметрическая билинейная форма на векторном пространстве E над k. Тогда алгебра Клиффорда $(C(g), \rho)$ существует. Отображение ρ инъективно, и $C(g)$ имеет размерность 2^n над k, где $n = \dim E$.*

[1]) См. стр. 126. — *Прим. ред.*

Для того чтобы доказать теорему 5, мы сначала найдем соотношения, которым должны удовлетворять алгебра L и линейное отображение ψ: $E \to L$, такое, что $\psi(X)^2 = g(X, X) \cdot 1$. Мы будем следовать рассуждениям Артина в „Геометрической алгебре".

Пусть $S_1, \ldots, S_r$ — подмножества заданного множества M. Определим их *сумму* (которая не будет объединением) как множество элементов из M, содержащихся в нечетном числе множеств S_i, $i = 1, \ldots, r$.

Легко проверяются следующие правила:

$$(S_1 + \ldots + S_r) + S_{r+1} = S_1 + \ldots + S_{r+1},$$
$$(S_1 + \ldots + S_r) \cap T = (S_1 \cap T) + \ldots + (S_r \cap T),$$

для любого подмножества T в M.

Пустое множество обозначается, как обычно, через $\varnothing$.

Пусть $\{v_1, \ldots, v_n\}$ — ортогональный базис для E над k. Положим $a_i = v_i^2$ и $\psi(v_i) = e_i$. Тогда по предположению

$$e_i^2 = a_i \text{ и } e_i e_j + e_j e_i = 0, \text{ если } i \neq j.$$

Пусть S — подмножество множества $M = \{1, \ldots, n\}$ и $i_1, \ldots, i_m$ — элементы S, упорядоченные так, что $i_1 < \ldots < i_m$. Положим $e_S = e_{i_1} \ldots e_{i_m}$. Индукцией легко показать, что для любых подмножеств S, T в $\{1, \ldots, n\}$

$$e_S e_T = \prod_{\substack{s \in S \\ t \in T}} (s, t) \prod_{i \in S \cap T} v_i^2 e_{S+T},$$

где символ (s, t) по определению равен 1 при $s \leqslant t$ и -1 при $s > t$. Таким образом, правило вычисления произведения двух „одночленов" от $e_1, \ldots, e_n$ определяется чисто комбинаторно в терминах S и T и заданных нам квадратов $v_1^2, \ldots, v_n^2$. Кроме того, алгебра, порожденная $\psi(E)$, порождается элементами $e_1, \ldots, e_n$.

Покажем теперь, как предыдущее комбинаторное правило позволяет нам определить универсальную алгебру.

Каждому подмножеству S из $\{1, \ldots, n\}$ сопоставим символ e_S. Пусть $C(g)$ — свободный модуль над k, порожденный этими символами e_S (S пробегает все подмножества в $\{1, \ldots, n\}$). Тогда $C(g)$ имеет размерность 2^n над k. Определим умножение в $C(g)$. Для подмножеств S, T множества $\{1, \ldots, n\}$ положим

$$\alpha(S, T) = \prod_{\substack{s \in S \\ t \in T}} (s, t) \prod_{i \in S \cap T} v_i^2.$$

Если $\sum_S a_S e_S$ и $\sum_T b_T e_T$ — элементы из $C(g)$ с коэффициентами a_S, $b_T \in k$, то определим их произведение следующим образом:

$$\left(\sum_S a_S e_S\right)\left(\sum_T b_T e_T\right) = \sum_{S,T} a_S b_T \alpha(S, T)\, e_{S+T}.$$

Мы должны показать, что это произведение ассоциативно. Для этого, очевидно, достаточно будет доказать, что для любых подмножеств S, T, R множества $\{1, \ldots, n\}$

$$(e_S e_T) e_R = e_S (e_T e_R);$$

это последнее соотношение будет проверяться в лоб.

По определению

$$e_S e_T = \alpha(S, T)\, e_{S+T}.$$

Приступая к доказательству, сделаем подстановку

$$(e_S e_T) e_R = \prod_{\substack{s \in S \\ t \in T}} (s, t) \prod_{\substack{j \in S+T \\ r \in R}} (j, r) \prod_{i \in S \cap T} v_i^2 \prod_{\lambda \in (S+T) \cap R} v_\lambda^2 e_{S+T+R}$$

и перепишем правую часть в более симметричной форме.

Правая часть состоит из произведений некоторых знаков и некоторых квадратов. Сначала рассмотрим знаки.

Если j будет пробегать S, а затем T, то любое $j \in S \cap T$ появится дважды. Таким образом, второе произведение совпадает с произведением, взятым по $j \in S$ и $j \in T$; другими словами, произведение, дающее знак, может быть записано в виде

$$\prod_{\substack{s \in S \\ t \in T}} (s, t) \prod_{\substack{s \in S \\ r \in R}} (s, r) \prod_{\substack{t \in T \\ r \in R}} (t, r).$$

Теперь займемся произведением квадратов. Имеем

$$(S + T) \cap R = (S \cap R) + (T \cap R).$$

Если ν принадлежит всем трем множествам S, T, R, то ν лежит в $S \cap T$, но не в $(S \cap R) + (T \cap R)$. Если ν принадлежит S и T, но не R, то ν лежит в $S \cap T$, но не в $(S \cap R) + (T \cap R)$. Если ν лежит в S и R, но не в T, или в T и R, но не в S, то ν не лежит в $S \cap T$, но лежит в $(S \cap R) + (T \cap R)$. Наконец, если ν лежит лишь в одном из множеств S, T, R или не лежит ни в одном из них, то ν не лежит ни в $S \cap T$, ни в $(S \cap R) + (T \cap R)$. Таким образом, последние два произведения могут быть записаны в виде произведения

$$\prod_\nu v_\nu^2$$

по тем ν, которые встречаются более чем в одном из множеств S, T, R. Это произведение симметрично по S, T, R. Из того, что мы показали,

сразу же следует равенство

$$(e_S e_T) e_R = e_S (e_T e_R).$$

Это и означает, что произведение, которое мы определили в $C(g)$, ассоциативно. Другие аксиомы кольца проверяются тривиально, и элементы $\{e_S\}$ образуют базис алгебры $C(g)$, которая имеет поэтому размерность 2^n.

Линейное отображение

$$\rho\colon E \to C(g),$$

для которого $\rho(v_i) = e_{\{i\}}$, очевидно, инъективно. Будем писать $e_i = e_{\{i\}}$. Если

$$X = x_1 v_1 + \ldots + x_n v_n,$$

то

$$\rho(X)^2 = (x_1 e_1 + \ldots + x_n e_n)(x_1 e_1 + \ldots + x_n e_n) = \\ = (x_1^2 a_1 + \ldots + x_n^2 a_n) e_\phi,$$

где e_ϕ — единичный элемент алгебры $C(g)$, поскольку $e_i e_j + e_j e_i = 0$ для $i \neq j$. Таким образом, наши требования, касающиеся квадратов, удовлетворяются.

Если $\psi\colon E \to L$ — любое такое линейное отображение в алгебру над k, что $\psi(X)^2 = g(X, X) \cdot 1$, то мы можем определить кольцевой гомоморфизм $C(g)$ в L, для которого требуемая диаграмма коммутативна. Действительно, пусть $e'_i = \psi(v_i)$. Положим

$$e'_S = e'_{i_1} \ldots e'_{i_m},$$

где $i_1 < \ldots < i_m$ — элементы множества S. Определим

$$\psi_*\colon C(g) \to L,$$

положив

$$\sum a_S e_S \mapsto \sum a_S e'_S.$$

Так как элементы $\{e_S\}$ образуют базис $C(g)$, то это отображение однозначно определено и является линейным отображением. Замечания в начале доказательства показывают, что это отображение является также гомоморфизмом колец, и диаграмма

$$\begin{array}{ccc} E & \xrightarrow{\rho} & C(g) \\ & {\scriptstyle\psi}\searrow \quad \swarrow{\scriptstyle\psi_*} & \\ & L & \end{array}$$

коммутативна. Это доказывает все, что требовалось.

§ 9. Знакопеременные формы

Пусть E — векторное пространство над полем k, на которое мы не налагаем теперь никаких ограничений. Пусть f — знакопеременная форма на E, т. е. билинейное отображение $f: E \times E \to k$, такое, что $f(x, x) = x^2 = 0$ для всех $x \in E$. Тогда

$$x \cdot y = -y \cdot x$$

для всех $x, y \in E$, что обнаруживается подстановкой $(x + y)$ вместо x в соотношение $x^2 = 0$.

Как и для симметрических форм, мы определяем *гиперболическую плоскость* (для знакопеременных форм) как двумерное невырожденное пространство. (На этот раз мы автоматически получаем элемент w, такой, что $w^2 = 0$, $w \neq 0$, так что нет надобности специально выделять это.) Если P — гиперболическая плоскость и $w \in P$, $w \neq 0$, то в P существует элемент $y \neq 0$, для которого $w \cdot y \neq 0$. Деля y на константу, мы можем считать, что $w \cdot y = 1$. Тогда $y \cdot w = -1$. Следовательно, матрица формы относительно базиса $\{w, y\}$ имеет вид

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Как и прежде, пара w, y называется *гиперболической парой*. Если заданы двумерное векторное пространство над k с билинейной формой и пара элементов $\{w, y\}$, удовлетворяющих соотношениям

$$w^2 = y^2 = 0, \quad y \cdot w = -1, \quad w \cdot y = 1,$$

то легко видеть, что рассматриваемая форма знакопеременная и (w, y) — гиперболическая плоскость для этой формы.

При заданной знакопеременной форме f на E мы будем говорить, что пространство E (или f) *гиперболическое*, если E является ортогональной суммой гиперболических плоскостей. Мы будем говорить, что E (или f) *нулевое*, если $x \cdot y = 0$ для всех $x, y \in E$.

Теорема 6. *Пусть f — знакопеременная форма на векторном пространстве E над k. Тогда E будет ортогональной суммой своего ядра и гиперболического подпространства. Если E невырождено, то E является гиперболическим пространством и его размерность четна.*

Доказательство. Дополнительное подпространство к ядру невырождено, и, следовательно, мы можем считать, что E невырождено. Пусть $w \in E$, $w \neq 0$. Существует элемент $y \in E$, для которого $w \cdot y \neq 0$. Тогда подпространство (w, y) невырождено, следовательно, является гиперболической плоскостью P. Имеем $E = P \oplus P^{\perp}$, и $P^{\perp}$ невырождено. Заканчиваем доказательство по индукции.

Следствие 1. *Все знакопеременные невырожденные формы заданной размерности над полем k изометричны.*

Из теоремы 6 видно, что существует базис пространства E, относительно которого матрица знакопеременной формы имеет вид

$$\begin{pmatrix} 0 & 1 & & & & & & \\ -1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & -1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & 0 & 1 & \\ & & & & & -1 & 0 & \\ & & & & & & & 0 \end{pmatrix}.$$

Для удобства записи мы переупорядочим базисные элементы нашей ортогональной суммы гиперболических плоскостей таким образом, чтобы матрица формы приняла вид

$$\begin{pmatrix} 0 & I_r & 0 \\ -I_r & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

где I_r — единичная матрица размера $r \times r$. Матрица

$$\begin{pmatrix} 0 & I_r \\ -I_r & 0 \end{pmatrix}$$

называется *стандартной знакопеременной матрицей.*

Следствие 2. *Пусть E — векторное пространство над k с невырожденной симметрической формой, обозначаемой через $\langle , \rangle$, и Ω — невырожденная знакопеременная форма на E. Тогда существуют разложение в прямую сумму $E = E_1 \oplus E_2$ и симметрический автоморфизм A пространства E (относительно $\langle , \rangle$), обладающие следующим свойством. Если x, $y \in E$ записаны в виде*

$$x = (x_1, x_2), \quad \text{где} \quad x_1 \in E_1 \quad \text{и} \quad x_2 \in E_2,$$
$$y = (y_1, y_2), \quad \text{где} \quad y_1 \in E_1 \quad \text{и} \quad y_2 \in E_2,$$

то

$$\Omega(x, y) = \langle Ax_1, y_2 \rangle - \langle Ax_2, y_1 \rangle.$$

Доказательство. Возьмем такой базис в E, что матрица формы Ω относительно этого базиса является стандартной знакопе-

ременной матрицей. Пусть f — симметрическая невырожденная форма на E, задаваемая относительно этого базиса матрицей

$$\begin{pmatrix} 0 & I_r \\ I_r & 0 \end{pmatrix}.$$

Тогда мы получаем разложение E в прямую сумму подпространств E_1, E_2 (соответствующих первым n и соответственно последним n координатам), такое, что

$$\Omega(x, y) = f(x_1, y_2) - f(x_2, y_1).$$

Так как форма $\langle , \rangle$ предполагается невырожденной, то мы можем найти автоморфизм A, обладающий желаемым свойством, причем A является симметрическим, поскольку форма f симметрическая.

§ 10. Пфаффиан

У знакопеременной матрицы G по определению ${}^tG = -G$ и диагональные элементы равны 0 Как мы видели в гл. XIII, § 6, это матрица знакопеременной формы Пусть G — матрица размера $n \times n$, где n — четное. (Для нечетного n см. упражнения)

Мы начнем с поля характеристики 0 В силу теоремы 6 существует неособая матрица C, для которой ${}^tCGC$ будет матрицей

$$\begin{pmatrix} 0 & I_r & 0 \\ -I_r & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

и, следовательно,

$$\det(C)^2 \det(G) = 1 \quad \text{или} \quad 0$$

в соответствии с тем, тривиально ядро знакопеременной формы или нет Таким образом, мы видим, что в любом случае $\det(G)$ является квадратом в поле

Перейдем теперь к кольцу целых чисел $\mathbf{Z}$. Пусть t_{ij} $(1 \leqslant i < j \leqslant n)$ — $n(n-1)/2$ алгебраически независимых элементов над $\mathbf{Q}$. Положим $t_{ii} = 0$ для $i = 1, \ldots, n$ и $t_{ij} = -t_{ji}$ для $i > j$. Тогда матрица $T = (t_{ij})$ — знакопеременная и, следовательно, $\det(T)$ есть квадрат в поле $\mathbf{Q}(t)$, полученном из $\mathbf{Q}$ присоединением всех переменных t_{ij}. Однако $\det(T)$ является многочленом из $\mathbf{Z}[t]$ и в силу однозначности разложения на множители в $\mathbf{Z}[t]$ $\det(T)$ — квадрат некоторого многочлена из $\mathbf{Z}[t]$. Запишем

$$\det(T) = P(t)^2.$$

Многочлен P однозначно определен с точностью до множителя ± 1. Если мы подставим такие значения для t_{ij}, чтобы матрица T приняла специальный вид

$$\begin{pmatrix} 0 & I_{n/2} \\ -I_{n/2} & 0 \end{pmatrix},$$

то получим, что существует однозначно определенный многочлен P с целочисленными коэффициентами, принимающий значение 1 для этого специализированного множества значений (t). Мы будем называть P *общим пфаффианом* размера n и обозначать его через Pf.

Пусть R — коммутативное кольцо. Имеем гомоморфизм

$$\mathbf{Z}[t] \to R[t],$$

индуцированный однозначно определенным гомоморфизмом $\mathbf{Z}$ в R. Образ общего пфаффиана размера n в $R[t]$ будет многочленом с коэффициентами в R, который мы по-прежнему обозначаем через Pf. Если G — знакопеременная матрица с коэффициентами в R, то обозначим через $\mathrm{Pf}(G)$ значение $\mathrm{Pf}(t)$, полученное после подстановки g_{ij} вместо t_{ij} в Pf. Так как определитель коммутирует с гомоморфизмами, то имеет место

Теорема 7. *Пусть R — коммутативное кольцо и $(g_{ij}) = G$ — знакопеременная матрица с $g_{ij} \in R$. Тогда*

$$\det(G) = (\mathrm{Pf}(G))^2.$$

Кроме того, для всякой матрицы C размера $n \times n$ над R

$$\mathrm{Pf}(CG^tC) = \det(C)\,\mathrm{Pf}(G).$$

Доказательство. Первое утверждение уже было доказано выше. Второе достаточно доказать над $\mathbf{Z}$. Пусть элементы u_{ij} $(i, j = 1, \ldots, n)$ алгебраически независимы над $\mathbf{Q}$, причем u_{ij}, t_{ij} алгебраически независимы над $\mathbf{Q}$. Пусть U — матрица (u_{ij}). Тогда

$$\mathrm{Pf}(UT^tU) = \pm \det(U)\,\mathrm{Pf}(T),$$

что получается немедленно взятием квадратов от обеих частей. Подставим значения в U и T, такие, что U становится единичной матрицей, а T — стандартной знакопеременной матрицей. Заключаем, что с правой стороны должен быть знак $+$. Тем самым, как обычно, наше утверждение справедливо для любых подстановок вместо U матрицы над R и вместо T знакопеременной матрицы над R, что и требовалось показать.

§ 11. Эрмитовы формы

Пусть k_0 — некоторое упорядоченное поле (подполе поля вещественных чисел, если вам хочется), и пусть $k = k_0(i)$, где $i = \sqrt{-1}$. Тогда k обладает автоморфизмом порядка 2, неподвижным полем для которого служит k_0.

Пусть E — конечномерное векторное пространство над k. Мы будем рассматривать эрмитову форму на E, т. е. отображение

$$E \times E \to k,$$

записываемое в виде

$$(x, y) \mapsto \langle x, y \rangle,$$

которое k-линейно по своему первому аргументу, k-антилинейно по второму аргументу и таково, что

$$\langle x, y \rangle = \overline{\langle y, x \rangle}$$

для всех $x, y \in E$.

Заметим, что $\langle x, x \rangle \in k_0$ для всех $x \in E$. Это по существу является причиной того, что доказательства утверждений, касающихся симметрических форм, сохраняются без существенных изменений в эрмитовом случае. Мы сейчас перечислим свойства, относящиеся к этому случаю.

Теорема 8. *Существует ортогональный базис. Если форма невырожденная, то существует целое число $r \geqslant 0$, такое, что, каков бы ни был ортогональный базис $\{v_1, \ldots, v_n\}$, среди n элементов*

$$\langle v_1, v_1 \rangle, \ldots, \langle v_n, v_n \rangle$$

точно r больше 0 и $n - r$ меньше 0.

Ортогональный базис $\{v_1, \ldots, v_n\}$, для которого $\langle v_i, v_i \rangle = 1$ или -1, называется *ортонормальным базисом.*

Следствие 1. *Предположим, что форма невырождена и что всякий положительный элемент в k_0 является квадратом. Тогда существует ортонормальный базис.*

Мы будем говорить, что эрмитова форма *положительно определенная*, если $\langle x, x \rangle > 0$ для всех $x \in E$. Мы будем говорить, что она *отрицательно определенная*, если $\langle x, x \rangle < 0$ для всех $x \in E$.

Следствие 2. *Предположим, что форма невырождена. Тогда E допускает ортогональное разложение $E = E^+ \perp E^-$, такое, что форма является положительно определенной на E^+ и отрицательно определенной на E^-. Размерность E^+ (или E^-) одинакова во всех таких разложениях.*

Доказательства теоремы 8 и ее следствий идентичны доказательствам аналогичных результатов для симметрических форм и предоставляются читателю.

Для любого k-линейного отображения $A\colon E \to E$ имеет место *поляризационное тождество*, а именно

$$\langle A(x+y),\ (x+y)\rangle - \langle A(x-y),\ (x-y)\rangle = 2\,[\langle Ax,\ y\rangle + \langle Ay,\ x\rangle].$$

Если $\langle Ax,\ x\rangle = 0$ для всех x, то, заменив x на ix, получим

$$\langle Ax,\ y\rangle + \langle Ay,\ x\rangle = 0,$$
$$i\langle Ax,\ y\rangle - i\langle Ay,\ x\rangle = 0.$$

Отсюда заключаем:

если $\langle Ax,\ x\rangle = 0$ *для всех* x, *то* $A = 0$.

Это единственное утверждение, которое не имеет аналога в случае симметрических форм. Наличие i при получении одного из предыдущих линейных уравнений существенно для вывода. На практике это утверждение используется в комплексном случае и аналогичная ситуация встречается в вещественном случае, когда отображение A симметрическое. Формулировка для симметрических отображений очевидна.

Предположим, что эрмитова форма — положительно определенная и что всякий положительный элемент в k_0 *является квадратом.*

Имеет место *неравенство Шварца*, а именно

$$|\langle x,\ y\rangle|^2 \leqslant \langle x,\ x\rangle\langle y,\ y\rangle,$$

доказательство которого снова получается разложением

$$0 \leqslant \langle \alpha x + \beta y,\ \alpha x + \beta y\rangle$$

и подстановкой $\alpha = \langle y,\ y\rangle$ и $\beta = -\langle x,\ y\rangle$.

Определим норму $|x|$, положив

$$|x| = \sqrt{\langle x,\ x\rangle}.$$

Тогда сразу же получаем *неравенство треугольника*

$$|x+y| \leqslant |x| + |y|$$

и для $\alpha \in k$ равенство

$$|\alpha x| = |\alpha|\,|x|.$$

Точно так же, как в симметрическом случае, для заданного базиса можно найти ортонормальный базис посредством индуктивного процесса вычитания последовательных проекций. Мы предоставляем это читателю.

§ 12. Спектральная теорема (эрмитов случай)

В этом параграфе E будет конечномерным векторным пространством над $\mathbf{C}$ размерности $\geqslant 1$, снабженным положительно определенной эрмитовой формой $(x, y) \mapsto \langle x, y\rangle$.

Пусть $A\colon E \to E$ — линейное отображение (т. е. $\mathbf{C}$-линейное отображение) пространства E в себя. Для фиксированного $y \in E$ отображение $x \mapsto \langle Ax, y\rangle$ есть линейный функционал и, следовательно, существует однозначно определенный элемент $y^* \in E$, такой, что

$$\langle Ax, y\rangle = \langle x, y^*\rangle$$

для всех $x \in E$. Определим отображение $A^*\colon E \to E$, положив $A^*y = y^*$. Непосредственно ясно, что отображение A^* линейное; мы будем называть A^* *сопряженным* к A относительно нашей эрмитовой формы.

Тривиально проверяются следующие формулы для произвольных линейных отображений A, B пространства E в себя:

$$(A+B)^* = A^* + B^*, \quad A^{**} = A,$$
$$(\alpha A)^* = \bar{\alpha} A^*, \qquad (AB)^* = B^* A^*.$$

Линейное отображение A^* называется *самосопряженным* (или *эрмитовым*), если $A^* = A$.

Предложение 5. *Отображение A тогда и только тогда эрмитово, когда $\langle Ax, x\rangle$ вещественно для всех $x \in E$.*

Доказательство. Пусть A эрмитово. Тогда

$$\langle Ax, x\rangle = \overline{\langle x, Ax\rangle} = \langle x, Ax\rangle,$$

откуда вытекает, что $\langle Ax, x\rangle$ вещественно. Обратно, предположим, что $\langle Ax, x\rangle$ вещественно для всех x. Тогда

$$\langle Ax, x\rangle = \overline{\langle Ax, x\rangle} = \langle x, Ax\rangle = \langle A^*x, x\rangle$$

и, значит, $\langle (A - A^*)x, x\rangle = 0$ для всех x.

Следовательно, $A = A^*$ в силу поляризации.

Пусть $A\colon E \to E$ — линейное отображение, Элемент $\xi \in E$ называется *собственным вектором* отображения A, если существует такое $\lambda \in \mathbf{C}$, что $A\xi = \lambda\xi$. Если $\xi \neq 0$, то мы будем говорить, что λ — *собственное значение* отображения A, принадлежащее ξ.

Предложение 6. *Пусть A эрмитово. Тогда все собственные значения отображения A вещественны. Если ξ, ξ' — собственные векторы $\neq 0$, обладающие собственными значениями λ, λ' соответственно, и если $\lambda \neq \lambda'$, то $\xi \perp \xi'$.*

Доказательство. Пусть λ — собственное значение, принадлежащее собственному вектору $\xi \neq 0$. Тогда $\langle A\xi, \xi\rangle = \langle \xi, A\xi\rangle$, и эти два числа равны соответственно $\lambda\langle \xi, \xi\rangle$ и $\bar{\lambda}\langle \xi, \xi\rangle$. Так как $\xi \neq 0$, то $\lambda = \bar{\lambda}$, т. е. λ вещественно. Далее, предположим, что ξ, ξ' и λ, λ' таковы, как описано выше. Тогда

$$\langle A\xi, \xi'\rangle = \lambda\langle \xi, \xi'\rangle = \langle \xi, A\xi'\rangle = \lambda'\langle \xi, \xi'\rangle,$$

откуда вытекает, что $\langle \xi, \xi'\rangle = 0$.

Лемма. *Пусть A: $E \to E$ — линейное отображение и $\dim E \geqslant 1$. Тогда у A существует по крайней мере один ненулевой собственный вектор.*

Доказательство. Рассмотрим $\mathbf{C}[A]$ — кольцо, порожденное A над $\mathbf{C}$. Как векторное пространство над $\mathbf{C}$ оно содержится в кольце эндоморфизмов пространства E, имеющем такую же конечную размерность, какова размерность кольца всех матриц размера $n \times n$, где $n = \dim E$. Следовательно, существует ненулевой многочлен P с коэффициентами в $\mathbf{C}$, для которого $P(A) = 0$. Разложим P в произведение линейных множителей

$$P(X) = (X - \lambda_1) \ldots (X - \lambda_m),$$

где $\lambda_j \in \mathbf{C}$. Тогда $(A - \lambda_1 I) \ldots (A - \lambda_m I) = 0$. Следовательно, все множители $A - \lambda_j I$ не могут быть изоморфизмами, а потому существует $\lambda \in \mathbf{C}$, такое, что $A - \lambda I$ — не изоморфизм. Значит, в его ядре имеется элемент $\xi \neq 0$ и мы получаем, что $A\xi - \lambda\xi = 0$. Это показывает, что ξ — ненулевой собственный вектор, что и требовалось.

Спектральная теорема (эрмитов случай). *Пусть E — ненулевое векторное пространство над полем комплексных чисел с положительно определенной эрмитовой формой, A: $E \to E$ — эрмитово линейное отображение. Тогда E обладает ортогональным базисом, состоящим из собственных векторов A.*

Доказательство. Пусть ξ_1 — некоторый ненулевой собственный вектор с собственным значением λ_1 и E_1 — подпространство, порожденное ξ_1. Тогда A отображает $E_1^{\perp}$ в себя, поскольку

$$\langle AE_1^{\perp}, \xi_1\rangle = \langle E_1^{\perp}, A\xi_1\rangle = \langle E_1^{\perp}, \lambda_1\xi_1\rangle = \lambda_1\langle E_1^{\perp}, \xi_1\rangle = 0,$$

а потому $AE_1^{\perp}$ перпендикулярно ξ_1.

Так как $\xi_1 \neq 0$, то $\langle \xi_1, \xi_1\rangle > 0$, и, поскольку наша эрмитова форма невырождена (будучи положительно определенной), имеем

$$E = E_1 \oplus E_1^{\perp}.$$

Ограничение нашей формы на $E_1^{\perp}$ является положительно определенным (если $\dim E > 1$). Из предложения 5 тотчас видно, что ограничение A на $E_1^{\perp}$ эрмитово. Следовательно, мы можем завершить наше доказательство по индукции.

Следствие 1. *В предположениях теоремы существует ортонормальный базис, состоящий из собственных векторов A.*

Доказательство. Разделим каждый вектор ортогонального базиса на его норму.

Следствие 2. *Пусть E — ненулевое векторное пространство над полем комплексных чисел с положительно определенной эрмитовой формой f. Пусть g — другая эрмитова форма на E. Тогда существует базис в E, ортогональный и для f, и для g.*

Доказательство. Будем писать $f(x, y) = \langle x, y\rangle$. Так как форма f, будучи положительно определенной, неособая, то существует однозначно определенное эрмитово линейное отображение A, такое, что $g(x, y) = \langle Ax, y\rangle$ для всех $x, y \in E$. Применим теорему к A и найдем описанный в ней базис, скажем $\{v_1, \ldots, v_n\}$. Пусть λ_i — собственное значение, такое, что $Av_i = \lambda_i v_i$. Тогда

$$g(v_i, v_j) = \langle Av_i, v_j\rangle = \lambda_i \langle v_i, v_j\rangle,$$

а потому наш базис ортогонален также для g, что и требовалось показать.

§ 13. Спектральная теорема (симметрический случай)

Пусть E — векторное пространство над полем вещественных чисел, g — симметрическая положительно определенная форма на E. Если A: $E \to E$ — линейное отображение, то, как мы знаем, сопряженное к нему относительно g отображение ${}^tA$ определяется условием

$$\langle Ax, y\rangle = \langle x, {}^tAy\rangle$$

для всех $x, y \in E$. Мы говорим, что отображение A *симметрическое*, если $A = {}^tA$. Как и прежде, элемент $\xi \in E$ называется собственным вектором A, если существует число $\lambda \in \mathbf{R}$, такое, что $A\xi = \lambda\xi$, и если $\xi \neq 0$, то ξ называется собственным значением.

Спектральная теорема (симметрический случай). *Пусть E — ненулевое векторное пространство над полем вещественных чисел, A: $E \to E$ — симметрическое линейное отображение. Тогда E обладает ортогональным базисом, состоящим из собственных векторов отображения A.*

Доказательство. Мы сведем теорему к эрмитову случаю. Для этого введем *комплексную оболочку* (или *комплексификацию*) пространства E. Пусть

$$E_{\mathbf{C}} = E \oplus E$$

— прямая сумма E с собой. Если $a+bi$ — комплексное число, $a, b \in R$, и если (x, y) — элемент из $E_{\mathbf{C}}$, где $x, y \in E$, то определяем действие $\mathbf{C}$ на $E_{\mathbf{C}}$ формулой

$$(a+bi)(x, y) = (ax - by, bx + ay).$$

Прямое вычисление показывает, что $E_{\mathbf{C}}$ будет векторным пространством над $\mathbf{C}$. Если мы отождествим E с первым слагаемым, а именно с $(E, 0)$, то увидим, что

$$E_{\mathbf{C}} = E + iE,$$

и с учетом этого отождествления определенная выше операция мотивируется тем фактом, что

$$(a+bi)(x+iy) = ax - by + i(bx + ay).$$

Если $x+iy \in E_{\mathbf{C}}$, где $x, y \in E$, то определим $A_{\mathbf{C}}$: $E_{\mathbf{C}} \to E_{\mathbf{C}}$, положив

$$A_{\mathbf{C}}(x+iy) = Ax + iAy.$$

Тогда $A_{\mathbf{C}}$ является $\mathbf{C}$-линейным отображением $E_{\mathbf{C}}$ в себя, как видно непосредственно из определений.

Введем теперь эрмитову форму на $E_{\mathbf{C}}$. Если

$$v = x+iy, \quad w = x'+iy', \quad \text{где} \quad x, y, x', y' \in E,$$

то положим

$$\langle v, w\rangle_h = \langle x, x'\rangle + \langle y, y'\rangle + i\langle y, x'\rangle - i\langle x, y'\rangle.$$

Снова непосредственно проверяется, что h — эрмитова положительно определенная форма, так как g — симметрическая положительно определенная форма. Кроме того, из определений тотчас вытекает, что отображение $A_{\mathbf{C}}$ эрмитово относительно h.

Применим спектральную теорему для эрмитовых отображений. Мы можем найти ортогональный базис $\{\xi_1, \ldots, \xi_n\}$ пространства $E_{\mathbf{C}}$ над $\mathbf{C}$, состоящий из собственных векторов отображения $A_{\mathbf{C}}$ с вещественными собственными значениями $\lambda_1, \ldots, \lambda_n$ соответственно. Запишем

$$\xi_\nu = x_\nu + iy_\nu,$$

где $x_\nu, y_\nu \in E$. По определению собственного вектора имеем

$$A_{\mathbf{C}}\xi_\nu = \lambda_\nu \xi_\nu = \lambda_\nu x_\nu + i\lambda_\nu y_\nu.$$

Но

$$A_{\mathbf{C}}\xi_\nu = Ax_\nu + iAy_\nu.$$

Следовательно, $Ax_\nu = \lambda_\nu x_\nu$ и $Ay_\nu = \lambda_\nu y_\nu$. Среди собственных векторов $x_1, y_1, \ldots, x_n, y_n$ отображения A заведомо имеется n линейно независимых. Дополнительная ортогонализация Грама — Шмидта тех из них, которые соответствуют одному и тому же собственному значению λ, приводит к искомому ортогональному базису для E над $\mathbf{R}$. Теорема доказана.

Замечания. Спектральные теоремы справедливы над любым вещественно замкнутым полем; наши доказательства сохраняются без изменений. Кроме того, эти доказательства разумным образом близки к тем, которые могли бы быть даны в анализе для гильбертовых пространств и компактных операторов. Существование собственных значений и собственных векторов, однако, должно быть доказано другим методом, например, с использованием теоремы Гельфанда, которую мы фактически доказали в гл. XII, или вариационного принципа (т. е. нахождения максимума или минимума квадратичной функции, зависящей от оператора).

Следствие 1. *В предположениях теоремы существует ортонормальный базис, состоящий из собственных векторов отображения A.*

Доказательство. Разделим каждый вектор ортогонального базиса на его норму.

Следствие 2. *Пусть E — ненулевое векторное пространство над полем вещественных чисел с положительно определенной симметрической формой f. Пусть g — другая симметрическая форма на E. Тогда существует базис E, ортогональный и для f, и для g.*

Доказательство. Будем писать $f(x, y) = \langle x, y\rangle$. Так как форма f, будучи положительно определенной, неособая, то существует однозначно определенное симметрическое линейное отображение A, такое, что $g(x, y) = \langle Ax, y\rangle$ для всех $x, y \in E$. Применим к A теорему и найдем указанный в ней базис. Ясно, что это ортогональный базис для g (ср. аналогичное доказательство в эрмитовом случае).

УПРАЖНЕНИЯ

1. Пусть E — векторное пространство над полем k и g — билинейная форма на E. Предположим, что $g(y, x) = 0$ всякий раз, когда $g(x, y) = 0$ для какой-нибудь пары $x, y \in E$. Показать, что g либо симметрическая, либо знакопеременная.

2. Указать явно, каким образом $WG(k)$ гомоморфно отображается на $W(k)$.

3. Показать, что группа $WG(k)$ может быть представлена в виде гомоморфного образа $\mathbf{Z}[k^*/k^{*2}]$. [*Указание*: использовать существование ортогонального базиса.]

4. Пусть E — модуль над $\mathbf{Z}$ свободный, размерности $n \geqslant 1$, и пусть f — билинейная знакопеременная форма на E. Показать, что существуют базис $\{e_i\}$ $(i = 1, \ldots, n)$ и целое число r, такие, что $2r \leqslant n$,

$$e_1 \cdot e_2 = a_1, \quad e_3 \cdot e_4 = a_2, \ \ldots, \ e_{2r-1} \cdot e_{2r} = a_r,$$

где $a_1, \ldots, a_r \in \mathbf{Z}$, $a_i \neq 0$ и a_i делит a_{i+1} для $i = 1, \ldots, r-1$ и, наконец, $e_i \cdot e_j = 0$ для всех других пар индексов $i \leqslant j$. Показать, что идеалы $\mathbf{Z}a_i$ однозначно определены. [*Указание*: взять гомоморфизм φ_f: $E \to E^*$ модуля E в дуальный модуль над $\mathbf{Z}$ и рассмотреть $\varphi_f(E)$ как свободный подмодуль в E^*.] Обобщить на кольца главных идеалов, когда вы узнаете основную теорему для модулей над этими кольцами.

5. Пусть E — конечномерное пространство над R, g — симметрическая положительно определенная форма на E, A — симметрический относительно g эндоморфизм пространства E. По определению $A \geqslant 0$ означает, что $\langle Ax, x\rangle \geqslant 0$ для всех $x \in E$. Показать, что $A \geqslant 0$ в том и только в том случае, если все собственные значения A не меньше 0.

6. Доказать все свойства пфаффиана, сформулированные в „Геометрической алгебре", стр. 142.

7. Теорема Витта справедлива и для знакопеременных форм. Доказать (или прочитать у Артина или Бурбаки).

8. Показать, что пфаффиан знакопеременной матрицы размера $n \times n$ равен 0, если n нечетно.

9. Дать определение отображений степени > 2 из одного модуля в другой. [*Указание*: для степени 3 рассмотреть выражение

$$f(x+y+z) - f(x+y) - f(x+z) - f(y+z) + f(x) + f(y) + f(z).]$$

Обобщить на отображения высших степеней утверждение, доказанное для квадратичных отображений (т. е. единственность различных полилинейных отображений, входящих в их определения).

10. (а) Пусть E — конечномерное пространство над полем комплексных чисел и h: $E \times E \to \mathbf{C}$ — эрмитова форма

$$h(x, y) = g(x, y) + if(x+y),$$

где f, g принимают вещественные значения. Показать, что g, f — $\mathbf{R}$-билинейные формы: g — симметрическая и f — знакопеременная.

(б) Пусть E — конечномерное пространство над $\mathbf{C}$, g: $E \times E \to \mathbf{C}$ — $\mathbf{R}$-билинейная форма. Предположим, что для всех $x \in E$ отображение $y \mapsto g(x, y)$ C-линейно и что R-билинейная форма

$$f(x, y) = g(x, y) - g(y, x)$$

вещественнозначна на $E \times E$. Показать, что на E существуют эрмитова форма h и симметрическая $\mathbf{C}$-билинейная форма ψ, такие, что $2ig = h + \psi$. Показать, что h и ψ однозначно определены.

11. Показать, что в условиях эрмитовой спектральной теоремы E обладает разложением в прямую сумму над $\mathbf{R}$, $E = F + iF$, таким, что E изоморфно комплексной оболочке F и A индуцирует линейное симметрическое отображение на F.

12. Пусть E — конечномерное пространство над полем комплексных чисел с положительно определенной эрмитовой формой, S — некоторое множество (С-линейных) эндоморфизмов E, не обладающее другими инвариантными подпространствами, кроме 0 и E (это означает, что если F — подпространство в E и $BF \subset F$ для всех $B \in S$, то $F = 0$ или $F = E$). Пусть A — эрмитово отображение E в себя, такое, что $AB = BA$ для всех $B \in S$. Показать, что $A = \lambda I$ для некоторого вещественного числа λ. [*Указание*: показать, что у A имеется точно одно собственное значение. Если бы было два собственных значения, скажем $\lambda_1 \neq \lambda_2$, то можно было бы найти два многочлена f и g с вещественными коэффициентами, для которых $f(A) \neq 0$, $g(A) \neq 0$, но $f(A)\, g(A) = 0$. Взять в качестве F ядро эндоморфизма $g(A)$ и получить противоречие.]

13. Пусть E обозначает то же, что и в упражнении 12, T — С-линейное отображение E в себя и

$$A = \frac{1}{2}(T + T^*).$$

Показать, что A эрмитово. Показать, что T можно записать в виде $A + iB$, где A, B эрмитовы и однозначно определены.

14. Пусть S — коммутативное множество С-линейных эндоморфизмов конечномерного пространства E, не имеющее инвариантного подпространства, отличного от 0 или E. Предположим, что $B^* \in S$, как только $B \in S$. Показать, что всякий элемент из S имеет вид αI для некоторого комплексного числа α и, следовательно, E одномерно. [*Указание*: пусть $B_0 \in S$. Положим

$$A = \frac{1}{2}(B_0 + B_0^*).$$

Показать, что $A = \lambda I$ для некоторого вещественного λ.]

15. Эндоморфизм B пространства E называется *нормальным*, если B коммутирует с B^*. Сформулировать и доказать спектральную теорему для нормальных эндоморфизмов.

16. Пусть E — конечномерное векторное пространство над полем вещественных чисел, $\langle\ ,\ \rangle$ — симметрическая положительно определенная форма на E, Ω — невырожденная знакопеременная форма на E. Показать, что существует разложение в прямую сумму

$$E = E_1 \oplus E_2,$$

обладающее следующим свойством. Если элементы x, $y \in E$ записаны в виде

$$x = (x_1, x_2), \quad \text{где} \quad x_1 \in E_1 \quad \text{и} \quad x_2 \in E_2,$$
$$y = (y_1, y_2), \quad \text{где} \quad y_1 \in E_1 \quad \text{и} \quad y_1 \in E_2,$$

то $\Omega(x, y) = \langle x_1, y_2\rangle - \langle x_2, y_1\rangle$. [*Указание*: использовать следствие 2 из теоремы 6. Показать, что эндоморфизм A — положительно определенный (см. упражнение 18), взять квадратный корень из A и преобразовать при его помощи прямое разложение, полученное в этом следствии.]

17. Пусть E — векторное пространство над полем вещественных чисел (как обычно, конечномерное). Для всякого эндоморфизма A пространства E примем за его *норму* $|A|$ наибольшую нижнюю грань всех чисел C, для которых $|Ax| \leqslant C|x|$. Показать, что эта норма удовлетворяет неравенству треугольника. Показать, что ряд

$$\exp(A) = I + A + \frac{A^2}{2!} + \ldots$$

сходится и что если A коммутирует с B, то $\exp(A+B)=\exp(A)\exp(B)$. Показать, что если A достаточно близок к I, то ряд

$$-\log(A)=\frac{(I-A)}{1}+\frac{(I-A)^2}{2}+\dots$$

сходится, и если A коммутирует с B, то

$$\log(AB)=\log A+\log B.$$

18. Пусть пространство E обладает фиксированной положительно определенной симметрической билинейной формой. Мы будем называть E *гильбертовым пространством* (конечномерным). *Линейный автоморфизм* A пространства E называется *гильбертовым*, если он является автоморфизмом формы, т. е. ${}^tAA=I$. В настоящих упражнениях мы будем писать A^* вместо ${}^tA$. Пусть A — симметрический эндоморфизм на E. Мы будем говорить, что A — *положительно определенный*, если $\langle Ax, x\rangle > 0$ для всех $x\in E$, $x\neq 0$.

Доказать: если A — симметрический (соответственно знакопеременный), то $\exp(A)$ — симметрический положительно определенный (соответственно гильбертов). Если A — линейный автоморфизм, достаточно близкий к I и являющийся симметрическим положительно определенным (соответственно гильбертовым), то $\log A$ — симметрический (соответственно знакопеременный).

19. Используя спектральную теорему, показать, что $\log A$ можно определить, когда A — симметрический положительно определенный, не обязательно близкий к I. Показать, что любой автоморфизм A пространства E может быть записан единственным образом в виде произведения $A=HP$, где H — гильбертов, а P — симметрический положительно определенный. [*Указание*: заметить, что A^*A — симметрический положительно определенный, и взять $P=(A^*A)^{1/2}$, где квадратный корень находится с помощью спектральной теоремы. Положив $H=AP^{-1}$, получить существование искомого произведения. Для единственности предположить, что $A=H_1P_1$, и положить $H_2=PP_1^{-1}$. Тогда $I=H_2^*H_2$; используя равенства $P^*=P$, $P_1^*=P_1$, заключить, что $P^2=P_1^2$. Взять log, разделить на 2 и, взяв exp, заключить, что $P=P_1$.]

20. (Т е й т) Пусть E, F — полные нормированные векторные пространства под полем вещественных чисел и $f\colon E\to F$ — отображение, обладающее следующим свойством. Существует число C, такое, что для всех x, $y\in E$ имеем

$$|f(x+y)-f(x)-f(y)|\leqslant C.$$

Показать, что существует единственное линейное отображение $g\colon E\to F$, для которого норма $|g-f|$ ограничена (т. е. $|g(x)-f(x)|$ ограничена как функция от x). Обобщить на билинейный случай. [*Указание*: положить

$$g(x)=\lim_{n\to\infty}\frac{f(2^nx)}{2^n}.]$$

Глава XV

Представление одного эндоморфизма

§ 1. Представления

Пусть k — коммутативное кольцо и E — модуль над k. Как обычно, мы обозначаем через $\mathrm{End}_k(E)$ кольцо k-эндоморфизмов E, т. е. кольцо k-линейных отображений E в себя.

Пусть R — некоторая k-алгебра (задаваемая кольцевым гомоморфизмом $k \to R$, который позволяет нам рассматривать R как k-модуль). Под *представлением* R в E понимают гомоморфизм k-алгебр $R \to \mathrm{End}_k(E)$, т. е. кольцевой гомоморфизм $\rho\colon R \to \mathrm{End}_k(E)$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} R & \longrightarrow & \mathrm{End}_k(E) \\ & \nwarrow \quad \nearrow & \\ & k & \end{array}$$

[Как обычно, мы рассматриваем $\mathrm{End}_k(E)$ как k-алгебру; если I обозначает тождественное отображение модуля E, то имеем гомоморфизм кольца k в $\mathrm{End}_k(E)$, задаваемый отображением $a \mapsto aI$. Мы будем использовать I также для обозначения единичной матрицы, когда выбраны базисы. Что мы имеем в виду, всегда будет ясно из контекста.]

Мы встретимся в дальнейшем с несколькими примерами представлений для различных типов колец (и коммутативных, и некоммутативных). В этой главе все кольца будут коммутативными.

Заметим, что E можно рассматривать как $\mathrm{End}_k(E)$-модуль. Следовательно, E можно рассматривать как R-модуль, определив действие R на E следующим образом:

$$(x, v) \mapsto \rho(x)\, v,$$

где $x \in R$ и $v \in E$. Мы будем обычно писать xv вместо $\rho(x)\, v$.

Подгруппа F в E, такая, что $RF \subset F$, будет называться *инвариантным* подмодулем в E. (Она одновременно R-инвариантна и k-инвариантна.) Мы будем также говорить, что она инвариантна относительно данного представления.

Мы будем говорить, что представление *неприводимо*, или *просто*, если $E \neq 0$ и если единственными инвариантными подмодулями

являются 0 и E. Неприводимым (или простым) называется в этом случае и сам модуль E.

Цель теории представлений состоит в том, чтобы описать структуру всех представлений различных интересных колец и классифицировать их неприводимые представления. В большинстве случаев мы будем брать в качестве k поле, которое может быть, а может и не быть алгебраически замкнутым. Трудности в доказательстве теорем о представлениях могут поэтому лежать в сложности или кольца R, или поля k, или модуля E, или всех трех вместе.

Указанное выше представление ρ называется *вполне приводимым*, или *полупростым*, если E есть R-прямая сумма R-подмодулей E_i

$$E = E_1 \oplus \ldots \oplus E_m,$$

причем каждый E_i неприводим. Мы также говорим, что E вполне приводим. Неверно, что все представления вполне приводимы, и, например, те, которые мы будем рассматривать в этой главе, как правило, не будут такими. Некоторые типы вполне приводимых представлений будут изучены позже.

Имеется специальный тип представлений, который будет встречаться особенно часто. Пусть $v \in E$, и пусть $E = Rv$. Мы пишем также $E = (v)$. Тогда мы говорим, что модуль E — *главный* (над R) и что представление — *главное*. В этом случае множество элементов $x \in R$, для которых $xv = 0$, будет левым идеалом $\mathfrak{a}$ в R (очевидно). Отображение R в E, задаваемое правилом

$$x \longmapsto xv,$$

индуцирует изоморфизм R-модулей

$$R/\mathfrak{a} \to E$$

(R рассматривается как левый модуль над собой и $R/\mathfrak{a}$ — как фактормодуль). При этом отображении единичному элементу 1 кольца R сопоставляется образующая v модуля E.

Примем следующее соглашение: если $v_1, \ldots, v_n \in E$, то будем обозначать через $(v_1, \ldots, v_n)$ подмодуль в E, порожденный элементами $v_1, \ldots, v_n$.

Пусть E имеет некоторое разложение в прямую сумму R-подмодулей

$$E = E_1 \oplus \ldots \oplus E_s.$$

Предположим, что каждый E_i свободен и имеет размерность $\geqslant 1$ над k. Пусть $\mathscr{B}_1, \ldots, \mathscr{B}_s$ — базисы над k для $E_1, \ldots, E_s$ соответственно. Тогда $\{\mathscr{B}_1, \ldots, \mathscr{B}_s\}$ есть базис для E. Пусть $\varphi \in R$, φ_i — эндоморфизмы, индуцированные φ на E_i, и M_i — матрица φ_i относительно базиса $\mathscr{B}_i$. Тогда матрица M эндоморфизма φ относительно

$\{\mathscr{B}_1, \ldots, \mathscr{B}_s\}$ принимает вид

$$\begin{pmatrix} M_1 & 0 & \ldots & 0 \\ 0 & M_2 & \ldots & 0 \\ \cdot & \cdot & & \\ \cdot & & \cdot & \\ \cdot & & & \cdot \\ 0 & \cdot & \cdot & \cdot \quad 0 \\ 0 & \cdot & \cdot & \cdot \quad 0 \quad M_s \end{pmatrix}.$$

Про матрицу такого типа говорят, что она разлагается на *блоки* $M_1, \ldots, M_s$. При наличии такого разложения изучение эндоморфизма φ или его матрицы полностью сводится (так сказать) к изучению блоков.

Это случается далеко не всегда, однако часто имеет место нечто почти столь же хорошее. Пусть E' — подмодуль в E, инвариантный относительно R. Предположим, что имеется базис E' над k, скажем $\{v_1, \ldots, v_m\}$, и что этот базис может быть дополнен до базиса

$$\{v_1, \ldots, v_m, v_{m+1}, \ldots, v_n\}.$$

Это всегда так, если k — поле.

Пусть $\varphi \in R$. Тогда матрица эндоморфизма φ относительно этого базиса имеет вид

$$\begin{pmatrix} M' & * \\ 0 & M'' \end{pmatrix}.$$

Действительно, так как E' отображается при φ в себя, то ясно, что мы получим M' в левом верхнем углу и нулевую матрицу под ним. Кроме того, для всякого $j = m+1, \ldots, n$ мы можем записать

$$\varphi v_j = c_{j1}v_1 + \ldots + c_{jm}v_m + c_{j,\,m+1}v_{m+1} + \ldots + c_{mn}v_n.$$

Транспонируя матрицу (c_{ji}), получаем матрицу

$$\begin{pmatrix} * \\ M'' \end{pmatrix},$$

стоящую справа в матрице, представляющей φ.

Рассмотрим, далее, точную последовательность

$$0 \to E' \to E \to E'' \to 0.$$

Пусть $\bar{v}_{m+1}, \ldots, \bar{v}_n$ — образы $v_{m+1}, \ldots, v_n$ при каноническом отображении $E \to E''$. Мы можем естественным образом определить линейное отображение

$$\varphi'' \colon E'' \to E'',$$

так чтобы $\overline{\varphi v} = \varphi''(\bar{v})$ для всех $v \in E$. Тогда ясно, что матрицей для φ'' относительно базиса $\{\bar{v}_{m+1}, \ldots, \bar{v}_n\}$ служит M''.

§ 2. Модули над кольцами главных идеалов

В этом параграфе мы предполагаем, что R — целостное кольцо главных идеалов. Все рассматриваемые модули и гомоморфизмы являются, если не оговорено противное, модулями над R и R-гомоморфизмами.

Теоремы этого параграфа обобщают утверждения, доказанные в гл. I для абелевых групп. Мы будем также указывать, как следует видоизменить доказательства из гл. I, чтобы после изменения терминологии получить доказательства для настоящего случая.

Пусть F — свободный модуль над R с базисом $\{x_i\}_{i\in I}$. Тогда мощность I однозначно определена (и называется размерностью F). Напомним, что это доказывается, скажем, рассмотрением простого элемента p в R и тем наблюдением, что F/pF есть векторное пространство над полем R/pR, размерность которого в точности равна мощности I. Таким образом, мы можем говорить о размерности свободного модуля над R.

Теорема 1. *Пусть F — свободный модуль и M — некоторый его подмодуль. Тогда M свободен и его размерность меньше или равна размерности F.*

Доказательство. Для простоты мы дадим доказательство для случая, когда F имеет конечный базис $\{x_i\}$, $i=1, \ldots, n$. Пусть M_r — пересечение M с $(x_1, \ldots, x_r)$ — модулем, порожденным элементами $x_1, \ldots, x_r$. Тогда $M_1 = M \cap (x_1)$ — подмодуль в (x_1), а потому имеет вид (a_1x_1) для некоторого $a_1 \in R$. Следовательно, M_1 либо нулевой, либо свободный размерности 1. Предположим по индукции, что M_r — свободный модуль размерности $\leqslant r$. Пусть $\mathfrak{a}$ — множество, состоящее из всех элементов $a \in R$, таких, что существует элемент $x \in M$, который может быть записан в виде

$$x = b_1x_1 + \ldots + b_rx_r + ax_{r+1},$$

где $b_i \in R$. Тогда, очевидно, $\mathfrak{a}$ — идеал, и, следовательно, главный идеал, порожденный некоторым элементом a_{r+1}. Если $a_{r+1} = 0$, то $M_{r+1} = M_r$ и индуктивный шаг сделан. Если $a_{r+1} \neq 0$, то пусть элемент $w \in M_{r+1}$ таков, что его коэффициент при x_{r+1} равен a_{r+1}. Если элемент $x \in M_{r+1}$, то его коэффициент при x_{r+1} делится на a_{r+1} и, значит, существует элемент $c \in R$, такой, что $x - cw$ лежит в M_r. Следовательно,

$$M = M_r + (w).$$

С другой стороны, ясно, что $M_r \cap (w)$ есть 0 и, следовательно, эта сумма прямая, что и доказывает нашу теорему. Отметим, что это доказательство с заменой простой индукции трансфинитной остается справедливым и в бесконечном случае.

Следствие. *Всякий подмодуль E' конечно порожденного модуля E конечно порожденный.*

Доказательство. Мы можем представить E как фактормодуль свободного модуля с конечным числом образующих; если $v_1, \ldots, v_n$ — образующие E, то возьмем свободный модуль F с базисом $\{x_1, \ldots, x_n\}$ и отобразим x_i на v_i. Прообраз E' в F свободен и конечно порожден, согласно теореме. Следовательно, E' — конечно порожденный модуль. Утверждение вытекает также из простейших свойств нетеровых колец и модулей.

Если желать перенести на модули над кольцом главных идеалов доказательства из гл. I, то нужно принять следующие определения. Свободный одномерный модуль над R называется *бесконечным циклическим*. Бесконечный циклический модуль изоморфен кольцу R, рассматриваемому как модуль над собой. Таким образом, всякий ненулевой подмодуль бесконечного циклического модуля является бесконечным циклическим. Доказательство, данное в гл. I для аналога теоремы 1, применимо теперь без дальнейших изменений.

Пусть E — модуль. Элемент x модуля E называется *периодическим*, если существует элемент $a \in R$, $a \neq 0$, для которого $ax = 0$. Мы говорим, что E — *периодический* модуль, если все его элементы периодические. Обобщением *конечной абелевой группы* служит *конечно порожденный периодический модуль*.

Пусть E — модуль. Обозначим через E_t подмодуль, состоящий из всех периодических элементов E; мы будем называть его *подмодулем кручения* модуля E. Если $E_t = 0$, то мы будем говорить, что E — *модуль без кручения*.

Теорема 2. *Пусть E — конечно порожденный модуль. Тогда модуль E/E_t свободный. Существует свободный подмодуль F в E, такой, что E есть прямая сумма*

$$E = E_t \oplus F.$$

Размерность такого подмодуля F однозначно определена.

Доказательство. Докажем сначала, что модуль E/E_t без кручения. Обозначим через $\bar{x}$ класс вычетов элемента $x \in E$ по модулю E_t. Пусть элемент $b \in R$, $b \neq 0$, таков, что $b\bar{x} = 0$. Тогда $bx \in E_t$ и, значит, существует элемент $c \in R$, $c \neq 0$, для которого $cbx = 0$. Следовательно, $x \in E_t$ и $\bar{x} = 0$, что доказывает отсутствие кручения у модуля E/E_t. Этот модуль является также конечно порожденным. Предположим теперь, что M — конечно порожденный модуль без кручения. Пусть $\{v_1, \ldots, v_n\}$ — максимальное множество элементов в M среди данного конечного множества образующих $\{y_1, \ldots, y_m\}$, такое, что множество $\{v_1, \ldots, v_n\}$ линейно независимо.

Если y — одна из образующих, то найдутся элементы $a, b_1, \ldots, b_n \in R$, не все равные 0, такие, что

$$ay + b_1v_1 + \ldots + b_nv_n = 0.$$

Тогда $a \neq 0$ (иначе мы придем в противоречие с линейной независимостью $v_1, \ldots, v_n$). Следовательно, ay лежит в $(v_1, \ldots, v_n)$. Таким образом, для каждого $j = 1, \ldots, m$ мы можем найти элемент $a_j \in R$, $a_j \neq 0$, такой, что a_jy_j лежит в $(v_1, \ldots, v_n)$. Пусть $a = a_1 \ldots \ldots a_m$ — произведение этих элементов. Тогда aM содержится в $(v_1, \ldots, v_n)$ и $a \neq 0$. Отображение

$$x \longmapsto ax$$

является инъективным гомоморфизмом, образ которого содержится в свободном модуле, а потому в силу теоремы 1 свободен. Этот образ изоморфен M, и мы заключаем, что модуль M свободен, что и требовалось доказать.

Чтобы теперь получить подмодуль F, нам нужна лемма.

Лемма 1. *Пусть E, E' — модули, причем модуль E' свободен. Пусть $f\colon E \to E'$ — сюръективный гомоморфизм. Тогда существует свободный подмодуль F в B, такой, что ограничение f на F индуцирует изоморфизм F с E', и такой, что $E = F \oplus \operatorname{Ker} f$.*

Доказательство. Пусть $\{x_i'\}_{i \in I}$ — базис модуля E'. Обозначим через x_i, $i \in I$, элемент из E, для которого $f(x_i) = x_i'$. Пусть F — подмодуль в E, порожденный всеми элементами x_i, $i \in I$. Тогда сразу же видно, что семейство элементов $\{x_i\}_{i \in I}$ линейно независимо и поэтому модуль F свободен. Для заданного $x \in E$ существуют элементы $a_i \in R$, такие, что

$$f(x) = \sum a_i x_i'.$$

Тогда $x - \sum a_i x_i$ лежит в ядре f, а потому $E = \operatorname{Ker} f + F$. Ясно, что $\operatorname{Ker} f \cap F = 0$ и, следовательно, эта сумма прямая, что и доказывает лемму.

Применив лемму к гомоморфизму $E \to E/E_t$ в теореме 2, получим наше разложение $E = E_t \oplus F$. Размерность F однозначно определена, поскольку для любого такого разложения E в прямую сумму модуль F изоморфен E/E_t.

Размерность свободного модуля F в теореме 2 называется *рангом* модуля E.

Чтобы получить структурную теорему для конечно порожденных модулей над R, можно действовать дальше точно так же, как в слу-

чае абелевых групп. Мы приведем словарь, который позволит нам перенести доказательства по существу без всяких изменений.

Пусть E — модуль над R, $x \in E$. Отображение $a \longmapsto ax$ является гомоморфизмом R на подмодуль, порожденный элементом x, и ядро этого гомоморфизма является главным идеалом, порожденным некоторым элементом $m \in R$. Мы будем говорить, что m — *период* элемента x. Отметим, что период m определен однозначно с точностью до умножения на единицу (если $m \neq 0$). Элемент $c \in R$, $c \neq 0$, называется *показателем* модуля E (соответственно элемента x), если $cE = 0$ (соответственно $cx = 0$).

Пусть p — простой элемент. Обозначим через $E(p)$ подмодуль в E, состоящий из всех элементов x, обладающих показателем вида $p^r (r \geqslant 1)$. Подмодуль, содержащийся в $E(p)$, называется *p-подмодулем* в E.

Выберем раз и навсегда некоторую систему представителей для простых элементов кольца R (по модулю единиц). Например, если R — кольцо многочленов от одного переменного над полем, то возьмем в качестве представителей неприводимые многочлены со старшим коэффициентом 1.

Пусть $m \in R$, $m \neq 0$. Обозначим через E_m ядро отображения $x \longmapsto mx$. Оно состоит из всех элементов модуля E, имеющих показатель m.

Модуль E называется *циклическим*, если он изоморфен фактормодулю $R/(a)$ для некоторого элемента $a \in R$. Не теряя общности, мы можем считать, что a является произведением простых элементов из нашей системы представителей (если $a \neq 0$). Мы могли бы сказать, что a есть порядок нашего модуля.

Пусть $r_1, \ldots, r_s$ — целые числа $\geqslant 1$. Модулем *типа*

$$(p^{r_1}, \ldots, p^{r_s})$$

называется p-модуль E, изоморфный прямому произведению циклических модулей $R/(p^{r_i})$ $(i = 1, \ldots, s)$. Если простой элемент p фиксирован, то можно говорить, что модуль имеет тип $(r_1, \ldots, r_s)$ (относительно p).

Все доказательства из гл. I, § 10, проходят теперь без изменений. Там, где раньше мы оперировали с величиной какого-либо целого положительного числа m, теперь мы будем в аналогичном рассуждении оперировать с числом простых сомножителей в простом разложении элемента. Имея дело со степенью p^r простого элемента, можно считать, что порядок определяется числом r. Читатель проверит дальше сам, что все доказательства из гл. I, § 10 теперь применимы.

Однако мы будем развивать теорию заново, не предполагая ничего известным из гл. I, § 10. Таким образом, наше изложение будет независимым.

Теорема 3. *Пусть E — конечно порожденный периодический модуль $\neq 0$. Тогда E будет прямой суммой*

$$E = \coprod_p E(p),$$

взятой по всем простым p, таким, что $E(p) \neq 0$. Каждый модуль $E(p)$ может быть записан в виде прямой суммы

$$E(p) = R/(p^{\nu_1}) \oplus \ldots \oplus R/(p^{\nu_s}),$$

где $1 \leqslant \nu_1 \leqslant \ldots \leqslant \nu_s$. Последовательность $\nu_1, \ldots, \nu_s$ однозначно определена.

Доказательство. Пусть a — некоторый показатель для E. Допустим, что $a = bc$, где $(b, c) = (1)$. Пусть $x, y \in R$ — такие элементы, что

$$1 = xb + yc.$$

Мы утверждаем, что $E = E_b \oplus E_c$. Наше первое утверждение получится затем по индукции из представления a в виде произведения степеней простых элементов. Пусть $v \in E$. Тогда

$$v = xbv + ycv.$$

Здесь $xbv \in E_c$, так как $cxbv = xav = 0$. Аналогично $ycv \in E_b$. Наконец, непосредственно видно, что $E_b \cap E_c = 0$. Следовательно, E есть прямая сумма E_b и E_c.

Теперь мы должны доказать, что $E(p)$ является прямой суммой указанного выше вида. Будем говорить, что элементы $y_1, \ldots, y_m$ некоторого модуля *независимы*, если, каково бы ни было соотношение

$$a_1 y_1 + \ldots + a_m y_m = 0,$$

где $a_i \in R$, мы должны иметь $a_i y_i = 0$ для всех i. (Отметим, что *независимость* не означает *линейной независимости*.) Тотчас видно, что элементы $y_1, \ldots, y_m$ тогда и только тогда независимы, когда модуль $(y_1, \ldots, y_m)$ обладает разложением в прямую сумму

$$(y_1, \ldots, y_m) = (y_1) \oplus \ldots \oplus (y_m)$$

циклических модулей (y_i), $i = 1, \ldots, m$.

Теперь нам нужен аналог леммы 1 для модулей, имеющих показатель, равный степени простого элемента.

Лемма 2. *Пусть E — периодический модуль показателя p^r $(r \geqslant 1)$, где p — некоторый простой элемент. Пусть $x_1 \in E$ — элемент периода p^r, $\bar{E} = E/(x_1)$ и $\bar{y}_1, \ldots, \bar{y}_m$ — независимые элементы из $\bar{E}$. Для всякого i существует представитель $y_i \in E$ класса $\bar{y}_i$, такой, что период y_i равен периоду $\bar{y}_i$. Элементы $x_1, y_1, \ldots, y_m$ независимы.*

Доказательство. Пусть элемент $\bar{y} \in \bar{E}$ имеет период p^n для некоторого $n \geqslant 1$ и y — представитель класса $\bar{y}$ в E. Тогда $p^n y \in (x_1)$ и, следовательно,

$$p^n y = p^s c x_1, \quad c \in R, \quad p \nmid c$$

для некоторого $s \leqslant r$. Если $s = r$, то мы видим, что y имеет тот же период, что и $\bar{y}$. Если $s < r$, то $p^s c x_1$ имеет период p^{r-s} и, следовательно, y имеет период p^{n+r-s}. Должно выполняться неравенство

$$n + r - s \leqslant r,$$

поскольку p^r — показатель для E. Таким образом, $s \geqslant n$ и мы видим, что

$$y - p^{s-n} c x_1$$

есть представитель для $\bar{y}$, период которого равен p^n.

Пусть y_i — представитель для $\bar{y}_i$, имеющий тот же период. Докажем, что элементы $x_1, y_1, \ldots, y_m$ независимы. Допустим, что $a, a_1, \ldots, a_m \in R$ такие элементы, что

$$a x_1 + a_1 y_1 + \ldots + a_m y_m = 0.$$

Тогда

$$a_1 \bar{y}_1 + \ldots + a_m \bar{y}_m = 0.$$

По предположению $a_i \bar{y}_i = 0$ для всякого i. Если p^{r_i} — период $\bar{y}_i$, то p^{r_i} делит a_i. Отсюда заключаем, что $a_i y_i = 0$ для всякого i и что, следовательно, $a x_1 = 0$; тем самым требуемая независимость доказана.

Чтобы теперь получить разложение $E(p)$ в прямую сумму, заметим сперва, что модуль $E(p)$ — конечно порожденный. Мы можем предполагать, не теряя общности, что $E = E(p)$. Пусть x_1 — элемент из E, период которого p^{r_1} таков, что число r_1 максимально. Пусть $\bar{E} = E/(x_1)$. Мы утверждаем, что $\dim \bar{E}_p$ как векторного пространства над R/pR строго меньше, чем $\dim E_p$. Действительно, если $\bar{y}_1, \ldots, \bar{y}_m$ — линейно независимые элементы из $\bar{E}_p$ над R/pR, то из леммы 2 вытекает, что $\dim E_p \geqslant m + 1$, так как мы всегда можем найти в (x_1) элемент, имеющий период p и не зависимый от $y_1, \ldots, y_m$. Следовательно, $\dim \bar{E}_p < \dim E_p$. Поэтому мы можем доказать существование разложения в прямую сумму по индукции. Если $\bar{E} \neq 0$, то существуют элементы $\bar{x}_2, \ldots, \bar{x}_s$, имеющие соответственно периоды $p^{r_2}, \ldots, p^{r_s}$ и такие, что $r_2 \geqslant \ldots \geqslant r_s$. В силу леммы 2 существуют представители $x_2, \ldots, x_s$ в E, такие, что x_i имеет период p^{r_i} и $x_1, \ldots, x_s$ независимы. Поскольку период p^{r_1}

был выбран максимальным, мы имеем неравенство $r_1 \geqslant r_2$ и наше разложение получено.

Единственность будет следствием более общей теоремы единственности, которую мы сейчас сформулируем.

Теорема 4. *Пусть E — конечно порожденный периодический модуль, $E \neq 0$. Тогда E изоморфен прямой сумме ненулевых слагаемых*

$$R/(q_1) \oplus \ldots \oplus R/(q_r),$$

где $q_1, \ldots, q_r$ — ненулевые элементы из R и $q_1 | q_2 | \ldots | q_r$. Последовательность идеалов $(q_1), \ldots, (q_r)$ однозначно определена предыдущими условиями.

Доказательство. Используя теорему 3, разложим E в прямую сумму p-подмодулей, скажем $E(p_1) \oplus \ldots \oplus E(p_l)$, а затем разложим каждый $E(p_i)$ в прямую сумму циклических подмодулей периодов $p_i^{r_{ij}}$. Символически мы изображаем это следующей диаграммой:

$$\begin{aligned} E(p_1)&: r_{11} \leqslant r_{12} \leqslant \ldots \\ E(p_2)&: r_{21} \leqslant r_{22} \leqslant \ldots \\ &\ldots\ldots\ldots \\ E(p_l)&: r_{l1} \leqslant r_{l2} \leqslant \ldots \end{aligned}$$

Предполагается, что горизонтальные строки имеют одинаковую длину, причем хотя бы одна из них состоит из ненулевых элементов. В начале же некоторых строк могут стоять показатели r_{ij}, равные нулю. Строки с исключенными из них нулями описывают типы модулей относительно простых элементов, указанных слева. Показатели r_{ij} расположены в возрастающем порядке, для всякого фиксированного $i = 1, \ldots, l$. Пусть $q_1, \ldots, q_r$ соответствуют столбцам этой матрицы показателей; другими словами, положим

$$\begin{aligned} q_1 &= p_1^{r_{11}} p_2^{r_{21}} \ldots p_l^{r_{l1}}, \\ q_2 &= p_1^{r_{12}} p_2^{r_{22}} \ldots p_l^{r_{l2}} \\ &\ldots\ldots\ldots\ldots \end{aligned}$$ [1])

Прямая сумма циклических модулей, представляемых первым столбцом, изоморфна $R/(q_1)$, потому что, как и в случае абелевых групп, прямая сумма циклических модулей, периоды которых взаимно просты, также является циклическим модулем. Аналогичное замечание справедливо для каждого столбца. Заметим, кроме того, что

[1]) Выписав последний элемент q_r, мы столкнулись бы с нелепыми показателями r_{ir}; к счастью, в явном виде они далее не выступают, так что особой необходимости в замене индекса r не ощущается. — *Прим. ред.*

наше доказательство в действительности располагает q_i в порядке возрастающей делимости, что и требовалось.

Теперь займемся единственностью. Пусть p — произвольный простой элемент. Предположим, что $E = R/(pb)$ для некоторого $b \in R$, $b \neq 0$. Тогда E_p есть подмодуль $bR/(pb)$, как это следует немедленно из однозначной разложимости на множители в R. Но ядром композиции отображений

$$R \to bR \to bR/(pb)$$

служит в точности (p). Таким образом, имеем изоморфизм

$$R/(p) \approx bR/(pb).$$

Пусть теперь модуль E представлен, как сказано в теореме, в виде прямой суммы из r членов. Элемент

$$v = v_1 \oplus \ldots \oplus v_r, \qquad v_i \in R/(q_i),$$

лежит в E_p в том и только в том случае, если $pv_i = 0$ для всех i. Следовательно, E_p есть прямая сумма ядер умножения на p в каждом члене. Но E_p — векторное пространство над $R/(p)$, и его размерность равна, таким образом, числу членов $R/(q_i)$, таких, что p делит q_i.

Предположим, что p — простой элемент, делящий q_1, а значит и q_i, для всех $i = 1, \ldots, r$. Пусть E имеет разложение в прямую сумму из s членов, удовлетворяющее условиям теоремы, скажем

$$E = R/(q_1') \oplus \ldots \oplus R/(q_s').$$

Тогда элемент p должен делить по крайней мере r элементов q_j', откуда $r \leqslant s$. По симметрии $r = s$ и p делит q_j' для всех j.

Рассмотрим модуль pE. В силу предыдущего замечания, записав $q_i = pb_i$, мы будем иметь

$$pE \approx R/(b_1) \oplus \ldots \oplus R/(b_r)$$

и $b_1 \mid \ldots \mid b_r$. Некоторые из b_i могут быть единицами, но те, которые не являются единицами, по индукции определяют свой главный идеал однозначно. Следовательно, если $(b_1) = \ldots = (b_j) = 1$, но $(b_{j+1}) \neq 1$, то последовательность идеалов

$$(b_{j+1}), \ldots, (b_r)$$

однозначно определена. Это доказывает наше утверждение о единственности и завершает доказательство теоремы 4.

Идеалы $(q_1), \ldots, (q_r)$ называются *инвариантами* модуля E.

Следующую теорему можно было бы рассматривать как следствие теоремы 4. Мы дадим для нее независимое доказательство. Использоваться в дальнейшем она не будет.

Теорема 5. *Пусть F — свободный модуль над R и M — его конечно порожденный подмодуль $\neq 0$. Тогда существуют базис $\mathscr{B}$ модуля F, элементы этого базиса $e_1, \ldots, e_r$ и ненулевые элементы $a_1, \ldots, a_r \in R$, такие, что*

(i) *элементы $a_1e_1, \ldots, a_re_r$ образуют базис M над R;*

(ii) *$a_i \mid a_{i+1}$ для $i = 1, \ldots, r-1$.*

Последовательность идеалов $(a_1), \ldots, (a_r)$ однозначно определена предыдущими условиями.

Доказательство. Пусть λ — некоторый функционал на F, другими словами, элемент из $\mathrm{Hom}_R(F, R)$. Положим $J_\lambda = \lambda(M)$. Тогда J_λ есть идеал в R. Выберем λ_1 так, чтобы идеал $\lambda_1(M)$ был максимален в множестве идеалов $\{J_\lambda\}$, т. е. чтобы в множестве $\{J_\lambda\}$ не было строго большего идеала.

Пусть $\lambda_1(M) = (a_1)$. Тогда $a_1 \neq 0$. Действительно, в M имеется ненулевой элемент; в выражении этого элемента через какой-нибудь базис модуля F над R имеется ненулевая координата; беря проекцию на эту координату, мы получим функционал, значение которого на M не равно 0. Пусть $x_1 \in M$ — элемент, для которого $\lambda_1(x_1) = a_1$. Для любого функционала g мы должны иметь $g(x_1) \in (a_1)$ [непосредственно вытекает из максимальности $\lambda_1(M)$]. Записав x_1 через любой базис в F, мы увидим, что все его коэффициенты должны делиться на a_1. (Если некоторый коэффициент не делится на a_1, то спроектируем на этот коэффициент и получим невозможный функционал.) Поэтому мы можем записать $x_1 = a_1e_1$ для некоторого элемента $e_1 \in F$.

Теперь докажем, что F есть прямая сумма

$$F = Re_1 \oplus \operatorname{Ker} \lambda_1.$$

Так как $\lambda_1(e_1) = 1$, то ясно, что $R(e_1) \cap \operatorname{Ker} \lambda_1 = 0$. Кроме того, для всякого $x \in F$ разность $x - \lambda_1(x)e_1$ лежит в ядре λ_1. Следовательно, F есть сумма указанных подмодулей, которая должна быть прямой.

Отметим, что модуль $\operatorname{Ker} \lambda_1$ — свободный как подмодуль свободного модуля (теорема 1). Положим

$$F_1 = \operatorname{Ker} \lambda_1 \quad \text{и} \quad M_1 = M \cap \operatorname{Ker} \lambda_1.$$

Тогда видно, что

$$M = Rx_1 \oplus M_1.$$

Таким образом, M_1 — подмодуль в F_1, причем его размерность на единицу меньше, чем размерность модуля M. Мы можем поэтому закончить доказательство по индукции. Читателю предлагается проверить справедливость утверждения (ii).

Чтобы получить единственность, мы должны охарактеризовать нашу последовательность идеалов $(a_1), \ldots, (a_r)$ всецело в терминах F и M.

Лемма 3. *Пусть L_a^s — множество всех s-линейных знакопеременных форм на F, J_s — идеал в R, порожденный всеми элементами $f(y_1, \ldots, y_s)$, где $f \in L_a^s$ и $y_1, \ldots, y_s \in M$. Тогда*

$$J_s = (a_1 \ldots a_s).$$

Доказательство. Покажем сначала, что $J_s \subset (a_1 \ldots a_s)$. Действительно, всякий элемент $y \in M$ может быть записан в виде

$$y_1 = c_1 a_1 e_1 + \ldots + c_r a_r e_r.$$

Следовательно, если $y_1, \ldots, y_s \in M$ и f — полилинейная знакопеременная форма на F, то элемент $f(J_1, \ldots, J_s)$ равен сумме членов вида

$$c_{i_1} \ldots c_{i_s} a_{i_1} \ldots a_{i_s} f(e_{i_1}, \ldots, e_{i_s}).$$

Такой член отличен от нуля, только когда $e_{i_1}, \ldots, e_{i_s}$ различны, а в этом случае он делится на $a_1 \ldots a_s$ и, следовательно, J_s содержится в указанном идеале.

Обратно, покажем, что существует s-линейная знакопеременная форма, которая дает в точности это произведение. Мы получим эту форму с помощью определителей. Мы можем записать F в виде прямой суммы

$$F = (e_1, \ldots, e_r) \oplus F_r$$

для некоторого подмодуля F_r. Пусть $f_i (i = 1, \ldots, r)$ — линейное отображение $F \to R$, для которого $f_i(e_j) = \delta_{ij}$, причем f_i имеет значение 0 на F_r. Для $v_1, \ldots, v_s \in F$ положим

$$f(v_1, \ldots, v_s) = \det(f_i(v_j)), \qquad i, j = 1, \ldots, s.$$

Тогда f — полилинейная знакопеременная форма, которая принимает значение

$$f(e_1, \ldots, e_s) = 1$$

и, следовательно, значение

$$f(a_1 e_1, \ldots, a_s e_s) = a_1 \ldots a_s.$$

Это доказывает нашу лемму.

Единственность, утверждаемая в теореме 5, теперь очевидна, так как прежде всего идеал (a_1) определен однозначно, затем идеал $(a_1 a_2)$ также определен однозначно и, следовательно, их частное (a_2) определено однозначно и т. д. по индукции. Теорема 5 доказана.

Мы будем называть $(a_1), \ldots, (a_r)$ *инвариантами* подмодуля M в F.

§ 3. Разложение над одним эндоморфизмом

Пусть k — поле и E — конечномерное векторное пространство над k, $E \neq 0$. Пусть $A \in \mathrm{End}_k(E)$ — линейное отображение E в себя, t — трансцендентный элемент над k. Определим некоторое представление кольца многочленов $k[t]$ в E. А именно: имеет место гомоморфизм

$$k[t] \to k[A] \subset \mathrm{End}_k(E),$$

который получается подстановкой A вместо t в многочлены. Кольцо $k[A]$ является подкольцом в $\mathrm{End}_k(E)$, порожденным A, и притом коммутативным, так как степени A коммутируют друг с другом. Таким образом, если $f(t)$ — многочлен и $v \in E$, то

$$f(t)\,v = f(A)\,v.$$

Ядро гомоморфизма $f(t) \mapsto f(A)$ есть главный идеал в $k[t]$, который $\neq 0$, поскольку $k[A]$ конечномерно над k. Он порождается однозначно определенным многочленом степени > 0 со старшим коэффициентом 1. Этот многочлен будет называться *минимальным многочленом* эндоморфизма A над k и будет обозначаться через $q_A(t)$. Разумеется, он не обязательно неприводим.

Предположим, что существует элемент $v \in E$, такой, что $E = k[t]\,v = k[A]\,v$. Это означает, что E порождается над полем k элементами

$$v,\ Av,\ A^2v,\ \ldots\ .$$

Мы назвали такие модули *главными*. Можно записать $E = Rv = (v)$, где $R = k[t]$.

Если $q_A(t) = t^d + a_{d-1}t^{d-1} + \ldots + a_0$, то элементы

$$v,\ Av,\ \ldots,\ A^{d-1}v$$

образуют базис для E над k. Это доказывается точно так же, как и аналогичное утверждение для конечных расширений полей. Во-первых, отметим, что они линейно независимы, так как любое соотношение линейной зависимости над k давало бы многочлен $g(t)$ меньшей степени, чем $\deg q_A$, и такой, что $g(A) = 0$. Во-вторых, они порождают E, так как любой многочлен $f(t)$ может быть записан в виде $f(t) = g(t)\,q_A(t) + r(t)$, где $\deg r < \deg q_A$. Следовательно, $f(A) = r(A)$.

Ясно, что относительно этого базиса матрица эндоморфизма A имеет следующий вид:

$$\begin{pmatrix} 0 & 0 & 0 \ldots 0 & -a_0 \\ 1 & 0 & 0 \ldots 0 & -a_1 \\ 0 & 1 & 0 \ldots 0 & -a_2 \\ \cdot & \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ 0 & 0 & 0 \quad\ 0 & -a_{d-2} \\ 0 & 0 & 0 \ldots 1 & -a_{d-1} \end{pmatrix}.$$

Если модуль E главный, то E изоморфен фактормодулю $k[t]/q_A(t)$ относительно отображения $f(t) \longmapsto f(A)v$. Многочлен q_A однозначно определен эндоморфизмом A и не зависит от выбора образующей v модуля E. Это по существу очевидно, так как если f_1, f_2 — два многочлена со старшим коэффициентом 1, то модуль $k[t]/f_1(t)$ тогда и только тогда изоморфен $k[t]/f_2(t)$, когда $f_1 = f_2$.

Если модуль E главный, то мы будем называть q_A *полиномиальным инвариантом* E относительно A, или просто *инвариантом*.

Теорема 6. *Пусть E — ненулевое конечномерное пространство над полем k, и пусть $A \in \mathrm{End}_k(E)$. Тогда E обладает разложением в прямую сумму*

$$E = E_1 \oplus \ldots \oplus E_r,$$

где каждое слагаемое E_i является главным $k[A]$-подмодулем с инвариантом $q_i \neq 0$, причем

$$q_1 \mid q_2 \mid \ldots \mid q_r.$$

Последовательность $(q_1, \ldots, q_r)$ однозначно определяется пространством E и эндоморфизмом A, и q_r есть минимальный многочлен для A.

Доказательство. Первое утверждение есть просто перефразировка на другом языке структурной теоремы для модулей над кольцами главных идеалов. Далее, ясно, что $q_r(A) = 0$, так как $q_i \mid q_r$ для всякого i. Никакой многочлен меньшей степени, чем q_r, не может аннулировать E, поскольку, в частности, такой многочлен не аннулирует E_r. Таким образом, q_r — минимальный многочлен.

Мы будем называть $(q_1, \ldots, q_r)$ *инвариантами* пары (E, A). Пусть $E = k^{(n)}$, и пусть A — матрица размера $n \times n$, которую мы можем рассматривать как линейное отображение E в себя. Инварианты $(q_1, \ldots, q_r)$ этого линейного отображения будут называться *инвариантами* матрицы A (над k).

Следствие 1. *Пусть k' — расширение поля k и A — матрица размера $n \times n$ над k. Инварианты матрицы A над k те же самые, что и ее инварианты над k'.*

Доказательство. Пусть $\{v_1, \ldots, v_n\}$ — базис $k^{(n)}$ над k. Тогда мы можем рассматривать его также как базис $k'^{(n)}$ над k'. (Единичные векторы лежат в k-пространстве, порожденном элементами $v_1, \ldots, v_n$; следовательно, $v_1, \ldots, v_n$ порождают n-мерное пространство $k'^{(n)}$ над k'.) Пусть $E = k^{(n)}$ и L_A (соответственно L'_A) — линейное отображение пространства E (соответственно $k'^{(n)}$), определенное матрицей A. Матрица отображения L_A относительно нашего

заданного базиса совпадает с матрицей отображения L'_A. Мы можем выбрать базис, который соответствует разложению

$$E = E_1 \oplus \ldots \oplus E_r,$$

определенному инвариантами $q_1, \ldots, q_r$. Отсюда вытекает, что инварианты не изменятся, когда мы поднимем этот базис до базиса $k'^{(n)}$.

Следствие 2. *Пусть A, B — матрицы размера $n \times n$ над полем k и k' — расширение k. Предположим, что существует обратимая матрица C' над k', такая, что $B = C'AC'^{-1}$. Тогда существует обратимая матрица C над k, такая, что $B = CAC^{-1}$.*

Доказательство. Упражнение.

Структурная теорема для модулей над кольцами главных идеалов дает нам два типа разложений. Один — в соответствии с инвариантами, как в предыдущей теореме. Другой — в соответствии со степенями простых элементов.

Пусть $E \neq 0$ — конечномерное векторное пространство над полем k и A: $E \to E$ — эндоморфизм из $\mathrm{End}_k(E)$. Пусть $q = q_A$ — его минимальный многочлен. Тогда q имеет разложение

$$q = p_1^{e_1} \ldots p_s^{e_s} \qquad (e_i \geqslant 1)$$

в произведение степеней (различных) простых элементов. Следовательно, E есть прямая сумма подмодулей

$$E = E(p_1) \oplus \ldots \oplus E(p_s),$$

где каждый $E(p_i)$ аннулируется многочленом $p_i^{e_i}$. Кроме того, каждый такой подмодуль может быть представлен в виде прямой суммы подмодулей, изоморфных $k[t]/p^e$ для некоторого неприводимого многочлена p и некоторого целого числа $e \geqslant 1$.

Теорема 7. *Пусть $q_A(t) = (t-\alpha)^e$ для некоторого $\alpha \in k$, $e \geqslant 1$. Предположим, что E изоморфно $k[t]/(q)$. Тогда E имеет базис над k, такой, что относительно этого базиса матрица эндоморфизма A имеет вид*

$$\begin{pmatrix} \alpha & 0 & \ldots & 0 \\ 1 & \alpha & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ \cdot & & & \cdot \\ 0 & \ldots & 1 & \alpha \end{pmatrix}$$

Доказательство. Так как E изоморфно $k[t]/q$, то существует элемент $v \in E$, такой, что $k[t]v = E$. Этот элемент соответствует единичному элементу кольца $k[t]$ при изоморфизме

$$k[t]/q \to E.$$

Мы утверждаем, что элементы

$$v,\ (t-\alpha)v,\ \ldots,\ (t-\alpha)^{e-1}v,$$

или, что эквивалентно,

$$v,\ (A-\alpha)v,\ \ldots,\ (A-\alpha)^{e-1}v,$$

образуют базис для E над k. Они линейно независимы над k, так как любое соотношение линейной зависимости давало бы соотношение линейной зависимости между

$$v,\ Av,\ \ldots,\ A^{e-1}v$$

и, следовательно, давало бы многочлен $g(t)$ степени, меньшей, чем $\deg q$, такой, что $g(A) = 0$. Так как $\dim E = e$, то отсюда следует, что наши элементы образуют базис для E над k. Но $(A-\alpha)^e = 0$. Ясно, что матрица эндоморфизма A относительно этого базиса имеет форму, указанную в нашей теореме.

Следствие. *Пусть k — алгебраически замкнутое поле, E — конечномерное ненулевое векторное пространство над k и $A \in \mathrm{End}_k(E)$. Тогда существует базис пространства E над k, такой, что матрица эндоморфизма A относительно этого базиса состоит из блоков, каждый из которых имеет вид, описанный в теореме.*

О матрице, имеющей форму, описанную в предыдущем следствии, говорят, что она имеет *жорданову каноническую форму*.

Замечание. Матрица (или эндоморфизм) N называется *нильпотентной*, если существует целое число $d > 0$, такое, что $N^d = 0$. Мы видим, что в теореме 7 или ее следствии матрица M записывается в виде

$$M = B + N,$$

где матрица N нильпотентна. Действительно, N есть треугольная матрица (т. е. она имеет нулевые коэффициенты на и над диагональю) и B — диагональная матрица, диагональные элементы которой являются корнями минимального многочлена. Такое разложение может быть получено всякий раз, когда поле k таково, что все корни минимального многочлена лежат в k. Отметим также, что единственным случаем, когда матрица N будет нулевой, будет тот, когда все корни минимального многочлена имеют кратность 1. В этом случае матрица M является диагональной матрицей с n различными элементами диагонали, где $n = \dim E = \deg q_A$.

§ 4. Характеристический многочлен

Пусть k — коммутативное кольцо и E — свободный модуль размерности n над k. Рассмотрим кольцо многочленов $k[t]$ и линейное отображение A: $E \to E$. Имеем гомоморфизм

$$k[t] \to k[A],$$

определяемый как и выше, который переводит многочлен $f(t)$ в $f(A)$, и E превращается в модуль над кольцом $R = k[t]$. Пусть M — любая матрица размера $n \times n$ над R (например, матрица отображения A относительно некоторого базиса в E). *Характеристическим многочленом* $P_M(t)$ мы называем определитель

$$\det(tI_n - M),$$

где I_n — единичная матрица размера $n \times n$. Это элемент из $k[t]$. Кроме того, если N — обратимая матрица над R, то

$$\det(tI_n - N^{-1}MN) = \det(N^{-1}(tI_n - M)N) = \det(tI_n - M).$$

Следовательно, характеристический многочлен у матрицы $N^{-1}MN$ тот же самый, что и у M. Мы можем поэтому определить характеристический многочлен отображения A (и обозначить его через P_A) как характеристический многочлен любой матрицы M, ассоциированной с A относительно некоторого базиса. (В случае $E = 0$ мы *по определению считаем характеристический многочлен равным* 1.)

Если φ: $k \to k'$ — гомоморфизм коммутативных колец и M — матрица размера $n \times n$ над k, то очевидно, что

$$P_{\varphi M}(t) = \varphi P_M(t),$$

где φP_M получается из P_M применением φ к коэффициентам P_M.

Теорема 8 (Кэли — Гамильтон). $P_A(A) = 0$.

Доказательство. Пусть $\{v_1, \ldots, v_n\}$ — базис E над k. Тогда

$$tv_j = \sum_{i=1}^{n} a_{ij} v_i,$$

где $(a_{ij}) = M$ — матрица отображения A относительно этого базиса. Пусть $B(t)$ обозначает матрицу $tI_n - M$. Очевидно, $B(t)$ — матрица с коэффициентами в $k[t]$. Пусть $\tilde{B}(t)$ — определенная в гл. XIII матрица с коэффициентами в $k[t]$, такая, что

$$\tilde{B}(t)\,B(t) = P_A(t)\,I_n.$$

Тогда

$$\tilde{B}(t)\,B(t)\begin{pmatrix} v_1 \\ \cdot \\ \cdot \\ \cdot \\ v_n \end{pmatrix} = \begin{pmatrix} P_A(t)\,v_1 \\ \cdot \\ \cdot \\ \cdot \\ P_A(t)\,v_n \end{pmatrix} = \begin{pmatrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix},$$

так как

$$B(t)\begin{pmatrix} v_1 \\ \cdot \\ \cdot \\ \cdot \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}.$$

Следовательно, $P_A(t)E = 0$, а потому $P_A(A)E = 0$. Это означает, что $P_A(A) = 0$, что и требовалось показать.

Пусть теперь k — поле. Пусть E — конечномерное векторное пространство над k и $A \in \mathrm{End}_k(E)$. Под *собственным вектором* w эндоморфизма A в E понимают элемент $w \in E$, такой, что существует элемент $\lambda \in k$, для которого $Aw = \lambda w$. Если $w \neq 0$, то λ определяется однозначно и называется *собственным значением* эндоморфизма A. Разумеется, различные собственные векторы могут иметь одинаковые собственные значения.

Теорема 9. *Собственные значения эндоморфизма A — это в точности корни его характеристического многочлена.*

Доказательство. Пусть λ — собственное значение. Тогда элемент $A - \lambda I$ необратим в $\mathrm{End}_k(E)$ и, значит, $\det(A - \lambda I) = 0$. Следовательно, λ — корень P_A. Рассуждение обратимо, тем самым доказано и обратное утверждение.

Для упрощения обозначений мы часто будем писать $A - \lambda$ вместо $A - \lambda I$.

Теорема 10. *Ненулевые собственные векторы $w_1, \ldots, w_m$ отображения A, имеющие различные собственные значения, линейно независимы.*

Доказательство. Предположим, что

$$a_1 w_1 + \ldots + a_m w_m = 0,$$

где $a_i \in k$, причем это самое короткое соотношение, в котором не все $a_i = 0$ (в предположении, что такое существует). Тогда $a_i \neq 0$ для всех i. Пусть $\lambda_1, \ldots, \lambda_m$ — собственные значения наших векторов. Применим к предыдущему соотношению $A - \lambda_1$. Получим соотношение

$$a_2(\lambda_2 - \lambda_1)w_2 + \ldots + a_m(\lambda_m - \lambda_1)w_m = 0,$$

которое короче исходного соотношения, — противоречие.

Следствие. *Если A имеет n различных собственных значений $\lambda_1, \ldots, \lambda_n$, принадлежащих собственным векторам $v_1, \ldots, v_n$, и $\dim E = n$, то $\{v_1, \ldots, v_n\}$ есть базис для E. Матрицей эндоморфизма A относительно этого базиса служит диагональная матрица*

$$\begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \ddots \\ 0 & & & \lambda_n \end{pmatrix}.$$

Предостережение. Не всегда верно, что существует базис E, состоящий из собственных векторов!

Замечание. Пусть k — подполе в k'. Если M — матрица над k, то мы можем определить ее характеристический многочлен как относительно k, так и относительно k'. Очевидно, что полученные таким путем характеристические многочлены равны. Пусть E — векторное пространство над k. Позже мы увидим, как расширить его до векторного пространства над k'. Всякое линейное отображение A продолжается до линейного отображения расширенного пространства, причем характеристический многочлен линейного отображения не изменяется. Действительно, если мы выберем базис E над k, то $E \approx k^{(n)}$ и $k^{(n)} \subset k'^{(n)}$ естественным образом. Таким образом, выбор базиса позволяет нам расширить векторное пространство, но создается впечатление, что результат зависит от выбора базиса. Инвариантное определение будет дано ниже.

Пусть $E = E_1 \oplus \ldots \oplus E_r$ — представление E в виде прямой суммы векторных пространств над k. Пусть $A \in \mathrm{End}_k(E)$, причем $AE_i \subset E_i$ для $i = 1, \ldots, r$. Тогда A индуцирует на E_i линейное отображение A_i. Мы можем выбрать базис для E, состоящий из базисов для $E_1, \ldots, E_r$, и тогда матрица для A будет состоять из блоков. Мы видим, таким образом, что

$$P_A(t) = \prod_{i=1}^{r} P_{A_i}(t).$$

Итак, характеристический многочлен мультипликативен на прямых суммах.

Наше предыдущее условие $AE_i \subset E_i$ можно также сформулировать, сказав, что E представимо как $k[A]$-прямая сумма $k[A]$-подмодулей или как $k[t]$-прямая сумма $k[t]$-подмодулей. Применим это к разложению пространства E, даваемому теоремой 6.

Теорема 11. *Пусть E — конечномерное векторное пространство над полем k, $A \in \mathrm{End}_k(E)$ и $q_1, \ldots, q_r$ — инварианты пары (E, A). Тогда $P_A(t) = q_1(t) \ldots q_r(t)$.*

Доказательство. Предположим, что $E = k^{(n)}$ и что A представляется матрицей M. Мы видели, что ни инварианты, ни характеристический многочлен не изменяются, когда мы расширяем поле k до большего поля. Следовательно, мы можем считать, что поле k алгебраически замкнуто. Ввиду теоремы 6 мы можем предполагать, что M имеет единственный инвариант q. Запишем

$$q(t) = (t - \alpha_1)^{e_1} \ldots (t - \alpha_s)^{e_s},$$

где $\alpha_1, \ldots, \alpha_s$ различны. Рассмотрим M как линейное отображение и разложим наше векторное пространство в прямую сумму подмодулей (над $k[t]$) с инвариантами

$$(t - \alpha_1)^{e_1}, \ldots, (t - \alpha_s)^{e_s}$$

соответственно (это есть разложение на слагаемые, соответствующие степеням простых элементов). Для каждого из этих подмодулей мы можем выбрать базис так, чтобы матрица индуцированного линейного отображения имела форму, описанную в теореме 7, после чего непосредственно видно, что характеристический многочлен отображения, имеющего инвариант $(t - \alpha)^e$, равен в точности $(t - \alpha)^e$. Теорема доказана.

Следствие. *Минимальный многочлен отображения A и его характеристический многочлен имеют одни и те же неприводимые множители.*

Доказательство. Это вытекает из того, что в силу теоремы 6 q_r есть минимальный многочлен.

Обобщим наше замечание, касающееся мультипликативности характеристического многочлена на прямых суммах.

Теорема 12. *Пусть k — коммутативное кольцо, и пусть в следующей диаграмме:*

$$\begin{array}{ccccccc} 0 & \to & E' & \to & E & \to & E'' \to 0 \\ & & \downarrow{\scriptstyle A'} & & \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle A''} \\ 0 & \to & E' & \to & E & \to & E'' \to 0 \end{array}$$

строки являются точными последовательностями свободных модулей над k, имеющих конечную размерность. Пусть, далее, вертикальные отображения являются k-линейными отображениями, для которых диаграмма коммутативна. Тогда

$$P_A(t) = P_{A'}(t)\, P_{A''}(t).$$

Доказательство. Мы можем предполагать, что E' — подмодуль в E. Выберем базис $\{v_1, \ldots, v_m\}$ для E'. Пусть $\{\bar{v}_{m+1}, \ldots, \bar{v}_n\}$ — базис для E'' и $v_{m+1}, \ldots, v_n$ — элементы из E, отображающиеся на $\bar{v}_{m+1}, \ldots, \bar{v}_n$ соответственно. Тогда $\{v_1, \ldots, v_m, v_{m+1}, \ldots, v_n\}$ будет базисом для E (доказательство такое же, как в теореме 3 из гл III, § 5), и мы находимся в ситуации, описанной в § 1. Матрица для A имеет форму

$$\begin{pmatrix} M' & * \\ 0 & M'' \end{pmatrix},$$

где M' — матрица для A' и M'' — матрица для A''. Взяв характеристический многочлен относительно этой матрицы, мы, очевидно, и получим наше мультипликативное свойство.

Теорема 13 *Пусть k — коммутативное кольцо, E — свободный модуль размерности n над k и $A \in \mathrm{End}_k(E)$. Пусть*

$$P_A(t) = t^n + c_{n-1}t^{n-1} + \ldots + c_0.$$

Тогда

$$\mathrm{tr}(A) = -c_{n-1} \quad \text{и} \quad \det(A) = (-1)^n c_0.$$

Доказательство Что касается определителя, то заметим, что $P_A(0) = c_0$. Подстановка $t = 0$ в определение характеристического многочлена через определитель доказывает, что $c_0 = (-1)^n \det A$

Перейдем к следу. Пусть M — матрица, представляющая A относительно некоторого базиса, $M = (a_{ij})$ Рассмотрим определитель $\det(tI_n - a_{ij})$. В его разложении по первому столбцу содержится диагональный член

$$(t - a_{11}) \ldots (t - a_{nn}),$$

который вносит в коэффициент при t^{n-1} вклад, равный

$$-(a_{11} + \ldots + a_{nn})$$

Никакой другой член в этом разложении ничего не добавляет к коэффициенту при t^{n-1}, так как степень t, встречающаяся в других членах, не превосходит t^{n-2}. Это доказывает наше утверждение, касающееся следа.

Следствие. *Пусть обозначения те же, что и в теореме* 12. *Тогда*

$$\mathrm{tr}(A) = \mathrm{tr}(A') + \mathrm{tr}(A'') \quad \text{и} \quad \det(A) = \det(A')\det(A'').$$

Доказательство. Очевидно.

Дадим теперь нашим результатам интерпретацию в терминах группы Эйлера — Гротендика.

Пусть k — коммутативное кольцо. Рассмотрим категорию, объектами которой являются пары (E, A), где E — k-модуль и $A \in \mathrm{End}_k(E)$. Определим морфизм

$$(E', A') \to (E, A)$$

как k-линейное отображение $E' \xrightarrow{k} E$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} E' & \xrightarrow{f} & E \\ {\scriptstyle A'}\downarrow & & \downarrow{\scriptstyle A} \\ E' & \xrightarrow{f} & E \end{array}$$

Мы можем определить ядро такого морфизма снова как пару. Действительно, пусть E'_0 — ядро $f\colon E' \to E$. Тогда A' отображает E'_0 в себя, так как $fA'E'_0 = AfE'_0 = 0$. Пусть A'_0 — ограничение A' на E'_0. Пара (E'_0, A'_0) по определению является ядром нашего морфизма.

Будем обозначать по-прежнему через f морфизм пары $(E', A') \to (E, A)$. Мы можем говорить о точной последовательности

$$(E', A') \to (E, A) \to (E'', A''),$$

понимая под этим, что точна индуцированная последовательность

$$E' \to E \to E''.$$

Мы будем также писать 0 вместо $(0, 0)$ в соответствии с нашим общим соглашением использовать символ 0 для всех тех вещей, которые ведут себя подобно нулевому элементу.

Заметим, что наши пары ведут себя теперь формально как модули и что они фактически образуют абелеву категорию.

Пусть k — поле, и пусть $\mathcal{A}$ состоит из всех пар (E, A), где E имеет конечную размерность над k. *Тогда теорема* 12 *утверждает, что характеристический многочлен является отображением Эйлера — Пуанкаре, определенным для всякого объекта из нашей категории* $\mathcal{A}$, *со значениями в мультипликативном моноиде многочленов со старшим коэффициентом* 1. Так как значения этого отображения лежат в моноиде, то здесь используется несколько более общее понятие, чем введенное в гл. IV, где мы брали значения в группе. Разумеется, когда k есть поле, что наиболее часто встречается в приложениях, мы можем считать, что значения нашего отображения лежат в мультипликативной группе отличных от нуля рациональных функций, так что применимы наши предыдущие рассмотрения.

Аналогичное замечание справедливо также для следа и определителя. *Если* k — *поле, то след есть отображение Эйлера в аддитивную группу поля, а определитель — отображение Эйлера*

в мультипликативную группу поля [1]). Отметим также, что все эти отображения (подобно всем отображениям Эйлера) определены на классах пар относительно изоморфизма и что они определены на группе Эйлера — Гротендика.

Теорема 14. *Пусть k — целостное кольцо, M — матрица размера $n \times n$ над k и f — многочлен из $k[t]$. Предположим, что $P_M(t)$ имеет разложение*

$$P_M(t) = \prod_{i=1}^{n} (t - \alpha_i)$$

на линейные множители над k. Тогда характеристический многочлен матрицы $f(M)$ задается формулой

$$P_{f(M)}(t) = \prod_{i=1}^{n} (t - f(\alpha_i))$$

и

$$\operatorname{tr}(f(M)) = \sum_{i=1}^{n} f(\alpha_i), \qquad \det(f(M)) = \prod_{i=1}^{n} f(\alpha_i).$$

Доказательство. Допустим сначала, что k — поле. Тогда, используя каноническое разложение на блоки, описанное в теореме 7 § 3, мы обнаруживаем, что наше утверждение совершенно очевидно. В случае когда k — кольцо, используем стандартный прием с подстановкой. Для этого, однако, необходимо знать, что если $X = (x_{ij})$ — матрица с алгебраически независимыми элементами над $\mathbf{Z}$, то $P_X(t)$ имеет n различных корней $y_1, \ldots, y_n$ [в алгебраическом замыкании поля $\mathbf{Q}(X)$], и что существует гомоморфизм

$$\mathbf{Z}[x_{ij}, y_1, \ldots, y_n] \to k,$$

отображающий X на M и $y_1, \ldots, y_n$ на $\alpha_1, \ldots, \alpha_n$. Но это очевидно для читателя, который прочитал главу о целых расширениях колец, а читатель, который этого не сделал, может забыть об этой части теоремы [2]).

УПРАЖНЕНИЯ

1. Пусть T — верхняя треугольная квадратная матрица над коммутативным кольцом (т. е. все элементы под диагональю и на ней равны 0). Показать, что T нильпотентна.

---

[1]) Точнее, в мультипликативную полугруппу, так как значение определителя может быть равно нулю. — *Прим. ред.*

[2]) Проще вложить k в поле частных. — *Прим. ред.*

2. Провести непосредственно доказательство того факта, что определитель матрицы

$$\begin{pmatrix} M_1 & & & * & * \\ 0 & M_2 & & & * \\ 0 & 0 & \ddots & & \\ \cdot & \cdot & \ddots & & \\ \cdot & \cdot & \cdot & \ddots & \\ \cdot & \cdot & \cdot & \cdot & \\ 0 & 0 & \dots & 0 & M_s \end{pmatrix},$$

где каждая M_i — квадратная матрица, равен произведению определителей матриц $M_1, \dots, M_s$

3. Пусть k — коммутативное кольцо и M, M' — квадратные матрицы размера $n \times n$ над k. Показать, что характеристические многочлены матриц MM' и $M'M$ равны.

4. Показать, что собственные значения матрицы

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

в поле комплексных чисел равны ± 1, $\pm i$.

5. Пусть M, M' — квадратные матрицы над полем k. Пусть соответственно q, q' — их минимальные многочлены. Показать, что минимальный многочлен матрицы

$$\begin{pmatrix} M & 0 \\ 0 & M' \end{pmatrix}$$

равен наименьшему общему кратному q, q'.

6. Пусть A — нильпотентный эндоморфизм конечномерного векторного пространства E над полем k. Показать, что $\operatorname{tr}(A) = 0$.

7. Пусть R — целостное кольцо главных идеалов, E — свободный модуль размерности n над R и $E^* = \operatorname{Hom}_R(E, R)$ — его дуальный модуль. Тогда E^* — свободный модуль размерности n. Пусть F — подмодуль в E. Показать, что $E^*/F^\perp$ можно рассматривать как подмодуль в F^* и что его инварианты те же самые, что и инварианты F в E

8. Пусть E — конечномерное векторное пространство над полем k и $A \in \operatorname{Aut}_k(E)$. Показать, что следующие условия эквивалентны:

(i) $A = I + N$, где N — нильпотентный эндоморфизм

(ii) Существует базис для E, такой, что у матрицы эндоморфизма A относительно этого базиса все диагональные элементы равны 1, а все элементы над диагональю равны 0.

(iii) Все корни характеристического многочлена эндоморфизма A (в алгебраическом замыкании поля k) равны 1.

9. Пусть k — поле характеристики 0 и M — матрица размера $n \times n$ над k. Показать, что M нильпотентна в том и только в том случае, если $\operatorname{tr}(M^\nu) = 0$ для $1 \leqslant \nu \leqslant n$.

10. Обобщить теорему 14 на рациональные функции (вместо многочленов), предполагая, что k — поле.

11. Пусть E — конечномерное пространство над полем k, $\alpha \in k$ и E_α — подпространство в E, порожденное всеми собственными векторами данного эндоморфизма A пространства E, имеющими α в качестве собственного значения. Показать, что всякий ненулевой элемент из E_α является собственным вектором эндоморфизма A с собственным значением α.

12. Пусть E — конечномерное пространство над полем k, $A \in \mathrm{End}_k(E)$ — собственный вектор для A. Пусть элемент $B \in \mathrm{End}_k(E)$ таков, что $AB = BA$. Показать, что Bv — также собственный вектор для A (если $Bv \neq 0$) с тем же собственным значением и что в случае алгебраически замкнутого поля k эндоморфизмы A и B имеют общий собственный вектор.

Диагонализируемые эндоморфизмы. Пусть E — конечномерное векторное пространство над полем k, $S \in \mathrm{End}_k(E)$. Мы говорим, что эндоморфизм S — *диагонализируемый*, если существует базис для E, состоящий из собственных векторов S. Матрица эндоморфизма S относительно этого базиса является диагональной матрицей.

13. (а) Если эндоморфизм S диагонализируем, то его минимальный многочлен над k имеет вид $q(t) = \prod_{i=1}^{m} (t - \lambda_i)$, где $\lambda_1, \ldots, \lambda_m$ — различные элементы из k.

(б) Обратно, если минимальный многочлен для S имеет предыдущий вид, то эндоморфизм S диагонализируем. [*Указание*: пространство может быть разложено в прямую сумму подпространств $E\lambda_i$, аннулируемых эндоморфизмами $S - \lambda_i$.]

(в) Показать, что если эндоморфизм S диагонализируем и F — такое подпространство в E, что $SF \subset F$, то S диагонализируем также как эндоморфизм F, т. е. что F имеет базис, состоящий из собственных векторов S.

(г) Пусть S, T — эндоморфизмы E. Предположим, что S, T коммутируют. Предположим также, что и S, и T оба диагонализируемы. Показать, что они одновременно диагонализируемы, т. е. что существует базис для E, состоящий из векторов, собственных как для S, так и для T. [*Указание*: если λ — собственное значение эндоморфизма S и E_λ — подпространство в E, состоящее из всех векторов v, таких, что $Sv = \lambda v$, то $TE_\lambda \subset E_\lambda$.]

14. Пусть E — конечномерное векторное пространство над алгебраически замкнутым полем k, $A \in \mathrm{End}_k(E)$. Показать, что эндоморфизм A может быть единственным образом записан в виде суммы

$$A = S + N,$$

где S диагонализируем, N нильпотентен и $SN = NS$. Показать, что S, N могут быть представлены в виде многочленов от A. [*Указание*: пусть $P_A(t) = \prod (t - \lambda_i)^{m_i}$ — разложение $P_A(t)$ с различными λ_i; E_i — ядро $(A - \lambda_i)^{m_i}$. Тогда E — прямая сумма E_i. Определить S на E так, что на всяком E_i будет $Sv = \lambda_i v$ для всех $v \in E_i$. Положить $N = A - S$. Показать, что S, N удовлетворяют нашим требованиям. Чтобы представить S в виде многочлена от A, рассмотреть многочлен $g(t) = \sum \lambda_i g_i(t)$, где многочлены $g_i(t)$ выбраны так, что для всякого i компонента в E_i любого элемента $v \in E$ равна $g_i(A)\, v$. Тогда $S = g(A)$ и $N = A - g(A)$.]

15. После того как вы прочитаете параграф о тензорных произведениях векторных пространств, вы легко сможете сделать следующее упражнение. Пусть E, F — конечномерные векторные пространства над алгебраически

замкнутым полем k, A: $E \to E$ и B: $F \to F$ — k-эндоморфизмы пространств E, F соответственно. Пусть

$$P_A(t) = \prod (t - \alpha_i)^{n_i} \quad \text{и} \quad P_B(t) = \prod (t - \beta_j)^{m_j}$$

— разложения их характеристических многочленов на различные линейные множители. Тогда

$$P_{A \otimes B}(t) = \prod_{i,\, j} (t - \alpha_i \beta_j)^{n_i m_j}.$$

[*Указание*: разложить E в прямую сумму подпространств E_i, где E_i — подпространство, аннулируемое некоторой степенью $A - \alpha_i$. То же самое сделать с F и получить разложение в прямую сумму подпространств F_j. Затем показать, что некоторая степень эндоморфизма $A \otimes B - \alpha_i \beta_j$ аннулирует $E_i \otimes F_j$. Использовать тот факт, что $E \otimes F$ есть прямая сумма подпространств $E_i \otimes F_j$ и что $\dim_k (E_i \otimes F_j) = n_i m_j$.]

16. Пусть Γ — свободная абелева группа размерности $n \geqslant 1$, Γ' — ее подгруппа, имеющая также размерность n. Пусть $\{v_1, \ldots, v_n\}$ — базис Γ и $\{w_1, \ldots, w_n\}$ — базис Γ'. Запишем

$$w_i = \Sigma a_{ij} v_j.$$

Показать, что индекс $(\Gamma : \Gamma')$ равен абсолютной величине определителя матрицы (a_{ij}).

17. Доказать теорему о нормальном базисе для конечного расширения конечного поля.

18. Пусть $A = (a_{ij})$ — квадратная матрица размера $n \times n$ над коммутативным кольцом k, A_{ij} — матрица, полученная вычеркиванием i-й строки и j-го столбца из A. Пусть $b_{ij} = (-1)^{i+j} \det(A_{ij})$ и B — матрица (b_{ij}). Показать, что $\det(B) = \det(A)^{n-1}$, сведя задачу к случаю, когда A — матрица с переменными коэффициентами над кольцом целых чисел. Использовать тот же метод для получения другого доказательства теоремы Гамильтона — Кэли о том, что $P_A(A) = 0$.

19. Пусть (E, A) и (E', A') — пары, состоящие из конечномерного векторного пространства над некоторым полем k и k-эндоморфизма. Показать, что эти пары изоморфны в том и только в том случае, если их инварианты равны.

Глава XVI

Полилинейные произведения

§ 1. Тензорное произведение

Пусть k — коммутативное кольцо. Для модулей $E_1, \ldots, E_n, F$ обозначим через

$$L^n(E_1, \ldots, E_n; F)$$

модуль n-линейных отображений

$$f\colon E_1 \times \ldots \times E_n \to F.$$

Напомним, что полилинейное отображение линейно над k по каждой переменной. Мы будем использовать слова „линейное отображение" и „гомоморфизм" как синонимы. *Если не оговорено противное, то все модули, гомоморфизмы, линейные и полилинейные отображения рассматриваются по отношению к кольцу k.*

Полилинейные отображения фиксированного множества модулей $E_1, \ldots, E_n$ можно рассматривать как объекты некоторой категории. Действительно, если

$$f\colon E_1 \times \ldots \times E_n \to F \quad \text{и} \quad g\colon E_1 \times \ldots \times E_n \to G$$

— полилинейные отображения, то мы определяем морфизм $f \to g$ как гомоморфизм $h\colon F \to G$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} & \overset{f}{\nearrow} & F \\ E_1 \times \ldots \times E_n & & \downarrow h \\ & \underset{g}{\searrow} & G \end{array}$$

Универсальный объект этой категории называется *тензорным произведением модулей* $E_1, \ldots, E_n$ (над k).

Докажем теперь, что тензорное произведение существует, и фактически построим его некоторым естественным способом. Из абстрактной чепухи нам, разумеется, известно, что тензорное произведение однозначно определено с точностью до единственного изоморфизма.

Пусть M — свободный модуль, порожденный множеством всех n-наборов $(x_1, \ldots, x_n)$ $(x_i \in E_i)$, т. е. порожденный множеством

$E_1 \times \ldots \times E_n$. Обозначим через N его подмодуль, порожденный всеми элементами следующего вида:

$$(x_1, \ldots, x_i + x_i', \ldots, x_n) - (x_1, \ldots, x_i, \ldots, x_n) - (x_1, \ldots, x_i', \ldots, x_n),$$

$$(x_1, \ldots, ax_i, \ldots, x_n) - a(x_1, \ldots, ax_i, \ldots, x_n),$$

где $x_i \in E_i$, $x_i' \in E_i$, $a \in k$. Имеем каноническое вложение

$$E_1 \times \ldots \times E_n \to M$$

нашего множества в порожденный им свободный модуль. Взяв композицию этого отображения с каноническим отображением $M \to M/N$ на фактормодуль, получим отображение

$$\varphi\colon E_1 \times \ldots \times E_n \to M/N.$$

Мы утверждаем, что φ полилинейно и является тензорным произведением.

Что φ полилинейно, — очевидно; все было как раз приспособлено для этой цели. Пусть

$$f\colon E_1 \times \ldots \times E_n \to G$$

— полилинейное отображение. По определению свободного модуля, порожденного множеством $E_1 \times \ldots \times E_n$, имеем индуцированное линейное отображение $M \to G$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} E_1 \times \ldots \times E_n & \nearrow & M \\ & \searrow^{f} & \downarrow \\ & & G \end{array}$$

Так как f полилинейно, то индуцированное отображение $M \to G$ принимает значение 0 на N. Следовательно, в силу универсального свойства фактормодулей это отображение может быть пропущено через M/N и, мы имеем гомоморфизм $f_*\colon M/N \to G$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} E_1 \times \ldots \times E_n & \overset{\varphi}{\nearrow} & M/N \\ & \underset{f}{\searrow} & \downarrow f_* \\ & & G \end{array}$$

Так как образ отображения φ порождает M/N, то индуцированное отображение f_* *однозначно определено.* Это доказывает все, что нам требовалось.

Модуль M/N будет обозначаться через $E_1 \otimes \ldots \otimes E_n$ или также через $\bigotimes_{i=1}^{n} E_i$. Мы построили специальное тензорное произведение

в классе тензорных произведений относительно изоморфизма, и именно за ним мы закрепим название тензорного произведения модулей $E_1, \ldots, E_n$. Для $x_i \in E_i$ будем записывать

$$\varphi(x_1, \ldots, x_n) = x_1 \otimes \ldots \otimes x_n = x_1 \otimes_k \ldots \otimes_k x_n.$$

Для всех i имеем

$$x_1 \otimes \ldots \otimes ax_i \otimes \ldots \otimes x_n = a(x_1 \otimes \ldots \otimes x_n),$$

$$x_1 \otimes \ldots \otimes (x_i + x_i') \otimes \ldots \otimes x_n =$$

$$= (x_1 \otimes \ldots \otimes x_i \otimes \ldots \otimes x_n) + (x_1 \otimes \ldots \otimes x_i' \otimes \ldots \otimes x_n),$$

где $x_i, x_i' \in E_i$ и $a \in k$.

В случае двух сомножителей, скажем E, F, всякий элемент из $E \otimes F$ может быть записан как сумма членов $x \otimes y$ с $x \in E$ и $y \in F$, поскольку такие члены порождают $E \otimes F$ над k и $a(x \otimes y) = ax \otimes y$ для $a \in k$.

Предостережение. Тензорное произведение может приводить к полному или частичному взаимному уничтожению модулей. Возьмем, например, тензорное произведение над $\mathbf{Z}$ абелевых групп $\mathbf{Z}/m\mathbf{Z}$ и $\mathbf{Z}/n\mathbf{Z}$, где m, n — взаимно простые целые числа, большие единицы. Тогда тензорное произведение

$$\mathbf{Z}/n\mathbf{Z} \otimes \mathbf{Z}/m\mathbf{Z} = 0.$$

Действительно, имеем $n(x \otimes y) = (nx) \otimes y = 0$ и $m(x \otimes y) = x \otimes (my) = 0$. Следовательно, $x \otimes y = 0$ для всех $x \in \mathbf{Z}/n\mathbf{Z}$ и $y \in \mathbf{Z}/m\mathbf{Z}$. А так как элементы вида $x \otimes y$ порождают тензорное произведение, то оно равно 0. Позднее мы найдем условия, при которых съеданий такого рода не происходит.

Во многих дальнейших результатах мы будем утверждать существование и единственность каких-либо линейных отображений тензорного произведения. Это существование доказывается использованием универсального свойства тензорного произведения, позволяющего пропускать через него билинейные отображения. Единственность вытекает из того факта, что линейные отображения принимают предписанное значение на элементах (скажем, для двух множителей) вида $x \otimes y$, поскольку такие элементы порождают тензорное произведение.

Докажем ассоциативность тензорного произведения.

Предложение 1. *Пусть E_1, E_2, E_3 — модули. Тогда существует однозначно определенный изоморфизм*

$$(E_1 \otimes E_2) \otimes E_3 \to E_1 \otimes (E_2 \otimes E_3),$$

такой, что

$$(x \otimes y) \otimes z \longmapsto x \otimes (y \otimes z)$$

для $x \in E_1$, $y \in E_2$ и $z \in E_3$.

Доказательство. Так как элементы вида $(x \otimes y) \otimes z$ порождают тензорное произведение, то единственность искомого линейного отображения очевидна. Чтобы доказать существование, возьмем $x \in E_1$. Отображение

$$\lambda_x\colon E_2 \times E_3 \to (E_1 \otimes E_2) \otimes E_3,$$

такое, что $\lambda_x(y, z) = (x \otimes y) \otimes z$, очевидно, билинейно и, следовательно, может быть пропущено через линейное отображение тензорного произведения

$$\bar{\lambda}_x\colon E_2 \otimes E_3 \to (E_1 \otimes E_2) \otimes E_3.$$

Отображение

$$E_1 \times (E_2 \otimes E_3) \to (E_1 \otimes E_2) \otimes E_3,$$

такое, что

$$(x, \alpha) \longmapsto \bar{\lambda}_x(\alpha)$$

для $x \in E_1$ и $\alpha \in E_2 \otimes E_3$, также, очевидно, билинейно, и оно пропускается через линейное отображение

$$E_1 \otimes (E_2 \otimes E_3) \to (E_1 \otimes E_2) \otimes E_3,$$

которое и обладает требуемыми свойствами (ясно из его построения).

Предложение 2. *Для всяких модулей E, F существует однозначно определенный изоморфизм*

$$E \otimes F \to F \otimes E,$$

такой, что $x \otimes y \longmapsto y \otimes x$ для $x \in E$ и $y \in F$.

Доказательство. Отображение $E \times F \to F \otimes E$, такое, что $(x, y) \longmapsto y \otimes x$, билинейно, и оно пропускается через линейное отображение тензорного произведения $E \otimes F$, переводящее $x \otimes y$ в $y \otimes x$. Так как это последнее отображение имеет обратное (по симметрии), то и получаем искомый изоморфизм.

Тензорное произведение обладает различными функториальными свойствами. Во-первых, пусть

$$f_i\colon E_i' \to E_i \quad (i = 1, \ldots, n)$$

— набор линейных отображений. Имеем индуцированное отображение произведения

$$\Pi f_i\colon \Pi E_i' \to \Pi E_i.$$

Если мы возьмем композицию Πf_i с каноническим отображением в тензорное произведение, то получим индуцированное линейное отображение, которое мы можем обозначить через $T(f_1, \ldots, f_n)$ и для

которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} E_1' \times \ldots \times E_n' & \to & E_1' \otimes \ldots \otimes E_n' \\ {\scriptstyle \Pi f_i}\downarrow & & \downarrow{\scriptstyle T(f_1, \ldots, f_n)} \\ E_1 \times \ldots \times E_n & \to & E_1 \otimes \ldots \otimes E_n. \end{array}$$

Непосредственно проверяется, что T функториально, а именно что для композиции линейных отображений $f_i \circ g_i$ $(i = 1, \ldots, n)$

$$T(f_1 \circ g_1, \ldots, f_n \circ g_n) = T(f_1, \ldots, f_n) \circ T(g_1, \ldots, g_n)$$

и

$$T(\mathrm{id}, \ldots, \mathrm{id}) = \mathrm{id}.$$

Заметим, что $T(f_1, \ldots, f_n)$—это однозначно определенное линейное отображение, действие которого на элемент $x_1' \otimes \ldots \otimes x_n'$ из $E_1' \otimes \ldots \otimes E_n'$ задается правилом

$$x_1' \otimes \ldots \otimes x_n' \mapsto f_1(x_1') \otimes \ldots \otimes f_n(x_n').$$

Мы можем рассматривать T как отображение

$$\prod_{i=1}^{n} L(E_i', E_i) \to L\left(\bigotimes_{i=1}^{n} E_i', \bigotimes_{i=1}^{n} E_i\right),$$

и читатель легко проверит, что это отображение полилинейное. Мы выпишем в явном виде, что́ это означает в случае двух множителей, когда наше отображение может быть записано так:

$$(f, g) \mapsto T(f, g).$$

Для заданных гомоморфизмов $f\colon F' \to F$ и $g_1, g_2\colon E' \to E$

$$T(f, g_1 + g_2) = T(f, g_1) + T(f, g_2),$$
$$T(f, ag_1) = aT(f, g_1).$$

В частности, выберем некоторый фиксированный модуль F и рассмотрим функтор $\tau = \tau_F$ (из категории модулей в категорию модулей), такой, что

$$\tau(E) = F \otimes E.$$

Тогда τ для всякой пары модулей E', E определяет линейное отображение

$$\tau\colon L(E', E) \to L(\tau(E'), \tau(E))$$

по формуле

$$\tau(f) = T(\mathrm{id}, f).$$

Замечание. Допуская вольность в обозначениях, иногда мы будем писать

$$f_1 \otimes \ldots \otimes f_n \text{ вместо } T(f_1, \ldots, f_n).$$

Это не надо путать с тензорным произведением элементов, взятым в тензорном произведении модулей

$$L(E_1', E_1) \otimes \ldots \otimes L(E_n', E_n).$$

Из контекста всегда будет ясно, что мы имеем в виду.

§ 2. *Основные свойства*

Самым основным соотношением, связывающим линейные отображения, билинейные отображения и тензорное произведение, является следующее: для трех модулей E, F, G

$$\boxed{L(E, L(F, G) \approx L^2(E, F; G) \approx L(E \otimes F, G)}.$$

Содержащиеся здесь изоморфизмы описываются естественным образом

(i) $$L^2(E, F; G) \to L(E, L(F, G)).$$

Если $f\colon E \times F \to G$ — билинейное отображение и $x \in E$, то отображение

$$f_x\colon F \to G,$$

для которого $f_x(y) = f(x, y)$, линейно. Кроме того, отображение $x \longmapsto f_x$ также линейно, и для получения (i) именно это отображение и сопоставляется f.

(ii) $$L(E, L(F, G)) \to L^2(E, F; G).$$

Пусть $\varphi \in L(E, L(F, G))$ и $f_\varphi\colon E \times F \to G$ — билинейное отображение, для которого

$$f_\varphi(x, y) = \varphi(x)(y).$$

Тогда $\varphi \longmapsto f_\varphi$ определяет (ii).

Ясно, что гомоморфизмы (i) и (ii) взаимно обратны и поэтому дают изоморфизм первых двух объектов в рамке.

(iii) $$L^2(E, F; G) \to L(E \otimes F, G).$$

Это то отображение, которое сопоставляет каждому билинейному отображению f индуцированное линейное отображение f_*. Сопоставление $f \longmapsto f_*$ инъективно (так как f_* однозначно определяет f) и сюръективно, так как любое линейное отображение тензорного произведения в композиции с каноническим отображением $E \times F \to E \otimes F$ определяет билинейное отображение на $E \times F$.

Предложение 3. *Пусть* $E = \coprod_{i=1}^{n} E_i$ *— прямая сумма. Имеет место изоморфизм*

$$F \otimes E \leftrightarrow \coprod_{i=1}^{n} (F \otimes E_i).$$

Доказательство. Изоморфизм задается абстрактной чепухой. Фиксируем F и рассмотрим функтор τ: $X \longmapsto F \otimes X$. Как мы видели выше, τ линеен. Имеем проекции π_i: $E \to E$ прямой суммы E на E_i, причем

$$\pi_i \circ \pi_i = \pi_i, \quad \pi_i \circ \pi_j = 0, \quad \text{если } i \neq j,$$

$$\sum_{i=1}^{n} \pi_i = \mathrm{id}.$$

Применив функтор τ, мы видим, что $\tau(\pi_i)$ удовлетворяют тем же соотношениям и, следовательно, дают разложение $\tau(E) = F \otimes E$ в прямую сумму. Отметим, что $\tau(\pi_i) = \mathrm{id} \otimes \pi_i$.

Следствие. *Пусть* I *— некоторое множество индексов и* $E = \coprod_{i \in I} E_i$. *Имеет место изоморфизм*

$$\left(\coprod_{i \in I} E_i\right) \otimes F \approx \coprod_{i \in I} (E_i \otimes F).$$

Доказательство. Пусть S — конечное подмножество в I. Имеем последовательность отображений

$$\left(\coprod_{i \in S} E_i\right) \times F \to \coprod_{i \in S} (E_i \otimes F) \to \coprod_{i \in I} (E_i \otimes F),$$

первое из которых билинейно, а второе, индуцированное включением S в I, линейно. Действительно, первое отображение очевидно. Если $S \subset S'$, то тривиальная коммутативная диаграмма показывает, что ограничение отображения

$$\left(\coprod_{i \in S'} E_i\right) \times F \to \coprod_{i \in I} (E_i \otimes F)$$

индуцирует наше предыдущее отображение на сумме по $i \in S$. Но мы имеем *вложение*

$$\left(\coprod_{i \in S} E_i\right) \times F \to \left(\coprod_{i \in S'} E_i\right) \times F.$$

Следовательно, в силу согласованности отображений с такими вложениями мы можем определить билинейное отображение

$$\left(\coprod_{i \in I} E_i\right) \times F \to \coprod_{i \in I} (E_i \otimes F),$$

а потому и линейное отображение

$$\left(\coprod_{i\in I} E_i\right)\otimes F \to \coprod_{i\in I}(E_i\otimes F).$$

Аналогичным образом определяется отображение в противоположном направлении, и ясно, что эти отображения взаимно обратны; следовательно, они дают изоморфизм.

Предположим теперь, что E — свободный модуль размерности 1 над k. Пусть $\{v\}$ — его базис. Рассмотрим $F\otimes E$. Всякий элемент из $F\otimes E$ может быть записан в виде суммы членов $y\otimes av$, где $y\in F$ и $a\in k$. Однако $y\otimes av = ay\otimes v$. Далее, при суммировании таких членов мы можем использовать линейность слева

$$\sum_{i=1}^{n}(y_i\otimes v)=\left(\sum_{i=1}^{n} y_i\right)\otimes v, \qquad y_i\in F.$$

Следовательно, всякий элемент имеет в действительности вид $y\otimes v$ с некоторым $y\in F$.

Имеем билинейное отображение

$$F\times E\to F,$$

такое, что $(y, av)\mapsto ay$, которое индуцирует линейное отображение

$$F\otimes E\to F.$$

Имеем также линейное отображение $F\to F\otimes E$, задаваемое формулой $y\mapsto y\otimes v$. Ясно, что эти отображения взаимно обратны, и, следовательно, имеем изоморфизм $F\otimes E\approx F$. Таким образом, всякий элемент из $F\otimes E$ может быть *единственным* образом записан в виде $y\otimes v$, $y\in F$.

Предложение 4. *Пусть E — свободный модуль над k с базисом $\{v_i\}_{i\in I}$. Тогда всякий элемент из $F\otimes E$ имеет однозначное представление вида*

$$\sum_{i\in I} y_i\otimes v_i, \qquad y_i\in F,$$

где почти все $y_i = 0$.

Доказательство. Это тотчас вытекает из рассмотрения одномерного случая и следствия предложения 1.

Следствие. *Пусть E, F — свободные модули над k с базисами $\{v_i\}_{i\in I}$ и $\{w_j\}_{j\in J}$ соответственно. Тогда модуль $E\otimes F$ свободен и имеет базис $\{v_i\otimes w_j\}$. При этом*

$$\dim(E\otimes F) = (\dim E)(\dim F).$$

Доказательство. Непосредственно вытекает из предложения.

Мы видим, что когда модуль E свободен над k, в тензорном произведении не происходит никаких съеданий. Всякий элемент из $F \otimes E$ может рассматриваться как „формальная" линейная комбинация элементов из базиса E с коэффициентами в F.

В частности, мы видим, что тензорное произведение $k \otimes E$ (или $E \otimes k$) изоморфно E относительно соответствия $x \mapsto x \otimes 1$.

Предложение 5. *Пусть E, F — свободные модули конечной размерности над k. Имеет место изоморфизм*

$$\mathrm{End}_k(E) \otimes \mathrm{End}_k(F) \to \mathrm{End}_k(E \otimes F),$$

являющийся однозначно определенным линейным отображением, таким, что

$$f \otimes g \mapsto T(f, g)$$

для $f \in \mathrm{End}_k(E)$ и $g \in \mathrm{End}_k(F)$.

[Отметим, что тензорное произведение слева взято в тензорном произведении двух модулей $\mathrm{End}_k(E)$ и $\mathrm{End}_k(F)$.]

Доказательство. Пусть $\{v_i\}$ — базис E и $\{w_j\}$ — базис F. Тогда $\{v_i \otimes w_j\}$ есть базис $E \otimes F$. Для всякой пары индексов (i', j') существуют однозначно определенные эндоморфизмы $f = f_{i, i'}$ модуля E и $g = g_{j, j'}$ модуля F, такие, что

$$f(v_i) = v_{i'} \quad \text{и} \quad f(v_\nu) = 0, \quad \text{если } \nu \neq i;$$
$$g(w_j) = w_{j'} \quad \text{и} \quad g(w_\mu) = 0, \quad \text{если } \mu \neq j.$$

Далее, семейства $\{f_{i, i'}\}$ и $\{g_{j, j'}\}$ образуют базисы для $\mathrm{End}_k(E)$ и $\mathrm{End}_k(F)$ соответственно. Затем

$$T(f, g)(v_\nu \otimes w_\mu) = \begin{cases} v_{i'} \otimes w_{j'}, & \text{если } (\nu, \mu) = (i, j), \\ 0, & \text{если } (\nu, \mu) \neq (i, j). \end{cases}$$

Таким образом, семейство $\{T(f_{i, i'}, g_{j, j'})\}$ есть базис для $\mathrm{End}_k(E \otimes F)$. Так как семейство $\{f_{i, i'} \otimes g_{j, j'}\}$ является базисом для $\mathrm{End}_k(E) \otimes \mathrm{End}_k(F)$, то утверждение нашего предложения становится теперь очевидным.

Предложение 5 показывает, что двусмысленность в использовании обозначения $f \otimes g$ не является на самом деле двусмысленностью в важном частном случае свободных конечномерных модулей. Позднее мы встретимся с важным приложением предложения 5, когда мы будем рассматривать тензорную алгебру модуля.

Предложение 6. *Пусть*

$$0 \to E' \xrightarrow{\varphi} E \xrightarrow{\psi} E'' \to 0$$

— точная последовательность и F — произвольный модуль. Тогда последовательность

$$F \otimes E' \to F \otimes E \to F \otimes E'' \to 0$$

— точная.

Доказательство. Для заданных $x'' \in E''$ и $y \in F$ существует элемент $x \in E$, такой, что $x'' = \psi(x)$, и, следовательно, $y \otimes x''$ есть образ элемента $y \otimes x$ при линейном отображении

$$F \otimes E \to F \otimes E''.$$

Поскольку элементы вида $y \otimes x''$ порождают $F \otimes E''$, то мы заключаем, что предыдущее линейное отображение сюръективно. Тривиально проверяется также, что образ отображения $F \otimes E' \to F \otimes E$ содержится в ядре

$$F \otimes E \to F \otimes E''.$$

Обратно, пусть I — образ отображения $F \otimes E' \to F \otimes E$ и

$$f\colon\ (F \otimes E)/I \to F \otimes E''$$

— каноническое отображение. Построим линейное отображение

$$g\colon\ F \otimes E'' \to (F \otimes E)/I,$$

такое, что $g \circ f = \mathrm{id}$. Отсюда, очевидно, будет следовать инъективность f, чем и будет доказано искомое обратное включение.

Пусть $y \in F$ и $x'' \in E''$. Возьмем элемент $x \in E$, для которого $\psi(x) = x''$. Определим отображение $F \times E'' \to (F \otimes E)/I$, положив

$$(y,\ x'') \longmapsto y \otimes x \pmod I.$$

Мы утверждаем, что это отображение правильно определено, т. е. не зависит от выбора элемента x, для которого $\psi(x) = x''$. Если $\psi(x_1) = \psi(x_2) = x''$, то $\psi(x_1 - x_2) = 0$, и по предположению $x_1 - x_2 = \varphi(x')$ для некоторого $x' \in E'$. Тогда

$$y \otimes x_1 - y \otimes x_2 = y \otimes (x_1 - x_2) = y \otimes \varphi(x').$$

Это показывает, что $y \otimes x_1 \equiv y \otimes x_2 \pmod I$, и доказывает, что наше отображение правильно определено. Оно, очевидно, билинейно и, следовательно, может быть пропущено через некоторое линейное отображение g тензорного произведения. Очевидно, что ограничение $g \circ f$ на элементы вида $y \otimes x \pmod I$ тождественно. А так как эти элементы порождают $(F \otimes E)/I$, то заключаем, что f инъективно, что и требовалось показать.

Не всегда верно, что точна последовательность

$$0 \to F \otimes E' \to F \otimes E \to F \otimes E'' \to 0.$$

Она точна, если первая последовательность в предложении 6 расщепляется, т. е., по существу, если E есть прямая сумма E' и E''. Это тривиальное следствие предложения 3, но читателю рекомендуется проследить детали, чтобы привыкнуть к формализму тензорного произведения.

Предложение 7. *Пусть* $\mathfrak{a}$ *— идеал в* k, E *— модуль над* k. *Тогда отображение* $(k/\mathfrak{a}) \times E \to E/\mathfrak{a}E$, *индуцированное сопоставлением*

$$(a, x) \longmapsto ax \pmod{\mathfrak{a}E}, \quad a \in k, \quad x \in E,$$

билинейно и индуцирует изоморфизм

$$(k/\mathfrak{a}) \otimes E \xrightarrow{\approx} E/\mathfrak{a}E.$$

Доказательство. Наше отображение $(a, x) \longmapsto ax \pmod{\mathfrak{a}E}$, очевидно, индуцирует билинейное отображение $k/\mathfrak{a} \times E$ на $E/\mathfrak{a}E$ и, следовательно, — линейное отображение $k/\mathfrak{a} \otimes E$ на $E/\mathfrak{a}E$. Мы можем построить обратное отображение, поскольку имеется правильно определенное линейное отображение

$$E \to k/\mathfrak{a} \otimes E,$$

такое, что $x \longmapsto \bar{1} \otimes x$, где $\bar{1}$ есть класс вычетов элемента 1 в $k/\mathfrak{a}$. Ясно, что $\mathfrak{a}E$ содержится в ядре этого последнего линейного отображения, и, таким образом, мы получаем гомоморфизм

$$E/\mathfrak{a}E \to k/\mathfrak{a} \otimes E,$$

который, как непосредственно проверяется, является обратным по отношению к гомоморфизму, описанному в формулировке предложения.

Сопоставление $E \longmapsto E/\mathfrak{a}E \approx k/\mathfrak{a} \otimes E$ часто называется *отображением редукции*. В следующем параграфе мы дадим интерпретацию этого отображения как некоторого расширения основного кольца.

§ 3. Расширение основного кольца

Пусть k — коммутативное кольцо и E — k-модуль. Мы акцентируем внимание на k, так как собираемся сейчас работать с несколькими кольцами. Пусть $k \to k'$ — гомоморфизм коммутативных колец, так что кольцо k' является k-алгеброй и может быть рассматриваемо также как k-модуль. Имеем 3-линейное отображение

$$k' \times k' \times E \to k' \otimes E,$$

определяемое правилом

$$(a, b, x) \longmapsto ab \otimes x.$$

Оно индуцирует линейное отображение над k

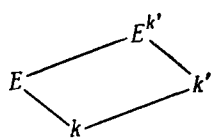
$$k' \otimes (k' \otimes E) \to k' \otimes E$$

и, следовательно, k-билинейное отображение $k' \times (k' \otimes E) \to k' \otimes E$. Непосредственно проверяется, что это последнее отображение превращает $k' \otimes E$ в k'-модуль, который мы будем называть *расширением E над k'* и обозначать через $E^{k'}$. Мы будем также говорить, что модуль $E^{k'}$ получен *расширением основного кольца* от k до k'.

Пример 1. Пусть $\mathfrak{a}$ — идеал в k и $k \to k/\mathfrak{a}$ — канонический гомоморфизм. Тогда расширение E над $k/\mathfrak{a}$ называется также *редукцией E* по модулю $\mathfrak{a}$. Эта ситуация часто встречается над кольцом целых чисел, когда мы производим редукцию по модулю простого числа p [т. е. по модулю простого идеала (p)].

Пример 2. Пусть k — поле и k' — его расширение. Тогда E — векторное пространство над k, а $E^{k'}$ — векторное пространство над k'. Мы видим, что в терминах базиса это есть то самое расширение, на которое мы ссылались в предыдущей главе. Этот пример будет более подробно развит в упражнениях.

Для наглядного изображения расширения основного кольца мы будем рисовать такие же диаграммы, как и в теории полей



Следствие предложения 4 дает нам

Предложение 8. *Пусть E — свободный модуль над k с базисом $\{v_i\}_{i \in I}$. Положим $v_i' = 1 \otimes v_i$. Тогда $E^{k'}$ будет свободным модулем над k' с базисом $\{v_i'\}_{i \in I}$.*

Мы уже использовали раньше частный случай этого предложения, когда доказывали, что размерность свободного модуля определена, т. е. что любые два базиса имеют одинаковую мощность. Действительно, в этом случае мы производили редукцию по модулю какого-либо максимального идеала кольца k, что позволяло свести вопрос к случаю векторных пространств над полем.

Когда колец несколько, желательно указывать k в обозначении тензорного произведения. Таким образом, следует писать

$$E^{k'} = k' \otimes E = k' \otimes_k E.$$

Имеет место транзитивность расширения основного кольца, а именно если $k \to k' \to k''$ — последовательность гомоморфизмов коммутативных колец, то имеет место изоморфизм

$$k'' \otimes_k E \approx k'' \otimes_{k'} (k' \otimes_k E),$$

причем этот изоморфизм является изоморфизмом k''-модулей. Доказательство тривиально и предоставляется читателю.

Если E обладает мультипликативной структурой, то мы можем расширять основное кольцо также и для этой структуры. Пусть $k \to A$ — гомоморфизм колец, такой, что всякий элемент образа k в A коммутирует со всеми элементами в A (т. е. некоторая k-алгебра). Пусть $k \to k'$ гомоморфизм коммутативных колец. Имеем 4-линейное отображение

$$k' \times A \times k' \times A \to k' \otimes A,$$

определяемое правилом

$$(a, x, b, y) \longmapsto ab \otimes xy.$$

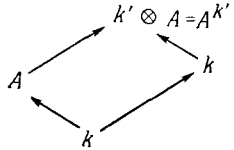
Получаем индуцированное линейное отображение над k

$$k' \otimes A \otimes k' \otimes A \to k' \otimes A$$

и, следовательно, индуцированное k-билинейное отображение

$$(k' \otimes A) \times (k' \otimes A) \to k' \otimes A.$$

Тривиально проверяется, что закон композиции на $k' \otimes A$, который мы только что определили, ассоциативен. В $k' \otimes A$ имеется единичный элемент, а именно $1 \otimes 1$. Имеется гомоморфизм кольца k' в $k' \otimes A$, задаваемый соответствием $a \longmapsto a \otimes 1$. Таким образом, тотчас видно, что $k' \otimes A = A^{k'}$ есть k'-алгебра. Отметим, что отображение $x \longmapsto 1 \otimes x$ есть гомоморфизм кольца A в $k' \otimes A$ и что мы получаем коммутативную диаграмму кольцевых гомоморфизмов



§ 4. Тензорное произведение алгебр

В предыдущих рассмотрениях ситуация была несимметричной: мы могли иметь дело с некоммутативной алгеброй A, но k' непременно должно было быть коммутативным. Предположим теперь, что мы

имеем дело с симметричной ситуацией, когда все рассматриваемые кольца коммутативны.

Предложение 9. *В категории коммутативных колец и в категории коммутативных алгебр над коммутативным кольцом существуют копроизведения. Если $k \to A$ и $k \to B$ — два гомоморфизма коммутативных колец, то их копроизведение над k — это гомоморфизм $k \to A \otimes B$, задаваемый правилом*

$$a \longmapsto a \otimes 1 = 1 \otimes a.$$

Доказательство. Мы ограничим наше доказательство случаем конечных копроизведений и, следовательно, в силу индуктивных соображений—случаем копроизведения двух кольцевых гомоморфизмов $k \to A$ и $k \to B$. (Для бесконечного случая необходим предельный процесс, аналогичный использованному в доказательстве следствия к предложению 3 и доступный читателю в качестве легкого упражнения.)

Пусть A, B — коммутативные кольца с заданными кольцевыми гомоморфизмами в некоторое коммутативное кольцо C

$$\varphi\colon A \to C \quad \text{и} \quad \psi\colon B \to C.$$

Тогда мы можем определить $\mathbf{Z}$-билинейное отображение

$$A \times B \to C,$$

положив $(x, y) \longmapsto \varphi(x)\psi(y)$. Отсюда в силу свойства универсальности тензорного произведения мы получаем однозначно определенный аддитивный гомоморфизм

$$A \otimes B \to C,$$

для которого $x \otimes y \longmapsto \varphi(x)\psi(y)$. Выше мы видели, что на $A \otimes B$ можно определить структуру кольца

$$(a \otimes b)(c \otimes d) = ac \otimes bd.$$

Тогда ясно, что наше отображение $A \otimes B \to C$ является гомоморфизмом колец. Имеем также два кольцевых гомоморфизма

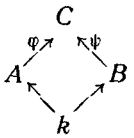
$$A \xrightarrow{f} A \otimes B \quad \text{и} \quad B \xrightarrow{g} A \otimes B,$$

задаваемых правилами

$$x \longmapsto x \otimes 1 \quad \text{и} \quad y \longmapsto 1 \otimes y,$$

причем, очевидно, $A \otimes B$ порождается образами колец A и B относительно этих гомоморфизмов. Теперь непосредственно видно, что $(A \otimes B, f, g)$ есть копроизведение наших колец A и B.

Если A, B, C — k-алгебры и если φ, ψ таковы, что коммутативна следующая диаграмма:



то $A \otimes_k B$ также есть k-алгебра (фактически это есть алгебра над k, над A или над B, в зависимости от того, какую из этих структур мы хотим использовать) и отображение $A \otimes_k B \to C$, полученное выше, дает гомоморфизм k-алгебр.

Любое коммутативное кольцо всегда можно рассматривать как $\mathbf{Z}$-алгебру (т. е. как алгебру над кольцом целых чисел). Таким образом, копроизведение коммутативных колец является частным случаем копроизведения k-алгебр.

§ 5. Тензорная алгебра модуля

Пусть G — коммутативный моноид, записываемый аддитивно. Под *G-градуированным кольцом* мы будем понимать кольцо A, для аддитивной группы которого задано представление в виде прямой суммы

$$A = \coprod_{r \in G} A_r,$$

а умножение в A отображает $A_r \times A_s$ в A_{r+s} для всех r, $s \in G$.

В частности, A_0 — подкольцо.

Элементы из A_r называются *однородными элементами степени r*.

Мы построим несколько примеров градуированных колец по следующему образцу. Пусть для всякого $r \in G$ задана абелева группа A_r (записываемая аддитивно), и пусть для всякой пары r, $s \in G$ задано отображение $A_r \times A_s \to A_{r+s}$. Предположим, что определяемая этими отображениями композиция ассоциативна и $\mathbf{Z}$-билинейна. Тогда прямая сумма $A = \coprod_{r \in G} A_r$ является кольцом: умножение вводится очевидным образом, а именно

$$\Big(\sum_{r \in G} x_r\Big)\Big(\sum_{s \in G} y_s\Big) = \sum_{t \in G}\Big(\sum_{r+s=t} x_r y_s\Big).$$

Применим эти соображения к случаю, когда G — моноид натуральных чисел 0, 1, 2, ...

Пусть k обозначает, как и прежде, коммутативное кольцо, и пусть E — некоторый модуль (т. е. k-модуль). Для всякого целого $r \geqslant 0$ положим

$$T^r(E) = \bigotimes_{i=1}^{r} E \quad \text{и} \quad T^0(E) = k.$$

Таким образом, $T^r(E) = E \otimes \ldots \otimes E$ (тензорное произведение, взятое r раз). Тогда T^r есть функтор, действие которого на линейные отображения задается следующим образом. Если $f\colon E \to F$ — линейное отображение, то

$$T^r(f) = T(f, \ldots, f)$$

в смысле § 1.

Из ассоциативности тензорного произведения получаем билинейные отображения

$$T^r(E) \times T^s(E) \to T^{r+s}(E),$$

являющиеся ассоциативными. Посредством этих билинейных отображений мы можем на прямой сумме

$$T(E) = \coprod_{r=0}^{\infty} T^r(E)$$

определить структуру кольца, а в действительности даже структуру алгебры (отображая k на $T^0(E) = k$). Мы будем называть $T(E)$ *тензорной алгеброй* модуля E над k. В общем случае она *не* коммутативна. Для обозначения кольцевой операции в $T(E)$ мы будем писать $x \otimes y$ ($x, y \in T(E)$).

Пусть $f\colon E \to F$ — линейное отображение. Тогда f для всякого $r \geqslant 0$ индуцирует линейное отображение

$$T^r(f)\colon T^r(E) \to T^r(F)$$

и, таким образом, индуцирует отображение на $T(E)$, которое мы будем обозначать символом $T(f)$. (Можно не опасаться путаницы с отображением из § 1, которое теперь следовало бы обозначать $T^1(f)$ и которое на самом деле равно f, так как $T^1(E) = E$.) Ясно, что $T(f)$ — это однозначно определенное линейное отображение, такое, что для $x_1, \ldots, x_r \in E$

$$T(f)(x_1 \otimes \ldots \otimes x_r) = f(x_1) \otimes \ldots \otimes f(x_r).$$

В действительности элементы из $T^1(E)$ являются образующими для $T(E)$ как алгебры над k. Мы видим, что $T(f)$ является гомоморфизмом алгебр. Таким образом, T может рассматриваться как функтор из категории модулей в категорию градуированных алгебр, причем $T(f)$ является гомоморфизмом степени 0.

В случае когда модуль E свободен и конечномерен над k, мы можем, используя предложение 4, полностью определить структуру $T(E)$. Пусть P — некоторая алгебра над k. Мы будем говорить, что P — *алгебра некоммутативных многочленов*, если существуют такие элементы $t_1, \ldots, t_n \in P$, что элементы

$$M_{(i)}(t) = t_{i_1} \ldots t_{i_r},$$

где $1 \leqslant i_v \leqslant n$, образуют базис для P над k. Мы можем назвать эти элементы *некоммутативными одночленами* от (t). Как обычно, принимается соглашение, что при $r = 0$ соответствующий одночлен совпадает с единичным элементом алгебры P. Мы видим, что $t_1, \ldots, t_n$ порождают P как алгебру над k и что P в действительности является градуированной алгеброй, однородная компонента P_r которой состоит из линейных комбинаций одночленов $t_{i_1} \ldots t_{i_r}$ с коэффициентами из k. Естественно сказать, что $t_1, \ldots, t_n$ — *независимые некоммутативные переменные над* k.

Предложение 10. *Пусть E — свободный модуль размерности n над k. Тогда алгебра $T(E)$ изоморфна алгебре некоммутативных многочленов от n переменных над k. Другими словами, если $\{v_1, \ldots, v_n\}$ — базис E над k, то элементы*

$$M_{(i)}(v) = v_{i_1} \otimes \ldots \otimes v_{i_r}, \quad 1 \leqslant i_v \leqslant n,$$

образуют базис $T^r(E)$ и всякий элемент из $T(E)$ имеет единственное представление в виде конечной суммы

$$\sum_{(i)} a_{(i)} M_{(i)}(v), \qquad a_{(i)} \in k,$$

где почти все $a_{(i)}$ равны 0.

Доказательство. Это тотчас следует из предложения 4, § 2.

Теперь будет дана интерпретация тензорного произведения линейных отображений в связи с понятием тензорной алгебры.

Для удобства мы до конца этого параграфа будем обозначать модуль эндоморфизмов $\mathrm{End}_k(E)$ *через* $L(E)$.

Образуем прямую сумму

$$(LT)(E) = \coprod_{r=0}^{\infty} L(T^r(E)),$$

которую для краткости будем также обозначать через $LT(E)$. [Разумеется, $LT(E)$ не равно $\mathrm{End}_k(T(E))$, так что мы должны рассматривать LT как единый символ.] Определив подходящим образом умножение в $LT(E)$, мы увидим, что LT есть функтор из категории модулей в категорию градуированных алгебр. Пусть $f \in L(T^r(E))$, $g \in L(T^s(E))$, $h \in L(T^m(E))$. Определим произведение $fg \in L(T^{r+s}(E))$ как $T(f, g)$ в обозначениях § 1, другими словами, как однозначно определенное линейное отображение, действие которого на элемент $x \otimes y$, где $x \in T^r(E)$ и $y \in T^s(E)$, задается формулой

$$x \otimes y \longmapsto f(x) \otimes g(y).$$

Ввиду ассоциативности тензорного произведения тотчас получаем ассоциативность $(fg)h = f(gh)$; кроме того, мы видим, что наше произведение билинейно. Следовательно, $LT(E)$ есть k-алгебра.

Имеет место гомоморфизм алгебр

$$T(L(E)) \to LT(E),$$

который в каждой размерности r задается линейным отображением

$$f_1 \otimes \ldots \otimes f_r \mapsto T(f_1, \ldots, f_r) = f_1 \ldots f_r.$$

Подчеркнем специально, что тензорное произведение слева взято из

$$L(E) \otimes \ldots \otimes L(E).$$

Отметим также, что этот гомоморфизм в общем случае не будет ни сюръективным, ни инъективным. Оказывается, однако, что когда E — свободный конечномерный модуль над k, то этот гомоморфизм обладает обоими этими свойствами, и, таким образом, в этом случае нам становится ясной структура $LT(E)$ как алгебры некоммутативных многочленов, порожденной $L(E)$. А именно, из предложения 5, § 2, получаем

Предложение 11. *Пусть E — свободный конечномерный модуль над k. Тогда имеет место изоморфизм алгебр*

$$T(L(E)) = T(\mathrm{End}_k(E)) \to LT(E) = \coprod_{r=0}^{\infty} \mathrm{End}_k(T^r(E)),$$

задаваемый отображением

$$f \otimes g \mapsto T(f, g).$$

Доказательство. В силу предложения 5 из § 2 в каждой размерности имеет место линейный изоморфизм и ясно, что наше отображение сохраняет умножение.

В частности, мы видим, что $LT(E)$ — алгебра некоммутативных многочленов.

§ 6. Знакопеременные произведения

Напомним, что r-линейное отображение $f\colon E^{(r)} \to F$ называется *знакопеременным*, если $f(x_1, \ldots, x_r) = 0$, как только $x_i = x_j$ для некоторых $i \neq j$.

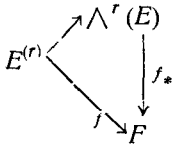
Пусть $\mathfrak{a}_r$ — подмодуль в $T^r(E)$, порожденный всеми элементами вида $x_1 \otimes \ldots \otimes x_r$, где $x_i = x_j$ для некоторых $i \neq j$. Положив

$$\bigwedge^r(E) = T^r(E)/\mathfrak{a}_r,$$

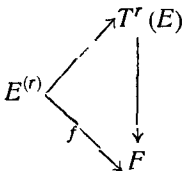
будем иметь r-линейное отображение $E^{(r)} \to \bigwedge^r(E)$ (называемое *каноническим*), получаемое из композиции

$$E^{(r)} \to T^r(E) \to T^r(E)/\mathfrak{a}_r = \bigwedge^r(E).$$

Ясно, что наше отображение является знакопеременным. *Более того, оно универсально по отношению к r-линейным знакопеременным отображениям на E.* Другими словами, если $f\colon E^{(r)} \to F$ такое отображение, то существует однозначно определенное линейное отображение $f_*\colon \bigwedge^r(E) \to F$, для которого коммутативна следующая диаграмма:



Отображение f_* существует, так как мы можем сначала получить индуцированное отображение $T^r(E) \to F$, делающее коммутативной диаграмму



а это индуцированное отображение обращается в нуль на $\mathfrak{a}_r$ и, следовательно, индуцирует f_*.

Таким образом, получаем функтор $\bigwedge^r$ из категории модулей со значениями в той же категории.

Образ элемента $(x_1, \ldots, x_r) \in E^{(r)}$ при каноническом отображении в $\bigwedge^r(E)$ будет обозначаться через $x_1 \wedge \ldots \wedge x_r$. Этот элемент является также образом $x_1 \otimes \ldots \otimes x_r$ при промежуточном гомоморфизме $T^r(E) \to \bigwedge^r(E)$.

Обозначим через $\bigwedge(E)$ прямую сумму $\coprod_{r=0}^{\infty} \bigwedge^r(E)$. Мы превратим $\bigwedge(E)$ в градуированную k-алгебру и будем называть ее *знакопеременной алгеброй* модуля E[1]). Сначала рассмотрим общую ситуацию с произвольными градуированными кольцами.

Пусть снова G — аддитивный моноид и $A = \coprod_{r \in G} A_r$ — G-градуированная k-алгебра. Предположим, что для каждого A_r задан подмодуль $\mathfrak{a}_r$, и пусть $\mathfrak{a} = \coprod_{r \in G} \mathfrak{a}_r$. Предположим, что $\mathfrak{a}$ — идеал в A. Тогда $\mathfrak{a}$

---

[1]) Более распространенным для $\bigwedge(E)$ является название *внешней алгебры модуля E*. Операция умножения в ней называется обычно *внешним произведением*. — *Прим. ред.*

называется *однородным идеалом*, и мы можем определить градуированную структуру на $A/\mathfrak{a}$. Далее, билинейное отображение

$$A_r \times A_s \to A_{r+s}$$

переводит $\mathfrak{a}_r \times A_s$ и $A_r \times \mathfrak{a}_s$ в $\mathfrak{a}_{r+s}$. Таким образом, используя представителей из A_r, A_s соответственно, мы можем определить билинейное отображение

$$A_r/\mathfrak{a}_r \times A_s/\mathfrak{a}_s \to A_{r+s}/\mathfrak{a}_{r+s}$$

и, следовательно, билинейное отображение $A/\mathfrak{a} \times A/\mathfrak{a} \to A/\mathfrak{a}$, которое превращает $A/\mathfrak{a}$ в градуированную k-алгебру.

Применим это к $T^r(E)$ и введенным выше модулям $\mathfrak{a}_r$. Если $x_i = x_j$ $(i \neq j)$ в произведении $x_1 \otimes \ldots \otimes x_r$, то $x_1 \otimes \ldots \otimes x_r \otimes \otimes y_1 \otimes \ldots \otimes y_s$ лежит в $\mathfrak{a}_{r+s}$ при любых $y_1, \ldots, y_s \in E$, и аналогично для произведения слева. Следовательно, прямая сумма $\coprod \mathfrak{a}_r$ есть идеал в $T(E)$, и мы можем определить на $T(E)/\mathfrak{a}$ структуру k-алгебры. Произведение однородных элементов задается формулой

$$((x_1 \wedge \ldots \wedge x_r), (y_1 \wedge \ldots \wedge y_s)) \mapsto x_1 \wedge \ldots \wedge x_r \wedge y_1 \wedge \ldots \wedge y_s.$$

Мы будем использовать символ $\wedge$ также для обозначения произведения в $\bigwedge(E)$. Это произведение называется *знакопеременным произведением*. Если $x \in E$ и $y \in E$, то $x \wedge y = -y \wedge x$, как это вытекает из того факта, что $(x+y) \wedge (x+y) = 0$.

Заметим, что $\bigwedge$ есть функтор из категории модулей в категорию градуированных k-алгебр. Для всякого линейного отображения $f\colon E \to F$ мы получаем отображение

$$\bigwedge(f)\colon \bigwedge(E) \to \bigwedge(F),$$

такое, что для $x_1, \ldots, x_r \in E$ имеем

$$\bigwedge(f)(x_1 \wedge \ldots \wedge x_r) = f(x_1) \wedge \ldots \wedge f(x_r).$$

Кроме того, $\bigwedge(f)$ является гомоморфизмом градуированных k-алгебр.

Предложение 12. *Пусть E — свободный модуль размерности n над k. Если $r > n$, то $\bigwedge^r(E) = 0$. Пусть $\{v_1, \ldots, v_n\}$ — базис для E над k. Если $1 \leqslant r \leqslant n$, то модуль $\bigwedge^r(E)$ свободен над k и элементы*

$$v_{i_1} \wedge \ldots \wedge v_{i_r}, \quad i_1 < \ldots < i_r,$$

образуют базис для $\bigwedge^r(E)$ над k. При этом

$$\dim_k \bigwedge^r(E) = \binom{n}{r}.$$

Доказательство. Сначала докажем наше утверждение для $r = n$. Всякий элемент из E может быть записан в виде $\sum a_i v_i$, и,

следовательно, $v_1 \wedge \ldots \wedge v_n$ порождает $\bigwedge^n(E)$, как это вытекает из формулы $x \wedge y = -y \wedge x$. С другой стороны, из теории определителей мы знаем, что для заданного $a \in k$ существует однозначно определенная полилинейная знакопеременная форма f_a на E, такая, что

$$f_a(v_1, \ldots, v_n) = a.$$

Следовательно, существует однозначно определенное линейное отображение

$$\bigwedge^n(E) \to k,$$

принимающее на $v_1 \wedge \ldots \wedge v_n$ значение a. Из этого тотчас вытекает, что $v_1 \wedge \ldots \wedge v_n$ служит базисом для $\bigwedge^n(E)$ над k.

Докажем теперь наше утверждение для $1 \leqslant r \leqslant n$. Предположим, что мы имеем некоторое соотношение

$$0 = \sum a_{(i)} v_{i_1} \wedge \ldots \wedge v_{i_r},$$

где $i_1 < \ldots < i_r$ и $a_{(i)} \in k$. Рассмотрим любой набор из r индексов $(j) = (j_1, \ldots, j_r)$, такой, что $j_1 < \ldots < j_r$, и обозначим через $j_{r+1}, \ldots, j_n$ те значения i, которые не встречаются среди $(j_1, \ldots, j_r)$. Возьмем знакопеременное произведение нашего соотношения с $v_{j_{r+1}} \wedge \ldots \wedge v_{j_n}$. Тогда во всех членах суммы, кроме (j)-члена, мы будем иметь знакопеременные произведения с повторяющимися компонентами и, следовательно, получим

$$0 = a_{(j)} v_{j_1} \wedge \ldots \wedge v_{j_r} \wedge \ldots \wedge v_{j_n}.$$

Перетасовывая сомножители в $v_{j_1} \wedge \ldots \wedge v_{j_n}$ так, чтобы получить $v_1 \wedge \ldots \wedge v_n$, мы можем только изменить знак в правой части этого равенства. Из сказанного в начале доказательства вытекает, что $a_{(j)} = 0$. Следовательно, мы доказали наше утверждение для $1 \leqslant r \leqslant n$.

При $r = 0$ мы имеем дело с пустым произведением и 1 служит базисом для $\bigwedge^0(E) = k$ над k. Случай $r > n$ мы в качестве тривиального упражнения предоставляем читателю.

Утверждение, касающееся размерности, тривиально, если принять во внимание тот факт, что существует биективное соответствие между множеством базисных элементов и подмножествами множества целых чисел $(1, \ldots, n)$.

Замечание. Можно провести первую часть доказательства, а именно для $\bigwedge^n(E)$, не предполагая известным существование определителей. Для этого нужно показать, что $\mathfrak{a}_n$ обладает в $T^n(E)$ одномерным дополнительным подмодулем. Это может быть сделано достаточно простыми средствами, что мы предоставляем читателю в качестве упражнения. В случае когда k — поле, это упражнение совсем три-

виально, поскольку сразу же проверяется, что $v_1 \otimes \ldots \otimes v_n$ не лежит в $\mathfrak{a}_n$. Этот другой подход к теореме доказывает тогда существование определителей.

§ 7. Симметрические произведения

Пусть $\mathfrak{S}_n$ обозначает симметрическую группу на n символах, действующую, скажем, на множестве целых чисел $(1, \ldots, n)$. Рассмотрим r-линейное отображение

$$f\colon E^{(r)} \to F;$$

оно называется *симметрическим*, если $f(x_1, \ldots, x_r) = f(x_{\sigma(1)}, \ldots, x_{\sigma(r)})$ для всех $\sigma \in \mathfrak{S}_r$.

Пусть $\mathfrak{b}_r$ — подмодуль в $T^r(E)$, порожденный всеми элементами вида

$$x_1 \otimes \ldots \otimes x_r - x_{\sigma(1)} \otimes \ldots \otimes x_{\sigma(r)},$$

где $x_i \in E$ и $\sigma \in \mathfrak{S}_r$. Введем фактормодуль

$$S^r(E) = T^r(E)/\mathfrak{b}_r$$

и рассмотрим прямую сумму

$$S(E) = \coprod_{r=0}^{\infty} S^r(E).$$

Непосредственно ясно, что прямая сумма

$$\mathfrak{b} = \coprod_{r=0}^{\infty} \mathfrak{b}_r$$

— идеал в $T(E)$ и, следовательно, $S(E)$ — градуированная k-алгебра, называемая *симметрической алгеброй* модуля E.

Далее, каноническое отображение

$$E^{(r)} \to S^r(E),$$

получаемое композицией отображений

$$E^{(r)} \to T^r(E) \to T^r(E)/\mathfrak{b}_r = S^r(E),$$

универсально для r-линейных симметрических отображений. Все это уже должно стать для читателя шаблонным.

Отметим, что S — функтор из категории модулей в категорию градуированных k-алгебр. Образ $(x_1, \ldots, x_r)$ при каноническом отображении

$$E^{(r)} \to S^r(E)$$

будет обозначаться просто через $x_1 \ldots x_r$.

Предложение 13. *Пусть E — свободный модуль размерности n над k, $\{v_1, \ldots, v_n\}$ — некоторый базис для E над k. Элементы этого базиса, рассматриваемые как элементы из $S^1(E)$ в $S(E)$, алгебраически независимы над k, и алгебра $S(E)$ изоморфна поэтому алгебре многочленов от n переменных над k.*

Доказательство. Взяв алгебраически независимые переменные $t_1, \ldots, t_n$ над k, образуем алгебру многочленов $k[t_1, \ldots, t_n]$. Пусть P_r — k-модуль однородных многочленов степени r. Определим отображение $E^{(r)} \to P_r$ следующим образом. Если $w_1, \ldots, w_r$ — элементы из E, которые могут быть записаны в виде

$$w_i = \sum_{\nu=1}^{n} a_{i\nu} v_\nu, \quad i = 1, \ldots, r,$$

то наше отображение задается правилом

$$(w_1 \ldots, w_r) \longmapsto (a_{11}t_1 + \ldots + a_{1n}t_n) \ldots (a_{r1}t_1 + \ldots + a_{rn}t_n).$$

Очевидно, что это отображение полилинейно и симметрично. Следовательно, оно может быть пропущено через линейное отображение $S^r(E)$ в P_r:

$$\begin{array}{ccc} E^{(r)} & \longrightarrow & S^r(E) \\ & \searrow \quad \swarrow & \\ & P_r & \end{array}$$

Из коммутативности нашей диаграммы ясно, что для всякого набора из r целых чисел $(i) = (i_1, \ldots, i_r)$ элемент $v_{i_1} \ldots v_{i_r}$ из $S^r(E)$ отображается на $t_{i_1} \ldots t_{i_r}$ в P_r. Так как одночлены $M_{(i)}(t)$ степени r линейно независимы над k, то одночлены $M_{(i)}(v)$ в $S^r(E)$ также линейно независимы над k, и наше отображение $S^r(E) \to P_r$ является изоморфизмом. Тотчас проверяется, что умножение в $S(E)$ соответствует умножению многочленов в $k[t]$ и, следовательно, отображение $S(E)$ в алгебру многочленов, описанное выше для каждой компоненты $S^r(E)$, индуцирует изоморфизм алгебры $S(E)$ на алгебру $k[t]$, что и требовалось.

§ 8. Кольцо Эйлера — Гротендика

Пусть k — поле и G — группа. Под (G, k)-*модулем* мы будем понимать пару (E, ρ), состоящую из k-пространства E и гомоморфизма

$$\rho\colon G \to \mathrm{Aut}_k(E).$$

Такой гомоморфизм называется также *представлением* G в E. Допуская вольность речи, мы будем также говорить, что k-пространство E является G-*модулем*. Группа G действует на E, и мы пи-

шем σx вместо $\rho(\sigma)x$. Поле k во всем последующем будет оставаться фиксированным.

Пусть $\mathfrak{M}(G)$ обозначает категорию, объектами которой являются (G, k)-модули. Морфизмами в $\mathfrak{M}(G)$ служат так называемые *G-гомоморфизмы*, т. е. k-линейные отображения $f: E \to F$, такие, что $f(\sigma x) = \sigma f(x)$.

Если E — G-модуль и $\sigma \in G$, то мы имеем по определению k-автоморфизм $\sigma: E \to E$. Поскольку T^r — функтор, для всякого r имеем индуцированный автоморфизм

$$T^r(\sigma): T^r(E) \to T^r(E),$$

так что $T^r(E)$ также является G-модулем. Беря прямую сумму, мы видим, что $T(E)$ есть G-модуль и, следовательно, T — функтор из категории G-модулей в категорию градуированных G-модулей. Аналогично для $\bigwedge^r$, S^r и $\bigwedge$, S.

Ясно, что ядром G-гомоморфизма будет G-модуль и фактормодулем G-модуля по G-подмодулю — снова G-модуль. Пусть $\mathfrak{M}_G$ — множество классов (G, k)-модулей относительно G-изоморфизма. Это множество является моноидом, сложение в котором представляется на модулях прямой суммой. Имеем *гомоморфизм Гротендика*

$$\gamma: \mathfrak{M}_G \to K(G)$$

моноида $\mathfrak{M}_G$ в группу Гротендика $K(G)$, взятую относительно точных последовательностей (ср. также с конструкцией в гл. IV, § 3). Для простоты мы пишем $K(G)$ вместо $K(\mathfrak{M}_G)$.

Если $[E]$ обозначает класс E относительно изоморфизма, то будем также писать $\gamma(E)$ вместо $\gamma([E])$.

Если E, F — G-модули, то их тензорное произведение $E \otimes F$ над k также является G-модулем. Здесь снова действие G на $E \otimes F$ задается функториально. Для всякого $\sigma \in G$ существует однозначно определенное k-линейное отображение $E \otimes F \to E \otimes F$, такое, что для $x \in E$, $y \in F$ имеем $x \otimes y \mapsto \sigma(x) \otimes \sigma(y)$. Тензорное произведение индуцирует закон композиции на $\mathfrak{M}_G$, так как тензорные произведения G-изоморфных модулей G-изоморфны. Мы утверждаем, что $\mathfrak{M}_G$ является также мультипликативным моноидом. Наш закон композиции ассоциативен, поскольку тензорное произведение ассоциативно. Существует единичный элемент, а именно класс модуля k над G, причем действие G на k определяется правилом $(\sigma, a) \mapsto a$ для всех $\sigma \in G$ и $a \in k$ (таким образом, $\sigma a = a$).

Произведение на $\mathfrak{M}_G$, очевидно, дистрибутивно относительно сложения, так как тензорное произведение прямой суммы есть прямая сумма тензорных произведений.

Наконец, поскольку $E \otimes F$ G-изоморфно $F \otimes E$, наше умножение в $\mathfrak{M}_G$ коммутативно. Таким образом, $\mathfrak{M}_G$ — моноид относительно сложения и коммутативный моноид относительно тензорного произведения,

причем умножение в нем $\mathbf{Z}$-билинейно по отношению к сложению.

Так как k — поле, то тензорное умножение точной последовательности G-модулей над k на любой G-модуль над k сохраняет точность. Благодаря этому *можно определить произведение в* $K(G)$, *которое однозначно задается условием*

$$\gamma(E)\gamma(F) = \gamma(E \otimes F)$$

для всех G-*модулей* E, F. Отсюда тривиально следует, что $K(G)$ есть кольцо и что γ — гомоморфизм как для аддитивного, так и для мультипликативного закона на $\mathfrak{M}_G$. Поэтому мы можем назвать $K(G)$ *кольцом Гротендика* группы G (над k). Так как G фиксирована, то мы будем также писать K вместо $K(G)$.

Если E — G-модуль, то мы пишем $\lambda^i(E)$ для обозначения элемента $\gamma(\bigwedge^i(E))$, другими словами, элемента в $K(G)$, который является образом при γ модуля $\bigwedge^i(E)$ или, более точно, класса этого модуля относительно изоморфизма.

Определим теперь отображение $\mathfrak{M}_G$ в кольцо степенных рядов $K[[t]]$, а именно отображение λ_t, такое, что

$$\lambda_t(E) = \sum_{i=0}^{\infty} \lambda^i(E)\, t^i.$$

Так как $\bigwedge^0(E) = k$, то $\lambda^0(E) = 1$. Следовательно, наше отображение является на самом деле отображением в мультипликативную группу степенных рядов, начинающихся с 1. Мы будем записывать эту группу в виде

$$1 + tK[[t]].$$

Таким образом, λ_t есть отображение

$$\lambda_t\colon \mathfrak{M}_G \to 1 + tK[[t]].$$

Предложение 14. *Для любых* k-*модулей* E, F *имеет место изоморфизм*

$$\coprod_{i+j=r} \bigwedge^i(E) \otimes \bigwedge^j(F) \to \bigwedge^r(E \oplus F).$$

Доказательство. Доказательство предоставляется читателю в качестве упражнения.

Следствие. *Отображение* λ_t, *описанное выше, является гомоморфизмом* $\mathfrak{M}_G$ *в мультипликативную группу* $1 + tK[[t]]$.

Ввиду универсальности $K(G)$ мы можем продолжить λ_t на $K(G)$ [*или, более точно, пропустить* λ_t через $K(G)$]. Индуцированное отображение на $K(G)$ будет снова обозначаться через λ_t.

Обозначим через $s^i(E)$ элемент $\gamma(S^i(E))$ в кольце Гротендика.

Предложение 15. *Для любого G-модуля E положим*

$$s_t(E) = \sum_{i=0}^{\infty} s^i(E)\, t^i.$$

Тогда $s_t(E)\lambda_{-t}(E) = 1$.

Доказательство этого утверждения сложнее, и необходимая для его получения техника составляет первую главу любого изложения, имеющего дело с более глубокими аспектами только что введенных структур.

В заключение — один пример.

Предположим, что E одномерно над k. Тогда $\lambda^i(E) = 0$ для $i > 0$. Следовательно,

$$\lambda_t(E) = 1 + \gamma(E)\, t$$

и

$$\lambda_{-t}(-\gamma(E)) = \frac{1}{1-\gamma(E)\,t} = 1 + \gamma(E)\,t + \gamma(E)^2 t^2 + \ldots.$$

В случае когда группа G тривиальна, можно дать простое доказательство предложения 15, сведя его к одномерному случаю.

§ 9. Некоторые функториальные изоморфизмы

Начнем с одного абстрактного определения. Пусть $\mathfrak{A}$, $\mathfrak{B}$ — две категории. Функторы из $\mathfrak{A}$ в $\mathfrak{B}$ (скажем, ковариантные от одной переменной) могут рассматриваться как объекты некоторой категории, морфизмы которой определяются следующим образом. Если L, M — два таких функтора, то морфизм $H\colon L \to M$ — это правило, которое каждому объекту X из $\mathfrak{A}$ сопоставляет морфизм $H_X\colon L(X) \to M(X)$ из $\mathfrak{B}$, такой, что для любого морфизма $f\colon X \to Y$ из $\mathfrak{A}$ коммутативна следующая диаграмма:

$$\begin{array}{ccc} L(X) & \xrightarrow{H_X} & M(X) \\ {\scriptstyle L(f)}\downarrow & & \downarrow{\scriptstyle M(f)} \\ L(Y) & \xrightarrow[H_Y]{} & M(Y) \end{array}$$

Мы можем поэтому говорить об изоморфизме функторов. Ниже мы увидим примеры подобных изоморфизмов в теории тензорных произведений. Категории, рассматриваемые в наших приложениях, являются аддитивными, т. е. в них множества морфизмов образуют аддитивные группы, а закон композиции $\mathbf{Z}$-билинеен. В этом случае функтор L называется *аддитивным*, если $L(f+g) = L(f) + L(g)$.

Пусть k — коммутативное кольцо. Мы будем рассматривать аддитивные функторы из категории k-модулей в себя, например, функтор перехода к дуальному модулю

$$E \longmapsto E^* = L(E, k) = \mathrm{Hom}_k(E, k).$$

Аналогично имеем функтор от двух переменных

$$(E, F) \longmapsto L(E, F) = \mathrm{Hom}_k(E, F),$$

который контравариантен по первому, ковариантен по второму аргументу и биаддитивен.

Мы приведем несколько примеров функториальных изоморфизмов, связанных с тензорным произведением; для этого нам будет удобно иметь общую теорему, дающую критерий того, когда морфизм функторов является на самом деле изоморфизмом.

Предложение 16. *Пусть L, M — два функтора (оба ковариантных или контравариантных) из категории k-модулей в себя. Предположим, что оба функтора аддитивны. Пусть $H\colon L \to M$ — морфизм функторов. Если $H_E\colon L(E) \to M(E)$ является изоморфизмом для всякого одномерного свободного модуля E над k, то H_E — изоморфизм для всякого конечномерного свободного модуля над k.*

Доказательство. Начнем с леммы.

Лемма. *Пусть E и E_i $(i = 1, \ldots, m)$ — модули над некоторым кольцом, $\varphi_i\colon E_i \to E$ и $\psi_i\colon E \to E_i$ — гомоморфизмы, обладающие следующими свойствами:*

$$\psi_i \circ \varphi_i = \mathrm{id}, \quad \psi_i \circ \varphi_j = 0 \text{ при } i \neq j,$$

$$\sum_{i=1}^{m} \varphi_i \circ \psi_i = \mathrm{id}.$$

Тогда отображение

$$x \longmapsto (\psi_1 x, \ldots, \psi_m x)$$

определяет изоморфизм E на прямое произведение $\prod_{i=1}^{m} E_i$, а отображение

$$(x_1, \ldots, x_m) \longmapsto \varphi_1 x_1 + \ldots + \varphi_m x_m$$

— изоморфизм прямого произведения на E. Обратно, если модуль E равен прямой сумме подмодулей E_i $(i = 1, \ldots, m)$ и если ψ_i — вложение E_i в E, а φ_i — проекция E на E_i, то эти отображения обладают указанными выше свойствами.

Доказательство. Доказательство шаблонно и по существу совпадает с доказательством предложения 2 из гл. III, § 3. Мы предоставляем его читателю в качестве упражнения.

Заметим, что семейства $\{\varphi_i\}$ и $\{\psi_i\}$, обладающие указанными в лемме свойствами, ведут себя функториально: если T — аддитивный функтор, скажем контравариантный, то семейства $\{T(\psi_i)\}$ и $\{T(\varphi_i)\}$ также обладают этими свойствами. Аналогично, если T — ковариантный функтор.

Применим лемму, взяв в качестве модулей E_i одномерные компоненты, возникающие из разложения E по какому-либо базису. Предположим, например, что оба функтора L, M ковариантны. Для всякого модуля E имеют место коммутативная диаграмма

$$\begin{array}{ccc} L(E) & \xrightarrow{H_E} & M(E) \\ {\scriptstyle L(\varphi_i)}\uparrow & & \uparrow{\scriptstyle M(\varphi_i)} \\ L(E_i) & \xrightarrow[H_{E_i}]{} & M(E_i) \end{array}$$

и аналогичная диаграмма, получающаяся заменой φ_i на ψ_i и обращением двух вертикальных стрелок. Следовательно, мы получаем разложение $L(E)$ в прямую сумму, определяемое отображениями $L(\psi_i)$ и $L(\varphi_i)$, и аналогично для $M(E)$ и отображений $M(\psi_i)$ и $M(\varphi_i)$. По предположению H_{E_i} — изоморфизмы. Отсюда тривиально вытекает, что H_E — изоморфизм. Чтобы, к примеру, доказать инъективность, запишем элемент $v \in L(E)$ в виде

$$v = \sum L(\varphi_i)\, v_i,$$

где $v_i \in L(E_i)$. Если $H_E v = 0$, то

$$0 = \sum H_E L(\varphi_i)\, v_i = \sum M(\varphi_i) H_{E_i} v_i,$$

и так как отображения $M(\varphi_i)$ дают разложение $M(E)$ в прямую сумму, то заключаем, что $H_{E_i} v_i = 0$ для всех i, откуда $v_i = 0$ и $v = 0$. Доказательство сюръективности столь же тривиально.

Если мы имеем дело с функтором от нескольких переменных, аддитивным по каждой из них, то, сохраняя все, кроме одной, *из этих переменных фиксированными, мы можем применить* предыдущее предложение. Именно так мы и поступаем в приводимых ниже следствиях.

Следствие 1. *Пусть E', E, F', F — свободные конечномерные модули над k. Имеет место функториальный изоморфизм*

$$L(E', E) \otimes L(F', F) \to L(E' \otimes F',\ E \otimes F),$$

такой, что

$$f \otimes g \longmapsto T(f, g).$$

Доказательство. Фиксируем E, F', F и рассматриваем $L(E', E) \otimes L(F', F)$ как функтор от одной переменной E'. Аналогично рассматриваем

$$L(E' \otimes F', E \otimes F)$$

как функтор от E'. Отображение $f \otimes g \longmapsto T(f, g)$ функториально, и, следовательно, согласно лемме, достаточно доказать, что оно дает изоморфизм, когда E' имеет размерность 1. Пусть модуль E' имеет размерность 1. Фиксируем его и рассмотрим два выражения, фигурирующих в следствии как функторы от E. Повторное применение леммы показывает, что достаточно установить, что наше отображение является изоморфизмом, когда E имеет размерность 1. Аналогично мы можем предполагать, что F, F' также имеют размерность 1. В этом случае проверка того, что отображение является изоморфизмом, тривиальна и следствие доказано.

Следствие 2. *Пусть E, F — свободные конечномерные модули. Имеет место изоморфизм*

$$\mathrm{End}_k(E) \otimes \mathrm{End}_k(F) \to \mathrm{End}_k(E \otimes F).$$

Доказательство. Частный случай следствия 1.

Отметим, что следствие 2 уже было доказано раньше, и мы упомянули его здесь только для того, чтобы видно было, как оно связано с принятой в этом параграфе точкой зрения.

Следствие 3. *Пусть E, F — свободные конечномерные модули над k. Имеет место функториальный изоморфизм*

$$E^* \otimes F \to L(E, F),$$

задаваемый для $x^* \in E^*$ и $y \in F$ отображением

$$x^* \otimes y \longmapsto \lambda,$$

где λ — такой элемент из $L(E, F)$, что $\lambda(x) = \langle x, x^* \rangle y$ для всех $x \in E$.

Обратный изоморфизм может быть описан следующим образом. Пусть $\{v_1, \ldots, v_n\}$ — базис в E и $\{v_1^*, \ldots, v_n^*\}$ — дуальный базис. Если A — элемент из $L(E, F)$, то его прообразом в тензорном произведении является элемент

$$\sum_{i=1}^{n} v_i^* \otimes A(v_i).$$

В частности, если $E = F$, то прообразом тождественного автоморфизма id_E служит элемент

$$\sum_{i=1}^{n} v_i^* \otimes v_i.$$

Доказательство следствия 3 получается сведéнием к случаю, когда оба модуля E, F одномерны, а в этом случае утверждение очевидно. Вывод указанной выше явной формулы для обратного отображения предоставляется читателю в качестве упражнения.

Дифференциальные геометры очень *любят* изоморфизм

$$L(E, E) \to E^* \otimes E$$

и часто, мысля геометрически о $L(E, E)$, используют в записи $E^* \otimes E$, благодаря чему без всякой надобности делается ударение на дуализации и совершенно не относящемся к делу формализме, тогда как значительно проще работать непосредственно с $L(E, E)$.

В дифференциальной геометрии обычно применяют к касательному пространству в точке многообразия различные функторы L и элементы получаемых таким образом пространств называют *тензорами* (типа L).

Следствие 4. *Пусть E, F — свободные конечномерные модули над k. Имеет место функториальный изоморфизм*

$$E^* \otimes F^* \to (E \otimes F)^*,$$

задаваемый для $x^* \in E^*$ и $y^* \in F^*$ отображением

$$x^* \otimes y^* \mapsto \lambda,$$

где λ — такой элемент из $(E \otimes F)^*$, что

$$\lambda(x \otimes y) = \langle x, x^* \rangle \langle y, y^* \rangle$$

для всех $x \in E$ и $y \in F$.

Доказательство. Такое же, как и выше.

Наконец, мы предлагаем в качестве упражнения следующий результат:

Предложение 17. *Пусть E — свободный конечномерный модуль над k. Функция следа на $L(E, E)$ равна композиции двух отображений*

$$L(E, E) \to E^* \otimes E \to k,$$

где первое отображение обратно к изоморфизму, описанному в следствии 3 предложения 16, а второе индуцировано билинейным отображением

$$(x^*, x) \mapsto \langle x, x^* \rangle.$$

Именно в тех ситуациях, когда встречается след, становится важным изоморфизм из следствия 3 и используется конечномерность E. Во многих же приложениях эта конечномерность не играет роли, и тогда лучше иметь дело непосредственно с $L(E, E)$.

УПРАЖНЕНИЯ

1. Пусть k — поле, $k(\alpha)$ — конечное расширение $f(X) = \mathrm{Irr}(\alpha, k, X)$, причем многочлен f сепарабелен, и k' — произвольное расширение над k. Показать, что $k(\alpha) \otimes k'$ — прямая сумма полей. Показать, что если поле k' алгебраически замкнуто, то эти поля соответствуют вложениям $k(\alpha)$ в k'.

2. Пусть k — поле, $f(X)$ — неприводимый многочлен над k и α — корень f. Показать, что $k(\alpha) \otimes k'$ изоморфно как k'-алгебра факторкольцу $k'[X]/(f(X))$.

3. Доказать предложение 14, построив естественный гомоморфизм и сравнив размерности левой и правой частей равенства.

4. Предположим, что группа G в § 8 тривиальна, и будем писать K вместо $K(1)$. Для $x \in K$ положим

$$\psi_{-t}(x) = -td \log \lambda_t(x) = -t \frac{\lambda_t'(x)}{\lambda_t(x)}, \quad \psi_t(x) = \sum_{k \geqslant 1} \psi^k(x) t^k.$$

Показать, что

$$\psi^k(x+y) = \psi^k(x) + \psi^k(y), \qquad \psi^k(xy) = \psi^k(x)\psi^k(y).$$

5. На модуле E над коммутативным кольцом задана билинейная форма. Объяснить, как действует расширение основного кольца: если $k \to k'$ — гомоморфизм коммутативных колец, то определить естественную билинейную форму на $E^{k'}$ над k'.

6. Пусть k — коммутативное кольцо. Обозначим через $L_a^r(E)$ модуль r-линейных знакопеременных отображений k-модуля E в k (т. е. модуль r-линейных знакопеременных форм на E). Положим, далее, $L_a^0(E) = k$ и

$$\Omega(E) = \prod_{r=0}^{\infty} L_a^r(E).$$

Показать, что $\Omega(E)$ — градуированная k-алгебра, умножение в которой определяется следующим образом. Если $\omega \in L_a^r(E)$, $\psi \in L_a^s(E)$ и $v_1, \ldots, v_{r+s}$ — элементы из E, то

$$(\omega \wedge \psi)(v_1, \ldots, v_{r+s}) = \sum \varepsilon(\sigma)\, \omega(v_{\sigma 1}, \ldots, v_{\sigma r})\, \psi(v_{\sigma(r+1)}, \ldots, v_{\sigma(r+s)}),$$

где сумма берется по всем перестановкам σ множества $(1, \ldots, r+s)$ таким, что $\sigma 1 < \ldots < \sigma r$ и $\sigma(r+1) < \ldots < \sigma(r+s)$.

7. Пусть E — свободный модуль размерности n над коммутативным кольцом k, $f\colon E \to E$ — линейное отображение и $\alpha_r(f) = \mathrm{tr}\, \Lambda^r(f)$, где $\Lambda^r(f)$ — эндоморфизм $\Lambda^r(E)$ в себя, индуцированный f. Имеем

$$\alpha_0(f) = 1, \quad \alpha_1(f) = \mathrm{tr}\, f, \quad \alpha_n(f) = \det f$$

и $\alpha_r(f) = 0$, если $r > n$. Показать, что

$$\det(1 + f) = \sum_{r \geqslant 0} \alpha_r(f).$$

[*Указание*: как обычно, доказать утверждение для случая, когда f представляется матрицей с переменными коэффициентами над кольцом целых чисел.] Интерпретировать $\alpha_r(f)$ в терминах коэффициентов характеристического многочлена отображения f.

8. Пусть E — конечномерный свободный модуль над коммутативным кольцом k, E^* — его дуальный модуль. Показать, что для всякого целого $r \geqslant 1$ $\wedge^r E$ и $\wedge^r E^*$ — модули, дуальные друг другу относительно билинейного отображения, такого, что

$$(v_1 \wedge \ldots \wedge v_r,\ v'_1 \wedge \ldots \wedge v'_r) \longmapsto \det(\langle v_i, v'_j \rangle),$$

где, как обычно, $\langle v_i, v'_j \rangle$ есть значение v'_j на v_i для $v_i \in E$ и $v'_j \in E^*$.

9. В обозначениях предыдущего упражнения пусть F — другой k-модуль, свободный и конечномерный и $f\colon E \to F$ — линейное отображение. Показать, что сопряженным к $\wedge^r f$ относительно билинейного отображения из предыдущего упражнения будет $\wedge^r ({}^t f)$, т. е. r-я знакопеременная степень сопряженного к f отображения.

10. Пусть P — алгебра некоммутативных многочленов от n переменных над полем k, $x_1, \ldots, x_r$ — различные элементы из P_1 (т. е. линейные выражения от переменных $t_1, \ldots, t_n$) и $a_1, \ldots, a_r \in k$. Показать, что если

$$a_1 x_1^{\nu} + \ldots + a_r x_r^{\nu} = 0$$

для всех целых $\nu = 1, \ldots, r$, то $a_i = 0$ для $i = 1, \ldots, r$. [*Указание*: взять гомоморфизм в алгебру коммутативных многочленов и проводить рассуждения там.]

11. Пусть G — конечное множество эндоморфизмов конечномерного векторного пространства E над полем k. Для всякого $\sigma \in G$ пусть c_σ — элемент из k. Показать, что если

$$\sum_{\sigma \in G} c_\sigma T^r(\sigma) = 0$$

для всех целых $r \geqslant 1$, то $c_\sigma = 0$ для всех $\sigma \in G$. [*Указание*: использовать предыдущее упражнение и предложение 11.]

12. (Стейнберг). Пусть G — конечный моноид, $k[G]$ — моноидная алгебра над некоторым полем k и $G \to \mathrm{End}_k(E)$ — точное (т. е. инъективное) представление, так что мы можем отождествить G с некоторым мультипликативным подмножеством в $\mathrm{End}_k(E)$. Показать, что T^r индуцирует представление группы G на $T^r(E)$, откуда по линейности получается представление алгебры $k[G]$ на $T^r(E)$. Показать, что если $\alpha \in k[G]$ и $T^r(\alpha) = 0$ для всех целых $r \geqslant 1$, то $\alpha = 0$. [*Указание*: применить предыдущее упражнение.]

13. Когда вы прочитаете главу о представлениях конечных групп, выведите из упражнения 12 следующую теорему Бернсайда. Пусть G — конечная группа, k — поле характеристики, взаимно простой с порядком G, и E — конечномерное (G, k)-пространство, такое, что представление группы G — точное. Тогда всякое неприводимое представление G встречается с кратностью $\geqslant 1$ в некоторой тензорной степени $T^r(E)$.

Глава XVII

Полупростота

Во многих приложениях модули разлагаются в прямую сумму простых подмодулей, и в этих случаях можно развить некую структурную теорию, как в общих предпосылках, так и для специальных приложений. Настоящая глава посвящена результатам, которые могут быть доказаны в общей ситуации. В следующей главе мы рассмотрим те дополнительные результаты, которые могут быть доказаны в важном классическом частном случае.

При доказательстве теоремы плотности я более или менее следовал Бурбаки.

§ 1. Матрицы и линейные отображения над некоммутативными кольцами

В гл. XIII мы рассматривали исключительно матрицы над коммутативными кольцами. Для наших нынешних целей надо исследовать более общую ситуацию.

Пусть K — кольцо. Матрица (φ_{ij}) с коэффициентами в K определяется точно так же, как мы это делали для коммутативных колец. Произведение матриц определяется по той же самой формуле. По-прежнему имеют место ассоциативность и дистрибутивность, в случае когда размеры матриц таковы, что соответствующие операции для них определены. В частности, квадратные матрицы размера $n \times n$ над K образуют кольцо, обозначаемое, как и раньше, символом $\mathrm{Mat}_n(K)$. Имеет место кольцевой гомоморфизм

$$K \to \mathrm{Mat}_n(K)$$

на диагональ.

Напомним, что *телом* называется кольцо с $1 \neq 0$, в котором всякий ненулевой элемент обладает мультипликативным обратным.

Если K — тело, то всякий ненулевой K-модуль имеет базис и мощности любых двух базисов равны. Доказательство такое же, как в коммутативном случае: в рассуждениях мы нигде не использовали коммутативности. Эта мощность по-прежнему называется размерностью

модуля над K, и модули над телами называются векторными пространствами.

Как и в коммутативном случае, мы можем всякому линейному отображению сопоставить матрицу, зависящую от выбора конечного базиса. Однако мы будем рассматривать несколько отличную ситуацию, которая нам потребуется для приложений к полупростым модулям.

Пусть R — кольцо, и пусть

$$E = E_1 \oplus \ldots \oplus E_n, \quad F = F_1 \oplus \ldots \oplus F_m$$

— R-модули, представленные в виде прямых сумм R-модулей. Мы хотим описать наиболее общий вид R-гомоморфизма модуля E в F.

Предположим сначала, что $F = F_1$ имеет одну компоненту. Пусть

$$\varphi\colon E_1 \oplus \ldots \oplus E_n \to F$$

— гомоморфизм и $\varphi_j\colon E_j \to F$ — ограничение φ на слагаемое E_j. Всякий элемент $x \in E$ имеет единственное представление $x = x_1 + \ldots + x_n$, где $x_j \in E_j$. Мы можем поэтому сопоставить элементу x столбец $X = {}^t(x_1, \ldots, x_n)$, компоненты которого лежат соответственно в $E_1, \ldots, E_n$, а гомоморфизму φ — строку $(\varphi_1, \ldots, \varphi_n)$, $\varphi_j \in \mathrm{Hom}_R(E_j, F)$. Тогда действие φ на элемент x из E описывается умножением матриц — строки на столбец.

Более общо, рассмотрим гомоморфизм

$$\varphi\colon E_1 \oplus \ldots \oplus E_n \to F_1 \oplus \ldots \oplus F_m.$$

Пусть $\pi_i\colon F_1 \oplus \ldots \oplus F_m \to F_i$ — проекция на i-й множитель. Мы можем применить наше предыдущее замечание к $\pi_i \circ \varphi$ для каждого i. При этом мы обнаружим, что существуют однозначно определенные элементы $\varphi_{ij} \in \mathrm{Hom}_R(E_j, F_i)$, такие, что φ имеет матричное представление

$$M(\varphi) = \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix},$$

причем действие φ на элемент x задается умножением матриц, а именно

$$\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{pmatrix}.$$

Обратно, если дана матрица (φ_{ij}) с $\varphi_{ij} \in \mathrm{Hom}_R(E_j, F_i)$, то с помощью нее можно определить элемент из $\mathrm{Hom}_R(E, F)$. Таким образом, мы получаем изоморфизм аддитивных групп между $\mathrm{Hom}_R(E, F)$ и этой группой матриц.

Пусть, в частности, E — фиксированный R-модуль и $K = \mathrm{End}_R(E)$. Тогда имеет место изоморфизм колец

$$\mathrm{End}_R(E^{(n)}) \to \mathrm{Mat}_n(K),$$

который всякому $\varphi \in \mathrm{End}_R(E^{(n)})$ сопоставляет матрицу

$$\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \varphi_{n1} & \cdots & \varphi_{nn} \end{pmatrix},$$

определенную выше и действующую слева на столбцы из $E^{(n)}$ с компонентами из E.

Замечание. Пусть E — одномерное векторное пространство над телом D и $\{v\}$ — его базис. Для всякого $a \in D$ существует единственное D-линейное отображение $f_a\colon E \to E$, такое, что $f_a(v) = a^{-1}v$. Тогда справедливо правило

$$f_a f_b = f_{ba}.$$

Таким образом, когда мы сопоставляем линейному отображению матрицу, зависящую от базиса, умножение оказывается скрученным. Тем не менее утверждение, которое мы сформулировали перед этим замечанием, правильно! Дело в том, что, когда E одномерно, мы берем φ_{ij} в $\mathrm{End}_D(E)$, а не в D. Поэтому K не изоморфно D (в некоммутативном случае), а антиизоморфно. Это единственный пункт, в котором формальная элементарная теория линейных отображений различается в коммутативном и некоммутативном случаях.

Напомним, что R-модуль E называется *простым*, если он $\neq 0$ и не содержит подмодулей, отличных от 0 или E.

Предложение 1. *Пусть E, F — простые R-модули. Тогда всякий ненулевой гомоморфизм E в F является изоморфизмом, а кольцо $\mathrm{End}_R(E)$ — телом.*

Доказательство. Пусть $f\colon E \to F$ — ненулевой гомоморфизм. Его образ и ядро — подмодули, следовательно, равны соответственно F и 0, так что f — изоморфизм. Если $E = F$, то f обратим, что и требовалось доказать.

(Предложение 1 известно как *лемма Шура.*)

Следующее предложение полностью описывает кольцо эндоморфизмов прямой суммы простых модулей.

Предложение 2. *Пусть* $E = E_1^{(n_1)} \oplus \ldots \oplus E_r^{(n_r)}$ *— прямая сумма простых модулей, где* E_i *между собой неизоморфны и каждый* E_i *повторяется в сумме* n_i *раз. Тогда с точностью до перестановки и изоморфизмов* $E_1, \ldots, E_r$ *(а также и их кратности) однозначно определены. Кольцо* $\mathrm{End}_R(E)$ *изоморфно кольцу матриц вида*

$$\begin{pmatrix} M_1 & \ldots & 0 \\ . & M_2 & . \\ . & . & . \\ . & . & . \\ 0 & \ldots & M_r \end{pmatrix},$$

где M_i *— матрица размера* $n_i \times n_i$ *над* $\mathrm{End}_R(E_i)$. *(Изоморфизм этот совпадает с тем, который соответствует разложению в прямую сумму.)*

Доказательство. Последнее утверждение вытекает из наших предыдущих рассмотрений, если принять во внимание предложение 1. Утверждение же о простых слагаемых и их кратностях в прямых суммах является следствием общей теоремы Жордана — Гёльдера.

В случае когда E обладает разложением в (конечную) прямую сумму простых подмодулей, число раз, которое простой модуль из данного класса изоморфных модулей встречается в разложении, будет называться *кратностью* этого простого модуля (или его класса относительно изоморфизма).

Кроме того, если модуль

$$E = E_1^{(n_1)} \oplus, \ldots, \oplus E_r^{(n_r)}$$

представлен в виде прямой суммы простых подмодулей, то мы будем называть $n_1 + \ldots + n_r$ *длиной* E. Во многих случаях мы будем также писать

$$E = n_1 E_1 \oplus \ldots \oplus n_r E_r = \prod_{i=1}^{r} n_i E_i.$$

§ 2. Условия, определяющие полупростоту

Пусть R *— кольцо. Если специально не оговаривается противное, то все модули и все гомоморфизмы в этом параграфе предполагаются* R*-модулями и* R*-гомоморфизмами.*

Следующие условия на модуль E эквивалентны:

ПП 1. E — сумма некоторого семейства простых подмодулей.

ПП 2. E — прямая сумма некоторого семейства простых подмодулей.

ПП 3. Всякий подмодуль F в E является прямым слагаемым, т. е. существует подмодуль F', такой, что $E = F \oplus F'$.

Сейчас мы докажем это.

Лемма. *Пусть* $E = \sum_{i \in I} E_i$ — *сумма (не обязательно прямая) простых подмодулей. Тогда существует подмножество* $J \subset I$, *такое, что* E — *прямая сумма* $\coprod_{j \in J} E_j$.

Доказательство. Пусть J — максимальное подмножество в I, такое, что сумма $\sum_{j \in J} E_j$ прямая. Мы утверждаем, что эта сумма в действительности равна E. Достаточно доказать, что каждый E_i содержится в этой сумме. Но пересечение нашей суммы с E_i является подмодулем в E_i и, следовательно, равно 0 или E_i. Если оно равно 0, то подмножество J немаксимально, поскольку мы можем присоединить к нему i. Следовательно, E_i содержится в сумме, и наша лемма доказана.

Лемма показывает, что ПП 1 влечет ПП 2. Чтобы убедиться, что ПП 2 влечет ПП 3, возьмем подмодуль F и максимальное подмножество J в I, такое, что сумма $F + \coprod_{j \in J} E_j$ — прямая. То же самое рассуждение, что и выше, показывает, что эта сумма равна E.

Чтобы доказать, что ПП 3 влечет ПП 1, докажем сначала, что всякий ненулевой подмодуль в E содержит некоторый простой подмодуль. Пусть F — ненулевой подмодуль и $v \in F$, $v \neq 0$. Тогда по определению Rv — главный подмодуль и ядро гомоморфизма

$$R \to Rv$$

есть левый идеал $L \neq R$. Следовательно, L содержится в максимальном левом идеале $M \neq R$ (в силу леммы Цорна). Тогда M/L есть максимальный подмодуль в R/L (не равный R/L) и, следовательно, Mv — максимальный подмодуль в Rv, не равный Rv и соответствующий M/L при изоморфизме

$$R/L \to Rv.$$

Мы можем записать $E = Mv \oplus M'$ для некоторого подмодуля M'. Тогда $Rv = Mv \oplus (M' \cap Rv)$, поскольку всякий элемент $x \in Rv$ может быть однозначно записан в виде суммы $x = \alpha v + x'$, где $\alpha \in R$ и $x' \in M'$, причем, очевидно, $x' = x - \alpha v$ лежит в Rv. Так как Mv максимален в Rv, то модуль $M' \cap Rv$ простой, что и требовалось установить.

Пусть E_0 — подмодуль в E, являющийся суммой всех простых подмодулей модуля E. Если $E_0 \neq E$, то $E = E_0 \oplus F$, где $F \neq 0$, а потому существует простой подмодуль в F вопреки определению E_0. Это доказывает, что ПП 3 влечет ПП1.

Модуль E, удовлетворяющий нашим трем условиям, называется *полупростым*.

Предложение 3. *Всякий подмодуль и всякий фактормодуль полупростого модуля полупросты.*

Доказательство. Пусть F — подмодуль и F_0 — сумма всех простых подмодулей в F. Запишем $E = F_0 \oplus F_0'$. Всякий элемент x из F имеет единственное представление $x = x_0 + x_0'$, где $x_0 \in F_0$ и $x_0' \in F_0'$. Но $x_0' = x - x_0 \in F$. Следовательно, F есть прямая сумма

$$F = F_0 \oplus (F \cap F_0').$$

Отсюда видно, что F_0 совпадает с F, который тем самым полупрост. Что касается фактормодуля, то запишем $E = F \oplus F'$. Тогда F' есть сумма своих простых подмодулей и каноническое отображение $E \to E/F$ индуцирует изоморфизм F' на E/F. Следовательно, модуль E/F полупрост.

§ 3. Теорема плотности

Пусть E — полупростой R-модуль. Обозначим через K кольцо $\mathrm{End}_R(E)$. Тогда E будет также K-модулем, причем действие K на E задается отображением

$$(\varphi, x) \longmapsto \varphi(x),$$

где $\varphi \in K$ и $x \in E$. Всякий элемент $\alpha \in R$ посредством отображения $f_\alpha(x) = \alpha x$ индуцирует K-гомоморфизм f_α: $E \to E$. Но именно это и означает условие

$$\varphi(\alpha x) = \alpha \varphi(x).$$

Таким образом, мы получаем гомоморфизм колец

$$R \to \mathrm{End}_K(E).$$

Возникает вопрос, насколько велик образ этого гомоморфизма. Теорема плотности утверждает, что он весьма большой.

Лемма. *Пусть E — полупростой модуль над R, $K = \mathrm{End}_R(E)$, $f \in \mathrm{End}_K(E)$, $x \in E$. Существует элемент $\alpha \in R$, такой, что $\alpha x = f(x)$.*

Доказательство. Так как E полупрост, то имеет место разложение в R-прямую сумму

$$E = Rx \oplus F$$

для некоторого подмодуля F. Пусть $\pi\colon E \to Rx$ — проекция. Тогда $\pi \in K$ и, следовательно,

$$f(x) = f(\pi x) = \pi f(x).$$

Это показывает, что $f(x) \in Rx$, что и требовалось.

Теорема плотности обобщает эту лемму на случай конечного числа элементов из E вместо одного. Для доказательства мы используем диагональный прием.

Теорема 1 (Джекобсон). *Пусть E — полупростой модуль над R, $K = \mathrm{End}_R(E)$, $f \in \mathrm{End}_K(E)$ и $x_1, \ldots, x_n \in E$. Тогда существует элемент $\alpha \in R$, такой, что*

$$\alpha x_i = f(x_i) \quad \text{для} \quad i = 1, \ldots, n.$$

Доказательство. Пусть $f^{(n)}\colon E^{(n)} \to E^{(n)}$ — прямая степень отображения f, так что

$$f^{(n)}(y_1, \ldots, y_n) = (f(y_1), \ldots, f(y_n)).$$

Положим $K' = \mathrm{End}_R(E^{(n)})$. Очевидно, K' есть не что иное, как кольцо матриц с коэффициентами в K. Так как f в своем действии на E коммутирует с элементами из K, то непосредственно видно, что $f^{(n)}$ лежит в $\mathrm{End}_{K'}(E^{(n)})$. Но модуль $E^{(n)}$ полупростой, поэтому в силу леммы существует элемент $\alpha \in R$, такой, что

$$(\alpha x_1, \ldots, \alpha x_n) = (f(x_1), \ldots, f(x_n)),$$

а это нам как раз и нужно было доказать.

Следствие 1. *Пусть E — конечномерное векторное пространство над алгебраически замкнутым полем k и R — подалгебра в $\mathrm{End}_k(E)$. Если E — простой R-модуль, то $R = \mathrm{End}_k(E)$.*

Доказательство. Мы утверждаем, что $\mathrm{End}_R(E) = k$. Во всяком случае, $\mathrm{End}_R(E)$ есть тело K, содержащее k в качестве подкольца, и всякий элемент из k коммутирует со всяким элементом из K. Пусть $\alpha \in K$. Тогда $k(\alpha)$ — поле. Далее, K содержится в $\mathrm{End}_k(E)$ как k-подпространство и поэтому конечномерно над k. Следовательно, поле $k(\alpha)$ конечно над k, а потому равно k, поскольку k алгебраически замкнуто. Это доказывает, что $\mathrm{End}_R(E) = k$. Пусть теперь $\{v_1, \ldots, v_n\}$ — базис для E над k и $A \in \mathrm{End}_k(E)$. Согласно теореме плотности, существует элемент $\alpha \in R$, такой, что

$$\alpha v_i = A v_i \quad \text{для} \quad i = 1, \ldots, n.$$

Так как действие эндоморфизма A определяется его действием на базис, то заключаем, что $R = \mathrm{End}_k(E)$.

Следствие 1 известно как *теорема Бернсайда*. Оно используется в следующей ситуации. Пусть E — конечномерное векторное пространство над полем k и G — подмоноид в $GL(E)$ (мультипликативный).

Под *G-инвариантным* подпространством в E понимается такое подпространство F, что $\sigma F \subset F$ для всех $\sigma \in G$. Мы будем говорить, что пространство E *G-просто*, если оно не содержит G-инвариантных подпространств, отличных от 0 и самого E, причем $E \neq 0$. Пусть $R = k[G]$ — подалгебра в $\mathrm{End}_k(E)$, порожденная G над k. Так как мы предположили, что G — моноид, то R состоит из линейных комбинаций

$$\sum a_i \sigma_i,$$

где $a_i \in k$ и $\sigma_i \in G$. Это означает, что подпространство F в E будет G-инвариантным в том и только в том случае, если оно R-инвариантно. Следовательно, пространство E тогда и только тогда G-просто, когда оно просто над R в том смысле, который мы рассматривали выше. Мы можем поэтому переформулировать теорему Бернсайда следующим образом.

Следствие 2. *Пусть E — конечномерное векторное пространство над алгебраически замкнутым полем k и G — (мультипликативный) подмоноид в $GL(E)$. Если E G-просто, то $k[G] = \mathrm{End}_k(E)$.*

Даже и в тех случаях, когда поле k не является алгебраически замкнутым, мы все-таки можем получить некоторый результат. Пусть вообще A — кольцо и E — простой A-модуль. Как мы видели, $\mathrm{End}_R(E)$ — тело, которое мы обозначим через D, и E — векторное пространство над D.

Пусть R — кольцо и E — произвольный R-модуль. Мы будем говорить, что E — *точный* модуль, если удовлетворяется следующее условие: соотношение $\alpha x = 0$, $\alpha \in R$, для всех $x \in E$ влечет $\alpha = 0$. В приложениях E будет векторным пространством над полем k, и мы будем иметь кольцевой гомоморфизм R в $\mathrm{End}_k(E)$. Тогда E становится R-модулем, точность которого имеет место тогда и только тогда, когда этот гомоморфизм инъективен.

Следствие 3 (Теорема Веддерберна). *Пусть R — кольцо и E — простой точный модуль над R. Предположим, что E конечномерен над $D = \mathrm{End}_R(E)$. Тогда $R = \mathrm{End}_D(E)$.*

Доказательство. Пусть $\{v_1, \ldots, v_n\}$ — базис E над D. Для заданного элемента $A \in \mathrm{End}_D(E)$ в силу теоремы 1 существует элемент $\alpha \in R$, такой, что

$$\alpha v_i = A v_i \quad \text{при} \quad i = 1, \ldots, n.$$

Следовательно, отображение $R \to \mathrm{End}_D(E)$ сюръективно. Предположение, что модуль E — точный над R, влечет, что это отображение инъективно, и наше следствие доказано.

§ 4. Полупростые кольца

Кольцо R называется *полупростым*, если $1 \neq 0$ и R полупросто как левый модуль над собой.

Предложение 4. *Если R полупросто, то всякий R-модуль полупрост.*

Доказательство. Всякий R-модуль является фактормодулем свободного модуля, а свободный модуль есть прямая сумма R с собой некоторое число раз. Чтобы завершить доказательство, мы можем теперь применить предложение 3.

Всякий левый идеал кольца R является R-модулем; он называется *простым*, если он прост как модуль. Два идеала L, L' называются *изоморфными*, если они изоморфны как модули.

Разложим теперь R в прямую сумму своих простых левых идеалов и получим тем самым структурную теорему для R.

Пусть $\{L_i\}_{i \in I}$ такое семейство простых левых идеалов, что никакие два идеала в нем не изоморфны и всякий простой левый идеал изоморфен одному из идеалов этого семейства. Мы будем говорить, что это семейство является семейством представителей для классов простых левых идеалов относительно изоморфизма.

Лемма. *Пусть L — простой левый идеал и E — простой R-модуль. Если L неизоморфен E, то $LE = 0$.*

Доказательство. Имеем $RLE = LE$, и LE есть подмодуль в E, равный, следовательно, 0 или E. Предположим, что $LE = E$. Пусть элемент $y \in E$ таков, что

$$Ly \neq 0.$$

Так как Ly — подмодуль в E, то $Ly = E$. Отображение $a \mapsto ay$ идеала L в E является гомоморфизмом L в E, сюръективным и, следовательно, ненулевым. Поскольку L прост, то этот гомоморфизм должен быть изоморфизмом.

Пусть

$$R_i = \sum_{L \cong L_i} L$$

— сумма всех простых левых идеалов, изоморфных L_i. Из леммы следует, что $R_i R_j = 0$, если $i \neq j$. В последующем это будет по-

стоянно использоваться. Отметим, что R_i есть левый идеал и что R представляется в виде суммы

$$R = \sum_{i \in I} R_i,$$

так как R — сумма простых левых идеалов. Следовательно, для любого $j \in I$

$$R_j \subset R_j R = R_j R_j \subset R_j,$$

где первое включение справедливо, поскольку R содержит единичный элемент, а последнее, — поскольку R_j есть левый идеал. Таким образом, R_j является также правым идеалом, т. е. R_j — двусторонний идеал для всякого $j \in I$.

Мы можем представить единичный элемент 1 кольца R в виде суммы

$$1 = \sum_{i \in I} e_i,$$

где $e_i \in R_i$. Эта сумма на самом деле конечна, почти все $e_i = 0$. Пусть, скажем, $e_i \neq 0$ для $i = 1, \ldots, s$, так что

$$1 = e_1 + \ldots + e_s.$$

Пусть $x \in R$. Запишем

$$x = \sum_{i \in I} x_i, \qquad x_i \in R_i.$$

Для $j = 1, \ldots, s$ имеем $e_j x = e_j x_j$, а также

$$x_j = 1 \cdot x_j = e_1 x_j + \ldots + e_s x_j = e_j x_j.$$

Кроме того, $x = e_1 x + \ldots + e_s x$. Это доказывает, что индексов i, отличных от $1, \ldots, s$, в сумме нет, а также, что i-я компонента x_i элемента x однозначно определена как $e_i x = e_i x_i$. Следовательно, сумма $R = R_1 + \ldots + R_s$ — прямая и, кроме того, e_i служит единичным элементом для R_i, которое является поэтому кольцом. Так как $R_i R_j = 0$ для $i \neq j$, то мы видим, что в действительности

$$R = \prod_{i=1}^{s} R_i$$

есть прямое произведение колец R_i.

Кольцо R называется *простым*, если оно полупросто и имеет только один класс простых левых идеалов относительно изоморфизма. Таким образом, мы доказали структурную теорему для полупростых колец.

Теорема 2. *Пусть R — полупростое кольцо. Существует только конечное число неизоморфных простых левых идеалов,*

скажем $L_1, \ldots, L_s$. *Если* $R_i = \sum_{L \approx L_i} L$ — *сумма всех простых левых идеалов, изоморфных* L_i, *то* R_i — *двусторонний идеал, который является также кольцом (с операциями, индуцированными* R), *и кольцо* R *изоморфно прямому произведению*

$$R = \prod_{i=1}^{s} R_i.$$

Каждое R_i *является простым кольцом. Если* e_i — *его единичный элемент, то* $1 = e_1 + \ldots + e_s$ *и* $R_i = Re_i$. *Далее,* $e_i e_j = 0$ *при* $i \neq j$ [1]).

Перейдем теперь к модулям.

Теорема 3. *Пусть* R — *полупростое кольцо и* E — R-*модуль* $\neq 0$. *Тогда*

$$E = \coprod_{i=1}^{s} R_i E = \coprod_{i=1}^{s} e_i E,$$

причем $R_i E$ — *подмодуль в* E, *равный сумме всех простых подмодулей, изоморфных* L_i.

Доказательство. Пусть E_i — сумма всех простых подмодулей в E, изоморфных L_i. Если V — простой подмодуль в E, то $RV = V$ и, следовательно, $L_i V = V$ для некоторого i. В силу предыдущей леммы имеем $L_i \approx V$. Следовательно, E есть прямая сумма $E_1, \ldots, E_s$. Наконец, ясно, что $R_i E = E_i$.

Следствие 1. *Пусть кольцо* R *полупросто. Тогда всякий простой модуль изоморфен одному из простых левых идеалов* L_i.

Следствие 2. *Простое кольцо имеет с точностью до изоморфизма только один простой модуль.*

Оба эти следствия непосредственно вытекают из теорем 2 и 3.

§ 5. Простые кольца

Лемма. *Пусть* R — *кольцо и* $\psi \in \mathrm{End}_R(R)$ — *гомоморфизм кольца* R, *рассматриваемого как* R-*модуль, в себя. Тогда существует элемент* $\alpha \in R$, *такой, что* $\psi(x) = x\alpha$ *для всех* $x \in R$.

Доказательство. Имеем $\psi(x) = \psi(x \cdot 1) = x\psi(1)$. Положим $\alpha = \psi(1)$.

---

[1]) Там, где идеалы R_i явно не указываются, мы будем называть e_i *идемпотентными* элементами, чтобы избежать путаницы с единицами в R. — *Прим. ред.*

Теорема 4. *Пусть R — простое кольцо. Тогда R — конечная прямая сумма простых левых идеалов. В R нет двусторонних идеалов, кроме 0 и R. Если L, M — простые левые идеалы, то существует элемент $\alpha \in R$, такой, что $L\alpha = M$. При этом $LR = R$.*

Доказательство. Так как кольцо R по определению полупросто, то оно является прямой суммой простых левых идеалов, скажем $\coprod_{j \in J} L_j$. Мы можем представить 1 в виде конечной суммы $1 = \sum_{j=1}^{m} \beta_j$, где $\beta_j \in L_j$. Тогда

$$R = \coprod_{j=1}^{m} R\beta_j = \coprod_{j=1}^{m} L_j.$$

Это доказывает наше первое утверждение. Что касается второго утверждения, то оно есть следствие третьего. Пусть, таким образом, L — простой левый идеал. Имеем разложение в прямую сумму $R = L \oplus L'$. Пусть π: $R \to L$ — проекция. Это R-эндоморфизм. Пусть M — любой другой простой левый идеал и σ: $L \to M$ — изоморфизм (существующий по определению простого кольца). Тогда отображение $\sigma \circ \pi$: $R \to R$ есть R-эндоморфизм. В силу леммы существует элемент $\alpha \in R$, такой, что

$$\sigma \circ \pi(x) = x\alpha \quad \text{для всех} \quad x \in R.$$

Применим это к элементу $x \in L$. Найдем

$$\sigma(x) = x\alpha \quad \text{для всех} \quad x \in L.$$

Отображение $x \mapsto x\alpha$ есть ненулевой R-гомоморфизм L в M и, следовательно, изоморфизм. Отсюда тотчас вытекает, что $LR = R$, и наша теорема тем самым доказана.

Следствие. *Пусть R — простое кольцо, L — его простой левый идеал и E — простой R-модуль. Тогда $LE = E$ и модуль E точный.*

Доказательство. Имеем $LE = L(RE) = (LR)E = RE = E$. Допустим, что $\alpha E = 0$ для некоторого $\alpha \in R$. Тогда $R\alpha RE = R\alpha E = 0$. Но $R\alpha R$ — двусторонний идеал. Следовательно, $R\alpha R = 0$ и $\alpha = 0$. Это доказывает, что модуль E точный.

Теорема 5 (Риффель). *Пусть R — кольцо, не содержащее двусторонних идеалов, отличных от 0 и R. Пусть L — левый идеал, $R' = \mathrm{End}_R(L)$ и $R'' = \mathrm{End}_{R'}(L)$. Тогда естественное отображение λ: $R \to R''$ является изоморфизмом.*

Доказательство. Ядро λ — двусторонний идеал, так что отображение λ инъективно. Так как LR — двусторонний идеал, то $LR = R$ и $\lambda(L)\lambda(R) = \lambda(R)$. Для любых x, $y \in L$ и $f \in R''$ имеем $f(xy) = f(x)y$, поскольку правое умножение на y является R-эндоморфизмом L. Следовательно, $\lambda(L)$ — левый идеал в R'', так что

$$R'' = R''\lambda(R) = R''\lambda(L)\lambda(R) = \lambda(L)\lambda(R) = \lambda(R),$$

что и требовалось доказать.

Теорема 5 показывает, что R можно представить как кольцо эндоморфизмов некоторого конечномерного модуля над телом. Обратно:

Теорема 6. *Пусть D — тело, E — конечномерное векторное пространство над D и $R = \mathrm{End}_D(E)$. Тогда кольцо R — простое и E — простой R-модуль. Кроме того, $D = \mathrm{End}_R(E)$.*

Доказательство. Покажем сначала, что E — простой R-модуль. Пусть $v \in E$, $v \neq 0$. Тогда элемент v может быть дополнен до базиса E над D и, значит, для заданного $w \in E$ существует элемент $\alpha \in R$, такой, что $\alpha v = w$. Следовательно, E не может содержать никакого инвариантного подпространства, кроме 0 и самого себя, т. е. E просто над R. Ясно, что E — точный модуль над R. Пусть $\{v_1, \ldots, v_m\}$ — базис E над D. Отображение

$$\alpha \longmapsto (\alpha v_1, \ldots, \alpha v_m)$$

кольца R в $E^{(m)}$ является инъективным R-гомоморфизмом R в $E^{(m)}$. Для заданных $(w_1, \ldots, w_m) \in E^{(m)}$ существует элемент $\alpha \in R$, такой, что $\alpha v_i = w_i$, и, следовательно, кольцо R R-изоморфно $E^{(m)}$. Это показывает, что R (как R-модуль над собой) изоморфно прямой сумме простых модулей, а потому полупросто. Далее, все эти простые модули изоморфны друг другу и, значит, в силу теоремы 2 кольцо R простое.

Остается доказать, что $D = \mathrm{End}_R(E)$. Заметим, что E — полупростой модуль над D, так как в векторном пространстве всякое подпространство обладает дополнительным подпространством. Мы можем поэтому применить теорему плотности (R и D теперь поменялись ролями!). Пусть $\varphi \in \mathrm{End}_R(E)$ и $v \in E$, $v \neq 0$. В силу теоремы плотности существует элемент $a \in D$, такой, что $\varphi(v) = av$. Пусть $w \in E$. Существует элемент $f \in R$, такой, что $f(v) = w$. Тогда

$$\varphi(w) = \varphi(f(v)) = f(\varphi(v)) = f(av) = af(v) = aw.$$

Таким образом, $\varphi(w) = aw$ для всех $w \in E$. Это означает, что $\varphi \in D$, что и завершает наше доказательство.

Теорема 7. *Пусть k — поле, E — конечномерное векторное пространство размерности m над k и $R = \mathrm{End}_k(E)$. Тогда*

R — k-пространство и

$$\dim_k R = m^2.$$

Кроме того, m есть число простых левых идеалов, содержащихся в произвольном разложении R в прямую сумму таких идеалов.

Доказательство. Пространство k-эндоморфизмов k-пространства E представляется пространством матриц размера $m \times m$ над k, так что размерность R как k-пространства равна m^2. С другой стороны, доказательство теоремы 6 показывает, что R как R-модуль R-изоморфен прямой сумме $E^{(m)}$. Но однозначность разложения модуля в прямую сумму простых модулей нам известна (предложение 2 § 1), что и доказывает наше утверждение.

Мы видим, что в терминологии § 1 целое число m, о котором идет речь в теореме 7, есть длина R.

Мы можем отождествить $R = \mathrm{End}_k(E)$ с кольцом матриц $\mathrm{Mat}_m(k)$, как только выбран базис E. В этом случае мы можем взять в качестве простых левых идеалов идеалы L_i $(i = 1, \ldots, m)$, состоящие из матриц с единственным ненулевым i-м столбцом. Элементы из L_1 выглядят, например, так:

$$\begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ a_{21} & 0 & \ldots & 0 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{m1} & 0 & \ldots & 0 \end{pmatrix}.$$

Мы видим, что R есть прямая сумма m столбцов.

Отметим также, что теорема 6 приводит к следующему утверждению: *если матрица $M \in \mathrm{Mat}_m(k)$ коммутирует со всеми элементами из $\mathrm{Mat}_m(k)$, то M — скалярная матрица.*

Действительно, такая матрица M может рассматриваться как R-эндоморфизм E, а мы в силу теоремы 6 знаем, что всякий такой эндоморфизм лежит в k. Разумеется, этот факт легко можно проверить также прямым вычислением.

§ 6. Сбалансированные модули

Пусть R — кольцо и E — модуль. Положим $R'(E) = \mathrm{End}_R(E)$ и $R''(E) = \mathrm{End}_{R'}(E)$. Пусть λ: $R \to R''$ — естественный гомоморфизм, при котором $\lambda_x(v) = xv$ для $x \in R$ и $v \in E$. Если λ — изоморфизм, то мы будем говорить, что модуль E — *сбалансированный*. Мы будем говорить, что модуль E — *образующий* (для R-модулей), если всякий модуль является гомоморфным образом (возможно, бесконечной)

прямой суммы модуля E с собой. Если E — образующий, то существует сюръективный гомоморфизм $E^{(n)} \to R$ (мы можем взять n конечным, так как R конечно порождено одним элементом 1).

Теорема 8 (Морита). *Всякий образующий E сбалансирован и конечно порожден над $R'(E)$.*

Доказательство (Фейт). Докажем сначала, что для любого модуля F модуль $R \oplus F$ сбалансирован. Отождествляем R и F в $R \oplus F$ с подмодулями $R \oplus 0$ и $0 \oplus F$ соответственно. Для $w \in F$ пусть ψ_w: $R \oplus F \to R \oplus F$ — отображение, при котором $\psi_w(x + v) = xw$. Тогда любой элемент $f \in R''(R \oplus F)$ коммутирует с π_1, π_2 и с каждым ψ_w. Отсюда мы тотчас заключаем, что $f(x + v) = f(1)(x + v)$ и что, следовательно, $R \oplus F$ — сбалансированный. Пусть E — образующий и $E^{(n)} \to R$ — сюръективный гомоморфизм. Так как R — свободный модуль, то $E^{(n)} \approx R \oplus F$ для некоторого модуля F, так что $E^{(n)}$ — сбалансированный. Пусть $g \in R''(E)$. Тогда $g^{(n)}$ коммутирует со всяким элементом $\varphi = (\varphi_{ij})$ из $R'(E^{(n)})$ (с компонентами $\varphi_{ij} \in R'(E)$) и, следовательно, существует некоторый $x \in R$, такой, что $g^{(n)} = \lambda_x^{(n)}$. Следовательно, $g = \lambda_x$, чем доказано, что E — сбалансированный, поскольку λ, очевидно, инъективно.

Чтобы доказать, что E конечно порожден над $R'(E)$, рассмотрим изоморфизмы аддитивных групп

$$R'(E)^{(n)} \approx \mathrm{Hom}_R(E^{(n)}, E) \approx \mathrm{Hom}_R(R, E) \oplus \mathrm{Hom}_R(F, E).$$

Они будут также, очевидно, изоморфизмами R'-модулей, если мы определим операцию из R' как композицию отображений (слева). Так как модуль $\mathrm{Hom}_R(R, E)$ R'-изоморфен E относительно отображения $h \mapsto h(1)$, то E является R'-гомоморфным образом модуля $R'^{(n)}$ и, следовательно, конечно порожден над R', что и доказывает теорему.

Пример. Пусть R — кольцо, не содержащее двусторонних идеалов, отличных от 0 и R. Если L — левый идеал $\neq 0$, то L — образующий, так как $LR = R$ и, следовательно, $R = \sum La_i$ для подходящих элементов $a_i \in R$. Таким образом, теорема 5 является следствием теоремы 8.

УПРАЖНЕНИЯ

1. (а) Назовем *радикалом* кольца R левый идеал N, являющийся пересечением всех максимальных левых идеалов в R. Показать, что $NE = 0$ для всякого простого R-модуля E. Показать, что N — двусторонний идеал. (б) Показать, что радикал кольца R/N равен 0.

2. Кольцо называется *артиновым*, если всякая убывающая последовательность левых идеалов $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \ldots$, где $\mathfrak{a}_i \neq \mathfrak{a}_{i+1}$, конечна. (а) Показать, что всякая конечномерная алгебра над полем артинова. (б) Показать,

что если кольцо R артиново, то всякий ненулевой левый идеал содержит простой левый идеал. (в) Показать, что в артиновом кольце R всякое непустое множество идеалов содержит минимальный идеал.

3. Пусть R — артиново кольцо, причем его радикал равен 0. Показать, что R полупросто. [*Указание*: получить вложение R в прямую сумму $\coprod R/M_i$, где $\{M_i\}$ — конечное множество максимальных левых идеалов.]

4. Пусть R — произвольное кольцо, M — конечно порожденный модуль и N — радикал в R. Показать, что если $NM = M$, то $M = 0$. [*Указание*: заметить, что сохраняет силу доказательство леммы Накаямы.]

5. Пусть R — артиново кольцо. Показать, что его радикал нильпотентен, т. е. что существует целое число $r \geqslant 1$, для которого $N^r = 0$. [*Указание*: рассмотреть убывающую последовательность степеней N^r и применить лемму Накаямы к надлежаще выбранному подмодулю в N^∞.]

6. Пусть R — полупростое коммутативное кольцо. Показать, что R — прямое произведение полей.

7. Пусть R — конечномерная коммутативная алгебра над полем k. Показать, что если R не содержит нильпотентных элементов $\neq 0$, то R — полупростая.

8. (К о л ч и н). Пусть $E \neq 0$ — конечномерное векторное пространство над полем k и G — подгруппа в $GL(E)$, такая, что всякий элемент $A \in G$ имеет вид $I + N$, где N — нильпотентный эндоморфизм. Показать, что существует элемент $v \in E$, $v \neq 0$, такой, что $Av = v$ для всех $A \in G$. [*Указание*: во-первых, свести вопрос к случаю, когда k алгебраически замкнуто, показав, что задача равносильна разрешимости некоторой системы линейных уравнений. Во-вторых, свести задачу к случаю, когда E — простой $k[G]$-модуль. Комбинируя теорему Бернсайда с тем фактом, что

$$\operatorname{tr}(A) = \operatorname{tr}(I) \quad \text{для всех} \quad A \in G,$$

показать, что если $A_0 \in G$, $A_0 = I + N$, то $\operatorname{tr}(NX) = 0$ для всех $X \in \operatorname{End}_k(E)$ и, следовательно, $N = 0$, $A_0 = I$.]

9. Пусть E — конечномерное векторное пространство над полем k, S — некоторое подмножество в $\operatorname{End}_k(E)$ и R — k-алгебра, порожденная элементами из S. Доказать, что следующие условия эквивалентны: алгебра R полупростая; E — полупростой R-модуль.

10. Пусть $A \in \operatorname{End}_k(E)$. Эндоморфизм A называется *полупростым*, если множество, состоящее из одного A, удовлетворяет условиям предыдущего упражнения. Показать, что элемент A из $\operatorname{End}_k(E)$ полупрост в том и только в том случае, если его минимальный многочлен не имеет множителей кратности > 1 над k.

11. Пусть E — конечномерное векторное пространство над полем k, S — коммутативное множество его эндоморфизмов и $R = k[S]$. Предположим, что алгебра R полупроста. Показать, что всякое подмножество из S полупросто.

12. Доказать, что R-модуль E тогда и только тогда является образующим, когда он сбалансирован и как модуль над R' конечно порожден и проективен.

Глава XVIII

Представления конечных групп

§ 1. Полупростота групповой алгебры

Пусть k — поле и G — группа. Образуем групповую алгебру $k[G]$. Как объяснялось в гл. V, § 1, она состоит из всех формальных линейных комбинаций

$$\sum_{\sigma \in G} a_\sigma \sigma$$

с коэффициентами $a_\sigma \in k$, почти все из которых равны 0. Произведение берется естественным образом:

$$\left(\sum_{\sigma \in G} a_\sigma \sigma\right)\left(\sum_{\tau \in G} b_\tau \tau\right) = \sum_{\sigma, \tau} a_\sigma b_\tau \sigma\tau.$$

Пусть E — векторное пространство над k. Всякий гомоморфизм алгебр

$$k[G] \to \mathrm{End}_k(E)$$

индуцирует гомоморфизм групп

$$G \to \mathrm{Aut}_k(E),$$

и таким образом, представление кольца $k[G]$ в E порождает представление группы G. Если задано такое представление, то мы будем также говорить, что $k[G]$ или G *действует* на E. Отметим, что задание представления превращает E в модуль над кольцом $k[G]$.

Обратно, если задано представление группы, скажем $\rho\colon G \to \mathrm{Aut}_k(E)$, то мы можем следующим образом продолжить ρ до представления алгебры $k[G]$. Пусть $\alpha = \sum a_\sigma \sigma$ и $x \in E$. Положим

$$\rho(\alpha)x = \sum a_\sigma \rho(\sigma) x.$$

Непосредственно проверяется, что этим определено продолжение ρ до кольцевого гомоморфизма $k[G]$ в $\mathrm{End}_k(E)$. Мы будем говорить, что представление ρ — *точное* на G, если отображение $\rho\colon G \to \mathrm{Aut}_k(E)$ инъективно. Продолжение ρ на $k[G]$ может, однако, и не быть точным.

Имея дело с фиксированным представлением группы G на E, мы часто будем писать σx вместо $\rho(\sigma)x$. Векторное пространство E

вместе с представлением ρ будет называться *G-модулем* или *G-пространством*, а также *(G, k)-пространством*, если нам захочется специально отметить поле k. Напомним, что если E, F — G-модули, то G-гомоморфизмом называется такое k-линейное отображение $f\colon E \to F$, что $f(\sigma x) = \sigma f(x)$ для всех $x \in E$ и $\sigma \in G$.

Отметим, что ядром заданного G-гомоморфизма $f\colon E \to F$ служит G-подмодуль в E и что k-факторпространство $F/f(E)$ допускает, и притом единственным образом, такое действие G, что каноническое отображение $F \to F/f(E)$ является G-гомоморфизмом.

Если G действует на k-пространствах E и F, то мы можем естественным образом определить действие G на $\mathrm{Hom}_k(E, F)$. Действительно, положим для $f \in \mathrm{Hom}_k(E, F)$ и $\sigma \in G$

$$(\sigma f)(x) = \sigma(f(\sigma^{-1}x)).$$

Тогда $(\sigma\tau)f = \sigma(\tau(f))$. Чтобы не произошло путаницы с композицией σ и f, мы, когда нам потребуется иметь дело с такой итерацией, будем писать $\sigma \circ f$ для обозначения отображения $x \mapsto \sigma(f(x))$ и аналогично $f \circ \sigma$. Отметим, что f является G-гомоморфизмом в том и только в том случае, если $\sigma f = f$ для всех $\sigma \in G$.

Пусть E — G-модуль. Мы будем обозначать через E^G подмодуль, состоящий из всех элементов $x \in E$, таких, что $\sigma x = x$ для всех $\sigma \in G$.

Под *тривиальным* представлением $\rho\colon G \to \mathrm{Aut}_k(E)$ мы будем понимать представление, при котором $\rho(G) = 1$. Представление тривиально тогда и только тогда, когда $\sigma x = x$ для всех $x \in E$ и всех $\sigma \in G$. В этом случае мы будем также говорить, что *G действует тривиально*. Это можно еще записать в виде $E = E^G$.

Пусть G — конечная группа и E — G-модуль. Мы можем определить операцию $\mathrm{Tr}_G\colon E \to E$, являющуюся k-гомоморфизмом, а именно положив

$$\mathrm{Tr}_G(x) = \sum_{\sigma \in G} \sigma x.$$

Отметим, что элементы $\mathrm{Tr}_G(x)$ лежат в E^G, т. е. неподвижны относительно действия всех элементов G. Действительно,

$$\tau\,\mathrm{Tr}_G(x) = \sum_{\sigma \in G} \tau\sigma x,$$

а умножение слева на τ лишь переставляет элементы из G.

Если, в частности, $f\colon E \to F$ — k-гомоморфизм G-модулей, то $\mathrm{Tr}_G(f)\colon E \to F$ является G-гомоморфизмом.

Предложение 1. *Пусть G — конечная группа, E', E, F, F' — G-модули и*

$$E' \xrightarrow{\varphi} E \xrightarrow{f} F \xrightarrow{\psi} F'$$

— k-гомоморфизмы, причем φ, ψ — G-гомоморфизмы. Тогда

$$\mathrm{Tr}_G(\psi \circ f \circ \varphi) = \psi \circ \mathrm{Tr}_G(f) \circ \varphi.$$

Доказательство. Имеем

$$\mathrm{Tr}_G(\psi \circ f \circ \varphi) = \sum_{\sigma \in G} \sigma(\psi \circ f \circ \varphi) = \sum_{\sigma \in G} (\sigma\psi) \circ (\sigma f) \circ (\sigma\varphi) =$$
$$= \psi \circ \left(\sum_{\sigma \in G} \sigma f\right) \circ \varphi = \psi \circ \mathrm{Tr}_G(f) \circ \varphi.$$

Теорема 1 (Машке). *Пусть G — конечная группа порядка n и k — поле, характеристика которого не делит n. Тогда групповое кольцо $k[G]$ полупросто.*

Доказательство. Пусть E — G-модуль и F — G-подмодуль. Так как k — поле, то существует k-подпространство F', такое, что E будет k-прямой суммой F и F'. Проекция на F есть k-линейное отображение $\pi\colon E \to F$. Очевидно, $\pi(x) = x$ для всех $x \in F$. Положим

$$\varphi = \frac{1}{n} \mathrm{Tr}_G(\pi).$$

Имеем два G-гомоморфизма

$$0 \to F \underset{\varphi}{\overset{j}{\rightleftarrows}} E,$$

причем j — вложение и $\varphi \circ j = \mathrm{id}$. Отсюда вытекает, что E есть G-прямая сумма F и $\mathrm{Ker}\,\varphi$, чем и доказано, что $k[G]$ полупросто.

Во всем последующем мы будем предполагать, что G — конечная группа и что все векторные пространства E над k конечномерны. Через n мы обычно обозначаем порядок группы G. Всюду предполагается, что характеристика поля k не делит n.

§ 2. Характеры

Пусть $\rho\colon k[G] \to \mathrm{End}_k(E)$ — некоторое представление. Под *характером* χ_ρ этого представления мы будем понимать k-значную функцию

$$\chi_\rho\colon k[G] \to k,$$

такую, что $\chi_\rho(\alpha) = \mathrm{tr}\,\rho(\alpha)$ для всех $\alpha \in k[G]$. След здесь — это след эндоморфизма, определенный в гл. XIII, § 2. При выбранном базисе для E над k он равен следу матрицы, представляющей $\rho(\alpha)$, т. е. сумме ее диагональных элементов. Как мы уже видели раньше, след не зависит от выбора базиса. Иногда мы вместо χ_ρ будем писать χ_E.

Мы будем также называть E *пространством представления* ρ.

Под *тривиальным* (или *единичным*) *характером* мы будем понимать характер представления группы G на k-пространстве, равном самому k, при котором $\sigma x = x$ для всех $x \in k$. Это функция, принимающая значение 1 на всех элементах из G. Мы будем обозначать ее через χ_0, а также через 1_G, если нам нужно будет подчеркнуть зависимость от G.

Отметим, что характеры являются функциями на G и что значения характера на элементах из $k[G]$ определяются его значениями на G (продолжение с G на $k[G]$ производится по k-линейности).

Мы будем говорить, что два представления ρ, φ группы G на пространствах E, F *изоморфны*, если между E и F существует G-изоморфизм. Очевидно, что если ρ, φ — изоморфные представления, то их характеры равны. (Иными словами, если E, F суть G-изоморфные G-пространства, то $\chi_E = \chi_F$.) Во всем дальнейшем мы будем интересоваться только классами представлений относительно изоморфизма.

Если E, F — G-пространства, то их прямая сумма $E \oplus F$ также является G-пространством с покомпонентным действием G. Если $x \oplus y \in E \oplus F$, где $x \in E$ и $y \in F$, то $\sigma(x \oplus y) = \sigma x \oplus \sigma y$.

Аналогично тензорное произведения $E \otimes_k F = E \otimes F$ есть G-пространство с действием G, задаваемым формулой $\sigma(x \otimes y) = \sigma x \otimes \sigma y$.

Предложение 2. *Для любых G-пространств E, F*

$$\chi_E + \chi_F = \chi_{E \oplus F} \quad \text{и} \quad \chi_E \chi_F = \chi_{E \otimes F}.$$

Доказательство. Первое соотношение выполняется ввиду того, что матрица элемента σ в представлении $E \oplus F$ разлагается на блоки, соответствующие представлению в E и представлению в F. Что касается второго соотношения, то, как мы знаем $\{v_i \otimes w_j\}$ — базис $E \otimes F$, где $\{v_i\}$ — базис E и $\{w_j\}$ — базис F над k. Пусть $(a_{\nu i})$ — матрица элемента σ относительно базиса пространства E и $(b_{\mu j})$ — его матрица относительно базиса пространства F. Тогда

$$\sigma(v_i \otimes w_j) = \sigma v_i \otimes \sigma w_j = \sum_{\nu} a_{\nu i} v_\nu \otimes \sum_{\mu} b_{\mu j} w_\mu =$$

$$= \sum_{\nu, \mu} a_{\nu i} b_{\mu j} v_\nu \otimes w_\mu.$$

По определению

$$\chi_{E \otimes F}(\sigma) = \sum_i \sum_j a_{ii} b_{jj} = \chi_E(\sigma) \chi_F(\sigma),$$

что и доказывает наше предложение.

Пусть $\rho\colon G \to \mathrm{Aut}_k(E)$ и $\varphi\colon G \to \mathrm{Aut}_k(F)$ — представления G на E и F соответственно. Мы определяем сумму $\rho + \varphi$ как описанное выше представление на $E \oplus F$. Очевидно, что сумма характеров есть

характер суммы представлений. В частности, характеры G, ассоциированные с представлениями G на k-пространствах, образуют моноид.

Аналогично мы определяем произведение $\rho \otimes \varphi$ как представление, ассоциированное с тензорным произведением пространств представления для ρ и φ соответственно. Таким образом, аддитивный моноид характеров, ассоциированных с представлениями, обладает мультипликативной структурой, которая дистрибутивна по отношению к сложению.

До сих пор у нас фигурировало понятие характера, ассоциированного с представлением. Естественно теперь рассматривать линейные комбинации таких характеров не только с положительными целочисленными коэффициентами. Таким образом, под (*обобщенным*) *характером* группы G мы будем понимать всякую функцию на G, которая может быть записана в виде линейной комбинации характеров представлений с произвольными целочисленными коэффициентами. Характеры, ассоциированные с представлениями, будут называться *собственными характерами*. Все, что мы определили, зависит, конечно, от поля k, и если нам будет нужно специально отметить поле k, мы будем к нашим высказываниям добавлять „*над* k“.

Заметим, что, согласно предложению 2, характеры образуют кольцо. В дальнейшем мы будем использовать преимущественно аддитивную, а не мультипликативную структуру.

Под *простым* (или *неприводимым*) *характером* группы G понимают характер простого представления (т. е. характер, ассоциированный с простым $k[G]$-модулем).

Принимая во внимание теорему 1 и результаты предыдущей главы, касающиеся структуры простых и полупростых модулей над полупростым кольцом (гл. XVII, § 4), получаем следующее утверждение.

Теорема 2. *Существует лишь конечное число простых характеров группы G (над k). Характеры представлений G являются линейными комбинациями простых характеров с целочисленными коэффициентами* $\geqslant 0$.

Мы будем использовать разложение полупростого кольца в прямое произведение

$$k[G] = \prod_{i=1}^{s} R_i,$$

где каждое R_i — простое кольцо. Мы имеем также соответствующее разложение единичного элемента из $k[G]$

$$1 = e_1 + \ldots + e_s.$$

где e_i — единичный элемент из R_i и $e_i e_j = 0$ при $i \neq j$. Точно так же $R_i R_j = 0$ при $i \neq j$. *Отметим, что* $s = s(k)$ *зависит от* k.

Если L_i — какой-нибудь типический простой модуль для R_i (скажем, один из простых левых идеалов), то мы обозначаем через χ_i характер представления на L_i.

Заметим, что $\chi_i(a) = 0$ *для всех* $a \in R_j$ *при* $i \neq j$. *Это фундаментальное соотношение ортогональности, и, хотя оно и очевидно, из него будут следовать все наши другие соотношения.*

Теорема 3. *Предположим, что* k *имеет характеристику* 0. *Тогда всякий собственный характер имеет единственное представление в виде линейной комбинации*

$$\chi = \sum_{i=1}^{s} n_i \chi_i, \quad n_i \in \mathbf{Z}, \ n_i \geqslant 0,$$

где $\chi_1, \ldots, \chi_s$ — *простые характеры* G *над* k. *Два представления изоморфны в том и только в том случае, если ассоциированные с ними характеры равны.*

Доказательство. Пусть E — пространство представления характера χ. Тогда в силу теоремы 3 из гл. XVII, § 4,

$$E \approx \coprod_{i=1}^{s} n_i L_i.$$

Сумма конечная, поскольку мы неизменно предполагаем, что E конечномерно. Так как e_i действует на L_i как единичный элемент, то

$$\chi_i(e_i) = \dim_k L_i.$$

Мы уже видели, что $\chi_i(e_j) = 0$, если $i \neq j$. Следовательно,

$$\chi(e_i) = n_i \dim_k L_i.$$

Так как $\dim_k L_i$ зависит только от структуры групповой алгебры, то мы получили способ находить значения кратностей n_i. А именно, n_i — число раз, с которым L_i входит (с точностью до изоморфизма) в пространство представления характера χ, — равно значению $\chi(e_i)$, разделенному на $\dim_k L_i$ (мы находимся в характеристике 0). Это доказывает нашу теорему.

Мы называем числа n_i, участвующие в теореме 3, *кратностями* χ_i в χ.

В обоих следствиях мы продолжаем предполагать, что k имеет характеристику 0.

Следствие 1. *Простые характеры*

$$\chi_1, \ldots, \chi_s$$

как функции на G *со значениями в* k *линейно независимы над* k.

Доказательство. Предположим, что $\sum a_i\chi_i = 0$, где $a_i \in k$. Применив это выражение к e_j, получим

$$0 = \left(\sum a_i\chi_i\right)(e_j) = a_j \dim_k L_j.$$

Следовательно, $a_j = 0$ для всех j.

В случае характеристики 0 мы называем *размерностью* собственного характера размерность ассоциированного пространства представления.

Следствие 2. *Функция* dim *есть гомоморфизм моноида собственных характеров в* $\mathbf{Z}$.

Пример. Пусть G — циклическая группа с образующей σ, порядок которой равен простому числу p. Рассмотрим групповую алгебру $\mathbf{Q}[G]$. Пусть

$$e_1 = \frac{1 + \sigma + \sigma^2 + \ldots + \sigma^{p-1}}{p}, \quad e_2 = 1 - e_1.$$

Тогда $\tau e_1 = e_1$ для любого $\tau \in G$ и, следовательно, $e_1^2 = e_1$ — идемпотентный элемент. Отсюда вытекает, что $e_2^2 = e_2$ и $e_1 e_2 = 0$. Поле $\mathbf{Q}e_1$ изоморфно $\mathbf{Q}$. Пусть $\omega = \sigma e_2$. Тогда $\omega^p = e_2$. Положим $\mathbf{Q}_2 = \mathbf{Q}e_2$. Так как элемент $\omega \neq e_2$ и удовлетворяет неприводимому уравнению

$$X^{p-1} + \ldots + 1 = 0$$

над $\mathbf{Q}_2$, то $\mathbf{Q}_2(\omega)$ изоморфно полю, полученному присоединением к полю рациональных чисел примитивного корня p-й степени из единицы. Следовательно, $\mathbf{Q}[G]$ обладает разложением в прямое произведение

$$\mathbf{Q}[G] \approx \mathbf{Q} \times \mathbf{Q}(\zeta),$$

где ζ — примитивный корень p-й степени из единицы.

В качестве другого примера рассмотрим любую конечную группу G. Пусть

$$e_1 = \frac{1}{n} \sum_{\sigma \in G} \sigma.$$

Тогда для любого $\tau \in G$ имеем $\tau e_1 = e_1$ и $e_1^2 = e_1$. Если мы положим $e_1' = 1 - e_1$, то $e_1'^2 = e_1'$ и $e_1' e_1 = e_1 e_1' = 0$. Таким образом, мы получаем, что для любого поля k (характеристика которого, согласно принятым соглашениям, не делит порядок $(G : 1)$)

$$k[G] = ke_1 \times k[G]\, e_1'$$

является разложением в прямое произведение. В частности, представление G на самой групповой алгебре $k[G]$ содержит одномерное представление на компоненте ke_1 с тривиальным характером.

§ 3. *Одномерные представления*

Допуская вольность речи, мы будем даже в случае характеристики $p > 0$ говорить, что *характер одномерен*, если он является гомоморфизмом $G \to k^*$.

Предположим, что E — одномерное векторное пространство над k. Пусть

$$\rho\colon G \to \mathrm{Aut}_k(E)$$

— представление и $\{v\}$ — базис E над k. Тогда для всякого $\sigma \in G$ имеем

$$\sigma v = \chi(\sigma)\, v,$$

где $\chi(\sigma) \in k$ — некоторый элемент, причем $\chi(\sigma) \neq 0$, так как σ индуцирует автоморфизм пространства E. Очевидно,

$$\tau\sigma v = \chi(\sigma)\,\tau v = \chi(\sigma)\,\chi(\tau)\, v = \chi(\tau\sigma)\, v$$

для любых σ, $\tau \in G$. Мы видим, что $\chi\colon G \to k^*$ — гомоморфизм и что наш одномерный характер является объектом той же природы, что и характеры, которые встречались в теореме Артина в теории Галуа.

Обратно, пусть $\chi\colon G \to k^*$ — гомоморфизм и E — одномерное k-пространство с базисом $\{v\}$. Положим $\sigma(av) = a\chi(\sigma)\, v$ для всех $a \in k$. Тогда видно, что это действие G на E определяет представление группы G, ассоциированным характером которого будет χ.

Так как группа G конечна, то

$$\chi(\sigma)^n = \chi(\sigma^n) = \chi(1) = 1.$$

Следовательно, значениями одномерных характеров являются корни n-й степени из единицы. Все одномерные характеры образуют группу по умножению. Для случая, когда G — конечная абелева группа, мы уже определили ее группу одномерных характеров в гл. I, § 11.

Теорема 4. *Пусть G — конечная абелева группа. Предположим, что поле k алгебраически замкнуто. Тогда всякое простое представление группы G одномерно. Простые характеры G являются гомоморфизмами G в k^*.*

Доказательство. Групповое кольцо $k[G]$ полупросто, коммутативно и является прямым произведением простых колец. Всякое простое кольцо есть кольцо матриц над k (в силу теоремы 5 § 5 предыдущей главы) и может быть коммутативным в том и только в том случае, если оно равно k.

Для всякого одномерного характера χ группы G имеем

$$\chi(\sigma)^{-1} = \chi(\sigma^{-1}).$$

Если k — поле комплексных чисел, то

$$\overline{\chi(\sigma)} = \chi(\sigma)^{-1} = \chi(\sigma^{-1}).$$

Следствие. *Пусть k — алгебраически замкнутое поле, G — конечная группа. Для любого характера χ и любого $\sigma \in G$ значение $\chi(\sigma)$ равно сумме корней из единицы с целочисленными коэффициентами (т. е. с коэффициентами из $\mathbf{Z}$ или $\mathbf{Z}/p\mathbf{Z}$ в зависимости от характеристики k).*

Доказательство. Пусть H — циклическая подгруппа, порожденная σ. Представление G, имеющее характер χ, можно, беря ограничение, рассматривать как представление для H. Таким образом, наше утверждение вытекает из теоремы 4.

§ 4. Пространство функций классов

Пусть k — некоторое поле, Под *функцией классов* на G (над k или со значениями в k) мы будем понимать функцию $f: G \to k$, такую, что $f(\sigma\tau\sigma^{-1}) = f(\tau)$ для всех σ, $\tau \in G$. Таким образом, функция классов может рассматриваться как функция на классах сопряженных элементов. Ясно, что характеры — это функции классов, так как для квадратных матриц

$$\operatorname{tr}(MM'M^{-1}) = \operatorname{tr}(M').$$

Мы всегда будем по линейности расширять область определения функции классов до группового кольца. Если

$$\alpha = \sum_{\sigma \in G} a_\sigma \sigma$$

и f — функция классов, то полагаем

$$f(\alpha) = \sum_{\sigma \in G} a_\sigma f(\sigma).$$

Пусть $\sigma_0 \in G$. Мы пишем $\sigma \sim \sigma_0$, если элемент $\sigma \in G$ сопряжен с σ_0, т. е. если существует элемент τ, для которого $\sigma_0 = \tau\sigma\tau^{-1}$. Элемент группового кольца, имеющий вид

$$\gamma = \sum_{\sigma \sim \sigma_0} \sigma,$$

будет также называться *классом сопряженных элементов.*

Предложение 3. *Пусть k — произвольное поле. Элемент из $k[G]$ тогда и только тогда коммутирует со всяким элементом из G, когда он является линейной комбинацией классов сопряженных элементов.*

Доказательство. Пусть $\alpha = \sum_{\sigma \in G} a_\sigma \sigma$, причем $\alpha\tau = \tau\alpha$ для всех $\tau \in G$. Тогда

$$\sum_{\sigma \in G} a_\sigma \tau\sigma\tau^{-1} = \sum_{\sigma \in G} a_\sigma \sigma.$$

Следовательно, $a_{\sigma_0} = a_\sigma$ для всякого σ, сопряженного с σ_0, а это и означает, что мы можем записать

$$\alpha = \sum_\gamma a_\gamma \gamma,$$

где сумма берется по всем классам сопряженных элементов γ.

Замечание. Отметим, что классы сопряженных элементов на самом деле образуют базис центра группового кольца $\mathbf{Z}[G]$ над $\mathbf{Z}$ и вследствие этого играют универсальную роль в теории представлений.

Отметим также, что классы сопряженных элементов линейно независимы над k и образуют базис для центра алгебры $k[G]$ над k.

Будем отныне предполагать, что k алгебраически замкнуто. Тогда

$$k[G] = \prod_{i=1}^{s} R_i$$

— прямое произведение простых колец и каждое R_i есть алгебра матриц над k. Центром прямого произведения, очевидно, будет произведение центров сомножителей. Обозначим через k_i образ k в R_i, другими словами,

$$k_i = ke_i,$$

где e_i — единичный элемент в R_i. Тогда центр алгебры $k[G]$ равен также пространству

$$\prod_{i=1}^{s} k_i,$$

которое s-мерно над k.

Пусть L_i — типический простой левый идеал в R_i. Тогда

$$R_i \approx \mathrm{End}_k(L_i).$$

Положим

$$d_i = \dim_k L_i.$$

Тогда

$$\boxed{d_i^2 = \dim_k R_i \quad \text{и} \quad \sum_{i=1}^{s} d_i^2 = n}.$$

Имеем также разложение R_i как (G, k)-пространства в прямую сумму

$$R_i \approx L_i^{(d_i)}.$$

Введенные выше обозначения будут далее оставаться фиксированными.

Мы можем суммировать некоторые из наших результатов следующим образом.

Предложение 4. *Пусть поле k алгебраически замкнуто. Тогда число классов сопряженных элементов группы G равно числу ее простых характеров и оба эти числа равны размерности s центра групповой алгебры $k[G]$. Классы сопряженных элементов $\gamma_1, \ldots, \gamma_s$ и идемпотентные элементы $e_1, \ldots, e_s$ образуют базисы центра $k[G]$.*

Число элементов в γ_i будет обозначаться через h_i, а в любом классе сопряженных элементов γ — через h_γ. Мы называем это число *порядком класса*. Центр групповой алгебры будет обозначаться через $Z_k(G)$.

Мы можем рассматривать $k[G]$ как G-модуль. Его характер будет называться *регулярным характером*; мы будем обозначать его через χ_{reg} или, если нужно подчеркнуть зависимость от G, через r_G. Представление на $k[G]$ называется *регулярным представлением*. Из нашего разложения $k[G]$ в прямую сумму получаем

$$\boxed{\chi_{\text{reg}} = \sum_{i=1}^{s} d_i \chi_i}.$$

Вычислим значения регулярного характера.

Предложение 5. *Пусть χ_{reg} — регулярный характер. Тогда*

$$\chi_{\text{reg}}(\sigma) = 0, \quad \text{если} \quad \sigma \in G, \quad \sigma \neq 1,$$

$$\chi_{\text{reg}}(1) = n.$$

Доказательство. Пусть $1 = \sigma_1, \ldots, \sigma_n$ — элементы группы G. Они образуют базис $k[G]$ над k. Матрица элемента 1 есть единичная матрица размера $n \times n$. Отсюда вытекает наше второе утверждение. Если $\sigma \neq 1$, то умножение на σ переставляет $\sigma_1, \ldots, \sigma_n$, и непосредственно ясно, что все диагональные элементы в матрице, представляющей σ, равны 0. Это доказывает все, что нам нужно.

Отметим, что мы имеем два естественных базиса для центра $Z_k(G)$ групповой алгебры. Во-первых, классы сопряженных элементов группы G. Во-вторых, элементы $e_1, \ldots, e_s$ (т. е. идемпотентные элементы колец R_i). Мы хотим найти соотношения между ними, т. е., другими словами, хотим найти коэффициенты в выражении e_i через элементы группы. В следующем параграфе значения этих коэффициентов будут интерпретированы как скалярные произведения. Это объяснит их таинственный вид.

Предложение 6. *Мы снова предполагаем, что поле k алгебраически замкнуто. Пусть*

$$e_i = \sum_{\tau \in G} a_\tau \tau, \quad a_\tau \in k.$$

Тогда

$$a_\tau = \frac{1}{n} \chi_{\text{reg}}(e_i \tau^{-1}) = \frac{d_i}{n} \chi_i(\tau^{-1}).$$

Доказательство. Для всех $\tau \in G$ имеем

$$\chi_{\text{reg}}(e_i \tau^{-1}) = \chi_{\text{reg}}\left(\sum_{\sigma \in G} a_\sigma \sigma \tau^{-1}\right) = \sum_{\sigma \in G} a_\sigma \chi_{\text{reg}}(\sigma \tau^{-1}).$$

В силу предложения 5

$$\chi_{\text{reg}}(e_i \tau^{-1}) = n a_\tau.$$

С другой стороны,

$$\chi_{\text{reg}}(e_i \tau^{-1}) = \sum_{j=1}^{s} d_j \chi_j(e_i \tau^{-1}) = d_i \chi_i(e_i \tau^{-1}) = d_i \chi_i(\tau^{-1}).$$

Следовательно,

$$d_i \chi_i(\tau^{-1}) = n a_\tau$$

для всех $\tau \in G$. Это доказывает наше предложение.

Следствие 1. *Каждый элемент e_i может быть выражен через элементы группы с коэффициентами, которые лежат в поле, порожденном над простым полем корнями m-й степени из единицы, где m — показатель группы G.*

Следствие 2. *Размерности d_i не делятся на характеристику поля k.*

Доказательство. Иначе было бы $e_i = 0$, что невозможно.

Следствие 3. *Простые характеры $\chi_1, \ldots, \chi_s$ линейно независимы над k.*

Доказательство. Можно применить доказательство следствия 1 теоремы 3, поскольку мы теперь знаем, что характеристика не делит d_i.

Следствие 4. *Предположим дополнительно, что k имеет характеристику 0. Тогда $d_i \mid n$ для всякого i.*

Доказательство. Умножая наше выражение для e_i на n/d_i, а также на e_i, получим

$$\frac{n}{d_i} e_i = \sum_{\sigma \in G} \chi_i(\sigma^{-1}) \sigma e_i.$$

Пусть ζ — примитивный корень m-й степени из единицы и M — модуль над $\mathbf{Z}$, порожденный конечным числом элементов $\zeta^{\nu}\sigma e_i$ ($\nu = 0, \ldots, m-1$ и $\sigma \in G$). Тогда из предыдущего соотношения тотчас видно, что умножение на n/d_i отображает M в себя. В силу определения целых элементов заключаем, что n/d_i — целый элемент над $\mathbf{Z}$ и, следовательно, лежит в $\mathbf{Z}$, что и требовалось.

Теорема 5. *Пусть поле k алгебраически замкнуто. Пусть $Z_k(G)$ — центр алгебры $k[G]$ и $X_k(G)$ — k-пространство функций классов на G. Тогда пространства $Z_k(G)$ и $X_k(G)$ дуальны друг другу относительно спаривания*

$$(f, \alpha) \longmapsto f(\alpha).$$

Простые характеры и идемпотентные элементы $e_1, \ldots, e_s$ образуют ортогональные друг другу базисы. При этом

$$\chi_i(e_j) = \delta_{ij} d_i.$$

Доказательство. Формула уже была получена в ходе доказательства теоремы 3. Оба пространства, о которых идет речь, имеют размерность s и $d_i \neq 0$. Наше предложение теперь очевидно.

§ 5. Соотношения ортогональности

В этом параграфе мы будем предполагать, что поле k алгебраически замкнуто.

Пусть R — подкольцо в k. Мы обозначаем через $X_R(G)$ R-подмодуль, порожденный над R характерами группы G. Это, таким образом, модуль функций, являющихся линейными комбинациями простых характеров с коэффициентами в R. Если R — простое кольцо (т. е. кольцо целых чисел $\mathbf{Z}$ или кольцо целых чисел $\bmod p$, когда k имеет характеристику p), то мы пишем вместо $X_R(G)$ просто $X(G)$.

Определим теперь некоторое билинейное отображение на $X(G) \times X(G)$. Для $f, g \in X(G)$ положим

$$\langle f, g \rangle = \frac{1}{n} \sum_{\sigma \in G} f(\sigma) g(\sigma^{-1}).$$

Теорема 6. *Выражение $\langle f, g \rangle$ для $f, g \in X(G)$ принимает значения в простом кольце. Простые характеры образуют ортонормальный базис для $X(G)$, другими словами,*

$$\langle \chi_i, \chi_j \rangle = \delta_{ij}.$$

Для всякого кольца $R \subset k$ это выражение имеет единственное продолжение до R-билинейной формы $X_R(G) \times X_R(G) \to R$, задаваемой той же самой формулой, что и выше.

Доказательство. В силу предложения 6

$$\chi_j(e_i) = \frac{d_i}{n} \sum_{\sigma \in G} \chi_i(\sigma^{-1}) \chi_j(\sigma).$$

Если $i \neq j$, то получаем слева 0, так что χ_i и χ_j ортогональны. Если $i = j$, то получаем слева d_i, а, как мы знаем из следствия 2 предложения 6, $d_i \neq 0$ в k. Следовательно, $\langle \chi_i, \chi_i \rangle = 1$. Так как всякий элемент из $X(G)$ есть линейная комбинация простых характеров с целочисленными коэффициентами, то значения нашего билинейного отображения лежат в простом кольце. Утверждение о продолжении очевидно, и тем самым наша теорема доказана.

Предположим, что k имеет характеристику 0. Пусть m — показатель группы G, и пусть R содержит корни m-й степени из единицы. Если R обладает автоморфизмом порядка 2, таким, что его действие на корни из единицы есть $\zeta \mapsto \zeta^{-1}$, то мы будем называть такой автоморфизм *сопряжением* и обозначать его через $a \mapsto \bar{a}$.

Теорема 7. *Пусть k имеет характеристику 0 и пусть R — подкольцо, содержащее корни m-й степени из единицы и обладающее сопряжением. Тогда определенная выше билинейная форма на $X(G)$ имеет единственное продолжение до эрмитовой формы*

$$X_R(G) \times X_R(G) \to R,$$

задаваемой формулой

$$\langle f, g \rangle = \frac{1}{n} \sum_{\sigma \in G} f(\sigma) \overline{g(\sigma)}.$$

Простые характеры образуют ортонормальный базис для $X_R(G)$ относительно этой формы.

Доказательство. В случае когда f, g лежат в $X(G)$, указанная в формулировке теоремы формула дает для выражения $\langle f, g \rangle$ то же самое значение, что и раньше. Таким образом, продолжение существует, и, очевидно, единственное.

Возвратимся к случаю, когда k имеет произвольную характеристику, взаимно простую с n.

Пусть $Z(G)$ обозначает аддитивную группу, порожденную классами сопряженных элементов $\gamma_1, \ldots, \gamma_s$ над простым кольцом. Она имеет размерность s. Определим билинейное отображение на $Z(G) \times Z(G)$. Если элемент $\alpha = \sum a_\sigma \sigma$ имеет коэффициенты в простом кольце, то мы обозначаем через α^- элемент $\sum a_\sigma \sigma^{-1}$.

Предложение 7. *Для* $\alpha, \beta \in Z(G)$ *можно определить выражение* $\langle \alpha, \beta \rangle$ *с помощью любого из следующих двух равных между собой выражений*:

$$\langle \alpha, \beta \rangle = \frac{1}{n} \chi_{\text{reg}}(\alpha\beta^-) = \frac{1}{n} \sum_{\nu=1}^{s} \chi_\nu(\alpha)\chi_\nu(\beta^-).$$

Значения этого выражения лежат в простом кольце.

Доказательство. Каждое из этих двух выражений линейно по обоим своим аргументам. Следовательно, чтобы доказать их равенство, достаточно доказать, что они совпадут, если мы заменим α на e_i и β — на элемент τ из G. Но тогда наше равенство, рассматриваемое уже над $Z_k(G) \times k[G]$, эквивалентно соотношению

$$\chi_{\text{reg}}(e_i\tau^{-1}) = \sum_{\nu=1}^{s} \chi_\nu(e_i)\chi_\nu(\tau^{-1}).$$

Так как $\chi_\nu(e_i) = 0$, за исключением $\nu = i$, то мы видим, что правая часть равна $d_i\chi_i(\tau^{-1})$. Таким образом, два наших выражения равны в силу предложения 6. Тот факт, что их значения лежат в простом кольце, вытекает из предложения 5: значения регулярного характера на элементах группы равны 0 или n и, следовательно, в случае характеристики 0 являются целыми числами, делящимися на n.

Как и в случае $X_R(G)$, мы будем использовать символ $Z_R(G)$ для обозначения R-модуля, порожденного $\gamma_1, \ldots, \gamma_s$ над произвольным подкольцом R в k.

Лемма. *Для всякого кольца* R, *содержащегося в* k, *спаривание из предложения 7 имеет единственное продолжение до отображения*

$$Z_R(G) \times Z(G) \to R,$$

которое R*-линейно по своему первому аргументу. Если* R *содержит корни* m*-й степени из единицы, где* m *есть показатель для* G, *а также содержит* $1/n$, *то* $e_i \in Z_R(G)$ *для всех* i. *Порядки классов* h_i *не делятся на характеристику поля* k, *и*

$$e_i = \sum_{\nu=1}^{s} \langle e_i, \gamma_\nu \rangle \frac{1}{h_\nu} \gamma_\nu.$$

Доказательство. Заметим, что h_i не делится на характеристику, будучи индексом некоторой подгруппы в G (группы изотропии любого элемента из γ_i, причем G действует посредством сопряжения), и, следовательно, h_i делит n. Продолжение нашего спаривания очевидно, поскольку $\gamma_1, \ldots, \gamma_s$ образуют базис для $Z(G)$ над простым

кольцом. Выражение e_i через этот базис есть только переформулировка предложения 6 в терминах рассматриваемого спаривания.

Пусть E — свободный модуль над подкольцом R поля k. Предположим, что у нас имеется симметрическая (или эрмитова) форма $\langle u, v\rangle$ на E. Пусть $\{v_1, \ldots, v_s\}$ — ортогональный базис для этого модуля. Если

$$v = a_1 v_1 + \ldots + a_s v_s,$$

где $a_i \in R$, то мы будем называть $a_1, \ldots, a_s$ *коэффициентами Фурье* элемента v относительно этого базиса. Через значения формы эти коэффициенты выражаются формулами

$$a_i = \frac{\langle v, v_i\rangle}{\langle v_i, v_i\rangle}$$

при условии, что $\langle v_i, v_i\rangle \neq 0$.

В следующей теореме мы покажем, что выражение для e_i через $\gamma_1, \ldots, \gamma_s$ является разложением Фурье.

Теорема 8. *Классы сопряженных элементов* $\gamma_1, \ldots, \gamma_s$ *образуют ортогональный базис для* $Z(G)$. *Имеет место соотношение* $\langle \gamma_i, \gamma_i\rangle = h_i$. *Для всякого кольца* R, *содержащегося в* k, *билинейное отображение из предложения 7 имеет единственное продолжение до* R*-билинейного отображения*

$$Z_R(G) \times Z_R(G) \to R.$$

Доказательство. Применим лемму. В силу линейности формула в лемме останется справедливой, если мы заменим R на k, а e_i — на любой элемент из $Z_k(G)$, в частности, если мы заменим e_i на γ_i. Но $\gamma_1, \ldots, \gamma_s$ — базис $Z_k(G)$ над k. Следовательно, $\langle \gamma_i, \gamma_i\rangle = h_i$ и $\langle \gamma_i, \gamma_j\rangle = 0$ при $i \neq j$, что и требовалось показать.

Следствие. *Пусть группа* G *коммутативна. Тогда*

$$\frac{1}{n}\sum_{\nu=1}^{n} \chi_\nu(\sigma)\,\chi_\nu(\tau^{-1}) = \begin{cases} 0, & \text{если } \sigma \neq \tau, \\ 1, & \text{если } \sigma = \tau. \end{cases}$$

Доказательство. Когда G коммутативна, всякий класс сопряженных элементов содержит точно один элемент и число простых характеров равно порядку группы.

Рассмотрим теперь для $Z(G)$ случай характеристики 0, так же как мы это делали для $X(G)$. Пусть k имеет характеристику 0 и R — подкольцо в k, содержащее корни m-й степени из единицы и обладающее сопряжением. Пусть $\alpha \in Z_R(G)$, $\alpha = \sum_{\sigma \in G} a_\sigma \sigma$, где $a_\sigma \in R$. Положим

$$\bar{\alpha} = \sum_{\sigma \in G} \bar{a}_\sigma \sigma^{-1}.$$

Теорема 9. *Пусть k имеет характеристику 0, и пусть R — подкольцо в k, содержащее корни m-й степени из единицы и обладающее сопряжением. Тогда спаривание из предложения 7 обладает единственным продолжением до эрмитовой формы*

$$Z_R(G) \times Z_R(G) \to R,$$

задаваемой формулами

$$\langle \alpha, \beta \rangle = \frac{1}{n} \chi_{\text{reg}}(\alpha\bar{\beta}) = \frac{1}{n} \sum_{\nu=1}^{s} \chi_\nu(\alpha)\,\overline{\chi_\nu(\beta)}.$$

Классы сопряженных элементов $\gamma_1, \ldots, \gamma_s$ образуют ортогональный базис для $Z_R(G)$. Если R содержит $1/n$, то $e_1, \ldots, e_s$ лежат в R и также образуют ортогональный базис для $Z_R(G)$. При этом $\langle e_i, e_i \rangle = d_i^2/n$.

Доказательство. В случае когда α, β лежат в $Z(G)$, формула, приведенная в формулировке теоремы, дает те же самые значения, что и выражение $\langle \alpha, \beta \rangle$ из предложения 7. Таким образом, продолжение существует и, очевидно, единственное. Используя вторую формулу, определяющую скалярное произведение, и вспоминая, что $\chi_\nu(e_i) = 0$ при $\nu \neq i$, мы видим, что $\langle e_i, e_j \rangle = 0$ при $i \neq j$ и

$$\langle e_i, e_i \rangle = \frac{1}{n} \chi_i(e_i)\,\overline{\chi_i(e_i)},$$

откуда и вытекает наше утверждение.

Отметим, что коэффициенты Фурье для e_i относительно базиса $\gamma_1, \ldots, \gamma_s$ одни и те же как по отношению к билинейной форме из теоремы 8, так и по отношению к эрмитовой форме из теоремы 9. Это следует из того факта, что $\gamma_1, \ldots, \gamma_s$ лежат в $Z(G)$ и образуют базис для $Z(G)$ над простым кольцом.

§ 6. Индуцированные характеры

Сохраняются обозначения предыдущего параграфа. Однако нам не потребуются все доказанные там результаты: все что нам нужно, — это билинейное спаривание на $X(G)$ и его продолжение до

$$X_R(G) \times X_R(G) \to R.$$

Символ $\langle\ ,\ \rangle$ может интерпретироваться и как билинейное продолжение, и как эрмитово продолжение, согласно теореме 7.

Пусть S — подгруппа в G. Имеется R-линейное отображение, называемое *отображением ограничения*

$$\text{Res}_S^G\colon\ X_R(G) \to X_R(S),$$

которое каждой функции классов на G сопоставляет ее ограничение на S. Это гомоморфизм колец. Ограничение f на S мы иногда будем обозначать через f_S.

Определим отображение в обратную сторону

$$\mathrm{Tr}_G^S\colon\ X_R(S)\to X_R(G),$$

которое мы будем называть *отображением индуцирования*. Именно, если $g\in X_R(S)$, то продолжаем g до g_0 на G, считая $g_0(\sigma)=0$ при $\sigma\notin S$ и затем полагая

$$\mathrm{Tr}_G^S(g)(\sigma)=\frac{1}{(S:1)}\sum_{\tau\in G} g_0(\tau\sigma\tau^{-1}).$$

Очевидно, $\mathrm{Tr}_G^S(g)$ есть функция классов на G. Если нет необходимости указывать в обозначении S или G, то мы часто будем писать g^* вместо $\mathrm{Tr}_G^S(g)$ и называть g^* *индуцированной функцией*. Ясно, что отображение Tr_G^S R-линейно.

Так как сейчас мы имеем дело с двумя группами S и G, то мы будем обозначать скалярное произведение через $\langle\ ,\ \rangle_S$ и $\langle\ ,\ \rangle_G$, когда оно берется относительно той или другой из этих групп. Следующая теорема среди прочего показывает, что отображения ограничения и индуцирования сопряжены друг с другом относительно нашей формы.

Теорема 10. *Пусть S — подгруппа в G. Тогда справедливы следующие правила*:

(i) (*Закон взаимности Фробениуса*). *Для $f\in X_R(G)$ и $g\in X_R(S)$ имеем*

$$\langle \mathrm{Tr}_G^S(g),\ f\rangle_G=\langle g,\ \mathrm{Res}_S^G(f)\rangle_S.$$

(ii) $\mathrm{Tr}_G^S(g)\,f=\mathrm{Tr}_G^S(gf_S)$.

(iii) *Если $T\subset S\subset G$ — подгруппы в G, то*

$$\mathrm{Tr}_G^S\circ\mathrm{Tr}_S^T=\mathrm{Tr}_G^T.$$

(iv) *Если $\sigma\in G$ и g^σ определено формулой $g^\sigma(\tau^\sigma)=g(\tau)$, где $\tau^\sigma=\sigma^{-1}\tau\sigma$, то*

$$\mathrm{Tr}_G^S(g)=\mathrm{Tr}_G^{S^\sigma}(g^\sigma).$$

(v) *Если ψ — собственный характер подгруппы S, то $\mathrm{Tr}_G^S(\psi)$ — собственный характер группы G.*

Доказательство. Докажем сначала (ii). Используем обозначение со звездочкой. Мы должны показать, что $g^*f=(gf_S)^*$. Имеем

$$(g^*f)(\tau)=\frac{1}{(S:1)}\sum_{\sigma\in G} g_0(\sigma\tau\sigma^{-1})f(\tau)=\frac{1}{(S:1)}\sum_{\sigma\in G} g_0(\sigma\tau\sigma^{-1})f(\sigma\tau\sigma^{-1}).$$

Последнее из полученных выражений равно $(gf_S)^*(\tau)$, что и доказывает (ii). Теперь просуммируем по всем τ из G выражения

$$g^*(\tau)f(\tau^{-1}) = \frac{1}{(S:1)}\sum_{\sigma\in G} g_0(\sigma\tau\sigma^{-1})f(\tau^{-1}) =$$

$$= \frac{1}{(S:1)}\sum_{\sigma\in G} g_0(\sigma\tau\sigma^{-1})f(\sigma\tau^{-1}\sigma^{-1}).$$

Ненулевой вклад в нашу двойную сумму внесут только те пары σ, τ, для которых произведения вида $\sigma\tau\sigma^{-1}$ будут элементами из S. Число пар (σ, τ), таких, что $\sigma\tau\sigma^{-1}$ есть некоторый фиксированный элемент из G, равно n (поскольку для всякого $\lambda \in G$ пара $(\sigma\lambda, \lambda^{-1}\tau\lambda)$ есть другая такая пара, а общее число пар равно n^2). Следовательно, наше просуммированное выражение справа равно

$$(G:1)\frac{1}{(S:1)}\sum_{\lambda\in S} g(\lambda)f(\lambda^{-1}).$$

Первое правило вытекает теперь из определений скалярного произведения в G и S соответственно.

Пусть теперь $g = \psi$ — собственный характер подгруппы S и $f = \chi$ — простой характер группы G. Из (i) находим, что коэффициенты Фурье для g^* являются целыми числами $\geqslant 0$. Действительно, $\mathrm{Res}_S^G(\chi)$ — собственный характер S. Поэтому скалярное произведение

$$\langle \psi, \mathrm{Res}_S^G(\chi)\rangle_S$$

есть целое число $\geqslant 0$. Следовательно, ψ^* — собственный характер G, что доказывает (v).

Для доказательства свойства транзитивности удобно ввести следующие обозначения.

Пусть $\{c\}$ — множество правых смежных классов G по подгруппе S. Для каждого смежного класса c выберем фиксированного представителя, обозначаемого через $\bar{c}$. Таким образом, если $\bar{c}_1, \ldots, \bar{c}_r$ — эти представители, то

$$G = \bigcup_c c = \bigcup_c S\bar{c} = \bigcup_{i=1}^{r} S\bar{c}_i.$$

Лемма. *Пусть g — некоторая функция классов на S. Тогда*

$$\mathrm{Tr}_G^S(g)(\xi) = \sum_{i=1}^{r} g_0(\bar{c}_i\xi\bar{c}_i^{-1}).$$

Доказательство. Мы можем сумму по всем $\sigma \in G$ в определении индуцированной функции разложить в двойную сумму

$$\sum_{\sigma\in G} = \sum_{\sigma\in S}\sum_{i=1}^{r};$$

заметим при этом, что всякий член $g_0(\sigma c\xi\bar{c}^{-1}\sigma^{-1})$ равен $g_0(\bar{c}\xi\bar{c}^{-1})$ при $\sigma\in S$, поскольку g — функция классов. Следовательно, достаточно в сумме по всем $\sigma\in S$ сократить множитель $1/(S:1)$, чтобы получить выражение, указанное в лемме.

Если $T\subset S\subset G$ — подгруппы в G и

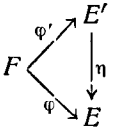
$$G=\bigcup \bar{S}c_i,\quad S=\bigcup T\bar{d}_j$$

— разложения на правые смежные классы, то $\{\bar{d}_j\bar{c}_i\}$ будет системой представителей для правых смежных классов G по T. Ввиду этого свойство транзитивности (iii) очевидно.

Мы предоставим (iv) читателю в качестве упражнения (которое, если принять во внимание лемму, тривиально).

§ 7. *Индуцированные представления*

Пусть G — конечная группа, S — ее подгруппа и F — некоторый S-модуль. Рассмотрим категорию $\mathscr{C}$, объектами которой являются S-гомоморфизмы $\varphi: F\to E$ модуля F в G-модули E. (Отметим, что всякий G-модуль можно рассматривать как S-модуль.) Если φ': $F\to E'$ — другой объект в $\mathscr{C}$, то определяем морфизм $\varphi'\to\varphi$ в $\mathscr{C}$ как G-гомоморфизм $\eta: E'\to E$, для которого коммутативна следующая диаграмма:



Универсальный объект в $\mathscr{C}$ задается с точностью до однозначно определенного G-изоморфизма. Его обозначением будет

$$\varphi_G^S: F\to \mathrm{Tr}_G^S(F).$$

Символ Tr призван напоминать о следе. Позже мы увидим оправдание для такого обозначения.

Ниже мы докажем, что универсальный объект всегда существует. Если $\varphi: F\to E$ — универсальный объект, то мы будем называть E *индуцированным модулем*. Этот модуль однозначно определен с точностью до единственного G-изоморфизма, для которого коммутативна соответствующая диаграмма. Для удобства мы выберем один индуцированный модуль, такой, что φ — включение. Мы закрепим тогда за этим специальным модулем $\mathrm{Tr}_G^S(F)$ название G-модуля, *индуцированного* S-модулем F.

Пусть $f: F'\to F$ — S-гомоморфизм. Если

$$\varphi_G^S: F'\to \mathrm{Tr}_G^S(F')$$

— G-модуль, индуцированный F', то существует однозначно определенный G-гомоморфизм $\mathrm{Tr}_G^S(F') \to \mathrm{Tr}_G^S(F)$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} F' & \xrightarrow{\varphi_G^S} & \mathrm{Tr}_G^S(F') \\ {\scriptstyle f}\downarrow & \searrow & \downarrow{\scriptstyle \mathrm{Tr}_G^S(f)} \\ F & \xrightarrow[\varphi_G^S]{} & \mathrm{Tr}_G^S(F) \end{array}$$

Это просто G-гомоморфизм, соответствующий универсальному свойству для S-гомоморфизма $\varphi_G^S \circ f$, изображенного в нашей диаграмме пунктирной линией. *Таким образом,* Tr_G^S *есть функтор из категории* S*-модулей в категорию* G*-модулей.*

Из универсальности и единственности индуцированного модуля мы получаем некоторые формальные свойства.

Tr_G^S *коммутирует с прямыми суммами: для данной прямой суммы* $S = F \oplus F'$

$$\mathrm{Tr}_G^S(F \oplus F') \approx \mathrm{Tr}_G^S(F) \oplus \mathrm{Tr}_G^S(F'),$$

причем прямая сумма справа — это G*-прямая сумма.*

Если f, g: $F' \to F$ — S*-гомоморфизмы, то*

$$\mathrm{Tr}_G^S(f+g) = \mathrm{Tr}_G^S(f) + \mathrm{Tr}_G^S(g).$$

Если $T \subset S \subset G$ *— подгруппы в* G *и* F *—* T*-модуль, то*

$$\mathrm{Tr}_G^S \circ \mathrm{Tr}_S^T(F) \approx \mathrm{Tr}_G^T(F).$$

Во всех трех случаях равенство между левой и правой частями наших соотношений тотчас следует из единственности универсального объекта. Проверку мы предоставим читателю.

Чтобы доказать существование индуцированного модуля, обозначим через $M_G^S(F)$ аддитивную группу функций $f: G \to F$, удовлетворяющих условию

$$\sigma f(\xi) = f(\sigma\xi)$$

для $\sigma \in S$ и $\xi \in G$. Определим действие G на $M_G^S(F)$, положив

$$(\sigma f)(\xi) = f(\xi\sigma)$$

для σ, $\xi \in G$. Ясно, что $M_G^S(F)$ — G-модуль.

Предложение 8. *Пусть отображение* $\varphi: F \to M_G^S(F)$ *таково, что для отображения* $\varphi(x) = \varphi_x$ *будет*

$$\varphi_x(\tau) = \begin{cases} 0 & \text{при } \tau \in S, \\ \tau x & \text{при } \tau \in S. \end{cases}$$

Тогда отображение φ *есть* S*-гомоморфизм, объект* $\varphi: F \to M_G^S(F)$ *универсален и гомоморфизм* φ *инъективен. Образ* φ *состоит из всех таких элементов* $f \in M_G^S(F)$, *что* $f(\tau) = 0$ *при* $\tau \notin S$.

Доказательство. Пусть $\sigma \in S$, $x \in F$ и $\tau \in G$. Тогда

$$(\sigma\varphi_x)(\tau) = \varphi_x(\tau\sigma).$$

Если $\tau \in S$, то последнее выражение равно $\varphi_{\sigma x}(\tau)$. Если $\tau \notin S$, то $\tau\sigma \notin S$ и, следовательно, оба выражения $\varphi_{\sigma x}(\tau)$ и $\varphi_x(\tau\sigma)$ равны 0. Таким образом, φ есть S-гомоморфизм и непосредственно ясно, что он инъективен. Далее, если $f \in M_G^S(F)$ таково, что $f(\tau) = 0$ для $\tau \notin S$, то из определений следует, что $f = \varphi_x$, где $x = f(1)$.

Остается доказать, что φ универсален. Чтобы это сделать, исследуем более детально структуру $M_G^S(F)$.

Предложение 9. *Пусть* $G = \bigcup_{i=1}^{r} S\bar{c}_i$ *— разложение* G *на правые смежные классы,* F_1 *— аддитивная группа функций из* $M_G^S(F)$, *принимающих значение* 0 *на элементах* $\xi \in G$, $\xi \notin S$. *Тогда*

$$M_G^S(F) = \prod_{i=1}^{r} \bar{c}_i^{-1} F_1,$$

где прямая сумма рассматривается как абелева группа.

Доказательство. Для всякого $f \in M_G^S(F)$ пусть f_i — такая функция, что

$$f_i(\xi) = \begin{cases} 0, & \text{если } \xi \notin S\bar{c}_i, \\ f(\xi), & \text{если } \xi \in S\bar{c}_i. \end{cases}$$

Очевидно, $f_i(\sigma\bar{c}_i) = (\bar{c}_i f_i)(\sigma)$ для всех $\sigma \in S$. Непосредственно видно, что $\bar{c}_i f_i$ лежит в F_1 и что

$$f = \sum_{i=1}^{r} \bar{c}_i^{-1}(\bar{c}_i f_i).$$

Таким образом, $M_G^S(f)$ есть сумма подгрупп $\bar{c}_i^{-1} F_1$. Ясно, что эта сумма прямая, что и требовалось.

Отметим, что $\{\bar{c}_1^{-1}, \ldots, \bar{c}_r^{-1}\}$ образуют систему представителей для левых смежных классов G по S. Действие G на $M_G^S(F)$ определяется предыдущим разложением в прямую сумму. Мы видим, что G переставляет слагаемые транзитивно. Слагаемое F_1 S-изоморфно исходному модулю F, как установлено в предложении 8.

Теорема 11. *Пусть* $\{\lambda_1, \ldots, \lambda_r\}$ — *некоторая система представителей левых смежных классов* G *по* S. *Тогда существует* G-*модуль* E, *содержащий* F *в качестве* S-*подмодуля и такой, что*

$$E = \coprod_{i=1}^{r} \lambda_i F$$

есть прямая сумма (как абелева группа). Пусть $\varphi : F \to E$ — *отображение включения. Тогда* φ *универсально в нашей категории* $\mathscr{C}$, *т. е.* E — *индуцированный модуль.*

Доказательство. Обычной теоретико-множественной процедурой замены F_1 на F в $M_G^S(F)$ получаем G-модуль E, содержащий F в качестве S-подмодуля и обладающий нужным нам разложением в прямую сумму. Пусть φ': $F \to E'$ — S-гомоморфизм в G-модуль E'. Определим отображение h: $E \to E'$ правилом

$$h(\lambda_1 x_1 + \ldots + \lambda_r x_r) = \lambda_1 \varphi'(x_1) + \ldots + \lambda_r \varphi'(x_r),$$

где $x_i \in F$. Это отображение правильно определено, так как наша сумма для E — прямая. Мы должны показать, что h — G-гомоморфизм. Пусть $\sigma \in G$. Тогда

$$\sigma\lambda_i = \lambda_{\sigma(i)}\tau_{\sigma, i},$$

где $\sigma(i)$ — некоторый индекс, зависящий от σ, i, а $\tau_{\sigma, i}$ — элемент из S, также зависящий от σ, i. Имеем

$$h(\sigma\lambda_i x_i) = h(\lambda_{\sigma(i)}\tau_{\sigma, i} x_i) = \lambda_{\sigma(i)}\varphi'(\tau_{\sigma, i} x_i).$$

Так как φ' — S-гомоморфизм, то это выражение равно

$$\lambda_{\sigma(i)}\tau_{\sigma, i}\varphi'(x_i) = \sigma h(\lambda_i x_i).$$

В силу линейности заключаем, что h — G-гомоморфизм, что и требовалось.

Предположим, что мы фиксировали основное поле k и рассматривали не произвольные модули, а только k-пространства, на которых имеется представление G. Ясно, что все наши конструкции и определения применимы и в этом контексте. Поэтому, имея представление подгруппы S на k-пространстве F, мы получаем индуцированное представление группы G на $\mathrm{Tr}_G^S(F)$.

Предложение 10. *Пусть* ψ — *характер представления подгруппы* S *на* k-*пространстве* F, E — *пространство индуцированного представления. Тогда характер* χ *представления на* E *равен индуцированному характеру* ψ^*, *т. е. задается формулой*

$$\chi(\xi) = \sum_c \psi_0(c\xi\bar{c}^{-1}),$$

где сумма берется по всем правым смежным классам с группы G по S, $\bar{c}$ — фиксированный представитель для c и ψ_0 — продолжение ψ на G, которое получается, если положить $\psi_0(\sigma) = 0$ для $\sigma \notin S$.

Доказательство. Пусть $\{w_1, \ldots, w_m\}$ — базис для F над k. Мы знаем, что

$$E = \coprod \bar{c}^{-1}F.$$

Пусть σ — элемент из G. Элементы $\{\overline{c\sigma}^{-1}w_j\}_{c,\,j}$ образуют базис для E над k.

Заметим, что $\bar{c}\sigma\overline{c\sigma}^{-1}$ есть элемент из S, так как

$$\overline{Sc}\sigma = Sc\sigma = S\overline{c\sigma}.$$

Имеем

$$\sigma(\overline{c\sigma}^{-1}w_j) = \bar{c}^{-1}(\bar{c}\sigma\overline{c\sigma}^{-1})w_j.$$

Пусть

$$(\bar{c}\sigma\overline{c\sigma}^{-1})_{\mu j}$$

— компоненты матрицы, представляющей действие $\bar{c}\sigma\overline{c\sigma}^{-1}$ на F относительно базиса $\{w_1, \ldots, w_m\}$. Тогда действие σ на E задается соотношениями

$$\sigma(\overline{c\sigma}^{-1}w_j) = \bar{c}^{-1}\sum_{\mu}(\bar{c}\sigma\overline{c\sigma}^{-1})_{\mu j}w_\mu = \sum_{\mu}(\bar{c}\sigma\overline{c\sigma}^{-1})_{\mu j}(\bar{c}^{-1}w_\mu).$$

По определению

$$\chi(\sigma) = \sum_{c\sigma = c}\sum_{j}(\bar{c}\sigma\overline{c\sigma}^{-1})_{jj}.$$

Но $c\sigma = c$ в том и только в том случае, если $\bar{c}\sigma\bar{c}^{-1} \in S$. Кроме того,

$$\psi(\bar{c}\sigma\bar{c}^{-1}) = \sum_{j}(\bar{c}\sigma\bar{c}^{-1})_{jj}.$$

Следовательно,

$$\chi(\sigma) = \sum_{c}\psi_0(\bar{c}\sigma\bar{c}^{-1}),$$

что и требовалось показать.

Следующие три параграфа, которые по существу независимы друг от друга, дают примеры индуцированных представлений. В каждом случае мы показываем, что какие-то представления либо индуцированы представлениями некоторых хорошо известных типов, либо являются линейными комбинациями с целочисленными коэффициентами таких представлений. Самое замечательное во всех этих результатах то, что все характеры

могут быть представлены как линейные комбинации индуцированных характеров, возникающих из одномерных характеров. Таким образом, теория характеров сводится к изучению одномерных, или абелевых характеров.

§ 8. Положительное разложение регулярного характера

Пусть G — конечная группа и $k = \mathbf{C}$ — поле комплексных чисел. Пусть, далее, 1_G — тривиальный характер, а r_G — регулярный характер.

Предложение 11. *Пусть H — подгруппа в G, ψ — характер H, ψ^* — индуцированный характер. Тогда кратность характера 1_H в ψ та же самая, что и кратность 1_G в ψ^*.*

Доказательство. В силу теоремы 10 (i) имеем

$$\langle \psi, 1_H \rangle_H = \langle \psi^*, 1_G \rangle_G.$$

Эти скалярные произведения как раз и являются интересующими нас кратностями.

Предложение 12. *Регулярное представление есть представление, индуцированное тривиальным характером на тривиальной подгруппе группы G.*

Доказательство. Это тотчас следует из определения индуцированного характера

$$\psi^*(\tau) = \sum_{\sigma \in G} \psi_0(\sigma\tau\sigma^{-1}),$$

если взять $\psi = 1$ на тривиальной подгруппе.

Следствие. *Кратность 1_G в регулярном характере r_G равна 1.*

Мы исследуем теперь характер

$$u_G = r_G - 1_G.$$

Теорема 12 (Брауэр). *Характер πu_G является линейной комбинацией с целыми положительными коэффициентами характеров, индуцированных одномерными характерами циклических подгрупп группы G.*

Доказательство состоит из двух предложений, дающих явное описание индуцированных характеров. Я обязан Серру приведенным далее изложением работы Брауэра.

Пусть A — циклическая группа порядка a. Определим на A функцию θ_A следующими условиями:

$$\theta_A(\sigma) = \begin{cases} a, & \text{если } \sigma \text{ — образующая группы } A, \\ 0 & \text{— в противном случае.} \end{cases}$$

Положим $\lambda_A = \varphi(a) r_A - \theta_A$ (где φ — функция Эйлера) и $\lambda_A = 0$, если $a = 1$.

Искомый результат содержится в следующих двух предложениях.

Предложение 13. *Пусть G — конечная группа порядка n. Тогда*

$$nu_G = \sum \lambda_A^*,$$

где сумма берется по всем циклическим подгруппам группы G.

Доказательство. Для данных функций классов χ, ψ на G имеем обычное скалярное произведение

$$\langle \psi, \chi \rangle_G = \frac{1}{n} \sum_{\sigma \in G} \psi(\sigma) \overline{\chi(\sigma)}.$$

Пусть ψ — любая функция классов на G. Тогда

$$\langle \psi, nu_G \rangle = \langle \psi, nr_G \rangle - \langle \psi, n1_G \rangle = \\ = n\psi(1) - \sum_{\sigma \in G} \psi(\sigma).$$

С другой стороны, используя тот факт, что индуцированный характер сопряжен с ограничением, получаем

$$\sum_A \langle \psi, \lambda_A^* \rangle = \sum_A \langle \psi \mid A, \lambda_A \rangle = \\ = \sum_A \langle \psi \mid A, \varphi(a) r_A - \theta_A \rangle = \\ = \sum_A \varphi(a) \psi(1) - \sum_A \frac{1}{a} \sum_{\sigma \text{ порождает } A} a\psi(\sigma) = \\ = n\psi(1) - \sum_{\sigma \in G} \psi(\sigma).$$

Так как функции в левой и правой частях утверждаемого равенства имеют одно и то же скалярное произведение с произвольной функцией классов, то они равны. Это доказывает наше предложение.

Предложение 14. *Если $A \neq \{1\}$, то λ_A есть линейная комбинация неприводимых нетривиальных характеров A с целыми положительными коэффициентами.*

Доказательство. Если A — циклическая группа простого порядка, то в силу предложения 13 $\lambda_A = n u_A$, и наше утверждение вытекает из стандартной структуры регулярного представления.

Чтобы доказать утверждение в общем случае, достаточно установить, что коэффициенты Фурье функции λ_A относительно характеров степени 1 являются целыми числами $\geqslant 0$. Пусть ψ — характер степени 1. Взяв скалярное произведение относительно A, получим

$$\langle \psi, \lambda_A \rangle = \varphi(a)\psi(1) - \sum_{\sigma\text{-образующая}} \psi(\sigma) =$$
$$= \varphi(a) - \sum_{\sigma\text{-образующая}} \psi(\sigma) =$$
$$= \sum_{\sigma\text{-образующая}} (1 - \psi(\sigma)).$$

Сумма $\sum \psi(\sigma)$, взятая по образующим A, является, с одной стороны, целым алгебраическим числом, а с другой стороны, рациональным числом (в силу любого из многочисленных элементарных соображений) и, следовательно, является целым рациональным числом. Далее, если характер ψ нетривиален, то вещественные части всех чисел

$$1 - \psi(\sigma)$$

будут > 0 для $\sigma \neq \mathrm{id}$ и 0 для $\sigma = \mathrm{id}$. Отсюда заключаем, что сумма должна быть равна целому положительному числу. Если ψ — тривиальный характер, то сумма, очевидно, равна 0. Наше предложение доказано.

§ 9. *Сверхразрешимые группы*

Пусть G — конечная группа. Мы будем говорить, что G *сверхразрешима*, если существует такая последовательность подгрупп

$$\{1\} \subset G_1 \subset G_2 \subset \ldots \subset G_m = G,$$

что каждая подгруппа G_i нормальна в G, и G_{i+1}/G_i — циклическая группа простого порядка.

Мы знаем из теории p-групп, что всякая p-группа сверхразрешима и что этим свойством обладает также прямое произведение p-группы с абелевой группой.

Предложение 15. *Всякая подгруппа и всякая факторгруппа сверхразрешимой группы сверхразрешимы.*

Доказательство. Очевидно (использовать стандартные теоремы о гомоморфизмах).

Предложение 16. *Пусть G — неабелева сверхразрешимая группа. Тогда существует нормальная абелева подгруппа, которая собственным образом содержит центр.*

Доказательство. Пусть C — центр группы G, $\bar{G} = G/C$, $\bar{H}$ — нормальная подгруппа простого порядка в $\bar{G}$ и H — ее полный прообраз в G при каноническом отображении $G \to G/C$. Если $\bar{\sigma}$ — образующая $\bar{H}$, то прообраз σ элемента $\bar{\sigma}$ вместе с C порождает H. Следовательно, H абелева, нормальна и собственным образом содержит центр.

Теорема 13 (Бликфельд). *Пусть G — сверхразрешимая группа, k — алгебраически замкнутое поле, $\operatorname{char} k \nmid (G:1)$, и пусть E — простое (G, k)-пространство. Если $\dim_k E > 1$, то существуют собственная подгруппа H в G и простое (H, k)-подпространство F в E, такие, что модуль E индуцирован подмодулем F.*

Доказательство. Так как простое представление над абелевой группой одномерно, то из наших условий вытекает, что G неабелева.

Мы дадим сначала доказательство нашей теоремы при дополнительном предположении, что модуль E — точный. (Это означает, что из условия $\sigma x = x$ для всех $x \in E$ следует, что $\sigma = 1$.) В конце мы легко избавимся от этого ограничения.

Лемма. *Пусть G — конечная группа и k — алгебраически замкнутое поле, $\operatorname{char} k \nmid (G:1)$. Пусть E — простое точное G-пространство над k. Предположим, что в G имеется нормальная абелева подгруппа H, собственным образом содержащая центр G. Тогда существуют собственная подгруппа H_1 в G, содержащая H и простое H_1-пространство F, такие, что E есть индуцированный модуль модуля F с H_1 на G.*

Доказательство. Рассмотрим E как H-пространство. Оно является прямой суммой простых H-пространств, и так как H абелева, каждое такое простое H-пространство одномерно.

Пусть $v \in E$ порождает одномерное H-пространство и ψ — его характер. Если $w \in E$ также порождает одномерное H-пространство с тем же самым характером ψ, то для всех $a, b \in k$ и $\tau \in H$ имеем

$$\tau(av + bw) = \psi(\tau)(av + bw).$$

Обозначив через F_ψ подпространство в E, порожденное всеми одномерными H-подпространствами, имеющими характер ψ, получаем разложение в H-прямую сумму

$$E = \coprod_{\psi} F_\psi.$$

Мы утверждаем, что $E \neq F_\psi$. В противном случае пусть $v \in E$, $v \neq 0$ и $\sigma \in G$. Тогда по предположению $\sigma^{-1}v$ порождает одномерное

H-пространство, имеющее характер ψ. Следовательно, для $\tau \in H$ имеем

$$\tau(\sigma^{-1}v) = \psi(\tau)\,\sigma^{-1}v,$$
$$(\sigma\tau\sigma^{-1})\,v = \sigma\psi(\tau)\,\sigma^{-1}v = \psi(\tau)\,v.$$

Это показывает, что $\sigma\tau\sigma^{-1}$ и τ одинаково действуют на элемент v из E. Так как H не содержится в центре G, то существуют $\tau \in H$ и $\sigma \in G$, такие, что $\sigma\tau\sigma^{-1} \neq \tau$, и мы получили противоречие с предположением, что представление E — точное.

Докажем, что G транзитивным образом переставляет пространства F_ψ.

Пусть $v \in F_\psi$. Для любых $\tau \in H$ и $\sigma \in G$ имеем

$$\tau(\sigma v) = \sigma(\sigma^{-1}\tau\sigma)\,v = \sigma\psi(\sigma^{-1}\tau\sigma)\,v = \psi_\sigma(\tau)\,\sigma v,$$

где ψ_σ — функция на H, задаваемая правилом $\psi_\sigma(\tau) = \psi(\sigma^{-1}\tau\sigma)$. Это показывает, что σ отображает F_ψ в F_{ψ_σ}. Однако в силу симметрии σ^{-1} отображает F_{ψ_σ} в F_ψ, и эти два отображения σ, σ^{-1} дают взаимно однозначное соответствие между F_{ψ_σ} и F_ψ. Таким образом, G переставляет пространства $\{F_\psi\}$.

Пусть $E' = GF_{\psi_0} = \sum \sigma F_{\psi_0}$ для некоторого фиксированного ψ_0. Тогда E' есть G-подпространство в E, и так как E предполагается простым, то $E' = E$. Это доказывает, что пространства $\{F_\psi\}$ переставляются транзитивно.

Пусть $F = F_{\psi_1}$ для некоторого фиксированного ψ_1. F есть H-подпространство в E. Пусть H_1 — подгруппа, состоящая из всех таких элементов $\tau \in G$, что $\tau F = F$. Тогда $H_1 \neq G$, так как $E \neq F_\psi$. *Мы утверждаем, что F — простое H_1-пространство и что E есть индуцированное пространство пространства F с H_1 на G.*

Чтобы это увидеть, возьмем разложение $G = \bigcup H_1\bar{c}$ группы G на правые смежные классы относительно подгруппы H_1. Элементы $\{\bar{c}^{-1}\}$ образуют систему представителей левых смежных классов относительно подгруппы H_1. Так как

$$E = \sum_{\sigma \in G} \sigma F,$$

то

$$E = \sum_c \bar{c}^{-1}F$$

Мы утверждаем, что эта последняя сумма прямая и что F — простое H_1-пространство.

Так как G переставляет пространства $\{F_\psi\}$, то по определению H_1 есть группа изотропии элемента F при действии G на этом множестве пространств, и что, следовательно, элементы орбиты — это в точности $\{\bar{c}^{-1}F\}$, где c пробегает все смежные классы. Таким

образом, пространства $\{\bar{c}^{-1}F\}$ различны, и мы имеем разложение в прямую сумму

$$E = \coprod_{c} \bar{c}^{-1}F.$$

Если W — собственное H_1-подпространство в F, то $\coprod \bar{c}^{-1}W$ — собственное G-подпространство в E, вопреки предположению, что E простое. Это доказывает наше утверждение.

Применяя теперь теорему 11, заключаем, что E — модуль, индуцированный F, что и доказывает теорему 13 в том случае, когда E — точный модуль.

Предположим теперь, что E неточный. Пусть G_0 — нормальная подгруппа в G, служащая ядром представления $G \to \mathrm{Aut}_k(E)$. Положим $\bar{G} = G/G_0$. Тогда E дает точное представление для $\bar{G}$. Поскольку E неодномерно, $\bar{G}$ неабелева и существуют собственная подгруппа $\bar{H}$ в $\bar{G}$ и простое $\bar{H}$-пространство F, такие, что

$$E = \mathrm{Tr}_{\bar{G}}^{\bar{H}}(F).$$

Пусть H — полный прообраз $\bar{H}$ при естественном отображении $G \to \bar{G}$. Тогда $H \supset G_0$ и F — простое H-пространство. При действии $\bar{G}$ как группы перестановок на множестве k-подпространств $\{\sigma F\}_{\sigma \in G}$, как мы знаем, $\bar{H}$ есть подгруппа изотропии одного из элементов. Следовательно, H есть подгруппа изотропии в G при том же самом действии. Снова применяя теорему 11, заключаем, что E индуцировано F, т. е.

$$E = \mathrm{Tr}_{G}^{H}(F),$$

и тем самым теорема 13 доказана.

Следствие. *Пусть G — произведение p-группы и циклической группы, k — алгебраически замкнутое поле,* $\mathrm{char}\, k \nmid (G : 1)$. *Если E — простое (G, k)-пространство и* $\dim_k E > 1$, *то E индуцируется одномерным представлением некоторой подгруппы.*

Доказательство. Применяем теорему шаг за шагом, используя транзитивность индуцированных представлений, пока не получим одномерное представление некоторой подгруппы.

§ 10. Теорема Брауэра

Пусть $k = \mathbf{C}$ — поле комплексных чисел, R — некоторое подкольцо в k. Мы будем иметь дело с кольцом $X_R(G)$, состоящим из всех линейных комбинаций с коэффициентами в R простых характеров G над k. (Это множество является кольцом в силу предложения 2 § 2.)

Пусть $H = \{H_\alpha\}$ — фиксированное семейство подгрупп в G, занумерованное индексами $\{\alpha\}$, и $V_R(G)$ — аддитивная подгруппа в $X_R(G)$, порожденная всеми функциями, которые индуцируются функциями из $X_R(H_\alpha)$ с H_α из нашего семейства. Другими словами,

$$V_R(G) = \sum_\alpha \mathrm{Tr}_G^{H_\alpha}(X_R(H_\alpha)).$$

Мы могли бы также сказать, что $V_R(G)$ — подгруппа, порожденная над R всеми характерами, индуцированными со всех H_α.

Лемма 1. *$V_R(G)$ есть идеал в $X_R(G)$.*

Доказательство. Это непосредственно вытекает из теоремы 10 (ii) § 6.

Во многих приложениях семейство подгрупп будет состоять из „элементарных" подгрупп. Пусть p — простое число. Под *p-элементарной группой* мы будем понимать произведение p-группы и циклической группы (порядок которой может предполагаться взаимно простым с p, поскольку мы можем включить p-часть циклического множителя в p-группу). Элемент $\sigma \in G$ называется *p-регулярным*, если его период взаимно прост с p, и *p-сингулярным*, если его период есть степень p. Каждый элемент $x \in G$ мы можем единственным образом представить в виде

$$x = \sigma\tau,$$

где элемент σ p-сингулярен, τ p-регулярен и σ, τ коммутируют. Действительно, если $p^r m$ — период x, где m взаимно просто с p, то $1 = \nu p^r + \mu m$, откуда $x = (x^m)^\mu (x^{p^r})^\nu$, что и дает нам наше разложение. Оно, очевидно, единственно, так как множители лежат в циклической подгруппе, порожденной x. Мы будем называть эти два множителя *p-сингулярным и p-регулярным множителями* x соответственно.

Предыдущее разложение показывает также, что имеет место

Предложение 17. *Все подгруппы и факторгруппы p-элементарной группы p-элементарны. Если S — подгруппа p-элементарной группы $P \times C$, где P — p-группа, а C — циклическая группа взаимно простого с p порядка, то $S = (S \cap P) \times (S \cap C)$.*

Доказательство. Очевидно.

Наша цель — показать среди прочего, что если семейство $\{H_\alpha\}$ таково, что всякая p-элементарная подгруппа в G содержится в некоторой H_α, то $V_R(G) = X_R(G)$ для любого кольца R. Разумеется, это было бы достаточно сделать для $R = \mathbf{Z}$, но для наших целей необходимо сначала доказать этот результат, используя некоторое большее кольцо. Основной результат содержится в теоре-

мах 15 и 16, принадлежащих Брауэру. Мы дадим изложение Брауэра — Тейта (Brauer R., Tate J., On the characters of finite groups, *Ann. of Math.*, **62** (1955), 1—7.)

Пусть R — кольцо $\mathbf{Z}[\zeta]$, где ζ — примитивный корень n-й степени из единицы. В R как $\mathbf{Z}$-модуле имеется базис, а именно $1, \zeta, \ldots, \zeta^{N-1}$, где N — некоторое целое число. Это тривиальный факт; мы можем взять в качестве N степень неприводимого многочлена элемента ζ над $\mathbf{Q}$. У этого неприводимого многочлена старший коэффициент равен 1 и все другие коэффициенты — целые числа, так что тот факт, что

$$1, \zeta, \ldots, \zeta^{N-1}$$

образуют базис $\mathbf{Z}[\zeta]$, вытекает из алгоритма Евклида. Больше ничего об этой степени N нам знать не нужно.

Мы докажем наше утверждение сначала для только что введенного кольца R. Остальное затем будет следовать из приводимой ниже леммы.

Лемма 2. *Если $d \in \mathbf{Z}$ и постоянная функция $d \cdot 1_G$ принадлежит V_R, то $d \cdot 1_G$ принадлежит $V_{\mathbf{Z}}$.*

Доказательство. Мы утверждаем, что $1, \zeta, \ldots, \zeta^{N-1}$ линейно независимы над $X_{\mathbf{Z}}(G)$. Действительно, соотношение линейной зависимости давало бы

$$\sum_{\nu=1}^{s} \sum_{j=0}^{N-1} c_{\nu j} \chi_\nu \zeta^j = 0,$$

где $c_{\nu j}$ — целые числа, не все равные 0. Но простые характеры линейно независимы над k. Предыдущее же соотношение есть соотношение между этими простыми характерами с коэффициентами в R, и мы получаем противоречие. Мы заключаем поэтому, что

$$V_R = V_{\mathbf{Z}} \oplus V_{\mathbf{Z}}\zeta \oplus \ldots \oplus V_{\mathbf{Z}}\zeta^{N-1}$$

есть прямая сумма (абелевых групп), и наша лемма доказана.

Если мы сможем доказать, что постоянная функция 1_G лежит в $V_R(G)$, то в силу леммы отсюда будет следовать, что она лежит в $V_{\mathbf{Z}}(G)$, и поскольку $V_{\mathbf{Z}}(G)$ — идеал, $X_{\mathbf{Z}}(G) = V_{\mathbf{Z}}(G)$.

Для доказательства нам потребуется ряд лемм.

Два элемента x, x' из G называются *p-сопряженными*, если их p-регулярные множители сопряжены в обычном смысле. Ясно, что p-сопряженность есть отношение эквивалентности; классы эквивалентности будут называться *классами p-сопряженных элементов* или просто *p-классами*.

Лемма 3. *Пусть $f \in X_R(G)$, причем $f(\sigma) \in \mathbf{Z}$ для всех $\sigma \in G$. Тогда f постоянна по модулю p на каждом p-классе.*

Доказательство. Пусть $x = \sigma\tau$, где элемент σ p-сингулярен, а τ p-регулярен и σ, τ коммутируют. Достаточно доказать, что

$$f(x) \equiv f(\tau) \pmod{p}.$$

Пусть H — циклическая подгруппа, порожденная x. Тогда ограничение f на H может быть записано в виде

$$f_H = \sum a_j \psi_j,$$

где $a_j \in R$ и ψ_j — простые характеры H, т. е. гомоморфизмы H в k^*. Для некоторой степени p^r мы имеем $x^{p^r} = \tau^{p^r}$, откуда $\psi_j(x)^{p^r} = \psi_j(\tau)^{p^r}$ и, следовательно,

$$f(x)^{p^r} \equiv f(\tau)^{p^r} \pmod{\mathfrak{P}},$$

где $\mathfrak{P}$ — максимальный идеал в R, лежащий над p. А так как по условию $f(x)$, $f(\tau) \in \mathbf{Z}$ и $\mathfrak{P} \cap \mathbf{Z} = (p)$, то $f(x)^{p^r} \equiv f(\tau)^{p^r} \pmod{p}$. Остается заметить, что $b^{p^r} \equiv b \pmod{p}$ для любого целого числа p.

Лемма 4. *Пусть τ — p-регулярный элемент в G, T — циклическая подгруппа, порожденная τ, и C — подгруппа в G, состоящая из всех элементов, коммутирующих с τ. Пусть, далее, P — силовская p-подгруппа в C. Тогда существует элемент $\psi \in X_R(T \times P)$, такой, что индуцированная функция $f = \psi^*$ обладает следующими свойствами*:

(1) $f(\sigma) \in \mathbf{Z}$ *для всех* $\sigma \in G$.

(2) $f(\sigma) = 0$, *если* σ *не принадлежит* p*-классу элемента* τ.

(3) $f(\tau) = (C : P) \not\equiv 0 \pmod{p}$.

Доказательство. Отметим прежде всего, что подгруппа в G, порожденная T и P, является прямым произведением $T \times P$. Пусть $\psi_1, \ldots, \psi_r$ — простые характеры циклической группы T. Предположим, что они продолжены на $T \times P$ посредством композиции с проекцией

$$T \times P \to T \to k^*.$$

Эти продолжения мы по-прежнему обозначаем через $\psi_1, \ldots, \psi_r$. Положим

$$\psi = \sum_{\nu=1}^{r} \overline{\psi_\nu(\tau)}\, \psi_\nu.$$

Соотношения ортогональности для простых характеров на T показывают, что

$$\psi(\tau y) = \psi(\tau) = (T:1) \qquad \text{для } y \in P,$$
$$\psi(\sigma) = 0, \text{ если } \sigma \in TP \qquad \text{и } \sigma \notin \tau P.$$

Мы утверждаем, что ψ^* удовлетворяет нашим требованиям.

Прежде всего ясно, что ψ лежит в $X_R(TP)$.

Для $\sigma \in G$ имеем

$$\psi^*(\sigma) = \frac{1}{(TP:1)} \sum_{x \in G} \psi_0(x\sigma x^{-1}) = \frac{1}{(P:1)} \mu(\sigma),$$

где $\mu(\sigma)$ — число элементов $x \in G$, таких, что $x\sigma x^{-1}$ лежит в τP. Число $\mu(\sigma)$ делится на $(P:1)$, поскольку если элемент x из G переводит σ посредством сопряжения в τP, то тем же свойством обладает всякий элемент из Px. Следовательно, значения ψ^* лежат в $\mathbf{Z}$.

Далее, $\mu(\sigma) \not\equiv 0$ только для p-сопряженного с τ элемента σ, откуда вытекает наше условие (2).

Наконец, равенство $x\tau x^{-1} = \tau y$ с $y \in P$ возможно только при $y = 1$ (так как период τ взаимно прост с p). Следовательно, $\mu(\tau) = (C:1)$, откуда следует наше условие (3).

Лемма 5. Предположим, что семейство подгрупп $\{H_\alpha\}$ покрывает G (т. е. всякий элемент из G лежит в некоторой подгруппе H_α). Если f — функция классов на G, принимающая значение в $\mathbf{Z}$ и такая, что все ее значения делятся на $n = (G:1)$, то f принадлежит $V_R(G)$.

Доказательство. Пусть γ — некоторый класс сопряженных элементов и p взаимно просто с n. Всякий элемент из G p-регулярен и все p-подгруппы в G тривиальны, так что в этом случае p-сопряженность есть то же самое, что сопряженность. Применяя лемму 4, мы найдем, что в $V_R(G)$ имеется функция, принимающая значение 0 на элементах $\sigma \notin \gamma$ и принимающая целочисленное значение, делящее n на элементах из γ. Умножая эту функцию на некоторое целое число, мы найдем, что в $V_R(G)$ имеется функция, принимающая значения n на всех элементах из γ и значение 0 на всех других элементах. Отсюда лемма следует непосредственно.

Теорема 14 (Артин). *Всякий характер группы G есть линейная комбинация с рациональными коэффициентами характеров, индуцированных с циклических подгрупп.*

Доказательство. Пусть в лемме 5 $\{H_\alpha\}$ — семейство циклических подгрупп группы G. Постоянная функция $n \cdot 1_G$ принадлежит

$V_R(G)$. В силу леммы 2 эта функция принадлежит $V_{\mathbf{Z}}(G)$, и, следовательно, $nX_{\mathbf{Z}}(G) \subset V_{\mathbf{Z}}(G)$. Таким образом,

$$X_{\mathbf{Z}}(G) \subset \frac{1}{n} V_{\mathbf{Z}}(G),$$

что и доказывает теорему.

Лемма 6. Пусть p — простое число, и пусть всякая p-элементарная подгруппа группы G содержится в некоторой H_α. Тогда существует функция $f \in V_R(G)$, значения которой лежат в $\mathbf{Z}$ и $\equiv 1 \pmod{p^r}$.

Доказательство. Применим леммы 3 и 4. Для всякого p-класса γ мы можем найти функцию f_γ из $V_R(G)$, значения которой равны 0 вне γ и $\not\equiv 0 \bmod p$ для элементов из γ. Пусть $f = \sum_\gamma f_\gamma$, где сумма берется по всем p-классам. Тогда $f(\sigma) \not\equiv 0 \pmod{p}$ для всех $\sigma \in G$ и $f^{(p-1)\,p^{r-1}}$ дает искомую функцию.

Лемма 7. Пусть p — простое число, и пусть всякая p-элементарная подгруппа группы G содержится в некоторой H_α. Пусть, далее, $n = n_0 p^r$, где n_0 взаимно просто с p. Тогда постоянная функция $n_0 \cdot 1_G$ принадлежит $V_Z(G)$.

Доказательство. В силу леммы 2 достаточно доказать, что $n_0 \cdot 1_G$ принадлежит $V_R(G)$. Пусть f — функция из леммы 6. Тогда

$$n_0 \cdot 1_G = n_0(1_G - f) + n_0 f.$$

Так как все значения функции $n_0(1_G - f)$ делятся на $n_0 p^r = n$, то эта функция лежит в $V_R(G)$, согласно лемме 5. С другой стороны, $n_0 f \in V_R(G)$, поскольку $f \in V_R(G)$. Это доказывает нашу лемму.

Теорема 15 (Брауэр). *Предположим, что для всякого простого числа p любая p-элементарная подгруппа группы G содержится в некоторой H_α. Тогда $X(G) = V_{\mathbf{Z}}(G)$. Всякий характер группы G есть линейная комбинация с целочисленными коэффициентами характеров, индуцированных с подгрупп H_α.*

Доказательство. Это непосредственное следствие леммы 7, так как мы можем найти в $V_{\mathbf{Z}}(G)$ функции $n_0 \cdot 1_G$ с n_0, взаимно простым с любым заданным простым числом.

Следствие. *Функция классов f на G тогда и только тогда принадлежит $X(G)$, когда ее ограничение на H_α принадлежит $X(H_\alpha)$ для каждого α.*

Доказательство. Предположим, что для каждого α ограничение f на H_α есть характер на H_α. В силу теоремы мы можем записать

$$1_G = \sum_\alpha c_\alpha \operatorname{Tr}_G^{H_\alpha}(\psi_\alpha),$$

где $c_\alpha \in \mathbf{Z}$ и $\psi_\alpha \in X(H_\alpha)$. Следовательно,

$$f = \sum_\alpha c_\alpha \operatorname{Tr}_G^{H_\alpha}\left(\psi_\alpha f_{H_\alpha}\right),$$

согласно теореме 10 (ii) § 6. Поэтому если $f_{H_\alpha} \in X(H_\alpha)$, то f принадлежит $X(G)$. Обратное, разумеется, тривиально.

Теорема 16 (Брауэр). *Всякий характер на G есть линейная комбинация с целочисленными коэффициентами характеров, индуцированных одномерными характерами подгрупп.*

Доказательство. В силу теоремы 15 и транзитивности индуцирования достаточно доказать, что всякий характер p-элементарной группы обладает свойством, сформулированным в теореме. Но мы уже доказали это в предыдущем параграфе (следствие теоремы 13).

§ 11. Поле определения представления

Пусть k — поле, G — группа и E — k-пространство. Предположим, что имеется представление G на E. Пусть k' — расширение поля k. Тогда G действует на $k' \otimes_k E$ по правилу

$$\sigma(a \otimes x) = a \otimes \sigma x$$

для $a \in k'$ и $x \in E$. Это отображение возникает из билинейного отображения произведения $k' \times E$, задаваемого соответствием

$$(a, x) \longmapsto a \otimes \sigma x.$$

Рассматривая $E' = k' \otimes_k E$ как расширение E посредством k', мы получаем представление G на E'.

Предложение 18. *Пусть обозначения те же, что и выше. Тогда характеры представлений группы G на E и на E' равны.*

Доказательство. Пусть $\{v_1, \ldots, v_m\}$ — базис E над k. Тогда

$$\{1 \otimes v_1, \ldots, 1 \otimes v_m\}$$

— базис E' над k'. Таким образом, матрицы, представляющие элемент σ из G относительно этих двух базисов, равны и, следовательно, равны их следы.

Обратно, пусть k' — поле и k — подполе. Представление G на k'-пространстве E' называется *определимым над* k, если существуют k-пространство E и представление G на E, такие, что E' G-изоморфно $k' \otimes_k E$.

Предложение 19. *Пусть E, F — пространства над k простых представлений конечной группы G. Пусть k' — расширение k. Предположим, что E, F не являются G-изоморфными. Тогда никакая k'-простая компонента пространства $E^{k'}$ не встречается в разложении $F^{k'}$ в прямую сумму k'-простых подпространств.*

Доказательство. Рассмотрим разложение

$$k[G] = \prod_{\mu=1}^{s(k)} R_\mu(k)$$

над k в прямую сумму простых колец. Не теряя общности, мы можем предполагать, что E, F — простые левые идеалы в $k[G]$: по предположению они будут принадлежать различным множителям этого произведения. Если мы теперь возьмем тензорное произведение с k', то получим не что иное, как $k'[G]$. Тем самым мы будем иметь разложение в прямое произведение над k'. Так как $R_\nu(k) R_\mu(k) = 0$ при $\nu \neq \mu$, то оно будет в действительности получаться разложением в прямое произведение каждого множителя $R_\mu(k)$

$$k'[G] = \prod_{\mu=1}^{s(k)} \prod_{i=1}^{m(\mu)} R_{\mu i}(k').$$

Пусть, скажем, $E = L_\nu$ и $F = L_\mu$, где $\nu \neq \mu$. Тогда $R_\mu E = 0$. Следовательно, $R_{\mu i} E^{k'} = 0$ для всякого $i = 1, \ldots, m(\mu)$. Отсюда вытекает, что никакая простая компонента в $E^{k'}$ не может быть G-изоморфна никакому из простых левых идеалов колец $R_{\mu i}$, а это и доказывает то, что нам было нужно.

Следствие. *Простые характеры $\chi_1, \ldots, \chi_{s(k)}$ группы G над k линейно независимы над любым расширением k' поля k.*

Доказательство. Это тотчас вытекает из предложения и линейной независимости k'-простых характеров над k'.

Предложения 18 и 19 являются по существу общими утверждениями совершенно абстрактной природы. В доказательстве следующей теоремы используется теорема Брауэра.

Теорема 17 (Брауэр). *Пусть G — конечная группа показателя m. Всякое представление G над полем комплексных чисел (или над алгебраически замкнутым полем характеристики 0)*

определим над полем $\mathbf{Q}(\zeta_m)$, *где* ζ_m — *примитивный корень* m-*й степени из единицы.*

Доказательство. Пусть χ — характер некоторого представления G над $\mathbf{C}$, т. е. собственный характер. В силу теоремы 16 мы можем записать

$$\chi = \sum_j c_j Tr_G^{S_j}(\psi_j), \qquad c_i \in \mathbf{Z},$$

где сумма берется по конечному числу подгрупп S_j и ψ_j — одномерный характер S_j. Ясно, что каждый характер ψ_j определим над $\mathbf{Q}(\zeta_m)$. Таким образом, определим над $\mathbf{Q}(\zeta_m)$ и индуцированный характер ψ_j^*, который может быть записан в виде

$$\psi_j^* = \sum_\mu d_{j\mu}\chi_\mu, \qquad d_{j\mu} \in \mathbf{Z},$$

где $\{\chi_\mu\}$ — простые характеры G над $\mathbf{Q}(\zeta_m)$. Следовательно,

$$\chi = \sum_\mu \left(\sum_j c_j d_{j\mu}\right)\chi_\mu.$$

Представление χ в виде линейной комбинации простых характеров над k единственно, и, следовательно, коэффициент

$$\sum_j c_j d_{j\mu}$$

$\geqslant 0$. Это доказывает все, что нам было нужно.

УПРАЖНЕНИЯ

Первые упражнения посвящены соотношениям ортогональности для коэффициентов матричных представлений. Эти соотношения являются несколько более общими, чем соотношения для характеров. Доказательства не зависят от изложения, данного в тексте, и, следовательно, дают альтернативный подход к получению тех же результатов, *не зависящий от предыдущей главы.* Используются только лемма Шура и полная приводимость.

1. Пусть G — конечная группа, k — произвольное поле, E, F — простые (G, k)-пространства и λ — k-линейный функционал на E. Пусть $x \in E$ и $y \in F$. Показать, что если E, F неизоморфны, то

$$\sum_{\sigma \in G} \lambda(\sigma x)\sigma^{-1}y = 0.$$

[*Указание*: для фиксированного y отображение $x \longmapsto \sum \lambda(\sigma x)\sigma^{-1}y$ является G-гомоморфизмом E в F.] В частности, для любого функционала μ на F

$$\sum_{\sigma \in G} \lambda(\sigma x)\,\mu(\sigma^{-1}y) = 0.$$

2. Показать, что утверждение упражнения 1 можно применить к каждому коэффициенту матричного представления группы G. В предположении, что

k алгебраически замкнуто и имеет характеристику, не делящую порядок G, вывести соотношение ортогональности $\langle \chi, \psi \rangle = 0$ для двух различных неприводимых характеров χ, ψ группы G над k, где скалярное произведение двух функций f, g на G определяется формулой

$$\langle f, g \rangle = \frac{1}{n} \sum_{\sigma \in G} f(\sigma)\, g(\sigma^{-1}).$$

Как обычно, n обозначает порядок группы G.

3. Пусть k — алгебраически замкнутое поле и E — простое (G, k)-пространство. Тогда любой G-эндоморфизм пространства E равен скалярному кратному тождественного. [*Указание*: тело $\mathrm{End}_{G,k}(E)$ конечномерно над k и, следовательно, совпадает с k.]

4. Пусть поле k алгебраически замкнуто, причем его характеристика не делит порядок G, E — векторное пространство размерности d над k.

(а) Пусть λ — функционал на E, $x \in E$ и $\varphi_{\lambda, x} \in \mathrm{End}_k(E)$ — эндоморфизм, для которого

$$\varphi_{\lambda, x}(y) = \lambda(y)\, x \quad \text{при всех} \quad y \in E.$$

Показать, что $\mathrm{tr}(\varphi_{\lambda, x}) = \lambda(x)$. [*Указание*: элемент $x \neq 0$ дополнить до подходящего базиса E и вычислить след относительно этого базиса.]

(б) Пусть $\rho\colon E \to \mathrm{Aut}_k E$ — простое представление группы G, и пусть x, $y \in E$. Тогда характеристика поля k не делит d и

$$\sum_{\sigma \in G} \lambda(\sigma x)\, \sigma^{-1} y = \frac{n}{d}\, \lambda(y)\, x.$$

Указание: для фиксированного y отображение

$$x \longmapsto \sum_{\sigma \in G} \lambda(\sigma x)\, \sigma^{-1} y$$

есть G-гомоморфизм пространства E в себя; следовательно, оно имеет вид cI для некоторого $c \in k$. В действительности оно равно

$$\sum_{\sigma \in G} \sigma^{-1} \circ \varphi_{\lambda, y} \circ \sigma.$$

Для простоты мы написали σ вместо $\rho(\sigma)$. След этого выражения равен, с одной стороны, $n\,\mathrm{tr}(\varphi_{\lambda, y})$, с другой стороны, dc. Выберем λ, y так, чтобы $\lambda(y) = 1$. Это показывает, что характеристика не делит d, и, значит, c можно выразить требуемым образом.]

(в) Если λ, μ — функционалы на E, то

$$\sum_{\sigma \in G} \lambda(\sigma x)\, \mu(\sigma^{-1} y) = \frac{n}{d}\, \lambda(y)\, \mu(x).$$

5. (а) Пусть χ — характер представления из упражнения 4. Показать, что $\langle \chi, \chi \rangle = 1$. [*Указание*: рассматривая ρ как матричное представление, имеем

$$\chi = \rho_{11} + \ldots + \rho_{dd}.]$$

В частности, если $\chi_1, \ldots, \chi_s$ — простые характеры и если положить

$$e_i = \frac{d_i}{n} \sum_{\sigma \in G} \chi_i(\sigma)\, \sigma^{-1},$$

то $\chi_j(e_i) = \delta_{ij} d_i$.

(б) Считая известным, что $\chi_{\text{reg}}(\sigma) = 0$ для $\sigma \neq 1$ и $\chi_{\text{reg}}(1) = n$, показать, что $\chi_{\text{reg}} = \sum d_i \chi_i$, где d_i — размерность χ_i. [*Указание*: записать $\chi_{\text{reg}} = \sum m_j \chi_j$ и вычислить скалярное произведение с χ_i, пользуясь соотношениями ортогональности, а также определениями.] Значения характера регулярного представления очевидны.

(в) Показать, что каждый элемент e_i может быть представлен в виде суммы классов сопряженных элементов с коэффициентами в k и, следовательно, лежит в центре алгебры $k[G]$.

(г) Пусть E_i — любое пространство представления для χ_i и ρ_i — соответствующее представление G (или $k[G]$) на E_i. Для $\alpha \in k[G]$ пусть $\rho_i(\alpha)$: $E_i \to E_i$ — такое отображение, что $\rho_i(\alpha)x = \alpha x$ для всех $x \in E_i$. Показать, что $\rho_i(e_i) = \mathrm{id}$ и что $\rho_i(e_j) = 0$ при $i \neq j$. [*Указание*: отображение $x \longmapsto e_i x$ в силу (в) есть G-гомоморфизм E_j в себя, и поэтому в соответствии с упражнением 3 является скалярным кратным тождественного. Если взять след и использовать соотношения ортогональности между простыми характерами, то, как тривиально вычисляется, это кратное равно соответственно 1 или 0.]

(д) Показать, что $\sum_{i=1}^{s} e_i = 1$.

(е) Пусть α лежит в центре $k[G]$. Тогда для любого i автоморфизм $\rho_i(\alpha)$ является кратным тождественного на E_i, скажем

$$\rho_i(\alpha) = c_i \rho_i(e_i) = c_i \cdot id_{E_i}, \qquad c_i \in k.$$

Вывести отсюда, что $\alpha = c_1 e_1 + \ldots + c_s e_s$ и что, следовательно, центр $Z_k[G]$ групповой алгебры $k[G]$ над k имеет размерность точно s. В частности, имеется точно s классов сопряженных элементов $\gamma_1, \ldots, \gamma_s$, которые также образуют базис центра $Z_k[G]$. [*Указание*: линейная комбинация $c_1 e_1 + \ldots + c_s e_s$ действует на каждом E_i так же, как и α. Поскольку $k[G]$ изоморфна прямой сумме $\coprod d_i E_i$, отсюда вытекает, что α равно этой линейной комбинации.]

6. Пусть f — функция классов. Показать, что

$$f = \sum_{i=1}^{s} \langle f, \chi_i \rangle \chi_i.$$

Для двух функций классов f, g вывести *формулу Планшереля*, а именно

$$\langle f, g \rangle = \sum_{i=1}^{s} \langle f, \chi_i \rangle \langle \chi_i, g \rangle.$$

7. Пусть $\rho^{(i)}$ обозначает представление унитарными матрицами на E_i и пусть $\rho^{(i)}_{\nu\mu}$ — коэффициенты этих матриц, рассматриваемые как функции на G ($i = 1, \ldots, s$ и $\nu, \mu = 1, \ldots, d_i$). Показать, что эти функции $\{\rho^{(i)}_{\nu\mu}\}$ образуют ортогональный базис относительно эрмитовой метрики пространства функций на G и что, следовательно, для любой функции f (не обязательно функции классов) мы имеем

$$f = \sum_{i=1}^{s} \sum_{\nu,\,\mu} \frac{1}{d_i} \langle f, \rho^{(i)}_{\nu\mu} \rangle \rho^{(i)}_{\nu\mu}.$$

8. Следующий формализм аналогичен артиновскому формализму L-рядов в теории чисел. (См. работу Артина „Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren" (Artin E., Collected papers, 1965), а также Lang S., L-series of a covering, *Proc. Nat. Acad. Sci. USA*, 1956.)

Мы рассматриваем некоторую категорию с объектами $\{U\}$. Как обычно, мы говорим, что конечная группа G действует на U, если задан гомоморфизм ρ: $G \to \mathrm{Aut}(U)$. При этом мы говорим, что U есть G-объект, а также, что ρ есть представление G на U. Мы говорим, что G действует тривиально, если $\rho(G) = \mathrm{id}$. Для простоты мы будем опускать ρ в обозначениях. Под *G-морфизмом* f: $U \to V$ *между G-объектами понимают такой морфизм, что* $f \circ \sigma = \sigma \circ f$ для всех $\sigma \in G$.

Мы будем предполагать, что для всякого G-объекта U существует объект U/G, на котором G действует тривиально, и G-морфизм $\pi_{U,G}$: $U \to U/G$, обладающий следующим универсальным свойством. Для всякого G-морфизма $U \to V$, где V — G-объект, на котором G действует тривиально, существует однозначно определенный морфизм $U/G \to V$, такой, что следующая диаграмма коммутативна:

$$\begin{array}{ccc} U & \to & U/G \\ & \searrow & \swarrow \\ & V & \end{array}$$

Тогда если f: $U \to U'$ — произвольный G-морфизм, то существует однозначно определенный морфизм f/G: $U/G \to U'/G$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} U & \xrightarrow{f} & U' \\ \downarrow & & \downarrow \\ U/G & \xrightarrow[f/G]{} & U'/G \end{array}$$

Показать, в частности, что если H — нормальная подгруппа в G, то G/H *естественным образом действует на* U/H.

Пусть k — алгебраически замкнутое поле характеристики 0. Предположим, что задан некоторый функтор E из нашей категории в категорию конечномерных k-пространств. Если U — объект из нашей категории и $f: U \to U'$ — некоторый морфизм, то получаем гомоморфизм

$$E(f) = f_*\colon E(U) \to E(U').$$

(Читатель может иметь в виду частный случай, когда мы имеем дело с категорией подходящих топологических пространств, а E — гомологический функтор некоторой данной размерности.)

Если G действует на U, то в силу функториальности мы получаем действие G на $E(U)$.

Пусть U — некоторый G-объект, F: $U \to U$ — G-морфизм и $P_F(t) = \prod (t - \alpha_i)$ — характеристический многочлен линейного отображения F_*: $E(U) \to E(U)$. Положим

$$Z_F(t) = \prod (1 - \alpha_i t)$$

и будем называть это выражение *дзета-функцией* F. Если F — тождественный морфизм, то $Z_F(t) = (1-t)^{B(U)}$, где $B(U)$ обозначает $\dim_k E(U)$.

Пусть χ — простой характер группы G, d_χ — размерность простого представления группы G, принадлежащего χ, и $n = (G:1)$. Определим линейное

отображение на $E(U)$, положив

$$e_\chi = \frac{d_\chi}{n} \sum_{\sigma \in G} \chi(\sigma^{-1})\, \sigma_*.$$

Показать, что $e_\chi^2 = e_\chi$ и что для любого положительного целого числа μ имеет место равенство $(e_\chi \circ F_*)^\mu = e_\chi \circ F_*^\mu$.

Пусть $P_\chi(t) = \prod (t - \beta_j(\chi))$ — характеристический многочлен отображения $e_\chi \circ F_*$. Полагаем

$$L_F(t, \chi, U/G) = \prod (1 - \beta_j(\chi)\, t).$$

Показать, что логарифмическая производная этой функции равна

$$-\sum_{\mu=1}^{\infty} \operatorname{tr}\left(e_\chi \circ F_*^\mu\right) t^{\mu-1}.$$

Определяем $L_F(t, \chi, U/G)$ для произвольных характеров по линейности. Если $V = U/G$, то, допуская вольность в обозначениях, мы будем также писать $L_F(t, \chi, U/V)$. Тогда для любых χ, χ' имеем по определению

$$L_F(t, \chi + \chi', U/V) = L_F(t, \chi, U/V)\, L_F(t, \chi', U/V).$$

Сделаем одно дополнительное предположение.

Предположим, что характеристический многочлен отображения

$$\frac{1}{n} \sum_{\sigma \in G} \sigma_* \circ F_*$$

равен характеристическому многочлену F/G на $E(U/G)$. Доказать следующие утверждения:

(а) Если $G = \{1\}$, то

$$L_F(t, 1, U/U) = Z_F(t).$$

(б) Пусть $f = F/G$. Тогда

$$L_F(t, 1, U/V) = Z_f(t).$$

(в) Пусть H — подгруппа в G и ψ — некоторый характер H. Пусть, далее, $W = U/H$ и ψ^* — индуцированный характор с H на G. Тогда

$$L_F(t, \psi, U/W) = L_F(t, \psi^*, U/V).$$

(г) Пусть подгруппа H нормальна в G. Тогда G/H действует на $U/H = W$. Пусть ψ — некоторый характер G/H, χ — характер G, получаемый композицией ψ с каноническим отображением $G \to G/H$, и $\varphi = F/H$ — морфизм, индуцированный на $U/H = W$. Тогда

$$L_\varphi(t, \psi, W/V) = L_F(t, \chi, U/V).$$

(д) Показать, что если $V = U/G$ и $B(V) = \dim_k \mathrm{E}(V)$, то $(1-t)^{B(V)}$ делит $(1-t)^{B(U)}$. Использовать регулярный характер для получения разложения $(1-t)^{B(U)}$ в произведение.

Добавление

Трансцендентность e и π

В приводимом ниже доказательстве мы следуем классическому методу Гельфонда и Шнейдера, надлежащим образом сформулированному. Этот метод основывается на теореме о значениях функций, удовлетворяющих дифференциальным уравнениям. Уже давно было понято, что такие значения подчинены некоторым жестким ограничениям. Здесь мы имеем дело с самым общим алгебраическим дифференциальным уравнением. Литература на эту тему все еще не богата, и бо́льшую ее часть читатель найдет в следующих монографиях:

Гельфонд А. О., Трансцендентные и алгебраические числа, Гостехиздат, 1952.

Schneider T., Einführung in die transcendenten Zahlen, Springer, Berlin, 1957.

Siegel C. L., Transcendental numbers, *Ann. Math. Studies*, *Princeton*, 1949.

Lang S., Introduction to transcendental numbers, Addison — Wesley Publ. Company, 1966.

Приложения и обобщения теоремы, сформулированной в этом добавлении, можно найти в двух моих статьях: Transcendental points on group varieties, *Topology*, **2**, (1963), 313—318, и Algebraic values of meromorphic functions, *Topology*, **3**, (1965), 183—191.

Мы будем предполагать, что читатель знаком с элементарными фактами, касающимися функций комплексного переменного. Пусть f — целая функция (т. е. функция, голоморфная на комплексной плоскости). Мы будем говорить, что f имеет порядок $\leqslant \rho$, если существует число $C > 1$, такое, что для всех достаточно больших R при $|z| \leqslant R$ имеет место неравенство

$$|f(z)| \leqslant C^{R^\rho}.$$

О мероморфной функции говорят, что она имеет порядок $\leqslant \rho$, если она является отношением целых функций порядка $\leqslant \rho$.

Теорема. *Пусть K — конечное расширение поля рациональных чисел, $f_1, \ldots, f_N$ — мероморфные функции порядка $\leqslant \rho$. Предположим, что поле $K(f_1, \ldots, f_N)$ имеет степень трансценденти-*

ности $\geqslant 2$ *над* K *и что дифференцирование* $D = d/dz$ *отображает кольцо* $K[f_1, \ldots, f_N]$ *в себя. Пусть* $w_1, \ldots, w_m$ *— различные комплексные числа, среди которых нет полюсов функций* f_i, *такие, что*

$$f_i(w_\nu) \in K$$

для всех $i = 1, \ldots, N$ *и* $\nu = 1, \ldots, m$. *Тогда* $m \leqslant 10\,\rho\,[K\colon \mathbf{Q}]$.

Следствие 1 (Эрмит — Линдеман). *Если* α *— алгебраическое число (над* $\mathbf{Q}$*), причем* $\alpha \neq 0$, *то* e^α *трансцендентно. В частности, трансцендентно число* π.

Доказательство. Допустим, что числа α и e^α — алгебраические. Положим $K = \mathbf{Q}(\alpha, e^\alpha)$. Две функции z и e^z алгебраически независимы над K (тривиально), и кольцо $K[z, e^z]$, очевидно, отображается в себя при дифференцировании. Наши функции принимают алгебраические значения из K в точках $\alpha, 2\alpha, \ldots, m\alpha$ для любого m — противоречие. Так как $e^{2\pi i} = 1$, то число $2\pi i$ трансцендентно.

Следствие 2. (Гельфонд — Шнейдер). *Если* α *— алгебраическое число* $\neq 0, 1$ *и если* β *— алгебраическое иррациональное число, то* $\alpha^\beta = e^{\beta \log \alpha}$ *трансцендентно.*

Доказательство. Рассуждаем, как в следствии 1, рассматривая функции $e^{\beta t}$ и e^t, которые алгебраически независимы, поскольку β предполагается иррациональным. Чтобы получить противоречие, как и в следствии 1, берем точки $\log \alpha, 2\log \alpha, \ldots, m \log \alpha$.

Прежде чем приводить основные рассуждения, доказывающие теорему, мы сформулируем несколько лемм. Первые две, принадлежащие Зигелю, относятся к целочисленным решениям линейных однородных уравнений.

Лемма 1. *Пусть*

$$\begin{aligned} a_{11}x_1 + \ldots + a_{1n}x_n &= 0, \\ \ldots\ldots\ldots\ldots\ldots & \\ a_{r1}x_1 + \ldots + a_{rn}x_n &= 0 \end{aligned}$$

— система линейных уравнений с целочисленными коэффициентами a_{ij}, *причем* $n > r$. *Пусть* A *— такое число, что* $|a_{ij}| \leqslant A$ *для всех* i, j. *Тогда существует целочисленное нетривиальное решение, для которого*

$$|x_j| \leqslant 2(nA)^{\frac{r}{n-r}}.$$

Доказательство. Рассматриваем нашу систему линейных уравнений как линейное уравнение $L(X) = 0$, где L — линейное отображение $\mathbf{Z}^{(n)} \to \mathbf{Z}^{(n)}$, определяемое матрицей из заданных коэффициентов. Для всякого положительного числа B обозначим через $\mathbf{Z}^{(n)}(B)$ мно-

жество таких векторов X из $\mathbf{Z}^{(n)}$, что $|X| \leqslant B$ (где $|X|$ — максимум абсолютных значений коэффициентов вектора X). Тогда L отображает $\mathbf{Z}^{(n)}(B)$ в $\mathbf{Z}^{(r)}(nBA)$. Число элементов в $\mathbf{Z}^{(n)}(B)$ равно $(2B+1)^n$. Найдем значение B, для которого существуют два различных элемента X, Y из $\mathbf{Z}^{(n)}(B)$, имеющих один и тот же образ $L(X) = L(Y)$. Для этого достаточно, чтобы выполнялось неравенство $(2B+1)^n > (2nBA+1)^r$, и, таким образом, достаточно, чтобы $B = (nA)^{r/(n-r)}$. Берем $X - Y$ в качестве решения нашей задачи.

Пусть K — конечное расширение поля $\mathbf{Q}$ и I_K — целое замыкание $\mathbf{Z}$ в K. Из упражнения 6 гл. IX мы знаем, что I_K — свободный модуль над $\mathbf{Z}$ размерности $[K : \mathbf{Q}]$. Мы считаем поле K содержащимся в поле комплексных чисел. Если $\alpha \in K$, то сопряженным с α будет элемент $\sigma\alpha$, где σ — некоторое вложение K в $\mathbf{C}$. Под *размером* $\operatorname{size}(M)$ некоторого множества M элементов из K мы будем понимать максимум абсолютных величин всех сопряженных с этими элементами.

Под *размером* $\operatorname{size}(X)$ *вектора* $X = (x_1, \ldots, x_n)$ мы будем понимать размер множества его координат.

Пусть $\omega_1, \ldots, \omega_M$ — базис модуля I_K над $\mathbf{Z}$, и пусть $\alpha \in I_K$; запишем

$$\alpha = a_1\omega_1 + \ldots + a_M\omega_M.$$

Пусть $\omega_1', \ldots, \omega_M'$ — дуальный базис к $\omega_1, \ldots, \omega_M$ относительно следа. Тогда мы можем выразить коэффициенты (Фурье) a_j элемента α в виде следов

$$a_j = \operatorname{Tr}(\alpha\omega_j').$$

След — это сумма по сопряженным. Следовательно, размер этих коэффициентов ограничен размером α, умноженным на фиксированную константу, зависящую от размера элементов ω_j'.

Лемма 2. *Пусть K — конечное расширение поля $\mathbf{Q}$ и*

$$\alpha_{11}x_1 + \ldots + \alpha_{1n}x_n = 0,$$
$$\alpha_{r1}x_1 + \ldots + \alpha_{rn}x_n = 0$$

— система линейных уравнений с коэффициентами в I_K, причем $n > r$. Пусть, далее, A — такое число, что $\operatorname{size}(\alpha_{ij}) \leqslant A$ для всех i, j. Тогда существует нетривиальное решение X из I_K, для которого

$$\operatorname{size}(X) \leqslant C_1(C_2nA)^{r/(n-r)},$$

где C_1, C_2 — некоторые константы, зависящие только от K.

Доказательство. Пусть $\omega_1, \ldots, \omega_M$ — базис I_K над $\mathbf{Z}$. Каждая компонента x_j может быть записана в виде

$$x_j = \xi_{j1}\omega_1 + \ldots + \xi_{jM}\omega_M,$$

где $\xi_{j\lambda}$ — неизвестные, а каждый коэффициент α_{ij} — в виде

$$\alpha_{ij} = a_{ij1}\omega_1 + \ldots + a_{ijM}\omega_M,$$

где $a_{ij\lambda} \in \mathbf{Z}$. Если мы перемножим $\alpha_{ij}x_j$, то найдем, что наши линейные уравнения с коэффициентами из I_K эквивалентны системе из rM линейных уравнений от nM неизвестных $\xi_{j\lambda}$ с коэффициентами в $\mathbf{Z}$, размеры которых ограничены константой CA, где C — число, зависящее только от размера элементов ω_λ и произведений $\omega_\lambda\omega_\mu$; другими словами, C зависит только от K. Применяя лемму 1, мы получаем решение в терминах $\xi_{j\lambda}$ и, следовательно, решение X из I_K, размер которого удовлетворяет нужной оценке.

Следующая лемма касается оценок производных. Под *размером* size (P) *многочлена* P с коэффициентами в K мы будем понимать размер множества его коэффициентов. *Знаменателем* для некоторого множества элементов из K будет любое положительное целое рациональное число, произведение которого со всяким элементом из этого множества является целым алгебраическим числом. Аналогичным образом мы определяем знаменатель для многочлена с коэффициентами в K. Сокращенно мы обозначаем „знаменатель“ через den.

Пусть

$$P(T_1, \ldots, T_N) = \sum \alpha_{(\nu)} M_{(\nu)}(T)$$

— многочлен с комплексными коэффициентами и

$$Q(T_1, \ldots, T_N) = \sum \beta_{(\nu)} M_{(\nu)}(T)$$

— многочлен с вещественными коэффициентами $\geqslant 0$. Мы будем говорить, что P *доминируется* многочленом Q, если $|\alpha_{(\nu)}| \leqslant \beta_{(\nu)}$ для всех (ν). Непосредственно проверяется, что отношение доминирования сохраняется при сложении, умножении и взятии частных производных по переменным $T_1, \ldots, T_N$.

Лемма 3. *Пусть K — поле конечной степени над $\mathbf{Q}$ и $f_1, \ldots, f_N$ — функции, голоморфные в некоторой окрестности точки $w \in \mathbf{C}$, причем $D = d/dz$ отображает кольцо $K[f_1, \ldots, f_N]$ в себя. Предположим также, что $f_i(w) \in K$ для всех i. Тогда существует целое число C_1, обладающее следующим свойством. Пусть $P(T_1, \ldots, T_N)$ — многочлен степени $\leqslant r$ с коэффициентами в K, и пусть $f = P(f_1, \ldots, f_N)$. Тогда для всех положительных целых чисел k будем иметь*

$$\text{size}\left(D^k f(w)\right) \leqslant \text{size}(P)\, r^k k!\, C_1^{k+r}.$$

Кроме того, для $D^k f(w)$ найдется знаменатель, ограниченный величиной $\text{den}(P)\, C_1^{k+r}$.

Доказательство. Существуют многочлены $P_i(T_1, \ldots, T_N)$ с коэффициентами в K, такие, что

$$Df_i = P_i(f_1, \ldots, f_N).$$

Пусть h — максимум их степеней. На $K[T_1, \ldots, T_N]$ имеется единственное дифференцирование $\overline{D}$, такое, что $\overline{D}T_i = P_i(T_1, \ldots, T_N)$. Для любого многочлена P имеем

$$\overline{D}(P(T_1, \ldots, T_N)) = \sum_{i=1}^{N} (D_iP)(T_1, \ldots, T_N) \cdot P_i(T_1, \ldots, T_N),$$

где $D_1, \ldots, D_N$ — частные производные. Многочлен P доминируется многочленом

$$\text{size}(P)(1 + T_1 + \ldots + T_N)^r,$$

и каждый P_i доминируется многочленом $\text{size}(P_i)(1 + T_1 + \ldots + T_N)^h$. Таким образом, $\overline{D}P$ доминируется многочленом

$$\text{size}(P)C_2r(1 + T_1 + \ldots + T_N)^{r+h}.$$

По индукции находим, что $\overline{D}^kP$ доминируется многочленом

$$\text{size}(P)C_3^k r^k k!(1 + T_1 + \ldots + T_N)^{r+kh}.$$

Подставляя вместо T_i значения $f_i(w)$, получим искомую оценку для $D^kf(w)$. Второе утверждение, касающееся знаменателей, также доказывается тривиальной индукцией.

Теперь мы переходим к основной части доказательства нашей теоремы. Пусть f, g — две функции из $f_1, \ldots, f_N$, алгебраически независимые над K, r — положительное целое число, делящееся на $2m$. В конце доказательства мы устремим r к бесконечности.

Пусть

$$F = \sum_{l,\, j=1}^{r} b_{ij} f^i g^j$$

имеет коэффициенты b_{ij} из K. Положим $n = r^2/2m$. Можно выбрать b_{ij} так, чтобы они не все равнялись 0 и чтобы

$$D^kF(w_\nu) = 0$$

для $0 \leqslant k < n$ и $\nu = 1, \ldots, m$. Действительно, мы должны решить систему из mn линейных уравнений от $r^2 = 2mn$ неизвестных. Заметим, что

$$\frac{mn}{2mn - mn} = 1.$$

Умножим эти уравнения на знаменатель для коэффициентов. Используя лемму 2 и оценку из леммы 3, мы можем на самом деле взять в качестве b_{ij} целые алгебраические числа, размер которых ограничен

величиной

$$O\left(r^n n!\, C_1^n\right) \leqslant O\left(n^{2n}\right)$$

при $n \to \infty$.

Так как f, g алгебраически независимы над K, то наша функция F не равна тождественно нулю. Пусть s — наименьшее целое число, такое, что все производные от F вплоть до порядка $s-1$ обращаются в нуль во всех точках $w_1, \ldots, w_m$, но $D^s F$ не обращается в нуль в одной из точек w, например в w_1. Тогда $s \geqslant n$. Положим

$$\gamma = D^s F(w_1) \neq 0.$$

Тогда γ есть элемент из K и в силу леммы 3 имеет знаменатель, ограниченный величиной $O\left(C_1^s\right)$ при $s \to \infty$. Пусть c — этот знаменатель. Норма элемента $c\gamma$ из K в $\mathbf{Q}$ есть тогда некоторое ненулевое целое рациональное число. Всякий сопряженный с $c\gamma$ элемент ограничен величиной $O(s^{5s})$. Следовательно, мы получаем

$$1 \leqslant \left| N_Q^K(c\gamma) \right| \leqslant O\left(s^{5s}\right)^{[K:\mathbf{Q}]-1} |\gamma|, \tag{1}$$

где $|\gamma|$ — фиксированное абсолютное значение $|\gamma|$, которое сейчас будет оценено сверху с помощью глобальных соображений.

Пусть θ — целая функция порядка $\leqslant \rho$, такая, что функции θf и θg — целые, причем $\theta(w_1) \neq 0$. Тогда $\theta^{2r} F$ — целая функция. Рассмотрим целую функцию

$$H(z) = \frac{\theta(z)^{2r} F(z)}{\prod_{\nu=1}^{m} (z - w_\nu)^s}.$$

Число $H(w_1)$ отличается от $D^s F(w_1)$ очевидным множителем, ограниченным числом $C_4^s s!$. В силу принципа максимума модуля его абсолютное значение ограничено максимумом H на окружности большого радиуса R. Если мы возьмем R достаточно большим, то разности $z - w_\nu$ будут иметь абсолютные значения, приблизительно равные R, и, следовательно, на окружности радиуса R функция $H(z)$ будет ограничена по абсолютной величине выражением вида

$$\frac{s^{3s} C_5^{2rR^\rho}}{R^{ms}}.$$

Возьмем $R = s^{1/2\rho}$. Тогда получим оценку

$$|\gamma| \leqslant \frac{s^{4s} C_6^s}{s^{ms/2\rho}}.$$

Пусть теперь r стремится к бесконечности. Тогда n и s также стремятся к бесконечности. Комбинируя последнее неравенство с неравенством (1), мы получаем искомую оценку для m. Это завершает доказательство.

Разумеется, мы не заботились особенно о степенях s, встречающихся в оценках, и число 10 может быть, очевидно, уменьшено, если проявить несколько большее внимание к оценкам.

Теорема, которую мы доказали, должна быть лишь простейшим результатом в далеко идущей теории, касающейся проблем степени трансцендентности. В некотором смысле, если не делается дополнительных предположений, эта теорема является наилучшей возможной. Например, если $P(t)$ — многочлен с целыми коэффициентами, то $e^{P(t)}$ будет принимать значение 1 во всех корнях P, которые являются алгебраическими числами. Далее, функции

$$t,\ e^t,\ e^{t^2},\ \ldots,\ e^{t^n}$$

алгебраически независимы, но принимают значения в $\mathbf{Q}(e)$ для всех целочисленных значений t.

Однако можно ожидать, что справедливы значительно более сильные результаты об алгебраической независимости. Линдеман доказал, что *если* $\alpha_1, \ldots, \alpha_n$ *— алгебраические числа, линейно независимые над* $\mathbf{Q}$, *то*

$$e^{\alpha_1},\ \ldots,\ e^{\alpha_n}$$

алгебраически независимы.

Более общо, Шенуэл высказал следующую гипотезу. *Если* $\alpha_1, \ldots, \alpha_n$ — комплексные числа, линейно независимые над $\mathbf{Q}$, то степень трансцендентности множества

$$\alpha_1,\ \ldots,\ \alpha_n,\ e^{\alpha_1},\ \ldots,\ e^{\alpha_n}$$

должна быть $\geqslant n$. (Может быть, необходимо наложить какие-то незначительные ограничения на числа $\alpha_1, \ldots, \alpha_n$, которые, однако, никак не будут влиять на приложения, поскольку все классические числа будут допустимыми.)

Из этого результата можно было бы тотчас вывести алгебраическую независимость e и π (рассмотрев $1,\ 2\pi i,\ e,\ e^{2\pi i}$), а также все другие утверждения о независимости, касающиеся обычной экспоненциальной функции и логарифма, которые, чувствуется, должны быть справедливы, например, утверждение, что π не может лежать в поле, полученном присоединением к алгебраическим числам значений экспоненциальной функции, взятием алгебраического замыкания и итерированием этих двух операций. Такие утверждения относятся к значениям экспоненциальной функции, лежащим в некоторых полях степени трансцендентности $< n$, и можно надеяться, что путем соответствующего углубления теоремы 1 желаемые результаты будут достигнуты.

УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ