Оглавление

Глава 1

Кольца алгебраических целых элементов

1.1 Введение

Определение 1. Конечное расширение $\mathbb{Q}$ называется алгебраическим числовым полем.

Определение 2. Пусть K — алгебраическое числовое поле, $\alpha \in K$ называется алгебраическим целым элементом, если существует унитарный многочлен $h \in \mathbb{Z}[x]$ такой, что $h(\alpha) = 0$. Множество всех алгебраических целых элементов из K обозначается как $\mathcal{O}_K$.

Чуть позже мы докажем, что $\mathcal{O}_K$ является подкольцом K.

Одной из ключевых задач алгебраической теории чисел является выяснение, когда кольцо $\mathcal{O}_K$ факториально. Например, в $\mathbb{Z}[\sqrt{-5}]$ имеем два разложения

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

и факториальности нет.

Важная идея, восходящая к Куммеру, заключается в разложении главного идеала в произведение простых: $(a) = p_1 p_2 \cdot \ldots \cdot p_n$. Для примера выше имеем

$$(6) = (2, 1 + \sqrt{-5})^2 (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

В курсе мы построим группу дробных идеалов I, в которой главные дробные идеалы (a), $a \in K^*$, образуют подгруппу P конечного индекса. Обозначим $h_K = (I : P)$. Мы покажем, что

$$h_K = 1 \iff \mathcal{O}_K \text{ — область главных идеалов} \iff \mathcal{O}_K \text{ факториально.}$$

В отличие от $\mathbb{Z}$ кольцо $\mathcal{O}_K$ может содержать бесконечно много единиц (обратимых элементов). Мы докажем, что $\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^r$, где $\mu(K)$ — конечная группа, состоящая из комплексных корней из единицы, которые лежат в K. Число r мы также определим. Указанный результат есть теорема Дирихле о единицах.

Наконец, обратимся к Великой теореме Ферма. Пусть p — нечётное простое число, $x, y, z \in \mathbb{Z} \setminus \{0\}$ такие, что $x^p + y^p = z^p$. Тогда

$$x^p = z^p - y^p = \prod_{i=0}^{p-1}(z - \xi_p^i y), \quad \xi_p = e^{2\pi i/p}.$$

Ламе в 1840-е годы вывел, что в силу взаимной простоты $z - \xi_p^i y$ каждая из этих скобок также является p-й степенью какого-то элемента из $\mathcal{O}_K$, где $K = \mathbb{Q}[\xi_p]$. Оказалось, что в общем случае из-за отсутствия факториальности в $\mathcal{O}_K$ такой вывод не верен. Идею Ламе развил Куммер, доказавший Великую теорему Ферма для регулярных простых, т. е. таких простых p, что $p \nmid h_K$.

1.2 Целая зависимость

Все рассматриваемые кольца коммутативны и с единицей, все ненулевые подкольца также содержат единицу всего кольца.

Определение 3. Пусть A — подкольцо (кольца) R, элемент $r \in R$ называется целым над A, если существует унитарный многочлен $f(x) \in A[x]$ такой, что $f(r) = 0$. Уравнение $f(x) = 0$ будем называть уравнением целой зависимости для r.

Алгебраическим целым называется $x \in \mathbb{C}$ целое над $\mathbb{Z}$.

Предложение 1. Пусть A — подкольцо R, $r \in R$. Следующие утверждения эквивалентны:

(1) элемент r цел над A,

(2) $A[r]$ — конечнопорождённый A-модуль,

(3) $A[r]$ содержится в подкольце B кольца R, причём B есть конечнопорождённый A-модуль.

(4) существует точный $A[r]$-модуль M такой, что M конечно порождён как A-модуль.

Доказательство. (1) $\Rightarrow$ (2). Пусть $f(x) \in A[x]$ — унитарный многочлен такой, что $f(r) = 0$. Обозначим $n = \deg f$, тогда $A[r]$ порождается над A элементами $1, r, \ldots, r^{n-1}$.

(2) $\Rightarrow$ (3). Берём $B = A[r]$.

(3) $\Rightarrow$ (4). Берём $M = B$. Так как $1_R \in B$, равенство $yB = 0$ влечёт $y = 0$.

(4) $\Rightarrow$ (1). Пусть $m_1, \ldots, m_n$ — порождающие M над A, при этом $rm_i = \sum\limits_{j=1}^{n} c_{ij} m_j$ для некоторых $c_{ij} \in A$. Обозначим $\vec{m} = (m_1, \ldots, m_n)^T$ и $C = (c_{ij})_{i,j=1}^n$, тогда

$$(rE - C)\vec{m} = 0, \tag{1.1}$$

где E обозначает единичную матрицу.

Определим $D = rE - C$, тогда, умножая (1.1) слева на сопряжённую матрицу D^*, получаем

$$D^*(D\vec{m}) = \det(D)\vec{m} = 0.$$

Значит, $\det(D)M = 0$ и в силу точности M заключаем, что $\det(D) = 0$. Зададим $f(x) = \det(xE - C)$, тогда $f(x)$ — унитарный многочлен из $A[x]$ и $f(r) = 0$. $\square$

Лемма 1. Пусть A — подкольцо R, $r_1, \ldots, r_n \in R$ — целые над A. Тогда $A[r_1, \ldots, r_n]$ — конечнопорождённый A-модуль.

Доказательство. Ведём индукцию по n, случай $n = 1$ следует из предложения 1. Пусть $\tilde{A} = A[r_1, \ldots, r_{n-1}]$ — конечнопорождённый A-модуль с порождающими $a_1, \ldots, a_t$. Поскольку r_n цел над $\tilde{A}$, найдётся $k \in \mathbb{N}$ такое, что $\tilde{A}[r_n]$ порождается над $\tilde{A}$ элементами $1, r_n, \ldots, r_n^k$. Тем самым элементы $a_i r_n^j$, $1 \leq i \leq t$, $0 \leq j \leq k$, порождают $A[r_1, \ldots, r_n]$ как A-модуль. □

Теорема 1. Пусть A — подкольцо R, множество всех элементов R целых над A (целое замыкание A в R) является подкольцом в R, содержащим A.

Доказательство. Пусть $b, c \in R$ — целые над A. По лемме 1 кольцо $A[b, c]$ — конечнопорождённый A-модуль. По предложению 1 (эквивалентность (1) $\Leftrightarrow$ (3)) элементы $b \pm c, bc \in A[b, c]$ являются целыми над A. Остаётся заметить, что любой $a \in A$ есть корень многочлена $x - a \in A[x]$, значит, A содержится в целом замыкании A в R. □

Лемма 2. Пусть A, B, C — подкольца R. Если C цело над B, т. е. любой элемент C цел над B, и B цело над A, то и C цело над A.

Доказательство. Пусть $r \in C$ и $r^n + b_{n-1}r^{n-1} + \ldots + b_r + b_0 = 0$, где $b_i \in B$. Значит, r цел над $A[b_0, \ldots, b_{n-1}]$, которое по лемме 1 является конечнопорождённым A-модулем. Поэтому и $(A[b_0, \ldots, b_{n-1}])[r]$ также является конечнопорождённым A-модулем. По предложению 1 ((1) $\Leftrightarrow$ (3)) r цел над A. □

Лемма 3. Пусть A — подкольцо R, а $\bar{A}$ — целое замыкание A в R. Тогда целое замыкание $\bar{A}$ в R совпадает с $\bar{A}$.

Доказательство. По определению $\bar{A}$ цело над A. Пусть $r \in R$ цел над $\bar{A}$, тогда по лемме 2 элемент r цел над A, и поэтому $r \in \bar{A}$. □

Определение 4. Область целостности A называется целозамкнутой, если целое замыкание A в её поле частных $Q(A)$ совпадает с A.

Из леммы 3 получаем

Следствие 1. Пусть A — область целостности, $\bar{A}$ — целое замыкание A в алгебраическом расширении L поля $Q(A)$. Тогда $\bar{A}$ целозамкнута.

Доказательство. Обозначим целое замыкание S в R как $\bar{S}^R$. Тогда $\overline{\bar{A}^L}^{Q(\bar{A})} = \bar{A}^L$ по лемме 3, поскольку $Q(\bar{A}) \subseteq L$. □

В частности, кольцо алгебраических целых $\mathcal{O}_K$ элементов из алгебраического числового поля K есть целозамкнутая область целостности. Нас интересует, при каких условиях целозамкнутая область целостности $\mathcal{O}_K$ факториальна. Докажем в некотором роде обратный результат.

Предложение 2. Пусть A — факториальная область целостности. Тогда A целозамкнута.

Доказательство. Пусть $r \in Q(A)$ и $r = a/b$, где $a, b \in A$ взаимно просты. Если r цел над A, тогда

$$(a/b)^n + c_{n-1}(a/b)^{n-1} + \ldots + c_1 a/b + c_0 = 0$$

для некоторых $c_i \in A$. Отсюда $a^n + b\tilde{c} = 0$ для некоторого $\tilde{c} \in A$. Элемент b делит a^n, в силу взаимной простоты a и b заключаем, что b — единица в A и $r = a/b \in A$. □

1.3 Локализация

Пусть R — область целостности, $(\emptyset \neq) S \subset R$ — мультипликативное подмножество, т. е. $0 \notin S$ и $a, b \in S$ влечёт, что $ab \in S$. Построим кольцо, содержащее R, в котором каждый элемент из S обратим. Для этого достаточно рассмотреть в поле частных $Q(R)$ подкольцо R_S, состоящее из дробей вида $\{f/g \mid g \in S\}$.

Определение 5. Пусть R — область целостности, $(\emptyset \neq) S \subset R$ — мультипликативное подмножество. Тогда кольцо R_S называется локализацией R относительно S.

Пример 1. Пусть $R = \mathbb{Z}$ и $S = \{1, n, n^2, \ldots\}$, где $n \in \mathbb{N}_{>0}$. Тогда $R_S = \{a/n^i \mid a \in \mathbb{Z},\ i \geq 0\}$.

Заметим, что при $S = R \setminus \{0\}$ получаем равенство $R_S = Q(R)$.

Пусть $1 \notin S$, тогда для расширенного мультипликативного множества $S' = S \cup \{1\}$ имеем $R_S = R_{S'}$. Поэтому можем считать, что S всегда содержит единицу кольца R. При этом вложение R в R_S осуществляется так: $r \to r/1$.

Определение 6. Идеал p кольца R называется простым (в некоммутативном случае первичным), если $p \neq R$ и для любых $a, b \in R$ принадлежность $ab \in p$ влечёт, что $a \in p$ или $b \in p$.

Идеал p кольца R прост тогда и только тогда, когда R/p — область целостности. Поэтому любой максимальный идеал является простым.

Теорема 2. Пусть R — область целостности, $S \subset R$ — мультипликативное подмножество. Существует взаимно однозначное соответствие между простыми идеалами R, не пересекающимися с S и простыми идеалами R_S. При этом соответствии простой идеал p кольца R переходит в простой идеал pR_S кольца R_S.

Доказательство. Пусть q — простой идеал R_S. Тогда $p = q \cap R$ — идеал в R, более того, p — простой идеал R, это следует из простоты q и определения 6. Ясно, что $pR_S \lhd R_S$ и $pR_S \subseteq q$. Покажем, что $pR_S = q$. Пусть $a/s \in q$, где $a \in R$ и $s \in S$. Тогда $(a/s)s = a \in p$, тем самым $a/s = a(1/s) \in pR_S$. Во-первых, мы доказали, что любой идеал в R_S имеет вид pR_S для некоторого идеала p в R. Во-вторых, из простоты идеала q следует, что $q \neq R_S$. Значит, q не содержит обратимых элементов, то есть $p \cap S = \emptyset$.

Пусть p — простой идеал R и $p \cap S = \emptyset$. Определим $q = pR_S$ и покажем, что q — простой идеал R_S. Пусть $r = a/s$ и $r' = a'/s'$ из R_S, где $r, r' \in R$, $s, s' \in S$, при этом $rr' \in q$. Тогда $rr' = aa'/ss' = \tilde{a}/\tilde{s}$ для подходящих $\tilde{a} \in p$ и $\tilde{s} \in S$. Следовательно, $aa'\tilde{s} = ss'\tilde{a} \in p$. Так как $p \cap S = \emptyset$, выводим, что $a \in p$ или $a' \in p$. Это влечёт, что $r \in q$ или $r' \in q$, то есть q — простой идеал. Наконец, покажем, что $p = q \cap R$. Имеем $p \subseteq q \cap R$, докажем обратное включение. Пусть $r \in q \cap R$, тогда $r = a/s$, где $a \in p$ и $s \in S$. Значит, $rs = a \in p$. Поскольку $s \notin p$, с необходимостью $r \in p$.

Мы показали, что соответствия $p \to pR_S$ и $q \to q \cap R$ взаимно обратны. □

Пусть p — простой идеал кольца R, а $S = R \setminus p$. Тогда S — мультипликативное множество в R, и R_S состоит из дробей a/b, где $b \notin p$. Для удобства будем обозначать $R_{R \setminus p}$ как R_p и называть локализацией относительно простого идеала p.

Определение 7. Кольцо, обладающее единственным максимальным идеалом, называется локальным кольцом.

Согласно определению произвольное поле F является локальным кольцом, поскольку F содержит единственный максимальный идеал, это (0).

Предложение 3. Пусть p — простой идеал области целостности R. Тогда R_p есть локальное кольцо, а pR_p — его единственный максимальный идеал.

Доказательство. По теореме 2 выполнено, что pR_p — простой идеал в R_p. Пусть Q — максимальный идеал в R_p. Так как Q прост, по теореме 2 он имеет вид qR_p для некоторого простого идеала q в R такого, что $q \cap (R \setminus p) = \emptyset$. Значит, $q \subseteq p$ и $Q \subseteq pR_p$. В силу максимальности получаем равенство $Q = pR_p$. □

Лемма 4. Пусть R — целозамкнутая область целостности, $S \subset R$ — мультипликативное подмножество. Тогда R_S целозамкнута.

Доказательство. Пусть $u \in Q(R)$ цел над R_S, тогда u — корень многочлена

$$h(x) = x^n + (r_{n-1}/s_{n-1})x^{n-1} + \ldots + r_0/s_0$$

для некоторых $r_i \in R$ и $S_i \in S$. Обозначим $s = s_0 \ldots s_{n-1}$, тогда $h(x) = x^n + (r'_{n-1}/s)x^{n-1} + \ldots + r'_0/s$, где $r'_i \in R$. Отсюда su — корень многочлена

$$x^n + r'_{n-1}x^{n-1} + sr'_{n-2}x^{n-1} + \ldots + s^{n-1}r'_0,$$

коэффициенты которого лежат в R. Значит, $su \in R$ и $u = su/s \in R_S$. □

1.4 Норма и след

Пусть F — поле, E — конечное расширение F. Для $x \in E$ определим $r_x \colon E \to E$ по правилу $r_x(y) = yx$. Выберем базис $u_1, \ldots, u_n$ пространства E над полем F, и пусть $A(x) = [r_x]_{u_1,\ldots,u_n}$, это матрица, столбцами которой являются векторы $r_x(u_i)$. Определим след и норму элемента $x \in E$ следующим образом:

$$T_{E/F}(x) = \mathrm{tr}(r_x) = \mathrm{tr}(A(x)), \quad N_{E/F}(x) = \det(r_x) = \det(A(x)).$$

Характеристическим многочленом элемента $x \in E$ называется $\mathrm{char}^x_{E/F}(t) = \det(tI - A(x))$, где I — единичная матрица. Известно, что

$$\mathrm{char}^x_{E/F}(t) = t^n - T_{E/F}(x)t^{n-1} + \ldots + (-1)^n N_{E/F}(x). \tag{1.2}$$

Лемма 5. Пусть E — конечное расширение поля F, $x, y \in E$, $a \in F$. Тогда

(1) $T_{E/F}(x + y) = T_{E/F}(x) + T_{E/F}(y)$, $T_{E/F}(ax) = aT_{E/F}(x)$;

(2) $N_{E/F}(xy) = N_{E/F}(x)N_{E/F}(y)$, $N_{E/F}(ax) = a^n N_{E/F}(x)$, где $n = \dim_F(E) = [E : F]$;

(3) если K — такое поле, что $F \subseteq K \subseteq E$, то $T_{E/F}(x) = T_{K/F}(T_{E/K}(x))$.

Доказательство. (1) и (2) следуют из равенств $r_{x+y} = r_x + r_y$, $r_{xy} = r_x r_y$ и $r_a = a \cdot \mathrm{id}$, то есть $A(a) = aI$.

(3) Пусть $a_1, \ldots, a_k$ — базис K над F, $b_1, \ldots, b_m$ — базис E над K. Для $x \in E$ и $y \in K$ имеем

$$xb_i = \sum_j \beta_{ji}(x)b_j, \quad ya_p = \sum_q \alpha_{qp}(y)a_q$$

для некоторых $\beta_{ji}(x) \in K$ и $\alpha_{qp}(y) \in F$.

Тогда $T_{K/F}(y) = \sum\limits_p \alpha_{pp}(y)$ и $T_{E/K}(x) = \sum\limits_i \beta_{ii}(x)$. Следовательно,

$$T_{K/F}(T_{E/K}(x)) = \sum_p \sum_i \alpha_{pp}(\beta_{ii}(x)).$$

С другой стороны, множество произведений $a_i b_j$ образует базис E над F,

$$xa_s b_t = \sum_j a_s \beta_{jt}(x) b_j = \sum_j \sum_i \alpha_{is}(\beta_{jt}(x)) a_i b_j.$$

Таким образом, $T_{E/F}(x) = \sum\limits_j \sum\limits_i \alpha_{ii}(\beta_{jj}(x))$. □

Лемма 6. Пусть E — конечное расширение поля F, $m_F^x(t)$ — минимальный многочлен элемента $x \in E$ над полем F. Тогда $\mathrm{char}_{E/F}^x(t) = (m_F^x(t))^r$, где $r = [E : F(x)]$.

Доказательство. Рассмотрим случай $r = 1$, то есть $E = F(x)$. Во-первых, $\deg(\mathrm{char}_{E/F}^x(t)) = n = \deg(m_F^x(t)) = [F(x) : F]$. Во-вторых, по теореме Гамильтона — Кэли выполняется $\mathrm{char}_{E/F}^x(r_x) = 0$. Тем самым $\mathrm{char}_{E/F}^x(x) = \mathrm{char}_{E/F}^x(r_x)1 = 0$. В силу унитарности многочленов заключаем, что $\mathrm{char}_{E/F}^x(t) = m_F^x(t)$.

Пусть $r > 1$, обозначим через $y_1, \ldots, y_s$ базис $F(x)$ над F и через $z_1, \ldots, z_r$ — базис E над $F(x)$. Введём $r_x(y_i) = \sum\limits_{k=1}^{s} a_{ki} y_k$ для некоторых $a_{ki} \in F$ и выпишем матрицу $A = (a_{ki})_{k,i=1}^s$ оператора умножения на x в расширении $F(x)/F$. В базисе $y_1 z_1, y_2 z_1, \ldots, y_s z_1, y_1 z_2, y_2 z_2, \ldots, y_s z_2, \ldots, y_1 z_r, \ldots, y_s z_r$ получаем в расширении E/F блочно-диагональную матрицу

$$[r_x]_{y_i z_j} = \begin{pmatrix} A & 0 & \ldots & 0 \\ 0 & A & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & A \end{pmatrix}$$

с r блоками равными A. Отсюда $\mathrm{char}_{E/F}^x(t) = (\det(tI - A))^r = (m_F^x(t))^r$, последнее равенство следует из уже разобранного случая $r = 1$. □

Следствие 2. Пусть E — конечное расширение поля F, $x \in E$, $[E : F] = n$, $[F(x) : F] = d$. Пусть $x_1, \ldots, x_d$ — корни $m_F^x(t)$ в $\bar{F}$. Тогда

$$\mathrm{char}_{E/F}^x(t) = \left(\prod_{i=1}^{d}(t - x_i)\right)^{n/d}, \quad T_{E/F}(x) = \frac{n}{d}\sum_{i=1}^{d} x_i, \quad N_{E/F}(x) = \left(\prod_{i=1}^{d} x_i\right)^{n/d}.$$

Доказательство. Равенство для характеристического многочлена следует из леммы 6. Далее,

$$N_{E/F}(x) = (-1)^n \left(\prod_{i=1}^{d}(-x_i)\right)^{n/d} = (-1)^{n+n}\left(\prod_{i=1}^{d} x_i\right)^{n/d} = \left(\prod_{i=1}^{d} x_i\right)^{n/d}.$$

Наконец, пусть $m_F^x(t) = t^d + a_{d-1}t^{d-1} + \ldots$, тогда по формулам Виета

$$T_{E/F}(x) = -(m_F^x(t))^{n/d}|_{t^{n-1}} = -(n/d)a_{d-1} = n/d\sum_{i=1}^{d} x_i. \quad \square$$

В случае, когда E — конечное сепарабельное расширение поля F степени n, мы получаем дополнительные выражения для характеристического многочлена, нормы и следа элемента из E. Напомним из теории Галуа, что при этих условиях существует ровно n различных инъективных вложений $\sigma_1, \dots, \sigma_n$ поля E в поле $\bar{F}$ (или в композит E и нормального замыкания поля F), тождественных на F. Поскольку любое конечное сепарабельное расширение является простым, то есть найдётся такой элемент $z \in E$, что $E = F(z)$, то σ_i задаются так: $\sigma_i|_F = \mathrm{id}$, $\sigma_i(z) = z_i$, где $(z =)z_1, \dots, z_n$ — корни минимального многочлена $m_F^z(t)$. Если расширение E поля F является нормальным, то вложения σ_i индуцируют автоморфизмы поля E.

Предложение 4. Пусть E — конечное сепарабельное расширение поля F степени n и $\sigma_1, \dots, \sigma_n$ — различные инъективные вложения поля E в $\bar{F}$, тождественные на F. Тогда для любого $x \in E$ выполнено

$$\mathrm{char}_{E/F}^x(t) = \prod_{i=1}^{n}(t - \sigma_i(x)), \quad T_{E/F}(x) = \sum_{i=1}^{n}\sigma_i(x), \quad N_{E/F}(x) = \prod_{i=1}^{n}\sigma_i(x).$$

Доказательство. Пусть $x_1, \dots, x_d$ — корни $m_F^x(t)$ в $\bar{F}$, тогда каждое из d различных F-вложений τ_i поля $F(x)$ в $\bar{F}$ отображает x в уникальный элемент x_i, и τ_i продолжается в точности до $n/d = [E : F(x)]$ F-вложений E в $\bar{F}$. Тогда набор $(\sigma_1(x), \dots, \sigma_n(x))$ состоит из $\tau_i(x) = x_i$, перечисленных n/d раз. Остаётся применить следствие 2:

$$\prod_{j=1}^{n}(t - \sigma_j(x)) = \left(\prod_{i=1}^{d}(t - \tau_i(x))\right)^{n/d} = \left(\prod_{i=1}^{d}(t - x_i)\right)^{n/d} = (m_F^x(t))^{n/d} = \mathrm{char}_{E/F}^x(t).$$

Формулы для следа и нормы выводятся из полученного равенства. □

Следствие 3. Пусть $F \subseteq K \subseteq E$ — башня конечных сепарабельных расширений. Тогда для любого $x \in E$ выполнено $N_{E/F}(x) = N_{K/F}(N_{E/K}(x))$.

Доказательство. Пусть L — нормальное расширение F, содержащее E (например, композит $\bar{F}^{\mathrm{norm}}$ и E). Обозначим через $\sigma_1, \dots, \sigma_n$ различные F-вложения K в L, а через $\tau_1, \dots, \tau_m$ — различные K-вложения E в L. Поскольку расширение L/F нормально, каждое из отображений σ_i, τ_j продолжается (каким-то образом) до автоморфизма L, поэтому можно рассматривать их композиции.

По предложению 4 имеем

$$N_{K/F}(N_{E/K}(x)) = \prod_{i=1}^{n}\sigma_i\left(\prod_{j=1}^{m}\tau_j(x)\right) = \prod_{i=1}^{n}\prod_{j=1}^{m}\sigma_i(\tau_j(x)).$$

Каждое из отображений $\sigma_i \circ \tau_j$ есть F-вложение E в L, их количество равно $nm = [E : K] \cdot [K : F] = [E : F]$. Отображения $\sigma_i \circ \tau_j|_E$ попарно различны. Действительно, пусть $\sigma_i \circ \tau_j = \sigma_k \circ \tau_l$. Тогда при ограничении этих отображений на поле K, получаем, что $\sigma_i = \sigma_k$. Отсюда выводим, что $\tau_j = \tau_l$ при ограничении на E.

Значит, по предложению 4 выполняется $N_{E/F}(x) = \prod_{i,j}(\sigma_i \circ \tau_j)(x)$. □

Пусть E/F — конечное расширение, определим симметричную билинейную форму $E \times E \to F$ как $(x, y) = T_{E/F}(xy)$.

Теорема 3. Конечное расширение E поля F сепарабельно тогда и только тогда, когда форма (x, y) невырожденная.

Доказательство. Пусть E/F — сепарабельное расширение. Предположим, что найдётся такой $x \in E$, что $(x, E) = 0$, то есть $T_{E/F}(xE) = 0$. Поскольку E — поле, получаем, что $T_{E/F}(E) = 0$. По предложению 4 это влечёт, что $\sum\limits_{i=1}^{n} \sigma_i(y) = 0$ для любого $y \in E$, где $n = [E : F]$. Это противоречит лемме Дедекинда.

Лемма 7 (Дедекинд). Любой набор различных вложений поля E в его надполе E' линейно независим над E'.

Доказательство. Пусть $\{\sigma_i \mid i \in I\}$ — набор различных вложений E в E'. Выберем его линейно зависимый поднабор $\sigma_1, \ldots, \sigma_r$ минимальной длины, тогда

$$\sigma_1(x) = \sum_{i=2}^{r} \alpha_i \sigma_i(x), \quad x \in E, \quad \alpha_i \in E'. \tag{1.3}$$

Подставим в (1.3) вместо x элемент xy:

$$\sigma_1(x)\sigma_1(y) = \sum_{i=2}^{r} \alpha_i \sigma_i(x)\sigma_i(y). \tag{1.4}$$

Умножая (1.3) на $\sigma_1(y)$ и вычитая из (1.4), получим

$$\sum_{i=2}^{r} \alpha_i \sigma_i(x)(\sigma_i(y) - \sigma_1(y)) = 0.$$

Поскольку последнее равенство выполнено для всех $x \in E$, значит, по выбору r имеем $\alpha_i(\sigma_i(y) - \sigma_1(y)) = 0$. Отображения σ_j попарно различные, значит, $\alpha_i = 0$. Заметим, что $\sigma_1(x) \not\equiv 0$, так как $\sigma_1(1) = 1$. □

Вернёмся к доказательству теоремы 3. Предположим, что форма невырожденная, но при этом расширение E поля F не является сепарабельным. Отсюда $\operatorname{char} F = p > 0$, где p — простое число, и мы можем рассмотреть сепарабельное замыкание[1] K поля F в E. Тогда выполнены следующие условия:

а) $\dim_K E = p^m$ для некоторого $m \geq 1$,

б) для $z \in E \setminus K$ минимальный многочлен $m_K^z(t)$ имеет вид $t^{p^s} - a$ для некоторых $s \geq 1$ и $a \in K$.

Покажем, что $(x, E) = 0$ для всех $x \in E \setminus K$. Если для $x \in E \setminus K$ и $y \in E$ выполнено $xy \notin K$, тогда б) влечёт, что $\operatorname{char}_K^{xy}(t) = (t^{p^s} - a)^{p^{m-s}}$ для некоторых $s \geq 1$ и $a \in K$. По (1.2) получаем $T_{E/K}(xy) = 0$. Применяем лемму 5, (3):

$$(x, y) = T_{E/F}(xy) = T_{K/F}(T_{E/K}(xy)) = 0.$$

Если $xy \in K$, тогда $T_{E/K}(xy) = xyT_{E/K}(1) = xyp^m = 0$, то есть также $(x, y) = 0$. Тем самым форма $(\cdot, \cdot)$ вырожденная, пришли к противоречию. □

[1] Ленг, Алгебра, стр. 250.

Предложение 5. Пусть A — область целостности, $K = Q(A)$, L — конечное сепарабельное расширение K, $B = \bar{A}^L$. Для $x \in B$ коэффициенты многочленов $\mathrm{char}^x_{L/K}(t)$ и $m^x_K(t)$ целы над A.

Доказательство. По формулам Виета и лемме 6 достаточно показать, что все корни x_i минимального многочлена $m^x_K(t)$ целы над A. Пусть $h(t)$ — уравнение целой зависимости для элемента $x \in B$ над A. Поскольку $A \subset K$, многочлен $h(t)$ делится на $m^x_K(t)$. Поэтому все элементы $x_1, \ldots, x_n$ являются корнями $h(t)$, значит, они целы над A. □

Следствие 4. В обозначениях предложения 5 пусть A целозамкнута, $x \in L$. Тогда x цел над A тогда и только тогда, когда $m^x_K(t) \in A[t]$.

Доказательство. Если $m^x_K(t) \in A[t]$, то x цел над A по определению. Обратное следует из предложения 5, так как коэффициенты $\mathrm{char}^x_{L/K}(t)$ и $m^x_K(t)$ лежат в K. □

Следствие 5. Пусть a — алгебраическое целое. Если $a \in \mathbb{Q}$, то $a \in \mathbb{Z}$.

Доказательство. Для $A = \mathbb{Z}$ и $L = \mathbb{Q}[a]$ применяем следствие 4: $m^a_{\mathbb{Q}}(t) = t - a$. Значит, $a \in \mathbb{Z}$. □

Предложение 6. В обозначениях предложения 5 существует базис L над K, состоящий из элементов из B. Более того, $L = Q(B)$.

Доказательство. Пусть $x \in L$, поскольку x алгебраичен над K, он является корнем многочлена

$$a_m t^m + \ldots + a_1 t + a_0 = 0, \quad a_m \neq 0,\ a_i \in A.$$

Тогда элемент $y = a_m x$ цел над A. Отсюда $L \subset Q(B)$, и, поскольку $Q(B)$ — наименьшее поле, содержащее B, получаем равенство $L = Q(B)$.

Пусть $x_1, \ldots, x_n$ — какой-то базис L над K. Найдём такие $a_i \in A$, что $y_i = a_i x_i \in B$. Тогда $y_1, \ldots, y_n$ — искомый базис. □

1.5 Дискриминант

Заметим, что норма и след элемента корректно определены, когда мы вместо расширений полей $F \subseteq E$ изучаем расширения колец $R \subseteq S$, но при этом S является свободным конечным R-модулем.

Определение 8. Пусть R и S — кольца, причём $R \subseteq S$ и S есть свободный R-модуль ранга n. Для $x_1, \ldots, x_n \in S$ определим дискриминант как $D(x_1, \ldots, x_n) = \det(T_{S/R}(x_i x_j))$.

Пусть $\vec{y} = C\vec{x}$, где $C \in M_n(R)$, $\det C \neq 0$. Тогда по свойству билинейной формы имеем $T_{S/R}(y_r y_s)_{r,s} = C^T T_{L/K}(x_i x_j)_{i,j} C$. Поэтому

$$D(\vec{y}) = \det{}^2(C) D(\vec{x}). \tag{1.5}$$

Определение 9. Пусть R и S — кольца, причём $R \subseteq S$ и S есть свободный R-модуль ранга n. Зададим дискриминантный идеал $\mathrm{disc}(S/R)$ в R как $(D(x_1, \ldots, x_n))$, где $x_1, \ldots, x_n$ — некоторый базис S над R.

Определение 9 корректно, поскольку для любого другого базиса $y_1, \ldots, y_n$ для S над R выполняется (1.5), а $\det C$ — обратимый элемент из R в силу равенства $\det(C)\det(C^{-1}) = 1$. Ниже мы покажем, что в случае, когда $A = \mathbb{Z}$, идеал $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})$ можно отождествить с целым числом — порождающим этого идеала.

Пусть A — область целостности, $K = Q(A)$, L — конечное сепарабельное расширение K степени n, $B = \bar{A}^L$. Для $x_1, \ldots, x_n \in L$ согласно определению $D(x_1, \ldots, x_n) \in K$. Если все $x_i \in B$, то $D(x_1, \ldots, x_n) \in B$ по предложению 5.

Лемма 8. Пусть L — конечное сепарабельное расширение K степени n, $\sigma_1, \ldots, \sigma_n$ — различные K-вложения поля L в $\bar{K}$. Тогда для любых $x_1, \ldots, x_n \in L$ выполнено $D(x_1, \ldots, x_n) = \det^2(\sigma_i(x_j))_{i,j=1}^n$.

Доказательство. По предложению 4 имеем

$$T_{L/K}(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j).$$

Обозначим $C = (\sigma_k(x_i))_{k,i} \in M_n(K)$, тогда $(T_{L/K}(x_i x_j))_{i,j} = C^T C$. Отсюда $D(\vec{x}) = \det^2(C)$. □

Пусть $f(t) \in K[t]$ — унитарный многочлен, через $\mathrm{Dis}(f)$ обозначим дискриминант многочлена $f(t)$, то есть элемент $\prod\limits_{i<j}(x_i - x_j)^2$, где $x_1, \ldots, x_n$ — корни $f(t)$ в $\overline{K}$.

Предложение 7. Пусть $L = K(x)$ — сепарабельное расширение K степени n, $x_1, \ldots, x_n$ — корни $m_K^x(t)$ в $\overline{K}$. Тогда

$$D(1, x, \ldots, x^{n-1}) = \prod_{i<j}(x_i - x_j)^2 = \mathrm{Dis}\big(m_K^x(t)\big).$$

Доказательство. Пусть $\sigma_1, \ldots, \sigma_n$ — различные K-вложения поля L в $\bar{K}$, то есть $\sigma_i(x) = x_i$, $i = 1, \ldots, n$. Тогда $\sigma_i(x^j) = x_i^j$ для любой степени $j \in \mathbb{N}$. По лемме 8 имеем $D(1, x, \ldots, x^{n-1}) = \det^2(A)$, где

$$A = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Утверждение следует из равенства $\det(A) = \prod\limits_{i<j}(x_i - x_j)$, выполненного для определителя Вандермонда. □

Следствие 6. В обозначениях предложения 7 выполняется $D(1, x, \ldots, x^{n-1}) = (-1)^{n(n-1)/2} N_{L/K}\big(\big(m_K^x\big)'(x)\big)$.

Доказательство. По предложению 7 имеем

$$D(1, x, \ldots, x^{n-1}) = \prod_{i<j}(x_i - x_j)^2 = (-1)^{n(n-1)/2} \prod_{i \neq j}(x_i - x_j) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} \prod_{j \neq i}(x_i - x_j).$$

Поскольку $\big(m_K^x\big)'(x_i) = \prod\limits_{j \neq i}(x_i - x_j)$, получаем

$$D(1, x, \ldots, x^{n-1}) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} \big(m_K^x\big)'(x_i) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} \big(m_K^x\big)'(\sigma_i(x)),$$

где σ_i есть K-вложение поля L в $\overline{K}$ такое, что $\sigma_i(x) = x_i$, $i = 1, \ldots, n$. Так как $\sigma_i\big(\big(m_K^x\big)'(x)\big) = \big(m_K^x\big)'(x_i)$, наконец, выводим по предложению 4:

$$D(1, x, \ldots, x^{n-1}) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} \sigma_i\big(\big(m_K^x\big)'(x)\big) = (-1)^{n(n-1)/2} N_{L/K}\big(\big(m_K^x\big)'(x)\big). \quad \square$$

Теорема 4. Пусть A — целозамкнутая область целостности, $K = Q(A)$, L — сепарабельное расширение K степени n, $B = \bar{A}^L$. Если A нётерова, тогда B — конечнопорождённый A-модуль и B — нётерово кольцо. Если A — область главных идеалов, то B — свободный A-модуль ранга n.

Доказательство. По предложению 6 найдётся базис $x_1, \ldots, x_n$ пространства L над K, состоящий из элементов из B. Пусть $y_1, \ldots, y_n$ — дуальный к нему базис L относительно формы $(\cdot, \cdot)$, то есть $(x_i, y_j) = \delta_{ij}$. Определим $N = Ax_1 + \ldots + Ax_n$ и $M = Ay_1 + \ldots + Ay_n$. Включение $N \subseteq B$ следует из того, что B есть подкольцо в L.

Покажем, что $B \subseteq M$. Пусть $z \in B$ и $z = \sum\limits_{j=1}^{n} a_j y_j$, где $a_j \in K$. По следствию 4 и лемме 6 имеем $T_{L/K}(x_i z) \in A$ для всех $i = 1, \ldots, n$, поскольку $x_i z \in B$. При этом

$$T_{L/K}(x_i z) = (x_i, z) = \left(x_i, \sum_{j=1}^{n} a_j y_j\right) = a_i.$$

Следовательно, $a_i \in A$, $i = 1, \ldots, n$, и $B \subset M$.

Пусть A нётерова, тогда любой подмодуль конечнопорождённого A-модуля M конечно порождён. Значит, B — конечно порождён как A-модуль. Пусть I — идеал в B, тогда I есть A-подмодуль и $I \subseteq B \subseteq M$. Поэтому I конечно порождён как A-модуль и тем самым конечно порождён как B-модуль. Отсюда B — нётерово кольцо.

Пусть A — область главных идеалов. Поскольку N и M — свободные A-модули ранга n, то по структурной теореме для конечнопорождённых модулей над областями главных идеалов B является также свободным модулем ранга n. $\square$

Следствие 7. Кольцо целых алгебраических чисел $\mathcal{O}_L$ является целозамкнутой нётеровой областью целостности, которая есть свободный $\mathbb{Z}$-модуль ранга $[L : \mathbb{Q}]$.

Доказательство. Утверждение следует из теоремы 4 и следствия 1, поскольку $\mathbb{Z}$ — нётерова область главных идеалов. $\square$

Определение 10. Пусть L — алгебраическое числовое поле, любой базис $\mathcal{O}_L$ как свободного $\mathbb{Z}$-модуля называется целым базисом L (или $\mathcal{O}_L$).

Целые базисы для алгебраических числовых полей существуют по следствию 7.

Следствие 8. Пусть L — алгебраическое числовое поле, значение дискриминанта совпадает на всех целых базисах L.

Доказательство. Пусть $\vec{x}, \vec{y}$ — два целых базиса L, тогда по (1.5) выполнено $D(\vec{y}) = \det^2(C) D(\vec{x})$. При этом $\det C = \pm 1$. Значит, $D(\vec{y}) = D(\vec{x})$. $\square$

Предложение 8. Пусть A — целозамкнутая область целостности, $K = Q(A)$, L — конечное сепарабельное расширение K, $B = \bar{A}^L$. Пусть $x_1, \ldots, x_n$ — базис L над K, состоящий из элементов из B. Обозначим $d = D(x_1, \ldots, x_n)$. Тогда выполнено $dB \subseteq Ax_1 + \ldots + Ax_n$.

Доказательство. Распишем элемент $z \in B$ по базису: $z = \sum\limits_{i=1}^{n} a_i x_i$, где $a_i \in K$. Тогда

$$(x_i, z) = T_{L/K}(x_i z) = \sum_{j=1}^{n} T_{L/K}(x_i x_j) a_j, \quad i = 1, \ldots, n.$$

Полученные равенства интепретируем как систему линейных уравнений относительно неизвестных a_j. Причём коэффициенты системы лежат по предложению 5 в A. Определитель матрицы системы по определению равен d, поэтому по правилу Крамеру получаем $a_j = \widetilde{a}_j / d$ для некоторых $\widetilde{a}_j \in A$. Отсюда $dz \in Ax_1 + \ldots + Ax_n$. $\square$

Глава 2

Дедекиндовы кольца

Замечательные свойства колец целых алгебраических чисел, установленные нами в следствии 7 главы I, естественным образом приводят нас к понятию дедекиндова кольца. Для таких колец мы докажем аналог основной теоремы арифметики, но только на уровне идеалов: любой идеал разлагается в произведение степеней простых идеалов. Этот результат будет обобщён следующим образом: любой дробный идеал разлагается в произведение целых степеней простых идеалов.

2.1 Определение и примеры

Определение 1. Область целостности A называется дедекиндовым кольцом, если A нётерова, целозамкнута и любой ненулевой простой идеал в A максимален.

Предложение 1. Область главных идеалов является дедекиндовым кольцом.

Доказательство. Пусть A — область главных идеалов. Ясно, что A нётерова, поскольку каждый идеал в A главный, то есть однопорождённый.

По предложению 2 гл. I любая факториальная область целостности целозамкнута, а произвольная область главных идеалов факториальна[1].

Наконец, ненулевой простой идеал I в A имеет вид (p), где p — неприводимый (простой) элемент, поэтому I максимален. □

Теорема 1. Пусть A — дедекиндово кольцо, $K = Q(A)$, L — конечное сепарабельное расширение K, $B = \bar{A}^L$. Тогда B — дедекиндово кольцо.

Доказательство. По теореме 4 гл. I заключаем, что B — нётерово кольцо. По следствию 1 гл. I знаем, что B также целозамкнута.

Пусть q — ненулевой простой идеал в B. Рассмотрим ненулевой элемент $z \in q$. Поскольку z алгебраичен над A, найдётся такой унитарный многочлен $h(t) \in A[t]$ минимальной степени, что $h(z) = 0$. Пусть $h(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$. Тогда $a_0 \neq 0$ и при этом $a_0 \in zB \cap A \subset q \cap A$. Значит, $q \cap A$ — ненулевой простой идеал в A. По условию $p := q \cap A$ максимален в A, и поэтому A/p — поле.

По теореме о гомоморфизмах выполнено $A/p = A/(A \cap q) \cong (A + q)/q$. Поэтому A/p можно рассматривать как подкольцо в B/q, которое является областью целостности, ведь q — простой идеал в B. Так как B цело над A, то и B/q цело над A/p. Следующая лемма влечёт, что B/q — поле, и поэтому q максимален в B. □

[1] ван дер Варден, Алгебра, стр. 79.

Лемма 1. Пусть область целостности B содержит поле F и цела над F. Тогда B — поле.

Доказательство. Пусть $(0 \neq) z \in B$. Элемент z алгебраичен над F, поэтому $F[z]$ конечномерно над F (предложение 1 гл. I). При этом линейное отображение $\varphi\colon F[z] \to F[z]$, заданное по правилу $\varphi(x) = zx$, является инъективным, так как B — область целостности. Значит, φ сюръективно и найдётся $y \in F[z]$ такой, что $zy = 1$. Таким образом, B — поле. □

Следствие 1. Пусть L — алгебраическое числовое поле, тогда $\mathcal{O}_L$ — дедекиндово кольцо.

Доказательство. Это следует из предложения 1 и теоремы 1. □

Предложение 2. Пусть R — дедекиндово кольцо, S — мультипликативное множество в R. Тогда R_S — дедекиндово кольцо.

Доказательство. По теореме 2 гл. I простому идеалу p в R, не пересекающемуся с S, соответствует простой идеал pR_S в R_S. Поскольку для ненулевых простых идеалов в R нет отношения включения, то его и нет для простых идеалов в R_S, то есть любой простой идеал в R_S максимален.

Пусть q — идеал в R_S, при доказательстве теоремы 2 гл. I мы вывели, что $q = (q \cap R)R_S$. Поскольку $q \cap R$ конечнопорождён в R, то q конечнопорождён в R_S.

По лемме 4 гл. I область целостности R_S целозамкнута. □

Докажем аналог китайской теоремы об остатках для идеалов, определив для этого взаимную простоту идеалов. Два натуральных числа n и m называются взаимно простыми, если $(n, m) = 1$. По линейному разложению наибольшего общего делителя это эквивалентно равенству $(n) + (m) = \mathbb{Z}$. По аналогии будем говорить, что идеалы I и J кольца B взаимно просты, если $I + J = B$.

Теорема 2 (китайская теорема об остатках). Пусть $J_1, \ldots, J_n$ — попарно взаимно простые идеалы в кольце B. Обозначим $I = \bigcap\limits_{i=1}^{n} J_i$. Тогда $B/I \cong B/J_1 \oplus \ldots \oplus B/J_n$ и $I = J_1 \ldots J_n$.

Доказательство. Покажем утверждение индукцией по n. При $n = 1$ всё тривиально выполняется. Пусть $n \geq 2$, зададим гомоморфизм $\varphi\colon B \to B/J_1 \oplus \ldots \oplus B/J_n$, действующий по формуле $\varphi(b) = (b+J_1, \ldots, b+J_n)$. Ясно, что выполнено $J_1 \ldots J_n \subseteq I$ и $\ker(\varphi) = I$.

Рассмотрим случай $n = 2$. Поскольку $J_1 + J_2 = B$, имеем $1 = q_1 + q_2$ для некоторых $q_i \in J_i$, $i = 1, 2$. Тогда $\varphi(q_1) = (q_1 + J_1, q_1 + J_2) = (\bar{0}, \overline{1 - q_2}) = (\bar{0}, \bar{1})$. Аналогично $\varphi(q_2) = (\bar{1}, \bar{0})$. Отсюда φ сюръективно. Значит, по теореме о гомоморфизмах выполнено $B/(J_1 \cap J_2) \cong B/J_1 \oplus B/J_2$. Пусть $c \in J_1 \cap J_2$, тогда $c = c1 = q_1 c + c q_2 \in J_1 J_2$, тем самым $J_1 \cap J_2 = J_1 J_2$.

Пусть $n > 2$. Для каждого $i \geq 2$ найдутся $a_i \in J_1$ и $b_i \in J_i$ такие, что $a_i + b_i = 1$. Тогда $1 = \prod\limits_{i=1}^{n}(a_i + b_i) \in J_1 + J_2 \ldots J_n$. Отсюда $J_1 + J_2 \ldots J_n = B$, то есть идеалы J_1 и $J_2 \ldots J_n$ взаимно просты. Применяем индукционное предположение и случай $n = 2$:

$$B/(J_1 \ldots J_n) = B/J_1(J_2 \ldots J_n) \cong B/J_1 \oplus B/(J_2 \ldots J_n) \cong B/J_1 \oplus B/J_2 \oplus \ldots \oplus B/J_n.$$

Также по индукции выводим равенства $J_1 \ldots J_n = J_1(J_2 \ldots J_n) = J_1 \cap (J_2 \ldots J_n) = J_1 \cap J_2 \cap \ldots \cap J_n$. □

2.2 Разложения идеалов

Лемма 2. Пусть A — нётерово кольцо. Тогда каждый ненулевой собственный идеал в A содержит некоторое произведение ненулевых простых идеалов A.

Доказательство. Пусть, от противного, J — максимальный идеал в A, не содержащий произведений ненулевых простых идеалов A; такой идеал найдётся в силу нётеровости A. Тогда J сам по себе не является простым идеалом. Значит, найдутся элементы $a_1, a_2 \in A \setminus J$ такие, что $a_1 a_2 \in J$. Определим идеалы $I_k = J + Aa_k$, $k = 1, 2$. Поскольку $J \subsetneq I_1$ и $J \subsetneq I_2$, идеалы I_1 и I_2 содержат произведения ненулевых простых идеалов. При этом $I_1 \cdot I_2 \subseteq J$, противоречие. □

Лемма 3. Пусть I и J — взаимно простые идеалы кольца A. Тогда I^k и J^l взаимно просты для любых $k, l \geq 1$.

Доказательство. Пусть $a \in I$ и $b \in J$ такие, что $a + b = 1$. Для $r = k + l - 1$ получаем

$$1 = (a+b)^r = \left(a^r + C_r^1 a^{r-1} b + \ldots + C_r^k a^k b^{r-k}\right) + \left(C_r^{k-1} a^{k-1} b^l + \ldots + b^r\right) \in I^k + J^l.$$

Следовательно, $I^k + J^l = A$. □

Лемма 4. Пусть p — максимальный идеал области целостности R и $q = pR_p$. Тогда $R/p^m \cong R_p/p^m R_p \cong R_p/q^m$ для любого $m \in \mathbb{N}_{>0}$.

Доказательство. Имеем $q^m = p^m R_p$ в силу следующих равенств: $q^m = (pR_p)^m = p^m R_p^m = p^m R_p$. Зададим отображение $\varphi\colon R/p^m \to R_p/p^m R_p$ как $\varphi(r + p^m) = r + p^m R_p$. Покажем сюръективность φ. Пусть $r/s \in R_p$, где $r \in R$ и $s \in S$. В силу максимальности идеала p выполнено $Rs + p = R$, значит, по лемме 3 верно $Rs + p^m = R$. Найдём $c \in R$ и $t \in p^m$ такие, что $cs + t = 1$. Отсюда находим $c = (1-t)/s$. Тогда

$$\varphi(rc + p^m) = rc + p^m R_p = r(1-t)/s + p^m R_p = r/s + p^m R_p. \quad \square$$

Предложение 3. Пусть A — нётерова целозамкнутая область целостности с единственным ненулевым простым идеалом p. Тогда A есть область главных идеалов.

Доказательство. Пусть $a \in p$ и $a \neq 0$. Рассмотрим A-модуль $M = A/(a)$ и определим аннулятор элемента $m \in M \setminus \{0\}$ как $\mathrm{Ann}(m) = \{r \in A \mid rm = 0\}$. Ясно, что $\mathrm{Ann}(m)$ является собственным идеалом в A. Так как A нётерова, найдётся $b \in A$ такой, что $q = \mathrm{Ann}(b + (a))$ максимален среди идеалов такого вида. Заметим, что $q \neq (0)$, поскольку $a \in q$. Покажем, что q — простой идеал и поэтому $q = p$. Предположим, что существуют $x, y \notin q$ такие, что $xy \in q$. Значит, $y(b + (a)) \neq \bar{0}$, но при этом $\mathrm{Ann}(yb + (a)) \supseteq q \cup \{x\}$, противоречие с максимальностью q.

Значит, $p = q$, тем самым $pb \subseteq (a)$ и $(b) \not\subseteq (a)$. Последнее влечёт, что элемент $b/a \in Q(A)$ не лежит в A. Покажем, что $a/b \in A$ и $p = (a/b)$. Из включения $pb \subseteq (a)$ выводим, что $pb/a \subseteq A$ и это идеал в A. Если $pb/a \subseteq p$, то по предложению 1 (пп. 1 и 4) гл. I элемент b/a цел над A, так как p — это $A[b/a]$-модуль и конечнопорождённый A-модуль. Область A целозамкнута, значит, $b/a \in A$, противоречие. Поскольку любой максимальный идеал в A является простым идеалом, значит, в A есть единственный максимальный идеал, это p. Так как pb/a — ненулевой идеал в A, не содержащийся в p, заключаем, что $pb/a = A$ и $p = A\pi$, где $\pi = a/b \in A$.

Теперь покажем, что любой идеал I в A — главный. Можем считать, что $I \neq (0)$ и $I \neq A$. Включение $\pi I \subseteq I$ перепишем как $I \subseteq \pi^{-1} I$. В цепочке

$$I \subseteq \pi^{-1} I \subseteq \pi^{-2} I \subseteq \dots$$

включений множеств, рассматриваемых как подмножества в $Q(A)$, ни на каком шаге не может быть равенство. Действительно, пусть $\pi^{-k} I = \pi^{-k-1} I$ для некоторого k. Тогда $\pi^{-k} I$ есть конечнопорождённый $A[\pi^{-1}]$-модуль, и опять по предложению 1 гл. I элемент $\pi^{-1} = b/a$ цел над A, противоречие. Заметим, что если $\pi^{-s} I \subseteq A$, то $\pi^{-s} I$ — идеал в A. В силу нётеровости найдётся n такое, что $\pi^{-n} I \subseteq A$ и $\pi^{-n-1} I \subsetneq A$. Предположим, что $\pi^{-n} I \subseteq p$. Из $p = A\pi$ выводим, что $\pi^{-n-1} I \subseteq A$, противоречие. Значит, $\pi^{-n} I = A$ и $I = (\pi^n)$. □

Следствие 2. Пусть A — дедекиндово кольцо и p — ненулевой простой идеал в A. Тогда для любого $m \in \mathbb{N}_{>0}$ произвольный собственный идеал A/p^m является степенью идеала p/p^m.

Доказательство. По лемме 4 можем рассматривать кольцо $A_p/p^m A_p$. По предложению 3 гл. 1 pA_p — единственный максимальный идеал в A_p. При этом A_p — дедекиндово кольцо по предложению 2, следовательно, pA_p — единственный ненулевой простой идеал в A_p. По доказательству предложения 3 любой идеал в A_p имеет вид (π^n) для некоторого $n \in \mathbb{N}$, где $pA_p = (\pi)$. Значит, и при факторизации получаем, что любой идеал $A_p/p^m A_p$ является степенью идеала $pA_p/p^m A_p$. □

Теорема 3. Пусть A — дедекиндово кольцо. Тогда любой собственный ненулевой идеал I в A представим в виде $P_1^{r_1} \dots P_n^{r_n}$, где P_i — попарно различные простые идеалы A, $r_i \in \mathbb{N}_{>0}$, причём идеалы P_i и числа r_i определены однозначно.

Доказательство. По лемме 2 идеал I содержит идеал $J = P_1^{s_1} \dots P_n^{s_n}$ — произведение степеней ненулевых попарно различных простых идеалов. По китайской теореме об остатках имеем

$$A/J \cong A/P_1^{s_1} \oplus \dots \oplus A/P_n^{s_n}.$$

По следствию 2 получаем, что $I/J \cong P_1^{r_1}/P_1^{s_1} \oplus \dots \oplus P_n^{r_n}/P_n^{s_n}$ для некоторых $r_i \leq s_i$. В силу взаимно однозначного соответствия между идеалами A, содержащими J, и идеалами A/J, заключаем, что $I = P_1^{r_1} \dots P_n^{r_n}$.

Идеалы $P_1, \dots, P_n$ определяются однозначно как простые идеалы, содержащие I. Число r_i находится из равенства $IA_{P_i} = P_i^{r_i} A_{P_i}$. □

Следствие 3. Пусть A — дедекиндово кольцо с конечным числом простых идеалов. Тогда A — область главных идеалов.

Доказательство. Пусть $P_1, \dots, P_n$ — все ненулевые простые идеалы A. По теореме 3 достаточно показать, что каждый P_i является главным. Выберем $x_1 \in P_1 \setminus P_1^2$. По китайской теореме об остатках найдётся элемент $x \in A$ такой, что

$$x \equiv x_1 \pmod{P_1^2}, \quad x \equiv 1 \pmod{P_j},\ j = 2, \dots, n.$$

Тогда $(x) \subseteq P_1$, но $(x) \not\subset P_1^2$ и $(x) \not\subset P_j$ при $j = 2, \dots, n$. По теореме 3 находим, что $(x) = P_1$. □

Предложение 4. Пусть A — дедекиндово факториальное кольцо. Тогда A — область главных идеалов.

Доказательство. Пусть P — ненулевой простой идеал A и пусть $(0 \neq)a \in P$. По упр. 2б) семинара №1 элемент a представим в виде произведения неприводимых элементов. Так как идеал P прост, то P содержит один из неприводимых множителей a, обозначим такой множитель как b. В факториальном кольце понятия неприводимого и простого элементов совпадают, поэтому (b) — простой идеал A. Тогда $0 \subsetneq (b) \subseteq P$ — цепочка простых идеалов, и, значит, $(b) = P$. □

2.3 Дробные идеалы

Определение 2. Пусть A — дедекиндово кольцо, $K = Q(A)$. Ненулевой A-подмодуль I в K такой, что $dI \subseteq A$ для некоторого $(0 \neq)d \in A$, называется дробным идеалом A. Элемент d называют знаменателем дробного идеала I.

Обычные идеалы дедекиндова кольца являются дробными идеалами (достаточно взять $d = 1$), их будем называть целыми идеалами A.

Дробный идеал I в A конечнопорождён, поскольку dI — идеал нётерова кольца A. Сумма, пересечение и произведение дробных идеалов являются дробными идеалами.

Определение 3. Пусть I — дробный идеал дедекиндова кольца A. Тогда множество $I^{-1} = \{x \in K \mid xI \subseteq A\}$ называется обратным к I.

Лемма 5. Пусть I — дробный идеал дедекиндова кольца A. Тогда I^{-1} — также дробный идеал A и $I \cdot I^{-1} = A$.

Доказательство. Ясно, что I^{-1} есть A-модуль. Возьмём ненулевой элемент $a \in I \cap A$, тогда $aI^{-1} \subseteq A$ по определению I^{-1}. Тем самым I^{-1} — дробный идеал A.

Заметим, что $I \cdot I^{-1} \lhd A$. Если $I \cdot I^{-1} \neq A$, тогда $I \cdot I^{-1} \subseteq P$ для некоторого простого идеала P. Переходя к локализации A_P, получаем включение $J \cdot J' \subseteq Q$, где $J = IA_P$, $J' = I^{-1}A_P$ и $Q = PA_P$.

Несложно показать равенство $J' = \{x \in K \mid xJ \subseteq A_P\}$. По предложению 3 $Q = (\pi)$ для некоторого элемента $\pi \in A_P$. Найдётся такое $k \in \mathbb{N}$, что π^k — знаменатель дробного идеала J'. Тогда $J = (\pi^m)$ для некоторого $m \in \mathbb{Z}$. Отсюда $J' = (\pi^{-m})$. Следовательно, $J \cdot J' = A_P$, противоречие. □

Теорема 4. Пусть A — дедекиндово кольцо. Множество $\mathrm{Id}(A)$ дробных идеалов относительно произведения $I \cdot J$ является свободной абелевой группой с множеством всех ненулевых простых идеалов в качестве порождающих.

Доказательство. Умножение в $\mathrm{Id}(A)$ коммутативно и ассоциативно, A выполняет роль единицы, так как $A \cdot I = I$ для любого дробного идеала I. По лемме 5 есть обратимость.

Покажем, что любой дробный идеал единственным образом представляется как произведение целых степеней простых идеалов. Пусть $I \in \mathrm{Id}(A)$, тогда для его знаменателя d по теореме 3 выписываем разложение на простые идеалы (для записи по одному и тому же набору простых идеалов допускаем нулевые степени):

$$dI = P_1^{r_1} \dots P_n^{r_n}, \quad (d) = P_1^{s_1} \dots P_n^{s_n}.$$

Тогда $I = P_1^{r_1 - s_1} \dots P_n^{r_n - s_n}$, единственность разложения следует из единственности разложения целых идеалов A. □

Группа $\mathrm{Id}(A)$ называется группой идеалов кольца A.

Любой ненулевой элемент $x \in K$ задаёт дробный идеал $(x) = xA$, называемый главным дробным идеалом. Заметим, что $(x) \cdot (x^{-1}) = A$, поэтому множество $P(A)$ всех главных дробных идеалов A образует подгруппу в $\mathrm{Id}(A)$.

Определение 4. Фактор-группа $\mathrm{Cl}(A) = \mathrm{Id}(A)/P(A)$ называется группой классов кольца A.

Определение 5. Пусть K — алгебраическое числовое поле, тогда $h_K = |\mathrm{Cl}(\mathcal{O}_K)|$ называется числом классов поля K.

Предложение 5. Пусть A — дедекиндово кольцо. Тогда следующие условия эквивалентны:

(1) $\mathrm{Cl}(A) = \{e\}$,

(2) A — область главных идеалов,

(3) A факториально.

Доказательство. Вывод (2) $\Rightarrow$ (3) известен из общего курса алгебры.

Доказательство (3) $\Rightarrow$ (2) следует из предложения 4.

(1) $\Rightarrow$ (2). Поскольку группа $\mathrm{Cl}(A)$ тривиальна, любой ненулевой целый идеал I в A является главным дробным идеалом, то есть $I = Ax$ для некоторого $x \in K^*$. Тогда $1 \cdot x = x \in A$ и $I = (x)$ — главный идеал.

(2) $\Rightarrow$ (1). Пусть J — дробный идеал A, тогда $dJ \lhd A$, где d — знаменатель J. Значит, $dJ = Aa$ для некоторого $a \in A$. Отсюда $J = A(a/d)$ — главный дробный идеал. Следовательно, $\mathrm{Cl}(A) = \{e\}$. □

Следствие 4. Пусть K — алгебраическое числовое поле, тогда

$$h_K = 1 \iff \mathcal{O}_K \text{ — область главных идеалов} \iff \mathcal{O}_K \text{ факториально.}$$

Тем самым вопрос о том, когда кольцо $\mathcal{O}_K$ факториально, мы свели к подсчёту числа h_K и проверке того, выполнено ли $h_K = 1$. В главе III мы докажем, что $h_K < \infty$ для произвольного алгебраического числового поля K.

2.4 Разложения простых идеалов в расширениях

Пусть A — дедекиндово кольцо, $K = Q(A)$, L — конечное сепарабельное расширение K, $B = \bar{A}^L$. Пусть P — ненулевой простой идеал в A. Поскольку B — дедекиндово кольцо (теорема 1), разлагаем PB по простым идеалам в B:

$$PB = P_1^{e_1} \dots P_g^{e_g}, \quad e_i \geq 1. \tag{2.1}$$

Число $e_i(P_i/P)$ называется индексом ветвления P_i над P. Если $e_i > 1$, то говорят, что простой идеал P разветвляется в B (или в L).

Лемма 6. Пусть Q — ненулевой простой идеал в B. Тогда Q встречается в разложении PB на простые идеалы тогда и только тогда, когда $Q \cap A = P$.

Доказательство. Пусть $Q \cap A = P$, тогда $P \subseteq Q$ и поэтому $PB \subseteq Q$. Следовательно, Q встречается в разложении PB на простые идеалы.

Пусть Q встречается в разложении PB, то есть $PB \subseteq Q$. Значит, $P \subseteq PB \cap A \subseteq Q \cap A$. Ненулевой идеал $Q \cap A$ в A является простым. Тем самым $P = Q \cap A$. □

Пусть P_i — простой идеал B из разложения (2.1). В доказательстве теоремы 1 мы фактически показали, что A/P является подполем в B/P_i. По теореме 4 гл. I знаем,

что B — конечнопорождённый A-модуль. Значит, B/P_i — конечномерное векторное пространство над A/P.

Определение 6. Относительной степенью (индексом инерции) P_i над P называется число $f_i = f_i(P_i/P) = [B/P_i : A/P]$.

Простой идеал P разлагается в L, если $e_i = f_i = 1$ для всех $i = 1, \ldots, g$. Если PB — простой идеал в B, то говорят, что P инертен в L.

Теорема 5. Пусть A — дедекиндово кольцо, L — конечное сепарабельное расширение $K = Q(A)$ степени m, $B = \bar{A}^L$. Пусть P — ненулевой простой идеал в A, $P_1, \ldots, P_g$ — простые идеалы B, делящие PB. Тогда для $e_i = e_i(P_i/P)$ и $f_i = f_i(P_i/P)$ выполнено *фундаментальное тождество*

$$\sum_{i=1}^{g} e_i f_i = m. \tag{2.2}$$

Если L/K — расширение Галуа, тогда $e_1 = \ldots = e_g$, $f_1 = \ldots = f_g$ и $efg = m$.

Доказательство. По китайской теореме об остатках имеем

$$B/PB = B/P_1^{e_1} \ldots P_g^{e_g} \cong B/P_1^{e_1} \oplus \ldots \oplus B/P_g^{e_g}.$$

Покажем, что $\sum\limits_{i=1}^{g} e_i f_i = \dim_{A/P}(B/PB)$, для этого достаточно установить, что $\dim_{A/P}\left(B/P_i^{e_i}\right) = e_i f_i$. Отметим изоморфизм конечномерных над полем A/P векторных пространств $B/P_i^{e_i} \cong \bigoplus\limits_{j=0}^{e_i-1} P_i^j/P_i^{j+1}$. Далее, P_i^j/P_i^{j+1} является B-модулем, не содержащим собственных B-подмодулей, иначе в B нашёлся бы идеал I, удовлетворяющий свойствам $P_i^j \subsetneq I \subsetneq P_i^{j+1}$. Аннулятором действия B на P_i^j/P_i^{j+1} является P_i, поэтому $\dim_{B/P_i}\left(P_i^j/P_i^{j+1}\right) = 1$. Значит, $\dim_{A/P}\left(P_i^j/P_i^{j+1}\right) = \dim_{A/P}(B/P_i) = f_i$. В итоге $\dim_{A/P}\left(B/P_i^{e_i}\right) = e_i f_i$.

Далее докажем, что $\dim_{A/P}(B/PB) = m$. Сперва установим это равенство в случае, когда B есть свободный A-модуль ранга m. Пусть $x_1, \ldots, x_m$ — базис B над A, покажем, что $x_i + PB$ образуют базис B/PB над A/P. Предположим, что $\sum\limits_{i=1}^{m}(a_i + P)(x_i + PB) = 0$ в B/PB для некоторых $a_i \in A$. Тогда $v = \sum\limits_{i=1}^{m} a_i x_i \in PB$, то есть $v = \sum\limits_{j} b_j y_j$, где $b_j \in B$ и $y_j \in P$. При этом $b_j = \sum\limits_{k=1}^{m} c_{kj} x_k$ для некоторых $c_{kj} \in A$. Следовательно, $a_k = \sum\limits_{j} c_{kj} y_j \in P$ для всех k. Отсюда следует, что $\bar{x}_1, \ldots, \bar{x}_m$ есть базис B/PB над A/P.

В общем случае введём $S = A \setminus P$, тогда $B_S = \bar{A}_S^L$ по упр. 4 семинара №5. Локализуем относительно S равенство (2.1), то есть вложим его в B_S и домножим на кольцо B_S. По теореме 2 гл. I простые идеалы в B, не пересекающиеся с S, находятся во взаимно однозначном соответствии с простыми идеалами кольца B_S, поэтому получаем разложение

$$PB_S = (P_1 B_S)^{e_1} \ldots (P_g B_S)^{e_g},$$

где P_iB_S — простой идеал в B_S. Уточним, что применение теоремы 2 гл. I корректно, поскольку по лемме 6 $P_i \cap A = P$, тем самым $P_i \cap S = \emptyset$.

По предложению 3 кольцо A_S — область главных идеалов, значит, по теореме 4 гл. I мы можем применить уже доказанную формулу:

$$\sum_{i=1}^{g} e_i f_i' = \dim_{A_S/PA_S}(B_S/PB_S) = m,$$

где $f_i' = \dim_{A_S/PA_S}(B_S/P_iB_S)$ Изоморфизмы $A/P \cong A_S/PA_S$, $B/PB \cong B_S/PB_S$ и равенство чисел $f_i' = f_i$ верны по лемме 4.

Докажем вторую часть теоремы. Пусть L/K — расширение Галуа. Для произвольного $\sigma \in \mathrm{Gal}(L/K)$ выполнено $\sigma(B) = B$. Действительно, пусть $x \in B$ и $h(t) \in A[t]$ — уравнение целой зависимости для x. Поскольку $\sigma(h(t)) = h(t)$, получаем, что $\sigma(x) \in B$. Аналогично $\sigma^{-1}(x) \in B$ для любого $x \in B$. Значит, $\sigma(B) = B$. Действуя σ на разложение (2.1), получаем $PB = \sigma(P_1)^{e_1} \dots \sigma(P_g)^{e_g}$. Поскольку автоморфизм сохраняет все алгебраические свойства колец, $\sigma(P_i)$ — простой идеал в B для любого $i = 1, \dots, g$. Также $e(\sigma(P_i)/P) = e(P_i/P)$ и $f(\sigma(P_i)/P) = f(P_i/P)$. Остаётся показать, что группа $\mathrm{Gal}(L/K)$ действует транзитивно на множестве идеалов $P_1, \dots, P_g$.

Пусть Q_1 и Q_2 — простые идеалы B, делящие PB и $\sigma(Q_1) \neq Q_2$ ни для какого $\sigma \in \mathrm{Gal}(L/K)$. По китайской теореме об остатках найдём $x \in Q_2$ и $x \notin \sigma(Q_1)$, $\sigma \in \mathrm{Gal}(L/K)$. По предложению 5 гл. I $N_{L/K}(x) \in A$, поскольку A целозамкнута. При этом по предложению 4 гл. I $N_{L/K}(x) = \prod\limits_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in Q_2$. Применяя лемму 6, получаем $N_{L/K}(x) \in A \cap Q_2 = P$. Опять же по лемме 6 выполнено $N_{L/K}(x) \in Q_1$. В силу простоты идеала Q_1 найдётся $\sigma \in \mathrm{Gal}(L/K)$ такой, что $\sigma(x) \in Q_1$, противоречие. □

Установим в терминах дискриминанта критерий разветвляемости простого идеала в расширении.

Предложение 6. Пусть K — алгебраическое числовое поле, p — простое число. Идеал $P = (p)$ разветвляется в K тогда и только тогда, когда $p \,|\, \mathrm{disc}(\mathcal{O}_K/\mathbb{Z})$.

Доказательство. Пусть $p\mathcal{O}_K = P_1^{e_1} \dots P_g^{e_g}$, где $P_1, \dots, P_g$ — попарно различные простые идеалы в $\mathcal{O}_K$. По китайской теореме об остатках $\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/P_1^{e_1} \oplus \dots \oplus \mathcal{O}_K/P_g^{e_g}$. Идеал P не разветвляется в K, если $e_1 = \dots = e_g = 1$, то есть если и только если $\mathcal{O}_K/p\mathcal{O}_K$ — сумма полей. Выберем базис $x_1, \dots, x_m$ кольца $\mathcal{O}_K$ над $\mathbb{Z}$. Так как $\mathcal{O}_K$ — свободный $\mathbb{Z}$-модуль, поэтому $\bar{x}_1, \dots, \bar{x}_m$ есть базис свободного $\mathbb{Z}/P$-модуля $\mathcal{O}_K/P\mathcal{O}_K$, доказательство аналогично выводу в теореме 5. Более того, $D(\bar{x}_1, \dots, \bar{x}_m) \equiv D(x_1, \dots, x_m) \pmod{P}$. Условие $p \,|\, \mathrm{disc}(\mathcal{O}_K/\mathbb{Z})$ эквивалентно тому, что

$$\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) \pmod{P} = \mathrm{disc}((\mathcal{O}_K/p\mathcal{O}_K)/(\mathbb{Z}/P)) = 0.$$

Покажем, что $\mathcal{O}_K/P\mathcal{O}_K$ есть сумма полей тогда и только тогда, когда $\mathrm{disc}((\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{Z}_p) \neq 0$.

Пусть $\mathcal{O}_K/p\mathcal{O}_K = F_1 \oplus \dots \oplus F_g$ — сумма полей, то есть F_i — конечное расширение $\mathbb{Z}_p$ и поэтому сепарабельно. Имеем

$$\mathrm{disc}((\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{Z}_p) = \prod_{i=1}^{g} \mathrm{disc}(F_i/\mathbb{Z}_p) \neq 0.$$

Равенство следует из того, что соответствующая матрица $T_{B/A}(x_ix_j)$ для базиса $\mathcal{O}_K/p\mathcal{O}_K$ над $\mathbb{Z}_p$, составленного из базисов $F_1,\dots,F_g$, является блочно-диагональной. Неравенство $\operatorname{disc}(F_i/\mathbb{Z}_p)\neq 0$ выполняется по теореме 3 гл. I.

Обратно, пусть $\mathcal{O}_K/p\mathcal{O}_K\cong \mathcal{O}_K/P_1^{e_1}\oplus\ldots\oplus\mathcal{O}_K/P_g^{e_g}$ не есть сумма полей. Тогда в $\mathcal{O}_K/p\mathcal{O}_K$ есть нильпотентный элемент $x\neq 0$. Дополним $x_1=x$ до базиса $x_1,\dots,x_t$ кольца $\mathcal{O}_K/p\mathcal{O}_K$ над $\mathbb{Z}_p$. Поскольку x_1x_i нильпотентен для любого $i=1,\dots,t$, имеем $T_{(\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{Z}_p}(x_1x_i)=0$ и поэтому $\operatorname{disc}((\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{Z}_p)=0$. □

Аналогично предложению 6 доказывается и утверждение в общем случае.

Следствие 5. Пусть A — дедекиндово кольцо, L — конечное сепарабельное расширение $K=Q(A)$, $B=\bar{A}^L$. Предположим, что для любого ненулевого простого идеала P в A поле A/P совершенно[2]. Пусть B есть свободный A-модуль. Тогда простой идеал P в A разветвляется в L тогда и только тогда, когда $P\supseteq\operatorname{disc}(B/A)$. В частности, лишь конечное число простых идеалов A разветвляется в L.

Теорема 6 (Дедекинда — Куммера). Пусть A — дедекиндово кольцо, $K=Q(A)$, L — конечное сепарабельное расширение K степени m, $B=\bar{A}^L$. Предположим, что $B=A[\alpha]$. Пусть P — простой идеал в A, а унитарные многочлены $g_1(t),\dots,g_n(t)\in A[t]$ таковы, что $\overline{m_K^\alpha}(t)=\overline{g_1}(t)^{e_1}\dots\overline{g_n}(t)^{e_n}$ — разложение на неприводимые многочлены в $(A/P)[t]$. Тогда имеем разложение на простые идеалы

$$PB=\prod_{i=1}^{n}(P,g_i(\alpha))^{e_i},\quad f_i=\deg g_i.$$

Доказательство. Зададим гомоморфизм $\varphi\colon A[t]\to B$ по правилу $\varphi(t)=\alpha$. По теореме о гомоморфизмах имеем $A[t]/(m_K^\alpha(t))\cong B$. Также выполнена следующая цепочка изоморфизмов:

$$A[\alpha]/(P,g_i(\alpha))\cong A[t]/(m_K^\alpha(t),P,g_i(t))\cong(A/P)[t]/(\overline{m_K^\alpha}(t),\overline{g_i}(t))\cong(A/P)[t]/(\overline{g_i}(t)).$$

Поскольку $\overline{g_i}(t)$ — неприводимый многочлен над $(A/P)[t]$, заключаем, что факторкольцо $(A/P)[t]/(\overline{g_i}(t))$ есть поле. Таким образом, идеал $Q_i=(P,g_i(\alpha))$ является максимальным и, следовательно, простым идеалом в кольце B. При этом $P\subset Q_i$ и $f_i=f(Q_i/P)=\dim_{A/P}(B/Q_i)=\deg g_i$.

Идеал $I=\prod\limits_{i=1}^{n}(P,g_i(\alpha))^{e_i}$ лежит в PB, так как $\prod\limits_{i=1}^{n}g_i(\alpha)^{e_i}\equiv_{PB} m_K^\alpha(\alpha)\equiv_{PB}0$. Многочлены $\overline{g_i}(t)$ — различные элементы кольца

$$(A/P)[t]/(\overline{m_K^\alpha}(t))\cong A[t]/(P,\overline{m_K^\alpha}(t))\cong A[\alpha]/PA[\alpha],$$

то есть $g_i(\alpha)$ попарно различны по модулю $PA[\alpha]$. Предположим, что $Q_i=Q_j$, тогда $g_i(\alpha)=p+bg_j(\alpha)$ для некоторых $p\in PB$ и $b=b_0+b_1\alpha+\ldots+b_{m-1}\alpha^{m-1}\in A[\alpha]$. Из $\overline{g_i}(t)=(\overline{b_0}+\overline{b_1}t+\ldots+\overline{b_{m-1}}t^{m-1})\overline{g_j}(t)$, унитарности и неприводимости многочленов $\overline{g_i}(t),\overline{g_j}(t)$ заключаем, что $b=b_0\equiv_P 1$, противоречие с тем, что $g_i(\alpha)\not\equiv_{PA[\alpha]}g_j(\alpha)$. Неравенство $e_i\geq e_i':=e(Q_i/P)$ следует из условия $Q_1^{e_1}\dots Q_n^{e_n}\subseteq PB$. По теореме 5 для разложения $PB=Q_1^{e_1'}\dots Q_n^{e_n'}$ выполнено $\sum\limits_{i=1}^{n}e_i'f_i=m=\deg(m_K^\alpha(t))=\sum\limits_{i=1}e_if_i$. Значит, $e_i=e(Q_i/P)$ для всех i и $PB=Q_1^{e_1}\dots Q_n^{e_n}$. □

[2]Поле F называется совершенным, если каждое конечное расширение F сепарабельно.

2.5 Норма идеала

Пусть A — дедекиндово кольцо, L — конечное сепарабельное расширение $K = Q(A)$, $B = \bar{A}^L$. Наша цель: определить гомоморфизм $N\colon \mathrm{Id}(B) \to \mathrm{Id}(A)$ так, чтобы диаграмма

$$\begin{array}{ccc} L^* & \xrightarrow{l\to(l)} & \mathrm{Id}(B) \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N} \\ K^* & \xrightarrow{k\to(k)} & \mathrm{Id}(A) \end{array} \tag{2.3}$$

была коммутативной. Поскольку мы хотим задать гомоморфизм, по теореме 3 достаточно определить N на простых идеалах B.

Пусть P — простой идеал A, $PB = P_1^{e_1} \dots P_g^{e_g}$ — разложение P на простые идеалы в B. Рассмотрим частный случай, когда P — главный идеал, то есть $P = (\pi)$. Тогда, с одной стороны, имеем

$$N(PB) = N(\pi B) = N_{L/K}(\pi)A = (\pi^m) = P^m, \quad m = [L : K].$$

С другой стороны, $N(PB) = N(P_1)^{e_1} \dots N(P_g)^{e_g}$. По теореме 5 выполнено $\sum\limits_{i=1}^{g} e_i f_i = m$, поэтому логично взять $N(P_i) = P^{f_i}$. Наконец, дадим определение нормы идеала.

Определение 7. Нормой (дробного) идеала B называется значение гомоморфизма $N\colon \mathrm{Id}(B) \to \mathrm{Id}(A)$, заданного на ненулевом простом идеале Q в B как $N(Q) = P^{f(Q/P)}$, где $P = Q \cap A$.

Для башни расширений $K \subseteq L \subseteq M$ выполняется $N^{L/K}(N^{M/L}(I)) = N^{M/K}(I)$, где $I \in \mathrm{Id}(C)$, $C = \bar{A}^M$, поскольку для простого идеала S в C, лежащего над простым идеалом Q в B и над простым идеалом P в A, имеем равенство $f(S/Q)f(Q/P) = f(S/P)$ в силу $[C/S\colon B/Q] \cdot [B/Q\colon A/P] = [C/S\colon A/P]$.

Выведем основные свойства нормы идеала.

Предложение 7. Пусть A — дедекиндово кольцо, L — конечное сепарабельное расширение $K = Q(A)$, $B = \bar{A}^L$. Тогда

а) $N(IB) = I^m$, где $m = [L : K]$, для любого ненулевого идеала I в A,

б) в расширении Галуа L/K для ненулевого простого идеала Q в B и для разложения $PB = (P_1 \dots P_g)^e$, где $P = Q \cap A$, выполняется

$$N(Q)B = (P_1 \dots P_g)^{ef} = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(Q),$$

в) $N_{L/K}(\beta)A = N(\beta B)$ для любого $\beta \in L^*$, то есть диаграмма 2.3 коммутативна.

Доказательство. а) Утверждение достаточно доказать для простых идеалов. Пусть $(0 \neq)P$ — простой идеал в A, тогда по определению и теореме 5

$$N(PB) = N(P_1^{e_1} \dots P_g^{e_g}) = P^{\sum\limits_{i=1}^{g} e_i f_i} = P^m.$$

б) По определению $N(Q)B = P^f B = (PB)^f = (P_1 \dots P_g)^{ef}$. При доказательстве теоремы 5 мы установили, что группа $\mathrm{Gal}(L/K)$ действует транзитивно на множестве простых идеалов $\{P_1, \dots, P_g\}$, расширяющих P, и каждый P_i встретится $m/g = ef$ раз.

в) Докажем формулу для случая $\beta \in B$. Сперва изучим случай, когда L/K — расширение Галуа. Поскольку отображение $\varphi\colon \mathrm{Id}(A) \to \mathrm{Id}(B)$, заданное по правилу $\varphi(I) = IB$, инъективно, достаточно доказать равенство $N_{L/K}(\beta)B = N(\beta B)B$. По пункту б), мультипликативности нормы идеала и предложению 4 гл. I выполнено

$$N(\beta B)B = \prod_{\sigma\in \mathrm{Gal}(L/K)} \sigma(\beta B) = \left(\prod_{\sigma\in \mathrm{Gal}(L/K)} \sigma(\beta)\right)B = N_{L/K}(\beta)B.$$

В общем случае рассмотрим E — конечное нормальное расширение поля K, содержащее L, также зададим $d = [E : L]$ и $C = \bar{B}^E$. По а), транзитивности нормы элемента, транзитивности нормы идеала и по уже доказанному случаю расширения Галуа вычисляем

$$N^{L/K}(\beta B)^d = N^{E/K}(\beta C) = N_{E/K}(\beta)A = N_{L/K}(\beta)^d A.$$

Группа $\mathrm{Id}(A)$ не содержит кручения, поэтому $N^{L/K}(\beta B) = N_{L/K}(\beta)A$.

Для произвольного $\beta \in L^*$ запишем $\beta = c/d$, где $c, d \in B$. Тогда верны равенства

$$N((c/d)B) = N(cB) \cdot N((1/d)B) = N_{L/K}(c)A \cdot N_{L/K}(1/d)A = N_{L/K}(c/d)A. \quad \square$$

Определение 8. Пусть K — алгебраическое числовое поле, I — ненулевой идеал $\mathcal{O}_K$. Тогда $\mathbb{N}(I) = |\mathcal{O}_K/I|$ называется считающей нормой идеала I.

Рассмотрим простейший пример, когда $K = \mathbb{Q}$, тогда $I = (a)$ для некоторого $(0 \neq) a \in \mathbb{Z}$. Тем самым $\mathbb{N}(I) = |\mathbb{Z}/(a)| = |a| < \infty$.

Лемма 7. Пусть K — алгебраическое числовое поле, I — ненулевой идеал $\mathcal{O}_K$. Тогда $\mathbb{N}(I) < \infty$ и $N(I) = (\mathbb{N}(I))$.

Доказательство. Пусть $I = P_1^{e_1} \dots P_g^{e_g}$ — разложение на простые идеалы в $\mathcal{O}_K$, а p_i — такое простое число, что $P_i \cap \mathbb{Z} = (p_i)$. Тогда $N(P_i) = (p_i)^{f_i}$, где $f_i = f_i(P_i/(p_i))$. По китайской теореме об остатках (теорема 2) $\mathbb{N}(I) = \prod\limits_{i=1}^{g} |\mathcal{O}_k/P_i^{e_i}|$. В доказательстве теоремы 5 установили, что $\dim_{\mathbb{Z}_{p_i}}(\mathcal{O}_k/P_i^{e_i}) = e_i f_i$, то есть $|\mathcal{O}_k/P_i^{e_i}| = p_i^{e_i f_i}$. Значит, $(\mathbb{N}(I)) = \prod\limits_{i=1}^{g} (p_i^{e_i f_i}) = N(I)$ по определению нормы идеала. $\square$

Замечание. Поясним, почему для любого $M \in \mathbb{N}$ найдётся лишь конечное число идеалов в $\mathcal{O}_K$ таких, что $\mathbb{N}(I) < M$. Действительно, пусть $I = P_1^{e_1} \dots P_g^{e_g}$, тогда $\mathbb{N}(I) = \prod\limits_{i=1}^{g} p_i^{e_i f_i}$, где $P_i \cap \mathbb{Z} = (p_i)$, $p_i > 0$, $f_i = f_i(P_i/(p_i))$. Тогда есть лишь конечное число простых чисел p_i (а значит, и идеалов P_i) и степеней e_i, не нарушающих неравенство $\mathbb{N}(I) < M$.

Глава 3

Конечность группы классов

В данной главе мы установим, что $h_K < \infty$. Применяя известный результат из геометрии (теорема Минковского) и подсчёт одного объёма, мы покажем, что каждый класс в $\mathrm{Cl}(\mathcal{O}_K)$ содержит целый идеал, норма которого ограничена некоторой константой. По замечанию из гл. II мы и выведем, что h_K конечно.

3.1 Теорема Минковского

Определение 1. Подгруппа H в $\mathbb{R}^n$ называется решёткой, если $H{=}\mathbb{Z}e_1{+}\ldots{+}\mathbb{Z}e_k$ для некоторого линейно независимого набора $e_1, \ldots, e_k$ в $\mathbb{R}^n$. Набор $e_1, \ldots, e_k$ назовём базисом решётки. Решётка называется полной, если $k = n$.

Определение 2. Пусть H — полная решётка в $\mathbb{R}^n$, множество

$$T = \left\{ x \in \mathbb{R}^n \mid x = \sum_{i=1}^{n} \alpha_i e_i,\ 0 \le \alpha_i < 1 \right\}$$

называется фундаментальным параллелепипедом в H.

Ясно, что T зависит от выбора базиса H, но его объём $\mathrm{vol}(T)$ не зависит, поскольку матрица перехода C от одного базиса решётки к другому унимодулярна, то есть $\det C = \pm 1$. Будем обозначать $\mathrm{vol}(H) = \mathrm{vol}(T)$.

Заметим, что параллелепипеды, полученные сдвигами какого-то фиксированного фундаментального параллелепипеда на векторы из решётки, полностью покрывают пространство $\mathbb{R}^n$ без пересечений: $\mathbb{R}^n = \dot{\bigcup\limits_{h \in H}} (h + T)$.

Определение 3. Подгруппа H в $\mathbb{R}^n$ называется дискретной, если для любого ограниченного множества Y в $\mathbb{R}^n$ выполнено $|H \cap Y| < \infty$.

Предложение 1. Подгруппа H в $\mathbb{R}^n$ является дискретной тогда и только тогда, когда H — решётка в $\mathbb{R}^n$.

Доказательство. Пусть H — решётка в $\mathbb{R}^n$ ранга k. Если $k < n$, то дополним какой-то фиксированный базис $v_1, \ldots, v_k$ решётки до базиса пространства $\mathbb{R}^n$ и заменим H на решётку $\mathbb{Z}v_1{+}\ldots{+}\mathbb{Z}v_n$ в $\mathbb{R}^n$. Определим сферу $U(m) = \left\{ \alpha_1 v_1{+}\ldots{+}\alpha_n v_n \mid \sum\limits_{i=1}^{n} \alpha_i^2 \le m^2 \right\}$. Сдвиги фундаментального параллелепипеда полной решётки покры-

вает всё пространство, поэтому для произвольного ограниченного множества Y в $\mathbb{R}^n$ для подходящего m выполнено $Y \subseteq U(m)$. Наконец, если $\sum\limits_{i=1}^{n} \alpha_i v_i \in H \cap U(m)$ и $\alpha_i \in \mathbb{Z}$, то $|\alpha_i| \leq m$. Следовательно, таких наборов (α_i) есть лишь конечное число.

Пусть H — дискретная подгруппа $\mathbb{R}^n$. Рассмотрим линейную оболочку $U = L(H)$. Выберем базис $v_1, \ldots, v_k$ подпространства U, состоящий из векторов из H. Введём $H' = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_k \subseteq H$ — решётку в U.

Покажем, что $|H/H'| < \infty$. Пусть λ_i, $i \in \mathcal{I}$, — представители классов в H/H'. Применим равенство $U = \dot{\bigcup\limits_{\lambda \in H'}} (\lambda + T)$, где T — фундаментальный параллелепипед H' относительно базиса $v_1, \ldots, v_k$. Значит, $\lambda_i = \lambda_i' + s_i$, $i \in \mathcal{I}$, для некоторых $\lambda_i' \in H'$ и $s_i \in T$. Поскольку $S = \{s_i = \lambda_i - \lambda_i' \mid i \in \mathcal{I}\}$ — подмножество в H, а T ограничено, в силу дискретности подгруппы H заключаем, что S конечно, и поэтому H/H' конечна. Пусть $q = |H/H'|$, тогда $qH \subseteq H'$, то есть $H \subseteq \frac{1}{q}\mathbb{Z}v_1 + \ldots + \frac{1}{q}\mathbb{Z}v_k$. По теореме о строении конечнопорождённых абелевых групп получаем, что H — свободная группа ранга k. Следовательно, H — решётка. □

Лемма 1. Пусть H — полная решётка в $\mathbb{R}^n$, T — её фундаментальный параллелепипед, а S — такое измеримое подмножество в $\mathbb{R}^n$, что $\mathrm{vol}(S) > \mathrm{vol}(T)$. Тогда найдутся различные $x, y \in S$, удовлетворяющие условию $x - y \in H$.

Доказательство. Равенство $\mathrm{vol}(S) = \sum\limits_{h \in H} \mathrm{vol}(S \cap (h + T))$ выполнено в силу счётной аддитивности. Если $(S - h_1) \cap (S - h_2) \cap T = \emptyset$ для любых $h_1 \neq h_2$, тогда $\mathrm{vol}(S) = \sum\limits_{h \in H} \mathrm{vol}((S - h) \cap T)) \leq \mathrm{vol}(T)$, противоречие. Значит, найдутся различные $h_1, h_2 \in H$, $x, y \in S$ такие, что $x - h_1 = y - h_2$, то есть $x - y = h_1 - h_2 \in H$ и $x \neq y$. □

Множество $X \subseteq \mathbb{R}^n$ называется центрально-симметричным, если для произвольного $x \in X$ выполнено $-x \in X$.

Теорема 1 (Минковского, 1897). Пусть H — полная решётка в $\mathbb{R}^n$, S — ограниченное измеримое центрально-симметричное выпуклое подмножество в $\mathbb{R}^n$. Если

а) $\mathrm{vol}(S) > 2^n \mathrm{vol}(H)$ или

б) $\mathrm{vol}(S) \geq 2^n \mathrm{vol}(H)$ и S компактно,

тогда $S \cap (H \setminus \{0\}) \neq \emptyset$.

Доказательство. а) Для множества $S' = S/2$ верно, что $\mathrm{vol}(S') > \mathrm{vol}(H)$. Тогда по лемме 1 найдутся различные $x, y \in S'$ такие, что $x - y \in H$. Поскольку $x - y = \frac{1}{2}(2x - 2y) \in S$, утверждение доказано.

б) Применим а) ко множеству $(1 + 1/m)S$, $m = 1, 2, \ldots$. Множество $(1 + 1/m)S$ ограничено, поэтому по предложению 1 оно содержит лишь конечное число точек из H. Следовательно, $S_m = (1+1/m)S \cap (H \setminus \{0\})$ — непустое компактное подмножество в $\mathbb{R}^n$. Так как $S_{m+1} \subseteq S_m$, заключаем, что $\bigcap\limits_{m=1}^{\infty} S_m \neq \emptyset$. Отсюда любой $x \in \bigcap\limits_{m=1}^{\infty} S_m$ лежит в $S \cap (H \setminus \{0\})$, поскольку $\bigcap\limits_{m=1}^{\infty} (1 + 1/m)S = S$ в силу компактности S. □

Пример. Пусть $H = \mathbb{Z}e_1 + \mathbb{Z}e_2$ — решётка в $\mathbb{R}^2$, где $e_1 = (1, 0)$ и $e_2 = (0, 1)$. Зададим $S = \{\alpha_1 e_1 + \alpha_2 e_2 \mid -1 < \alpha_1, \alpha_2 < 1\}$. С одной стороны, $\mathrm{vol}(S) = 4 = 2^2 \mathrm{vol}(H)$. С другой стороны, $S \cap H = \{0\}$. Значит, условие компактности в теореме 1б) существенно.

3.2 Подсчёт объёма

Отождествим пространство $\mathbb{R}^n$ с $\mathbb{R}^r \times \mathbb{C}^s$, где $n = r + 2s$. Определим

$$B_t = \left\{ (y_1, \dots, y_r, z_1, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid \sum_{i=1}^{r} |y_i| + 2 \sum_{j=1}^{s} |z_j| \le t \right\}, \quad t \ge 0.$$

Теорема 2. $\mathrm{vol}(B_t) = 2^r(\pi/2)^s t^n/n!$.

Доказательство. Обозначим $V(r, s, t) = \mathrm{vol}(B_t)$. Докажем формулу индукцией по $r + s$. База индукции следует из равенств

$$V(1, 0, t) = \mathrm{vol}\{y_1 \in \mathbb{R} \mid |y_1| \le t\} = 2t,$$
$$V(0, 1, t) = \mathrm{vol}\{z_1 \in \mathbb{C} \mid 2|z_1| \le t\} = \pi(t/2)^2,$$

второе равенство есть ничто иное как подсчёт площади круга радиуса $t/2$.

Докажем индукционный шаг. Для подсчёта $V(r+1, s, t)$ добавим переменную y_0: $(y_0, y_1, \dots, y_r, z_1, \dots, z_s) \in B_t$, тогда выражаем

$$V(r+1, s, t) = \int_{-t}^{t} V(r, s, t - |y_0|)\, dy_0 = 2^r(\pi/2)^s 2/n! \int_0^t (t - y_0)^n\, dy_0$$
$$= 2^{r+1}(\pi/2)^s 1/n! \left(-\frac{(t-y_0)^{n+1}}{n+1} \right) \Big|_0^t = 2^{r+1}(\pi/2)^s t^{n+1}/(n+1)!.$$

Для подсчёта $V(r, s+1, t)$ добавим переменную z_0: $(y_1, \dots, y_r, z_0, z_1, \dots, z_s) \in B_t$. Пусть $z_0 = x_0 + iy_0$, где $x_0, y_0 \in \mathbb{R}$. При переходе к полярным координатам $z_0 = \rho e^{i\theta}$ получаем $dx_0 dy_0 = \rho\, d\rho d\theta$. Поэтому

$$V(r, s+1, t) = \int_{|z_0| \le t/2} V(r, s, t - 2|z_0|)\, dz_0$$
$$= 2^r(\pi/2)^s 1/n! \int_0^{t/2} \int_0^{2\pi} (t - 2\rho)^n \rho\, d\rho d\theta = 2^r(\pi/2)^{s+1} t^{n+2}/(n+2)!,$$

поскольку при замене $x = 2\rho$ и по формуле интегрирования по частям выводим

$$4 \int_0^{t/2} (t - 2\rho)^n \rho\, d\rho = \int_0^t (t - x)^n x\, dx = \left(-\frac{(t-x)^{n+1}}{n+1} x \right) \Big|_0^t - \int_0^t \frac{-(t-x)^{n+1}}{n+1}\, dx$$
$$= \frac{t^{n+2}}{(n+1)(n+2)}. \quad \square$$

3.3 Конечность группы классов

Пусть K — алгебраическое числовое поле степени n над $\mathbb{Q}$. Пусть $\sigma_1, \dots, \sigma_n$ — вложения поля K в $\mathbb{C}$, оставляющие $\mathbb{Q}$ неподвижным. Выберем такую нумерацию σ_j, что $\sigma_1, \dots, \sigma_r$ и только они отображают K в $\mathbb{R}$. При этом $\sigma_{r+1}, \dots, \sigma_n$ разбиваются на пары комплексно-сопряжённых, так как для любого $\mathbb{Q}$-вложения $\psi\colon K \to \mathbb{C}$ такого, что $\psi(K) \not\subset \mathbb{R}$, отображение $\overline{\psi}$, заданное по правилу $\overline{\psi}(x) = \overline{\psi(x)}$, также является $\mathbb{Q}$-вложением K в $\mathbb{C}$. Следовательно, $n = r + 2s$ и $\sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_s, \overline{\sigma_s}$ исчерпывают $\mathbb{Q}$-вложения K в $\mathbb{C}$, образ которых не содержится в $\mathbb{R}$.

Определим вложение σ поля K в $\mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$ так:

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_r(x), \operatorname{Re}\sigma_{r+1}(x), \operatorname{Im}\sigma_{r+1}(x), \dots, \operatorname{Re}\sigma_{r+s}(x), \operatorname{Im}\sigma_{r+s}(x))^T.$$

Лемма 2. Пусть $x_1, \dots, x_n$ — базис K над $\mathbb{Q}$, $H = \mathbb{Z}x_1 + \ldots + \mathbb{Z}x_n$. Тогда $\sigma(H)$ — полная решётка в $\mathbb{R}^n$ и $\operatorname{vol}(\sigma(H)) = 2^{-s}|\det((\sigma_i(x_j))_{i,j=1}^n)|$.

Доказательство. Пусть $A = (\sigma(x_1) \dots \sigma(x_n))$ и $B = (B^1 \dots B^n)$, где $B^i = (\sigma_1(x_i), \dots, \sigma_r(x_i), \sigma_{r+1}(x_i), \overline{\sigma_{r+1}}(x_i), \dots, \sigma_{r+s}(x_i), \overline{\sigma_{r+s}}(x_i))^T$. Обозначим $\sigma_{r+1}(x_j) = a_j + ib_j$ для $a_j, b_j \in \mathbb{R}$. Элементарными преобразованиями приводим строки B_{r+1} и B_{r+2} к виду

$$\begin{pmatrix} a_1 + ib_1 & \dots & a_n + ib_n \\ a_1 - ib_1 & \dots & a_n - ib_n \end{pmatrix} \rightsquigarrow \begin{pmatrix} a_1 + ib_1 & \dots & a_n + ib_n \\ 2a_1 & \dots & 2a_n \end{pmatrix} \rightsquigarrow \begin{pmatrix} ib_1 & \dots & ib_n \\ 2a_1 & \dots & 2a_n \end{pmatrix}.$$

Таким же образом поступаем со всеми парами строк B_{r+2k+1} и B_{r+2k+2}, где $k = 1, \dots, s-1$. Отсюда $\det B = (-2i)^s \det A$, и $\sigma(x_1), \dots, \sigma(x_n)$ образуют базис решётки $\sigma(H)$. Значит,

$$\operatorname{vol}(\sigma(H)) = |\det A| = 2^{-s}|\det B| = 2^{-s}|\det((\sigma_i(x_j)))|. \quad \square$$

Следствие 1 (теорема Брилля, 1877). Пусть K — алгебраическое числовое поле. Тогда $\operatorname{sign}(\operatorname{disc}(K/\mathbb{Q})) = (-1)^s$.

Доказательство. В терминах доказательства леммы 2 и по лемме 8 гл. I имеем $\operatorname{sign}(\operatorname{disc}(K/\mathbb{Q})) = \operatorname{sign}(\det^2 B) = \operatorname{sign}((-2i)^{2s}) = (-1)^s$. $\square$

Следствие 2. Пусть K — алгебраическое числовое поле, $(0 \neq) I \lhd \mathcal{O}_K$. Тогда $\sigma(I)$ — полная решётка в $\mathbb{R}^n$ и $\operatorname{vol}(\sigma(I)) = 2^{-s}\mathbb{N}(I)\sqrt{|\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})|}$.

Доказательство. По теореме о строении конечнопорождённых модулей над областью главных идеалов найдём $a_1, \dots, a_n \in \mathbb{Z}$ и $x_1, \dots, x_n \in \mathcal{O}_K$ такие, что $x_1, \dots, x_n$ — базис $\mathcal{O}_K$ над $\mathbb{Z}$ и $a_1x_1, \dots, a_nx_n$ — базис I над $\mathbb{Z}$. Тогда $\mathbb{N}(I) = |a_1 \dots a_n|$ по определению 8 гл. II. Это влечёт

$$\operatorname{vol}(\sigma(I)) = 2^{-s}|\det((\sigma_i(a_jx_j)))| = 2^{-s}|a_1 \dots a_n| \cdot |\det((\sigma_i(x_j)))| = 2^{-s}\mathbb{N}(I)\sqrt{|\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})|},$$

что и требовалось доказать. $\square$

Лемма 3. Пусть K — алгебраическое числовое поле, $(0 \neq) I \lhd \mathcal{O}_K$. Тогда найдётся $(0 \neq) x \in I$ такой, что $|N_{K/\mathbb{Q}}(x)| \leq n!/n^n(4/\pi)^s\mathbb{N}(I)\sqrt{|\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})|}$.

Доказательство. Множество B_t, определённое в §2, компактно, выпукло и центрально-симметрично. Выберем t так, чтобы

$$t^n = 2^{n-r}\pi^{-s}n!\mathbb{N}(I)\sqrt{|\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})|}. \tag{3.1}$$

Тогда по теореме 2 и по следствию 2 выполнено $\mathrm{vol}(B_t) = 2^n \mathrm{vol}(\sigma(I))$. По теореме 1б) имеем $B_t \cap (\sigma(I) \setminus \{0\}) \neq \emptyset$, то есть найдётся $(0 \neq) x \in I$ такой, что $\sigma(x) \in B_t$. Применяя предложение 4 гл. I, по неравенству о средних оцениваем

$$\begin{aligned} |N_{K/\mathbb{Q}}(x)| &= |\sigma_1(x)| \dots |\sigma_r(x)| \cdot |\sigma_{r+1}(x)|^2 \dots |\sigma_{r+s}(x)|^2 \\ &\leq (|\sigma_1(x)| + \dots + |\sigma_r(x)| + 2|\sigma_{r+1}(x)| + \dots + 2|\sigma_{r+s}(x)|)^n / n^n \leq t^n / n^n, \end{aligned}$$

так как $\sigma(x) \in B_t$. Вместе с (3.1) полученная оценка завершает доказательство. □

Следствие 3. Пусть K — алгебраическое числовое поле. Тогда каждый класс в $\mathrm{Cl}(K)$ содержит целый идеал I такой, что

$$\mathbb{N}(I) \leq n!/n^n (4/\pi)^s \sqrt{|\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})|}. \tag{3.2}$$

Доказательство. Пусть J' — дробный идеал из данного класса в $\mathrm{Cl}(K)$. Не теряя общности, можем считать, что $J = (J')^{-1}$ — целый идеал, иначе умножаем на подходящий главный идеал $\mathcal{O}_K$. Выберем $(0 \neq) x \in J$, удовлетворяющий неравенству из леммы 3. Заметим, что $I = xJ'$ — целый идеал $\mathcal{O}_K$, при этом $(x) = I \cdot J$. По лемме 7 и предложению 7 гл. II имеем

$$\mathbb{N}(I \cdot J) = \mathbb{N}(I)\mathbb{N}(J) = |N_{K/\mathbb{Q}}(x)| \leq n!/n^n (4/\pi)^s \mathbb{N}(J) \sqrt{|\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})|},$$

откуда следует неравенство (3.2). □

Теорема 3. Пусть K — алгебраическое числовое поле. Тогда $\mathrm{Cl}(K)$ конечна.

Доказательство. По следствию 3 каждый класс в $\mathrm{Cl}(K)$ содержит такой целый идеал I, что выполнено неравенство (3.2). По замечанию из §5 гл. II существует лишь конечное число идеалов, чья считающая норма ограничена данной константой. □

Предложение 2. Пусть K — алгебраическое числовое поле степени $n \geq 2$ и $d_K = \mathrm{disc}(\mathcal{O}_K/\mathbb{Z})$. Тогда $|d_K| \geq \frac{n^{2n}}{(n!)^2} \left(\frac{\pi}{4}\right)^{2s} \geq \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1}$.

Доказательство. По формуле (3.2) имеем $1 \leq \mathbb{N}(I) \leq n!/n^n (4/\pi)^s \mathbb{N}(I) \sqrt{|d_K|}$, то есть $|d_K| \geq \frac{n^{2n}}{(n!)^2} \left(\frac{\pi}{4}\right)^{2s}$. Так как $2s \leq n$ и $\pi/4 < 1$, оцениваем $|d_K| \geq \frac{n^{2n}}{(n!)^2} \left(\frac{\pi}{4}\right)^n := a_n$. В последовательности чисел $\{a_n\}_{n \geq 2}$ имеем $a_2 = \pi^2/4$ и

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4} \cdot \frac{(n+1)^2 (n+1)^{2n} (n!)^2}{((n+1)!)^2 n^{2n}} = \frac{\pi}{4} \left(1 + \frac{1}{n}\right)^{2n} > \frac{3\pi}{4},$$

поскольку $(1 + 1/n)^{2n} = 1 + 2 + \dots > 3$. Отсюда $|d_K| \geq \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1}$, так как $a_n \geq \left(\frac{3\pi}{4}\right)^{n-2} a_2 = \left(\frac{3\pi}{4}\right)^{n-2} \cdot \frac{3\pi}{4} \cdot \frac{\pi}{3} = \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1}$. □

Следствие 4. Пусть K — алгебраическое числовое поле степени $n \geq 2$. Тогда $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) \neq \pm 1$. В частности, найдётся простое число p такое, что (p) разветвляется в $\mathcal{O}_K$.

Доказательство. По предложению 2 имеем $|\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})| \geq \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1} > 1$. Остаётся применить предложение 6 гл. II. □

Теорема 4 (Эрмит, 1857). Для любого $d \in \mathbb{Z}$ существует лишь конечное число алгебраических числовых полей K таких, что $\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = d$.

Доказательство. Обозначим $d_K = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$. Логарифмируя правую оценку из предложения 2, получаем неравенство $n \leq C \ln |d_K|$ для подходящей константы $C > 0$. Покажем, что найдётся лишь конечное число полей K с фиксированными значениями d_K, r и s. Определим множество B при $r > 0$ как

$$B = \{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid \\ |y_1| \leq 2^n (2/\pi)^s \sqrt{|d_K|},\ |y_2|, \ldots, |y_r|, |z_1|, \ldots, |z_s| \leq 1/2\},$$

а при $r = 0$ как

$$B = \{(z_1, \ldots, z_s) \in \mathbb{C}^s \mid |z_1 - \bar{z}_1| \leq 2^n (2/\pi)^{s-1} \sqrt{|d_K|},\ |z_1 + \bar{z}_1|, |z_2|, \ldots, |z_s| \leq 1/2\}.$$

Тогда B — выпуклое компактное и центрально-симметричное подмножество в $\mathbb{R}^n$, и $\operatorname{vol}(B) = 2^{n-s}\sqrt{|d_K|} = 2^n \operatorname{vol}(\sigma(\mathcal{O}_K))$ по следствию 2. По теореме Минковского найдётся $(0 \neq) x \in \mathcal{O}_K$ такой, что $\sigma(x) \in B$. Докажем, что $K = \mathbb{Q}[x]$.

При $r > 0$ выполнено $|\sigma_i(x)| \leq 1/2$, $i = 2, \ldots, n$. По предложению 4 гл. I верно, что $|N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{n} |\sigma_i(x)| \geq 1$, поскольку $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$ по предложению 5 гл. I. Отсюда $|\sigma_1(x)| \geq 1$ и поэтому $\sigma_1(x) \neq \sigma_i(x)$ для любого $i \neq 1$. Предположим, что $K \neq \mathbb{Q}[x]$, тогда отображение $\sigma_1|_{\mathbb{Q}[x]} \colon \mathbb{Q}[x] \to \mathbb{C}$ имеет $[K : \mathbb{Q}[x]] - 1$ продолжений отличных от σ_1. Получили противоречие с тем, что $\sigma_1(x) \neq \sigma_i(x)$ для $i = 2, \ldots, n$.

При $r = 0$ аналогично выписываем $|\sigma_1(x)| = |\overline{\sigma}_1(x)| \geq 1$ и поэтому $\sigma_1(x) \neq \sigma_i(x)$ для $i = 3, \ldots, n$. Равенство $\sigma_1(x) = \overline{\sigma}_1(x)$ не выполняется, поскольку $|\operatorname{Re}(\sigma_1(x))| \leq 1/4$ по заданию множества B. Как и выше, заключаем, что $K = \mathbb{Q}[x]$.

В итоге отмечаем, что $|\sigma_i(x)|$ ограничены. Поэтому минимальный многочлен $m^x_{\mathbb{Q}}(t) \in \mathbb{Z}[t]$ степени n имеет ограниченные коэффициенты. Значит, таких многочленов есть лишь конечное число, что влечёт конечность числа их корней. $\square$

Глава 4

Теорема Дирихле о единицах

В этой главе мы опишем строение группы единиц (обратимых элементов) произвольного алгебраического числового поля K. Как и в третьей главе, мы будем активно применять теорию Минковского.

4.1 Группа единиц

Определение 1. Группой единиц алгебраического числового поля K называется $\mathcal{O}_K^*$ — группа обратимых элементов в кольце $\mathcal{O}_K$.

Лемма 1. Элемент $x \in \mathcal{O}_K$ обратим тогда и только тогда, когда $N_{K/\mathbb{Q}}(x) = \pm 1$.

Доказательство. Пусть $x \cdot x^{-1} = 1$, тогда

$$1 = N_{K/\mathbb{Q}}(x \cdot x^{-1}) = N_{K/\mathbb{Q}}(x) N_{K/\mathbb{Q}}(x^{-1}).$$

По предложению 5 гл. I. $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$, следовательно, $N_{K/\mathbb{Q}}(x) = \pm 1$.

Пусть $N_{K/\mathbb{Q}}(x) = \pm 1$, тогда по определению нормы элемента $\mathrm{char}^x_{K/\mathbb{Q}}(t) = t^n + \ldots + (-1)^n N_{K/\mathbb{Q}}(x)$, то есть $x(x^{n-1} + \ldots) = \pm 1$. Значит, $x \in \mathcal{O}_K^*$. □

Пусть, как и в гл. III, $n = [K : \mathbb{Q}]$, $\sigma_1, \ldots, \sigma_n$ — попарно различные $\mathbb{Q}$-вложения K в $\mathbb{C}$, среди которых в точности $\sigma_1, \ldots, \sigma_r$ отображают K в $\mathbb{R}$, а $\sigma_{r+s+1} = \overline{\sigma_{r+1}}$, $\ldots$, $\sigma_{r+2s} = \overline{\sigma_{r+s}}$, где $n = r + 2s$. Зададим логарифмическое вложение $l\colon \mathcal{O}_K^* \to \mathbb{R}^{r+s}$ следующим образом:

$$l(x) = (\ln|\sigma_1(x)|, \ldots, \ln|\sigma_r(x)|, \ln|\sigma_{r+1}(x)|, \ldots, \ln|\sigma_{r+s}(x)|),$$

это гомоморфизм групп.

Лемма 2. Пусть Y — ограниченное подмножество в $\mathbb{R}^n$. Тогда множество $Y' = \{x \in \mathcal{O}_K^* \mid l(x) \in Y\}$ конечно.

Доказательство. Поскольку Y ограничено, выполнено $|\sigma_i(x)| \leq A$ для всех $i = 1, \ldots, r+s$, $x \in Y'$ и подходящей константы A. Отсюда элементарные симметрические многочлены от $\sigma_i(x)$ по модулю также ограничены некоторой константой A'. По предложению 5 гл. I эти многочлены — целые числа. Отсюда есть лишь конечное число многочленов $\mathrm{char}^x_{K/\mathbb{Q}}(t)$ элементов $x \in Y'$. Значит, и корней минимальных многочленов $m^x_{K/\mathbb{Q}}(t)$, $x \in Y'$, также конечное число. □

Следствие 1. Пусть $\mu_K = \ker l$. Тогда μ_K — конечная циклическая группа, состоящая в точности из всех корней из единицы, лежащих в K.

Доказательство. Возьмём $Y = \{0\}$ в лемме 2, тогда группа μ_k конечна. Известно, что конечная подгруппа K^* является циклической. Пусть ε_t — корень степени t из единицы, лежащий в K. Тогда $|\sigma_i(\varepsilon_t)|^t = |\sigma_i(\varepsilon_t)^t| = 1$. Отсюда $|\sigma_i(\varepsilon_t)| = 1$ и $l(\varepsilon_t) = 0$. □

Теорема 1 (Дирихле). Пусть K — алгебраическое числовое поле, тогда $\mathcal{O}_K^* \cong \mathbb{Z}^{r+s-1} \times \mu_K$.

Доказательство. По лемме 2 имеем, что $l(\mathcal{O}_K^*)$ — дискретная подгруппа $\mathbb{R}^{r+s}$. По предложению 1 гл. III заключаем, что $l(\mathcal{O}_K^*)$ — свободный $\mathbb{Z}$-модуль ранга $t \leq r+s$, отсюда и по теореме о гомоморфизмах $\mathcal{O}_K^* \cong \mathbb{Z}^t \times \mu_K$. Остаётся показать, что $t = r+s-1$. Применяя предложение 4 гл. I и лемму 1, выписываем для произвольного $x \in \mathcal{O}_K^*$ равенство

$$\pm 1 = N_{K/\mathbb{Q}}(x) = \left(\prod_{i=1}^{r} \sigma_i(x)\right) \cdot \left(\prod_{j=r+1}^{r+s} \sigma_j(x)\overline{\sigma_j(x)}\right).$$

Беря модули и логарифмируя, получаем, что $l(\mathcal{O}_K^*)$ содержится в гиперплоскости

$$U = \left\{(y_1, \ldots, y_{r+s}) \in \mathbb{R}^{r+s} \mid \sum_{i=1}^{r} y_i + 2\sum_{j=r+1}^{r+s} y_j = 0\right\}.$$

Докажем, что $t \geq r+s-1$, или эквивалентно, что любая линейная форма, зануляющаяся на $l(\mathcal{O}_K^*)$, зануляется и на U. Для этого для произвольной ненулевой функции $f\colon U \to \mathbb{R}$ найдём единицу $u \in \mathcal{O}_K^*$ такую, что $f(l(u)) \neq 0$.

Отождествим точку $(y_1, \ldots, y_{r+s}) \in U$ с точкой $(y_1, \ldots, y_{r+s-1}) \in \mathbb{R}^{r+s-1}$. Выражаем $f(y_1, \ldots, y_{r+s-1}) = c_1 y_1 + \ldots + c_{r+s-1} y_{r+s-1}$ для некоторых $c_i \in \mathbb{R}$. Для набора $(\lambda_1, \ldots, \lambda_{r+s}) \in \mathbb{R}_{>0}^{r+s}$ определим

$$\alpha = \prod_{i=1}^{r} \lambda_i \prod_{j=r+1}^{r+s} \lambda_j^2. \tag{4.1}$$

Выберем α так, чтобы выполнялось неравенство $\alpha \geq (2/\pi)^s \sqrt{|\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})|}$. Для множества $B_\lambda = \{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid |y_i| \leq \lambda_i,\ |z_j| \leq \lambda_{j+r}\}$ имеем

$$\mathrm{vol}(B_\lambda) = \left(\prod_{i=1}^{r} 2\lambda_i\right)\left(\prod_{j=r+1}^{r+s} \pi\lambda_j^2\right) = 2^r \pi^s \alpha \geq 2^{n-s}\sqrt{|\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})|}.$$

По теореме Минковского и лемме 3 гл. III найдётся $(0 \neq) x_\lambda \in \mathcal{O}_K$ такой, что $\sigma(x_\lambda) \in B_\lambda$.

По определению множества B_λ выполнено $|\sigma_i(x_\lambda)| \leq \lambda_i$ для всех $i = 1, \ldots, r+s$. Таким образом,

$$1 \leq |N_{K/\mathbb{Q}}(x_\lambda)| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{r} \lambda_i \prod_{j=r+1}^{r+s} \lambda_j^2 = \alpha.$$

Отсюда

$$|\sigma_i(x_\lambda)| = \frac{|N_{K/\mathbb{Q}}(x_\lambda)|}{\prod\limits_{j\neq i}|\sigma_j(x_\lambda)|} \geq \frac{1}{\prod\limits_{j\neq i}|\sigma_j(x_\lambda)|} \geq \frac{\lambda_i}{\alpha}.$$

Значит, $\lambda_i/\alpha \leq |\sigma_i(x_\lambda)| \leq \lambda_i$, что эквивалентно $0 \leq \ln(\lambda_i) - \ln(|\sigma_i(x_\lambda)|) \leq \ln\alpha$.

Для выбранной ранее функции f оцениваем

$$\left|f(l(x_\lambda)) - \sum_{i=1}^{r+s-1} c_i \ln\lambda_i\right| = \left|\sum_{i=1}^{r+s-1} c_i(\ln(|\sigma_i(x_\lambda)|) - \ln\lambda_i)\right| \leq \left(\sum_{i=1}^{r+s-1}|c_i|\right)\ln\alpha. \qquad (4.2)$$

Выберем $\beta > \left(\sum\limits_{i=1}^{r+s-1}|c_i|\right)\ln\alpha$, а для каждого $h \in \mathbb{N}_{>0}$ возьмём $\lambda_{i,h} \in \mathbb{R}_{>0}$, $i = \overline{1, r+s-1}$, совокупно удовлетворяющие равенству $\sum\limits_{i=1}^{r+s-1} c_i \ln\lambda_{i,h} = 2\beta h$. Дополнительно зададим $\lambda_{r+s,h} > 0$ так, чтобы выполнялось (4.1). Обозначим $\lambda(h) = (\lambda_{1,h}, \ldots, \lambda_{r+s,h})$ и $x_h = x(\lambda(h))$. По (4.2) получаем $|f(l(x_h)) - 2\beta h| < \beta$, то есть $(2h-1)\beta < f(l(x_h)) < (2h+1)\beta$. Следовательно,

$$\beta < f(l(x_1)) < 3\beta < f(l(x_2)) < 5\beta < \ldots.$$

Эти неравенства влекут, что значения $f(l(x_h))$ попарно различны. Напомним, что $\mathbb{N}((x_h)) \leq \alpha$. По замечанию в конце гл. II существует лишь конечное число идеалов, чья считающая норма не превосходит α. Значит, $(x_{h_1}) = (x_{h_2})$ для некоторых $h_1 \neq h_2$. Поэтому $\left(x_{h_1}^{-1}x_{h_2}\right) = \mathcal{O}_K$ и $u = x_{h_1}^{-1}x_{h_2} \in \mathcal{O}_K^*$. Остаётся проверить, что $f(l(u)) = f(l(x_{h_2})) - f(l(x_{h_1})) \neq 0$. □

Согласно теореме Дирихле любой элемент $u \in \mathcal{O}_K^*$ представим в виде $u = \xi u_1^{m_1}, \ldots u_{r+s-1}^{m_{r+s-1}}$, где $\xi \in \mu_K$, $m_i \in \mathbb{Z}$.

Определение 3. Набор единиц $u_1, \ldots u_{r+s-1}$ называется множеством основных единиц алгебраического числового поля K.

4.2 S-единицы

Пусть K — алгебраическое числовое поле, $\alpha \in K^*$ и $(\alpha) = P_1^{a_1}\ldots P_k^{a_k}$ — разложение главного дробного идеала по степеням простых идеалов в $\mathcal{O}_K$. Будем обозначать $a_i = \mathrm{ord}_{P_i}(\alpha)$.

Зафиксируем конечное множество S простых идеалов и определим кольцо

$$\mathcal{O}_K(S) = \bigcap_{P\notin S}(\mathcal{O}_K)_P = \{\alpha \in K^* \mid \mathrm{ord}_P(\alpha) \geq 0 \text{ для } P \notin S\} \cup \{0\}.$$

Определение 4. Группой S-единиц называется множество $\mathcal{O}_K(S)^* = \{\alpha \in O_K(S) \mid \mathrm{ord}_P(\alpha) = 0,\ P \notin S\}$.

Теорема 2. Пусть K — алгебраическое числовое поле, S — конечное множество простых идеалов в $\mathcal{O}_K$. Тогда группа S-единиц является конечнопорождённой группой ранга $r + s + |S| - 1$.

Доказательство. Пусть $S = \{P_1, \ldots, P_t\}$. Зададим гомоморфизм $\varphi\colon \mathcal{O}_K(S)^* \to \mathbb{Z}^t$ по формуле

$$\varphi(u) = (\mathrm{ord}_{P_1}(u), \ldots, \mathrm{ord}_{P_t}(u)).$$

Имеем $\ker(\varphi) = \mathcal{O}_K^* \cong \mathbb{Z}^{r+s-1} \times \mu_K$. Покажем, что $\mathrm{Im}\,(\varphi)$ является подгруппой $\mathbb{Z}^t$ ранга t. По определению и теореме 3 гл. III выполнено $P_i^{h_K} = (\pi_i)$, где $\pi_i \in \mathcal{O}_K$. При этом $\varphi(\pi_i) = (0, \ldots, 0, \underset{i}{h_K}, \ldots, 0)$. Ясно, что элементы $\varphi(\pi_1), \ldots, \varphi(\pi_t)$ порождают в $\mathbb{Z}^t$ подгруппу ранга t. □

Пример. Пусть $K = \mathbb{Q}$, а $S = \{(2), (3), (5)\}$, тогда $\mathcal{O}_K(S)^* = \{\pm 2^k 3^l 5^m \mid k, l, m \in \mathbb{Z}\}$, её ранг равен $1 + 0 + 3 - 1 = 3$.

4.3 Аналитическая формула числа классов

Определение 5. Пусть K — алгебраическое числовое поле, $u_1, \ldots u_{r+s-1}$ — множество основных единиц K. Тогда $R_K = |\det((\ln|\sigma_i(u_j)|)_{i,j=1}^{r+s-1})|$ называется регулятором K.

Регулятор поля не зависит от выбора множества основных единиц.

Пусть $R = \mathbb{Q}[\sqrt{d}]$, где d свободно от квадратов. При $d > 1$ имеем $R_K = |\ln(|u|)|$, где u — основная единица поля K. При $d < 0$ имеем $R_K = 1$.

Определение 6. Пусть K — алгебраическое числовое поле. Дедекиндовой дзета-функцией называется ряд $\zeta_K(z) = \sum\limits_{I \lhd \mathcal{O}_K} \dfrac{1}{\mathbb{N}(I)^z}$, $\mathrm{Re}\, z > 1$.

При $K = \mathbb{Q}$ получаем дзета-функцию Римана $\zeta(z) = \sum\limits_{n \geq 1} \dfrac{1}{n^z}$, $\mathrm{Re}\, z > 1$. Ряд $\zeta_K(z)$ сходится абсолютно и равномерно в области $\mathrm{Re}\, z > 1$. Как и для дзета-функции Римана, существует аналитическое продолжение $\zeta_K(z)$ с единственным простым полюсом в точке $z = 1$ на полупроскость $\mathrm{Re}\, z > 1 - \delta_K$ для некоторого $\delta_K > 0$.

Приведём без доказательства замечательный результат, связывающий в единой формуле дзета-функцию Дедекинда, число классов поля, регулятор поля, дискриминант поля и количество корней из единицы, принадлежащих данному полю.

Теорема 3. Пусть K — алгебраическое числовое поле с r вещественными и s комплексными вложениями в $\mathbb{C}$. Тогда верна следующая формула:

$$\mathrm{Res}_{z=1}\zeta_K(z) = \frac{2^r(2\pi)^s R_K h_K}{|\mu_K|\sqrt{|\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})|}}. \tag{4.3}$$

Для $K = \mathbb{Q}$ получаем $\mathrm{Res}_{z=1}\zeta(z) = \dfrac{2^1(2\pi)^0 \cdot 1 \cdot 1}{2 \cdot 1^{1/2}} = 1$.

В зависимости от поля K формула (4.3) применяется как для вычисления h_K, так и для вычисления R_K.

Глава 5

Круговые поля

В последней главе мы сперва изучим для круговых полей кольцо целых, разветвляемость простых идеалов и группу единиц. Применяя полученные результаты, мы приведём данное Куммером доказательство теоремы Ферма для регулярных простых. Отметим, что круговые поля представляют и самостоятельный интерес. По теореме Кронекера — Вебера любое конечное расширение K поля $\mathbb{Q}$ с абелевой группой Галуа является подполем подходящего кругового поля.

5.1 Круговые многочлены

Определение 1. Круговым полем называется поле $\mathbb{Q}[\zeta]$, где ζ — первообразный корень степени n из единицы.

Напомним, что корень ζ степени n из единицы называется первообразным, если $\zeta^d \neq 1$ для всех $d = 1, \ldots, n-1$. Пусть ζ — первообразный корень степени n из единицы. Тогда ζ^m является первообразным корнем степени n из единицы тогда и только тогда, когда $(m, n) = 1$.

Определение 2. Минимальный многочлен $\Phi_n(t) \in \mathbb{Q}[t]$ первообразного корня степени n из единицы называется круговым многочленом.

Многочлен $\Phi_n(t)$ не зависит от выбора первообразного корня и $\Phi_n(t) = \prod\limits_{m \leq n,\, (m,n)=1} (t - \zeta^m)$, где ζ — какой-то первообразный корень степени n из единицы. Поскольку каждый корень степени n из единицы является первообразным корнем степени d из единицы для единственного d, получаем

$$t^n - 1 = \prod_{d|n} \Phi_d(t). \tag{5.1}$$

Имеем $[\mathbb{Q}[\zeta]:\mathbb{Q}] = \varphi(n)$, где $\varphi(n)$ — функция Эйлера. Известно, что $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \cong \mathbb{Z}_n^*$.

Пусть p — простое, тогда согласно (5.1) выполнено $t^p - 1 = \Phi_1(t)\Phi_p(t) = (t-1)\Phi_p(t)$. Отсюда $\Phi_p(t) = \dfrac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \ldots + 1$. По мультипликативной версии формулы обращения Мёбиуса, применённой к (5.1), выводим $\Phi_n(t) = \prod\limits_{d|n} (t^d - 1)^{\mu(n/d)}$.

В частности, $\Phi_{p^k}(t) = \dfrac{t^{p^k} - 1}{t^{p^{k-1}} - 1} = \Phi_p(t^{p^{k-1}})$.

5.2 Кольца целых кругового поля

Лемма 1. Пусть p — простое, $n = p^r$, ζ — первообразный корень степени n из единицы, $K = \mathbb{Q}[\zeta]$. Положим $P = (1-\zeta)$. Тогда P — простой идеал в $\mathcal{O}_K$ и $p\mathcal{O}_K = P^e$, где $e = [K : \mathbb{Q}] = \varphi(n)$. Более того, $N_{K/\mathbb{Q}}(1-\zeta) = p$.

Доказательство. Пусть ζ' — ещё один первообразный корень степени n из единицы. Поскольку $\zeta' = \zeta^s$ и $\zeta = (\zeta')^t$ для некоторых s, t, не делящихся на p, то $\mathbb{Q}[\zeta] = \mathbb{Q}[\zeta']$ и $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta']$. Далее,

$$\frac{1-\zeta'}{1-\zeta} = \frac{1-\zeta^s}{1-\zeta} = 1 + \zeta + \ldots + \zeta^{s-1} \in \mathbb{Z}[\zeta], \quad \frac{1-\zeta}{1-\zeta'} = 1 + \zeta' + \ldots + (\zeta')^{t-1} \in \mathbb{Z}[\zeta].$$

Значит, $\frac{1-\zeta'}{1-\zeta}, \frac{1-\zeta}{1-\zeta'} \in \mathbb{Z}[\zeta]^* \subseteq \mathcal{O}_K^*$. Распишем

$$p = \Phi_{p^r}(1) = \prod_{|\zeta'|=p^r} (1-\zeta') = \prod_{|\zeta'|=p^r} \frac{1-\zeta'}{1-\zeta}(1-\zeta) = u(1-\zeta)^e,$$

где $u \in \mathcal{O}_K^*$. Следовательно, $p\mathcal{O}_K = (1-\zeta)^e = P^e$. По теореме 5 гл. II имеем $e = efg$, значит, $f = g = 1$ и $p\mathcal{O}_K = P^e$ есть разложение на простые идеалы, то есть P прост.

По предложению 4 гл. I считаем $N_{K/\mathbb{Q}}(1-\zeta) = \prod\limits_{(j,p^r)=1} (1-\zeta^j) = \Phi_{p^r}(1) = p$. □

Лемма 2. Пусть p — простое, $n = p^r > 2$, ζ — первообразный корень степени n из единицы, $K = \mathbb{Q}[\zeta]$. Тогда $D(1, \zeta, \ldots, \zeta^{e-1}) = (-1)^{e/2} p^m$, где $e = [K : \mathbb{Q}] = \varphi(n)$, $m = p^{r-1}(pr - r - 1)$. Тем самым в K разветвляется только простой идеал (p).

Доказательство. По следствию 6 гл. I имеем $D(1, \zeta, \ldots, \zeta^{e-1}) = \pm N_{K/\mathbb{Q}}(\Phi_n'(\zeta))$. Из равенства $\Phi_{p^k}(t) = \dfrac{t^{p^k}-1}{t^{p^{k-1}}-1}$ вычисляем $\Phi_n'(\zeta) = \dfrac{p^r}{\zeta(\zeta^{p^{r-1}}-1)}$. Значит,

$$p^{re} = N_{K/\mathbb{Q}}(p^r) = N_{K/\mathbb{Q}}(\zeta(\zeta^{p^{r-1}}-1)\Phi_n'(\zeta)) = N_{K/\mathbb{Q}}(\zeta) N_{K/\mathbb{Q}}(\zeta^{p^{r-1}}-1) N_{K/\mathbb{Q}}(\Phi_n'(\zeta)).$$

Находим $N_{K/\mathbb{Q}}(\zeta) = (-1)^e$ по свободному коэффициенту многочлена $\Phi_n(t) = m_{K/\mathbb{Q}}^{\zeta}(t)$. По следствию 1 гл. III выполнено $\operatorname{sgn}(D(1, \zeta, \ldots, \zeta^{e-1})) = (-1)^{e/2}$. Для завершения доказательства леммы установим равенство $N_{K/\mathbb{Q}}(1-\zeta^{p^s}) = p^{p^s}$ индукцией по $0 \le s \le r-1$. Случай $s = 0$ следует из леммы 1. Поскольку ζ^{p^s} есть первообразный корень степени p^{r-s} из единицы, ещё раз применяем лемму 1: $N_{\mathbb{Q}[\zeta^{p^s}]/\mathbb{Q}}(1-\zeta^{p^s}) = p$. По следствию 3 гл. I для промежуточного поля $M = \mathbb{Q}[\zeta^{p^s}]$ расписываем

$$N_{K/\mathbb{Q}}(1-\zeta^{p^s}) = N_{M/\mathbb{Q}}(N_{K/M}(1-\zeta^{p^s})) = N_{M/\mathbb{Q}}(1-\zeta^{p^s})^{[K:M]} = p^{p^s}.$$

По предложению 6 гл. II в K разветвляется только простой идеал (p). □

Теорема 1. Пусть ζ — первообразный корень степени $n>2$ из единицы, $K = \mathbb{Q}[\zeta]$.

а) Тогда $\mathcal{O}_K = \mathbb{Z}[\zeta]$ и поэтому $1, \zeta, \ldots, \zeta^{\varphi(n)-1}$ — целый базис $\mathcal{O}_K$.

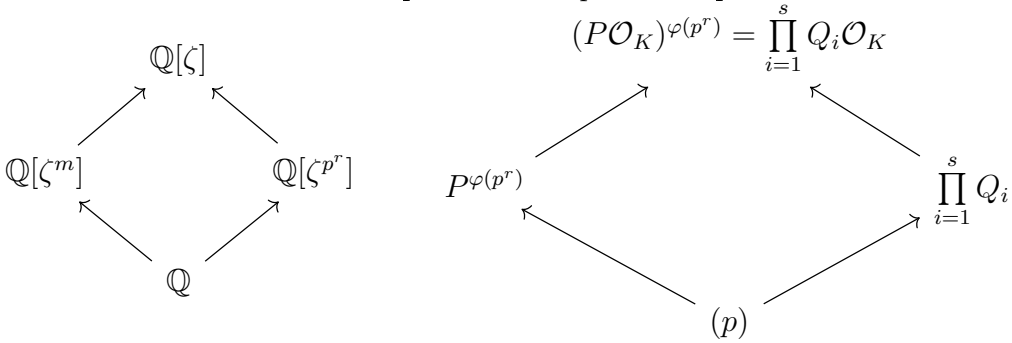
б) Идеал (p) для нечётного простого p разветвляется в $\mathcal{O}_K$ тогда и только тогда, когда $p \mid n$. Идеал (2) разветвляется в $\mathcal{O}_K$ тогда и только тогда, когда $4 \mid n$. Для простого $p \mid n$ выполнено $p\mathcal{O}_K = (R_1 \ldots R_s)^{\varphi(p^r)}$, где $n = p^r m$ и $(p, m) = 1$, а $R_1, \ldots, R_s$ — попарно различные простые идеалы в $\mathcal{O}_K$.

Доказательство. Докажем утверждение индукцией по количеству различных простых делителей n. Если $n = p^r$, где p — простое, то б) следует по лемме 2. Установим, что в этом случае $\mathcal{O}_K = \mathbb{Z}[\zeta]$. По предложению 8 гл. I выполнено $d\mathcal{O}_K \subset \mathbb{Z}[\zeta]$, где $d = D(1, \zeta, \ldots, \zeta^{\varphi(n)-1}) = \pm p^m$ по лемме 2. Тем самым $p^m\mathcal{O}_K \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$. По лемме 1 имеем $[\mathcal{O}_K/(1-\zeta) : \mathbb{Z}_p] = 1$, обозначим $\pi = 1 - \zeta$. Тогда $\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K$ и поэтому $\mathcal{O}_K = \mathbb{Z}[\zeta] + \pi\mathcal{O}_K$. Подставляя это равенство, умноженное на π, получаем

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + \pi\mathcal{O}_K = \mathbb{Z}[\zeta] + (1-\zeta)\mathbb{Z}[\zeta] + \pi^2\mathcal{O}_K = \mathbb{Z}[\zeta] + \pi^2\mathcal{O}_K.$$

Повторяя это рассуждение, получим $\mathcal{O}_K = \mathbb{Z}[\zeta] + \pi^k\mathcal{O}_K$ для любого $k \geq 1$. Берём $k = m\varphi(n)$ и заключаем, что $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

По упр. 2а) семинара №12, если (p) разветвляется в $\mathcal{O}_K$, то $p \mid n$. Пусть $n = p^r m$, где $(p, m) = 1$, $r \geq 1$ и $m > 1$. Поскольку ζ^m — первообразный корень степени p^r, а ζ^{p^r} — первообразный корень степени m, то $\mathbb{Q}[\zeta] = \mathbb{Q}[\zeta^m]\mathbb{Q}[\zeta^{p^r}]$, Запишем башню полей и поясним неизбежный вид разложения $p\mathcal{O}_K$ на простые идеалы:



По лемме 1 имеем $p\mathcal{O}_{\mathbb{Q}[\zeta^m]} = P^{\varphi(p^r)}$, где $P = (1 - \zeta_{p^r})$. Так как p не разветвляется в кольце $\mathcal{O}_{\mathbb{Q}[\zeta^{p^r}]}$, значит, $p\mathcal{O}_{\mathbb{Q}[\zeta^{p^r}]} = Q_1 \ldots Q_s$ для некоторого $s \geq 1$. Поскольку при разложении каждого идеала $Q_i\mathcal{O}_K$ получаем $\varphi(p^r)$-ю степень какого-то идеала, а $[\mathbb{Q}[\zeta_n] : \mathbb{Q}[\zeta^{p^r}]] = \varphi(p^r)$, то из-за фундаментального тождества (теорема 5 гл. II) с необходимостью получаем, что $Q_i\mathcal{O}_K = R_i^{\varphi(p^r)}$, где R_i прост в $\mathcal{O}_K$.

По индукционному предположению $\mathcal{O}_{\mathbb{Q}[\zeta^{p^r}]} = \mathbb{Z}[\zeta^{p^r}]$. Остаётся доказать, что $\mathcal{O}_K = \mathbb{Z}[\zeta^m, \zeta^{p^r}] = \mathbb{Z}[\zeta]$. Это следует из леммы 3 (см. ниже), поскольку $(\mathrm{disc}(\mathcal{O}[\zeta_{p^r}]/\mathbb{Z}), \mathrm{disc}(\mathcal{O}[\zeta_m]/\mathbb{Z})) = 1$ по лемме 2 и упр. 2а) семинара №12. □

Лемма 3. Пусть K и L — конечные расширения $\mathbb{Q}$ и $[KL : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$. Обозначим $d = (\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}), \mathrm{disc}(\mathcal{O}_L/\mathbb{Z}))$. Тогда $\mathcal{O}_{KL} \subseteq \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$.

Доказательство. Пусть $\alpha_1, \ldots, \alpha_m$ и $\beta_1, \ldots, \beta_n$ — целые базисы $\mathcal{O}_K$ и $\mathcal{O}_L$ соответственно. Тогда $\alpha_i\beta_j$ — базис $\mathcal{O}_{KL}$ над $\mathbb{Q}$. Поэтому любой элемент $\gamma \in \mathcal{O}_{KL}$ представим в виде

$$\gamma = \sum_{i,j} \frac{a_{ij}}{r}\alpha_i\beta_j, \quad a_{ij}, r \in \mathbb{Z}. \tag{5.2}$$

При этом считаем, что r не имеет со всем набором a_{ij} общих делителей. Покажем, что d делится на r.

Заметим, что любое вложение $\sigma\colon K \to \mathbb{C}$ единственным образом продолжается до вложения $\sigma\colon KL \to \mathbb{C}$, оставляющего L неподвижным. Действительно, пусть $K = \mathbb{Q}[\alpha]$, тогда $KL = L[\alpha]$. Условие леммы влечёт, что $m_{\mathbb{Q}}^{\alpha}(t) = m_L^{\alpha}(t)$. Значит, найдётся единственный L-гомоморфизм $L[\alpha] \to \mathbb{C}$, отправляющий α в $\sigma(\alpha)$.

Применим σ к (5.2): $\sigma(\gamma) = \sum\limits_i \sigma(\alpha_i)x_i$, где $x_i = \sum\limits_j \frac{a_{ij}}{r}\beta_j$. Для всех различных вложений $\sigma_1, \ldots, \sigma_m$ поля K в $\mathbb{C}$ получаем систему линейных уравнений на x_i:

$$\sum_i \sigma_k(\alpha_i)x_i = \sigma_k(\gamma), \quad k = 1, \ldots, m.$$

По правилу Крамера $x_i = D_i/\det(\sigma_j(\alpha_q))$. Пусть $d_K = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$. Тогда по лемме 8 гл. I выполнено $d_K x_i = D_i \det(\sigma_j(\alpha_q))$. В правой части последнего равенства имеем произведение алгебраических целых чисел, поэтому и $d_K x_i \in \mathbb{A}_\mathbb{Z}$. Поскольку $d_K x_i = \sum\limits_j \frac{d_K a_{ij}}{r}\beta_j$ и $\beta_1, \ldots, \beta_n$ — целый базис $\mathcal{O}_L$, следовательно, $d_K a_{ij}/r \in \mathbb{Z}$. Отсюда $r \mid d_K$.

Аналогично $r \mid d_L$ и $r \mid (d_K, d_L) = d$. □

5.3 Единицы круговых полей

Пусть $n \geq 3$ и ζ — первообразный корень степени n из единицы. Определим поле $\mathbb{Q}[\zeta]^+ = \mathbb{Q}[\zeta + 1/\zeta] \subset \mathbb{R}$. При этом $[\mathbb{Q}[\zeta] : \mathbb{Q}[\zeta]^+] = 2$, так как $m^{\zeta}_{\mathbb{Q}[\zeta]^+}(t) = t^2 - (\zeta + 1/\zeta)t + 1$. Значит, $\mathbb{Q}[\zeta] = \mathbb{Q}[\zeta]^+ + \zeta\mathbb{Q}[\zeta]^+$.

Предложение 1 (Кронекер, 1857). Пусть p — нечётное простое, $n = p^r$, ζ — первообразный корень степени n из единицы, $K = \mathbb{Q}[\zeta]$. Тогда любая единица $u \in \mathcal{O}_K^*$ представима в виде $u = \zeta^m v$ для некоторых $m \in \mathbb{Z}$ и $v \in \mathcal{O}^*_{\mathbb{Q}[\zeta]^+}$.

Доказательство. Обозначим $\alpha = u/\bar{u}$, поскольку $u, \bar{u} \in \mathcal{O}_K^*$, то и $\alpha \in \mathcal{O}_K^*$. Более того, при любом вложении $\sigma\colon \mathbb{Q}[\zeta] \to \mathbb{C}$ выполнено $|\sigma(\alpha)| = 1$. Это следует из того факта, что $\sigma(\bar{x}) = \overline{\sigma(x)}$ для любого $x \in K$. Докажем это утверждение, полагая, что $\sigma(\zeta) = \zeta^k$. Сперва отметим, что σ оставляет подполе $\mathbb{Q}[\zeta]^+$ неподвижным, поскольку $\sigma(\zeta+1/\zeta) = \zeta^k+1/\zeta^k \in \mathbb{Q}[\zeta]^+$. Теперь представим $x = a+\zeta b$ для $a, b \in \mathbb{Q}[\zeta]^+$. С одной стороны, $\sigma(\overline{a + \zeta b}) = \sigma(a) + \sigma(\zeta^{-1})\sigma(b) = \sigma(a) + \zeta^{-k}\sigma(b)$. С другой стороны, $\overline{\sigma(a + \zeta b)} = \sigma(a) + \overline{\sigma(\zeta)}\sigma(b) = \sigma(a) + \zeta^{-k}\sigma(b)$.

Тогда по определению логарифмического вложения $l(x)$ из гл. IV получаем, что $\alpha \in \ker(l) = \mu(K)$. Покажем, что $\mu(K) = \{\pm\zeta^a \mid a = 0, \ldots, n-1\}$. Пусть ζ_q — первообразный корень максимальной степени q, лежащий в $\mu(K)$. Такое q найдётся, поскольку функция $\varphi(n)$ растёт с ростом n. Из равенства $\zeta_q\zeta_n = \zeta_{[q,n]}$ выводим, что $[q, n] = q$, то есть $q = ns$ для некоторого s. Так как $q \geq n$, то $\mathbb{Q}[\zeta_q] = \mathbb{Q}[\zeta_n]$, и поэтому $\varphi(q) = \varphi(ns) = \varphi(n)$. Из свойств функции Эйлера имеем $\varphi(ns) \geq \varphi(n)\varphi(s)$. Значит, $\varphi(s) \leq 1$ и $s = 1$ или $s = 2$. Поскольку n нечётно, то $s = 2$ и $q = 2n$.

Таким образом, $\alpha = \pm\zeta^a$. Покажем, что в точности $\alpha = \zeta^a$. По теореме 1 можем записать $u = b_0 + b_1\zeta + \ldots + b_{\varphi(n)-1}\zeta^{\varphi(n)-1}$, где $b_i \in \mathbb{Z}$. Тогда

$$u \equiv_{(1-\zeta)} b_0 + b_1 + \ldots + b_{\varphi(n)-1} \equiv_{(1-\zeta)} b_0 + b_1 1/\zeta + \ldots + b_{\varphi(n)-1}1/\zeta^{\varphi(n)-1} \equiv_{(1-\zeta)} \bar{u}.$$

Если $\alpha = -\zeta^a$, то $\bar{u} \equiv_{(1-\zeta)} u \equiv_{(1-\zeta)} -\zeta^a\bar{u} \equiv_{(1-\zeta)} -\bar{u}$. Следовательно, $1 - \zeta \mid 2\bar{u}$ в $\mathbb{Z}[\zeta]$, т. е. $(1-\zeta)$ лежит над (2). Получаем противоречие, так как $(1-\zeta) \cap \mathbb{Z} = (p)$, а $p > 2$.

Значит, $\alpha = \zeta^a$. Так как $n = p^r$ нечётно, найдётся $r \in \mathbb{N}$ такое, что $2r \equiv_n a$. Запишем $\zeta = u/\bar{u} = \zeta^{2r}$ или $u = \zeta^{2r}\bar{u}$. Получаем искомое разложение $u = \zeta^r v$, где $v = \zeta^{-r}u$. При этом $\bar{v} = \zeta^r\bar{u} = v$. Пусть $v = a + \zeta b$ для $a, b \in \mathbb{Q}[\zeta]^+$. Тогда условие $\bar{v} = v$ влечёт, что $a + \zeta b = a + b/\zeta$ или $(\zeta^2 - 1)b = 0$. Отсюда $b = 0$ и $v \in \mathbb{Q}[\zeta]^+$. □

5.4 Теорема Ферма

Определение 3. Пусть p — нечётное простое число, ζ — первообразный корень степени p из единицы, $K = \mathbb{Q}[\zeta]$. Число p называется регулярным, если $p \nmid h_K$.

Для простых p выполнено $h_{\mathbb{Q}[\zeta]} = 1$ тогда и только тогда, когда $p \leq 19$.

Гипотеза (Зигель, 1964). Асимптотически доля регулярных простых среди всех простых чисел составляет $1/\sqrt{e} \approx 60,65\%$.

Критерий Куммера гласит, что нечётное простое число p регулярно тогда и только тогда, когда числители всех чисел Бернулли $B_2, B_4, \ldots, B_{p-3}$ не делятся на p. Напомним, что числа Бернулли задаются разложением в ряд $\dfrac{t}{e^t - 1} = \sum\limits_{n=0}^{\infty} B_n \dfrac{t^n}{n!}$.

Докажем теорему Ферма для регулярных простых степеней p в так называемом первом случае, когда p взаимно просто с каждым из искомых чисел x, y и z.

Теорема 2 (Куммер, 1847). Пусть p — регулярное простое число. Тогда не существует целых решений уравнения

$$x^p + y^p = z^p \tag{5.3}$$

таких, что $(p, xyz) = 1$.

Доказательство. При необходимости деля на общий делитель, можем считать, что x, y, z попарно взаимно просты.

Рассмотрим случай $p = 3$. Так как для любого целого числа t выполнено $t^3 \equiv_9 0, \pm 1$, получаем, что $x^3 + y^3 \equiv_9 0, \pm 2$. Отсюда уравнение (5.3) для $p = 3$ не имеет решений, поскольку $(3, z) = 1$ по условию.

Считаем, что $p \geq 5$. Пусть ζ — первообразный корень степени p из единицы, $K = \mathbb{Q}[\zeta]$. Тогда $t^p - 1 = \prod\limits_{i=0}^{p-1}(t - \zeta^i)$, откуда при замене $t = -x/y$ и домножении на $-y^p$ получаем

$$x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta^i y) = z^p. \tag{5.4}$$

Лемма 4. Идеалы $(x + \zeta^i y)$ в $\mathcal{O}_K$ попарно взаимно просты.

Доказательство. Обозначим, как и выше, $P = (1-\zeta)$. Отметим, что $P = (1-\zeta)$ для любого $i = 1, \ldots, p-1$, так как $1 - \zeta^i = u_i(1-\zeta)$ для некоторой единицы $u_i \in \mathcal{O}_K^*$.

Предположим, что Q — простой идеал $\mathcal{O}_K$, делящий $(x + \zeta^i y)$ и $(x + \zeta^j y)$ для $1 \leq i < j \leq p - 1$. Тогда $Q \,|\, ((x + \zeta^i y) - (x + \zeta^j y)) = (\zeta^i y(1 - \zeta^{j-i})) = P(y)$. Значит, $Q \,|\, P$ или $Q \,|\, (y)$. Аналогично $Q \,|\, (\zeta^j(x + \zeta^i y) - \zeta^i(x + \zeta^j y)) = (\zeta^i x(1 - \zeta^{j-i})) = P(x)$ и $Q \,|\, P$ или $Q \,|\, (x)$. Поскольку $(x, y) = 1$, идеалы (x) и (y) взаимно просты. Отсюда $P = Q$. Следовательно, $x + y \equiv x + \zeta^i y \equiv_P 0$. Так как $P \cap \mathbb{Z} = (p)$, выводим, что $p \,|\, x+y$. Тогда по малой теореме Ферма $z \equiv_p z^p = x^p + y^p \equiv_p x + y \equiv_p 0$, противоречие с тем, что $(p, z) = 1$. □

Перед тем, как перейти к следующей лемме, стоит отметить, что в кольце $\mathcal{O}_K$ сравнимость $a \equiv_{p\mathcal{O}_K} b$ значительно сильнее, чем $a \equiv_P b$, поскольку по лемме 1 выполнено $p\mathcal{O}_K = P^{p-1}$. Если выше мы показывали, что для любого элемента $a \in \mathcal{O}_K$ найдётся $b \in \mathbb{Z}$ такой, что $a \equiv_P b$, то по модулю $p\mathcal{O}_K$ это, вообще говоря, не верно. Тем не менее, докажем эту эквивалентность для p-х степеней элементов $\mathcal{O}_K$.

Лемма 5. Для любого $a \in \mathcal{O}_K$ найдётся $b \in \mathbb{Z}$ такой, что $a^p \equiv_{p\mathcal{O}_K} b$.

Доказательство. Пусть $a = b_0 + b_1\zeta + \ldots + b_{p-2}\zeta^{p-2}$, тогда

$$a^p \equiv_{p\mathcal{O}_K} b_0^p + (b_1\zeta)^p + \ldots + (b_{p-2}\zeta^{p-2})^p \equiv_{p\mathcal{O}_K} b_0^p + b_1^p + \ldots + b_{p-2}^p.$$

Здесь воспользовались тем, что $p\mathcal{O}_K = (1-\zeta)^{p-1}$, значит, $0 \equiv_{p\mathcal{O}_K} (1-\zeta)^p \equiv_{p\mathcal{O}_K} 1-\zeta^p$. Остаётся задать $b = b_0^p + b_1^p + \ldots + b_{p-2}^p$. □

Лемма 6. Пусть $a = b_0+b_1\zeta+\ldots+b_{p-1}\zeta^{p-1} \in \mathcal{O}_K$, $b_j \in \mathbb{Z}$ и один из коэффициентов b_i равен 0. Если $a \in n\mathcal{O}_K$ для некоторого целого n, тогда $n \mid b_j$ для всех $j = 0, \ldots, p-1$.

Доказательство. Пусть $b_i = 0$, тогда $1, \zeta, \ldots, \widehat{\zeta^i}, \ldots, \zeta^{p-1}$ — целый базис $\mathcal{O}_K$. Это следует из теоремы 1 и равенства $1 + \zeta + \ldots + \zeta^{p-1} = 0$. Тогда $a = nd$, где $d = \sum\limits_{j=0}^{p-1} c_j\zeta^j$, $c_j \in \mathbb{Z}$ и $c_i = 0$. Из единственности разложения по базису получаем, что $n \mid b_j$. □

Вернёмся к доказательству теоремы 2. По формуле (5.4) имеем $(z)^p = (x+y)(x+\zeta y)\ldots(x+\zeta^{p-1}y)$. В силу леммы 4 и из-за однозначного разложения идеала в $\mathcal{O}_K$ в произведение простых идеалов получаем, что $(x+\zeta^i y) = Q_i^p$, где $Q_i \triangleleft \mathcal{O}_K$. В группе классов $\mathrm{Cl}(\mathcal{O}_K)$ выполнено $\overline{Q_i^p} = \overline{(x+\zeta^i y)} = \bar{1}$. По условию $p \nmid h_K$, значит, $\bar{Q}_i = \bar{1}$, то $Q_i = (\alpha_i)$ для некоторого $\alpha_i \in \mathcal{O}_K$. Обозначим $\alpha := \alpha_1$.

Имеем $x + \zeta y = u\alpha^p$, где $u \in \mathcal{O}_K^*$. По предложению 1 представляем $u = \zeta^r v$ для некоторой единицы $v \in \mathcal{O}_{\mathbb{Q}[\zeta]^+}^*$. По лемме 5 же найдём $b \in \mathbb{Z}$, удовлетворяющее сравнению $\alpha^p \equiv_{p\mathcal{O}_K} b$. Тогда выводим

$$x + \zeta y = u\alpha^p \equiv_{p\mathcal{O}_K} \zeta^r v b, \quad x + y/\zeta = \overline{x+\zeta y} \equiv_{p\mathcal{O}_K} \zeta^{-r} v b,$$

что влечёт равенство $\zeta^{-r}(x+\zeta y) \equiv_{p\mathcal{O}_K} \zeta^r(x+y/\zeta)$. В итоге выписываем соотношение

$$x + \zeta y - \zeta^{2r}x - \zeta^{2r-1}y \equiv_{p\mathcal{O}_K} 0. \tag{5.5}$$

Если $1, \zeta, \zeta^{2r-1}, \zeta^{2r}$ попарно различны, то по лемме 6 p делит и x, и y, что противоречит условию теоремы.

Остаётся три случая:

1) $1 = \zeta^{2r}$. Тогда по (5.5) имеем $\zeta y - \zeta^{2r-1}y \equiv_{p\mathcal{O}_K} 0$. По лемме 6 $p \mid y$, противоречие.

2) $\zeta = \zeta^{2r-1}$. Согласно (5.5) выполнено $x - \zeta^2 x \equiv_{p\mathcal{O}_K} 0$, то есть $p \mid x$, противоречие.

3) $1 = \zeta^{2r-1}$. Тогда $\zeta = \zeta^{2r}$ и (5.5) принимает вид $(x-y)(1-\zeta) \equiv_{p\mathcal{O}_K} 0$. По лемме 6 $p \mid (x-y)$. Покажем, что мы с самого начала доказательства могли считать, что $p \nmid (x-y)$. Предположим, что числа x, y, z удовлетворяют сравнениям $x \equiv_p y \equiv_p -z$, тогда по малой теореме Ферма $x^p + y^p \equiv_p -2z \equiv_p z$. Значит, $p \mid 3z$, противоречие. Если $x \not\equiv_p y$, мы показали требуемое. Если $x \not\equiv_p -z$, тогда совершим замену $y = -z$ и $z = -y$ и опять же получим искомое условие. □

Теперь перейдём ко второму случаю теоремы Ферма, когда $p \mid xyz$. Можем считать, что только одно из чисел x, y, z делится на p. Мы приведём доказательство теоремы Ферма в этом случае, опирающееся на лемму Куммера. Этот важный вспомогательный факт мы приводим без доказательства.

Лемма 7. Пусть $u \in \mathcal{O}_K^*$ и найдётся $b \in \mathbb{Z}$ такой, что $u \equiv_{p\mathcal{O}_K} b$. Тогда $u = v^p$ для некоторой единицы $v \in \mathcal{O}_K^*$.

Теорема 3 (Куммер, 1847). Пусть p — регулярное простое число. Тогда у уравнения (5.3) не существует нетривиальных целых решений.

Доказательство. Поскольку p нечётное, без ограничения общности полагаем, что $p \mid z$, то есть $z = p^k z_0$, где $(p, z_0) = 1$. По лемме 1 $p = u'(1-\zeta)^{p-1}$ для некоторой единицы $u' \in \mathcal{O}_K^*$. Тогда

$$x^p + y^p = u(1-\zeta)^{pm} z_0^p, \tag{5.6}$$

где $m = k(p-1) \geq 1$. Покажем, что соотношение вида (5.6) невозможно ни для каких $x, y, z_0 \in \mathcal{O}_K$ таких, что $(x), (y), (z_0)$ взаимно просты с P, $u \in \mathcal{O}_K^*$ и $m \geq 1$.

Пусть, от противного, нашлись x, y, z_0, u, m, связанные соотношением (5.6) и удовлетворяющие указанным условиям. Среди всех таких наборов выберем такой, что m минимально.

Запишем

$$\prod_{i=0}^{p-1}(x + \zeta^i y) = P^{pm}(z_0)^p. \tag{5.7}$$

Из-за однозначности разложения идеалов в $\mathcal{O}_K$ на простые заключаем, что один из идеалов $(x + \zeta^q y)$ делится на P. Поскольку $x + \zeta^j y \equiv_P x + \zeta^q y$ для любых j, получаем, что все идеалы $(x+\zeta^j y)$ делятся на P. При этом, если $(x+\zeta^i y) \equiv_{P^2} (x+\zeta^j y)$, то $\zeta^i y(1-\zeta^{j-i}) \equiv_{P^2} 0$. Последнее сравнение противоречит тому, что идеалы (y) и P взаимно просты. Отсюда числа $\dfrac{x+\zeta^j y}{1-\zeta}$, $j = 0, \ldots, p-1$, попарно несравнимы по модулю P. По лемме 1 выполнено $\mathbb{N}(P) = |\mathcal{O}_K/P| = p$, следовательно, эти числа задают все фактор-классы $\mathcal{O}_K/P$. В частности, $(x+\zeta^j y)/(1-\zeta) \in P$ для некоторого j. Заменяя y на $\zeta^j y$, можем считать, что $x + y \in P^2$. Таким образом, $x + \zeta^j y \in P \setminus P^2$ для $j = 1, \ldots, p-1$. Более того, левая часть (5.7) делится на P^{p+1}, значит, $m \geq 2$.

Обозначим через J наибольший общий делитель идеалов (x) и (y). Поскольку (x) и (y) взаимно просты с P, то и $P \nmid J$. Отсюда найдутся такие идеалы $Q_0, \ldots, Q_{p-1}$ в $\mathcal{O}_K$, что

$$(x+y) = P^{p(m-1)+1} J Q_0, \quad (x+\zeta^j y) = PJQ_j,\ j = 1, \ldots, p-1.$$

Покажем, что идеалы $Q_0, \ldots, Q_{p-1}$ попарно взаимно просты. Если I делит Q_i и Q_j при $i < j$, то $(x+\zeta^i y)$ и $(x+\zeta^j y)$ делятся на PJI. Тогда $y(1-\zeta^{j-i}), x(1-\zeta^{j-i}) \in PJI$, что влечёт, что $x, y \in JI$. Получено противоречие с выбором идеала J.

Подставляя полученные выражения в (5.7), извлекаем равенство идеалов $J^p P^{pm} Q_0 \ldots Q_{p-1} = P^{pm}(z_0)^p$. Идеалы $Q_0, \ldots, Q_{p-1}$ попарно взаимно просты, поэтому $Q_i = R_i^p$ для некоторых идеалов R_i в $\mathcal{O}_K$. Из представлений $(x+y) = P^{p(m-1)+1} J R_0^p$ и $(x+\zeta^j y) = PJR_j^p$, $j = 1, \ldots, p-1$, выводим равенство дробных идеалов

$$(x+\zeta^j y) P^{p(m-1)} = (x+y)(R_j R_0^{-1})^p, \quad j = 1, \ldots, p-1. \tag{5.8}$$

Значит, идеалы $(R_j R_0^{-1})^p$ являются главными дробными идеалами. Как и выше, в силу $p \nmid h_K$, заключаем, что $R_j/R_0 = (\alpha_j/\beta_j)$ для некоторых $\alpha_j, \beta_j \in \mathcal{O}_K$. Идеалы R_j и R_0 взаимно просты с P, поэтому можем считать, что $\alpha_j, \beta_j \notin P$.

Перепишем (5.8) в виде

$$(x+\zeta^j y)(1-\zeta)^{p(m-1)} = u_j(x+y)(\alpha_j/\beta_j)^p, \quad j = 1, \ldots, p-1, \tag{5.9}$$

где $u_j \in \mathcal{O}_K^*$. Используя равенство $(x+\zeta y)(1+\zeta)-(x+\zeta^2 y) = \zeta(x+y)$, вычитаем (5.9) при $j=2$ из (5.9) при $j=1$, умноженного на $1+\zeta$. Получаем

$$u_1(1+\zeta)(x+y)(\alpha_1/\beta_1)^p - u_2(x+y)(\alpha_2/\beta_2)^p = \zeta(x+y)(1-\zeta)^{p(m-1)}.$$

Следовательно,

$$(\alpha_1\beta_2)^p - \frac{u_2}{u_1(1+\zeta)}(\alpha_2\beta_1)^p = \frac{\zeta}{u_1(1+\zeta)}(1-\zeta)^{p(m-1)}(\beta_1\beta_2)^p.$$

Имеем $1+\zeta = (1-\zeta^2)/(1-\zeta) \in \mathcal{O}_K^*$. Обозначаем $\alpha = \alpha_1\beta_2$, $\beta = \alpha_2\beta_1$ и $\gamma = \beta_1\beta_2$. Тогда последнее равенство переписываем в виде

$$\alpha^p + \varepsilon\beta^p = \varepsilon'(1-\zeta)^{p(m-1)}\gamma^p, \tag{5.10}$$

где $\varepsilon, \varepsilon' \in \mathcal{O}_K^*$, а $\alpha, \beta, \gamma \in \mathcal{O}_K \setminus P$.

Поскольку $m \geq 2$, заключаем, что $p(m-1) \geq p$, отсюда $\alpha^p + \varepsilon\beta^p \equiv_{p\mathcal{O}_K} 0$. Так как (β) и P взаимно просты, то по лемме 3 гл. II найдётся элемент β', удовлетворяющий сравнению $\beta\beta' \equiv_{p\mathcal{O}_K} 1$. Отсюда и по лемме 5 выполнено $\varepsilon \equiv_{p\mathcal{O}_K} (-\alpha\beta')^p \equiv_{p\mathcal{O}_K} c$ для некоторого $c \in \mathbb{Z}$. Применяя лемму 7, получаем, что $\varepsilon = \eta^p$ для некоторой $\eta \in \mathcal{O}_K^*$.

Тогда (5.10) принимает вид $\alpha^p + (\eta\beta)^p = \varepsilon'(1-\zeta)^{p(m-1)}\gamma^p$, совпадающий с (5.6), но уже вовлекающий меньшее значение $m' = m-1 \geq 1$. Противоречие. □

5.5 Уравнение Рамануджана — Нагеля

Числом Мерсенна называется число вида $2^n - 1$, где $n \geq 1$. Найдено много простых чисел Мерсенна вида $2^p - 1$, где p само является простым числом. Эйлер доказал, что произвольное чётное совершенное число (такое n, что сумма всех делителей числа n равна $2n$) имеет вид $2^{p-1}(2^p-1)$, где $2^p - 1$ — простое число Мерсенна.

Рассмотрим следующую задачу: описать все числа Мерсенна, которые одновременно являются треугольными, то есть имеют вид $\frac{y(y+1)}{2}$. Равенство $2^m - 1 = \frac{y(y+1)}{2}$ можно переписать так: $2^{m+3} - 8 = 4y^2 + 4$ или $2^{m+3} - 7 = (2y+1)^2$. Таким образом, мы приходим к диофантову уравнению

$$2^n = x^2 + 7. \tag{5.11}$$

В 1913 году С. Рамануджан выдвинул гипотезу о том, что уравнение (5.11) при $n, x \geq 1$ имеет пять решений: $(n,x) \in \{(3,1),(4,3),(5,5),(7,11),(15,181)\}$.

Теорема 4 (Нагель, 1948). Уравнение (5.11) имеет ровно пять перечисленных выше решений.

Доказательство. Пусть n чётно, то есть $n = 2m$. Тогда $7 = 2^{2m} - x^2 = (2^m - x)(2^m + x)$. Отсюда $7 = 2^m + x$ и $1 = 2^m - x$. Тем самым находим решение $(n,x) = (4,3)$.

Пусть n нечётно. Рассмотрим алгебраическое числовое поле $K = \mathbb{Q}[\sqrt{-7}]$. В кольце целых $\mathcal{O}_K$ разлагаем $2^n = (x+\sqrt{-7})(x-\sqrt{-7})$. Так как 2^n чётно, значит, x нечётно и $\frac{x \pm \sqrt{-7}}{2} \in \mathcal{O}_K$. Обозначим $m = n-2 \geq 1$. Тогда

$$2^m = \left(\frac{1+\sqrt{-7}}{2}\right)^m \left(\frac{1-\sqrt{-7}}{2}\right)^m = \left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right).$$

По задаче 9 семинара №10 кольцо $\mathcal{O}_K$ факториально. Поскольку $N_{K/\mathbb{Q}}(\frac{1\pm\sqrt{-7}}{2}) = 2$, элементы $\frac{1\pm\sqrt{-7}}{2}$ неприводимы и поэтому просты. При этом они взаимно просты, так как их сумма равна 1. Покажем, что $\frac{x\pm\sqrt{-7}}{2}$ взаимно просты. Обозначим $d = (\frac{x+\sqrt{-7}}{2}, \frac{x-\sqrt{-7}}{2})$. Тогда $d \,|\, \sqrt{-7}$. Отсюда $N_{K/\mathbb{Q}}(d)$ делит и 2^m, и 7, значит, $N_{K/\mathbb{Q}}(d) = \pm 1$.

Так как $\mathcal{O}_K^* = \{\pm 1\}$ (задача 2 семинара №11), выполняются равенства

$$\frac{x+\sqrt{-7}}{2} = \pm\left(\frac{1+\varepsilon\sqrt{-7}}{2}\right)^m, \quad \frac{x-\sqrt{-7}}{2} = \pm\left(\frac{1-\varepsilon\sqrt{-7}}{2}\right)^m,$$

где $\varepsilon \in \{\pm 1\}$. При всех вариантах верно, что

$$\left(\frac{1+\sqrt{-7}}{2}\right)^m - \left(\frac{1-\sqrt{-7}}{2}\right)^m = \pm\sqrt{-7}. \tag{5.12}$$

Если $m = 1$, то получаем решение $(n, x) = (3, 1)$.

Пусть $m > 1$. Покажем, что в правой части (5.12) должен быть знак минус. От противного, запишем $a = \frac{1+\sqrt{-7}}{2}$, $b = \frac{1-\sqrt{-7}}{2}$ и $a^m - b^m = a - b$. Выводим

$$a^2 = (1-b)^2 = 1 - 2b + b^2 = 1 - (ab)b + b^2 = 1 + b^2(1-a) \equiv_{b^2\mathcal{O}_K} 1.$$

Значит, $a - b = a^m - b^m \equiv_{b^2\mathcal{O}_K} a$ (m нечётно) и $b \in b^2\mathcal{O}_K$, противоречие.

Остаётся рассмотреть случай $a^m - b^m = b - a$, то есть

$$-\sqrt{-7} = \left(\frac{1+\sqrt{-7}}{2}\right)^m - \left(\frac{1-\sqrt{-7}}{2}\right)^m = \frac{2\sqrt{-7}}{2^m}(C_m^1 + C_m^3(\sqrt{-7})^2 + \ldots + C_m^m(\sqrt{-7})^{m-1}).$$

Отсюда $-2^{m-1} \equiv_7 m$. Так как m нечётно, получаем три варианта: $m \equiv_6 1, 3, 5$. Предыдущее сравнение вместе с тем фактом, что $2^6 \equiv_7 1$, влечёт, что $m \equiv_7 6, 3, 5$ соответственно. Итого $m \equiv_{42} 3, 5, 13$. Для $m = 3, 5, 13$ находим решения $(n, x) = (5, 5), (7, 11), (15, 181)$.

Для завершения доказательства теоремы покажем, что нет двух различных решений, соответствующих $m_1 < m_2$, таких, что $m_1 \equiv_{42} m_2$. Обозначим через $l \geq 1$ максимальную степень 7, которая делит $m_2 - m_1$.

Запишем

$$a^{m_2} = a^{m_1}a^{m_2-m_1} = a^{m_1}\left(\frac{1}{2}\right)^{m_2-m_1}(1+\sqrt{-7})^{m_2-m_1}. \tag{5.13}$$

При этом выполнены сравнения

$$\left(\frac{1}{2}\right)^{m_2-m_1} = \left[\left(\frac{1}{2}\right)^6\right]^{\frac{m_2-m_1}{6}} \equiv_{7^{l+1}} 1, \quad (1+\sqrt{-7})^{m_2-m_1} \equiv_{7^{l+1}} 1 + (m_2-m_1)\sqrt{-7}.$$

Поскольку $a^{m_1} \equiv_7 \frac{1+m_1\sqrt{-7}}{2^{m_1}}$, подстановка трёх выписанных сравнений в (5.13) и их аналогов для b влекут

$$a^{m_2} \equiv_{7^{l+1}} a^{m_1} + \frac{(m_2-m_1)\sqrt{-7}}{2^{m_1}}, \quad b^{m_2} \equiv_{7^{l+1}} b^{m_1} - \frac{(m_2-m_1)\sqrt{-7}}{2^{m_1}}.$$

Числа m_1, m_2 задаются условиями $a^{m_2} - b^{m_2} = a^{m_1} - b^{m_1} = -\sqrt{-7}$, тогда разность предыдущих выражений даёт $(m_2-m_1)\sqrt{-7} \equiv_{7^{l+1}\mathcal{O}_K} 0$ и окончательно $7^{l+1} \,|\, m_2 - m_1$, противоречие с выбором l. $\square$

Предметный указатель