ВВЕДЕНИЕ

Истоки алгебры зародились в древних цивилизациях Египта и Древней Греции. Именно там стали изучать действия над целыми и рациональными числами. В Древней Греции были сформулированы знаменитые задачи на построение при помощи циркуля и линейки: задача о триссекции угла, задача об удвоении куба и др.

Мы проследим развитие алгебры на примере решения уравнений. Рассмотрим следующее уравнение

$$a\,x = b. \tag{1}$$

Здесь a и b – некоторые известные числа, а x – неизвестное. Это линейное уравнение от одной неизвестной. Что значит "решить уравнение"? Это значит: найти все его решения или доказать, что решений нет. При этом надо указывать множество в котором ищется решение, так как может оказаться, что в одном множестве решений не существует, но существует в некотором более широком. Под решением уравнения (1) мы понимаем такое число x^0, которое при подстановке в уравнение вместо неизвестной, приводит к верному равенству.

При изучении любого уравнения (или системы уравнений) нас интересуют следующие два вопроса: имеет ли данное уравнение решение и если ответ утвердительный, то как найти все множество решений? Из школьного курса алгебры известно, что уравнение (1) разрешимо тогда и только тогда, когда a отлично от нуля, либо, когда $a = b = 0$. В первом случае решение единственно и определяется равенством $x = a^{-1}\,b$, а во втором случае решением является любое число.

Более сложным по сравнению с (1) является уравнение

$$a\,x^2 + b\,x + c = 0, \quad a \neq 0. \tag{2}$$

где опять a, b, c – заданные числа, а x – неизвестная. Это так называемое *квадратичное уравнение* от одной неизвестной. Такие уравнения умели решать еще в IX в. на Востоке. В это же время возник и сам термин "алгебра". Решения уравнения (2) определяются по формуле

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4\,a\,c}}{2\,a}. \tag{3}$$

Теперь мы можем пойти дальше и определить алгебраическое уравнение степени n от одной неизвестной:

$$a_0\,x^n + a_1\,x^{n-1} + \ldots + a_{n-1}\,x + a_n = 0, \quad a_0 \neq 0. \tag{4}$$

Что известно про решения таких уравнений? При $n = 3$ известна *формула Кардано*, похожая на формулу (3), которая позволяет найти корни любого уравнения

третьей степени. При $n = 4$ существует *метод Феррари*, позволяющий сводить решение уравнения 4-й степени к решению уравнения 3-й степени. Формулы для решения уравнений 3-й и 4-й степени были получены итальянскими математиками: Кардано, Тарталья, феррари в XVI в. После этого многие математики пытались найти аналогичные формулы для решения общего уравнения 5-й степени. Эти попытки продолжались до тех пор, пока в XIX в. А. Руффини (1765–1822) и Н. Абель (1802–1829) не доказали, что общее уравнение (4) при $n \geq 5$ не разрешимо в радикалах, т. е. не существует формул, выражающих решение произвольного уравнения через коэффициенты при помощи основных алгебраических операций: сложения, вычитания, умножения, деления, возведения в степени извлечения корня. Подчеркнем, что речь идет именно об уравнении общего вида, так как легко указать конкретные уравнения сколь угодно высокой степени, разрешимые в радикалах. Например, уравнение

$$x^{100} - 3\,x^{50} + 2 = 0$$

сотой степени легко сводится к квадратному уравнению.

Французский математик Эварист Галуа (1811–1832), занимаясь условиями разрешимости уравнения в радикалах, создал теорию, которая в настоящее время называется *теорией Галуа*. Эту теорию можно считать началом современной алгебры. Э. Галуа впервые ввел такие понятия, как *группа*, *поле*, *автоморфизм*. Помимо критерия разрешимости уравнения в радикалах теория Галуа позволяет доказать неразрешимость задачи о трисекции угла, задачи об удвоении куба и ряда других задач, сформулированных еще в Древней Греции.

Интересна судьба Э. Галуа. По нашим меркам у него не было даже высшего образования. При поступлении в Политехническую школу Галуа провалился на экзамене по математике, запустив тряпку для стирания с доски в голову экзаменатора, посчитав его вопросы слишком тривиальными. В 1829 г. Галуа поступил в Нормальную школу, из которой был отчислен за свои политические убеждения. Затем сидел в тюрьме и в 1832 г. убит на дуэли. За свою жизнь он написал несколько работ, которые представил во французскую Академию наук. К сожалению, некоторые из них были потеряны, а некоторые не получили признания современников. После этого имя Эвариста Галуа надолго было предано забвению. Все его математические работы попали к Огюсту Шевалье, но тот не смог найти никого, кто согласился бы их издать. Только в 1846 г. Ж. Лиувиль впервые опубликовал их в основанном им математическом журнале.

Математические работы Галуа составляют шестьдесят небольших страниц. Никогда еще труды столь малого объема не доставляли автору такой широкой известности. Через несколько десятков лет после смерти Галуа немецкий математик Давид Гильберт назвал теорию Галуа “установлением определенного остова понятий”. Сам галуа так писал о цели своих исследований: “Подчинить вычисления своей воле,

сгруппировать математические операции, научиться их классифицировать по степени трудности, а не по внешним признакам – вот задачи математиков будущего так, как я их понимаю, вот путь, по которому я хочу пойти."

Мы разобрали одно из возможных обобщений уравнения (1), получив при этом уравнение n-й степени от одной неизвестной. Возможно и обобщение в другом направлении. Сохраним условие линейности, но будем рассматривать уравнения, зависящие от нескольких неизвестных. Придем к *системе линейных уравнений.* Систему m линейных уравнений от n неизвестных можно записать в виде

$$\begin{cases} a_{1,1}\,x_1 + a_{1,2}\,x_2 + \ldots + a_{1,n}\,x_n = b_1, \\ a_{2,1}\,x_1 + a_{2,2}\,x_2 + \ldots + a_{2,n}\,x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m,1}\,x_1 + a_{m,2}\,x_2 + \ldots + a_{m,n}\,x_n = b_m, \end{cases}$$

где $a_{i,j}, b_i$ – заданные числа, а x_j – неизвестные. При исследовании системы нас будут интересовать следующие вопросы: разрешима ли система? как описать все множество решений? *Решением* мы называем упорядоченную n-ка чисел $x^0 = (x_1^0, x_2^0, \ldots, x_n^0)$, которые при подстановке в систему дают верные равенства. Системы такого вида хорошо изучены и научимся отвечать на оба поставленных вопроса.

Если ввести следующие таблицы

$$A = \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \ldots & \ldots & \ldots \\ a_{m,1} & \ldots & a_{m,n} \end{pmatrix}, \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

которые называются *матрицей системы*, *столбцом неизвестных* и *столбцом свободных членов*, то нашу систему можно записать в виде

$$A\,X = B.$$

Сравните эту запись с уравнением (1). Видим, что по форме они очень похожи. Более того, иногда решение системы можно находить по формуле $X = A^{-1}\,B$.

ОБОЗНАЧЕНИЯ

Введем обозначения, которые будем использовать на протяжении нашего курса. Символом

$$A = \{a_1, a_2, \ldots\}$$

обозначается множество A, состоящее из элементов $a_1, a_2, \ldots$. Запись $a \in A$ означает, что элемент a принадлежит множеству A; запись $a \notin A$ означает, что a не принадлежит множеству A. Если B является подмножеством множества A, то символически это обозначается так $B \subseteq A$. Пустое множество будем обозначать символом $\emptyset$. Если $A = \{a_1, a_2, \ldots, a_n\}$ – конечное множество, то символом $|A| = n$ обозначается число элементов множества A.

Для числовых множеств будем использовать следующие обозначения:

$$\mathbb{N} = \{1, 2, \ldots\}$$

– *множество натуральных чисел*;

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$$

– *множество целых чисел*;

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N} \right\}$$

– *множество рациональных чисел*; символом $\mathbb{R}$ будем обозначать множество вещественных чисел, которое можно представлять как множество точек на вещественной оси;

$$\mathbb{R}_+ = \{r \in \mathbb{R} \mid r > 0\}$$

– множество положительных вещественных чисел;

$$\mathbb{R}_{\geq 0} = \{r \in \mathbb{R} \mid r \geq 0\}$$

– множество неотрицательных вещественных чисел;

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}, i^2 = -1\}$$

– *множество комплекснных чисел.*

Если $A_1, A_2, \ldots, A_n$ – непустые множества, то их *декартовым произведением* $A_1 \times A_2 \times \ldots \times A_n$ называется множество упорядоченных n-ок:

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i\}.$$

В частности, если $A_1 = A_2 = \ldots = A_n = A$, то декартово произведение $A_1 \times A_2 \times \ldots \times A_n$ называется n-й *декартовой степенью* множества A и обозначать A^n.

Отображение множества A в множество B будем обозначать либо

$$\varphi : A \longrightarrow B \text{ либо } A \xrightarrow{\varphi} B.$$

Если $a \in A$, то образ элемента a при отображении φ обозначается либо $\varphi(a)$, либо $a\varphi$.

Г л а в а 1

ОСНОВНЫЕ ПОНЯТИЯ АЛГЕБРЫ

§ 1. Алгебраическая система. Изоморфизм

1.1. Алгебраическая операция, алгебраическая система. Множества и отображения на них – вот два основных объекта, к изучению которых сводится любая математическая теория. Пусть задано некоторое непустое множество A и функция $f : A^n \longrightarrow A$, аргументы которой пробегают множество A и она принимает при этом значения из A. В этом случае мы говорим, что на множестве A определена n-арная *алгебраическая операция.* В частности, если $n = 1$, то операция называется *унарной,* если $n = 2$, то – *бинарной,* если $n = 3$, то – *тернарной* и т. д.

В школьном курсе вы уже встречались с такими операциями как сложение и умножение. При этом для их обозначения используется не функциональная запись $f(x, y)$, более привычная: $x + y$ и $x \cdot y$. В дальнейшем мы тоже будем использовать подобные обозначения для бинарных операций.

Как следует из определения, всякая алгебраическая операция определена на некотором множестве. Поэтому можно дать такое

О п р е д е л е н и е. *Алгебраической системой* называется непустое множество A с определенными на нем алгебраическими операциями:

$$\mathfrak{A} = \langle A;\ f_i\,(i \in I)\rangle,$$

где I – некоторое множество индексов, конечное или бесконечное.

Чтобы проиллюстрировать это понятие, приведем

П р и м е р ы алгебраических систем:

1) $\mathfrak{A}_1 = \langle$ {действительные числа}; взятие среднего арифметического, умножение на $10\rangle = \langle \mathbb{R}; \frac{a+b}{2}, 10a\rangle$;

3) $\mathfrak{A}_2 = \langle$ {положительные действительные числа}; взятие среднего геометрического, возведение в 10-ю степень$\rangle = \langle \mathbb{R}_+; \sqrt{ab}, a^{10}\rangle$;

2) $\mathfrak{A}_3 = \langle$ {точки на плоскости}; взятие центра тяжести треугольника с заданными вершинами$\rangle$.

Как видно уже из этих примеров алгебраических систем существует достаточно много и изучать все системы довольно проблематично. Определяемое ниже понятие изоморфизма позволяет сократить число изучаемых систем.

1.2. Изоморфизм алгебраических систем. Заданы две алгебраические системы

$$\mathfrak{A} = \langle A;\ f_i\,(i \in I)\rangle, \quad \mathfrak{A}' = \langle A';\ f_i'\,(i \in I)\rangle$$

с одинаковыми наборами алгебраических операций (т. е. арность операции f_i равна арности операции f_i' для всех $i \in I$). Пусть установлено взаимно однозначное отображение

$$\varphi : A \longrightarrow A',$$

множества A *на* множество A', которое сохраняет операции, т. е. φ такое отображение для которого выполняются следующие свойства:

1) φ – *однозначно*, т. е. одному элементу из A соответствует один элемент из A';

2) φ – *универлентно*, т. е. два разных элемента из A переходят в два разных элемента из A';

3) φ – отображение *на*, т. е. для всякого $a' \in A'$ существует $a \in A$ такой, что $a\varphi = a'$;

4) φ *сохраняет операции*, т. е. для всех индексов $i \in I$ и всех наборов $a_1, \ldots, a_{n_i}$ элементов из A справедливо равенство

$$f_i(a_1, \ldots, a_{n_i})\varphi = f_i'(a_1\varphi, \ldots, a_{n_i}\varphi),$$

где n_i – арность операции f_i. В этом случае φ называется *изоморфным отображением* или *изоморфизмом* системы $\mathfrak{A}$ на систему $\mathfrak{A}'$. При этом системы $\mathfrak{A}$ и $\mathfrak{A}'$ называются *изоморфными*, что символически записывается так: $\mathfrak{A} \simeq \mathfrak{A}'$.

Изоморфные системы с алгебраической точки зрения одинаковы, т. е. все свойства системы $\mathfrak{A}$ выполняются и в $\mathfrak{A}'$. Поэтому в алгебре их не различают или рассматривают как точные копии друг друга – подобно тому, как мы не различаем экземпляров одного и того же романа, напечатанных разным шрифтом и на разной бумаге, если интересуемся только содержанием романа. Теперь мы можем дать определение нашего предмета. *Алгебра* – это наука, изучающая алгебраические системы с точностью до изоморфизма.

П р и м е р изоморфных систем. Покажем, что алгебраические системы $\mathfrak{A}_1$ и $\mathfrak{A}_2$ из приведенного выше примера изоморфны. Рассмотрим отображение

$$\varphi : \mathbb{R} \longrightarrow \mathbb{R}_+,$$

определенное правилом $a\varphi = 2^a$. Из школьного курса известно, что φ – взаимно однозначно и *на*. Чтобы проверить, что φ сохраняет операции, мы должны проверить следующие два равенства

$$\left(\frac{a+b}{2}\right)\varphi = \sqrt{a\varphi \cdot b\varphi},$$

$$(10a)\varphi = (a\varphi)^{10},$$

справедливость которых следует из свойств показательной функции.

У п р а ж н е н и е. Для всякого натурального числа n на множестве целых чисел определим унарную операцию f_n, правилом $f_n(x) = nx$. Докажите, что алгебраическая система $U_2 = \langle \mathbb{Z}; f_2 \rangle$ изоморфна алгебраической системе $U_3 = \langle \mathbb{Z}; f_3 \rangle$.

У п р а ж н е н и е. Для каких натуральных n и m имеет место изоморфизм $U_n \simeq U_m$?

Множество, с определенной на нем одной унарной операцией называется *унаром.* Это простейшая (в смысле определения) алгебраическая система.

1.3. Подсистема. *Подсистемой* алгебраической системы $\mathfrak{A} = \langle A;\ f_i\,(i \in I) \rangle$ называется такое подмножество B множества A, которое замкнуто относительно сужений операций f_i на B т. е. эти операции являются алгебраическими и на B (они называются *индуцированными*) и множество B само является алгебраической системой $\mathfrak{B} = \langle B;\ f_i|_B\,(i \in I) \rangle$ относительно индуцированных операций. Если $\mathfrak{B}$ является подсистемой системы $\mathfrak{A}$, то $\mathfrak{A}$ называется *надсистемой* системы $\mathfrak{B}$.

П р и м е р. Подсистемой алгебраической системы $\mathfrak{A} = \langle \mathbb{Z}; + \rangle$ является система $\mathfrak{B} = \langle 2\mathbb{Z}; + \rangle$, где $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ – множество четных чисел.

В этом параграфе мы ввели основные понятия: алгебраическая система, подсистема, изоморфизм. Далее будем изучать конкретные алгебраические системы: группы, кольца, поля, векторные пространства и в них рассматривать подгруппы, подкольца, подполя, подпространства, а также интерпретировать понятие изоморфизма.

§ 2. Группы

2.1. Аксиоматика. Некоторые алгебраические системы столь часто встречаются в различных областях математики, что их изучение стало предметом самостоятельных теорий. Именно таково понятие группы – предмет теории групп. Группа – это множество с одной бинарной операцией, подчиняющейся некоторым аксиомам. В теории групп бинарную операцию называют обычно умножением и обозначают точкой (которую почти всегда опускают), реже используют $+$, $\odot$, $*$ и другие символы. Запись операции точкой называют еще *мультипликативной записью*, а запись плюсом – *аддитивной записью.*

О п р е д е л е н и е. *Группой* называется алгебраическая система $\langle G; \cdot \rangle$ с одной бинарной операцией $\cdot$, для которой выполнены следующие аксиомы:

1. Операция *ассоциативна*, т. е. $(ab)c = a(bc)$ для любых a, b, c из G.

2. Операция гарантирует единицу, т. е. в G существует такой элемент e – он называется *единицей*, – что $ae = ea = a$ для любого a из G.

3. Операция гарантирует обратные элементы, т. е для любого a из G существует в G такой элемент x – он называется *обратным* к a, – что $ax = xa = e$.

В дальнейшем, если понятно о какой операции идет речь, будем обозначать группу, определенную на множестве G тем же символом G.

Установим некоторые следствия из определения.

С л е д с т в и е 1. *В каждой группе существует единственный единичный элемент.*

Действительно, пусть e' и e'' – единичные элементы группы G. Тогда $e'e'' = e''$, с другой стороны $e'e'' = e'$. Следовательно $e' = e''$.

С л е д с т в и е 2. *В каждой группе для каждого a существует единственный обратный элемент, который будем обозначать символом a^{-1}.*

Действительно, предположим, что x и y – два обратных для элемента a. Рассмотрим равенство $(xa)y = x(ay)$, справедливое в силу аксиомы ассоциативности. По определению обратного элемента, левая часть этого равенства равна

$$(xa)y = ey = y,$$

аналогичным образом преобразуем правую часть:

$$x(ay) = xe = x.$$

Следовательно $x = y$.

С л е д с т в и е 3. *Для любых элементов a, b группы G справедливо равенство* $(ab)^{-1} = b^{-1}a^{-1}$.

Действительно,

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e.$$

Благодаря ассоциативности в группах элемент $(ab)c = a(bc)$ можно записывать просто как abc, по той же причине однозначно определено произведение n элементов $a_1a_2 \dots a_n$ – без указания скобок, но в указанном порядке. Произведение n элементов, равных a, называется n-й *степенью* элемента a и обозначается a^n. Полагают, далее, $a^0 = e$ и для $n < 0$ $a^n = (a^{-n})^{-1}$ или $a^n = (a^{-1})^{-n}$, что, как легко видеть, одно и то же.

У п р а ж н е н и е. Если a – произвольный элемент группы, m, n – целые числа, то $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

О п р е д е л е н и е. Группа $\langle G;\cdot\rangle$ называется *коммутативной* или *абелевой* если операция $\cdot$ удовлетворяет следующей аксиоме коммутативности: для любых a, b из G справедливо равенство $ab = ba$.

Операцию в абелевой группе обычно обозначают символом $+$, единичный элемент называют *нулевым элементом* и обозначают символом 0, а обратный к элементу $a \in G$ называю *противоположным* и обозначают символом $-a$.

П р и м е р ы групп:

1) $\langle\mathbb{Z};+\rangle$ – множество целых чисел относительно операции сложения;

2) $\langle 2\mathbb{Z};+\rangle$ – множество четных чисел относительно операции сложения;

3) $\langle\mathbb{Q}^*;\cdot\rangle$ – множество ненулевых рациональных чисел относительно операции умножения;

4) $\langle\{$вращения квадрата$\}$; композиция вращений$\rangle$.

Нетрудно проверить, что все эти группы являются абелевыми.

2.2. Изоморфизм. В соответствии с общим определением изоморфизма алгебраических систем, группы $\langle G;\cdot\rangle$ и $\langle G';\odot\rangle$ называются *изоморфными,* если существует взаимно однозначное отображение φ множества G *на* множество G', сохраняющее операцию умножения, т. е. выполнены следующие условия:

1) φ – однозначно,

2) φ – унивалентно,

3) φ – отображение *на*,

4) для любых элементов $x, y \in G$ справедливо равенство

$$(x\cdot y)\varphi = x\varphi\odot y\varphi.$$

Например, множество $\mathbb{R}_+$ положительных действительных чисел – группа относительно обычного умножения чисел, множество $\mathbb{R}$ всех действительных чисел – группа относительно обычного сложения чисел, а отображение $\varphi:\mathbb{R}_+\longrightarrow\mathbb{R}$, определяемое формулой $a\varphi = \log_2 a$, – изоморфизм $\mathbb{R}_+$ на $\mathbb{R}$.

2.3. Подгруппы. Подмножество группы G называется ее *подгруппой,* если оно замкнуто относительно операции, имеющейся в G и само является группой относительно индуцированной операции. Если H – подгруппа группы G, то пишем $H \le G$.

П р и м е р ы.

1. Группа $\langle\mathbb{Z};+\rangle$, ее подгруппа $\langle 2\mathbb{Z};+\rangle$.

2. Группа $\langle\mathbb{R}_+;\cdot\rangle$ не является подгруппой группы $\langle\mathbb{R};+\rangle$, так как имеет другую операцию.

Сформулируем необходимые и достаточные условия того, что некоторое подмножество является подгруппой.

Л е м м а 1. *Подмножество $H \subseteq G$ является подгруппой группы G в том и только том случае, когда выполнены следующие два условия*:

а) *из того, что* $a, b \in H$ *следует, что и* $ab \in H$ (*замкнутость относительно умножения*);

б) *из того, что* $a \in H$ *следует, что и* $a^{-1} \in H$ (*замкнутость относительно взятия обратного*).

Д о к а з а т е л ь с т в о. Если H является подгруппой, то очевидно, что условия а) и б) выполняются.

Покажем теперь, что если выполнены условия а) и б) то H является подгруппой. Для этого надо проверить аксиомы группы.

1. Аксиома ассоциативности $(ab)c = a(bc)$ выполнена для H, так как она выполняется для G.

3. Аксиома существования обратного элемента следует из условия б).

2. Пусть $a \in H$; по условию б) $a^{-1} \in H$, найдем $aa^{-1} = e$ и по условию а) $e \in H$.

Лемма доказана.

Условия леммы (замкнутость относительно умножения и взятия обратного) символически записывают так:

$$HH \subseteq H, \quad H^{-1} \subseteq H.$$

Установим следующее утверждение

Л е м м а 2. *Пересечение любого семейства подгрупп некоторой группы является подгруппой.*

Д о к а з а т е л ь с т в о. Пусть в группе G задано семейство подгрупп H_α, $\alpha \in J$. Рассмотрим их пересечение $H = \bigcap_{\alpha \in J} H_\alpha$. Покажем, что H – подгруппа группы G. По предыдущей лемме достаточно доказать, что для H выполнены условия а) и б). Выберем два элемента $a, b \in H$. Тогда $a, b \in H_\alpha$ для любого индекса $\alpha \in J$. Так как H_α – группа, то $ab \in H_\alpha$. Следовательно, $ab \in H$ и условие а) установлено. Рассмотрим элемент $a \in H$. Тогда обратный элемент $a^{-1} \in H_\alpha$ для любого индекса $\alpha \in J$. Так как H_α является группой, то существует обратный элемент $a^{-1} \in H_\alpha$ для всех $\alpha \in J$. Следовательно, $a^{-1} \in H$ и условие б) справедливо. Таким образом, пересечение H является подгруппой.

2.4. Порождающие множества. Если M – некоторое подмножество группы G, то пересечение (M) всех подгрупп, содержащих M, называется подгруппой, *порожденной множеством* M, а само M – *порождающим множеством* подгруппы (M):

$$(M) = \bigcap_{H \leq G, M \subseteq H} H.$$

В этом случае говорят, что элементы множества M являются *порождающими элементами* подгруппы (M). Подгруппу (M) иногда обозначают также через $\mathrm{гр}(M)$.

Т е о р е м а. *Если* M *– подмножество группы* G, *то*

$$(M) = \{m_1^{\varepsilon_1} m_2^{\varepsilon_2} \ldots m_n^{\varepsilon_n} \mid m_i \in M, \varepsilon_i = \pm 1, n = 1, 2, \ldots\}.$$

Д о к а з а т е л ь с т в о. Обозначим правую часть через H. Так как подгруппа (M) содержит все m_i из M, то справедливо включение $(M) \supseteq H$. С другой стороны, очевидно, что $HH \subseteq H$, $H^{-1} \subseteq H$, поэтому ввиду леммы 1 множество H – подгруппа, содержащая M. Отсюда $H \supseteq (M)$ и окончательно $H = (M)$.

Укажем порождающие множества некоторых, встречавшихся ранее групп.

П р и м е р ы.

1) $\mathbb{Z} = (1)$, т. е группа целых чисел по сложению порождается единицей;

2) $\mathbb{Q} = \left(\frac{1}{n} \mid n = 1, 2, \ldots\right)$;

3) $\mathbb{Q}^* = (-1, 2, 3, 5, 7, 11, \ldots)$.

Подгруппа, порожденная одним элементом a называется *циклической.* По теореме она состоит из всевозможных степеней порождающего элемента:

$$(a) = \{a^n \mid n = 0, \pm 1, \pm 2, \ldots\}.$$

Как видно из примера 1 группа $\mathbb{Z}$ является циклической. В следующем параграфе мы познакомимся с конечными циклическими группами. Все они устроены довольно просто. Если же мы рассмотрим группы порожденные двумя элементами, то таких групп существует очень много. Более того, знаменитая теорема Хигмана, утверждает, что всякая счетная группа является подгруппой некоторой двупорожденной группы.

§ 3. Кольца и поля

3.1. Определения и примеры. В школьном курсе вы уже встречались с множествами, на котором определены операции сложения и умножения. Таковыми, в частности, являются целые числа, рациональные, вещественные. Это и есть примеры колец и полей. В этом параграфе мы дадим формальные определения.

О п р е д е л е н и е. *Кольцом* называется алгебраическая система $\langle K; +, \cdot \rangle$ с двумя бинарными операциями ($+$ – сложение, $\cdot$ – умножение), для которых выполнены следующие аксиомы:

С1. Сложение *ассоциативно*, т. е. $(a + b) + c = a + (b + c)$ для любых a, b, c из K.

С2. Сложение *коммутативно*, т. е. $a + b = b + a$ для любых a, b из K.

С3. Существование нулевого элемента, т. е в K существует такой элемент 0 – он называется *нулем*, – что $a + 0 = a$ для любого a из K.

С4. Существование противоположного элемента, т. е. для любого a из K существует в K такой элемент x – он называется *противоположным* к a, – что $a + x = 0$.

У1. Умножение *ассоциативно*, т. е. $a(bc) = (ab)c$ для любых a, b, c из K.

СУ1. Сложение и умножение удовлетворяют правой дистрибутивности, т. е. $(a + b)c = ac + bc$ для любых a, b, c из K.

СУ2. Сложение и умножение удовлетворяют левой дистрибутивности, т. е. $c(a + b) = ca + cb$ для любых a, b, c из K.

Иными словами, по сложению K является абелевой абелевой группой (выполнены аксиомы С1 – С4); по умножению K является полугруппой. *Полугруппой* называется алгебраическая система с одной бинарной ассоциативной операцией.

Так же, как и для групп можно показать, что нулевой элемент единственный и для всякого элемента a из K существует единственный противоположный, который будем обозначать символом $-a$.

П р и м е р ы колец:

1. Множество целых (рациональных, вещественных чисел) с операциями сложения и умножения является кольцом.

2. Множество натуральных чисел с этими же операциями кольцом не является.

3. Рассмотрим множество функций

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$

определенных для всех вещественных значений x и принимающих вещественные значения. Если определить операции сложения и умножения функций по правилу

$$(f + g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x),$$

то множество функций с этими операциями является кольцом.

Укажем некоторые следствия из аксиом кольца.

С л е д с т в и е. *Во всяком кольце произведение любого элемента на нулевой элемент есть нулевой элемент.*

Действительно,

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 = 0.$$

Прибавляя к обеим частям этого равенства по элементу $-(a \cdot 0)$, получим, что $a \cdot 0 = 0$. Аналогично доказывается, что $0 \cdot a = 0$.

О п р е д е л е н и е. *Полем* называется алгебраическая система $\langle P; +, \cdot \rangle$ с двумя бинарными операциями ($+$ – сложение, $\cdot$ – умножение), для которых выполнены следующие аксиомы:

С1. Сложение *ассоциативно*, т. е. $(a + b) + c = a + (b + c)$ для любых a, b, c из P.

С2. Сложение *коммутативно*, т. е. $a + b = b + a$ для любых a, b из P.

С3. Существование нулевого элемента, т. е в P существует такой элемент 0 – он называется *нулем*, – что $a + 0 = a$ для любого a из P.

С4. Существование противоположного элемента, т. е. для любого a из P существует в P такой элемент x – он называется *противоположным* к a, – что $a + x = 0$.

У1. Умножение *ассоциативно*, т. е. $a(bc) = (ab)c$ для любых a, b, c из P.

У2. Умножение *коммутативно*, т. е. $ab = ba$ для любых a, b из P.

У3. Существование единичного элемента, т. е. в P существует такой элемент $1 \neq 0$ – он называется *единицей*, что $1a = a$ для любого a из P.

У4. Существование обратного элемента, т. е. для любого a из P отличного от нуля существует в P такой элемент y – он называется *обратным* к a, – что $ay = 1$.

СУ. Дистрибутивность, т. е. $(a + b)c = ac + bc$ для любых a, b, c из P.

Нетрудно показать, что в поле существует единственный нулевой элемент и единственный единичный элемент; противоположный и обратный к a определяются единственным образом и обозначаются соответственно $-a$ и a^{-1}.

Каждое поле является кольцом. С другой стороны, поле можно определить как кольцо в котором выполнены аксиомы У2–У4. Если положить $P^* = P \setminus \{0\}$, то $\langle P^*; \cdot\rangle$ – группа. Она называется *мультипликативной группой поля*. Из аксиомы У3 следует, что поле содержит по крайней мере два элемента. В силу коммутативности умножения в поле правая дистрибутивность равносильна левой дистрибутивности.

П р и м е р поля. Множество рациональных (вещественных) чисел с операциями сложения и умножения образует поле.

Существуют кольца, которые не являются полями. Например, кольцо целых чисел не является полем.

3.2. Кольца вычетов. Существуют кольца состоящие из конечного числа элементов.

П р и м е р. Рассмотрим алгебраическую систему $\langle\{\overline{0}, \overline{1}, \overline{2}\}; +, \cdot\rangle$, где операции сложения и умножения определены правилами

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Нетрудно проверить, что полученная алгебраическая система является кольцом и полем.

П р и м е р. Алгебраическая система $\langle\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}; +, \cdot\rangle$, в которой операции сложения и умножения определены правилами

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

является кольцом, но не полем (проваливается аксиома У4).

Разобранные примеры являются частными случаями общего семейства *колец вычетов по модулю* n. Будем обозначать символом $\mathbb{Z}_n$ множество остатков от деления целых чисел на n. Для произвольного целого числа a символом $\overline{a}$ будем обозначать

остаток от деления a на n. Определим на множестве $\mathbb{Z}_n$ операции сложения и умножения по правилу

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

У п р а ж н е н и е. Алгебраическая система

$$\mathbb{Z}_n = \langle \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}; +, \cdot \rangle$$

всегда является кольцом, но полем является тогда и только тогда, когда n – простое число.

Нетрудно видеть, что если мы рассмотрим множество $\mathbb{Z}_n$ только относительно операции сложения, то оно является абелевой группой, которая порождается элементом $\overline{1}$, т. е. является циклической. Таким образом, мы знаем два примера циклических групп: $\mathbb{Z}$ и $\mathbb{Z}_n$. Оказывается, что с точностью до изоморфизма ими и исчерпываются все циклические группы.

У п р а ж н е н и е. Любая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$, любая циклическая группа конечного порядка n изоморфна группе $\mathbb{Z}_n$.

Порядком конечной группы мы называем число ее элементов.

У п р а ж н е н и е. Пусть $n \in \mathbb{N}$. Существует поле из n элементов тогда и только тогда, когда n – степень простого числа.

3.3. Делители нуля. Рассматривая кольцо вычетов $\mathbb{Z}_4$, видим, что $\overline{2} \cdot \overline{2} = \overline{0}$, т. е. произведение двух ненулевых элементов равно нулю.

О п р е д е л е н и е. Если в кольце K найдутся ненулевые элементы a и b такие, что $a \cdot b = 0$, то они называются *делителями нуля.*

Делители нуля существуют не только в конечных кольцах, но и в бесконечных.

П р и м е р. Покажем, что кольцо вещественных функций обладает делителями нуля. Действительно, полагая

$$f(x) = \begin{cases} 0 & \text{при} \quad x \le 0, \\ x & \text{при} \quad x > 0, \end{cases} \qquad g(x) = \begin{cases} x & \text{при} \quad x \le 0, \\ 0 & \text{при} \quad x > 0, \end{cases}$$

видим, что обе эти функции отличны от нуля, а их произведение равно нулю, т. е. функции, которая при любом x принимает значение 0.

У п р а ж н е н и е. Никакое поле не содержит делителей нуля.

Именно это свойство вещественных чисел и имелось в виду, когда в школе вас учили, что если произведение двух выражений равно нулю, то хотя бы одно из них равно нулю.

Из отсутствия делителей нуля в кольце K вытекает, что любое равенство можно сократить на ненулевой общий множитель. Действительно, если $c\,a = c\,b$, $a, b, c \in K$, и $c \neq 0$, то $c\,(a-b) = 0$, откуда заключаем, что $a - b = 0$, т. е. $a = b$.

3.4. Характеристика поля. Если P – поле, то в нем есть единица 1. Возьмем ее и будем складывать с собой. Возможно, что на некотором шаге получим 0. Если впервые 0 получим на m-м шаге:

$$\underbrace{1+1+\ldots+1}_{m}=0,$$

то говорим, что *характеристика поля* P равна m.

Как мы знаем, в числовых полях такое невозможно. В этом случае говорим, что поле имеет характеристику 0. Примерами полей конечной характеристики служат все конечные поля; существую, впрочем, и бесконечные поля, имеющие конечную характеристику.

Если поле имеет характеристику 2, то $1+1=0$, а потому и для любого элемента $a\in P$ сумма $a+a=0$, т. е. каждый элемент есть противоположный к себе.

У п р а ж н е н и е. Характеристика поля – либо 0, либо – простое число.

3.5. Изоморфизм для колец и полей. Два кольца K и K' *изоморфны,* если существует взаимно однозначное отображение *на*

$$\varphi : K \longrightarrow K'$$

такое, что для всех $a, b \in K$ справедливы равенства:

$$(a+b)\varphi = a\varphi + b\varphi,$$

$$(ab)\varphi = a\varphi \cdot b\varphi.$$

П р и м е р. Рассмотрим кольцо $\langle\{\overline{0},\overline{1}\};+,\cdot\rangle$, состоящее из двух элементов с операциями сложения и умножения, заданными таблицами

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

и другое кольцо $\langle\{$ н, ч $\};+,\cdot\rangle$ для которого

$+$	ч	н
ч	ч	н
н	н	ч

$\cdot$	ч	н
ч	ч	ч
н	ч	н

Нетрудно проверить, что эти два кольца изоморфны, если установить соответствие:

$$\overline{0} \longmapsto \text{ч}, \quad \overline{1} \longmapsto \text{н}.$$

3.6. Подкольцо, подполе. Подмножества кольца (поля) называется *подкольцом* (*подполем*), если оно замкнуто относительно сложения и умножения и само является кольцом (полем) относительно этих индуцированных операций.

Л е м м а 1. *Подмножество L кольца K тогда и только тогда является подкольцом, когда оно замкнуто относительно сложения, умножения и взятия противоположного элемента, т. е., когда выполняются следующие условия*:

а) *для любых $a, b \in L$ сумма $a + b \in L$*,

б) *для любых $a, b \in L$ произведение $ab \in L$*,

в) *для любого $a \in L$ противоположный $-a \in L$.*

Подмножество L поля P тогда и только тогда является подполем, когда оно замкнуто относительно сложения, умножения, взятия противоположного элемента и взятие обратного элемента. Последнее означает:

г) *для любого $a \in L, a \neq 0$ обратный элемент $a^{-1} \in L$.*

Д о к а з а т е л ь с т в о. Рассмотрим множество L с операцией сложения. Так как выполнены условия а) и в), то ввиду леммы 1 из § 2 $\langle L; + \rangle$ является подгруппой группы $\langle K; + \rangle$, а так как выполнено условие б), то $\langle L; +, \cdot \rangle$ – подкольцо. Для доказательства второго утверждения достаточно заметить, что в силу условий б) и г) $\langle L \setminus \{0\}; \cdot \rangle$ является подгруппой группы $\langle P \setminus \{0\}; \cdot \rangle$, а потому $\langle L; +, \cdot \rangle$ является подполем.

Л е м м а 2. *Пересечение любого множества подколец* (*подполей*) *снова является подкольцом* (*подполем*).

Д о к а з а т е л ь с т в о. Пусть K – некоторое кольцо, L_α, $\alpha \in J$, – семейство подколец и $L = \bigcap_{\alpha \in J} L_\alpha$ – их пересечение. Чтобы доказать, что L – подкольцо, надо доказать, что L замкнуто относительно сложения, умножения и взятия противоположного, т. е.:

а) если $a, b \in L$, то $a + b \in L$;

б) если $a, b \in L$, то $ab \in L$;

в) если $a \in L$, то $-a \in L$.

Для доказательства а) заметим, что если $a, b \in L$, то $a, b \in L_\alpha$ для любого $\alpha \in J$. Следовательно, $a + b \in L_\alpha$ для любого $\alpha \in J$, но это и означает, что $a + b \in L$.

б) Если $a, b \in L$, то $a, b \in L_\alpha$ для любого $\alpha \in J$. Следовательно, $ab \in L_\alpha$ для любого $\alpha \in J$, т. е. $ab \in L$.

в) Пусть $a \in L$. Тогда $a \in L_\alpha$ для любого $\alpha \in J$, но тогда $-a \in L_\alpha$ для любого $\alpha \in J$ и следовательно, $-a \in L$.

Если теперь K – поле, а L_α – семейство подполей, то мы должны установить следующее утверждение:

г) если $a \in L$, $a \neq 0$, то $a^{-1} \in L$.

Заметим, что если $a \in L$, то $a \in L_\alpha$ для любого $\alpha \in J$ и $a^{-1} \in L_\alpha$ для любого $\alpha \in J$, но это и означает, что $a^{-1} \in L$. Лемма доказана.

Подкольцом кольца K, порожденным множеством M называется пересечение всех подколец, содержащих M, т. е.

$$(M) = \bigcap L_\alpha, \quad L_\alpha - \text{подкольцо в } K, \quad L_\alpha \supseteq M.$$

Подполем поля P, порожденным множеством M называется пересечение всех подполей, содержащих M.

П р и м е р ы. 1) Кольцо $\langle \mathbb{Z}; +, \cdot \rangle$ порождается 1. Аналогично, поле $\langle \mathbb{Q}; +, \cdot \rangle$ порождается 1.

2) В поле $\langle \mathbb{R}; +, \cdot \rangle$ рассмотрим подкольцо, порожденное элементами 1 и $\sqrt{2}$. Нетрудно заметить, что это подкольцо состоит из чисел

$$\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Более того, это подкольцо является подполем.

У п р а ж н е н и е. Поле L_2 не изоморфно полю L_3, где

$$L_n = \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}, n \in \mathbb{N} \text{ и не является квадратом.}$$

У п р а ж н е н и е. При каких натуральных p и q имеет место изоморфизм $L_p \simeq L_q$?

§ 4. Группы подстановок

4.1. Определения. Пусть

$$M_n = \{1, 2, 3, \ldots, n\}$$

– конечное множество. *Подстановкой* множества M_n называется взаимно однозначное отображение этого множества на себя. Всякую подстановку можно записать в виде

$$a = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix},$$

где внизу находятся элементы из M_n, в которые переходят верхние. Очевидно, что одна и та же подстановка может быть записана несколькими способами, например,

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 3 & 2 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

На множестве подстановок определим умножение.

Произведением двух подстановок называется третья, равная последовательному выполнению первой, а затем второй.

П р и м е р. Если

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix},$$

то их произведения

$$ab = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \quad ba = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

Из этого примера видим, что операция умножения подстановок не коммутативна.

Обозначим

$$S_n = \{\text{подстановка множества } M_n\}$$

и будем называть *множеством подстановок степени* n. Нетрудно проверить, что $|S_n| = n!$, где символом $|A|$ обозначается число элементов множества A.

Справедлива

Т е о р е м а 1. *Множество S_n с операцией умножения образует группу. При $n \geq 3$ она некоммутативна.*

Д о к а з а т е л ь с т в о. То, что $\langle S_n; \cdot \rangle$ является алгебраической системой следует из определения произведения подстановок. Проверим аксиомы группы.

1) Ассоциативность: проверим, что для любых подстановок a, b, c из S_n справедливо равенство

$$(ab)c = a(bc).$$

Для этого обозначим $ab = d$, $dc = f$ – левая часть равенства; $bc = g$, $ag = h$ – правая часть равенства. Выберем некоторый символ $i \in M_n = \{1, 2, \ldots, n\}$ и подействуем на него подстановкой f, Получим

$$if = (id)c = i((ab)c) = ((ia)b)c.$$

Действуя подстановкой h, получим

$$ih = (ia)g = ((ia)b)c.$$

Следовательно, на каждый символ $i \in M_n$ подстановки f и h действуют одинаково, но это означает, что они равны, т. е. ассоциативность умножения выполняется.

2) Легко проверить, что единичным элементом является подстановка

$$e = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix},$$

оставляющая все символы на месте.

3) Пусть

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

– произвольная подстановка. Нетрудно убедиться, что обратной является подстановка

$$a^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Покажем, что при $n \geq 3$ группа S_n некоммутативна. Положим

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix}.$$

Тогда $1(ab) = 2$, т. е. подстановка ab переводит символ 1 в символ 2, а $1(ba) = 3$, т. е. подстановка ba переводит символ 1 в символ 3. Следовательно, $ab \neq ba$. Теорема доказана.

Из этой теоремы, в частности, следует, что группа S_3 порядка 6 неабелева.

У п р а ж н е н и е. Существует ли неабелева группа порядка меньше 6?

4.2. Разложение подстановки в произведение независимых циклов. Рассмотрим подстановку

$$\begin{pmatrix} \dots & i_1 & \dots & i_2 & \dots & i_{s-1} & \dots & i_s & \dots \\ \dots & i_2 & \dots & i_3 & \dots & i_s & \dots & i_1 & \dots \end{pmatrix},$$

где все невыписанные символы остаются на месте. Тогда эту подстаноку будем записывать в виде $(i_1 i_2 \dots i_{s-1} i_s)$ и называть *циклической подстановкой* или *циклом.*

П р и м е р. Подстановка

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 3 & 4 & 7 & 6 & 2 \end{pmatrix}$$

имеет следующее представление в виде цикла $a = (257)$. Заметим, что этот цикл можно записать несколькими способами:

$$(257) = (572) = (725).$$

Две циклические подстановки, или короче, два цикла называются *независимыми*, если их множества действительно перемещаемых символов не пересекаются. Легко заметить, что независимые циклы перестановочны.

П р и м е р. Пара зависимых циклов:

$$(123),\ (257)$$

(оба содержат символ 2); пара независимых циклов:

$$(134),\ (257).$$

Т е о р е м а 2. *Всякая нетождественная подстановка может быть разложена в произведение независимых циклов. Это разложение единственно с точностью до порядка множителей.*

Д о к а з а т е л ь с т в о. Пусть a – некоторая подстановка из S_n и t – число действительно перемещаемых символов. Проведем доказательство индукцией по t. Очевидно, что $t \geq 2$. При $t = 2$ имеем

$$a = \begin{pmatrix} \dots & i & \dots & j & \dots \\ \dots & j & \dots & i & \dots \end{pmatrix} = (ij)$$

– цикл и утверждение теоремы справедливо.

При $t > 2$ представим нашу подстановку в таком виде

$$a = \begin{pmatrix} \dots & i_1 & \dots & i_2 & \dots & i_{s-1} & \dots & i_s & \dots \\ \dots & i_2 & \dots & i_3 & \dots & i_s & \dots & i_1 & \dots \end{pmatrix}.$$

Здесь мы выбрали некоторый символ i_1 и следим за тем, куда он переходит. Начиная с некоторого момента символы будут повторяться и первым повтором будет символ i_1 (символы, отмеченные точками тоже как-то перемещаются).

Определим подстановку

$$b = \begin{pmatrix} \dots & i_1 & \dots & i_2 & \dots & i_{s-1} & \dots & i_s & \dots \\ \dots & i_2 & \dots & i_3 & \dots & i_s & \dots & i_1 & \dots \end{pmatrix},$$

в которой невыписанные символы остаются на месте и подстановку

$$c = \begin{pmatrix} \dots & i_1 & \dots & i_2 & \dots & i_{s-1} & \dots & i_s & \dots \\ \dots & i_1 & \dots & i_2 & \dots & i_{s-1} & \dots & i_s & \dots \end{pmatrix},$$

в которой невыписанные символы переходят в те, в которые переходят символы подстановки a, а выписанные остаются на месте.

Заметим, что $bc = a$. При этом b – это цикл, в b и c нет общих перемещаемых символов и в c число перемещаемых символов равно $t - s$, т. е. на s меньше чем в a. По предположению индукции:

$$c = c_1\, c_2\, \dots\, c_p$$

– произведение независимых циклов. Следовательно

$$a = b\, c_1\, c_2\, \dots\, c_p$$

– произведение независимых циклов. Таким образом, мы представили всякую подстановку $a \in S_n$ в виде произведения независимых циклов.

Докажем единственность. Пусть

$$a = c_1\, c_2\, \ldots\, c_k = d_1\, d_2\, \ldots\, d_l$$

– два разложения подстановки a в произведения независимых циклов. Заметим, что если какой-то символ встречается в одной записи, то он встречается и в другой (так как если символ перемещается, то это указывается в любой записи). Возьмем некоторый перемещаемый символ i и передвинем его в начало соответствующего цикла, а также поставим этот цикл на первое место. Будем иметь

$$c_1 = (i\, \alpha\, \beta\, \ldots\, \delta), \qquad d_1 = (i\, \alpha'\, \beta'\, \ldots\, \delta').$$

Это означает, что подстановка a содержит, с одной стороны фрагмент

$$\begin{pmatrix} \ldots & i & \ldots \\ \ldots & \alpha & \ldots \end{pmatrix},$$

а с другой стороны, фрагмент

$$\begin{pmatrix} \ldots & i & \ldots \\ \ldots & \alpha' & \ldots \end{pmatrix},$$

(учесть, что циклы независимы). Следовательно, $\alpha = \alpha'$. Теорема доказана.

4.3. Декримент. Четность подстановки. *Декрементом* подстановки называется разность между числом действительно перемещаемых символов и числом независимых циклов.

П р и м е р. Пусть

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 1 & 7 & 2 & 3 & 5 & 8 \end{pmatrix} = (163)(2475).$$

Тогда декремент d равен $7 - 2 = 5$.

Если декремент подстановки – четное число, то подстановка называется *четной.* Если декремент – нечетное число, то подстановка называется *нечетной.* Подстановка, переставляющая только два символа называется *транспозицией.* Очевидно, транспозиция – нечетная подстановка.

Т е о р е м а 3. *При умножении произвольной подстановки на транспозицию ее четность меняется.*

Д о к а з а т е л ь с т в о. Пусть

$$a = (i_1\, i_2,\, \ldots\, i_r)\, (j_1\, j_2,\, \ldots\, j_s)\, \ldots$$

– разложение подстановки a в произведение независимых циклов. Пусть при этом k – число действительно перемещаемых символов и l – число независимых циклов, декремент $d = k - l$. Рассмотрим транспозицию $b = (p\,q)$. При этом символы p и q могут либо входить, либо не входить в независимые циклы подстановки a. Разберем все эти случаи и результаты поместим в таблицу:

	случаи	a
1	p и q не входят в a	$(i_1\,i_2\,\ldots\,i_r)\,(j_1\,j_2\,\ldots\,j_s)\,\ldots$
2	p входит, q не входит в a	$(p\,i_2\,\ldots\,i_r)\,(j_1\,j_2\,\ldots\,j_s)\,\ldots$
3	p не входит, q входит в a	$(q\,i_2\,\ldots\,i_r)\,(j_1\,j_2\,\ldots\,j_s)\,\ldots$
4	p и q входя в один цикл	$(p\,\ldots\,q\,\ldots)\,(j_1\,j_2\,\ldots\,j_s)\,\ldots$
5	p и q входя в разные циклы	$(p\,\ldots)\,(q\,\ldots)\,(j_2\,\ldots\,j_s)\,\ldots$

ab	k'	l'	d'
$(i_1\,i_2\,\ldots\,i_r)\,(j_1\,j_2\,\ldots\,j_s)\,\ldots\,(p\,q)$	$k+2$	$l+1$	$d+1$
$(p\,i_2\,\ldots\,i_r\,q)\,(j_1\,j_2\,\ldots\,j_s)\,\ldots$	$k+1$	l	$d+1$
$(q\,i_2\,\ldots\,i_r\,p)\,(j_1\,j_2\,\ldots\,j_s)\,\ldots$	$k+1$	l	$d+1$
$(p\,\ldots)\,(q\,\ldots)\,(j_1\,j_2\,\ldots\,j_s)\,\ldots$	k	$l+1$	$d-1$
$(p\,\ldots\,q\,\ldots)\,(j_1\,j_2\,\ldots\,j_s)\,\ldots$	k	$l-1$	$d+1$

где k' – число действительно перемещаемых символов подстановки ab, l' – число ее независимых циклов, а $d' = k' - l'$ – декремент. Анализируя последний столбец полученной таблицы,получаем требуемое утверждение.

Т е о р е м а 4. *В группе S_n число четных и нечетных подстановок одно и то же и равно $\frac{1}{2}n!$.*

Д о к а з а т е л ь с т в о. Пусть

$$P = \{a_1,\, a_2,\, \ldots,\, a_s\}$$

– множество всех четных подстановок из S_n. Возьмем транспозицию $t = (1\,2)$ и рассмотрим множество подстановок

$$Pt = \{a_1t,\, a_2t,\, \ldots,\, a_st\}.$$

По теореме 3 все эти подстановки нечетные. Чтобы доказать теорему, надо доказать, что

1) в Pt все подстановки различны;

2) всякая нечетная подстановка из S_n содержится в множестве Pt.

Докажем 1). Предположим, что $a_it = a_jt$. Умножая обе части этого равенства справа на t, получим $a_it^2 = a_jt^2$. Учитывая, что t^2 – тождественная подстановка, получим $a_i = a_j$, но так как в P все подстановки различны, то $a_i \neq a_j$.

Для доказательства 2) возьмем некоторую нечетную подстановку b и найдем $a = bt$. По теореме 3, a – четная подстановка, а все четные подстановки содержатся в множестве P. Следовательно, $a = a_i$ для некоторого i. Тогда в множестве $P\,t$ находим $a_i t = bt^2 = b$. Пункт 2) установлен.

Следовательно, число четных и нечетных подстановок в S_n одно и то же, а так как в S_n содержится $n!$ элементов, то это число равно $\frac{1}{2}n!$. Теорема доказана.

4.4. Порождающие множества. Транспозиции являются простейшими подстановками. Как показывает следующая теорема, множество транспозиций является порождающим множеством группы подстановок.

Т е о р е м а 5. *Всякая подстановка разлагается в произведение транспозиций. Это разложение не единственно, но четность числа транспозиций всегда одна и та же и совпадает с четностью самой подстановки.*

Следующее равенство показывает, что одна и та же подстановка может иметь различные разложения в произведение транспозиций:

$$(2\,3) = (1\,2)\,(1\,3)\,(1\,2).$$

Д о к а з а т е л ь с т в о т е о р е м ы. Рассмотрим некоторую подстановку a и представим ее в виде произведения независимых циклов:

$$a = c_1\,c_2\,\ldots, c_s.$$

Легко проверить, что каждый цикл разлагается в произведение транспозиций:

$$(i_1\,i_2\,\ldots\,i_t) = (i_1\,i_2)\,(i_1\,i_3)\,\ldots\,(i_1\,i_t).$$

Следовательно, и сама подстановка a разлагается в произведение транспозиций:

$$a = t_1\,t_2\,\ldots\,t_k.$$

Так как транспозиция – нечетная подстановка, а при умножении ее на транспозицию получаем четную подстановку, то по теореме 3 четность k равна четности a. Теорема доказана.

Отметим, что найденное в теореме множество порождающих группы S_n при $n > 2$ не является минимальным ($S_2 = \text{гр}((1,2))$ – циклическая группа порядка 2).

У п р а ж н е н и е. Группа S_n порождается множеством транспозиций $(1,2)$, $(1,3)$, $\ldots$, $(1,n)$.

Оказывается, что и это множество не является минимальным.

У п р а ж н е н и е. Группа S_n, $n > 2$ порождается транспозицией $(1,2)$ и циклом $(1,2,\ldots,n)$.

Четные подстановки образуют подгруппу группы S_n, которая называется *знакопеременной группой* и обозначается символом A_n.

О п р е д е л е н и е. *Знаком подстановки* τ назовем следующее число:

$$\operatorname{sign}\tau = \begin{cases} +1 & \text{если } \tau \text{ четная,} \\ -1 & \text{если } \tau \text{ нечетная.} \end{cases}$$

С л е д с т в и е. *Справедливы следующие равенства*:

$$\operatorname{sign}(\sigma\cdot\tau) = \operatorname{sign}\sigma\cdot\operatorname{sign}\tau,$$

$$\operatorname{sign}(\sigma^{-1}) = \operatorname{sign}\sigma.$$

Д о к а з а т е л ь с т в о. Представим подстановки σ и τ в виде произведения транспозиций:

$$\sigma = \sigma_1\,\sigma_2\,\ldots\,\sigma_s, \qquad \tau = \tau_1\,\tau_2\,\ldots\,\tau_t.$$

Тогда

$$\sigma\,\tau = \sigma_1\,\sigma_2\,\ldots\,\sigma_s\,\tau_1\,\tau_2\,\ldots\,\tau_t.$$

$$\sigma^{-1} = \sigma_s\,\ldots\,\sigma_2\,\sigma_1.$$

По теореме 5

$$\operatorname{sign}\sigma = (-1)^s, \quad \operatorname{sign}\tau = (-1)^t, \quad \operatorname{sign}(\sigma\,\tau) = (-1)^{s+t}, \quad \operatorname{sign}(\sigma^{-1}) = (-1)^s.$$

Следствие установлено.

§ 5. Кольца матриц

5.1. Суперпозиция линейных замен. Рассмотрим две линейных замены переменных с коэффициентами из кольца K:

$$\begin{cases} x_1 = a_{11}\,y_1 + \ldots + a_{1n}\,y_n, \\ x_2 = a_{21}\,y_1 + \ldots + a_{2n}\,y_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_r = a_{r1}\,y_1 + \ldots + a_{rn}\,y_n, \end{cases} \qquad a_{ij} \in K,$$

$$\begin{cases} y_1 = b_{11}\,z_1 + \ldots + b_{1s}\,z_s, \\ y_2 = b_{21}\,z_1 + \ldots + b_{2s}\,z_s, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_n = b_{n1}\,z_1 + \ldots + b_{ns}\,z_s, \end{cases} \qquad b_{kl} \in K.$$

Если подставить вторую замену в первую, то получим

$$x_i = a_{i1}\,y_1 + \ldots + a_{in}\,y_n = a_{i1}(b_{11}\,z_1 + \ldots + b_{1s}\,z_s) + \ldots + a_{in}(b_{n1}\,z_1 + \ldots + b_{ns}\,z_s) =$$

$$= (a_{i1}\,b_{11} \,+\, a_{i2}\,b_{21} \,+\ldots+\, a_{in}\,b_{n1})\,z_1 + \ldots + (a_{i1}\,b_{1s} \,+\, a_{i2}\,b_{2s} \,+\ldots+\, a_{in}\,b_{ns})\,z_s =$$

$$= c_{i1}\,z_1 \,+\, c_{i2}\,z_2 \,+\ldots+\, c_{is}\,z_s,$$

где

$$c_{ij} = a_{i1}\,b_{1j} \,+\, a_{i2}\,b_{2j} \,+\ldots+\, a_{in}\,b_{nj} = \sum_{k=1}^{n} a_{ik}\,b_{kj}.$$

Такая замена переменных, когда в одну подставляется другая, называется *суперпозицией линейных замен*. Получается опять линейная замена:

$$\begin{cases} x_1 = c_{11}\,z_1 \,+\,\ldots\,+ c_{1s}\,z_s, \\ x_2 = c_{21}\,z_1 \,+\,\ldots\,+ c_{2s}\,z_s, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_r = c_{r1}\,z_1 \,+\,\ldots\,+ c_{rs}\,z_s, \end{cases} \qquad c_{kl} \in K.$$

5.2. Матрицы. Сложение и умножение матриц. При работе с подобными объектами удобно использовать матрицы. Матрицей размера $r \times n$ над кольцом K называется таблица

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{r1} & a_{r2} & \ldots & a_{rn} \end{pmatrix}, \quad a_{ij} \in K.$$

В дальнейшем будем записывать такие матрицы как $A = (a_{ij})_{i,j=1}^{r,n}$ или, если размеры матрицы ясны, просто как $A = (a_{ij})$. Множество всех матриц размера $r \times n$ над кольцом K будем обозначать $M_{r\times n}(K)$.

Пусть заданы две матрицы, имеющие одинаковые размеры с элементами из одного кольца:

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{r1} & a_{r2} & \ldots & a_{rn} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ b_{r1} & b_{r2} & \ldots & b_{rn} \end{pmatrix}.$$

Тогда их *суммой* называется матрица

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \ldots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{12} & \ldots & a_{2n} + b_{1n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{r1} + b_{r1} & a_{r2} + b_{r2} & \ldots & a_{rn} + b_{rn} \end{pmatrix}.$$

Если матрицы

$$F = \begin{pmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & f_{2n} \\ .... & .... & .... & .... \\ f_{r1} & f_{r2} & \dots & f_{rn} \end{pmatrix}$$

и

$$G = \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1s} \\ g_{21} & g_{22} & \dots & g_{2s} \\ .... & .... & .... & .... \\ g_{n1} & g_{n2} & \dots & g_{ns} \end{pmatrix}$$

таковы, что число столбцов в F совпадает с числом строк в G, то мы можем определить *произведение*

$$F \cdot G = H = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1s} \\ h_{21} & h_{22} & \dots & h_{2s} \\ .... & .... & .... & .... \\ h_{r1} & h_{r2} & \dots & h_{rs} \end{pmatrix},$$

где

$$h_{ij} = f_{i1}\, g_{1j} \,+\, f_{i2}\, g_{2j} + \ldots + f_{in}\, g_{nj} = \sum_{k=1}^{n} f_{ik}\, g_{kj}.$$

Сравните полученную формулу с формулой для коэффициентов при суперпозиции линейных замен.

П р и м е р. Произведение двух матриц:

$$\begin{pmatrix} 1 & 2 & -1 \\ 2 & 3 & 0 \end{pmatrix} \cdot \begin{pmatrix} 7 & 2 & 3 \\ -1 & 0 & 5 \\ 4 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 12 \\ 11 & 4 & 21 \end{pmatrix}.$$

5.3. Кольцо матриц. Как мы знаем, если матрицы квадратные, т. е. имеют размеры $n \times n$, то их можно складывать и умножать. Будем называть такие матрицы *матрицами степени* n. Определим множество

$$M_n(K) = \{\text{матрицы степени } n \text{ над } K\} = M_{n\times n}(K).$$

Т е о р е м а 1. *Если K – кольцо, то $\langle M_n(K);\, +,\, \cdot \rangle$ – кольцо. Если K – кольцо с единицей, то $\langle M_n(K);\, +,\, \cdot \rangle$ – кольцо с единицей.*

Д о к а з а т е л ь с т в о. То, что операции сложения и умножения матриц являются алгебраическими следует из определения. Проверим аксиомы кольца.

С1. Рассмотрим матрицы $A, B, C \in M_n(K)$. Нам надо доказать, что

$$(A + B) + C = A + (B + C).$$

Рассмотрим элемент, стоящий на месте (i, j) в матрице $(A + B) + C$. Он равен $(a_{ij} + b_{ij}) + c_{ij}$. Так как K – кольцо, то

$$(a_{ij} + b_{ij}) + c_{ij} = a_{ij} + (b_{ij} + c_{ij}).$$

Следовательно, сложение матриц ассоциативно.

С2. Устанавливается аналогичным образом, используя тот факт, что сложение в кольце K коммутативно.

С3. В качестве нулевого элемента надо взять матрицу, у которой на всех местах стоят нули.

С4. Легко проверить, что если матрица $A \in M_n(K)$ имеет вид

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ .... & .... & .... & .... \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix},$$

то противоположная

$$-A = \begin{pmatrix} -a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & -a_{22} & \dots & -a_{2n} \\ .... & .... & .... & .... \\ -a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Для проверки ассоциативности умножения (аксиома У1): $(AB)C = A(BC)$, введем обозначения:

$$AB = D, \quad DC = F, \quad BC = G, \quad AG = H.$$

Нужно доказать, что $F = H$. Имеем

$$f_{ij} = \sum_{k=1}^{n} d_{ik}\, c_{kj} = \sum_{k=1}^{n} \left(\sum_{l=1}^{n} a_{il}\, b_{lk} \right) c_{kj} = \sum_{k=1}^{n} \sum_{l=1}^{n} (a_{il}\, b_{lk})\, c_{kj}.$$

С другой стороны,

$$h_{ij} = \sum_{p=1}^{n} a_{ip}\, g_{pj} = \sum_{p=1}^{n} a_{ip} \left(\sum_{q=1}^{n} b_{pq}\, c_{qj} \right) = \sum_{p=1}^{n} \sum_{q=1}^{n} a_{ip}\, (b_{pq}\, c_{qj}) = \sum_{l=1}^{n} \sum_{k=1}^{n} a_{il}\, (b_{lk}\, c_{kj}),$$

где последнее равенство вытекает из следующего равенства:

$$\sum_{i=1}^{n} a_i = \sum_{p=1}^{n} a_p = a_1 + \ldots + a_n,$$

которое показывает, что индекс суммирования можно обозначить любой буквой.

Далее нам потребуется

Л е м м а 1. *Если* α_{ij}, $1 \le i \le r$, $1 \le j \le s$, – *элементы кольца* K, *то*

$$\sum_{i=1}^{r}\sum_{j=1}^{s} \alpha_{ij} = \sum_{j=1}^{s}\sum_{i=1}^{r} \alpha_{ij}.$$

Д о к а з а т е л ь с т в о. Построим матрицу

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1s} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2s} \\ .... & .... & .... & .... \\ \alpha_{r1} & \alpha_{r2} & \ldots & \alpha_{rs} \end{pmatrix}.$$

Сначала складываем элементы в каждой строке, а затем складываем полученные элементы:

$$(\alpha_{11} + \alpha_{12} + \ldots + \alpha_{1s}) + \ldots + (\alpha_{r1} + \alpha_{r2} + \ldots + \alpha_{rs}) = \sum_{i=1}^{r}\sum_{j=1}^{s} \alpha_{ij};$$

затем складываем элементы в каждом столбце и находим сумму полученных элементов:

$$(\alpha_{11} + \alpha_{21} + \ldots + \alpha_{r1}) + \ldots + (\alpha_{1s} + \alpha_{2s} + \ldots + \alpha_{rs}) = \sum_{j=1}^{s}\sum_{i=1}^{r} \alpha_{ij}.$$

Из коммутативности сложения в K следует, что эти две суммы совпадают. Лемма доказана.

Воспользовавшись этой леммой, получим

$$\sum_{l=1}^{n}\sum_{k=1}^{n} a_{il}\,(b_{lk}\,c_{kj}) = \sum_{k=1}^{n}\sum_{l=1}^{n} (a_{il}\,b_{lk})\,c_{kj}.$$

Следовательно, аксиома У1 установлена.

Для доказательства СУ1: $(A + B)C = AC + BC$, введем обозначения:

$$A + B = D, \quad DC = F, \quad AC = G, \quad BC = H, \quad G + H = U.$$

Нам надо доказать, что $F = U$. Для этого вычислим элемент, стоящий на месте (i, j) в матрице F. Имеем

$$f_{ij} = \sum_{k=1}^{n} d_{ik}\, c_{kj} = \sum_{k=1}^{n} (a_{ik} + b_{ik})\, c_{kj}.$$

С другой стороны,

$$u_{ij} = g_{ij} + h_{ij} = \sum_{k=1}^{n} a_{ik}\, c_{kj} + \sum_{k=1}^{n} b_{ik}\, c_{kj} = \sum_{k=1}^{n} (a_{ik} + b_{ik}) c_{kj},$$

где в последнем равенстве мы воспользовались коммутативностью сложения и правой дистрибутивностью в кольце K.

Аксиома СУ2 проверяется аналогично.

Если K – кольцо с единицей 1, то единицей кольца $M_n(K)$ является единичная матрица E, у которой на главной диагонали стоят 1, а на всех остальных местах – нули. Теорема доказана.

5.4. Диагональные матрицы и трансвекции. В кольце $M_n(K)$ введем два класса матриц.

О п р е д е л е н и е. *Диагональной матрицей* называется матрица у которой все элементы вне главной диагонали равны нулю:

$$\mathrm{diag}(\alpha_1, \ldots, \alpha_n) = \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 \\ .... & .... & .... & .... \\ 0 & 0 & \ldots & \alpha_n \end{pmatrix}.$$

О п р е д е л е н и е. *Трансвекцией* $T_{ij}(\beta)$, $1 \le i \ne j \le n$, называется матрица, у которой на главной диагонали стоят 1, на месте (i, j) – элемент $\beta \in K$, а на всех остальных местах – нули.

Посмотрим, что происходит при умножении произвольной матрицы на диагональную. Если матрицу умножить на диагональную справа, то получим

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ .... & .... & .... & .... \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 \\ .... & .... & .... & .... \\ 0 & 0 & \ldots & \alpha_n \end{pmatrix} = \begin{pmatrix} a_{11}\alpha_1 & a_{12}\alpha_2 & \ldots & a_{1n}\alpha_n \\ a_{21}\alpha_1 & a_{22}\alpha_2 & \ldots & a_{2n}\alpha_n \\ .... & .... & .... & .... \\ a_{n1}\alpha_1 & a_{n2}\alpha_2 & \ldots & a_{nn}\alpha_n \end{pmatrix}.$$

Если матрицу умножить на диагональную слева, то получим

$$\begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 \\ .... & .... & .... & .... \\ 0 & 0 & \ldots & \alpha_n \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ .... & .... & .... & .... \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} = \begin{pmatrix} a_{11}\alpha_1 & a_{12}\alpha_1 & \ldots & a_{1n}\alpha_1 \\ a_{21}\alpha_2 & a_{22}\alpha_2 & \ldots & a_{2n}\alpha_2 \\ .... & .... & .... & .... \\ a_{n1}\alpha_n & a_{n2}\alpha_n & \ldots & a_{nn}\alpha_n \end{pmatrix}.$$

Таким образом, справедлива

Л е м м а 2. *При умножении произвольной матрицы на диагональную матрицу* $\mathrm{diag}(\alpha_1,\ldots,\alpha_n)$ *справа первый столбец умножается на* α_1*, второй – на* α_2 *и т. д. При умножении произвольной матрицы на диагональную матрицу* $\mathrm{diag}(\alpha_1,\ldots,\alpha_n)$ *слева первая строка умножается на* α_1*, вторая – на* α_2 *и т. д.*

Пусть дана трансвекция $T_{ij}(\beta)$, при умножении ее на произвольную матрицу справа, получим

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ .... & .... & .... & .... \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \cdot T_{ij}(\beta) = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1,j-1} & a_{1i}\beta + a_{1j} & a_{1,j+1} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2,j-1} & a_{2i}\beta + a_{2j} & a_{2,j+1} & \ldots & a_{2n} \\ .... & .... & .... & .... & .... & \ldots & \ldots & .... \\ a_{n1} & a_{n2} & \ldots & a_{n,j-1} & a_{ni}\beta + a_{nj} & a_{n,j+1} & \ldots & a_{nn} \end{pmatrix},$$

где сумма стоит в j-м столбце.

При умножении слева, получим матрицу

$$T_{ij}(\beta) \cdot \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ .... & .... & .... & .... \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ .... & .... & .... & .... \\ a_{i-1,1} & a_{i-1,2} & \ldots & a_{i-1,n} \\ a_{i1} + \beta a_{j1} & a_{i2} + \beta a_{j2} & \ldots & a_{in} + \beta a_{jn} \\ a_{i+1,1} & a_{i+1,2} & \ldots & a_{i+1,n} \\ .... & .... & .... & .... \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

где сумма стоит в i-й строке.

Справедлива

Л е м м а 3. *При умножении произвольной матрицы на трансвекцию* $T_{ij}(\beta)$ *справа к ее* j*-у столбцу прибавляется* i*-й столбец, умноженный на* β*. При умножении произвольной матрицы на трансвекцию* $T_{ij}(\beta)$ *слева к ее* i*-й строке прибавляется* j*-я строка, умноженная на* β*.*

Отметим также следующие свойства трансвекций.

Л е м м а 4. 1) *Для произведения трансвекций справедливо равенство*

$$T_{ij}(\beta) \cdot T_{ij}(\gamma) = T_{ij}(\beta + \gamma).$$

2) *Обратной к трансвекции* $T_{ij}(\beta)$ *является трансвекция* $T_{ij}(-\beta)$.

Д о к а з а т е л ь с т в о. 1) По лемме 3 умножение $T_{ij}(\beta)$ справа на трансвекцию $T_{ij}(\gamma)$ соответствует тому, что мы к j-у столбцу матрицы $T_{ij}(\beta)$ прибавляем i–й столбец, умноженный на γ. В результате получим трансвекцию $T_{ij}(\beta + \gamma)$.

2) По пункту 1) имеем

$$T_{ij}(\beta) \cdot T_{ij}(-\beta) = T_{ij}(0),$$

а $T_{ij}(0)$ – единичная матрица.

5.5. Разложение матрицы в произведение диагональной и трансвекций. Основным результатом настоящего пункта является доказательство следующего утверждения.

Т е о р е м а 2. *Пусть P – поле. Всякая матрица $A \in M_n(P)$ разлагается в произведение*

$$A = T_1\, T_2\, \ldots\, T_r\, D\, T_{r+1}\, T_{r+2}\, \ldots\, T_s,$$

где D – диагональная матрица, T_i, $i = 1, 2, \ldots, s$, – трансвекции.

Д о к а з а т е л ь с т в о. Назовем *элементарными преобразованиями матрицы* следующие преобразования:

1) прибавление к одной строке матрицы другой ее строки, умноженной на ненулевой элемент из P;

2) прибавление к одному столбцу матрицы другого ее столбца, умноженного на ненулевой элемент из P.

Используя индукцию по n, докажем, что при помощи этих элементарных преобразований всякую матрицу можно привести к диагональной матрице.

При $n = 1$ матрица A диагональная.

Предположим, что матрицы порядка $n-1$ мы умеем приводить к диагональному виду. Рассмотрим матрицу $A = (a_{ij}) \in M_n(P)$ степени n. В зависимости от вида этой матрицы рассмотрим несколько случаев.

Случай 1: $a_{11} \neq 0$. Так как P – поле, то существует элемент a_{11}^{-1} – обратный к элементу a_{11}. Умножим первый столбец матрицы A на $-a_{1j}a_{11}^{-1}$ и прибавим к j-у столбцу, $j = 2, 3, \ldots, n$. Получим матрицу у которой все элементы, стоящие в первой строке, за исключением первого элемента равны нулю:

$$\begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ a_{21} & a'_{22} & \ldots & a'_{2n} \\ .... & .... & .... & .... \\ a_{n1} & a'_{n2} & \ldots & a'_{nn} \end{pmatrix}.$$

Умножим 1-ю строку на $-a_{i1}a_{11}^{-1}$ и прибавим к i-й строке для всех $i = 2, 3, \ldots, n$. Получим матрицу

$$\left(\begin{array}{c|ccc} a_{11} & 0 & \ldots & 0 \\ \hline 0 & * & \ldots & * \\ .... & .... & .... & .... \\ 0 & * & \ldots & * \end{array}\right).$$

Применяя предположение индукции, приведем эту матрицу при помощи элементарных преобразований к диагональному виду:

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & b_2 & \dots & 0 \\ .... & .... & .... & .... \\ 0 & 0 & \dots & b_n \end{pmatrix}.$$

Случай 2: $a_{11} = 0$, но какой-то элемент a_{1j} или a_{i1}, $i, j \in \{2, 3, \dots, n\}$, отличен от нуля. Если $a_{1j} \neq 0$, то умножим j-й столбец на единицу и прибавим к 1-м столбцу. Если $a_{i1} \neq 0$, то умножим i-ю строку на 1 и прибавим к 1-й строке. В обоих случаях приходим к разобранному выше случаю 1.

Случай 3: весь первый столбец и вся первая строка матрицы A состоят из нулей. В этом случае, воспользовавшись предположением индукции, приведем ее к диагональному виду.

Возвращаемся к доказательству теоремы. Как следует из леммы 3, умножение матрицы на трансвекцию справа соответствует элементарному преобразованию столбцов матрицы, а умножение матрицы на трансвекцию слева соответствует элементарному преобразованию строк матрицы. Таким образом, мы установили, что найдутся трансвекции $U_1, U_2, \dots, U_r, U_{r+1}, \dots, U_s$ такие, что

$$U_1\, U_2\, \dots\, U_r\, A\, U_{r+1}\, \dots\, U_s = D,$$

где D – некоторая диагональная матрица.

Воспользовавшись далее леммой 4, получим

$$A = U_r^{-1}\, U_{r-1}^{-1}\, \dots\, U_1^{-1}\, D\, U_s^{-1}\, \dots\, U_{s+1}^{-1},$$

где каждая U_i^{-1}, $i = 1, 2, \dots, s$, как следует из леммы 4 является трансвекцией. Теорема доказана.

§ 6. Определители

6.1. Определитель обратимости матрицы. Если K – кольцо, то матрицы степени n над K образуют кольцо, но не поле. Нетрудно заметить, что не всякая ненулевая матрица обладает обратной.

П р и м е р. Рассмотрим ненулевую матрицу

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

и покажем, что у нее не существует обратной. Действительно, найдем произведение

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} z & t \\ 0 & 0 \end{pmatrix},$$

и очевидно, что ни для каких $x, y, z, t \in K$ последняя матрица не является единичной.

Как по произвольной матрице узнать: имеет ли она обратную?

Введем следующее

О п р е д е л е н и е. *Определитель обратимости матрицы* или просто *определитель* матрицы $A \in M_n(P)$ есть следующий элемент из поля P:

$$\det A = |A| = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ .... & .... & .... & .... \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \sum_{\sigma \in S_n} \operatorname{sign} \sigma \cdot a_{1,1\sigma}\, a_{2,2\sigma}\, \dots\, a_{n,n\sigma},$$

где S_n – множество подстановок степени n.

Если A имеет степень n, то $\det A$ называют *определителем порядка* n. Покажем, как используя это определение можно вычислять определители порядка 2 и 3.

П р и м е р 1. При $n = 2$ множество S_n содержит две подстановки:

$$\sigma_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Причем, $\operatorname{sign} \sigma_1 = +1$, $\operatorname{sign} \sigma_2 = -1$. Тогда

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \operatorname{sign} \sigma_1 \cdot a_{1,1\sigma_1}\, a_{2,2\sigma_1} + \operatorname{sign} \sigma_2 \cdot a_{1,1\sigma_2}\, a_{2,2\sigma_2} = a_{11}\, a_{22} - a_{12}\, a_{21}.$$

П р и м е р 2. При $n = 3$ множество S_n содержит 6 подстановок:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Причем, три первых имеют знак $+1$, а три последних – знак -1. Следовательно,

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}\, a_{22}\, a_{33} + a_{12}\, a_{23}\, a_{31} + a_{13}\, a_{21}\, a_{32} - a_{13}\, a_{22}\, a_{31} - a_{12}\, a_{21}\, a_{33} - a_{11}\, a_{23}\, a_{32}.$$

6.2. Свойства определителей. Матрица $C \in M_n(P)$ называется *полураспавшейся,* если она имеет вид

$$C = \begin{pmatrix} A & * \\ \mathbf{0} & B \end{pmatrix}, \quad A \in M_r(P), \quad B \in M_{n-r}(P), \quad \mathbf{0} \in M_{(n-r)\times r}(P), \quad 1 < r < n.$$

1. *Определитель полураспавшейся матрицы вычисляется по формуле*:

$$\det \begin{pmatrix} A & * \\ \mathbf{0} & B \end{pmatrix} = \det A \cdot \det B.$$

Д о к а з а т е л ь с т в о. Рассмотрим полураспавшуюся матрицу

$$C = \left(\begin{array}{cccc|ccc} a_{11} & a_{12} & \dots & a_{1r} & a_{1,r+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{r1} & a_{r2} & \dots & a_{rr} & a_{r,r+1} & \dots & a_{rn} \\ \hline 0 & 0 & \dots & 0 & b_{r+1,r+1} & \dots & b_{r+1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & b_{n,r+1} & \dots & b_{nn} \end{array}\right).$$

Найдем произведение

$$\det A \cdot \det B = \sum_{\sigma \in S_r} \operatorname{sign}\sigma \cdot a_{1,1\sigma}\, a_{2,2\sigma}\, \dots\, a_{r,r\sigma} \cdot \sum_{\tau \in S_{n-r}} \operatorname{sign}\tau \cdot b_{r+1,(r+1)\tau}\, b_{r+2,(r+2)\tau}\, \dots\, b_{n,n\tau} =$$

$$= \sum_{\sigma \in S_r, \tau \in S_{n-r}} \operatorname{sign}\sigma \operatorname{sign}\tau \cdot a_{1,1\sigma}\, a_{2,2\sigma}\, \dots\, a_{r,r\sigma}\, b_{r+1,(r+1)\tau}\, b_{r+2,(r+2)\tau}\, \dots\, b_{n,n\tau},$$

где σ – подстановка множества $\{1, 2, \dots, r\}$, а τ – подстановка множества $\{r+1, r+2, \dots, n\}$.

Обозначим

$$\widetilde{\sigma} = \left(\begin{array}{cccc|ccc} 1 & 2 & \dots & r & r+1 & \dots & n \\ 1\sigma & 2\sigma & \dots & r\sigma & r+1 & \dots & n \end{array}\right), \quad \widetilde{\tau} = \left(\begin{array}{cccc|ccc} 1 & 2 & \dots & r & r+1 & \dots & n \\ 1 & 2 & \dots & r & (r+1)\tau & \dots & n\tau \end{array}\right),$$

– подстановки множества $\{1, 2, \dots, n\}$, т. е. обе эти подстановки действуют на одном множестве, лежат в группе S_n и мы можем их перемножать. При этом

$$\operatorname{sign}\sigma = \operatorname{sign}\widetilde{\sigma}, \quad \operatorname{sign}\tau = \operatorname{sign}\widetilde{\tau}.$$

Следовательно,

$$\det A \cdot \det B = \sum_{\widetilde{\sigma}, \widetilde{\tau} \in S_n} \operatorname{sign}\widetilde{\sigma} \cdot \operatorname{sign}\widetilde{\tau} \cdot a_{1,1\widetilde{\sigma}}\, a_{2,2\widetilde{\sigma}}\, \dots\, a_{r,r\widetilde{\sigma}}\, b_{r+1,(r+1)\widetilde{\tau}}\, b_{r+2,(r+2)\widetilde{\tau}}\, \dots\, b_{n,n\widetilde{\tau}} =$$

$$= \sum_{\widetilde{\sigma}, \widetilde{\tau} \in S_n} \operatorname{sign}(\widetilde{\sigma} \cdot \widetilde{\tau}) \cdot a_{1,1\widetilde{\sigma}\widetilde{\tau}}\, a_{2,2\widetilde{\sigma}\widetilde{\tau}}\, \dots\, a_{r,r\widetilde{\sigma}\widetilde{\tau}}\, b_{r+1,(r+1)\widetilde{\sigma}\widetilde{\tau}}\, b_{r+2,(r+2)\widetilde{\sigma}\widetilde{\tau}}\, \dots\, b_{n,n\widetilde{\sigma}\widetilde{\tau}} =$$

$$= \sum_{\pi \in S_n} \operatorname{sign}\pi \cdot a_{1,1\pi}\, a_{2,2\pi}\, \dots\, a_{r,r\pi}\, b_{r+1,(r+1)\pi}\, b_{r+2,(r+2)\pi}\, \dots\, b_{n,n\pi} = \det C.$$

Здесь мы воспользовались таким фактом: если некоторая подстановка $\pi \in S_n$ не представима в виде $\widetilde{\sigma}\widetilde{\tau}$, то произведение $c_{1,1\pi}\, c_{2,2\pi}\, \ldots\, c_{n,n\pi}$ обращается в нуль так как содержит элемент $c_{kl} = 0$. Докажем его. Пусть подстановка имеет вид

$$\pi = \left(\begin{array}{ccc|ccc} \ldots & i & \ldots & \ldots & k & \ldots \\ \ldots & j & \ldots & \ldots & l & \ldots \end{array} \right), \quad i, l \leq r, \quad k, j > r,$$

то в соответствующем произведении содержится множитель $c_{kl} = 0$.

О п р е д е л е н и е. Матрица $A^t \in M_{s\times r}(P)$ называется *транспонированной к матрице* $A \in M_{r\times s}(P)$, если ее i-й столбец совпадает с i-й строкой матрицы A.

П р и м е р. Для матрицы

$$A = \begin{pmatrix} 2 & -1 & 3 \\ 0 & 5 & -2 \end{pmatrix}$$

транспонированной будет

$$A^t = \begin{pmatrix} 2 & 0 \\ -1 & 5 \\ 3 & -2 \end{pmatrix}.$$

Для квадратной матрицы транспонировать – это все равно, что повернуть матрицу относительно главной диагонали. Для квадратных матриц справедливо следующее свойство.

2. *Определитель транспонированной матрицы равен определителю самой матрицы*:

$$\det A^t = \det A.$$

Д о к а з а т е л ь с т в о. Обозначим элементы матрицы A^t символами b_{ij}. Тогда $b_{ij} = a_{ji}$, $1 \leq i, j \leq n$. Находим определитель матрицы A^t:

$$\det A^t = \sum_{\sigma\in S_n} \operatorname{sign}\sigma \cdot b_{1,1\sigma}\, b_{2,2\sigma}\, \ldots\, b_{n,n\sigma} = \sum_{\sigma\in S_n} \operatorname{sign}\sigma \cdot a_{1\sigma,1}\, a_{2\sigma,2}\, \ldots\, a_{n\sigma,n} =$$

$$= \sum_{\sigma\in S_n} \operatorname{sign}\sigma \cdot a_{1,1\sigma}\, a_{2,2\sigma}\, \ldots\, a_{n,n\sigma} = \det A.$$

3. *При перестановке двух строк матрицы ее определитель меняет знак.*

Д о к а з а т е л ь с т в о. Пусть

$$B = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{j1} & a_{j2} & \ldots & a_{jn} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

– матрица, полученная из A перестановкой i-й и j-й строк. Тогда

$$\det B = \sum_{\sigma\in S_n} \operatorname{sign}\sigma \cdot a_{1,1\sigma}\, a_{2,2\sigma} \,\ldots\, a_{j,i\sigma} \,\ldots\, a_{i,j\sigma} \,\ldots\, a_{n,n\sigma} =$$

$$= \sum_{\sigma\in S_n} \operatorname{sign}\sigma \cdot a_{1,1\tau\sigma}\, a_{2,2\tau\sigma} \,\ldots\, a_{i,i\tau\sigma} \,\ldots\, a_{j,j\tau\sigma} \,\ldots\, a_{n,n\tau\sigma} =$$

$$= -\sum_{\tau\sigma\in S_n} \operatorname{sign}\tau\sigma \cdot a_{1,1\tau\sigma}\, a_{2,2\tau\sigma} \,\ldots\, a_{i,i\tau\sigma} \,\ldots\, a_{j,j\tau\sigma} \,\ldots\, a_{n,n\tau\sigma},$$

где $\tau = (i,j)$ – транспозиция и действие подстановки $\tau\sigma$ определяется следующим образом

$$i\tau\sigma = j\sigma, \quad j\tau\sigma = i\sigma, \quad k\tau\sigma = k\sigma \text{ если } k \neq i,j.$$

При этом мы использовали такой факт: если

$$\{\sigma_1, \sigma_2, \ldots, \sigma_{n!}\}$$

– множество всех подстановок из S_n, то

$$\{\tau\sigma_1, \tau\sigma_2, \ldots, \tau\sigma_{n!}\}$$

– тоже множество всех подстановок из S_n.

С л е д с т в и е. *Если две строки матрицы одинаковы, то ее определитель равен нулю.*

Действительно, если характеристика поля P отлична от 2, то переставляя две строки, получим $-\det A$.

У п р а ж н е н и е. Докажите следствие для полей характеристики 2.

4. *Если матрица в одной из строчек содержит сумму, то ее определитель записывается как сумма определителей:*

$$\det A = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{i-1,1} & a_{i-1,2} & \ldots & a_{i-1,n} \\ b_1+c_1 & b_2+c_2 & \ldots & b_n+c_n \\ a_{i+1,1} & a_{i+1,2} & \ldots & a_{i+1,n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{n1} & d_{n2} & \ldots & d_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{i-1,1} & a_{i-1,2} & \ldots & a_{i-1,n} \\ b_1 & b_2 & \ldots & b_n \\ a_{i+1,1} & a_{i+1,2} & \ldots & a_{i+1,n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} +$$

$$+ \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{i-1,1} & a_{i-1,2} & \ldots & a_{i-1,n} \\ c_1 & c_2 & \ldots & c_n \\ a_{i+1,1} & a_{i+1,2} & \ldots & a_{i+1,n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix},$$

где сумма стоит в i-й строке.

Д о к а з а т е л ь с т в о следует из равенства

$$\det A = \sum_{\sigma\in S_n} \operatorname{sign}\sigma \cdot a_{1,1\sigma}\, a_{2,2\sigma}\, \ldots\, a_{i-1,(i-1)\sigma}\, (b_{i\sigma} + c_{i\sigma})\, a_{i+1,(i+1)\sigma}\, \ldots\, a_{n,n\sigma} =$$

$$= \sum_{\sigma\in S_n} \operatorname{sign}\sigma \cdot a_{1,1\sigma}\, a_{2,2\sigma}\, \ldots\, a_{i-1,(i-1)\sigma}\, b_{i\sigma}\, a_{i+1,(i+1)\sigma}\, \ldots\, a_{n,n\sigma} +$$

$$+ \sum_{\sigma\in S_n} \operatorname{sign}\sigma \cdot a_{1,1\sigma}\, a_{2,2\sigma}\, \ldots\, a_{i-1,(i-1)\sigma}\, c_{i\sigma}\, a_{i+1,(i+1)\sigma}\, \ldots\, a_{n,n\sigma}.$$

5. *Если все элементы некоторой строки матрицы умножить на $\alpha \in P$, то ее определитель умножится на α*

Действительно, пусть матрица B получается из матрицы A умножением i-й строки на α. Тогда

$$\det B = \sum_{\sigma\in S_n} \operatorname{sign}\sigma \cdot a_{1,1\sigma}\, a_{2,2\sigma}\, \ldots\, (\alpha a_{i,i\sigma})\, \ldots\, a_{n,n\sigma} =$$

$$= \alpha \sum_{\sigma\in S_n} \operatorname{sign}\sigma \cdot a_{1,1\sigma}\, a_{2,2\sigma}\, \ldots\, a_{i,i\sigma}\, \ldots\, a_{n,n\sigma} = \alpha \det A.$$

С л е д с т в и е. *Если две строки матрицы пропорциональны, то ее определитель равен нулю.*

Для формулировки последнего свойства определителей введем

О п р е д е л е н и е. *Линейной комбинацией строк* матрицы

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ .... & .... & .... & .... \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} = \begin{pmatrix} A_1 \\ A_2 \\ .... \\ A_n \end{pmatrix}$$

с коэффициентами $\beta_1, \beta_2, \ldots, \beta_n$ из P называется строка

$$\beta_1 A_1 + \beta_2 A_2 + \ldots + \beta_n A_n = \left(\sum_{i=1}^{n} \beta_i a_{i1}, \sum_{i=1}^{n} \beta_i a_{i2}, \ldots, \sum_{i=1}^{n} \beta_i a_{in} \right).$$

Линейная комбинация называется *нетривиальной*, если не все коэффициенты β_i равны нулю.

П р и м е р. Линейной комбинацией строк матрицы

$$\begin{pmatrix} 2 & -1 & 3 & 4 \\ 0 & 5 & 1 & 2 \\ 3 & -1 & 0 & 1 \end{pmatrix}$$

с коэффициентами $(-1, 0, 2)$ является строка

$$-1(2, -1, 3, 4) + 0(0, 5, 1, 2) + 3(3, -1, 0, 1) = (4, -1, 3, -2).$$

6. *Определитель матрицы не изменится, если к какой-нибудь ее строке прибавить линейную комбинацию остальных строк* (*кроме нее самой*).

Д о к а з а т е л ь с т в о. Рассмотрим матрицу

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ .... & .... & .... & .... \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} = \begin{pmatrix} A_1 \\ A_2 \\ .... \\ A_n \end{pmatrix},$$

где A_i – i-я строка матрицы A. Если к первой строке матрицы прибавить линейную комбинацию остальных строк, то ввиду свойства 4 определитель полученной матрицы равен

$$\begin{vmatrix} A_1 + \beta_2 A_2 + \ldots + \beta_n A_n \\ A_2 \\ \vdots \\ A_n \end{vmatrix} = \begin{vmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{vmatrix} + \begin{vmatrix} \beta_2 A_2 \\ A_2 \\ \vdots \\ A_n \end{vmatrix} + \ldots + \begin{vmatrix} \beta_n A_n \\ A_2 \\ \vdots \\ A_n \end{vmatrix}.$$

Заметим, что в правой части все определители кроме первого равны нулю. Действительно, во втором определителе первая строка пропорциональна второй, в третьем – первая строка пропорциональна третьей и т. д. и, наконец, в последнем определителе первая строка пропорциональна последней. По следствию свойства 5, заключаем, что все они равны нулю. Таким образом, сумма, стоящая в правой части равна определителю матрицы A.

Говорят, что между строк матрицы A существует нетривиальная линейная зависимость, если некоторая нетривиальная линейная комбинация строк равна нулевой строке.

С л е д с т в и е. *Если между строками матрицы существует нетривиальная линейная зависимость, то ее определитель равен* 0.

Мы сформулировали свойства определителей 4–6 для строк матрицы, но ввиду свойства 2, они справедливы и для столбцов.

6.3. Существование обратной матрицы. Теперь мы можем сформулировать критерий существования обратной матрицы.

Т е о р е м а 1. *Матрица тогда и только тогда обратима, когда ее определитель не равен нулю.*

Эта теорема вытекает из следующего более общего утверждения

Т е о р е м а 2. *Пусть P – поле, $A \in M_n(P)$, тогда равносильны следующие утверждения*:

1) *существует $X \in M_n(P)$ такая, что $AX = XA = E$*;

2) *существует $Y \in M_n(P)$ такая, что $AY = E$*;

3) *существует $Z \in M_n(P)$ такая, что $ZA = E$*;

4) *определитель $\det A$ не равен нулю.*

Д о к а з а т е л ь с т в о. 1) $\Rightarrow$ 2), 1) $\Rightarrow$ 3). Очевидно.

2) $\Rightarrow$ 4) (импликация 3) $\Rightarrow$ 4) устанавливается аналогично). Представим матрицу A в виде произведения диагональной и трансвекций:

$$A = T_1\, T_2\, \ldots T_r\, D\, T_{r+1}\, \ldots\, T_s.$$

Покажем, что справедливо равенство

$$\det A = \det D.$$

Действительно, так как умножить матрицу справа на трансвекцию это все равно, что к одной строке прибавить другую строку, умноженную на некоторый коэффициент, то по свойству 6 получаем требуемое равенство.

Следовательно,

$$\det A = \det D = \alpha_1\, \alpha_2\, \ldots\, \alpha_n,$$

где α_i – коэффициенты диагональной матрицы $D = \operatorname{diag}(\alpha_1\, \alpha_2\, \ldots\, \alpha_n)$.

Предположим, что $A\,Y = E$. Имеем

$$T_1\, T_2\, \ldots T_r\, D\, T_{r+1}\, \ldots\, T_s\, Y = E$$

и надо доказать, что все $\alpha_i \neq 0$. Так как каждая трансвекция обратима, то

$$D\, T_{r+1}\, \ldots\, T_s\, Y = T_r^{-1}\, T_{r-1}^{-1}\, \ldots T_1^{-1}.$$

Отсюда

$$D\, T_{r+1}\, \ldots\, T_s\, Y\, T_1\, T_2\, \ldots T_r = E.$$

Если бы некоторое $\alpha_i = 0$, то и вся строка матрицы D была бы нулевой и при умножении ее на любую матрицу эта строка была бы нулевой. Приходим к противоречию, так как справа стоит единичная матрица E, у которой все строки ненулевые. Следовательно, все $\alpha_i \neq 0$, а потому и $\det A = \alpha_1\, \alpha_2\, \ldots\, \alpha_n \neq 0$.

4) $\Rightarrow$ 1). Так как

$$\alpha_1\, \alpha_2\, \ldots\, \alpha_n = \det D = \det A \neq 0,$$

то все $\alpha_i \neq 0$, а потому обладают обратными. Тогда и для матрицы D существует обратная:

$$D^{-1} = \operatorname{diag}(\alpha_1^{-1},\, \alpha_2^{-1},\, \ldots,\, \alpha_n^{-1}).$$

В качестве матрицы X возьмем матрицу

$$X = T_s^{-1}\, T_{s-1}^{-1}\, \ldots T_{r+1}^{-1}\, D^{-1}\, T_r^{-1}\, \ldots\, T_1^{-1}.$$

Теорема доказана.

6.4. Определитель произведения матриц. Справедлива

Т е о р е м а 3. *Определитель произведения равен произведению определителей*:

$$\det(A \cdot B) = \det A \cdot \det B.$$

Д о к а з а т е л ь с т в о разобьем на несколько случаев.

Случай 1: хотя бы одна из матриц A или B необратима. Тогда по теореме 2 либо $\det A = 0$, либо $\det B = 0$. Покажем, что в этом случае матрица AB также необратима. Предположим противное, т. е. найдется матрица X такая, что

$$(AB)X = X(AB) = E.$$

Тогда $A(BX) = E$ и по теореме 2 $\det A \neq 0$. С другой стороны, $(XA)B = E$ и опять по теореме 2 $\det B \neq 0$. Противоречие. Следовательно, обратной к матрице AB не существует, а потому $\det(AB) = 0$.

Случай 2: обе матрицы A и B обратимы. По теореме 2 $\det A \neq 0$, $\det B \neq 0$. Пусть

$$A = T_1\, T_2\, \ldots T_r\, D\, T_{r+1}\, \ldots\, T_s,$$

где $D = \operatorname{diag}(\alpha_1,\, \alpha_2,\, \ldots,\, \alpha_n)$ – диагональная матрица, а T_i – трансвекция. Аналогично

$$B = U_1\, U_2\, \ldots U_p\, F\, U_{p+1}\, \ldots\, U_q,$$

где $F = \operatorname{diag}(\beta_1,\, \beta_2,\, \ldots,\, \beta_n)$ – диагональная матрица, а U_j – трансвекция.

По свойству 6 имеем

$$\det A = \det D = \alpha_1\, \alpha_2\, \ldots\, \alpha_n,$$

$$\det B = \det F = \beta_1\, \beta_2\, \ldots\, \beta_n,$$

и произведение

$$DF = \operatorname{diag}(\alpha_1\beta_1,\, \alpha_2\beta_2,\, \ldots,\, \alpha_n\beta_n)$$

имеет определитель

$$\det(DF) = \alpha_1\, \alpha_2\, \ldots,\, \alpha_n\, \beta_1\, \beta_2\, \ldots\, \beta_n = \det D \cdot \det F.$$

Рассмотрим произведение

$$AB = T_1\, T_2\, \ldots T_r\, D\, T_{r+1}\, \ldots\, T_s \cdot U_1\, U_2\, \ldots U_p\, F\, U_{p+1}\, \ldots\, U_q =$$

$$= T_1\,T_2\,\ldots T_r\,(D\,T_{r+1}D^{-1})\,(D\,T_{r+2}D^{-1})\ldots(D\,T_sD^{-1})\times$$
$$\times DF\,(F^{-1}U_1F)\;\ldots(F^{-1}U_pF)\,U_{p+1}\;\ldots\;U_q.$$

Заметим, что каждая матрица $D\,T_iD^{-1}$ и $F^{-1}\,U_jF$ является трансвекцией.

Л е м м а . *Если* $D = \mathrm{diag}D = (\alpha_1,\,\alpha_2,\,\ldots,\,\alpha_n)$ – *диагональная матрица, то*

$$D^{-1}\,T_{ij}(\beta)\,D = T_{ij}\left(\beta\frac{\alpha_j}{\alpha_i}\right),$$

т. е. матрица, сопряженная с трансвекцией при помощи диагональной матрицы опять является трансвекцией.

Из этой леммы следует, что матрицы DT_iD^{-1} и $F^{-1}U_jF$ являются трансвекциями, а потому

$$\det(AB) = \det(DF) = \det D\cdot\det F = \det A\cdot\det B.$$

Теорема доказана.

6.5. Разложение определителя по строке. Пусть $A = (a_{ij})$ – матрица из $M_n(P)$. Символом M_{ij} будем обозначать матрицу, полученную из A вычеркиванием i-й строки и j-го столбца. Очевидно, M_{ij} опять является квадратной матрицей. *Алгебраическим дополнением* в A к элементу a_{ij} называется элемент

$$A_{ij} = (-1)^{i+j}\det(M_{ij}).$$

При этом определитель $\det(M_{ij})$ называется *дополняющим минором.*

Т е о р е м а 4. *Для всякой строки матрица* $A \in M_n(P)$ *справедливо равенство*

$$\sum_{k=1}^{n} a_{ik}\,A_{jk} = \begin{cases} \det A & \text{при} \quad i = j, \\ 0 & \text{при} \quad i \neq j. \end{cases}$$

Д о к а з а т е л ь с т в о разбивается на несколько случаев.

Случай 1. $i = j$. В этом случае

$$\det A = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{i1} & 0 & \ldots & 0 \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ 0 & a_{i2} & \ldots & 0 \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} + \ldots$$

$$+ \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ 0 & 0 & \ldots & a_{in} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}.$$

В каждом из определителей, стоящих в правой части, будем переставлять i-ю строку с предыдущей, пока не поставим ее на место первой строки. Затем переставляем столбцы так, чтобы в каждом определителе на месте $(1,1)$ стоял ненулевой элемент. Получим

$$\det A = (-1)^{i-1}\left|\begin{array}{c|ccc} a_{i1} & 0 & \dots & 0 \\ \hline * & & & \\ \dots & & M_{i1} & \\ * & & & \end{array}\right| + (-1)^{i}\left|\begin{array}{c|ccc} a_{i2} & 0 & \dots & 0 \\ \hline * & & & \\ \dots & & M_{i2} & \\ * & & & \end{array}\right| + \dots$$

$$+(-1)^{i+n-2}\left|\begin{array}{c|ccc} a_{in} & 0 & \dots & 0 \\ \hline * & & & \\ \dots & & M_{in} & \\ * & & & \end{array}\right| =$$

$$= (-1)^{i-1}\, a_{i1}\det(M_{i1}) + (-1)^{i}\, a_{i2}\det(M_{i2}) + \ldots + (-1)^{i+n-2}\, a_{in}\det(M_{in}) =$$

$$= a_{i1}\, A_{i1} + a_{i2}\, A_{i2} + \ldots + a_{in}\, A_{in},$$

где в предпоследнем равенстве мы воспользовались первым свойством определителей (определитель полураспавшейся матрицы), а в последнем – определением алгебраического дополнения.

Случай 2. $i \neq j$. Рассмотрим матрицу B, которая получается из матрицы A, если вместо j-й строки поставить i-ю. Расписывая определитель матрицы B по j-й строке, ввиду предыдущего случая имеем

$$\det B = a_{i1}A_{j1} + a_{i2}A_{j2} + \ldots + a_{in}A_{jn},$$

но как мы знаем из свойств определителя, если в некоторой квадратной матрице две строки одинаковы, то ее определитель равен нулю. Следовательно, $\det B = 0$ и

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \ldots + a_{in}A_{jn} = 0.$$

Теорема доказана.

6.6. Применение к системам линейных уравнений. *Системой линейных уравнений* называется следующее выражение

$$\left\{\begin{array}{c} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m, \end{array}\right. \qquad a_{ij}, b_i \in P. \tag{1}$$

Матрица

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ .... & .... & .... & .... \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

называется *матрицей системы*, а столбцы

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix},$$

столбцом неизвестных и *столбцом свободных членов* соответственно. Кратко систему (1) можно записать в таком виде

$$A\,X = B.$$

Решением системы (1) называется n-ка

$$(x_1^0,\, x_2^0,\, \dots,\, x_n^0) \in P^n,$$

удовлетворяющая всем уравнениям системы.

Изучая системы, мы хотим ответить на следующие вопросы: имеет ли система решения, а если имеет, то как их найти?

Если в системе $m = n$, т. е. число уравнений равно числу неизвестных, то мы можем найти определитель матрицы A. Если он отличен от нуля, то говорим, что *система невырожденная*. Для невырожденных систем справедлива

Т е о р е м а 5. *Всякая невырожденная система* (1) *имеет единственное решение, которое дается формулой*

$$\left(\frac{d_1}{d},\, \frac{d_2}{d},\, \dots,\, \frac{d_n}{d}\right),$$

где $d = \det A$ *– определитель матрицы системы, а* d_j *– определитель матрицы, получаемой из* A *заменой* j*-го столбца столбцом свободных членов.*

Д о к а з а т е л ь с т в о. Вначале докажем существование решений. Так как по условию определитель матрицы A отличен от нуля, то она имеет обратную. Найдем $X = A^{-1}\,B$. Тогда

$$A\,X = A\,(A^{-1}\,B) = (A\,A^{-1})\,B = E\,B = B.$$

Следовательно, решение существует.

Докажем единственность решения. Пусть Y – решение, т. е. $AY = B$. Умножим обе части этого равенства слева на A^{-1}. Получим $A^{-1}(AY) = A^{-1}B$, т. е. $Y = A^{-1}B$, а потому $X = Y$. Следовательно, решение единственно.

Покажем, что решение задается формулой

$$\left(\frac{d_1}{d}, \frac{d_2}{d}, \ldots, \frac{d_n}{d}\right).$$

По теореме 4 имеем

$$d_j = \begin{vmatrix} a_{11} & \ldots & a_{1,j-1} & b_1 & a_{1,j+1} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2,j-1} & b_2 & a_{2,j+1} & \ldots & a_{2n} \\ \ldots. & \ldots. & \ldots. & \ldots & \ldots & \ldots. & \\ a_{n1} & \ldots & a_{n,j-1} & b_n & a_{n,j+1} & \ldots & a_{nn} \end{vmatrix} = b_1 A_{1j} + b_2 A_{2j} + \ldots + b_n A_{nj} = \sum_{k=1}^{n} b_k A_{kj}.$$

Подставим выражения $x_j = \frac{d_j}{d}$ в i-е уравнение системы:

$$\sum_{j=1}^{n} a_{ij} x_j = \sum_{j=1}^{n} a_{ij} \frac{d_j}{d} = \frac{1}{d} \sum_{j=1}^{n} a_{ij} d_j = \frac{1}{d} \sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{n} b_k A_{kj}\right) =$$

$$= \frac{1}{d} \sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij} b_k A_{kj} = \frac{1}{d} \sum_{k=1}^{n} \sum_{j=1}^{n} a_{ij} b_k A_{kj} = \frac{1}{d} \sum_{k=1}^{n} b_k \left(\sum_{j=1}^{n} a_{ij} A_{kj}\right) = \frac{1}{d} b_i d = b_i.$$

Здесь в предпоследнем равенстве мы использовали теорему 4. Теорема доказана.

Формулы, полученные в этой теореме называются *формулами Крамера.*

6.7. Применение к вычислению обратной матрицы. Как мы знаем, матрица $A \in M_n(P)$ обратима тогда и только тогда, когда ее определитель отличен от нуля. Справедлива

Т е о р е м а 6. *Если* $A = (a_{ij}) \in M_n(P)$ *и* $\det A \neq 0$, *то обратная матрица может быть найдена по формуле*

$$A^{-1} = \begin{pmatrix} \frac{A_{11}}{d} & \frac{A_{21}}{d} & \ldots & \frac{A_{n1}}{d} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ \frac{A_{1r}}{d} & \frac{A_{2r}}{d} & \ldots & \frac{A_{rn}}{d} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ \frac{A_{1n}}{d} & \frac{A_{2n}}{d} & \ldots & \frac{A_{nn}}{d} \end{pmatrix},$$

где $d = \det A$, A_{ij} – *алгебраическое дополнение к элементу* a_{ij} *в матрице* A.

Д о к а з а т е л ь с т в о. Пусть $Y = (y_{ij}) = (\frac{A_{ji}}{d})$ – матрица из теоремы. Надо доказать, что $AY = YA = E$. Обозначим $AY = C$. Тогда

$$c_{pq} = \sum_{r=1}^{n} a_{pr} y_{rq} = \sum_{r=1}^{n} a_{pr} \frac{A_{qr}}{d} = \frac{1}{d} \sum_{r=1}^{n} a_{pr} A_{qr}.$$

По теореме 4 имеем

$$\frac{1}{d}\sum_{r=1}^{n} a_{pr}\,A_{qr} = \begin{cases} 1 & \text{если} \quad p = q, \\ 0 & \text{если} \quad p \neq q. \end{cases}$$

Следовательно, $C = E$ – единичная матрица. Аналогично проверяется, что $YA = E$. Теорема доказана.

Матрица

$$A^* = \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ .... & .... & .... & .... \\ A_{1r} & A_{2r} & \dots & A_{rn} \\ .... & .... & .... & .... \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix}$$

называется *присоединенной матрицей* к матрице A. Очевидно, что

$$AA^* = A^*A = \operatorname{diag}(d, d, \dots, d).$$

П р и м е р. Для матрицы

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

с отличным от нуля определителем $\det A = \alpha\,\delta - \beta\,\gamma \neq 0$ обратная находится по формуле

$$A^{-1} = \frac{1}{\alpha\,\delta - \beta\,\gamma} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}.$$

§ 7. Поле комплексных чисел

7.1. Определение. Предположим, что мы знаем, что такое поле действительных чисел $\mathbb{R}$. Хотим построить поле комплексных чисел $\mathbb{C}$. Для этого построим поле P со следующими свойствами:

1) $\mathbb{R}$ является подполем поля P;

2) в P существует элемент ξ, для которого справедливо равенство $\xi^2 + 1 = 0$;

3) подполе поля P, порожденное $\mathbb{R}$ и ξ совпадает с P.

Следующая теорема гарантирует существование такого поля P.

Т е о р е м а 1. *Поле P со свойствами* 1) – 3) *существует. Любые два поля со свойствами* 1) – 3) *изоморфны.* Любое из таких полей называется *полем комплексных чисел.*

Доказательство этой теоремы разобьем на две части. Вначале докажем существование, а потом единственность.

7.2. Существование поля комплексных чисел. Рассмотрим следующее подмножество матриц

$$C' = \left\{ \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \mid \alpha, \beta \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R}).$$

Покажем, что это множество с операциями сложения и умножения матриц является алгебраической системой Для этого надо убедиться, что операции сложения и умножения являются алгебраическими. Возьмем две матрицы

$$A = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}, \quad B = \begin{pmatrix} \gamma & \delta \\ -\delta & \gamma \end{pmatrix}$$

из C'. Находя их сумму и произведение, получим

$$A + B = \begin{pmatrix} \alpha+\gamma & \beta+\delta \\ -(\beta+\delta) & \alpha+\gamma \end{pmatrix}, \quad A \cdot B = \begin{pmatrix} \alpha\gamma - \beta\delta & \alpha\delta + \beta\gamma \\ -(\beta\gamma + \alpha\delta) & -\beta\delta + \alpha\gamma \end{pmatrix}.$$

Следовательно, операции действительно являются алгебраическими и мы имеем алгебраическую систему

$$\langle C'; +, \cdot \rangle.$$

Покажем, что эта алгебраическая система является полем. Для этого надо проверить все аксиомы поля. Аксиомы С1, С2, У1, СУ1, СУ2 выполняются для всех квадратных матриц. Чтобы проверить аксиому С3, заметим, что нулевая матрица принадлежит множеству C', чтобы проверить С4, заметим, что если некоторая матрица лежит в C', то и противоположная лежит в C'.

Для проверки У2 находим

$$A \cdot B = \begin{pmatrix} \alpha\gamma - \beta\delta & \alpha\delta + \beta\gamma \\ -\beta\gamma - \alpha\delta & -\beta\delta + \alpha\gamma \end{pmatrix}, \quad B \cdot A = \begin{pmatrix} \gamma\alpha - \delta\beta & \gamma\beta + \delta\alpha \\ -\gamma\beta - \delta\alpha & -\delta\beta + \gamma\alpha \end{pmatrix}.$$

Следовательно, $A \cdot B = B \cdot A$.

У3. Единичная матрица

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

очевидно лежит в C'.

Покажем наконец, что для всякой ненулевой матрицы $A \in C'$ найдется обратная, лежащая в C'. Так как A – ненулевая, то либо $\alpha \neq 0$, либо $\beta \neq 0$, а потому $\det A = \alpha^2 + \beta^2 \neq 0$. Следовательно, обратная матрица существует. Используя теорему о вычислении обратной матрицы, находим

$$A^{-1} = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} = \begin{pmatrix} \frac{\alpha}{\alpha^2+\beta^2} & -\frac{\beta}{\alpha^2+\beta^2} \\ \frac{\beta}{\alpha^2+\beta^2} & \frac{\alpha}{\alpha^2+\beta^2} \end{pmatrix},$$

т. е. A^{-1} лежит в C'. Следовательно, C' является полем.

Рассмотрим отображение $\varphi : \mathbb{R} \longrightarrow C'$, определенное формулой

$$\alpha\varphi = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \quad \text{где} \quad \alpha \in \mathbb{R}.$$

Легко заметить, что это отображение однозначно и унивалентно. Покажем, что оно сохраняет операции. Для этого надо проверить, что для любых $\alpha, \beta \in \mathbb{R}$ справедливы равенства:

$$(\alpha + \beta)\varphi = \alpha\varphi + \beta\varphi, \quad (\alpha \cdot \beta)\varphi = \alpha\varphi \cdot \beta\varphi.$$

Эти равенства следуют из правил сложения и умножения диагональных матриц:

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} = \begin{pmatrix} \alpha+\beta & 0 \\ 0 & \alpha+\beta \end{pmatrix}, \quad \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \cdot \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} = \begin{pmatrix} \alpha\cdot\beta & 0 \\ 0 & \alpha\cdot\beta \end{pmatrix}.$$

Заметим, что отображение φ не является отображением *на*, а является вложением.

Обозначим символом R' следующее подмножество диагональных матриц

$$R' = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \mid \alpha \in \mathbb{R} \right\} \subseteq C'.$$

Фактически мы доказали, что $\varphi(\mathbb{R}) = R'$, т. е. поле $\mathbb{R}$ измоморфно R'.

Введем множество

$$C = (C' \setminus R') \cup \mathbb{R}.$$

Хотим перенести операции из множества матриц C' на множество C.

П р и м е р. Рассмотрим сумму следующих матриц из C':

$$\begin{pmatrix} 3 & -1 \\ 1 & 3 \end{pmatrix} + \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}.$$

В результате получим матрицу из C', но она не входит в C.

Определим на C операции $+$ и $\cdot$ следующим образом. Если z_1 и z_2 – два элемента из C, то положим

$$z_1 + z_2 = \begin{cases} z_1 + z_2 & \text{если} \quad z_1 \notin R', z_2 \notin R', z_1 + z_2 \notin R', \\ \alpha & \text{если} \quad z_1 \notin R', z_2 \notin R', z_1 + z_2 = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \in R', \\ z_1 + \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} & \text{если} \quad z_1 \notin R', z_2 = \beta \in \mathbb{R}, \\ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + z_2 & \text{если} \quad z_1 = \alpha \in \mathbb{R}, z_2 \notin R', \\ \alpha + \beta & \text{если} \quad z_1 = \alpha \in \mathbb{R}, z_2 = \beta \in \mathbb{R}, \end{cases}$$

– их сумма;

$$z_1 \cdot z_2 = \begin{cases} z_1 \cdot z_2 & \text{если} \quad z_1 \notin R', z_2 \notin R', z_1 \cdot z_2 \notin R', \\ \alpha & \text{если} \quad z_1 \notin R', z_2 \notin R', z_1 \cdot z_2 = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \in R', \\ z_1 \cdot \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} & \text{если} \quad z_1 \notin R', z_2 = \beta \in \mathbb{R}, \\ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \cdot z_2 & \text{если} \quad z_1 = \alpha \in \mathbb{R}, z_2 \notin R', \\ \alpha \cdot \beta & \text{если} \quad z_1 = \alpha \in \mathbb{R}, z_2 = \beta \in \mathbb{R}, \end{cases}$$

– их произведение.

По построению, имеем изоморфизм:

$$\langle\, C;\, +,\, \cdot \,\rangle \simeq \langle\, C';\, +,\, \cdot \,\rangle.$$

Покажем, что C – то поле, которое мы хотели построить. Для этого надо проверить, что выполняются условия 1)–3):

1) по построению, поле $\mathbb{R}$ содержится в C;

2) покажем, что в качестве ξ можно взять матрицу

$$\imath = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in C.$$

Действительно,

$$\imath^2 = \imath \cdot \imath = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Последняя матрица не лежит в C, но в C лежит число -1. Следовательно,

$$\imath^2 = -1, \quad \text{т. е} \quad \imath^2 + 1 = 0;$$

3) покажем, что подполе поля C, порожденное $\mathbb{R}$ и $\imath$ совпадает с C. Для этого заметим, что

$$C = \{\alpha + \imath\, \beta \,|\, \alpha,\, \beta \in \mathbb{R}\}.$$

Действительно, рассмотрим произведение:

$$\imath\beta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} = \begin{pmatrix} 0 & \beta \\ -\beta & 0 \end{pmatrix}$$

и сумму:

$$\alpha + \imath\beta = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} 0 & \beta \\ -\beta & 0 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix},$$

но из таких матриц и состоит множество C.

Пусть теперь L – подполе поля C, порожденное $\mathbb{R}$ и $\imath$. В этом поле лежат вещественные числа, лежит $\imath$, а так как поле замкнуто относительно операций сложения и умножения, то и всякий элемент $\alpha+\imath\beta$ лежит в L, т. е. $C \subseteq L$, а по условию $L \subseteq C$. Следовательно, $L = C$ и существование доказано.

7.3. Единственность поля комплексных чисел. Надо доказать, что любые два поля со свойствами 1)–3) изоморфны. Вначале поймем, как устроено поле P. Докажем, что

$$P = \{\alpha + \xi\,\beta \,|\, \alpha, \beta \in \mathbb{R}\}.$$

Обозначим

$$M = \{\alpha + \xi\,\beta \,|\, \alpha, \beta \in \mathbb{R}\}.$$

Надо доказать два включения

$$P \supseteq M, \quad P \subseteq M.$$

Первое включение следует из того, что P содержит $\mathbb{R}$ и ξ.

Чтобы доказать второе включение, покажем, что M – подполе в P. Для этого надо доказать, что M замкнуто относительно сложения, умножения, взятия противоположного и обратного.

а) проверим, что M замкнуто относительно сложения, имеем

$$(\alpha + \xi\,\beta) + (\alpha' + \xi\,\beta') = (\alpha + \alpha') + \xi\,(\beta + \beta') \in M;$$

б) проверим, что M замкнуто относительно умножения, имеем

$$(\alpha + \xi\,\beta) \cdot (\alpha' + \xi\,\beta') = (\alpha\alpha' - \beta\beta') + \xi\,(\alpha\beta' + \alpha'\beta) \in M;$$

в) легко заметить, что противоположным к элементу $\alpha + \xi\,\beta$ является элемент $-(\alpha + \xi\,\beta) = (-\alpha) + \xi\,(-\beta)$;

г) рассмотрим $\alpha + \xi\,\beta \neq 0$, тогда

$$(\alpha + \xi\,\beta)^{-1} = \frac{\alpha}{\alpha^2 + \beta^2} - \xi\frac{\beta}{\alpha^2 + \beta^2} \in M.$$

Следовательно, M является подполем поля P.

Покажем, что M содержит все действительные числа и элемент ξ. Первое следует из равенства $\alpha = \alpha + \xi \cdot 0 \in M$, а второе из равенства $\xi = 0 + \xi \cdot 1 \in M$. Но тогда по свойству 3) определения поля P имеем включение $P \subseteq M$.

Докажем, что любое поле P со свойствами 1) – 3) изоморфно полю C'. Так как если два поля изоморфны некоторому третьему полю то они изоморфны между собой, то отсюда и последует нужное утверждение.

Т е о р е м а 2. *Отображение $\omega : C' \longrightarrow P$, действующее по правилу*

$$\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \omega = \alpha + \xi\,\beta,$$

является изоморфизмом.

Д о к а з а т е л ь с т в о. По определению изоморфизма мы должны проверить следующие условия для ω:

1) однозначность;

2) унивалентность;

3) отображение *на*;

4) для любых $z_1, z_2 \in C'$ справедливо равенство $(z_1 + z_2)\omega = z_1\omega + z_2\omega$;

5) для любых $z_1, z_2 \in C'$ справедливо равенство $(z_1 \cdot z_2)\omega = z_1\omega \cdot z_2\omega$.

Условие 1) справедливо в силу определения.

2) Пусть

$$\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \omega = \alpha + \xi\,\beta, \quad \begin{pmatrix} \alpha' & \beta' \\ -\beta' & \alpha' \end{pmatrix} \omega = \alpha' + \xi\,\beta',$$

и предположим, что $\alpha + \xi\,\beta = \alpha' + \xi\,\beta'$. Тогда $\alpha - \alpha' = \xi\,(\beta - \beta')$. Если $\beta - \beta' \neq 0$, то $\xi = \frac{\alpha - \alpha'}{\beta - \beta'} \in \mathbb{R}$, но в поле $\mathbb{R}$ нет элемента, удовлетворяющего равенству $\xi^2 + 1 = 0$. Противоречие. Следовательно $\beta = \beta'$, $\alpha = \alpha'$.

3) Было доказано выше, так как мы доказали, что

$$P = \{\alpha + \xi\,\beta \,|\, \alpha, \beta \in \mathbb{R}\}.$$

4) Левая часть равенства имеет вид

$$\left[\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} + \begin{pmatrix} \alpha' & \beta' \\ -\beta' & \alpha' \end{pmatrix}\right] \omega = \begin{pmatrix} \alpha + \alpha' & \beta + \beta' \\ -(\beta + \beta') & \alpha + \alpha' \end{pmatrix} \omega = (\alpha + \alpha') + \xi\,(\beta + \beta'),$$

правая часть имеет вид

$$(\alpha + \xi\,\beta) + (\alpha' + \xi\,\beta') = (\alpha + \alpha') + \xi\,(\beta + \beta').$$

Видим, что они равны, а потому равенство справедливо. Свойство 5) устанавливается аналогично. Теорема доказана.

Множество комплексных чисел будем обозначать символом

$$\mathbb{C} = \{a + \imath\, b \,|\, a, b \in \mathbb{R}\}.$$

7.4. Геометрическая интерпретация поля комплексных чисел. Как мы установили выше, всякое комплексное число $z \in \mathbb{C}$ единственным образом представимо в виде $z = a + \imath\, b$. Сопоставим этому числу точку на плоскости с координатами (a, b).

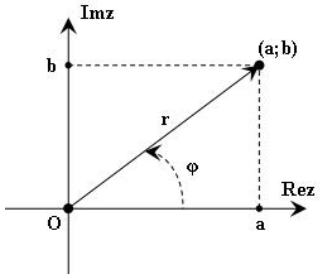

Рис. 1

Это же число z можно представить и в таком виде $z = r(\cos\varphi + \imath \sin\varphi)$, $r \in \mathbb{R}$, $r \geq 0$, $0 \leq \varphi < 2\pi$. При этом a называется *действительной частью числа* z и обозначается $\operatorname{Re} z$; b называется *мнимой частью числа* z и обозначается $\operatorname{Im} z$; $r = \sqrt{a^2 + b^2}$ называется *модулем числа* z и обозначается $|z|$, а φ называется *аргументом числа* z и обозначается $\arg z$.

Комплексно-сопряженным к числу $z = a + \imath\, b$ называется число $\overline{z} = a - \imath\, b$. Очевидно, если $z \in \mathbb{R}$, то $\overline{z} = z$.

У п р а ж н е н и е. $\operatorname{Re}(z_1 + z_2) = \operatorname{Re} z_1 + \operatorname{Re} z_2$, $\operatorname{Im}(z_1 + z_2) = \operatorname{Im} z_1 + \operatorname{Im} z_2$.

У п р а ж н е н и е. $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$, $\quad \arg(z_1 \cdot z_2) = \arg z_1 + \arg z_2$.

§ 8. Общая линейная группа и ее важнейшие подгруппы

Пусть $\mathrm{M}_n(P)$ – множество всех матриц степени n над полем P. Определим следующие множества

$$\mathrm{GL}_n(P) = \{A \in \mathrm{M}_n(P) \,|\, \det A \neq 0\},$$
$$\mathrm{SL}_n(P) = \{A \in \mathrm{M}_n(P) \,|\, \det A = 1\},$$
$$\mathrm{O}_n(P) = \{A \in \mathrm{M}_n(P) \,|\, A \cdot A' = E\},$$
$$\mathrm{U}_n = \left\{A \in \mathrm{M}_n(\mathbb{C}) \,|\, A \cdot \overline{A'} = E\right\},$$

где A' – матрица, транспонированная к A, а $\overline{A'}$ – матрица, полученная из A транспонированием и взятием комплексно-сопряженного к каждому элементу, т. е. если $A = (a_{ij})$, то в матрице A' на месте (i, j) стоит элемент a_{ji}, а в матрице $\overline{A'}$ на месте (i, j) стоит элемент $(\overline{a_{ji}})$. Множество U_n мы определяем только в случае, когда $P = \mathbb{C}$ – поле комплексных чисел.

Заметим, что в определении $\mathrm{O}_n(P)$ мы требуем, чтобы выполнялось равенство $A \cdot A' = E$, которое означает, что для A существует правая обратная, но по теореме о существовании обратной матрицы отсюда следует, что A' является и левой обратно, т. е. справедливо равенство $A' \cdot A = E$. Аналогичным образом, получаем, что всякая матрица A из U_n удовлетворяет равенству $\overline{A'} \cdot A = E$.

Покажем, что все эти множества являются группами относительно умножения матриц. Для этого нам потребуются два вспомогательных утверждения.

Л е м м а 1. *Для любых матриц* $A, B \in \mathrm{M}_n(P)$ *справедливо равенство*

$$(A \cdot B)^t = B^t \cdot A^t.$$

Д о к а з а т е л ь с т в о. Обозначим

$$A \cdot B = C, \quad C^t = D, \quad A^t = F, \quad B^t = G, \quad G \cdot F = H.$$

Надо доказать, что $D = H$. Имеем

$$d_{ij} = c_{ji} = \sum_{k=1}^{n} a_{jk}\, b_{ki},$$

$$h_{ij} = \sum_{k=1}^{n} g_{ik}\, f_{kj} = \sum_{k=1}^{n} b_{ki}\, a_{jk} = \sum_{k=1}^{n} a_{jk}\, b_{ki},$$

т. е. $d_{ij} = h_{ij}$. Лемма доказана.

Л е м м а 2. *Для любой матрицы* $A \in \mathrm{GL}_n(P)$ *справедливо равенство*

$$(A^t)^{-1} = (A^{-1})^t.$$

Д о к а з а т е л ь с т в о следует из равенства

$$(A^{-1})^t \cdot A^t = (A\, A^{-1})^t = E^t = E.$$

Т е о р е м а. *Относительно матричного умножения* $\mathrm{GL}_n(P)$ *– группа, а* $\mathrm{SL}_n(P)$, $\mathrm{O}_n(P)$ *– ее подгруппы.*

Д о к а з а т е л ь с т в о. Установим, что $\mathrm{GL}_n(P)$ – группа. Пусть A, B – две матрицы из $\mathrm{GL}_n(P)$. Тогда $\det A \neq 0$, $\det B \neq 0$ и по свойству определителей

$$\det(AB) = \det A \cdot \det B \neq 0.$$

Следовательно, операция умножения является алгебраической на множестве $\mathrm{GL}_n(P)$. Проверим аксиомы группы. Ассоциативность умножения выполнена в $\mathrm{M}_n(P)$, а потому и в $\mathrm{GL}_n(P)$. Единичная матрица существует в $\mathrm{M}_n(P)$ и, очевидно, она лежит в $\mathrm{GL}_n(P)$. Так как для всякой матрицы $A \in \mathrm{GL}_n(P)$ ее определитель отличен от нуля, то существует A^{-1} такая, что $A \cdot A^{-1} = E$. Тогда из свойства определителей $\det A \cdot \det A^{-1} = 1$, а потому $\det A^{-1} \neq 0$. Следовательно, A^{-1} лежит в $\mathrm{GL}_n(P)$. Таким образом, мы доказали, что $\mathrm{GL}_n(P)$ является группой.

Очевидно, что множества $\mathrm{SL}_n(P)$, $\mathrm{O}_n(P)$, содержатся в $\mathrm{GL}_n(P)$. Чтобы доказать, что каждое из них является подгруппой, надо доказать замкнутость относительно умножения и взятия обратного.

Если A, B – две матрицы из $\mathrm{SL}_n(P)$, то

$$\det(AB) = \det A \cdot \det B = 1,$$

т. е. их произведение опять лежит в $\mathrm{SL}_n(P)$. Мы знаем, что A^{-1} существует, а из того, что $\det A \cdot \det A^{-1} = 1$ следует, что $\det A^{-1} = 1$. Таким образом, A^{-1} тоже лежит в $\mathrm{SL}_n(P)$ и мы установили, что $\mathrm{SL}_n(P)$ – подгруппа группы $\mathrm{GL}_n(P)$.

Рассмотрим множество $\mathrm{O}_n(P)$. Так как $A \cdot A^{-1} = E$, то $\det A \neq 0$, а потому $\mathrm{O}_n(P)$ содержится в $\mathrm{GL}_n(P)$. Если A и B – две матрицы из $\mathrm{O}_n(P)$, то $A \cdot A^t = E$ и $B \cdot B^t = E$. Произведение $A \cdot B$ лежит в $\mathrm{O}_n(P)$ если

$$(AB) \cdot (AB)^t = E.$$

Обратная матрица A^{-1} лежит в $\mathrm{O}_n(P)$ если

$$(A^{-1}) \cdot (A^{-1})^t = E.$$

По лемме 1,

$$(A\,B) \cdot (A\,B)^t = (A\,B) \cdot (B^t\,A^t) = A \cdot (B\,B^t)\,A^t = E.$$

Следовательно, множество $\mathrm{O}_n(P)$ замкнуто относительно умножения.

Для доказательства замкнутости относительно взятия обратного воспользуемся леммой 2. Таким образом, множество $\mathrm{O}_n(P)$ является подгруппой. Теорема доказана.

У п р а ж н е н и е. Докажите, что U_n является подгруппой группы $\mathrm{GL}_n(\mathbb{C})$.

Определенные нами группы носят специальные названия. Группа $\mathrm{GL}_n(P)$ называется *общей линейной группой*, группа $\mathrm{SL}_n(P)$ – *специальной линейной группой*, группа $\mathrm{O}_n(P)$ – *ортогональной линейной группой* и U_n – *унитарной линейной группой.*