Лекции об алгебраических числах

Ю.В. Нестеренко

настоящий текст представляет собой конспект семестрового специального курса лекций, читающегося на механико-математическом факультете МГУ.

Оглавление

Глава 1

Алгебраические числа

1.1 Конечные и алгебраические расширения полей

Определение 1. *Если E - некоторое поле и F - его подполе, то E называется* расширением *поля F.*

Определение 2. *1. Элемент $\alpha \in E$ называется* алгебраическим над полем F, *если существует многочлен $f(x) \in F[x]$, $f(x) \neq 0$, с условием $f(\alpha) = 0$.*

2. Среди всех таких многочленов выберем многочлен наименьшей степени и со старшим коэффициентом 1. Этот многочлен называется минимальным многочленом *α над F. Его степень называется* степенью *α над F.*

Пример 1. *Пусть $E = \mathbb{C}$, $F = \mathbb{Q}$. Числа $\alpha = 7; i; \sqrt[3]{2}$ алгебраические над полем $\mathbb{Q}$ степеней $1, 2, 3$ соответственно. Их минимальные многочлены равны $x - 7$, $x^2 + 1$ и $x^3 - 2$.*

Минимальный многочлен, очевидно, неприводим над полем F.

Определение 3. *Для любого расширения полей $E \supset F$ и элементов $\alpha_1, \ldots, \alpha_m \in E$ символом $F(\alpha_1, \ldots, \alpha_m)$ будет обозначаться наименьшее подполе E, содержащее как поле F, так и все элементы α_j.*

Поле $F(\alpha_1, \ldots, \alpha_m)$ состоит из всевозможных элементов

$$\frac{A(\alpha_1, \ldots, \alpha_m)}{B(\alpha_1, \ldots, \alpha_m)}, \qquad A, B \in F[x_1, \ldots, x_m], \quad B(\alpha_1, \ldots, \alpha_m) \neq 0.$$

Следующее утверждение описывает структуру расширений, порождаемых одним элементом, так называемых *простых* расширений. Например, $\mathbb{C} = \mathbb{R}(i) \supset \mathbb{R}$ – простое расширение.

Лемма 1. *Пусть $E \supset F$ - расширение полей и элемент $\alpha \in E$ алгебраичен над F, $\deg \alpha = n$. Тогда каждый элемент поля $F(\alpha)$ единственным образом представляется в виде*

$$\alpha = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}, \qquad r_j \in F. \tag{1.1}$$

Другими словами, поле $F(\alpha)$ является n - мерным линейным пространством над F, а элементы $1, \alpha, \ldots, \alpha^{n-1}$ составляют некоторый базис этого линейного пространства.

Доказательство. Пусть $p(x)$ – минимальный многочлен α над F. Согласно определению каждый элемент $\beta \in F(\alpha)$ может быть представлен в виде $\beta = \frac{A(\alpha)}{B(\alpha)}$, где $A(x), B(x) \in F[x]$, причем $B(\beta) \neq 0$. Многочлен $p(x)$ неприводим над F, поэтому возможны два случая. Либо $B(x)$ делится на $p(x)$, либо эти многочлены взаимно просты. Если $p(x)$ – делитель $B(x)$, то каждый корень $p(x)$ и, в частности, α, должен быть корнем многочлена $B(x)$. Но это неверно. Значит многочлены $p(x)$ и $B(x)$ взаимно просты. В этом случае существуют многочлены $u(x), v(x) \in F[x]$, для которых выполняется равенство $u(x)p(x) + v(x)B(x) = 1$. Подставляя в него $x = \alpha$ и пользуясь тем, что $p(\alpha) = 0$, находим $v(\alpha)B(\alpha) = 1$ и, следовательно, $\beta = A(\alpha)v(\alpha)$. Определим теперь многочлены $q(x), r(x) \in F[x]$ условиями

$$A(x)v(x) = q(x)p(x) + r(x), \qquad \deg r(x) < \deg p(x) = n.$$

Подставляя $x = \alpha$ в последнее равенство, находим $\beta = r(\alpha)$, что доказывает (1.1), поскольку многочлен $r(x)$ имеет вид $r(x) = r_0 + r_1 x + \ldots + r_{n-1}x^{n-1}$, $r_j \in F$.

Так как степень α над F равна n, то элементы $1, \alpha, \ldots, \alpha^{n-1}$ линейно независимы над F и, значит, составляют базис линейного пространства $F(\alpha)$ над F. □

В любом расширении $E \supset F$ поле E можно рассматривать как линейное пространство над F.

Определение 4. *Расширение $E \supset F$ называется конечным, если поле E есть конечномерное линейное пространство над F. Размерность этого пространства над F называется степенью расширения и обозначается $[E : F]$.*

Лемма 2. *Пусть $E \supset F, F \supset K$ - конечные расширения полей. Тогда расширение $E \supset K$ конечно, причем*

$$[E : K] = [E : F] \cdot [F : K].$$

Если $x_1, \ldots, x_n$ - базис F над K и $y_1, \ldots, y_m$ - базис E над F, то $x_i y_j$, $1 \le i \le n, 1 \le j \le m$, - базис E над K.

Доказательство. Элементы $x_i y_j$ линейно независимы над K. Действительно, из равенств

$$0 = \sum_{i=1}^{n} \sum_{j=1}^{m} c_{i,j} x_i y_j = \sum_{j=1}^{m} y_j (\sum_{i=1}^{n} c_{i,j} x_i), \qquad c_{i,j} \in K,$$

в силу линейной независимости y_j над F и включений $\sum_{i=1}^{n} c_{i,j} x_i \in F$, находим

$$\sum_{i=1}^{n} c_{i,j} x_i = 0, \qquad j = 1, \ldots, m. \tag{1.2}$$

Учитывая, что x_i линейно независимы над K, получаем из (1.2) равенства $c_{i,j} = 0$. Итак, попарные произведения $x_i y_j$ линейно независимы над полем K.

Элементы y_j составляют базис поля E над F, поэтому любой элемент $\beta \in E$ может быть представлен в виде

$$\beta = d_1 y_1 + \ldots + d_m y_m, \qquad d_j \in F. \tag{1.3}$$

Пользуясь тем, что x_i составляют базис поля F над K находим представление

$$d_j = c_{1,j} x_1 + \ldots + c_{n,j} x_n, \qquad c_{i,j} \in K. \tag{1.4}$$

Из (1.3) и (1.4) получаем равенство

$$\beta = \sum_{i=1}^{n} \sum_{j=1}^{m} c_{i,j} x_i y_j,$$

завершающее доказательство того, что совокупность всех попарных произведений $x_i y_j$ составляет базис линейного пространства E над K. Размерность этого линейного пространства равна $mn = [E : F] \cdot [F : K]$. $\square$

Следствие 1. *Пусть $E \supset F \supset K$ - расширения полей. Расширение $E \supset K$ конечно тогда и только тогда, когда конечны оба расширения $E \supset F$ и $F \supset K$.*

Доказательство. 1. Пусть $E \supset K$ конечное расширение. Любой набор элементов поля E линейно независимых над полем F будет линейно независим и над полем K. Поэтому $[E : F] \le [E : K]$, т.е. расширение $E \supset F$ конечно.

Поле F есть линейное подпространство конечномерного линейного пространства E над K. Поэтому размерность F над K конечна и, значит, $F \supset K$ – конечное расширение.

2. Утверждение в обратную сторону следует из леммы 2. □

Теорема 1. *1. Если $E \supset K$ - конечное расширение, то каждый элемент поля E алгебраичен над K.*

2. Расширение $E \supset K$ конечно тогда и только тогда, когда существуют элементы $\alpha_1, \ldots, \alpha_m \in E$ алгебраические над K такие, что $E = K(\alpha_1, \ldots, \alpha_m)$.

Доказательство. 1. Пусть $\alpha \in E$ и $[E : K] = n$. Тогда элементы

$$1, \alpha, \alpha^2, \ldots, \alpha^n,$$

принадлежащие E, линейно зависимы над K. Соотношение

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0, \qquad a_j \in K,$$

означает, что α есть корень многочлена $f(x) = a_n x^n + \ldots + a_1 x + a_0$, т.е. α алгебраичен над K.

2. а) Если $E \supset K$ конечное расширение, $[E : K] = m$ и $\alpha_1, \ldots, \alpha_m$ – базис E над K, то каждый элемент α поля E представим в виде $\alpha = c_1\alpha_1 + \ldots + c_m\alpha_m$, где $c_j \in K$. Но тогда $\alpha \in K(\alpha_1, \ldots, \alpha_m)$. Последнее включение справедливо для любого элемента $\alpha \in E$, так что $E \subset K(\alpha_1, \ldots, \alpha_m)$. Обратное включение очевидно, поэтому $E = K(\alpha_1, \ldots, \alpha_m)$.

б) Пусть $E = K(\alpha_1, \ldots, \alpha_m)$ и все $\alpha_1, \ldots, \alpha_m$ алгебраичны над K. Докажем утверждение индукцией по m. При $m = 1$ оно следует из леммы 1. Определим $F = K(\alpha_1, \ldots, \alpha_{m-1})$. Согласно индуктивному предположению расширение $F \supset K$ конечно. Элемент α_m алгебраичен над полем K и, следовательно, алгебраичен над полем F. Поскольку $E = F(\alpha_m)$, то по лемме 1 расширение $E \supset F$ конечно. Теперь согласно лемме 2 можно утверждать, что расширение $E \supset K$ конечно. □

Определение 5. *Пусть E, F - подполя поля L, содержащие поле K.* Композитом *E, F (обозначение EF) называется наименьшее подполе L, содержащее поля E и F.*

Поле EF состоит из всевозможных элементов вида

$$\frac{A(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)}{B(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)}, \quad A, B \in K[x_1, \ldots, x_r, y_1, \ldots, y_s], \tag{1.5}$$

где $\alpha_i \in E, \beta_j \in F$ и знаменатель отличен от нуля.

Следствие 2. *Пусть E, F - подполя поля L, содержащие поле K и конечные над ним. Тогда расширение $EF \supset K$ конечно.*

Доказательство. Если $E \supset K$, $F \supset K$ конечны, то согласно теореме 1 существуют элементы $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ алгебраические над K, для которых $E = K(\alpha_1, \ldots, \alpha_m)$ и $F = K(\beta_1, \ldots, \beta_n)$. Но тогда

$$EF = K(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$$

и согласно теореме 1 расширение $EF \supset K$ конечно. □

Определение 6. *Расширение $E \supset F$ называется* алгебраическим*, если каждый элемент поля E алгебраичен над полем F.*

Следствие 3. *Пусть $E \supset F$, $F \supset K$ - алгебраические расширения полей. Тогда расширение $E \supset K$ - алгебраическое.*

Доказательство. Пусть $\alpha \in E$. Так как α алгебраичен над F, то существует многочлен $f(x) = x^n + \beta_{n-1}x^{n-1} + \ldots + \beta_1 x + \beta_0 \in F[x]$ с условием $f(\alpha) = 0$. Поскольку $\beta_j \in F$ и, значит, алгебраичны над K, то по теореме 1 расширение $K(\beta_{n-1}, \ldots, \beta_0) \supset K$ конечно. Расширение

$$K(\alpha, \beta_{n-1}, \ldots, \beta_0) \supset K(\beta_{n-1}, \ldots, \beta_0)$$

конечно по лемме 1, поэтому согласно лемме 2 будет конечным и расширение $K(\alpha, \beta_{n-1}, \ldots, \beta_0) \supset K$. Теперь первое утверждение теоремы 1 дает нам, что α алгебраичен над K. □

Следствие 4. *Пусть E, F - подполя поля L, содержащие поле K и алгебраические над ним. Тогда $EF \supset K$ - алгебраическое расширение.*

Доказательство. Каждый элемент α поля EF может быть представлен в виде (1.5) с некоторыми $\alpha_1, \ldots, \alpha_r \in E$, $\beta_1, \ldots, \beta_s \in F$. Тогда $\alpha \in K(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$. Все элементы α_j, β_j алгебраичны над полем K, поэтому согласно теореме 1 расширение $K(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s) \supset K$ конечно. Из первого утверждения теоремы 1 следует теперь, что α алгебраичен над K. □

Лемма 3. *Пусть K - поле и $f(x)$ - многочлен с коэффициентами из $K, \deg f \geq 1$. Существует расширение $L \supset K$, в котором многочлен $f(x)$ имеет корень.*

Доказательство. Утверждение достаточно доказать для неприводимых многочленов. Пусть $f(x)$ – неприводимый многочлен. В этом случае фактор кольцо $L = K[x]/(f(x))$ является полем. Элемент $x \pmod{f(x)} \in L$ есть корень многочлена $f(x)$. □

Следствие 5. *Для каждого поля K и многочлена $f(x) \in K[x]$ существует расширение $E \supset K$ над которым многочлен $f(x)$ раскладывается на линейные множители, т.е.*

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n), \qquad c \in K, \quad \alpha_j \in E.$$

Определение 7. *$K(\alpha_1, \ldots, \alpha_n)$ - поле разложения многочлена $f(x)$ над полем K.*

Пример 2. *Полем разложения $f(x) = x^3 - 2$ над $\mathbb{Q}$ является поле $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.*

Можно доказать, что поле разложения любого многочлена единственно с точностью до изоморфизма.

1.2 Алгебраические числовые поля

В этом параграфе мы кратко суммируем доказанные выше утверждения для подполей поля комплексных чисел.

Определение 8. *1. Комплексное число α называется* алгебраическим, *если существует многочлен $p(x) \in \mathbb{Q}[x]$, $p(x) \neq 0$, с условием $p(\alpha) = 0$. Среди всех таких многочленов выберем многочлен наименьшей степени и со старшим коэффициентом 1. Такой многочлен определяется по α единственным способом и называется* минимальным многочленом α.

2. Степенью *алгебраического числа α называется степень его минимальноо многочлена, она обозначается* $\deg \alpha$.

3. Числами сопряженными *с α называются все корни минимального многочлена α.*

Минимальный многочлен любого алгебраического числа неприводим и не имеет кратных корней.

Из теоремы 1 следует, что арифметические операции (сложение, вычитание, умножение и деление), примененные к алгебраическим числам, дают алгебраические числа. Иначе говоря, множество всех алгебраических чисел является полем.

Поле называется алгебраически замкнутым, если каждое его алгебраическое расширение тривиально, т.е. совпадает с ним самим. Например, поле всех комплексных чисел алгебраически замкнуто. По следствию 3 корни любого многочлена с алгебраическими коэффициентами являются алгебраическими числами, т.е. поле всех алгебраических чисел алгебраически замкнуто.

Мы будем обозначать поле всех алгебраических чисел символом $\overline{\mathbb{Q}}$.

Определение 9. *Всякое подполе $\mathbb{C}$, являющееся конечным расширением $\mathbb{Q}$, называется* полем алгебраических чисел.

1.3 Теорема о примитивном элементе

Теорема 2. *Всякое поле алгебраических чисел E может быть порождено одним алгебраическим числом. Другими словами, существует такое число $\theta \in E$, что $E = \mathbb{Q}(\theta)$.*

Число θ, порождающее поле E, называется *примитивным элементом E*.

Пример 3. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Доказательство теоремы 2. Согласно определению и теореме 1 всякое поле алгебраических чисел порождается конечным набором алгебраических чисел. Докажем сначала нужное утверждение для поля, порожденного двумя алгебраическими числами, т.е. будем считать, что $E = \mathbb{Q}(\alpha, \beta)$. Пусть степени чисел α, β равны соответственно m и n, а

$$f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0, \qquad g(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0$$

– их минимальные многочлены. Корни этих многочленов, т.е. числа сопряженные с α, β, обозначим $\alpha_1, \ldots, \alpha_m$ и $\beta_1, \ldots, \beta_n$ соответственно. При этом будем считать $\alpha = \alpha_1$, $\beta = \beta_1$. Все числа α_i равно как и числа β_j различны между собой.

Выберем $c \in \mathbb{Q}$ так, чтобы

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1, \qquad (i,k) \neq (1,1). \tag{1.6}$$

Это, очевидно, можно сделать, ведь каждое уравнение $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ при $(i,k) \neq (1,1)$ имеет не более одного решения, а поле $\mathbb{Q}$ бесконечно.

Положим $\theta = \alpha + c\beta$ и обозначим $L = \mathbb{Q}(\theta)$. Справедливо включение $L \subset \mathbb{Q}(\alpha, \beta)$. В дальнейших рассуждениях будет использоваться многочлен

$$h(x) = f(\theta - cx) \in L[x].$$

Принадлежащие кольцу $L[x]$ многочлены $g(x)$ и $h(x)$ имеют общий корень β. Поэтому они имеют нетривиальный общий делитель $d(x) \in L[x]$. Число β является корнем многочлена $d(x)$. Так как $d(x)$ – делитель неприводимого над полем K многочлена $g(x)$, то $d(x)$ не имеет кратных корней.

Предположим, что $\deg d(x) > 1$. Тогда многочлен $d(x)$ имеет корень γ, отличный от β. Все корни $d(x)$ содержатся среди корней многочлена $g(x)$. Поэтому $\gamma = \beta_k$ с некоторым номером $k > 1$. Учитывая, что γ является также корнем многочлена $h(x)$, т.е. $0 = h(\gamma) = f(\theta - c\gamma)$, заключаем, что $\theta - c\gamma = \alpha_i$ с некоторым номером i. Но тогда $\theta = \alpha_i + c\beta_k$ вопреки (1.6).

Получившееся противоречие доказывает, что $\deg d(x) = 1$, т.е. $d(x) = ax + b \in L[x]$. Но тогда $\beta = -b/a \in L$ и $\alpha = \theta - c\beta \in L$. Следовательно, $\mathbb{Q}(\alpha, \beta) = L = \mathbb{Q}(\theta)$, чем и завершается доказательство теоремы 2 для полей, порожденных двумя числами.

Пусть теперь $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$. Если считать теорему доказанной для полей, порожденных $m - 1$ числом, то $\mathbb{Q}(\xi_1, \ldots, \xi_{m-1}) = \mathbb{Q}(\eta)$ для некоторого алгебраического числа η. Так что $E = \mathbb{Q}(\eta, \xi_m)$. Пользуясь уже доказанным утверждением для полей, порожденных двумя числами, заключаем, что с некоторым $\theta \in E$ будет выполняться равенство $E = \mathbb{Q}(\theta)$. □

Примитивный элемент поля может выбираться различными способами. Из доказательства теоремы 2 получаем

Следствие 6. *Примитивный элемент поля $E = \mathbb{Q}(\xi_1, \ldots, \xi_m)$ может быть выбран в виде*

$$\theta = c_1\xi_1 + \ldots + c_m\xi_m, \qquad c_j \in \mathbb{Q}.$$

Этот факт установлен при $m = 2$ в ходе доказательства теоремы 2. В общем случае он легко доказывается индукцией по m.

Следствие 7. *Пусть E - подполе $\mathbb{C}$. Эквивалентны следующие свойства:*

1. *E есть поле алгебраических чисел.*
2. *Расширение $E \supset \mathbb{Q}$ порождается конечным набором алгебраических чисел.*
3. *Расширение $E \supset \mathbb{Q}$ порождается одним алгебраическим числом.*

Теорема 2 справедлива для любого расширения $E \supset K$, которое конечно и обладает некоторым свойством сепарабельности, см. [7], гл. VII. В случае бесконечного поля K все рассуждения сохраняются без изменений. Если же множество элементов поля K конечно, не всегда можно гарантировать выполнение условия (1.6). В этом случае теорема доказывается иным способом. Приведем соответствующие рассуждения.

Если K – конечное поле, то поле E также будет конечным. Обозначим буквой p характеристику полей K и E. Тогда $E \supset K \supset F_p$. Если $n = [E : F_p]$, то поле E содержит p^n элементов. Рассмотрим многочлен

$$g(x) = (x^p - x)(x^{p^2} - x) \cdots (x^{p^{n-1}} - x).$$

Для его степени имеем оценку сверху

$$\deg g(x) = p + p^2 + \ldots + p^{n-1} = \frac{p^n - 1}{p - 1} - 1 < p^n.$$

Отсюда следует, что все элементы поля E не могут быть корнями $g(x)$, и потому найдется элемент $\theta \in E$, для которого $g(\theta) \neq 0$.

Обозначим $d = \deg \theta$ и $L = F_p(\theta) \subset E$. Тогда поле L содержит p^d элементов и мультипликативная группа ненулевых элементов L имеет порядок $p^d - 1$. В частности, это означает равенства $\theta^{p^d-1} = 1$ и $\theta^{p^d} = \theta$. Из определения элемента θ теперь следует неравенство $d \geq n$. Но $d = [L : F_p] \leq [E : F_p] = n$, так что $d = n$ и $E = L = F_p(\theta)$. Включения $E = F_p(\theta) \subset K(\theta) \subset E$ доказывают теперь необходимое равенство $E = K(\theta)$.

Элемент θ с условием $E = K(\theta)$ называется *примитивным элементом поля E над K*.

1.4 Нормальные расширения полей. Группа Галуа

Определение 10. *Пусть F - поле алгебраических чисел. Отображение $\sigma : F \to \mathbb{C}$ называется* вложением, *если оно есть гомоморфизм (сохраняет арифметические операции) и инъективно (образы различных элементов различны). Пусть E - поле алгебраических чисел, содержащее F и $\tau : E \to \mathbb{C}$ - вложение. В случае, если τ на поле F совпадает с σ, говорят, что τ является* продолжением *σ на поле E. Если при этом σ тождественно на F, то говорят, что τ есть* вложение *поля E* над *F.*

Каждое вложение $\sigma : F \to \mathbb{C}$ есть вложение над $\mathbb{Q}$. Это легко проверить, доказав последовательно, что образом 1 под действием σ будет также 1, что натуральные числа остаются неизменными, что остаются неизменными отрицательные числа и 0, наконец, что $\sigma(p/q) = p/q$ для любого рационального числа p/q.

Пример. Пусть $F = \mathbb{Q}(\sqrt{2})$ и отображение σ переводит каждое число $\alpha = a + b\sqrt{2} \in F$, $a, b \in \mathbb{Q}$ в $a - b\sqrt{2}$. Тогда σ есть вложение $\mathbb{Q}(\sqrt{2})$ в $\mathbb{C}$.

Лемма 4. *Пусть E - поле алгебраических чисел и τ - вложение E над F. Тогда для любого $\alpha \in E$ число $\tau(\alpha)$ сопряжено с α над F.*

Говорят, что алгебраические числа α, β сопряжены над полем F, если их минимальные многочлены над F совпадают.

Доказательство. Пусть $p(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_m \in F[x]$ – минимальный многочлен числа α над полем F. Применяя к равенству

$$\alpha^m + a_{m-1}\alpha^{m-1} + \ldots + a_m = p(\alpha) = 0$$

вложение τ и пользуясь тем, что τ тождествен на F и сохраняет арифметические операции, получим

$$\tau(\alpha)^m + a_{m-1}\tau(\alpha)^{m-1} + \ldots + a_m = p(\tau(\alpha)) = 0.$$

Получившееся равенство означает, что число $\tau(\alpha)$ есть корень многочлена $p(x)$, т.е. согласно определению сопряжено с α. □

Пусть F – поле алгебраических чисел и $\sigma : F \to \sigma(F) \subset \mathbb{C}$ - вложение. Для сокращения записи условимся использовать обозначения $\overline{a} = \sigma(a)$ для каждого числа $a \in F$. Для каждого многочлена $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in F[x]$ будем также обозначать $\overline{f}(x) = \overline{a}_n x^n + \ldots + \overline{a}_1 x + \overline{a}_0$.

Лемма 5. *Пусть $E \supset F$ - поля алгебраических чисел, $\sigma : F \to \mathbb{C}$ - вложение. Тогда существует ровно $n = [E : F]$ вложений поля E, продолжающих σ.*

Пусть θ - примитивный элемент поля E над F и $p(x) = a_n x^n + \cdots + a_0 \in F[x]$ - минимальный многочлен θ. Пусть также $\overline{\theta}$ - некоторый корень многочлена $\overline{p}(x)$. Тогда отображение $\tau : E \to \mathbb{C}$, переводящее число

$$\alpha = r_0 + r_1\theta + \cdots + r_{n-1}\theta^{n-1} \in E, \qquad r_i \in F$$

в

$$\tau(\alpha) = \overline{r}_0 + \overline{r}_1\overline{\theta} + \cdots + \overline{r}_{n-1}\overline{\theta}^{n-1} \tag{1.7}$$

есть вложение, продолжающее σ. В частности, $\tau(\theta) = \overline{\theta}$.

Доказательство. Докажем сначала, что отображение, определенное равенством (1.7) есть вложение поля E, продолжающее σ. Тот факт, что ограничение τ на поле F совпадает с σ очевидно следует из определения (1.7). Ведь для чисел $\alpha \in F$ имеем $\tau(\alpha) = \overline{\alpha} = \sigma(\alpha)$.

Докажем, что определенное (1.7) отображение сохраняет сложение и умножение. Пусть $\alpha = a(\theta), \beta = b(\theta)$, где $a(x), b(x) \in F[x]$ и $\deg a(x) <$

n, $\deg b(x) < n$. Тогда согласно (1.7) имеем $\tau(\alpha) = \overline{a}(\overline{\theta})$ и $\tau(\beta) = \overline{b}(\overline{\theta})$. Поскольку $\alpha + \beta = a(\theta) + b(\theta)$ и $\deg(a(x) + b(x)) < n$, то

$$\tau(\alpha + \beta) = \overline{a}(\overline{\theta}) + \overline{b}(\overline{\theta}) = \tau(\alpha) + \tau(\beta).$$

Далее, определим многочлены $u(x), v(x) \in F[x]$ условиями

$$a(x)b(x) = u(x)p(x) + v(x), \qquad \deg v(x) < \deg p(x) = n. \tag{1.8}$$

Из равенства (1.8) следует, что $\alpha\beta = a(\theta)b(\theta) = v(\theta)$. Согласно определению τ теперь находим $\tau(\alpha\beta) = \overline{v}(\overline{\theta})$. Кроме того из (1.8) следует $\overline{v}(x) = \overline{a}(x)\overline{b}(x) - \overline{u}(x)\overline{p}(x)$. Поэтому $\overline{v}(\overline{\theta}) = \overline{a}(\overline{\theta})\overline{b}(\overline{\theta}) = \tau(\alpha)\tau(b)$. Итак, доказаны равенства

$$\tau(\alpha + \beta) = \tau(\alpha) + \tau(\beta), \qquad \tau(\alpha\beta) = \tau(\alpha)\tau(b).$$

Поскольку $\tau(0) = \sigma(0) = 0$, то $0 = \tau(\alpha + (-\alpha)) = \tau(\alpha) + \tau(-\alpha)$. Отсюда находим $\tau(-\alpha) = -\tau(\alpha)$ и $\tau(\beta - \alpha) = \tau(\beta) + \tau(-\alpha) = \tau(\beta) - \tau(\alpha)$. Равенство $\tau(\beta/\alpha) = \tau(\beta)/\tau(\alpha)$ доказывается аналогично, поскольку $\tau(1) = \sigma(1) = 1$.

Итак, отображение τ, определенное (1.7) есть вложение поля E, продолжающее σ с поля F.

Минимальный многочлен $p(x)$ числа θ неприводим над полем F. Поэтому многочлен $\overline{p}(x)$ будет неприводим над полем $\sigma(F)$. В частности, это означает, что он имеет n различных корней $\overline{\theta}_1, \ldots, \overline{\theta}_n$. Следовательно, описанная в условии леммы конструкция позволяет определить n вложений $\tau_1, \ldots, \tau_n$, продолжающих с F на E вложение σ. Все они будут различны, поскольку при $j \neq k$ выполняется $\tau_j(\theta) = \overline{\theta}_j \neq \overline{\theta}_k = \tau_k(\theta)$.

Наконец, докажем, что каждое продолжение вложения σ с поля F на E совпадает с одним из построенных τ_j. Если $\varkappa$ – вложение поля E, продолжающее σ, то из равенства $p(\theta) = 0$ следует $\overline{p}(\varkappa(\theta)) = 0$. Это значит, что число $\varkappa(\theta)$ совпадает с каким-то из корней многочлена $\overline{p}(x)$. Если $\varkappa(\theta) = \overline{\theta}_j$, то для любого элемента $\alpha = a(\theta) \in E$ имеем

$$\varkappa(\alpha) = \overline{a}(\varkappa(\theta)) = \overline{a}(\overline{\theta}_j) = \tau_j(\alpha).$$

Итак, вложение $\varkappa$ совпадает с τ_j. □

Если E – поле алгебраических чисел, содержащее поле F, то каждое вложение E над F является продолжением тождественного вложения поля F. Поэтому согласно лемме 5 можно утверждать, что количество вложений E над F равно степени расширения $E \supset F$, т.е. $[E : F]$.

Каждое вложение поля алгебраических чисел оставляет неподвижными рациональные числа, т.е. является вложением над $\mathbb{Q}$. Следовательно,

количество вложений произвольного алгебраического числового поля E равно степени этого поля, т.е. $[E : \mathbb{Q}]$.

Элементы поля F остаются неподвижными под действием любого вложения поля E над F. Верно и обратное утверждение.

Следствие 8. *Если $E \supset F$ – поля алгебраических чисел, $\alpha \in E$, и для любого вложения τ поля E над F имеем $\tau(\alpha) = \alpha$, то $\alpha \in F$.*

Доказательство. Каждое вложение поля E над F является, согласно условию следствия, вложением над полем $F(\alpha)$, и наоборот, каждое вложение над $F(\alpha)$ будет вложением над F. Поэтому количество вложений E над $F(\alpha)$, т.е. $[E : F(\alpha)]$ равно количеству вложений над F, т.е. $[E : F]$. Это и равенство

$$[E : F] = [E : F(\alpha)] \cdot [F(\alpha) : F],$$

следующее из леммы 2, означают, что $[F(\alpha) : F] = 1$, т.е. $F(\alpha) = F$. Последнее равенство может выполняться лишь в случае $\alpha \in F$. □

Теорема 3. *Пусть $E \supset F$ - поля алгебраических чисел. Эквивалентны следующие утверждения:*

1. Всякое вложение τ поля E над F есть автоморфизм поля E.

2. Для каждого числа $\alpha \in E$ все его сопряженные над F принадлежат E.

3. Всякий неприводимый многочлен $f(x) \in F[x]$, имеющий корень в E, раскладывается над E на линейные множители.

4. Если $E = F(\alpha_1, \ldots, \alpha_m)$, то все сопряженные над F каждого из α_i принадлежат полю E.

Доказательство. 1) $\Rightarrow$ 2) Пусть $\alpha \in E$ и $\overline{\alpha}$ – число, сопряженное с α над полем F. По лемме 5 существует вложение $\sigma : F(\alpha) \to \mathbb{C}$ над F такое, что $\overline{\alpha} = \sigma(\alpha)$. Пусть τ – продолжение σ на E. Тогда τ – автоморфизм поля E над F. Поскольку $\tau(\alpha) = \sigma(\alpha) = \overline{\alpha}$, получаем, что $\overline{\alpha} \in E$.

2) $\Rightarrow$ 3) Пусть $f(x) \in F[x]$ – неприводимый многочлен и $\alpha \in E$ – его корень. Если $p(x) \in F[x]$ – минимальный многочлен α над полем F, то, поскольку $p(x)$ также неприводим над полем F, выполняется равенство $f(x) = c \cdot p(x), c \in F$. Все корни многочлена $p(x)$ согласно условию лежат в поле E. Поэтому и совпадающие с ними корни многочлена $f(x)$ также принадлежат полю E.

3) $\Rightarrow$ 4) Обозначим $p_i(x) \in F[x]$ – минимальный многочлен числа α_i над полем F. Согласно условию все корни этого многочлена, т.е. все числа, сопряженные с α_i над F, принадлежат полю E.

4) $\Rightarrow$ 1) Пусть τ – некоторое вложение поля E над F. По лемме 4 число $\tau(\alpha_i)$ сопряжено с α_i и потому $\tau(\alpha_i) \in E$, $i = 1, \ldots, m$. Каждое

число ξ из поля E может быть представлено в виде $\xi = \frac{A(\alpha_1,\ldots,\alpha_m)}{B(\alpha_1,\ldots,\alpha_m)}$, где $A, B \in F[x_1,\ldots,x_m]$, причем $B(\alpha_1,\ldots,\alpha_m) \neq 0$. Последнее неравенство означает, что

$$B(\tau(\alpha_1),\ldots,\tau(\alpha_m)) = \tau(B(\alpha_1,\ldots,\alpha_m)) \neq 0.$$

Теперь имеем

$$\tau(\xi) = \frac{A(\tau(\alpha_1),\ldots,\tau(\alpha_m))}{B(\tau(\alpha_1),\ldots,\tau(\alpha_m))} \in E.$$

Включение $\tau(\xi) \in E$, выполняющееся для любого числа $\xi \in E$, означает, что $\tau(E) \subset E$.

Отображение τ поля E линейно над F. Поэтому образ $\tau(E) \supset F$ есть линейное подпространство E. Но τ – вложение, и потому имеет нулевое ядро. Это значит, что $\dim_F \tau(E) = \dim_F E$. Следовательно $\tau(E) = E$ и τ есть автоморфизм поля E над F. □

Определение 11. *Расширение $E \supset F$ называется нормальным, если оно удовлетворяет утверждениям теоремы 3. По иному в этом случае говорят: поле E нормально над F.*

Пример 4. *Поле $\mathbb{Q}(\sqrt{2})$ нормально над $\mathbb{Q}$. Поле $\mathbb{Q}(\sqrt[4]{2})$ не нормально, т.к. не содержит число $i\sqrt[4]{2}$, сопряженное с $\sqrt[4]{2}$ над $\mathbb{Q}$.*

Определение 12. *Два поля алгебраических чисел E и F, содержащие поле K, называются* сопряженными *над K, если существует такое вложение $\tau : E \to \mathbb{C}$ над K, что $\tau(E) = F$.*

Следствие 9. *Пусть $E \supset F \supset K$ - поля алгебраических чисел, причем расширение $E \supset K$ нормально. Тогда поле E нормально над F, а все поля, сопряженные с F над K, содержатся в E.*

Доказательство. Каждое вложение σ поля E в $\mathbb{C}$ над F является одновременно и вложением над полем K. Нормальность расширения $E \supset K$ означает, что σ есть автоморфизм поля E. Согласно первому утверждению теоремы 3 можно утверждать, что $E \supset F$ – нормальное расширение.

Согласно определению нормальности, каждое вложение σ поля E над K есть автоморфизм поля E. В частности, это означает равенство $\sigma(E) = E$, из которого следует, что $\sigma(F) \subset E$. □

Определение 13. *Пусть $E \supset K$ - нормальное расширение. Согласно первому утверждению теоремы 3 все вложения поля E над K образуют группу. Эта группа называется* группой Галуа *расширения $E \supset K$, обозначается она $G(E/K)$.*

Если при этом F - промежуточное поле между E и K, то $G(E/F) \subset G(E/K)$.

Теорема 4. *Пусть $E \supset K$ - нормальное расширение. Определенное выше отображение*

$$\phi : F \longrightarrow G(E/F).$$

устанавливает взаимно однозначное соответствие между совокупностью подполей E, содержащих K, и множеством подгрупп $G(E/K)$.

Доказательство. Пусть H – подгруппа группы Галуа $G(E/K)$ и $F = E^H$ – совокупность неподвижных относительно действия H элементов поля E. Очевидно, F есть подполе E. Тогда $H \subset G(E/F)$, и

$$|H| \leq |G(E/F)| = [E : F]. \tag{1.9}$$

Пусть $\alpha \in E$ такое число, что $E = F(\alpha)$. Обозначим

$$f(x) = \prod_{j=1}^{r}(x - \sigma_j(\alpha)),$$

где $\sigma_1, \ldots, \sigma_r$ – все элементы группы H. Для любого элемента $\tau \in H$ множество автоморфизмов $\tau\sigma_1, \ldots, \tau\sigma_r$ есть некоторая перестановка множества $\sigma_1, \ldots, \sigma_r$, ведь H – группа. Поэтому

$$\tau(f)(x) = \prod_{j=1}^{r}(x - \tau\sigma_j(\alpha)) = \prod_{j=1}^{r}(x - \sigma_j(\alpha)) = f(x).$$

Так как это верно для любого $\tau \in H$, то, согласно следствию 8, получаем $f(x) \in F[x]$. И далее, поскольку $f(\alpha) = 0$, находим

$$[E : F] = \deg_F \alpha \leq \deg f(x) = r = |H|. \tag{1.10}$$

Сравнивая (1.9) и (1.10), заключаем, что $|H| = |G(E/F)|$, т.е. $H = G(E/F)$. Таким образом, отображение $F \to G(E/F)$ есть отображение "на".

Предположим теперь, что существует еще одно поле $F_1 \subset E$, для которого выполняется равенство $G(E/F_1) = H$. Тогда любой элемент $\sigma \in H$ оставляет неподвижными все числа из поля F_1, и, значит, согласно определению F имеет место включение $F_1 \subset E^H = F$. Вместе с тем справедливы равенства

$$[E : F_1] = |G(E/F_1)| = |G(E/F)| = [E : F].$$

Согласно лемме 2 можно утверждать, что $[F : F_1] = 1$, т.е. $F_1 = F$. $\square$

Следствие 10. *Для любых двух полей алгебраических чисел $F \supset K$ существует лишь конечное число промежуточных подполей.*

Доказательство. Согласно теореме о примитивном элементе найдется число $\alpha \in F$, порождающее поле F, т.е. $F = K(\alpha)$. Обозначим буквами $\alpha_1, \alpha_2, \ldots \alpha_m$ – все корни минимального многочлена α над полем K, т.е. числа, сопряженные с α над K. Пусть также $E = K(\alpha_1, \ldots, \alpha_m)$. Согласно теореме 3 расширение $E \supset K$ нормально. В силу теоремы 4 существует взаимно однозначное соответствие между подполями E, содержащими поле K, и подгруппами группы $G(E/K)$. Группа $G(E/K)$ конечна, поэтому будет конечной и совокупность ее подмножеств. В частности, совокупность подгрупп $G(E/K)$ конечна. Отсюда следует конечность множества промежуточных подполей между E и K. Но каждое поле, промежуточное между F и K, будет лежать между E и K. Это завершает доказательство следствия. □

Можно доказать, см. [7, гл.8], что в условиях теоремы 4 для любого $\tau \in G(E/K)$ и промежуточного подполя F имеет место равенство $G(E/\tau F) = \tau G(E/F)\tau^{-1}$ и, следовательно, подполям F нормальным над K соответствуют нормальные подгруппы в $G(E/K)$.

1.5 Норма и след в алгебраических расширениях.

Пусть $E \supset K$ - конечное расширение и $\alpha \in E$. Умножение элементов E на α определяет некоторое линейное отображение поля E на себя, $x \to \alpha x$. Если $n = [E : K]$ и $\omega_1, \ldots, \omega_n$ – базис поля E над K, то

$$\alpha\omega_i = \sum_{j=1}^{n} a_{i,j}\omega_j, \qquad a_{i,j} \in K, \tag{1.11}$$

и $A = \|a_{i,j}\|$ – матрица линейного отображения – умножения на α в базисе ω_j.

Определение 14. *След матрицы этого линейного отображения называется* следом α *(обозначение $Tr_K^E(\alpha)$ или $Tr(\alpha)$), а определитель матрицы отображения* - нормой α *(обозначение $N_K^E(\alpha)$ или $N(\alpha)$). Таким образом,*

$$Tr(\alpha) = Tr(A) = a_{1,1} + a_{2,2} + \ldots + a_{n,n}, \qquad N(\alpha) = \det A.$$

Величины $Tr(\alpha)$ и $N(\alpha)$ являются элементами поля K и, как хорошо известно, не зависят от выбора базиса в E.

Лемма 6. *Для любых чисел $\alpha, \beta \in E$ выполняются равенства*
1. $Tr(\alpha+\beta) = Tr(\alpha) + Tr(\beta)$, и $Tr(\lambda\alpha) = \lambda Tr(\alpha)$ при любом $\lambda \in K$.
2. $N(\alpha\beta) = N(\alpha)N(\beta)$.

Доказательство. Аналогично (1.11) имеем

$$\beta\omega_i = \sum_{j=1}^{n} b_{i,j}\omega_j, \qquad b_{i,j} \in K, \tag{1.12}$$

и $B = \|b_{i,j}\|$. Равенства (1.11) и (1.12) могут быть записаны в матричном виде $\alpha\overline{\omega} = A\overline{\omega}$ и $\beta\overline{\omega} = B\overline{\omega}$, где $\overline{\omega}$ – вектор-столбец с элементами $\omega_1, \ldots, \omega_n$. Отсюда следует, что $(\alpha+\beta)\overline{\omega} = (A+B)\overline{\omega}$ и, значит, $A+B$ есть матрица умножения на $\alpha+\beta$. Имеем

$$Tr(\alpha+\beta) = Tr(A+B) = Tr(A) + Tr(B) = Tr(\alpha) + Tr(\beta).$$

Из (1.11) следует $\lambda\alpha\overline{\omega} = \lambda A\overline{\omega}$, причем все элементы матрицы λA принадлежат полю K. Значит, λA есть матрица умножения на $\lambda\alpha$. В соответствии с определением находим

$$Tr(\lambda\alpha) = Tr(\lambda A) = \lambda Tr(A) = \lambda Tr(\alpha).$$

Из (1.11) и (1.12) следует

$$\alpha\beta\overline{\omega} = \alpha B\overline{\omega} = B\alpha\overline{\omega} = BA\overline{\omega}.$$

Это доказывает, что BA есть матрица линейного отображения – умножения на $\alpha\beta$. Теперь имеем

$$N(\alpha\beta) = \det(BA) = \det(B)\cdot\det(A) = N(\beta)N(\alpha).$$

□

Определение 15. *Пусть $\alpha \in E$ и A - матрица, соответствующая умножению на α в некотором базисе. Многочлен $f_\alpha(x) = \det\|x\cdot I - A\|$, где I – единичная $n\times n$ матрица, называется* характеристическим многочленом *числа α.*

Характеристический многочлен не зависит от выбора базиса поля. Если $f_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, то, как легко проверить,

$$Tr(\alpha) = -a_{n-1}, \qquad N(\alpha) = (-1)^n a_0. \tag{1.13}$$

Лемма 7. *Имеет место равенство*

$$f_\alpha(x) = p_\alpha(x)^s,$$

где $p_\alpha(x)$ *- есть минимальный многочлен* α *над* K *и* $s = [E : K(\alpha)]$.

Доказательство. Выберем базис расширения $E \supset K$ некоторым специальным образом. Пусть $\theta_1, \ldots, \theta_s$ – какой-либо базис поля E над $K(\alpha)$ и $m = [K(\alpha) : K] = \deg p_\alpha(x)$. По лемме 2 совокупность чисел $\theta_i\alpha^j$, $1 \le i \le s$, $0 \le j < m$ составляет базис поля E над K. Обозначим буквой A матрицу умножения на α в этом базисе.

Для того, чтобы вычислить A запишем $p_\alpha(x) = x^m + c_{m-1}x^{m-1} + \ldots + c_1x + c_0$ и заметим, что справедливы равенства

$$\alpha \cdot \theta_i = \alpha\theta_i, \quad \alpha \cdot \alpha\theta_i = \alpha^2\theta_i, \ldots, \quad \alpha \cdot \alpha^{m-2}\theta_i = \alpha^{m-1}\theta_i,$$

$$\alpha \cdot \alpha^{m-1}\theta_i = -c_0\theta_i - c_1\alpha\theta_i - \ldots - c_{m-1}\alpha^{m-1}\theta_i.$$

Из них следует, что матрица A распадается на s одинаковых блоков

$$C = \begin{pmatrix} 0 & 1 & \ldots & 0 \\ & & \ddots & \\ 0 & 0 & \ldots & 1 \\ -c_0 & -c_1 & \ldots & -c_{m-1} \end{pmatrix},$$

расположенных на главной диагонали. Таким образом,

$$f_\alpha(x) = (\det \|xI_m - C\|)^s,$$

где I_s – единичная матрица размера $s \times s$.

Прибавляя к первому столбцу матрицы $xI_m - C$ ее второй столбец, умноженный на x, затем третий столбец, умноженный на x^2, и т.д., получаем матрицу с тем же определителем, в левом нижнем углу которой стоит многочлен $p_\alpha(x)$, а остальные элементы первого столбца равны 0. Отсюда следует равенство $\det \|xI_m - C\| = p_\alpha(x)$, завершающее доказательство леммы 7. □

Следствие 11. *Пусть* M *- совокупность всех вложений поля* E *над* K. *Множество чисел* $\sigma(\alpha)$, $\sigma \in M$, *совпадает с множеством корней многочлена* $f_\alpha(x)$. *Справедливы равенства*

$$Tr(\alpha) = \sum_{\sigma \in M} \sigma(\alpha), \qquad N(\alpha) = \prod_{\sigma \in M} \sigma(\alpha). \tag{1.14}$$

Доказательство. Согласно лемме 5 существует ровно m вложений σ_1, $\ldots, \sigma_m$ поля $K(\alpha)$ в поле комплексных чисел над K. При этом числа $\alpha_j = \sigma_j(\alpha)$ составляют множество всех корней минимального многочлена $p_\alpha(x)$. По той же лемме каждое из вложений σ_j допускает ровно s продолжений $\tau_{j,i}$, $1 \le i \le s$, на поле E. Полученные $ms = n$ вложений $\tau_{j,i}$ исчерпывают совокупность всех вложений поля E над K. Таким образом, совокупность образов α при всех вложениях поля E в $\mathbb{C}$ над K состоит из корней многочлена $p_\alpha(x)$, каждый из которых повторяется ровно s раз. Согласно лемме 7 это множество совпадает с совокупностью корней многочлена $f_\alpha(x)$. Равенства (1.14) следуют теперь из (1.13) и формул Виета, связывающих корни многочлена с его коэффициентами. □

Следствие 12. *Если* $p_\alpha(x) = x^m + c_1 x^{m-1} + \cdots + c_m$ *и* $s = [E : K(\alpha)]$, *то*

$$Tr(\alpha) = -s \cdot c_1, \qquad N(\alpha) = (-1)^n c_m^s.$$

Доказательство. Достаточно подставить в равенства (1.13) представления $a_{n-1} = sc_{m-1}$ и $a_0 = c_0^s$, следующие из леммы 7. □

1.6 Дискриминант совокупности чисел и его свойства.

Определение 16. *Пусть* $E \supset K$ *- поля алгебраических чисел,* $[E : K] = n$, *и* $\xi_1 \ldots, \xi_n$ *набор чисел из поля* E. Дискриминантом *этого набора называется определитель* $\Delta(\xi_1, \ldots, \xi_n) = \det \|Tr(\xi_i \xi_j)\|$, $1 \le i, j \le n$.

Лемма 8. *Пусть* $\sigma_1, \ldots, \sigma_n$ *- вложения поля* E *над* K. *Тогда для любых чисел* $\xi_1, \ldots, \xi_n \in E$ *справедливо равенство*

$$\Delta(\xi_1, \ldots, \xi_n) = (\det \|\sigma_i(\xi_j)\|)^2.$$

Эта лемма, в частности, означает, что при любых перестановках чисел ξ_i величина дискриминанта не меняется, и он действительно может быть назван дискриминантом совокупности чисел без указания порядка их следования.

Доказательство. Равенства

$$Tr(\xi_j \xi_k) = \sum_{i=1}^{n} \sigma_i(\xi_j)\sigma_i(\xi_k), \qquad 1 \le i, k \le n,$$

выполняющиеся согласно следствию 11, могут быть переписаны в матричном виде следующим образом

$$Tr(\xi_j\xi_k) = \|\sigma_i(\xi_j)\| \cdot \|\sigma_i(\xi_k)\|^T.$$

Приравнивая определители левой и правой частей, получаем нужное представление для дискриминанта. □

Лемма 9. *Пусть* $\xi_1, \ldots, \xi_n$ *и* $\omega_1, \ldots, \omega_n$ *- два набора чисел из поля* E *и*

$$\xi_i = \sum_{k=1}^{n} c_{i,k}\omega_k, \quad c_{i,k} \in K,\ 1 \le i \le n \tag{1.15}$$

Тогда

$$\Delta(\xi_1, \ldots, \xi_n) = (\det \|c_{i,k}\|)^2 \Delta(\omega_1, \ldots, \omega_n).$$

Доказательство. Из равенств (1.15), пользуясь линейностью следа, находим

$$Tr(\xi_i\xi_j) = \sum_{k=1}^{n}\sum_{\ell=1}^{n} c_{i,k}c_{j,\ell}Tr(\omega_k\omega_\ell).$$

Определив матрицу $C = \|c_{i,j}\|$, найденные равенства можно переписать в матричном виде

$$\|Tr(\xi_i\xi_j)\| = C \cdot \|Tr(\omega_k\omega_\ell)\| \cdot C^T. \tag{1.16}$$

Для завершения доказательства достаточно приравнять определители левой и правой частей (1.16). □

Теорема 5. *Числа* $\omega_1, \ldots, \omega_n \in E$ *образуют базис поля* E *над* K *тогда и только тогда, когда* $\Delta(\omega_1, \ldots, \omega_n) \neq 0$.

Доказательство. Если числа $\omega_1, \ldots, \omega_n$ линейно зависимы над K, то найдутся не все равные нулю $c_i \in K$, для которых выполняется равенство

$$c_1\omega_1 + \ldots + c_n\omega_n = 0.$$

Умножая это равенство на ω_i и вычисляя след, находим

$$0 = Tr(\omega_i \cdot 0) = Tr(\omega_i \sum_{j=1}^{n} c_j\omega_j) = \sum_{j=1}^{n} c_j Tr(\omega_i\omega_j).$$

Получившиеся равенства справедливы при всех $i = 1, \ldots, n$, поэтому столбцы матрицы $\|Tr(\omega_i\omega_j)\|$ линейно зависимы над K, и $\Delta(\omega_1, \ldots, \omega_n) = 0$.

Для того, чтобы доказать утверждение в обратную сторону, заметим, что равенство $\Delta(\omega_1, \ldots, \omega_n) = 0$ означает линейную зависимость столбцов матрицы $\|Tr(\omega_i\omega_j)\|$, т.е. наличие нетривиального набора чисел $c_j \in K$, для которого выполняются равенства

$$\sum_{j=1}^{n} c_j Tr(\omega_i\omega_j) = 0, \qquad i = 1, \ldots, n. \tag{1.17}$$

Обозначив $\alpha = c_1\omega_1 + \ldots + c_n\omega_n$, можно переписать равенства (1.17) в виде

$$Tr(\alpha\omega_i) = 0, \qquad i = 1, \ldots, n.$$

Поскольку числа ω_i образуют базис расширения $E \supset K$, то в случае $\alpha \neq 0$ с некоторыми $d_j \in K$ справедливо представление $\alpha^{-1} = d_1\omega_1 + \ldots + d_n\omega_n$. Поэтому

$$n = Tr(1) = Tr(\alpha\alpha^{-1}) = \sum_{i=1}^{n} d_i Tr(\alpha\omega_i) = 0.$$

Получившееся противоречие означает $\alpha = 0$ и, следовательно, означает линейную зависимость чисел ω_j над K. □

Следствие 13. *Пусть $\omega_1, \ldots, \omega_n$ - базис поля E над K. Тогда для любой совокупности чисел $b_1, \ldots, b_n \in K$ найдется единственное число $\alpha \in E$ с условием $Tr(\alpha\omega_i) = b_i$, $i = 1, \ldots, n$.*

Доказательство. Система линейных уравнений

$$\sum_{j=1}^{n} Tr(\omega_i\omega_j)x_j = b_i, \qquad i = 1, \ldots, n,$$

с коэффициентами из поля K и отличным от нуля, согласно теореме 5, определителем $\Delta(\omega_1, \ldots, \omega_n)$, имеет при любом выборе чисел $b_i \in K$, единственное решение $x_i = c_i$. При этом $c_i \in K$. Обозначив $\alpha = c_1\omega_1 + \ldots + c_n\omega_n$, получаем требуемое число. □

Следствие 14. *Пусть $\omega_1, \ldots, \omega_n$ - базис поля E над K. Существует базис $\omega_1', \ldots, \omega_n'$ поля E с условием*

$$Tr(\omega_i\omega_j') = \begin{cases} 1, \text{ если} & i = j, \\ 0, \text{ если} & i \neq j. \end{cases} \tag{1.18}$$

Доказательство. Число $\omega_j^{'}$ находится с помощью следствия 13, примененного к вектор-столбцу с номером j единичной матрицы размера $n \times n$. Предположим, что найденные числа $\omega_j^{'}$ удовлетворяют соотношению

$$c_1\omega_1^{'} + \ldots + c_n\omega_n^{'} = 0, \qquad c_j \in K.$$

Умножив его на ω_i, пользуясь линейностью следа и равенствами (1.18), находим

$$0 = Tr(\omega_i \sum_{j=1}^{n} c_j\omega_j^{'}) = c_i, \qquad i = 1, \ldots, n.$$

Но это означает линейную независимость чисел $\omega_j^{'}$ над полем K. Таким образом, найденные числа составляют базис поля E над K. □

Два базиса, связанные соотношениями (1.18), называются *взаимными*. Это отношение симметрично. Взаимный базис позволяет выражать коэффициенты представления заданного числа через заданный базис. Так, если $\alpha = \sum_{j=1}^{n} a_j\omega_j$, $a_j \in K$, то $a_j = Tr(\alpha\omega_j^{'})$.

1.7 Модули и порядки.

Далее мы будем использовать без доказательства факты о свободных абелевых группах. Они сведены в следующее утверждение.

Предложение 1. *Пусть G - конечно порожденная абелева группа (аддитивная), не имеющая элементов конечного порядка. Тогда G свободна, т.е существуют такие линейно независимые над $\mathbb{Z}$ элементы $\omega_1, \ldots, \omega_m \in G$ (базис), что $G = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_m$. Количество m элементов в базисе не зависит от выбора базиса. Всякая подгруппа $H \subset G$ конечно порождена и потому свободна. Базис $\eta_1, \ldots, \eta_k$ подгруппы H может быть выбрана так, что*

$$\begin{array}{lllllllll}
\eta_1 & = c_{11}\omega_1 + & c_{12}\omega_2 + \cdots + & c_{1k}\omega_k + \cdots + & c_{1m}\omega_m, \\
\eta_2 & = & c_{22}\omega_2 + \cdots + & c_{2k}\omega_k + \cdots + & c_{2m}\omega_m, \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
\eta_k & = & & c_{km}\omega_k + \cdots + & c_{km}\omega_m,
\end{array}$$

где $c_{i,j} \in \mathbb{Z}$, $c_{i,i} > 0$.

Доказательство. См. [1, гл. 2, п.2] □

Следующее утверждение о дискретных подгруппах в $\mathbb{R}^n$ стоит особняком в настоящем параграфе. Оно понадобится несколько позже при доказательстве теоремы Дирихле о единицах, см. § 1.10. Вместе с тем его доказательство идейно близко к излагаемому здесь материалу.

Определение 17. *Аддитивная подгруппа $G \subset \mathbb{R}^m$ называется* дискретной, *если при любом действительном C она содержит лишь конечное множество элементов x, удовлетворяющих неравенству $|x| \leq C$.*

Лемма 10. *Пусть G дискретная подгруппа $\mathbb{R}^m$. Тогда G свободная абелева группа.*

Доказательство. Пусть $e_1, \ldots, e_k$ – максимальный набор элементов из G, линейно независимых над $\mathbb{R}$. Конечно, выполняется неравенство $k \leq m$. Пусть также

$$H = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_k \subset G$$

– подгруппа, порожденная элементами e_j. Докажем, что индекс $(G : H)$ конечен. Положим для этого

$$C = |e_1| + \ldots + |e_m|,$$

и обозначим $\mathfrak{M}$ совокупность всех элементов η группы G, удовлетворяющих неравенству $|\eta| < C$. Согласно определению совокупности e_j любой элемент $x \in G$ может быть представлен в виде

$$x = \xi_1 e_1 + \ldots + \xi_k e_k, \qquad \xi_j \in \mathbb{R}.$$

Определим целые числа $u_j = [\xi_j]$ и положим $y = u_1 e_1 + \ldots + u_k e_k \in H$. Тогда вектор $x - y = \{\xi_1\}e_1 + \ldots + \{\xi_k\}e_k \in G$ удовлетворяет неравенству $|x - y| \leq C$ и, значит, содержится в множестве $\mathfrak{M}$. Доказанное означает, что каждый смежный класс G по подгруппе H содержит некоторый элемент из конечного множества $\mathfrak{M}$ и потому индекс $N = (G : H)$ конечен.

По теореме Лагранжа, примененной к факторгруппе G/H, для каждого элемента $x \in G$ справедливо включение $Nx \in H$, т.е.

$$G \subset H_1 = \mathbb{Z} \cdot \frac{1}{N} e_1 + \ldots + \mathbb{Z} \cdot \frac{1}{N} e_m.$$

Таким образом, G есть подгруппа свободной группы H_1. Согласно предложению 1 можно утверждать, что группа G свободна. □

Перейдем теперь к изучению основного в этом и последующих параграфах понятия – модулей поля алгебраических чисел.

Определение 18. *Пусть K - поле алгебраических чисел и $\mu_1, \ldots, \mu_m$ - произвольная конечная система чисел из K. Совокупность M всех линейных комбинаций*

$$c_1\mu_1 + \cdots + c_m\mu_m, \qquad c_j \in \mathbb{Z},$$

называется модулем *в поле K. Сами числа $\mu_1, \ldots, \mu_m$ называются* образующими *модуля M. Если μ_i, $1 \le i \le m$ линейно независимы над $\mathbb{Q}$, то эта система образующих называется* базисом *M.*

Лемма 11. *Пусть M - модуль в поле K, тогда M имеет базис, состоящий не более чем из $n = [K : \mathbb{Q}]$ элементов. Всякая аддитивная подгруппа модуля также является модулем.*

Доказательство. Согласно определению модуль M есть конечно порожденная аддитивная группа, а так как он к тому же содержится в поле, то не имеет элементов конечного порядка. Согласно предложению 1 M свободен и, значит, имеет конечный базис. По тому же предложению каждая аддитивная подгруппа M конечно порождена, так что сама является модулем. □

Для каждого модуля M в поле K символом E_M будем обозначать совокупность элементов $\alpha \in K$, для которых $\alpha M \subset M$. Итак,

$$E_M = \{\alpha \in K \,|\, \alpha M \subset M\}.$$

Множество E_M содержит все целые числа и, очевидно, является кольцом. Оно называется *кольцом множителей* модуля M.

Определение 19. *Модуль M в поле K называется* полным, *если он имеет базис, состоящий из $n = [K : \mathbb{Q}]$ элементов.*

Лемма 12. *Кольцо множителей полного модуля само является полным модулем.*

Доказательство. Фиксируем какой-либо ненулевой элемент $\gamma \in M$. Согласно определению кольца множителей имеем включение $\gamma E_M \subset M$, так что $E_M \subset \gamma^{-1}M$. Поскольку множество $\gamma^{-1}M$ является модулем, а E_M – его аддитивная подгруппа, по лемме 11 можно утверждать, что E_M есть модуль.

Пусть $\omega_1, \ldots, \omega_n$ – базис M. Одновременно он является и базисом поля K. Поэтому для любого числа $\alpha \in K$ все произведения $\alpha\omega_i$ могут

быть представлены в виде линейных комбинаций ω_j с рациональными коэффициентами, т.е.

$$\alpha\omega_i = \sum_{j=1}^{n} a_{i,j}\omega_j, \qquad a_{i,j} \in \mathbb{Q}.$$

Пусть d – наименьший общий знаменатель всех коэффициентов $a_{i,j}$. Тогда $da_{i,j} \in \mathbb{Z}$ и, следовательно, $d\alpha\omega_i \in M$, $i = 1, \ldots, n$. По другому это можно записать в виде $d\alpha \in E_M$. Итак, каждое число поля после домножения на некоторое натуральное число может быть помещено в кольцо множителей E_M.

Если применить доказанное свойство к каждому из чисел ω_i, то можно утверждать, что с некоторым натуральным b выполняются включения $b\omega_i \in E_M$. Значит, кольцо множителей E_M содержит n линейно независимых чисел, и потому является полным модулем. □

Определение 20. *Множество $E \subset K$ называется* порядком, *если E - кольцо с 1 и полный модуль.*

Для каждого полного модуля M - множество E_M есть порядок. Для любого порядка E, как легко проверить, выполняется равенство $E_E = E$. Поэтому любой порядок является своим кольцом множителей.

1.8 Целые алгебраические числа. Фундаментальный базис и дискриминант поля.

По существу в этом параграфе мы начинаем изучение арифметики полей алгебраических чисел.

Определение 21. *Многочлен $f(x) \in \mathbb{Z}[x]$ называется* примитивным, *если его коэффициенты в совокупности взаимно просты.*

Лемма 13 (Лемма Гаусса). *Произведение примитивных многочленов является примитивным многочленом.*

Доказательство. Пусть

$$f(x) = a_m x^m + \ldots + a_1 x + a_0, \qquad g(x) = b_\ell x^\ell + \ldots + b_1 x + b_0$$

– какие-либо примитивные многочлены. Их произведение может быть представлено в виде

$$f(x)g(x) = c_{m+\ell} x^{m+\ell} + \ldots + c_1 x + c_0,$$

где

$$c_k = \sum_{i+j=k} a_i b_j, \qquad k = 0, 1, \ldots, m+\ell. \tag{1.19}$$

Предположим, что многочлен $f(x)g(x)$ не примитивен. Тогда его коэффициенты c_k имеют нетривиальный общий делитель, и можно найти простое число p, делящее все коэффициенты c_k.

Коэффициенты многочлена $f(x)$ взаимно просты в совокупности, поэтому не все они делятся на число p. Обозначим буквой u наименьший индекс с условием $p \nmid a_u$. Аналогично обозначим буквой v наименьший индекс с условием $p \nmid b_v$. Выберем также $k = u + v$. Если в сумме (1.19) индекс i удовлетворяет неравенству $i < u$, то $p|a_i$. Точно так же в случае $j < v$ имеет место делимость $p|b_j$. Следовательно, при выбранном значении k имеет место сравнение

$$c_k \equiv a_u b_v \pmod{p}. \tag{1.20}$$

Согласно нашему предположению целое число c_k делится на p, а по определению индексов u и v оба множителя a_u, b_v, стоящие справа, на p не делятся. Но тогда сравнение (1.20) невозможно, ведь p – простое число. Получившееся противоречие завершает доказательство леммы Гаусса. □

Пусть M - произвольный модуль поля K.

Лемма 14. *Если $\alpha \in E_M$, то минимальный многочлен $p_\alpha(x)$ числа α имеет целые коэффициенты. В частности, $N(\alpha)$, $Tr(\alpha) \in \mathbb{Z}$.*

Доказательство. Пусть $\xi_1, \ldots, \xi_m$ – базис модуля M. Если $\alpha \in M$, то с некоторыми целыми коэффициентами $a_{i,j}$ справедливы равенства

$$\alpha\omega_i = \sum_{j=1}^{n} a_{i,j}\omega_j, \qquad a_{i,j} \in \mathbb{Z}, \quad i = 1, \ldots, m. \tag{1.21}$$

Если обозначить $f(x) = \det \|xI_m - A\|$, где $A = \|a_{i,j}\|$, а I_m – единичная $m \times m$ матрица, то $f(x) \in \mathbb{Z}[x]$ и согласно равенствам (1.21) выполняется $f(\alpha) = 0$. Но тогда многочлен $f(x)$ делится на минимальный многочлен $p_\alpha(x)$ числа α, т.е. $f(x) = p_\alpha(x)g(x)$.

Старшие коэффициенты многочленов $f(x), p_\alpha(x)$ равны 1, поэтому и старший коэффициент $g(x)$ также равен 1. Пусть d - наименьший общий знаменатель коэффициентов многочлена $p_\alpha(x)$. Так как его старший коэффициент равен 1, то справедливо представление $p_\alpha(x) = \frac{1}{d}q(x)$, где

$q(x) \in \mathbb{Z}[x]$ – примитивный многочлен. Аналогично имеет место представление $g(x) = \frac{1}{c}h(x)$, где c – общий знаменатель коэффициентов многочлена $g(x)$ и $h(x)$ – примитивный многочлен. Со вновь введенными обозначениями имеем равенство $dc \cdot f(x) = q(x)h(x)$. Многочлен $q(x)h(x)$ примитивен согласно лемме Гаусса, а многочлен $f(x)$ по своему определению имеет целые коэффициенты. Поэтому $dc = 1$ и $d = 1$. Но тогда $p_\alpha(x) = q(x) \in \mathbb{Z}[x]$.

Теперь согласно следствию 12 можно утверждать, что $Tr(\alpha) = sc_1$ и $N(\alpha) = (-1)^n c_m^s$ есть целые числа. □

Определение 22. *Алгебраическое число $\alpha \in \mathbb{C}$ называется* целым алгебраическим, *если $p_\alpha(x) \in \mathbb{Z}[x]$. Для любого поля алгебраических чисел K символом $\mathbb{Z}_K$ будет обозначаться подмножество K, состоящее из целых алгебраических чисел.*

Из этого определения и леммы 14 следует, что элементы любого кольца множителей являются целыми алгебраическими числами, т.е. для любого модуля M имеет место включение $E_M \subset \mathbb{Z}_K$.

Кроме того, ясно, что каждое рациональное и одновременно целое алгебраическое число будет обычным целым числом, т.е. будет принадлежать $\mathbb{Z}$.

Теорема 6. *Множество $\mathbb{Z}_K$ есть порядок. Для каждого модуля $M \subset K$ имеем $E_M \subset \mathbb{Z}_K$, т.е. $\mathbb{Z}_K$ есть максимальный порядок в поле K.*

Доказательство. В силу сказанного выше достаточно доказать лишь, что $\mathbb{Z}_K$ есть порядок. Установим сначала, что $\mathbb{Z}_K$ – кольцо. Пусть $\alpha, \beta \in \mathbb{Z}_K$, $r = \deg \alpha$ и $s = \deg \beta$. Рассмотрим модуль M с системой образующих

$$\alpha^i \beta^j, \quad 0 \le i < r, \quad 0 \le j < s$$

Так как минимальный многочлен $p_\alpha(x)$ имеют целые коэффициенты, то $\alpha \in E_M$. Чтобы доказать это запишем $p_\alpha(x) = x^r + a_{r-1}x^{r-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. При $i < r - 1$ произведение $\alpha \cdot \alpha^i \beta^j = \alpha^{i+1}\beta^j$ есть один из образующих элементов модуля M. Если же $i = r - 1$, находим

$$\alpha \cdot \alpha^{r-1}\beta^j = \alpha^r \beta^j = -a_0\beta^j - a_1\alpha\beta^j - \cdots - a_{r-1}\alpha^{r-1}\beta^j \in M,$$

так что и число $\alpha \cdot \alpha^{r-1}\beta^j$ лежит в модуле M. Но проверенные выше включения означают, что $\alpha \in E_M$. Аналогично доказывается включение $\beta \in E_M$.

Поскольку E_M есть кольцо, имеем включения $\alpha \pm \beta, \alpha\beta \in E_M$. А так как $E_M \subset \mathbb{Z}_K$, заключаем, что $\alpha \pm \beta, \alpha\beta \in \mathbb{Z}_K$. Эти включения

доказывают, что $\mathbb{Z}_K$ есть кольцо. Согласно определению $1 \in \mathbb{Z}_K$, так что $\mathbb{Z}_K$ есть кольцо с единицей.

Выберем какой-нибудь полный модуль T. Согласно лемме 12 кольцо множителей E_T есть полный модуль, т.е. имеет базис, состоящий из $n = [K : \mathbb{Q}]$ элементов. Пусть $E_T = \{\omega_1, \ldots, \omega_n\}$. Обозначим $\omega_1', \ldots, \omega_n'$ взаимный к $\{\omega_j\}$ базис поля K. Пусть $\alpha \in \mathbb{Z}_K$. Так как числа ω_j' составляют базис поля K, то с некоторыми рациональными c_j имеет место равенство

$$\alpha = c_1\omega_1' + \ldots + c_n\omega_n'.$$

Умножая это равенство на число ω_i и вычисляя след, находим

$$Tr(\omega_i\alpha) = \sum_{j=1}^{n} c_j Tr(\omega_i\omega_j') = c_i.$$

Так как $\alpha \in \mathbb{Z}_K$ и $\omega_i \in E_T \subset \mathbb{Z}_K$, а также, поскольку $\mathbb{Z}_K$, как уже доказано, является кольцом, заключаем, что $\omega_i\alpha \in \mathbb{Z}_K$. Согласно лемме 14 можно утверждать, что $c_i = Tr(\omega_i\alpha) \in \mathbb{Z}$. Так как последнее включение имеет место при любом $i = 1, \ldots, n$, то $\alpha \in \mathbb{Z}\omega_1' + \ldots + \mathbb{Z}\omega_1'$. Это доказывает включение

$$\mathbb{Z}_K \subset \{\omega_1', \ldots, \omega_n'\}.$$

В силу леммы 11 можно сделать заключение, что $\mathbb{Z}_K$ есть модуль. Поскольку E_T есть полный модуль и $E_T \subset \mathbb{Z}_K$, получаем, что $\mathbb{Z}_K$ есть полный модуль. Это завершает доказательство теоремы. □

Из теоремы 6 следует, что кольцо $\mathbb{Z}_K$ может быть представлено в виде

$$\mathbb{Z}_K = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n,$$

где числа $\omega_j \in K$ линейно независимы над $\mathbb{Q}$.

Определение 23. *Кольцо $\mathbb{Z}_K$ называется* кольцом целых алгебраических чисел *поля K. Любой базис ω_j кольца $\mathbb{Z}_K$ называется* фундаментальным базисом *поля K.*

Определение 24. *Если $\xi_1, \ldots, \xi_n$ - базис полного модуля M, то величина $D_M = \Delta(\xi_1, \ldots, \xi_n)$ называется* дискриминантом модуля M. *Дискриминант кольца целых чисел $\mathbb{Z}_K$ поля K называется* дискриминантом поля K. *Он будет обозначаться D_K.*

Любые два базиса произвольного полного модуля M связаны линейным преобразованием, матрица которого $\|c_{i,j}\|$ имеет целые элементы и обратима над кольцом целых чисел. Другими словами $\det\|c_{i,j}\| = \pm 1$. В силу леммы 9 можно утверждать, что дискриминант полного модуля не зависит от выбора в нем базиса.

Если $E = \{\xi_1, \ldots, \xi_n\}$ - порядок, то все попарные произведения $\xi_i\xi_j$ принадлежат $E \subset \mathbb{Z}_K$, т.е. являются целыми алгебраическими числами. Так что в силу леммы 14 дискриминант D_E есть целое число. В частности, $D_K \in \mathbb{Z}$.

Кроме того, из включения $E \subset \mathbb{Z}_K$ следует, что любой элемент базиса E выражается в виде линейной комбинации элементов фундаментального базиса с целыми коэффициентами. Согласно лемме 9 можно заключить, что дискриминант D_E делится в кольце целых чисел на дискриминант D_K поля K.

1.9 Теорема Минковского о выпуклом теле.

В дальнейшем будет использоваться понятие n–мерного объема множеств (мера Жордана).

Теорема 7 (Блихфельд). *Пусть $\mathfrak{L}$ - подмножество $\mathbb{R}^n$ с объемом $V(\mathfrak{L})$ (может быть и бесконечным). Предположим, что либо $V(\mathfrak{L}) > 1$, либо $V(\mathfrak{L}) = 1$ и $\mathfrak{L}$ компактно. Тогда в $\mathfrak{L}$ найдутся две различные точки $\overline{x}_1, \overline{x}_2$ с условием $\overline{x}_1 - \overline{x}_2 \in \mathbb{Z}^n$.*

Доказательство. Для каждого вектора $\overline{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n$ определим множество

$$C(\overline{u}) = \{\overline{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n \,|\, u_j \le x_j < u_j + 1\}.$$

Эти множества, очевидно, не пересекаются и объединение их по всем векторам $\overline{u} \in \mathbb{Z}$ составляет все пространство $\mathbb{R}^n$. Поэтому справедливы равенства

$$\mathfrak{L} = \cup_{\overline{u}}(\mathfrak{L} \cap C(\overline{u})), \qquad V(\mathfrak{L}) = \sum_{\overline{u}} V(\mathfrak{L} \cap C(\overline{u})).$$

Заметим, что если $V(\mathfrak{L}) = \infty$, то последний ряд расходится.

Обозначим для краткости буквой C единичный куб, соответствующий нулевому вектору, и

$$\mathfrak{L}(\overline{u}) = (\mathfrak{L} \cap C(\overline{u})) - \overline{u} = C \cap (\mathfrak{L} - \overline{u}). \tag{1.22}$$

Тогда $V(\mathfrak{L}(\overline{u})) = V(\mathfrak{L} \cap C(\overline{u}))$ и

$$V(\mathfrak{L}) = \sum_{\overline{u}} V(\mathfrak{L}(\overline{u})). \tag{1.23}$$

Рассмотрим сначала случай $V(\mathfrak{L}) > 1$. Согласно (1.22) все множества $\mathfrak{L}(\overline{u})$ расположены в единичном кубе C. Но сумма их объемов, согласно (1.23) превосходит объем C, равный 1. Следовательно, существуют два различных вектора $\overline{u}_1, \overline{u}_2 \in \mathbb{Z}^n$, для которых $\mathfrak{L}(\overline{u}_1) \cap \mathfrak{L}(\overline{u}_2) \neq \emptyset$. Пусть $\overline{v}_0 \in \mathfrak{L}(\overline{u}_1) \cap \mathfrak{L}(\overline{u}_2)$. Обозначим

$$\overline{x}_1 = \overline{v}_0 + \overline{u}_1 \in \mathfrak{L}, \qquad \overline{x}_2 = \overline{v}_0 + \overline{u}_2 \in \mathfrak{L}.$$

Тогда $\overline{x}_1 - \overline{x}_2 = \overline{u}_1 - \overline{u}_2 \in \mathbb{Z}^n$, причем точки $\overline{x}_1, \overline{x}_2$ различны. Утверждение доказано.

В случае $V(\mathfrak{L}) = 1$ по условию множество $\mathfrak{L}$ компактно, т.е. ограничено и замкнуто. В частности, существует постоянная $B > 0$ такая, что любой вектор $\overline{x} \in \mathfrak{L}$ удовлетворяет неравенству $|\overline{x}| \leq B$. Для каждого натурального k обозначим $\mathfrak{L}_k = (1+1/k)\mathfrak{L}$ – множество, полученное растяжением в $1+1/k$ раз множества $\mathfrak{L}$. Тогда $V(\mathfrak{L}_k) = (1+1/k)^n V(\mathfrak{L}) > 1$. По доказанному существуют различные точки $\overline{x}_k, \overline{\hat{y}}_k \in \mathfrak{L}_k$ с условием $\overline{x}_k - \overline{\hat{y}}_k \in \mathbb{Z}^n$. Так как каждая точка $\overline{x}$ из множества $\mathfrak{L}_k$ удовлетворяет неравенству $|\overline{x}| \leq (1+1/k)B \leq 2B$, то можно выбрать подпоследовательность $k(\ell)$ для которой обе последовательности $\overline{x}_{k(\ell)}, \overline{\hat{y}}_{k(\ell)}$ сходятся, т.е.

$$\overline{x}_{k(\ell)} \to \overline{x}_0, \qquad \overline{\hat{y}}_{k(\ell)} \to \overline{\hat{y}}_0.$$

Включение $(1+1/k)^{-1}\overline{x}_k \in \mathfrak{L}$ в силу замкнутости множества $\mathfrak{L}$ означает, что $\overline{x}_0 \in \mathfrak{L}$. Аналогично имеет место включение $\overline{\hat{y}}_0 \in \mathfrak{L}$. А так как $\overline{x}_{k(\ell)} - \overline{\hat{y}}_{k(\ell)} \in \mathbb{Z}^n$, и последовательность целых чисел, имеющая предел, стабилизируется, то для всех достаточно больших номеров ℓ должно выполняться равенство $\overline{x}_0 - \overline{\hat{y}}_0 = \overline{x}_{k(\ell)} - \overline{\hat{y}}_{k(\ell)} \in \mathbb{Z}^n$. Это завершает доказательство теоремы. □

Теорема 8 (Минковский). *Пусть $\mathfrak{L}$ - симметричное относительно начала координат выпуклое тело с объемом $V(\mathfrak{L})$ (возможно бесконечным). Предположим, что либо $V(\mathfrak{L}) > 2^n$, либо $V(\mathfrak{L}) = 2^n$ и $\mathfrak{L}$ компактно. Тогда $\mathfrak{L}$ содержит по крайней мере одну точку из $\mathbb{Z}^n$, не совпадающую с началом координат.*

Доказательство. Применим к телу $2^{-1}\mathfrak{L}$ теорему Блихфельда. Так как $V(2^{-1}\mathfrak{L}) = 2^{-n}V(\mathfrak{L}) \geq 1$ и тело $2^{-1}\mathfrak{L}$ компактно в случае $V(\mathfrak{L}) = 2^n$, найдутся две различные точки $\overline{x}_1, \overline{x}_2 \in 2^{-1}\mathfrak{L}$ с условием $\overline{v} = \overline{x}_1 - \overline{x}_2 \in$

$\mathbb{Z}^n$. Заметим, что $\overline{v} \neq 0$. Справедливы включения $2\overline{x}_1 \in \mathfrak{L}$, $2\overline{x}_2 \in \mathfrak{L}$. Поскольку $\mathfrak{L}$ центрально симметрично относительно начала координат, имеем $-2\overline{x}_2 \in \mathfrak{L}$. Равенство

$$\overline{v} = \frac{2\overline{x}_1 + (-2\overline{x}_2)}{2}.$$

в силу выпуклости множества $\mathfrak{L}$ означает, что $\overline{v} \in \mathfrak{L}$. □

Применим теорему Минковского к параллелепипеду.

Следствие 15. *Пусть даны n линейных форм*

$$L_p(\overline{x}) = \sum_{q=1}^{n} a_{p,q} x_q, \qquad p = 1, \ldots, n,$$

с такими действительными коэффициентами $a_{p,q}$, что $\Delta = \det \|a_{p,q}\| \neq 0$, и положительные числа $\varkappa_1, \ldots, \varkappa_n$, удовлетворяющие неравенству

$$\varkappa_1 \cdots \varkappa_n \geq |\Delta|.$$

Тогда существует такая отличная от начала координат точка $\overline{x}_0 = (x_1^0, \ldots, x_n^0) \in \mathbb{Z}^n$, что

$$|L_p(\overline{x}_0)| \leq \varkappa_p, \qquad p = 1, \ldots, n.$$

Доказательство. Обозначим

$$\mathfrak{L} = \{\overline{x} \in \mathbb{R}^n \mid \quad |L_p(\overline{x})| \leq \varkappa_p,\, p = 1, \ldots, n\}. \tag{1.24}$$

Для любых точек $\overline{x}_1, \overline{x}_2 \in \mathfrak{L}$ и любого действительного $a, 0 \leq a \leq 1$, выполняются неравенства

$$|L_p(a\overline{x}_1 + (1-a)\overline{x}_2)| \leq a|L_p(\overline{x}_1)| + (1-a)|L_p(\overline{x}_2)| \leq a\varkappa_p + (1-a)\varkappa_p = \varkappa_p.$$

Значит $\mathfrak{L}$ – выпуклое множество. Оно, очевидно, симметрично относительно начала координат, а формулы Крамера, позволяющие выразить x_k в виде линейной комбинации $L_p(\overline{x})$ с постоянными коэффициентами, доказывают ограниченность $\mathfrak{L}$. Множество $\mathfrak{L}$, определенное нестрогими неравенствами (см. (1.24)), очевидно, замкнуто, так что $\mathfrak{L}$ – компакт. Оценим теперь объем множества $\mathfrak{L}$. В следующем далее вычислении кратного интеграла используется переход к новым переменным интегрирования $y_p, p = 1, \ldots, n$, связанным со старыми переменными равенствами $y_p = L_p(\overline{x})$. Имеем

$$V(\mathfrak{L}) = \int_{\mathfrak{L}} dx_1 \cdots dx_n = |\Delta|^{-1} \int_{|y_k| \leq \varkappa_k} dy_1 \cdots dy_n = 2^n |\Delta|^{-1} \varkappa_1 \cdots \varkappa_n \geq 2^n.$$

Применяя теперь к построенному телу $\mathfrak{L}$ теорему Минковского, получаем нужное утверждение. □

Рассмотрим поле алгебраических чисел K степени n. Пусть θ – примитивный элемент K и $\theta_1, \ldots, \theta_n$ – все числа, сопряженные с θ. Одно из них совпадает с θ. Обозначим буквой s количество действительных чисел среди θ_j. Оставшиеся числа разбиваются на пары комплексно сопряженных, количество таких пар обозначим буквой t. Справедливо равенство $n = s+2t$. Будем считать, что нумерация сопряженных выбрана так, что все числа $\theta_1, \ldots, \theta_s$ действительны, а при $j = 1, \ldots, t$ каждое из чисел θ_{s+j} комплексно сопряжено с θ_{s+t+j}. Соответствующим образом перенумеруем и вложения поля K в $\mathbb{C}$. Тогда в силу леммы 5 при $i = 1, \ldots, s$ для каждого $\alpha \in K$ числа $\sigma_i(\alpha)$ действительны, а при $j = 1, \ldots, t$ числа $\sigma_{s+j}(\alpha)$ и $\sigma_{s+t+j}(\alpha)$ комплексно сопряжены.

Следствие 16. *Пусть M – полный модуль поля K с дискриминантом D_M и $\varkappa_1, \ldots, \varkappa_{s+t}$ положительные числа с условием*

$$\varkappa_1 \cdots \varkappa_s \cdot \varkappa_{s+1}^2 \cdots \varkappa_{s+t}^2 \geq \sqrt{|D_M|}.$$

Тогда модуль M содержит число $\alpha \neq 0$, удовлетворяющее неравенствам

$$|\sigma_k(\alpha)| \leq \varkappa_k, \qquad k = 1, \ldots, s+t.$$

Доказательство. Пусть $\xi_1, \ldots, \xi_n$ – базис модуля M. Тогда каждый элемент $\alpha \in M$ представим в виде

$$\alpha = x_1\xi_1 + \cdots + x_n\xi_n, \qquad x_j \in \mathbb{Z}.$$

Определим линейные формы

$$M_j(\overline{x}) = \sum_{k=1}^{n} \sigma_j(\xi_k) \cdot x_k, \qquad j = 1, \ldots, s+t, \tag{1.25}$$

$$M'_j(\overline{x}) = \sum_{k=1}^{n} \overline{\sigma_j(\xi_k)} \cdot x_k, \qquad j = s+1, \ldots, s+t \tag{1.26}$$

с комплексными коэффициентами. Положим также

$$L_j(\overline{x}) = M_j(\overline{x}), \qquad j = 1, \ldots, s,$$

$$L_k(\overline{x}) = \frac{M_k(\overline{x}) + M'_k(\overline{x})}{2}, \quad L'_k(\overline{x}) = \frac{M_k(\overline{x}) - M'_k(\overline{x})}{2i}, \quad k = s+1, \ldots, s+t.$$

Линейные формы $L_k(\overline{x}), L'_k(\overline{x})$ имеют действительные коэффициенты.

Рассмотрим систему неравенств

$$|L_j(\overline{x})| \le \varkappa_j,\ j = 1, \dots, s, \quad |L_k(\overline{x})|,\ |L'_k(\overline{x})| \le \frac{\varkappa_k}{\sqrt{2}}, \quad k = s+1, \dots, s+t. \tag{1.27}$$

Для того, чтобы применить к ней следствие 15, необходимо оценить определитель $\Delta(L)$ системы (1.27). Заметим, что определитель $\Delta(M)$ совокупности линейных форм (1.25), (1.26) согласно лемме 8 удовлетворяет равенству

$$|\Delta(M)| = \sqrt{|D_M|}.$$

Поскольку при каждом $k = s+1, \dots, s+t$ матрица перехода от пары линейных форм $M_k(\overline{x}), M'_k(\overline{x})$ к паре форм $L_k(\overline{x}), L'_k(\overline{x})$ имеет вид

$$\begin{pmatrix} 2^{-1} & 2^{-1} \\ (2i)^{-1} & -(2i)^{-1} \end{pmatrix},$$

а ее определитель есть $i/2$, то получаем $\Delta(L) = \Delta(M) \cdot (i/2)^t$ и

$$|\Delta(L)| = |\Delta(M)| \cdot 2^{-t} = 2^{-t} \cdot \sqrt{|D_M|} \le \varkappa_1 \cdots \varkappa_s \left(\frac{\varkappa_{s+1}}{\sqrt{2}}\right)^2 \cdots \left(\frac{\varkappa_{s+t}}{\sqrt{2}}\right)^2.$$

Согласно следствию 15 существует ненулевой вектор $\overline{u} = (u_1, \dots, u_n) \in \mathbb{Z}^n$, удовлетворяющий неравенствам (1.27). Положим теперь

$$\alpha = u_1\xi_1 + \cdots + u_n\xi_n \in M.$$

При $j = 1, \dots, s$ имеем

$$|\sigma_j(\alpha)| = |M_j(\overline{u})| = |L_j(\overline{u})| \le \varkappa_j.$$

Если же индекс j удовлетворяет неравенствам $s+1 \le j \le s+t$, то

$$|\sigma_j(\alpha)| = |M_j(\overline{u})| = \sqrt{|L_j(\overline{u})|^2 + |L'_j(\overline{u})|^2} \le \varkappa_j.$$

□

1.10 Теорема Дирихле о единицах.

Определение 25. *Пусть K - поле алгебраических чисел и $\mathbb{Z}_K$ - кольцо целых чисел поля K. Число $\varepsilon \in \mathbb{Z}_K$ называется* единицей *кольца $\mathbb{Z}_K$, если и ε^{-1} принадлежит $\mathbb{Z}_K$.*

Единицы образуют мультипликативную группу. Она будет обозначаться буквой Γ. Теорема Дирихле описывает структуру этой группы. Ниже будут использованы обозначения, введенные перед формулировкой следствия 16.

Теорема 9. *В группе* Γ *существуют единицы* $\varepsilon_1, \ldots, \varepsilon_r$, $r = s + t - 1$, *и* $\zeta = e^{2\pi i/m}$ *- некоторый корень из* 1 *такие, что каждая единица* ε *однозначно представляется в виде*

$$\varepsilon = \zeta^k \cdot \varepsilon_1^{k_1} \cdots \varepsilon_r^{k_r}, \tag{1.28}$$

где $k, k_1, \ldots, k_r \in \mathbb{Z}$, *причем* $0 \leq k < m$.

Лемма 15. *Для каждого* $\alpha \in \mathbb{Z}_K$ *существует такое число* $\beta \in \mathbb{Z}_K$, *что* $\alpha\beta = N(\alpha)$.

Доказательство. Пусть $\alpha \in \mathbb{Z}_K$ и $f_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ - характеристический многочлен числа α, см. определение 15. Из равенства (1.13), поскольку $f_\alpha(\alpha) = 0$, следует

$$N(\alpha) = (-1)^n a_0 = (-1)^n(-\alpha^n - a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha) = \alpha\beta,$$

где $\beta = (-1)^{n-1}(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1) \in \mathbb{Z}_K$. □

Следствие 17. *Число* $\varepsilon \in \mathbb{Z}_K$ *будет единицей тогда и только тогда, когда* $N(\varepsilon) = \pm 1$.

Доказательство. Из равенства $\varepsilon\varepsilon^{-1} = 1$ в силу мультипликативности нормы следует $1 = N(1) = N(\varepsilon\varepsilon^{-1}) = N(\varepsilon)N(\varepsilon^{-1})$. Учитывая, что ε - единица, т.е. $\varepsilon, \varepsilon^{-1} \in \mathbb{Z}_K$, имеем $N(\varepsilon), N(\varepsilon^{-1}) \in \mathbb{Z}$. Поэтому $N(\varepsilon) = \pm 1$.

Наоборот, если мы предположим, что $\varepsilon \in \mathbb{Z}_K$ и $N(\varepsilon) = \pm 1$, то согласно лемме 15 с некоторым числом $\beta \in \mathbb{Z}_K$ должно выполняться равенство $\pm 1 = \varepsilon\beta$. Но тогда $\varepsilon^{-1} = \pm\beta \in \mathbb{Z}_K$. Таким образом, ε - единица. □

Определим отображение $\phi : \Gamma \to \mathbb{R}^{s+t}$ следующим образом

$$\phi(\varepsilon) = (\log|\sigma_1(\varepsilon)|, \ldots, \log|\sigma_s(\varepsilon)|, 2\log|\sigma_{s+1}(\varepsilon)|, \ldots, 2\log|\sigma_{s+t}(\varepsilon)|).$$

Из равенства $\sigma_j(\varepsilon_1\varepsilon_2) = \sigma_j(\varepsilon_1) + \sigma_j(\varepsilon_2)$, справедливого при любом j и для любых единиц $\varepsilon_1, \varepsilon_2 \in \Gamma$, следует, что это отображение является гомоморфизмом Γ в аддитивную группу $\mathbb{R}^{s+t}$.

Лемма 16. *Для каждого положительного числа* N *в кольце* $\mathbb{Z}_K$ *существует лишь конечное число элементов* α, *удовлетворяющих неравенствам*

$$|\sigma_j(\alpha)| \leq N, \qquad j = 1, \ldots, n.$$

Доказательство. Из условия следует, что все числа, сопряженные с α, по абсолютной величине не превосходят N. Теперь согласно теореме Виета можно заключить, что все коэффициенты минимального многочлена числа α не превосходят $2^n N^n$. Поскольку $\alpha \in \mathbb{Z}_K$, то этот многочлен имеет целые коэффициенты, и, значит, множество таких многочленов конечно. Отсюда следует конечность множества чисел α, удовлетворяющих условию леммы. □

Следствие 18. *Ядро отображения ϕ конечно. Существует корень из единицы $\zeta = e^{2\pi i/m} \in \Gamma$ такой, что это ядро есть мультипликативная группа, порожденная ζ.*

Доказательство. Ядро ϕ есть совокупность единиц ε, удовлетворяющих равенству $\phi(\varepsilon) = 0$. Для каждой из них имеем

$$|\sigma_j(\varepsilon)| = 1, \qquad 1 \le j \le s+t. \tag{1.29}$$

Учитывая равенство $\overline{\sigma_j(\varepsilon)} = \sigma_{j+t}(\varepsilon)$, заключаем, что все числа, $\sigma_j(\varepsilon), 1 \le j \le n$, по абсолютной величине равны 1. Теперь согласно лемме 16 можно утверждать, что ядро отображения ϕ конечно. Это ядро есть мультипликативная группа. Обозначив ее порядок буквой m, получим, по теореме Лагранжа, что все элементы ядра являются корнями многочлена $x^m - 1$. Число корней этого многочлена в поле K не превосходит m. Отсюда следует, что ядро состоит в точности из корней степени m из 1, то-есть его элементами являются числа $\zeta^k, 0 \le k < m$, где $\zeta = e^{2\pi i/m}$. □

Следствие 19. *Образ Γ при отображении ϕ есть свободная абелева группа ранга не выше $r = s + t - 1$.*

Доказательство. Образ отображения ϕ есть подгруппа в аддитивной группе $\mathbb{R}^{s+t}$. Эта подгруппа дискретна. Действительно, при любом $c > 0$ условие $|\phi(\varepsilon)| \le c$ означает, что $|\sigma_j(\varepsilon)| \le e^c, 1 \le j \le n$. Совокупность чисел из $\mathbb{Z}_K$, удовлетворяющих этим неравенствам, конечна согласно лемме 16. Итак, $\operatorname{Im}\phi$ есть дискретная подгруппа $\mathbb{R}^{s+t}$. В силу леммы 10 можно утверждать, что $\operatorname{Im}\phi$ есть свободная подгруппа $\mathbb{R}^{s+t}$.

Эта подгруппа расположена в плоскости $x_1 + \cdots + x_{s+t} = 0$. Действительно, для каждой единицы ε согласно лемме 15 имеем

$$\sum_{j=1}^{s} \ln|\sigma_j(\varepsilon)| + 2\sum_{j=s+1}^{s+t} \ln|\sigma_j(\varepsilon)| = \ln|N(\varepsilon)| = 0.$$

Поэтому ранг $\operatorname{Im}\phi$ не превосходит $s + t - 1$. □

Далее мы докажем, что ранг подгруппы $\operatorname{Im}\phi$ равен $r = s+t-1$. Для этого будут построены единицы $\eta_1, \ldots, \eta_r$, образы которых при отображении ϕ линейно независимы в $\mathbb{R}^{s+t}$.

Определение 26. *Два числа α и β из кольца $\mathbb{Z}_K$ называются* ассоциированными, *если существует единица $\varepsilon \in \mathbb{Z}_K$ такая, что $\alpha = \varepsilon\beta$.*

Лемма 17. *Среди чисел кольца $\mathbb{Z}_K$ с фиксированной нормой a существует только конечное множество попарно не ассоциированных.*

Доказательство. Пусть $\omega_1, \ldots, \omega_n$ - фундаментальный базис поля K и два числа $\alpha, \beta \in \mathbb{Z}_K$ удовлетворяют условиям

$$\alpha = a_1\omega_1 + \ldots + a_n\omega_n, \qquad \beta = b_1\omega_1 + \ldots + b_n\omega_n, \quad a_j, b_j \in \mathbb{Z},$$
$$a_j \equiv b_j \pmod{a}, \quad N(\alpha) = a, \quad N(\beta) = a.$$

Докажем, что числа α, β ассоциированы. Из заданных условий следует, что $\alpha - \beta = a\eta, \eta \in \mathbb{Z}_K$. Поэтому справедливы равенства

$$\frac{\alpha}{\beta} = 1 + \frac{N(\beta)}{\beta}\eta, \qquad \frac{\beta}{\alpha} = 1 - \frac{N(\alpha)}{\alpha}\eta.$$

Из них в силу леммы 15 находим $\varepsilon = \alpha/\beta, \varepsilon^{-1} = \beta/\alpha \in \mathbb{Z}_K$. Это доказывает ассоциированность α и β.

Количество классов вычетов по модулю a равно $|a|$. Приведенное выше рассуждение доказывает, что количество попарно неассоциированных чисел с нормой a не превосходит $|a|^n$. □

Лемма 18. *Существуют единицы $\eta_1, \ldots, \eta_{s+t}$ такие, что*

$$|\sigma_\ell(\eta_\ell)| > 1, \qquad |\sigma_j(\eta_\ell)| < 1, \quad j \neq \ell$$

при всех j, $\ell = 1, \ldots, s+t$.

Доказательство. Фиксируем некоторый индекс $\ell, 1 \leq \ell \leq s+t$. Покажем, как построить единицу η_ℓ, удовлетворяющую условиям леммы.

Выбрав некоторое целое число $\nu \geq 1$ положим

$$\varkappa_j = (2|D|)^{-\nu}, \quad \text{при всех} \quad j \neq \ell$$

и определи $\varkappa_\ell$ так, чтобы

$$\varkappa_1 \cdots \varkappa_s \varkappa_{s+1}^2 \cdots \varkappa_{s+t}^2 = \sqrt{2|D|},$$

где D - дискриминант поля K. Согласно следствию 16 найдется число $\beta_\nu \in \mathbb{Z}_K$, удовлетворяющее неравенствам

$$|\sigma_i(\beta_\nu)| \le \varkappa_i = (2|D|)^{-\nu}, \qquad i = 1, \dots, s+t. \tag{1.30}$$

Пользуясь теперь тем, что $\beta_\nu \in \mathbb{Z}_K$ и, значит, $|N(\beta_\nu)| \ge 1$, находим при $j \ne \ell$

$$1 \le |N(\beta_\nu)| = \prod_{i=1}^{n} |\sigma_i(\beta_\nu)| \le |\sigma_j(\beta_\nu)| \cdot \frac{\varkappa_1 \cdots \varkappa_s \varkappa_{s+1}^2 \cdots \varkappa_{s+t}^2}{\varkappa_j} =$$

$$|\sigma_j(\beta_\nu)| \cdot \frac{\sqrt{2|D|}}{(2|D|)^{-\nu}}. \tag{1.31}$$

Последнее неравенство получено заменой в произведении всех множителей $|\sigma_i(\beta_\nu)|$ кроме одного, при $i = j$, превосходящими их величинами $\varkappa_i$. Из (1.31) следует, что

$$|\sigma_j(\beta_\nu)| \ge (2|D|)^{-\nu-1/2} \quad \text{при всех} \quad j \ne \ell. \tag{1.32}$$

Каждое число в построенной последовательности $\beta_\nu, \nu = 1, 2, \dots$ удовлетворяет неравенству

$$|N(\beta_\nu)| = \prod_{i=1}^{n} |\sigma_i(\beta_\nu)| \le \varkappa_1 \cdots \varkappa_s \varkappa_{s+1}^2 \cdots \varkappa_{s+t}^2 = \sqrt{2|D|}. \tag{1.33}$$

Здесь при $j > s$ использовалось равенство $|\sigma_j(\beta_\nu)| = |\sigma_{j+t}(\beta_\nu)|$. Неравенство (1.33) означает, что в последовательности чисел $\beta_\nu, \nu \ge 1$, можно выбрать бесконечную подпоследовательность чисел с одинаковой нормой. Согласно же лемме 17 в этой подпоследовательности можно выбрать два ассоциированных числа $\beta_{\nu_1}, \beta_{\nu_2}, \nu_1 < \nu_2$. Положим $\eta_\ell = \beta_{\nu_2}/\beta_{\nu_1}$. Пользуясь теперь неравенствами (1.30) и (1.33), при $j \ne \ell$ находим

$$|\sigma_j(\eta_\ell)| = \frac{|\sigma_j(\beta_{\nu_2})|}{|\sigma_j(\beta_{\nu_1})|} \le \frac{(2|D|)^{-\nu_2}}{(2|D|)^{-\nu_1-1/2}} \le (2|D|)^{-1/2} < 1.$$

Доказанное неравенство справедливо при любом $j \ne \ell$. А из равенства

$$|\sigma_1(\eta_\ell)| \cdots |\sigma_s(\eta_\ell)| \cdot |\sigma_{s+1}(\eta_\ell)|^2 \cdots |\sigma_{s+t}(\eta_\ell)|^2 = |N(\eta_\ell)| = 1,$$

поскольку все сомножители при $j \ne \ell$ меньше 1, находим $|\sigma_\ell(\eta_\ell)| > 1$. $\square$

Лемма 19. *При $r \ge 1$ векторы $\phi(\eta_1), \dots, \phi(\eta_r)$ линейно независимы над $\mathbb{R}$.*

Доказательство. Для краткости записи дальнейших рассуждений положим $u_j = 1$, при $1 \le j \le s$ и $u_j = 2$, при $s < j \le s + t$. Если векторы $\phi(\eta_1), \dots, \phi(\eta_r)$ линейно зависимы над $\mathbb{R}$, то ранг матрицы

$$\| u_j \ln |\sigma_j(\eta_\ell)| \|_{1 \le j \le s+t, 1 \le \ell \le r}$$

меньше r. Это, в частности, означает линейную зависимость первых r столбцов этой матрицы (при $j = 1, \dots, r$), так что с некоторыми действительными числами a_j, не все из которых равны 0 выполняются равенства

$$\sum_{j=1}^{r} a_j u_j \ln |\sigma_j(\eta_\ell)| = 0, \qquad \ell = 1, \dots, r.$$

Не уменьшая общности можно считать, что $a_1 = \max_i a_i > 0$. Тогда при $\ell = 1$ имеем

$$0 = \sum_{j=1}^{r} a_j u_j \ln |\sigma_j(\eta_1)| \ge a_1 \sum_{j=1}^{r} u_j \ln |\sigma_j(\eta_1)| = -a_1 u_{s+t} \ln |\sigma_{s+t}(\eta_1)| > 0.$$

Здесь были использованы неравенства $|\sigma_j(\eta_1)| < 1$, выполняющиеся при $j > 1$. Полученное таким образом противоречие означает линейную независимость векторов $\phi(\eta_\ell)$, $\ell = 1, \dots, r$. □

Доказательство теоремы 9. Из следствия 19 и леммы 19 следует, что $\operatorname{Im}\phi$ есть решетка ранга r. При $r = 0$ выполняется равенство $\Gamma = \operatorname{Ker}\phi$ и справедливость утвержденя теоремы обеспечивается следствием 18.

Далее будем считать $r \ge 1$. Обозначим $\varepsilon_1, \dots, \varepsilon_r$ - единицы группы Γ такие, что векторы $\phi(\varepsilon_1), \dots, \phi(\varepsilon_r)$ образуют базис решетки $\operatorname{Im}\phi$.

Если $\varepsilon \in \Gamma$, то существует набор целых чисел $k_1, \dots, k_r$, для которых выполняется равенство $\phi(\varepsilon) = k_1\phi(\varepsilon_1) + \dots + k_r\phi(\varepsilon_r)$. Тогда для единицы $\eta = \varepsilon \cdot \varepsilon_1^{-k_1} \cdots \varepsilon_r^{-k_r}$ имеем

$$\phi(\eta) = \phi(\varepsilon) - k_1\phi(\varepsilon_1) - \dots - k_r\phi(\varepsilon_r) = 0.$$

Значит, $\eta \in \operatorname{Ker}\phi$ и согласно следствию 18 существует целое число $k, 0 \le k < m$, для которого $\eta = \zeta^k$. Таким образом, выполняется равенство (1.28).

Предположив, что единица ε может быть представлена в виде (1.28) двумя различными способами, находим

$$\varepsilon = \zeta^k \cdot \varepsilon_1^{k_1} \cdots \varepsilon_r^{k_r} = \zeta^\ell \cdot \varepsilon_1^{\ell_1} \cdots \varepsilon_r^{\ell_r}, \qquad 0 \le k, \ell < m. \tag{1.34}$$

Применяя к этим равенствам отображение ϕ, получаем

$$\phi(\varepsilon) = k_1\phi(\varepsilon_1) + \dots + k_r\phi(\varepsilon_r) = \ell_1\phi(\varepsilon_1) + \dots + \ell_r\phi(\varepsilon_r).$$

В силу единственности разложения вектора по базису решетки отсюда следует $k_1 = \ell_1, \ldots, k_r = \ell_r$. Теперь из (1.34) находим $k = \ell$. □

Определение 27. *Единицы $\varepsilon_1, \ldots, \varepsilon_r$, существование которых доказано в теореме Дирихле, называются* основными *единицами порядка $\mathbb{Z}_K$.*

Отметим, что структура группы единиц любого порядка поля K описывается подобно теореме 9.

1.11 Идеалы в кольце $\mathbb{Z}_K$.

В кольцах целых чисел может не выполняться свойство единственности разложения элементов в произведение простых. Так в поле $K = \mathbb{Q}(\sqrt{-23})$ кольцо целых чисел имеет вид $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\omega$, где $\omega = \frac{1+\sqrt{-23}}{2}$. В этом кольце нет единственности разложения на простые множители:

$$3 \cdot 3 \cdot 3 = 27 = (2 + \sqrt{-23}) \cdot (2 - \sqrt{-23}).$$

Легко проверить, что каждое из чисел $3, 2 \pm \sqrt{-23}$ не может быть разложено в произведение необратимых элементов кольца $\mathbb{Z}_K$, т.е. является простым.

Основной результат этого параграфа - теорема 10, утверждающая, что в кольцах $\mathbb{Z}_K$ имеет место единственность разложения идеалов в произведение простых. Часто это свойство используется вместо отсутствующей единственности разложения чисел и служит его эффективной заменой.

Напомним, что *идеал* в кольце $\mathbb{Z}_K$ есть аддитивная подгруппа $\mathbb{Z}_K$, замкнутая относительно умножения на элементы $\mathbb{Z}_K$. Идеал $\mathfrak{p} \subset \mathbb{Z}_K$ называется *простым*, если для любых двух элементов $a, b \in \mathbb{Z}_K$ включение $ab \in \mathfrak{p}$ возможно лишь в случаях $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$.

Каждый идеал $\mathfrak{a} \subset \mathbb{Z}_K$ есть полный модуль с кольцом множителей $\mathbb{Z}_K$. Верно и обратное - каждый полный модуль $M \subset \mathbb{Z}_K$ с кольцом множителей $E_M = \mathbb{Z}_K$ есть идеал в кольце $\mathbb{Z}_K$.

Определение 28. *Дробным идеалом поля K называется полный модуль $M \subset K$, для которого $E_M = \mathbb{Z}_K$.*

Всякий идеал в кольце $\mathbb{Z}_K$ есть дробный идеал. Кольцо $\mathbb{Z}_K$ также является дробным идеалом.

Определение 29. *Пусть M, M_1, M_2 - дробные идеалы поля K. Определим M_1M_2 как множество конечных сумм попарных произведений элементов из M_1 и M_2, т.е.*

$$M_1 \cdot M_2 = \left\{ \sum_i \alpha_i \cdot \beta_i \,; \quad \alpha_i \in M_1,\, \beta_i \in M_2 \right\}.$$

Определим также

$$M^{-1} = \{\alpha \in K \,; \quad \alpha \cdot M \subset \mathbb{Z}_K\}\,.$$

Далее будет доказано, что так определенные множества являются дробными идеалами, и относительно введенной операции умножения совокупность всех дробных идеалов есть абелева группа.

Лемма 20. *1. В условиях определения 29 множества M_1M_2 и M^{-1} есть дробные идеалы.*

2. Операция умножения ассоциативна и коммутативна.

3. $M \cdot M^{-1} \subset \mathbb{Z}_K$.

4. Если $M \subset \mathbb{Z}_K$, то $M^{-1} \supset \mathbb{Z}_K$.

Доказательство. По определению M_1M_2 есть конечно порожденная абелева группа. Действительно, если $\xi_1, \ldots, \xi_n$ и $\eta_1, \ldots, \eta_n$ есть базисы дробных идеалов M_1, M_2 соответственно, то каждый элемент M_1M_2 может быть представлен в виде линейной комбинации чисел $\xi_i\eta_j, i, j = 1, \ldots, n$ с целыми коэффициентами. Значит, M_1M_2 есть модуль, и $\xi_i\eta_j$ – его система образующих. Пусть $\alpha \in \mathbb{Z}_K$. Тогда $\alpha M_1 \subset M_1$, и $\alpha M_1M_2 \subset M_1M_2$. Это значит, что $\mathbb{Z}_K \subset E_{M_1M_2}$. Но тогда M_1M_2 есть полный модуль и согласно теореме 6 можно утверждать, что M_1M_2 есть дробный идеал.

Для каждого ненулевого элемента $\xi \in M$ согласно определению выполняется включение $\xi M^{-1} \subset \mathbb{Z}_K$. Отсюда следует, что M^{-1} есть аддитивная подгруппа модуля $\xi^{-1}\mathbb{Z}_K$ и потому является модулем.

Для каждого элемента $\eta \in M^{-1}$ имеем $\eta M \subset \mathbb{Z}_K$, так что при любом $\alpha \in \mathbb{Z}_K$ справедливо включение $\alpha\eta M \subset \mathbb{Z}_K$ и, значит, $\alpha\eta \in M^{-1}$. Последнее включение выполняется при любом $\eta \in M^{-1}$, так что $\alpha M^{-1} \subset M^{-1}$ и $\mathbb{Z}_K \subset E_{M^{-1}}$. Согласно теореме 6 можно утверждать, что M^{-1} есть дробный идеал.

Ассоциативность умножения следует из того, что для любых трех дробных идеалов M_1, M_2, M_3 с базисами $\{\xi_i\}, \{\eta_j\}, \{\zeta_k\}$ оба дробных идеала $(M_1M_2)M_3$ и $M_1(M_2M_3)$ имеют системой образующих числа

$$\xi_i\eta_j\zeta_k, \qquad i, j, k = 1, \ldots, n.$$

Включение $MM^{-1} \subset \mathbb{Z}_K$ сразу же следует из определения M^{-1}.

Пусть $M \subset \mathbb{Z}_K$. Для любого $\alpha \in \mathbb{Z}_k$ имеем $\alpha M \subset M \subset \mathbb{Z}_K$, так что $\alpha \in M^{-1}$. Это завершает доказательство леммы. □

Теорема 10. *Для каждого идеала $\mathfrak{a} \subset \mathbb{Z}_K$ существует единственным образом определенные совокупности простых идеалов $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset \mathbb{Z}_K$ и натуральных чисел $k_1, \ldots, k_r$ такие, что*

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}.$$

Последующие леммы необходимы для доказательства теоремы 10. В дальнейшем нетривиальными мы будем называть идеалы кольца $\mathbb{Z}_K$ отличные от самого кольца и от нулевого идеала.

Лемма 21. *Пусть $\mathfrak{a} \subset \mathbb{Z}_K$ - нетривиальный идеал в кольце $\mathbb{Z}_K$. Тогда $\mathfrak{a} \cap \mathbb{Z} \neq (0)$ и факторкольцо $\mathbb{Z}/\mathfrak{a}$ конечно.*

Доказательство. Пусть α – ненулевой элемент идеала $\mathfrak{a} \subset \mathbb{Z}_K$. Обозначим $p(x) = x^d + b_{d-1}x^{d-1} + \ldots + b_1 x + b_0 \in \mathbb{Z}[x]$ – минимальный многочлен числа α. Тогда имеет место равенство

$$b_0 = \alpha(-\alpha^{d-1} - b_{d-1}\alpha^{d-2} - \ldots - b_1) = \alpha\gamma, \qquad \gamma \in \mathbb{Z}_K,$$

из которого следует, что $b_0 \in \mathfrak{a} \cap \mathbb{Z}$. Поскольку $b_0 \neq 0$, это доказывает первое утверждение.

Обозначим $a = |b_0| \in \mathfrak{a}$ и пусть $\omega_1, \ldots, \omega_n$ – какой-либо базис кольца $\mathbb{Z}_K$. Обозначим также буквой S конечное множество, состоящее из чисел

$$k_1\omega_1 + \cdots + k_n\omega_n, \qquad k_j \in \mathbb{Z}, \quad 0 \leq k_j < a.$$

Пусть β – какое-либо число из кольца $\mathbb{Z}_K$. Тогда имеем $\beta = c_1\omega_1 + \cdots + c_n\omega_n$, $c_j \in \mathbb{Z}$. Определим теперь целые числа q_j, r_j равенствами

$$c_j = aq_j + r_j, \quad 0 \leq r_j < a, \quad j = 1, \ldots, n.$$

Из этих определений следует, что

$$\beta - a(q_1\omega_1 + \cdots + q_n\omega_n) = \gamma \in S.$$

По другому это равенство может быть переписано в виде $\beta \equiv \gamma \pmod{\mathfrak{a}}$ и означает, что каждый класс вычетов кольца $\mathbb{Z}_K$ по модулю идеала $\mathfrak{a}$ содержит некоторый элемент из множества S. Но эти множества – смежные классы по идеалу $\mathfrak{a}$, имеют лишь тривиальные пересечения. Следовательно количество смежных классов не превосходит количества элементов в множестве S. □

Заметим, что для любого нетривиального идеала $\mathfrak{a} \subset \mathbb{Z}_K$ пересечение $\mathfrak{a} \cap \mathbb{Z}$ есть нетривиальный идеал в кольце $\mathbb{Z}$. Но это кольцо есть кольцо главных идеалов, так что с некоторым целым числом $a > 0$ выполняется равенство $\mathfrak{a} \cap \mathbb{Z} = (a)$.

Напомним, что нетривиальный идеал $\mathfrak{m}$ в кольце A называется *максимальным*, если он не содержится ни в каком другом нетривиальном идеале. Из этого определения следует, что факторкольцо $A/\mathfrak{m}$ есть поле и потому не имеет делителей нуля. Но это свойство означает, что идеал $\mathfrak{m}$ прост. Итак, каждый максимальный идеал прост. В кольцах целых алгебраических чисел справедливо и обратное утверждение.

Предложение 2. *Каждый простой идеал в $\mathbb{Z}_K$ максимален.*

Доказательство. Пусть $\mathfrak{p} \subset \mathbb{Z}_K$ – простой идеал, и $\alpha \in \mathbb{Z}_K$, $\alpha \notin \mathfrak{p}$. Рассмотрим классы вычетов $\alpha^m \pmod{\mathfrak{p}}$, $m = 1, 2, \ldots$. Факторкольцо $\mathbb{Z}_K/\mathfrak{p}$ конечно, поэтому существуют два натуральных числа $m > \ell$, такие, что $\alpha^m \equiv \alpha^\ell \pmod{\mathfrak{p}}$. Обозначим $d = m - \ell \geq 1$. Тогда $\alpha^\ell(\alpha^d - 1) \in \mathfrak{p}$, и поскольку $\alpha \notin \mathfrak{p}$, а идеал $\mathfrak{p}$ прост, заключаем, что $\alpha^d - 1 \in \mathfrak{p}$ или $\alpha^d \equiv 1 \pmod{\mathfrak{p}}$. Положим $\beta = \alpha^{d-1} \in \mathbb{Z}_K$. Тогда $\alpha\beta \equiv 1 \pmod{\mathfrak{p}}$. Но это значит, что класс вычетов $\alpha \pmod{\mathfrak{p}}$ обратим в факторкольце $\mathbb{Z}_K/\mathfrak{p}$.

Так как, по доказанному, каждый ненулевой элемент факторкольца $\mathbb{Z}_K/\mathfrak{p}$ имеет в этом кольце обратный, то $\mathbb{Z}_K/\mathfrak{p}$ есть поле, а $\mathfrak{p}$ – максимальный идеал в кольце $\mathbb{Z}_K$. □

Следствие 20. *Если $\mathfrak{p}$ - простой идеал и $\mathfrak{p} \cap \mathbb{Z} = (p)$, то p – простое число, и количество элементов в поле вычетов $F_q = \mathbb{Z}_K/\mathfrak{p}$ равно p^f, где $f = [F_q : F_p]$ – степень расширения.*

Доказательство. Так как идеал $\mathfrak{p}$ прост, то пересечение $\mathfrak{p} \cap \mathbb{Z} = (p)$ есть простой идеал в кольце $\mathbb{Z}$. Но тогда образующая p должна быть простым числом. Из эквивалентности

$$a, b \in \mathbb{Z}, \quad a \equiv b \pmod{p} \quad \Leftrightarrow \quad a, b \in \mathbb{Z}, \quad a \equiv b \pmod{\mathfrak{p}}$$

следует, что отображение $a \pmod{p} \to a \pmod{\mathfrak{p}}$ из поля $F_p = \mathbb{Z}/p\mathbb{Z}$ в поле $\mathbb{Z}_K/\mathfrak{p}$ есть гомоморфизм с нулевым ядром, так что поле F_p можно считать содержащимся в поле $F_q = \mathbb{Z}_K/\mathfrak{p}$. Каждый элемент поля F_q имеет единственное разложение по базису расширения $F_q \supset F_p$ с коэффициентами из поля F_p. Отсюда следует, что $q = p^f$, где $f = [F_q : F_p]$ – степень расширения. □

Лемма 22. *Если в кольце $\mathbb{Z}_K$ задана возрастающая последовательность идеалов $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$, то существует номер m такой, что*

$$\mathfrak{a}_k = \mathfrak{a}_m, \qquad \textit{при каждом} \qquad k \geq m,$$

т.е. любая такая последовательность стабилизируется.

Доказательство. Обозначим $\mathfrak{a} = \cup_{i=1}^{\infty} \mathfrak{a}_i$. Это множество есть аддитивная подгруппа в $\mathbb{Z}_K$ и выдерживает умножение на элементы кольца $\mathbb{Z}_K$. Действительно, если $\alpha \in \mathbb{Z}_K$ и $\beta \in \mathfrak{a}$, то с некоторым индексом j выполняется включение $\beta \in \mathfrak{a}_j$. Но тогда $\alpha\beta \in \mathfrak{a}_j \subset \mathfrak{a}$. Это доказывает, что $\mathfrak{a}$ есть идеал кольца $\mathbb{Z}_K$.

Пусть $\xi_1, \ldots, \xi_n$ – базис $\mathfrak{a}$ как $\mathbb{Z}$ - модуля, т.е. $\mathfrak{a} = \mathbb{Z}\xi_1 + \ldots + \mathbb{Z}\xi_n$. Идеалы $\mathfrak{a}_j$ образуют возрастающую по включению последовательность, поэтому найдется такой номер m, что $\xi_i \in \mathfrak{a}_m$, для всех $i = 1, \ldots, n$. Но тогда $\mathfrak{a} \subset \mathfrak{a}_m$ и $\mathfrak{a} = \mathfrak{a}_m$. □

Из последней леммы следует, что в каждой совокупности S идеалов кольца $\mathbb{Z}_K$ можно найти идеал $\mathfrak{a}$, не содержащийся ни в каком другом идеале из множества S, т.е. строгое включение $\mathfrak{a} \subset \mathfrak{b}$ возможно лишь тогда, когда идеал $\mathfrak{b}$ не содержится в S. В противном случае для каждого идеала $\mathfrak{a}_i \in S$ существовал бы строго больший идеал $\mathfrak{a}_{i+1} \in S$ и такая цепочка была бы бесконечной.

Лемма 23. *Для каждого нетривиального идеала $\mathfrak{a} \subset \mathbb{Z}_K$ существуют простые идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset \mathbb{Z}_K$ такие, что*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{a}.$$

Доказательство. Предположим, что в кольце $\mathbb{Z}_K$ существуют идеалы, для которых утверждение леммы неверно и обозначим буквой S совокупность всех таких идеалов. Тогда в соответствии с леммой 22 в множестве S можно найти идеал $\mathfrak{a}$, не содержащийся ни в каком другом идеале из S. Включение $\mathfrak{a} \in S$ означает, что идеал $\mathfrak{a}$ не прост, а тогда существуют числа

$$\alpha, \beta \in \mathbb{Z}_K, \quad \alpha\beta \in \mathfrak{a}, \quad \alpha \notin \mathfrak{a},\ \beta \notin \mathfrak{a}. \tag{1.35}$$

Пусть $(\mathfrak{a}, \alpha)$ – идеал, порожденный элементами $\mathfrak{a}$ и числом α, т.е. состоящий из чисел вида $u + \alpha v$, где $u \in \mathfrak{a}$, $v \in \mathbb{Z}_K$. Если $(\mathfrak{a}, \alpha) = \mathbb{Z}_K$, то с некоторым числом $v \in \mathbb{Z}_K$ выполняется сравнение $1 \equiv \alpha v \pmod{\mathfrak{a}}$. Умножая его на β, приходим к сравнению

$$\beta \equiv \alpha\beta v \pmod{\mathfrak{a}} \equiv 0 \pmod{\mathfrak{a}},$$

или включению $\beta \in \mathfrak{a}$, что неверно. Значит, включение $(\mathfrak{a}, \alpha) \subset \mathbb{Z}_K$ строгое.

Аналогично определим идеал $(\mathfrak{a}, \beta) \neq \mathbb{Z}_K$. Из (1.35) следует, что оба идеала $(\mathfrak{a}, \alpha)$ и $(\mathfrak{a}, \beta)$ строго содержат идеал $\mathfrak{a}$ и потому не принадлежат

множеству S. Но тогда существуют две совокупности простых идеалов $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ и $\mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_r$, для которых имеют место включения

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subset (\mathfrak{a}, \alpha), \qquad \mathfrak{p}_{s+1} \cdots \mathfrak{p}_r \subset (\mathfrak{a}, \beta).$$

Перемножая эти включения, находим

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \cdot \mathfrak{p}_{s+1} \cdots \mathfrak{p}_r \subset (\mathfrak{a}, \alpha) \cdot (\mathfrak{a}, \beta) \subset (\mathfrak{a}, \alpha\beta) \subset \mathfrak{a}.$$

Но это включение противоречит определению множества S. Получившееся противоречие доказывает, что множество S пусто. □

Предложение 3. *Для каждого дробного идеала M поля K справедливо равенство*

$$M \cdot M^{-1} = \mathbb{Z}_K. \tag{1.36}$$

Доказательство. 1. Достаточно доказать существование дробного идеала M_1, для которого выполнено равенство $MM_1 = \mathbb{Z}_K$. Действительно, тогда согласно определению имеем $M_1 \subset M^{-1}$ и из включений

$$\mathbb{Z}_K = MM_1 \subset MM^{-1} \subset \mathbb{Z}_K$$

находим $MM^{-1} = \mathbb{Z}_K$.

2. Пусть $\mathfrak{p}$ – простой идеал в кольце $\mathbb{Z}_K$. Докажем сначала, что выполняющееся согласно лемме 20 включение $\mathbb{Z}_k \subset \mathfrak{p}^{-1}$, – строгое. Выберем для этого какой-нибудь ненулевой элемент $a \in \mathfrak{p}$. Согласно лемме 23 найдутся простые идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, произведение которых содержится в главном идеале $(a) \subset \mathbb{Z}_K$. Будем считать, что при этом идеалы выбраны так, что r принимает наименьшее возможное значение. Имеют место включения

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}.$$

Если ни один из идеалов $\mathfrak{p}_j$ не содержится в $\mathfrak{p}$, то можно выбрать элементы $b_j \in \mathfrak{p}_j$, $b_j \notin \mathfrak{p}$. Перемножая их, находим

$$b_1 b_2 \cdots b_r \in \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{p},$$

вопреки простоте идеала $\mathfrak{p}$. Итак, по крайней мере один из идеалов $\mathfrak{p}_j$ должен содержаться в $\mathfrak{p}$. Не уменьшая общности можно считать, что $\mathfrak{p}_1 \subset \mathfrak{p}$. В соответствии с предложением 2 идеал $\mathfrak{p}_1$ максимален, но тогда должно выполняться равенство $\mathfrak{p}_1 = \mathfrak{p}$.

Из минимальности r следует, что $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (a)$ и, следовательно, найдется элемент $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$, $b \notin (a)$. Положим $c = ba^{-1}$. Так как $b \notin (a)$, то $c \notin \mathbb{Z}_K$. Имеем включения

$$c\mathfrak{p} = a^{-1}b\mathfrak{p} \subset a^{-1}\mathfrak{p}_2 \cdots \mathfrak{p}_r\mathfrak{p}_1 \subset a^{-1}(a) \subset \mathbb{Z}_K.$$

Но тогда $c \in \mathfrak{p}^{-1}$, так что дробный идеал $\mathfrak{p}^{-1}$ строго содержит кольцо $\mathbb{Z}_K$.

3. Докажем теперь нужное равенство для простых идеалов кольца $\mathbb{Z}_K$. Если $\mathfrak{p}$ – простой идеал, то

$$\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset \mathbb{Z}_K.$$

Из равенства $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ следует $\mathfrak{p}^{-1} \subset E_{\mathfrak{p}} \subset \mathbb{Z}_K$, что противоречит пункту 2 доказательства. Значит, включение $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1}$ строгое. Но идеал $\mathfrak{p}$, согласно предложению 2 максимален, так что должно выполняться равенство $\mathfrak{p}\mathfrak{p}^{-1} = \mathbb{Z}_K$.

4. Обозначим буквой S совокупность всех идеалов кольца $\mathbb{Z}_K$, для которых равенство (1.36) не выполняется. Предположим, что множество S непусто и обозначим буквой $\mathfrak{a}$ такой идеал в S, который не содержится ни в каком другом идеале из этого множества.

В множестве всех идеалов, содержащих $\mathfrak{a}$, выберем какой-нибудь максимальный идеал $\mathfrak{p}$. Этот идеал прост. Согласно пункту 3 доказательства находим

$$\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = \mathbb{Z}_K.$$

Если $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, то имеем $\mathfrak{p}^{-1} \subset E_{\mathfrak{a}} \subset \mathbb{Z}_K$, что противоречит пункту 2. Значит, включение $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$ – строгое. Если $\mathfrak{a}\mathfrak{p}^{-1} = \mathbb{Z}_K$, то согласно пункту 1 доказательства идеал $\mathfrak{a}$ удовлетворяет равенству (1.36), что противоречит его принадлежности к множеству S. Итак, $\mathfrak{b} = \mathfrak{a}\mathfrak{p}^{-1}$ – нетривиальный идеал кольца $\mathbb{Z}_K$, строго содержащий $\mathfrak{a}$. Тогда $\mathfrak{b} \notin S$ и $\mathfrak{b}\mathfrak{b}^{-1} = \mathbb{Z}_K$. Таким образом, получаем равенство $\mathfrak{a}\mathfrak{p}^{-1}\mathfrak{b}^{-1} = \mathbb{Z}_K$, противоречащее пункту 1 доказательства. Значит, множество S пусто, а равенство (1.36) выполняется для любого идеала кольца $\mathbb{Z}_K$.

5. Пусть, наконец, M – произвольный дробный идеал поля K. С некоторыми числами $\xi_1, \ldots, \xi_n$ из поля K выполняется равенство $M = \mathbb{Z}\xi_1 + \ldots + \mathbb{Z}\xi_n$. Если a - натуральное число, для которого $a\xi_j \in \mathbb{Z}_K$, $j = 1, \ldots, n$, то $aM \subset \mathbb{Z}_K$ – нетривиальный идеал кольца $\mathbb{Z}_K$. Обозначив $M_1 = (aM)^{-1}$, получим, согласно пункту 4, $aMM_1 = \mathbb{Z}_K$ или $MM_2 = \mathbb{Z}_K$, где $M_2 = aM_1$. Теперь по пункту 1 доказательства заключаем, что для дробного идеала M выполняется равенство (1.36). □

Следствие 21. *Дробные идеалы образуют группу по умножению с единицей $\mathbb{Z}_K$.*

Доказательство. Операция умножения в множестве дробных идеалов определена в начале параграфа. Как доказано в лемме 20 она ассоциативна. Для каждого дробного идеала M имеем равенство $E_M = \mathbb{Z}_K$, так что $\mathbb{Z}_K M \subset M$. Учитывая, что $1 \in \mathbb{Z}_K$, получаем равенство $\mathbb{Z}_K \cdot M = M$.

Кроме того, согласно предложению 3 имеем $MM^{-1} = \mathbb{Z}_K$. Это значит, что дробный идеал $\mathbb{Z}_K$ есть единица группы, а M^{-1} – обратный элемент к M. □

Следствие 22. *Для каждого идеала* $\mathfrak{a} \subset \mathbb{Z}_K$, $\mathfrak{a} \neq (0)$, *существуют простые идеалы* $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ *такие, что*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Доказательство. Обозначим буквой S совокупность идеалов кольца $\mathbb{Z}_K$, для которых следствие неверно. В предположении, что S непусто, обозначим буквой $\mathfrak{a}$ принадлежащий S идеал, не содержащийся ни в каких других идеалах из S. Пусть также $\mathfrak{p}$ – максимальный в кольце $\mathbb{Z}_K$ идеал, содержащий $\mathfrak{a}$. Тогда

$$\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = \mathbb{Z}_K.$$

Если $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}\mathfrak{p}^{-1} = \mathbb{Z}_K$, то умножая это равенство на $\mathfrak{p}$, находим $\mathfrak{a} = \mathfrak{p}$, что противоречит включению $\mathfrak{a} \in S$. Значит, $\mathfrak{a}\mathfrak{p}^{-1}$ – нетривиальный идеал в кольце $\mathbb{Z}_K$. Равенство $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$ также невозможно, ведь в этом случае $\mathfrak{p}^{-1} \subset E_{\mathfrak{a}} \subset \mathbb{Z}_K$ вопреки второму пункту доказательства предложения 3. Итак, $\mathfrak{a}\mathfrak{p}^{-1}$ нетривиальный идеал кольца $\mathbb{Z}_K$, строго содержащий идеал $\mathfrak{a}$. Поэтому $\mathfrak{a}\mathfrak{p}^{-1} \notin S$ и для $\mathfrak{a}\mathfrak{p}^{-1}$ выполнено утверждение следствия. Это значит, что с некоторыми простыми идеалами $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ выполняется равенство

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Умножая это равенство на идеал $\mathfrak{p}$ и пользуясь предложением 3, находим $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r$, вопреки включению $\mathfrak{a} \in S$. Это противоречие доказывает пустоту множества S и завершает доказательство следствия. □

Доказанное следствие устанавливает часть утверждения теоремы 10 – возможность разложения идеалов кольца $\mathbb{Z}_K$ в произведение простых идеалов. Теперь можно завершить доказательство этой теоремы.

Доказательство теоремы 10. Осталось доказать единственность разложения. Обозначим буквой S совокупность идеалов кольца $\mathbb{Z}_K$, которые можно разложить в произведение простых идеалов по крайней мере двумя различными способами. Предположим, что множество S непусто и выберем в нем идеал $\mathfrak{a}$, для которого существуют различные разложения

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s \tag{1.37}$$

с наименьшим возможным значением суммы $r+s$. Не уменьшая общности можно считать, что $r \leq s$. Справедливо включение

$$\mathfrak{p}_1 \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Если ни один из идеалов q_j не содержится в идеале $\mathfrak{p}_1$, то можно найти числа $b_1, \ldots, b_s$, удовлетворяющие условиям

$$b_j \in \mathfrak{q}_j, \quad b_j \notin \mathfrak{p}_1, \qquad j = 1, \ldots s.$$

Но тогда имеем

$$b_1 \cdots b_s \in \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{p}_1,$$

вопреки простоте идеала $\mathfrak{p}_1$. Значит, по крайней мере один из идеалов q_j содержится в идеале $\mathfrak{p}_1$. Не уменьшая общности можно считать, что $\mathfrak{q}_1 \subset \mathfrak{p}_1$. Учитывыая, что каждый простой идеал кольца $\mathbb{Z}_K$ и, в частности, идеал $\mathfrak{q}_1$ максимален, заключаем, что $\mathfrak{q}_1 = \mathfrak{p}_1$. Умножая теперь равенство (1.37) на дробный идеал $\mathfrak{p}_1^{-1}$ и пользуясь предложением 3, находим

$$\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s. \tag{1.38}$$

Учитывая, что количество простых идеалов, участвующих в последнем равенстве меньше $r+s$, заключаем, что $\mathfrak{b} \notin S$.

Если $r \geq 2$, то $\mathfrak{b}$ - нетривиальный идеал кольца $\mathbb{Z}_K$ и, так как $\mathfrak{b} \notin S$ то этот идеал лишь единственным способом может быть разложен в произведение простых идеалов. Тогда $r-1 = s-1$ и множества простых идеалов $\mathfrak{p}_j$ и $\mathfrak{q}_j$, участвующих в разложении (1.38) состоят из одинаковых идеалов и, может быть, отличаются лишь порядком их следования. Но это противоречит тому, что в (1.37) присутствуют различные разложения идеала $\mathfrak{a}$ в произведение простых идеалов.

Итак, $r = 1$, т.е. идеал $\mathfrak{a} = \mathfrak{p}_1$ прост и $\mathfrak{b} = \mathbb{Z}_K$. Если $s \geq 2$, то имеем включение

$$1 \in \mathbb{Z}_K = \mathfrak{b} = \mathfrak{q}_2 \cdots \mathfrak{q}_s \subset \mathfrak{q}_s,$$

что невозможно, так как простой идеал $\mathfrak{q}_s$ нетривиален. В случае $s = 1$ представления (1.37) не будут различными, что также невозможно. Итак, во всех случаях мы приходим к противоречию, что доказывает пустоту множества S и завершает доказательство теоремы. □

Следствие 23. *Каждый дробный идеал единственным способом представляется в виде произведения целых степеней (положительных или отрицательных) простых идеалов.*

Доказательство. Если $M = \mathbb{Z}\xi_1 + \cdots + \mathbb{Z}\xi_n$ – дробный идеал поля K и a – натуральное число с условием $a\xi_j \in \mathbb{Z}_K$, $j = 1, \ldots n$, то aM – нетривиальный идеал в кольце $\mathbb{Z}_K$. Идеалы (a) и aM могут быть разложены в произведение простых идеалов

$$(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_r, \qquad aM = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Из этих равенств следует

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot M = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Умножая получившееся равенство на дробные идеалы $\mathfrak{p}_1^{-1}, \ldots, \mathfrak{p}_r^{-1}$, находим

$$M = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

и это доказывает, что группа дробных идеалов порождается простыми идеалами. Предположим, что имеет место равенство

$$\mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_m^{k_m} = \mathfrak{p}_1^{\ell_1} \cdots \mathfrak{p}_m^{\ell_m}, \tag{1.39}$$

где $\mathfrak{p}_1, \ldots, \mathfrak{p}_u$ – различные простые идеалы, а показатели степени k_j, ℓ_j есть целые числа, может быть и равные нулю. Обозначим

$$N = \max_{1 \le j \le m} \{|k_j|, |\ell_j|\}.$$

Умножив равенство (1.39) на идеал $(\mathfrak{p}_1 \cdots \mathfrak{p}_m)^N$ и пользуясь единственностью разложения идеалов кольца $\mathbb{Z}_K$ в произведение простых идеалов, находим $N + k_j = N + \ell_j$ и, следовательно, $k_j = \ell_j$ при всех $j = 1, \ldots, m$. Это завершает доказательство следствия. □

Показатель, с которым простой идеал $\mathfrak{p}$ входит в разложение дробного идеала M будет обозначаться $\nu_{\mathfrak{p}}(M)$. Следствие 23 означает, что для любых двух дробных идеалов M_1 и M_2 справедливо равенство

$$\nu_{\mathfrak{p}}(M_1 \cdot M_2) = \nu_{\mathfrak{p}}(M_1) + \nu_{\mathfrak{p}}(M_2). \tag{1.40}$$

Для каждого $\alpha \in K$ будем обозначать $\nu_{\mathfrak{p}}(\alpha) = \nu_{\mathfrak{p}}((\alpha))$, где (α) - дробный идеал, порожденный α, т.е. $(\alpha) = \alpha\mathbb{Z}_K$.

Следствие 24. *1. Для любых двух дробных идеалов M_1, M_2 включение $M_1 \subset M_2$ выполняется в том и только том случае, когда для любого простого идеала $\mathfrak{p}$ имеет место неравенство*

$$\nu_{\mathfrak{p}}(M_1) \ge \nu_{\mathfrak{p}}(M_2).$$

2. Пусть $\mathfrak{a}$ - идеал в кольце $\mathbb{Z}_K$. Элемент $\alpha \in K$ принадлежит $\mathfrak{a}$ тогда и только тогда, когда для любого простого идеала $\mathfrak{p}$ выполняется неравенство $\nu_{\mathfrak{p}}(\alpha) \ge \nu_{\mathfrak{p}}(\mathfrak{a})$.

Доказательство. Имеет место цепочка эквивалентных утверждений

а) $M_1 \subset M_2$,

б) $M_1 M_2^{-1} \subset \mathbb{Z}_K$,

в) $\nu_{\mathfrak{p}}(M_1 M_2^{-1}) \geq 0$ для каждого простого идеала $\mathfrak{p} \subset \mathbb{Z}_K$,

г) $\nu_{\mathfrak{p}}(M_1) \geq \nu_{\mathfrak{p}}(M_2)$ для каждого простого идеала $\mathfrak{p} \subset \mathbb{Z}_K$.

Эквивалентность а) и б) следует из того, что $M_2 M_2^{-1} = \mathbb{Z}_K$. Эквивалентность б) и в) выполняется в силу того, что каждый идеал кольца $\mathbb{Z}_K$ представляется в виде произведения неотрицательных степеней простых идеалов и притом единственным способом. Эквивалентность в) и г) следует из равенства (1.40). Следующая отсюда эквивалентность а) и г) доказывает первое утверждение.

Легко видеть, что включение $\alpha \in \mathfrak{a}$ выполняется тогда и только тогда, когда $(\alpha) \subset \mathfrak{a}$. Теперь очевидно, что второе утверждение следует из первого. □

Следствие 25. *1.* $\nu_{\mathfrak{p}}(\alpha\beta) = \nu_{\mathfrak{p}}(\alpha) + \nu_{\mathfrak{p}}(\beta)$,

2. $\nu_{\mathfrak{p}}(\alpha/\beta) = \nu_{\mathfrak{p}}(\alpha) - \nu_{\mathfrak{p}}(\beta)$,

3. $\nu_{\mathfrak{p}}(\alpha+\beta) \geq \min(\nu_{\mathfrak{p}}(\alpha), \nu_{\mathfrak{p}}(\beta))$, *и если* $\nu_{\mathfrak{p}}(\alpha) < \nu_{\mathfrak{p}}(\beta)$, *то* $\nu_{\mathfrak{p}}(\alpha+\beta) = \nu_{\mathfrak{p}}(\alpha)$.

Доказательство. Первое утверждение есть непосредственное следствие равенства (1.40). Второе утверждение имеет место, так как согласно первому $\nu_{\mathfrak{p}}(\alpha/\beta) + \nu_{\mathfrak{p}}(\beta) = \nu_{\mathfrak{p}}(\alpha/\beta \cdot \beta) = \nu_{\mathfrak{p}}(\alpha)$.

Обозначим $k = \min(\nu_{\mathfrak{p}}(\alpha), \nu_{\mathfrak{p}}(\beta))$. Будем считать сначала, что $\alpha, \beta \in \mathbb{Z}_K$. Тогда из второго утверждения следствия 24 находим $\alpha \in \mathfrak{p}^k$, $\beta \in \mathfrak{p}^k$ и, значит, $\alpha+\beta \in \mathfrak{p}^k$. Применяя опять второе утверждение следствия 24, получаем $\nu_{\mathfrak{p}}(\alpha+\beta) \geq k$, что доказывает первое неравенство из пункта 3 в случае $\alpha, \beta \in \mathbb{Z}_K$. Предположим теперь, что α, β – произвольные числа. Для некоторого натурального d выполняются включения $d\alpha, d\beta \in \mathbb{Z}_K$. Применяя доказанное неравенство к числам $d\alpha, d\beta$, и пользуясь равенством из пункта 1, легко получаем нужное неравенство и в общем случае.

Предположим теперь, что

$$\nu_{\mathfrak{p}}(\alpha) < \nu_{\mathfrak{p}}(\beta). \tag{1.41}$$

Из определения величины $\nu_{\mathfrak{p}}(\beta)$ непосредственно следует, что $\nu_{\mathfrak{p}}(\beta) = \nu_{\mathfrak{p}}(-\beta)$. Отсюда находим

$$\nu_{\mathfrak{p}}(\alpha) = \nu_{\mathfrak{p}}((\alpha+\beta)+(-\beta)) \geq \min(\nu_{\mathfrak{p}}(\alpha+\beta), \nu_{\mathfrak{p}}(\beta)).$$

В силу неравенства (1.41) отсюда следует $\nu_{\mathfrak{p}}(\alpha) \geq \nu_{\mathfrak{p}}(\alpha+\beta)$, что и завершает доказательство последнего утверждения. □

Последнее утверждение следствия 25 естественно распространиется на произвольное количество слагаемых.

Следствие 26. *Пусть $\mathfrak{p}_1, \dots \mathfrak{p}_r$ - различные простые идеалы и $a_1, \dots, a_r$ - произвольные целые неотрицательные числа. Тогда существует число $\alpha \in \mathbb{Z}_K$ такое, что*

$$\nu_{\mathfrak{p}}(\alpha) = a_j, \qquad j = 1, \dots, r.$$

Доказательство. Выберем целое число $N > a_j$, $j = 1, \dots, r$ и рассмотрим идеалы

$$\mathfrak{a}_j = \mathfrak{p}_j^{a_j} \prod_{i \neq j} \mathfrak{p}_i^N.$$

В силу первого утверждения следствия 24 находим $\mathfrak{a}_j \not\subset \mathfrak{p}_j^{a_j+1}$. Поэтому существуют числа $\alpha_j \in \mathfrak{a}_j$, $\alpha_j \notin \mathfrak{p}_j^{a_j+1}$.

Применяя второе утверждение следствия 24 к числу α_j и идеалам $\mathfrak{a}_j$, $\mathfrak{p}_j^{a_j+1}$, заключаем, что $\nu_{\mathfrak{p}_j}(\alpha_j) = a_j$. В случае $i \neq j$ с помощью второго утверждения следствия 24 находим $\nu_{\mathfrak{p}_i}(\alpha_j) \geq N$.

Положим $\alpha = \alpha_1 + \ldots + \alpha_r$. Для каждого индекса j в этой сумме присутствует лишь одно слагаемое α_j, для которого выполнено неравенство $\nu_{\mathfrak{p}_j}(\alpha_i) < N$. Последнее утверждение следствия 25 дает нам $\nu_{\mathfrak{p}_j}(\alpha) = \nu_{\mathfrak{p}_j}(\alpha_j) = a_j$. □

Следствие 27. *Множество простых идеалов в кольце $\mathbb{Z}_K$ бесконечно.*

Доказательство. Сопоставим каждому простому числу p конечный набор простых идеалов, входящих в разложение главного идеала $(p) \subset \mathbb{Z}_K$. Заметим, что при этом сопоставлении различным простым числам ставятся в соответствие различные простые идеалы. Действительно, допустим, что простой идеал $\mathfrak{p}$ входит в разложение идеалов $(p), (q)$, где p, q – различные простые числа. По следствию 24 имеют место включения $p \in \mathfrak{p}, q \in \mathfrak{p}$. Учитывая, что $\mathbb{Z} \cap \mathfrak{p} = (a)$ есть главный идеал, заключаем, что в кольце $\mathbb{Z}$ простые числа p, q имеют общий делитель a, что невозможно. Итак, каждому простому числу сопоставляется конечное множество простых идеалов, причем эти множества не пересекаются. Отсюда следует нужное утверждение. □

1.12 Норма идеала.

Определение 30. *Нормой идеала $\mathfrak{a} \subset \mathbb{Z}_K$ называется количество элементов в факторкольце $\mathbb{Z}_K/\mathfrak{a}$.*

Теорема 11. *Для любых двух идеалов* $\mathfrak{a}, \mathfrak{b} \subset \mathbb{Z}_K$ *выполняется равенство*

$$N(\mathfrak{ab}) = N(\mathfrak{a}) \cdot N(\mathfrak{b}).$$

Доказательство. Теорему достаточно доказать в предположении, что идеал $\mathfrak{b}$ прост. Чтобы проверить это, допустим, что утверждение справедливо для простых идеалов и воспользуемся индукцией по количеству простых идеалов, входящих в разложение $\mathfrak{b}$. Если $\mathfrak{b} = \mathfrak{p}\mathfrak{b}_1$, то согласно индуктивному предположению имеем равенства

$$\begin{aligned} N(\mathfrak{ab}) =& N(\mathfrak{ab}_1\mathfrak{p}) = N(\mathfrak{ab}_1)N(\mathfrak{p}) = N(\mathfrak{a})N(\mathfrak{b}_1)N(\mathfrak{p}) = \\ & N(\mathfrak{a})N(\mathfrak{b}_1\mathfrak{p}) = N(\mathfrak{a})N(\mathfrak{b}). \end{aligned}$$

В дальнейшем будем считать, что идеал $\mathfrak{b} = \mathfrak{p}$ прост. Положим $\mathfrak{c} = \mathfrak{ap}$. Так как $\nu_\mathfrak{p}(\mathfrak{c}) > \nu_\mathfrak{p}(\mathfrak{a})$, то по следствию 24 имеем $\mathfrak{a} \not\subset \mathfrak{c}$. Значит найдется число $t \in \mathfrak{a}$, $t \notin \mathfrak{c}$. Справедливы включения $\mathfrak{c} \subset (\mathfrak{c}, t) \subset \mathfrak{a}$, из которых согласно следствию 24 получаем

$$\nu_\mathfrak{q}(\mathfrak{c}) \geq \nu_\mathfrak{q}((\mathfrak{c}, t)) \geq \nu_\mathfrak{q}(\mathfrak{a}), \quad \text{для любого простого идеала} \quad \mathfrak{q} \subset \mathbb{Z}_K.$$

Учитывая, что разложения на множители идеалов $\mathfrak{c}$ и $\mathfrak{a}$ отличаются лишь одним простым множителем $\mathfrak{p}$, заключаем, что либо $(\mathfrak{c}, t) = \mathfrak{a}$, либо $(\mathfrak{c}, t) = \mathfrak{c}$. Так как $t \notin \mathfrak{c}$, находим $\mathfrak{a} = (\mathfrak{c}, t)$.

Для каждого простого идеала $\mathfrak{q}$ имеем

$$\nu_\mathfrak{q}(t) \geq \nu_\mathfrak{q}(\mathfrak{a}),$$

так что в случае $\mathfrak{q} \neq \mathfrak{p}$ выполняется неравенство

$$\nu_\mathfrak{q}(t) \geq \nu_\mathfrak{q}(\mathfrak{c}). \tag{1.42}$$

Если $\nu_\mathfrak{p}(t) \geq 1 + \nu_\mathfrak{p}(\mathfrak{a}) = \nu_\mathfrak{p}(\mathfrak{c})$, то согласно следствию 24 должно выполняться включение $t \in \mathfrak{c}$, что неверно. Таким образом, $\nu_\mathfrak{p}(t) \leq \nu_\mathfrak{p}(\mathfrak{a})$, откуда находим

$$\nu_\mathfrak{p}(t) = \nu_\mathfrak{p}(\mathfrak{a}). \tag{1.43}$$

Рассмотрим гомоморфизм $f : \mathbb{Z}_K \to \mathbb{Z}_K/\mathfrak{a}$. Так как $\mathfrak{c} \subset \mathfrak{a} = \operatorname{Ker} f$, то f может быть представлен в виде композиции двух гомоморфизмов

$$f : \mathbb{Z}_K \to \mathbb{Z}_K/\mathfrak{c} \xrightarrow{\varphi} \mathbb{Z}_K/\mathfrak{a}.$$

Так как оба эти гомоморфизма есть отображения "на", то находим равенства

$$N(\mathfrak{c}) = |\mathbb{Z}_K/\mathfrak{c}| = |\mathbb{Z}_K/\mathfrak{a}| \cdot |\operatorname{Ker} \varphi| = N(\mathfrak{a}) \cdot |\operatorname{Ker} \varphi|. \tag{1.44}$$

Для того, чтобы сосчитать количество элементов в $\operatorname{Ker}\varphi$, заметим, что $\beta \pmod{\mathfrak{c}} \in \operatorname{Ker}\varphi$ тогда и только тогда, когда $\beta \in \mathfrak{a}$. По доказанному ранее это включение означает, что с некоторыми $\alpha \in \mathbb{Z}_K$ и $\gamma \in \mathfrak{c}$ выполняется равенство $\beta = \alpha t + \gamma$. Отсюда следует $\beta \pmod{\mathfrak{c}} = \alpha t \pmod{\mathfrak{c}}$. Итак, все элементы ядра $\operatorname{Ker}\varphi$ имеют вид $\alpha t \pmod{\mathfrak{c}}$. Очевидно, что и каждый элемент такого вида принадлежит ядру φ.

Элементы $\alpha_1, \alpha_2 \in \mathbb{Z}_K$, для которых выполняется сравнение $\alpha_1 t \equiv \alpha_2 t \pmod{\mathfrak{c}}$, удовлетворяют условию $(\alpha_1 - \alpha_2)t \in \mathfrak{c}$. Учитывая, неравенство (1.42), а также следующее из (1.43) неравенство $\nu_{\mathfrak{p}}(t) \geq \nu_{\mathfrak{p}}(\mathfrak{c}) - 1$, заключаем, согласно следствию 24, что включение $(\alpha_1 - \alpha_2)t \in \mathfrak{c}$ имеет место тогда и только тогда, когда $\alpha_1 - \alpha_2 \in \mathfrak{p}$. Иными словами, количество различных элементов $\alpha t \pmod{\mathfrak{c}}, \alpha \in \mathbb{Z}_K$ равно количеству классов вычетов $\alpha \pmod{\mathfrak{p}}$, то-есть равно $|\mathbb{Z}_K/\mathfrak{p}| = N(\mathfrak{p})$. Таким образом, $|\operatorname{Ker}\varphi| = N(\mathfrak{p})$. Подставляя эту величину в (1.44), получаем требуемое равенство, что и завершает доказательство теоремы. □

Следующее утверждение будет доказано в несколько большей общности, чем это необходимо сейчас. Но в таком виде оно будет использовано в дальнейшем. Если M – полный модуль, содержащийся в $\mathbb{Z}_K$, то оба множества M и $\mathbb{Z}_K$ могут рассматриваться как абелевы группы по сложению. Вычислим индекс подгруппы M в группе $\mathbb{Z}_K$, другими словами количество элементов в факторгруппе $\mathbb{Z}_K/M$.

Лемма 24. *Пусть M – полный модуль, $M \subset \mathbb{Z}_K$. Тогда число $|\mathbb{Z}_K/M|$ равно абсолютной величине определителя матрицы перехода от какого-либо базиса $\mathbb{Z}_K$ к базису M.*

Доказательство. Очевидно, абсолютная величина указанного в формулировке определителя не зависит от выбора базисов в M и $\mathbb{Z}_K$. Пусть $\omega_1, \ldots, \omega_n$ – какой-либо фундаментальный базис поля K, т.е. базис кольца $\mathbb{Z}_K$. Согласно предложению 1 можно выбрать базис $\eta_1, \ldots, \eta_n$ модуля M так, что

$$\eta_i = c_{i,i}\omega_i + \cdots c_{i,n}\omega_n, \qquad c_{i,j} \in \mathbb{Z}, \quad c_{i,i} > 0.$$

Определитель матрицы перехода от базиса ω_j к базису η_j равен $c_{1,1} \cdots c_{nn}$.

Рассмотрим множество

$$\mathfrak{M} = \{r_1\omega_1 + \cdots + r_n\omega_n \mid \quad r_i \in \mathbb{Z}, \quad 0 \leq r_i < c_{i,i}\},$$

состоящее из $c_{1,1} \cdots c_{n,n}$ элементов. Каждое число $\alpha \in \mathbb{Z}_K$ сравнимо по модулю M с каким-либо числом из множества $\mathfrak{M}$. Действительно, пусть

$$\alpha = k_1\omega_1 + \ldots + k_n\omega_n, \qquad k_i \in \mathbb{Z}.$$

Определим целые числа q_1, r_1 условиями

$$k_1 = c_{1,1}q_1 + r_1, \qquad 0 \le r_1 < c_{1,1}.$$

Тогда

$$\alpha - q_1\eta_1 = r_1\omega_1 + b_{2,2}\omega_2 + \cdots + b_{2,n}\omega_n, \qquad b_{2,j} \in \mathbb{Z}.$$

Определим целые числа q_2, r_2 условиями

$$b_{2,2} = c_{2,2}q_2 + r_2, \qquad 0 \le r_2 < c_{2,2}.$$

Тогда

$$\alpha - q_1\eta_1 - q_2\eta_2 = r_1\omega_1 + r_2\omega_2 + b_{3,3}\omega_3 + \cdots + b_{3,n}\omega_n, \qquad b_{3,j} \in \mathbb{Z}.$$

Продолжая этот процесс мы найдем целые числа q_i, r_i такие, что

$$\alpha - q_1\eta_1 - \ldots - q_n\eta_n = r_1\omega_1 + \ldots + r_n\omega_n, \quad 0 \le r_i < c_{i,i}.$$

Обозначив $\xi = r_1\omega_1 + \ldots r_n\omega_n \in \mathfrak{M}$, получим $\alpha - \xi = q_1\eta_1 + \ldots q_n\eta_n \in M$. Это доказывает, что количество элементов в факторгруппе $\mathbb{Z}_K/M$ не превосходит количества элементов в множестве $\mathfrak{M}$.

Докажем теперь, что никакие два элемента из $\mathfrak{M}$ не сравнимы между собой по модулю M. Допустим, что для некоторых двух чисел

$$\xi_1 = u_1\omega_1 + \ldots + u_n\omega_n, \quad \xi_2 = v_1\omega_1 + \ldots + v_n\omega_n, \quad u_i, v_i \in \mathbb{Z},$$

из множества $\mathfrak{M}$ выполняется включение $\xi_1 - \xi_2 \in M$. Тогда с некоторыми целыми коэффициентами b_j, λ_j имеют место равенства

$$\xi_1 - \xi_2 = \lambda_1\eta_1 + \ldots + \lambda_n\eta_n = (u_i - v_i)\omega_i + \ldots + (u_n - v_n)\omega_n,$$

где i – наименьший индекс с условием $u_i \ne v_i$. Пользуясь разложениями чисел η_j по базису ω_ℓ и сравнивая коэффициенты при ω_j, находим $\lambda_1 = \ldots = \lambda_{i-1} = 0$, $u_i - v_i = c_{i,i}\lambda_i \ne 0$. Из включения $\xi_1, \xi_2 \in \mathfrak{M}$ следует $|u_i - v_i| < c_{i,i}$, так что находим $|\lambda_i| < 1$. Но это неравенство невозможно, ведь λ_i – отличное от нуля целое число. Итак, никакие два элемента множества $\mathfrak{M}$ не сравнимы между собой по модулю M. Следовательно,

$$c_{1,1}c_{2,2}\cdots c_{n,n} = |\mathfrak{M}| = |\mathbb{Z}/M|.$$

□

Лемма 25. *Если* $\mathfrak{a}$ *- идеал в кольце* $\mathbb{Z}_K$*, то*

$$D_{\mathfrak{a}} = N(\mathfrak{a})^2 \cdot D,$$

где D *- дискриминант поля* K*.*

Доказательство. Идеал $\mathfrak{a} \subset \mathbb{Z}_K$ является полным модулем. Поэтому к нему применимо утверждение леммы 24. Пусть $\omega_1, \ldots, \omega_n$ – фундаментальный базис поля K и базис $\eta_1, \ldots, \eta_n$ идеала $\mathfrak{a}$ выбран так же как в доказательстве леммы 24. Тогда $N(\mathfrak{a}) = |\mathbb{Z}_K/\mathfrak{a}| = c_{1,1} \cdots c_{n,n}$. По лемме 9 находим

$$D_{\mathfrak{a}} = \Delta(\eta_1, \ldots, \eta_n) = (c_{1,1} \cdots c_{n,n})^2 \Delta(\omega_1, \ldots, \omega_n) = N(\mathfrak{a})^2 \cdot D. \qquad (1.45)$$

□

Следствие 28. *Для каждого числа $\alpha \in \mathbb{Z}_K$ справедливо равенство*

$$N((\alpha)) = |N(\alpha)|.$$

Доказательство. С некоторыми целыми числами $a_{i,j}$ выполняются равенства

$$\alpha\omega_i = \sum_{j=1}^{n} a_{i,j}\omega_j,$$

причем $\det \|a_{i,j}\| = N(\alpha)$ согласно определению нормы числа. По лемме 24, примененной к идеалу

$$(\alpha) = \mathbb{Z}\alpha\omega_1 + \ldots \mathbb{Z}\alpha\omega_n.$$

имеем

$$|\det \|a_{i,j}\|\,| = |\mathbb{Z}_K/(\alpha)\,| = N((\alpha)).$$

Сравнивая получившиеся равенства, получаем утверждение следствия. □

1.13 Группа классов идеалов и число классов поля.

Дробные идеалы поля алгебраических чисел K образуют мультипликативную группу, а главные дробные идеалы - подгруппу в ней. Факторгруппа группы дробных идеалов по подгруппе главных идеалов называется *группой классов идеалов* поля K.

Заметим, что в каждом классе идеалов содержатся целые идеалы. Действительно, если $M = \mathbb{Z}\xi_1 + \ldots + \mathbb{Z}\xi_n$ – дробный идеал и d – общий знаменатель ξ_j, т.е. натуральное число, для которого $d\xi_j \in \mathbb{Z}_K$. Тогда

$$M_1 = (d)M = \mathbb{Z}d\xi_1 + \ldots + \mathbb{Z}d\xi_n \subset \mathbb{Z}_K$$

есть идеал кольца $\mathbb{Z}_K$. Идеалы M и M_1 лежат в одном классе идеалов.

Теорема 12. *1. В любом классе идеалов содержится целый идеал $\mathfrak{b}$, для которого $N(\mathfrak{b}) \le \sqrt{|D|}$, где D - дискриминант поля.*

2. Группа классов идеалов конечна.

Доказательство. Пусть C – некоторый класс идеалов. Выберем в классе C^{-1} какой-либо целый идеал $\mathfrak{a}$. Определим $\varkappa = \sqrt[2n]{|D_{\mathfrak{a}}|}$. Так как $\varkappa^n = \sqrt{|D_{\mathfrak{a}}|}$, то по следствию 16 в идеале $\mathfrak{a}$ найдется ненулевой элемент α с условиями

$$|\sigma_j(\alpha)| \le \varkappa, \qquad j = 1, \dots, n.$$

Включение $\alpha \in \mathfrak{a}$ означает, что главный идеал (α) делится на идеал $\mathfrak{a}$, т.е. с некоторым целым идеалом $\mathfrak{b}$ выполняется равенство $(\alpha) = \mathfrak{a}\mathfrak{b}$. Отсюда следует, что идеал $\mathfrak{b}$ принадлежит классу C. Оценим далее норму этого идеала.

Пользуясь мультипликативностью нормы идеалов (теорема 11), следствием 28 о норме главного идеала, представлением нормы из следствия 11, а также леммой 25, находим

$$N(\mathfrak{a})N(\mathfrak{b}) = N((\alpha)) = |N(\alpha)| = \prod_{j=1}^{n} |\sigma_j(\alpha)| \le \varkappa^n = \sqrt{|D_{\mathfrak{a}}|} = N(\mathfrak{a})\sqrt{|D|}.$$

Таким образом, $N(\beta) \le \sqrt{|D|}$.

Докажем теперь, что множество идеалов с нормой, ограниченной числом $\sqrt{|D|}$ конечно. Действительно, если

$$\mathfrak{b} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_s^{k_s}, \qquad N(\mathfrak{b}) \le \sqrt{|D|}, \tag{1.46}$$

то из равенств $N(\mathfrak{p}_j) = p_j^{f_j}$, где p_j есть единственное простое число, содержащееся в простом идеале $\mathfrak{p}_j$, и f_j – степень поля вычетов $\mathbb{Z}_K/\mathfrak{p}_j$ над F_{p_j}, см. следствие 20, а также в силу мультипликативности нормы идеала находим

$$p_1^{f_1 k_1} \cdots p_s^{f_s k_s} = N(\mathfrak{b}) \le \sqrt{|D|}. \tag{1.47}$$

Это неравенство во-первых означает ограниченность показателей k_j в равенстве (1.46), а во вторых конечность множества S простых делителей норм идеалов $\mathfrak{b}$, удовлетворяющих неравенству (1.46). Заметим, что каждый простой идеал $\mathfrak{p}_j$ делит простое число p_j, т.е. присутствует в разложении главного идеала (p_j) в произведение простых идеалов. Множество главных идеалов (p), $p \in S$ конечно, значит, будет конечным и множество T простых идеалов, входящих в разложения (p), $p \in S$. Конечность множества T и ограниченность показателей k_j означают конечность множества идеалов $\mathfrak{b}$, удовлетворяющих неравенству (1.46). $\square$

Определение 31. *Порядок группы классов идеалов поля K называется числом классов этого поля.*

Число классов идеалов поля K будет обозначаться $h(K)$.

Следствие 29. *Если h - число классов поля K, то для любого идеала $\mathfrak{a}$ идеал $\mathfrak{a}^h$ есть главный идеал.*

Доказательство. Утверждение очевидно, так как каждый класс идеалов C согласно теореме Лагранжа удовлетворяет равенству $C^h = I$, где I – единичный элемент группы классов идеалов, т.е. класс, состящий из главных идеалов. □

Следствие 30. *Равенство $h(K) = 1$ выполняется тогда и только тогда, когда в кольце целых чисел $\mathbb{Z}_K$ поля K имеет место единственность разложения чисел на простые сомножители.*

Доказательство. Равенство $h(K) = 1$ означает, что каждый идеал кольца $\mathbb{Z}_K$ главный. Но, как хорошо известно, в кольце главных идеалов разложение на простые сомножители единственно с точностью до обратимых элементов.

Для того, чтобы доказать утверждение в обратную сторону рассмотрим какой-либо простой элемент $\pi \in \mathbb{Z}_K$. Главный идеал $(\pi) \subset \mathbb{Z}_K$ будет простым. Действительно, включение $\alpha\beta \in (\pi)$ для некоторых целых чисел α, β означает, что $\pi | \alpha\beta$. В силу единственности разложения целых чисел поля K в произведение простых чисел, заключаем, что либо $\pi|\alpha$, либо $\pi|\beta$, т.е. $\alpha \in (\pi)$ или $\beta \in (\pi)$. Это доказывает, что главный идеал (π) прост.

Пусть $\mathfrak{p}$ – произвольный простой идеал кольца $\mathbb{Z}_K$ и $\delta \in \mathfrak{p}$ – какое-нибудь отличное от нуля число. Если $\delta = \pi_1 \cdots \pi_r$ - разложение δ на простые сомножители, то из включения $\pi_1 \cdots \pi_r \in \mathfrak{p}$ и простоты идеала $\mathfrak{p}$ следует, что хотя бы один из сомножителей π_j принадлежит идеалу $\mathfrak{p}$. Не уменьшая общности можно считать, что $\pi_1 \in \mathfrak{p}$. Но тогда $(\pi_1) \subset \mathfrak{p}$ и, так как по доказанному идеал (π_1) прост, а в кольце $\mathbb{Z}_K$ каждый простой идеал максимален, заключаем, что $\mathfrak{p} = (\pi_1)$ – главный идеал. Итак, в кольце $\mathbb{Z}_K$ каждый простой идеал будет главным. Поскольку каждый идеал раскладывается в произведение простых идеалов, отсюда следует, что $\mathbb{Z}_K$ есть кольцо главных идеалов и $h(K) = 1$. □

Существует лишь девять мнимых квадратичных полей $K = \mathbb{Q}(\sqrt{-d})$ с числом классов $h(K) = 1$. Это поля с

$$d = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

Повидимому существует бесконечное множество действительных квадратичных полей с числом классов 1. Такая гипотеза была высказана еще К.Ф. Гауссом и до сих пор не доказана.

1.14 Разложение простых чисел.

В этом параграфе мы рассмотрим, как разлагаются в произведения простых идеалов главные идеалы $(p) \subset \mathbb{Z}_K$, порожденные простыми числами $p \in \mathbb{Z}$. Это, очевидно, даст возможность получить разложение произвольного главного идеала (a), $a \in \mathbb{Z}$. Кроме того, при некоторых условиях будет найдена структура всех простых идеалов в $\mathbb{Z}_K$.

Напомним, что если $\mathfrak{p}$ - простой идеал в $\mathbb{Z}_K$, то $\mathfrak{p} \cap \mathbb{Z} = (p)$, где p - простое число. При этом поле вычетов $\mathbb{Z}_K/\mathfrak{p}$ есть конечное расширение F_p. Если f - степень этого расширения, то $N(\mathfrak{p}) = p^f$.

Теорема 13. *Пусть $p \in \mathbb{Z}$ - простое число и в кольце $\mathbb{Z}_K$ справедливо разложение*

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Тогда

$$\sum_{j=1}^{r} e_j f_j = [K : \mathbb{Q}],$$

где f_j - степень поля вычетов идеала $\mathfrak{p}_j$.

Доказательство. Для каждого из простых идеалов $\mathfrak{p}_j$ справедливо равенство $N(\mathfrak{p}_j) = p_j^{f_j}$. Пользуясь следствием 28 и мультипликативностью нормы идеала, находим

$$p^n = N(p) = N((p)) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r} = p^{e_1 f_1 + \cdots + e_r f_r}.$$

Это равенство завершает доказательство. □

Определение 32. *Показатель e_j в формулировке теоремы 13 называется индексом ветвления простого идеала $\mathfrak{p}_j$. Если $e_1 = \cdots = e_r = 1$, то говорят, что p не разветвлено в поле K.*

Можно доказать, что если $K \supset \mathbb{Q}$ - нормальное расширение, то в условиях теоремы 13 справедливы равенства

$$e_1 = \cdots = e_r = e, \qquad f_1 = \cdots = f_r = f,$$

так что $efr = [K : \mathbb{Q}]$.

Определение 33. *Пусть* $K = \mathbb{Q}(\theta)$, $\theta \in \mathbb{Z}_K$, $n = [K : \mathbb{Q}]$. *Тогда* $\mathbb{Z}[\theta]$ *есть аддитивная подгруппа в* $\mathbb{Z}_K$. *Индекс этой подгруппы будем называть индексом числа* θ *в* $\mathbb{Z}_K$.

Если d - индекс числа θ, то d есть порядок факторгруппы $\mathbb{Z}_K/\mathbb{Z}[\theta]$. Тоесть для каждого $\alpha \in \mathbb{Z}_K$ имеем $d\alpha \in \mathbb{Z}[\theta]$. Из леммы 24 следует, что число d равно абсолютной величине определителя матрицы $C = \|c_{i,j}\|_{1\le i,j\le n}$, $c_{i,j} \in \mathbb{Z}$, для которой выполняются равенства

$$\theta^{i-1} = \sum_{j=1}^{n} c_{i,j}\omega_j, \qquad 1 \le i \le n,$$

где $\omega_1, \ldots, \omega_n$ есть фундаментальный базис поля K. В частности, представление индекса в виде абсолютной величины определителя матрицы перехода означает равенство

$$D_\theta = d^2 \cdot D, \tag{1.48}$$

где D – дискриминант поля K, см. лемму 9.

В дальнейшем, как и ранее, мы будем предполагать, что $\theta \in \mathbb{Z}_K$ есть примитивный элемент поля K, $n = [K : \mathbb{Q}]$. Кроме того, в утверждениях будет присутствовать некоторое простое число p. Для каждого многочлена $u(x) \in \mathbb{Z}[x]$ будем обозначать символом $\overline{u}(x)$ многочлен в кольце $F_p[x]$, коэффициенты которого есть классы вычетов по модулю p соответствующих коэффициентов многочлена $u(x)$.

Лемма 26. *Пусть* $\mathfrak{p}$ - *простой идеал в кольце* $\mathbb{Z}_K$ *и* $\mathfrak{p} \cap \mathbb{Z} = (p)$, *где* p - *простое число. Если* $u(x), v(x) \in \mathbb{Z}[x]$ *таковы, что* $\overline{u}(x), \overline{v}(x)$ *взаимно просты в кольце* $F_p[x]$, *то либо* $u(\theta) \notin \mathfrak{p}$, *либо* $v(\theta) \notin \mathfrak{p}$.

Доказательство. Предположим, что $u(\theta) \in \mathfrak{p}$ и $v(\theta) \in \mathfrak{p}$. Так как многочлены $\overline{u}(x)$ и $\overline{v}(x)$ взаимно просты в кольце $F_p[x]$, то существуют многочлены $a(x), b(x) \in \mathbb{Z}[x]$, для которых выполняется равенство

$$1 = \overline{u}(x)\overline{a}(x) + \overline{v}(x)\overline{b}(x)$$

или равенство

$$1 = u(x)a(x) + v(x)b(x) + pc(x), \tag{1.49}$$

где $c(x)$ – некоторый многочлен с целыми коэффициентами. Подставляя в (1.49) число θ вместо x, находим

$$1 = u(\theta)a(\theta) + v(\theta)b(\theta) + pc(\theta),$$

что невозможно, так как $p \in \mathfrak{p}$ по условию и $u(\theta) \in \mathfrak{p}$, $v(\theta) \in \mathfrak{p}$ по предположению. □

Лемма 27. *Пусть* $\mathfrak{p}$ *- простой идеал в кольце* $\mathbb{Z}_K$ *и* $\mathfrak{p} \cap \mathbb{Z} = (p)$*, где* p *- простое число. Пусть* $\overline{g}(x)$ *неприводим в кольце* $F_p[x]$ *и* $g(\theta) \in \mathfrak{p}$*. Тогда* $[\mathbb{Z}_K/\mathfrak{p} : F_p] \geq \deg \overline{g}(x)$*.*

Доказательство. Пусть $d = \deg \overline{g}(x)$ и $\overline{\theta} = \theta \pmod{\mathfrak{p}} \in \mathbb{Z}_K/\mathfrak{p}$. Предположим, что элементы $1, \overline{\theta}, \ldots, \overline{\theta}^{d-1}$ линейно зависимы над F_p. Тогда существует такой многочлен $u(x) \in \mathbb{Z}[x]$, что

$$\deg u(x) \leq d-1, \qquad \overline{u} \neq 0, \qquad u(\theta) \in \mathfrak{p}. \tag{1.50}$$

Поскольку $g(\theta) \in \mathfrak{p}$, то по лемме 26 многочлены $\overline{u}(x)$ и $\overline{g}(x)$ должны иметь нетривиальный общий делитель. Но в силу (1.50) это противоречит неприводимость многочлена $\overline{g}(x)$. Это доказывает, что $[\mathbb{Z}_K/\mathfrak{p} : F_p] \geq d$. □

Теорема 14. *Пусть* p *- простое число, не делящее индекс числа* θ*,* $q_\theta(x)$ *- минимальный многочлен* θ*. Пусть также*

$$\overline{q}_\theta(x) = \prod_{j=1}^{r} \overline{g}_j(x)^{e_j}$$

- разложение на неприводимые множители над полем F_p *с некоторыми многочленами* $g_j(x) \in \mathbb{Z}[x]$*. Тогда* $\mathfrak{p}_j = (p, g_j(\theta))$*,* $j = 1, \ldots, r$*, - простые идеалы, и в кольце* $\mathbb{Z}_K$ *справедливо равенство*

$$(p) = \prod_{j=1}^{r} \mathfrak{p}_j^{e_j}. \tag{1.51}$$

Кроме того $\deg \mathfrak{p}_j$ *– степень поля вычетов идеала* $\mathfrak{p}_j$ *равна* $\deg \overline{g}_j(x)$*.*

Доказательство. Докажем сначала, что $(p, g_i(\theta))$ есть собственный идеал при каждом $j = 1, \ldots, r$. Если это не так, то с некоторыми числами $\xi, \eta \in \mathbb{Z}_K$ выполняется равенство

$$1 = p\xi + g_j(\theta)\eta. \tag{1.52}$$

Как указывалось выше, справедливы включения $d\xi, d\eta \in \mathbb{Z}[\theta]$, где d – индекс числа θ. Пусть $u(x), v(x) \in \mathbb{Z}[x]$ – многочлены, для которых $d\xi = u(\theta)$ и $d\eta = v(\theta)$. Из равенства (1.52) следует, что с некоторым многочленом $w(x) \in \mathbb{Z}[x]$ выполняется тождество

$$d = pu(x) + g_j(x)v(x) + q_\theta(x)w(x).$$

Приводя его по модулю p, находим

$$d = \overline{g}_j(x)\overline{v}(x) + \overline{q}_\theta(x)\overline{w}(x),$$

что невозможно, так как правая часть делится на $\overline{g}_j(x)$, а согласно условию $p \nmid d$, то-есть $d \neq 0$ в F_p.

Пусть теперь $\mathfrak{p}_j$ – какой-нибудь простой идеал, содержащий $(p, g_j(\theta))$. Если $\alpha \in \mathfrak{p}_j$, то $d\alpha \in \mathbb{Z}[\theta]$ и, значит, с некоторым многочленом $h(x) \in \mathbb{Z}[x]$ выполняется равенство $d\alpha = h(\theta)$. Поскольку $h(\theta) \in \mathfrak{p}_j$ и $g_j(\theta) \in \mathfrak{p}_j$, то согласно лемме 26 многочлены $\overline{h}(x)$ и $\overline{g}_j(x)$ в кольце $F_p[x]$ имеют нетривиальный общий делитель. Поскольку $\overline{g}_j(x)$ неприводим, заключаем, что $\overline{g}_j(x) \mid \overline{h}(x)$. Последнее свойство может быть переписано в виде $h(x) = g_j(x)s(x) + pr(x)$, где $r(x), s(x) \in \mathbb{Z}[x]$. Подставляя в это равенство θ вместо переменной x, находим

$$d\alpha = h(\theta) = g_j(\theta)s(\theta) + pr(\theta),$$

или $d\alpha \in (p, g_j(\theta))$. Учитывая, что целые числа p, d взаимно просты, можно утверждать, что с некоторыми целыми a, b выполняется равенство $1 = pa + db$ и, следовательно,

$$\alpha = pa\alpha + bd\alpha \in (p, g_j(\theta)).$$

Последнее включение означает, что $(p, g_j(\theta)) = \mathfrak{p}_j$ есть простой идеал.

Пусть теперь $\mathfrak{p}$ - произвольный простой идеал в кольце $\mathbb{Z}_K$, содержащий p. Из условия теоремы следует, что с некоторым многочленом $u(x) \in \mathbb{Z}[x]$ выполняется равенство

$$\prod_{j=1}^{r} g_j(x)^{e_j} = q_\theta(x) + pu(x).$$

Подставляя в него θ вместо x, и пользуясь равенством $q_\theta(\theta) = 0$, находим

$$\prod_{j=1}^{r} g_j(\theta)^{e_j} = pu(\theta) \in \mathfrak{p}. \tag{1.53}$$

Это включение, в силу простоты $\mathfrak{p}$, означает, что с некоторым индексом j выполняется $g_j(\theta) \in \mathfrak{p}$. Но тогда $\mathfrak{p}_j \subset \mathfrak{p}$ и $\mathfrak{p}_j = \mathfrak{p}$. Итак, простые идеалы $\mathfrak{p}_j$ и только они входят в разложение (p) в произведение простых идеалов

$$(p) = \prod_{j=1}^{r} \mathfrak{p}_j^{e'_j}. \tag{1.54}$$

Здесь e'_j – некоторые натуральные числа.

Обозначим степень поля вычетов идеала $\mathfrak{p}_j$ буквой f_j. Согласно лемме 27 выполняется неравенство $f_j \geq d_j = \deg \overline{g}_j(x)$. Для каждого $\alpha \in \mathbb{Z}_K$ будем обозначать символом $\overline{\alpha}$ класс вычетов $\alpha \pmod{\mathfrak{p}_j}$. Так как $\eta = d\xi \in \mathbb{Z}[\theta]$ и с определенными выше числами a, b выполняется равенство $\xi = pa\xi + b\eta$, то $\overline{\xi} = \overline{b\eta}$ и, следовательно, $\mathbb{Z}_K/\mathfrak{p}_j = \mathbb{Z}[\theta]/\mathfrak{p}_j$. Это равенство означает, что

$$\mathbb{Z}_K/\mathfrak{p}_j = F_p + F_p\overline{\theta} + \cdots + F_p\overline{\theta}^{d_j-1}.$$

Но тогда $f_j \leq d_j$ и, следовательно, $f_j = d_j$.

Так как $\deg \overline{q}_\theta = n$, то справедливо равенство

$$n = \sum_{j=1}^{r} e_j f_j. \tag{1.55}$$

С другой стороны, равенство (1.54) и теорема 13 означают, что

$$n = \sum_{j=1}^{r} e'_j f_j. \tag{1.56}$$

Покажем, что при любом j выполняется неравенство $e'_j \leq e_j$. Согласно (1.55) и (1.56) это приведет к равенствам $e'_j = e_j$, что и завершит доказательство теоремы.

Если при некотором j имеем $e'_j = 1$, то нужное неравенство при этом j, очевидно, выполняется. Пусть далее $e'_j \geq 2$. Выберем $\alpha \in \mathfrak{p}_j$ так, что $\nu_{\mathfrak{p}_j}(\alpha) = 1$. С некоторыми $\beta, \gamma \in \mathbb{Z}_K$ выполняется равенство

$$\alpha = \beta p + \gamma g_j(\theta).$$

Тогда

$$1 = \nu_{\mathfrak{p}_j}(\alpha) \geq \min\left(\nu_{\mathfrak{p}_j}(p), \nu_{\mathfrak{p}_j}(g_j(\theta))\right),$$

и, в силу $\nu_{\mathfrak{p}_j}(p) = e'_j \geq 2$, находим $\nu_{\mathfrak{p}_j}(g_j(\theta)) = 1$. Из равенства (1.53), поскольку $\nu_{\mathfrak{p}_j}(g_i(\theta)) = 0$ при $i \neq j$, теперь находим

$$e'_j = \nu_{\mathfrak{p}_j}(p) \leq e_j \nu_{\mathfrak{p}_j}(g_j(\theta)) = e_j.$$

Это завершает доказательство теоремы 14. □

Следствие 31. *Если поле $K = \mathbb{Q}(\theta)$ и примитивный элемент θ таковы, что $\mathbb{Z}_K = \mathbb{Z}[\theta]$, то утверждение теоремы 14 выполняется для любого простого числа p.*

Действительно, в этом случае индекс θ равен 1.

Теорема 15. *Пусть* $[K:\mathbb{Q}]=n, K=\mathbb{Q}(\theta), \theta\in\mathbb{Z}_K$ *и* p *- простое число,* $p\nmid D_\theta=\Delta(1,\theta,\ldots,\theta^{n-1})$. *Тогда* p *не разветвлено в поле* K.

Доказательство. Из (1.48) следует, что индекс d числа θ не делится на p. Поэтому в рассматриваемой ситуации можно применять теорему 14.

Пусть $\mathfrak{p}=(p,g(\theta))$ – один из простых идеалов, входящих в разложение (1.51) и e – соответствующий индекс ветвления. Многочлен $\overline{g}(x)\in F_p[x]$ неприводим.

Предположим, что $e\geq 2$. В соответствии с теоремой 14 справедливо равенство

$$q_\theta(x)=g(x)^2u(x)+pv(x),$$

где $u(x),v(x)$ – некоторые многочлены из $\mathbb{Z}[x]$. Дифференцируя это равенство по переменной x, и подставляя в результат $x=\theta$, находим

$$q'_\theta(\theta)=g(\theta)\alpha+pv'(\theta)\in\mathfrak{p},\qquad \alpha\in\mathbb{Z}_K.$$

Включение $q'_\theta(\theta)\in\mathfrak{p}$ означает, что $p\mid N(q'_\theta(\theta))$.

Пусть $\theta_1,\ldots,\theta_n$ – все числа, сопряженные с θ. Тогда

$$N(q'_\theta(\theta))=\prod_{i=1}^{n}q'_\theta(\theta_i)=(-1)^{n(n-1)/2}\prod_{1\leq i<j\leq n}(\theta_i-\theta_j)^2=$$
$$(-1)^{n(n-1)/2}(\det\|\theta_i^{k-1}\|_{1\leq i,k\leq n})^2=(-1)^{n(n-1)/2}D_\theta.$$

Так как по условию $p\nmid D_\theta$, то получаем противоречие, доказывающее, что в условиях теоремы неравенство $e\geq 2$ невозможно. □

Теорема 16. *Пусть* $K=\mathbb{Q}(\theta),\theta\in\mathbb{Z}_K$, D *- дискриминант поля* K, p *- простое число.*

1. Если $\nu_p(D_\theta)\leq 1$, *то* $p\nmid d$ *и* $\nu_p(D)=\nu_p(D_\theta)$.

2. Если $q_\theta(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0, p|a_i, p^2\nmid a_0$ *(условие Эйзенштейна), то* $\nu_p(D_\theta)=\nu_p(D)$.

Доказательство. Первое утверждение сразу же следует из равенства (1.48).

Для доказательства второго утверждения отметим, что если для индекса d числа θ выполняется равенство $\nu_p(d)=0$, то согласно (1.48) имеем $\nu_p(D_\theta)=\nu_p(D)$. Таким образом нужное утверждение выполняется. Поэтому далее будем считать, что $\nu_p(d)\geq 1$ и приведем это предположение к противоречию.

Индекс d обладает свойством $d\mathbb{Z}_K\subset\mathbb{Z}[\theta]$. Пусть a – наименьшее натуральное число, для которого $a\mathbb{Z}_K\subset\mathbb{Z}[\theta]$ и $\omega_1,\ldots,\omega_n$ – фундаментальный

базис поля K. Тогда $a\omega_i \in \mathbb{Z}[\theta]$ при любом i, т.е. с некоторыми целыми коэффициентами $c_{i,j}$ выполняются равенства

$$a\omega_i = \sum_{j=1}^{n} c_{i,j}\theta^{j-1}, \qquad i = 1, \ldots, n.$$

Из этих равенств следует, что

$$\Delta(a\omega_1, \ldots, a\omega_n) = (\det C)^2 D_\theta = (\det C)^2 d^2 D,$$

где $C = \|c_{i,j}\|$. С другой стороны

$$\Delta(a\omega_1, \ldots, a\omega_n) = a^{2n} D.$$

Сравнивая два получившихся выражения, находим, что $a^{2n} = (d \det C)^2$ и, согласно нашему предположению, $p \mid a$. Пусть $a = pa_1, 1 \leq a_1 < a$. Из определения a следует, что найдется число $\alpha \in \mathbb{Z}_K$ с условием $a_1\alpha \notin \mathbb{Z}[\theta]$. Учитывая, что $a_1 p\alpha \in \mathbb{Z}[\theta]$, получаем

$$\xi = a_1\alpha = \frac{b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}}{p},$$

где все b_i – целые числа, и по крайней мере одно из них не делится на p.

Пусть j – наименьшее число с условием $p \nmid b_j$. Обозначим $\zeta = b_j\theta^{n-1}/p$. Справедливо равенство

$$p\xi\theta^{n-j-1} = (b_0 + b_1\theta + \cdots + b_{j-1}\theta^{j-1})\theta^{n-j-1} + b_j\theta^{n-1} + \\ \theta^n(b_{j+1} + b_{j+2}\theta + \cdots + b_{n-1}\theta^{n-j-2}).$$

Из него, поскольку $p|b_i$, $i < j$, а также, поскольку согласно условию,

$$\frac{\theta^n}{p} = -\frac{a_{n-1}}{p}\theta^{n-1} - \cdots - \frac{a_0}{p} \in \mathbb{Z}[\theta] \subset \mathbb{Z}_K,$$

заключаем $\zeta = \frac{b_j\theta^{n-1}}{p} \in \mathbb{Z}_K$. Но тогда справедливо равенство

$$N(\zeta) = \left(\frac{b_j}{p}\right)^n N(\theta)^{n-1},$$

где $N(\zeta), N(\theta)$ – целые числа. Учитывая, что $p \nmid b_j$, заключаем, что $p^n \mid N(\theta)^{n-1}$ и, значит, $p^2 \mid N(\theta) = (-1)^n a_0$. Но это согласно условию невозможно. Таким образом, неравенство $d \geq 1$ приведено к противоречию, что завершает доказательство теоремы. $\square$

Глава 2

Задачи

2.1 Неприводимость многочленов над $\mathbb{Q}$

Для доказательства неприводимости многочленов полезны бывают следующие утверждения.

Теорема 17 (Критерий Эйзенштейна). *Пусть p - простое число и многочлен $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ таков, что $p|a_j$, $j \geq 0$ и $p^2 \nmid a_0$. Тогда $f(x)$ неприводим.*

Теорема 18. *Пусть $n \geq 2$ — целое число, $a \in \mathbb{Q}, a \neq 0$, причем для любого простого делителя p числа n уравнение $x^p = a$ не имеет решений в $\mathbf{Q}$. Пусть также, при $4 \mid n$ и уравнение $4x^4 + a$ не имеет рациональных решений. Тогда многочлен $x^n - a$ неприводим над $\mathbf{Q}$.*

Доказательство. См. [7], стр. 252. □

Иногда для доказательства неприводимости многочлена $f(x) \in \mathbb{Z}[x]$ используется следующее соображение. Если p - такое простое число, что многочлен $f(x) \pmod p \in F_p[x]$ неприводим, то $f(x)$ неприводим над полем рациональных чисел $\mathbb{Q}$.

1.1. Многочлен второй степени приводим тогда и только тогда, когда его дискриминант есть квадрат.

1.2. Многочлены $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ и $a \cdot f(x)$, $a \in \mathbb{Q}$, а также $f(x)$ и $g(x) = a_n^{n-1} f(x/a_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \cdot a_n^{n-1} \in \mathbb{Z}[x]$ приводимы или неприводимы одновременно.

1.3. Доказать, что многочлен $x^3 - x - 1$ неприводим.

1.4. Рациональные корни многочлена $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ содержатся среди чисел p/q, $p, q \in \mathbb{Z}, q > 0$, с условиями $p|a_0, q|a_n$.

1.5. Если многочлен $f(x) \in \mathbb{Z}[x]$ приводим, то он может быть разложен в произведение многочленов с целыми коэффициентами.

1.6. Доказать, что многочлен $x^4 - 2$ неприводим.

1.7. Если p - простое число, то многочлен $x^m - p$ неприводим. Из этого утверждения следует, что поле всех алгебраических чисел имеет бесконечную степень над $\mathbb{Q}$ (не является конечным расширением).

1.8. Доказать неприводимость многочлена $x^4 + 1$.

1.9. Доказать неприводимость многочлена $x^{p-1} + \cdots + x + 1$, при простом p.

1.10. Доказать критерий Эйзенштейна.

1.11. Доказать необходимость условий теоремы 18.

1.12. Доказать неприводимость многочленов $x^5 - x + 1$, $x^5 - 5x^4 - 6x - 1$.

1.13. Доказать неприводимость многочленов $x^5 - x^2 + 1$, $x^4 + x^3 + 1$, $x^4 + 2x^2 + x + 3$.

Следующие несколько задач посвящены доказательству утверждения, что *многочлен $x^p - x - a$, где p — простое число и a — целое число, не делящееся на p, неприводим.*

1.14. Доказать, что если $g(x)$ - неприводимый делитель $x^p - x - a$ в кольце $F_p[x]$, $\deg g(x) < p$, то при всех $j = 0, 1, \ldots, p-1$ многочлен $x^p - x - a$ делится в кольце $F_p[x]$ на $g(x + j)$. Здесь символом F_p обозначается поле из p элементов.

1.15. Доказать, что все многочлены $g(x + j)$ в кольце $F_p[x]$ различны.

1.16. Вывести из задач 2.1.14 и 2.1.15, что степень многочлена $g(x)$ равна 1.

1.17. Вывести из задач 2.1.14-2.1.16, что многочлен $x^p - x - a$ неприводим по модулю p. Доказать, что отсюда следует неприводимость $x^p - x - a$ над полем рациональных чисел.

2.2 Многочлены деления круга

Пусть n - натуральное и $\zeta = \exp(\frac{2\pi i}{n}) \in \mathbb{C}$. Определим многочлен

$$\Phi_n(x) = \prod_k (x - \zeta^k),$$

где произведение берется по всем целым k, $0 \le k \le n$, $(k, n) = 1$. Согласно определению $\deg \Phi_n(x) = \phi(n)$.

2.1. Доказать, что $x^n - 1 = \prod_{d|n} \Phi_d(x)$, и вывести отсюда, что $\Phi_n(x) \in \mathbb{Z}[x]$.

2.2. Доказать, что

$$\Phi_1(x) = x - 1,\ \Phi_2(x) = x + 1,\ \Phi_3(x) = x^2 + x + 1,\ \Phi_4(x) = x^2 + 1,$$
$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1,\ \Phi_6(x) = x^2 - x + 1.$$

2.3. Если p – простое число, то $\Phi_{p^{r+1}}(x) = \Phi_p(x^{p^r})$.
2.4. Если $n \geq 3$ нечетно, то $\Phi_{2n}(x) = \Phi_n(-x)$.
2.5. Если p – простое число, $p \nmid n$, то $\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$.
2.6. Справедливо тождество

$$\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)},$$

где $\mu(d)$ - функция Мебиуса.
2.7. Если $n = p_1^{r_1} \cdots p_s^{r_s}$ – разложение на неприводимые множители, то

$$\Phi_n(x) = \Phi_{p_1 \cdots p_s}(x^{p_1^{r_1 - 1} \cdots p_s^{r_s - 1}}).$$

2.8. Доказать неприводимость многочлена $\Phi_{p^k}(x)$, пользуясь критерием Эйзенштейна.

Следующие далее задачи доказывают, что при $n \geq 1$ все многочлены $\Phi_n(x)$ неприводимы над $\mathbb{Q}$.

2.9. Пусть $f(x) \in \mathbb{Q}[x]$ - неприводимый многочлен со старшим коэффициентом 1, корнем которого является ζ и $x^n - 1 = f(x) \cdot h(x)$. Тогда $f(x), h(x) \in \mathbb{Z}[x]$.

2.10. Пусть p - простое число, $p \nmid n$. Тогда многочлены $\overline{f}(x) = f(x) \pmod p$ и $\overline{h}(x) = h(x) \pmod p$ в $F_p[x]$ взаимно просты.

2.11. Многочлен $f(x)$ делит либо $f(x^p)$, либо $h(x^p)$.

2.12. Если $f(x) \mid h(x^p)$, то $\overline{f(x)}$ и $\overline{h(x)}$ имеют общий делитель в кольце $F_p[x]$.

2.13. Вывести из задач 2.2.10-2.2.12, что $f(x) \mid f(x^p)$ и, следовательно, ζ^p - корень многочлена $f(x)$.

2.14. Доказать, что если $\eta = \zeta^k$, $(k, n) = 1$, то $f(\eta) = 0$. Из последнего утверждения следует, что $f(x) = \Phi_n(x)$ и, значит, $\Phi_n(x)$ неприводим.

2.3 Конечные расширения

3.1. Число α есть корень многочлена $x^3 - x - 1$ и $\beta = 2\alpha^2 - \alpha$. Найти многочлен с коэффициентами из $\mathbb{Q}$, корнем которого является β.

3.2. Представить число $\alpha = \frac{1}{\sqrt[3]{4} - \sqrt[3]{2} + 3}$ в виде $r_0 + r_1\sqrt[3]{2} + r_2\sqrt[3]{4}$, $r_j \in \mathbb{Q}$.

3.3. Найти степень порождающего элемента для расширений:
1) $\mathbb{Q}(\sqrt[5]{3}) \supset \mathbb{Q}$, 2) $\mathbb{Q}(e^{2\pi i/5}) \supset \mathbb{Q}$, 3) $F_7(i) \supset F_7$, где i - корень многочлена $x^2+1 \in F_7[x]$, 4) $\mathbb{Q}(z) \supset \mathbb{Q}\left(\frac{z^3}{z+1}\right)$.

3.4. Может ли $\sqrt[2]{2} \in \mathbb{Q}(\sqrt[3]{2})$?

3.5. Доказать, что при $n \geq 3$ поле алгебраических чисел нечетной степени не может содержать примитивный корень n-й степени из 1.

3.6. Доказать, что поля $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt{3})$ различны. Вывести отсюда, что $\deg(\sqrt{2}+\sqrt{3}) = 4$.

3.7. Пусть $\alpha, \alpha_1, \ldots, \alpha_m \in \mathbb{Q}$, $m \geq 0$. Доказать с помощью индукции по m, что если

$$\sqrt{\alpha} \in \mathbb{Q}(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_m}),$$

то с некоторым $\gamma \in \mathbb{Q}$ и целыми $k_1, \ldots, k_m$, $0 \leq k_j \leq 1$, выполняется равенство

$$\alpha = \alpha_1^{k_1} \cdots \alpha_m^{k_m} \gamma^2.$$

3.8. Доказать с помощью задачи 2.3.7, что для любых различных простых чисел $p_j, j = 1, \ldots, m$, имеем

$$[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m}) : \mathbb{Q}] = 2^m.$$

Справедливо и более общее утверждение: Если $a_j = p_j q_j \in \mathbb{Q}, j = 1, \ldots, r$, где $p_1, \ldots, p_m$ — различные простые числа, а числители и знаменатели всех рациональных чисел q_j взаимно просты с $p_1 \cdots p_m$, то

$$[\mathbf{Q}(\sqrt{a_1}, \ldots, \sqrt{a_m}) : \mathbf{Q}] = 2^m.$$

Композитом подполей K и L поля E называется наименьшее подполе E, содержащее эти поля (обозначение KL). Если $K = \mathbb{Q}(\xi)$, $L = \mathbb{Q}(\eta)$, то $KL = \mathbb{Q}(\xi, \eta)$.

3.9. Доказать, что

$$\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

3.10. Пусть $\zeta = e^{2\pi i/3}$, $\alpha = \zeta\sqrt[3]{2}$ и $\beta = \zeta^2\sqrt[3]{2}$. Обозначим

$$E = \mathbb{Q}(\alpha), \quad F = \mathbb{Q}(\beta).$$

Найти $[E : \mathbf{Q}], [F : \mathbf{Q}], [EF : F], [EF : E], [EF : \mathbb{Q}], [E \cap F : \mathbf{Q}]$.

Далее при любом целом $m \geq 1$ будет использоваться обозначение $\zeta_m = e^{2\pi i/m}$.

3.11. Доказать, что при $(m,n) = 1$ композит полей $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$ равен $\mathbb{Q}(\zeta_{mn})$.

3.12. Пусть натуральные числа m, n взаимно просты. Доказать, что

$$[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_m)] = \varphi(n).$$

Две последние задачи означают, что многочлен $\Phi_n(x)$ неприводим над полем $\mathbb{Q}(\zeta_m)$ при $(m,n) = 1$.

3.13. С помощью задачи 2.3.12 доказать, что $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

3.14. Пусть $F = \mathbb{Q}(\zeta_n)$, $n \geq 3$, и $K = \mathbb{Q}(\cos\frac{2\pi}{n})$. Докажите, что $K \subset F$ и $[K : \mathbb{Q}] = \varphi(n)/2$, т.е. $\cos\frac{2\pi}{n}$ есть алгебраическое число степени $\varphi(n)/2$.

2.4 Нормальные расширения. Группа Галуа.

4.1. Пусть $F = \mathbb{Q}(\sqrt[3]{2})$. Найти поля, сопряженные с F. Пусть E - одно из этих полей, отличное от F. Найти $E \cap F$ и EF. Вычислить $[E : \mathbb{Q}]$ и $[EF : F]$.

4.2. Пусть $E = \mathbb{Q}(\sqrt[4]{2})$ и $F = \mathbb{Q}(\sqrt{2})$.

4.2.1. Найти $[E : F]$.

4.2.2. Проверить, что расширения $E \supset F$ и $F \supset \mathbb{Q}$ нормальны, но $E \supset \mathbb{Q}$ не нормально.

4.2.3. Пусть σ – такой автоморфизм поля F, что $\sigma(\sqrt{2}) = -\sqrt{2}$. Построить все продолжения σ на поле E.

4.3. Пусть K – алгебраическое числовое поле и E – поле разложения некоторого многочлена $f(x) \in K[x]$. Доказать, что расширение $E \supset K$ нормально. Доказать обратное утверждение, что любое нормальное расширение поля K есть поле разложения некоторого многочлена.

4.4. Пусть многочлен $f(x) \in K[x]$ не имеет кратных корней и E – поле разложения $f(x)$; пусть также $x_1, \ldots, x_n$ – корни $f(x)$ в E, т.е. $E = K(x_1, \ldots, x_n)$. Доказать, что для любого автоморфизма τ поля E над K набор чисел $(\tau(x_1), \ldots, \tau(x_n))$ является перестановкой множества $(x_1, \ldots, x_n)$, причем разным автоморфизмам соответствуют разные перестановки. Таким образом, группа автоморфизмов поля E над K вкладывается в группу S_n подстановок на n элементах.

4.5. Пусть $f(x) = x^3 + px + q \in K[x]$ – неприводимый многочлен, x_1, x_2, x_3 – его корни и $E = K(x_1, x_2, x_3)$. Обозначим

$$\delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$$

и $\Delta = \delta^2$.

2.4.5.1. Проверить, что Δ не меняется под действием любого автоморфизма поля E над K и потому $\Delta \in K$. Доказать, что $\Delta = -4p^3 - 27q^2$.

2.4.5.2. Доказать, что если $\delta \notin K$, то $[E : K] = 6$, и в этом случае группа автоморфизмов поля E над K совпадает с S_3.

2.4.5.3. Пусть группа автоморфизмов E над K совпадает с S_3 и σ – автоморфизм E соответствующий подстановке (x_1, x_2). Проверить, что $\sigma(\delta) = -\delta$ и, следовательно, $\delta \notin K$.

2.4.5.4. Доказать, что группа автоморфизмов поля E над K совпадает с подгруппой четных подстановок A_3 тогда и только тогда, когда $\Delta = \gamma^2, \gamma \in K$. В этом случае она циклична и порождается автоморфизмом, соответствующим перестановке (x_1, x_2, x_3).

4.6. Вычислить группу Галуа многочлена $x^3 - 9x - 9 \in \mathbb{Q}[x]$. Будет ли нормальным поле $\mathbb{Q}(\alpha)$, где α - корень этого многочлена. В случае нормальности найти выражение двух других корней данного многочлена через α.

4.7. Вычислить группу Галуа многочлена $x^3 - x - 1 \in \mathbb{Q}[x]$. Будет ли нормальным поле $\mathbb{Q}(\alpha)$, где α - корень этого многочлена.

4.8. Вычислить группу Галуа многочлена $x^3 - 2x - 2$. Будет ли нормальным поле $\mathbb{Q}(\alpha)$, где α - корень этого многочлена.

4.9. Верны ли утверждения задачи 4.5 для конечного поля F_p при $p \neq 2, 3$?

4.10. Пусть $f(x) = x^4 - 3$.

2.4.10.1. Доказать, что $f(x)$ неприводим над $\mathbb{Q}$ и, что $K = \mathbb{Q}(\theta, i)$, где $\theta = \sqrt[4]{3}$ есть поле разложения для $f(x)$.

2.4.10.2. Доказать, что $[K : \mathbb{Q}] = 8$, и, следовательно порядок группы Галуа G поля K над $\mathbb{Q}$ равен 8. Вычислить степени $[K : \mathbb{Q}(\theta)]$ и $[K : \mathbb{Q}(i)]$.

2.4.10.3. Пусть автоморфизмы $\tau, \sigma \in G$, определены равенствами

$$\tau(\theta) = \theta,\ \tau(i) = -i, \qquad \sigma(i) = i,\ \sigma(\theta) = i\theta.$$

Вычислить порядки этих автоморфизмов в G. Доказать, что $\tau \notin (\sigma)$, что $G = (\sigma, \tau)$ и, что $\tau\sigma = \sigma^3\tau$.

4.11. Пусть p - нечетное простое число, $\zeta = e^{2\pi i/p}$, $K = \mathbb{Q}(\zeta)$. Следующие задачи вычисляют все подполя K.

2.4.11.1. Доказать, что $[K : \mathbb{Q}] = p - 1$ и поле K нормально. Сопряженные ζ есть ζ^k, $1 \leq k < p$. Обозначим G - группу Галуа поля K над $\mathbb{Q}$.

Для каждого $k \in \mathbb{Z}, 1 \leq k \leq p-1$, определим $\sigma_k \in G$ так, что $\sigma_k(\zeta) = \zeta^k$. Проверить, что $\sigma_u \sigma_v = \sigma_w$, где $w \equiv uv \pmod{p}$.

2.4.11.2. Предыдущая задача устанавливает изоморфизм между G и $(\mathbb{Z}/p\mathbb{Z})^*$. Пусть g - первообразный корень по модулю p. Доказать, что группа G циклическая и $\tau = \sigma_g$ есть ее образующая.

2.4.11.3. Пусть $p-1 = rf$. Доказать, что группа G имеет единственную подгруппу порядка f и она порождается τ^r.

2.4.11.4. Пусть F_r - подполе неподвижных элементов группы (τ^r). Доказать, что $[F_r : \mathbb{Q}] = r$.

2.4.11.5. Обозначим $\zeta_0 = \zeta$ и определим $\zeta_{k+1} = \tau(\zeta_k)$. Пусть также

$$\eta_k = \zeta_k + \zeta_{k+r} + \ldots + \zeta_{k+(f-1)r}, \qquad k = 0, 1, \ldots, r-1.$$

(эти числа называются Гауссовыми периодами). Доказать, что

$$\tau_r(\eta_k) = \eta_k,$$

и, следовательно, $\eta_k \in F_r$, $k = 0, \ldots r-1$.

2.4.11.6. Доказать, что числа $\eta_0, \ldots, \eta_{r-1}$ линейно независимы над $\mathbb{Q}$, и, следовательно, образуют базис F_r над $\mathbb{Q}$. Вместе с тем $\eta_0 + \cdots + \eta_{r-1} = -1$.

2.4.11.7. Доказать, что числа η_k сопряжены над $\mathbb{Q}$, так что степень η_0 над $\mathbb{Q}$ равна r. Вывести отсюда, что $F_r = \mathbb{Q}(\eta_0)$.

4.12. Найти все подполя $\mathbb{Q}(e^{2\pi i/5})$ и $\mathbb{Q}(e^{2\pi i/7})$.

4.13. В этой задаче при $r = 2$ разбирается некоторый способ вычисления минимального многочлена для гауссовых периодов. Будут использованы обозначения из 2.4.11.

2.4.13.1. Доказать, что

$$\eta_0 \eta_1 = \sum_{a=0}^{p-1} \nu(a) \zeta^a,$$

где $\nu(a)$ есть количество представлений a в виде $a \equiv g^u + g^v \pmod{p}$, $1 \leq u, v < p$, u четно, v нечетно.

2.4.13.2. Доказать, что при a, не делящемся на p, имеет место равенство $\nu(a) = \nu(ag)$. Вывести отсюда, что $\nu(a) = \nu(1)$ при любом a, не делящемся на p.

2.4.13.3. Доказать, что

$$\nu(0) = \begin{cases} 0 & \text{если } p \equiv 1 \pmod 4, \\ \frac{p-1}{2} & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

2.4.13.4. Пользуясь результатами задач 2.4.13.1-2.4.13.3 доказать, что

$$\eta_0\eta_1 = \begin{cases} \frac{1-p}{4} & \text{если } p \equiv 1 \pmod 4, \\ \frac{p+1}{4} & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Пользуясь результатом задачи 4.11.6 найти минимальный многочлен чисел η_0, η_1 над $\mathbb{Q}$.

4.14.1. Доказать, что

$$\Sigma = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k = \eta_0 - \eta_1,$$

где $\left(\frac{k}{p}\right)$ - символ Лежандра и η_0, η_1 вычислены при $r = 2$, см. задачу 2.4.11. Сумма Σ называется суммой Гаусса.

2.4.14.2. Доказать, что $\Sigma^2 = \left(\frac{-1}{p}\right) p$. Это показывает, что $\sqrt{p} \in K$ при $p \equiv 1 \pmod 4$ и $\sqrt{-p} \in K$ при $p \equiv 3 \pmod 4$.

2.5 Модули и кольца множителей

В этом параграфе будут использоваться следующие ниже обозначения:

d – целое свободное от квадратов число, т.е. число, не делящееся на квадрат никакого простого числа;

$K = \mathbb{Q}(\sqrt{d})$ – квадратичное расширение поля рациональных чисел. Каждый элемент K единственным способом представим в виде $u+v\sqrt{d}$, где $u, v \in \mathbb{Q}$;

α' – число, сопряженное с $\alpha = u + v\sqrt{d}$, а именно $\alpha' = u - v\sqrt{d}$;

$Tr(\alpha) = \alpha + \alpha' = 2u$ – след α;

$N(\alpha) = \alpha \cdot \alpha' = u^2 - dv^2$ – норма α;

Если α, α' - корни многочлена $at^2 + bt + c$, $a, b, c \in \mathbb{Z}$, $(a, b, c) = 1$, $a > 0$, то справедливы равенства $Tr(\alpha) = -\frac{b}{a}$, $N(\alpha) = \frac{c}{a}$. Величина $D(\alpha) = b^2 - 4ac$ называется дискриминантом α.

$\mathbb{Z}_K$ – кольцо целых чисел поля K. Справедливо равенство

$$\mathbb{Z}_K = \{1, \omega\} = \mathbb{Z} + \mathbb{Z}\omega,$$

где

$$\omega = \begin{cases} \sqrt{d} & \text{если} \quad d \equiv 2, 3 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{если} \quad d \equiv 1 \pmod 4, \end{cases}$$

D_M – дискриминант полного модуля $M = \{\xi, \eta\}$, равный

$$D_M = \det \begin{pmatrix} Tr(\xi^2) & Tr(\xi\eta) \\ Tr(\eta\xi) & Tr(\eta^2) \end{pmatrix} = \det \begin{pmatrix} \xi & \xi' \\ \eta & \eta' \end{pmatrix}^2.$$

$D = D_{\mathbb{Z}_K}$ – дискриминант поля K. Имеем

$$D = \begin{cases} 4d, & \text{если} \quad d \equiv 2,3 \pmod 4, \\ d, & \text{если} \quad d \equiv 1 \pmod 4. \end{cases}$$

Базис каждого модуля M может быть линейно выражен через базис кольца множителей E_M с коэффициентами в $\mathbb{Q}$. Абсолютная величина определителя матрицы коэффициентов в этом выражении не зависит от выбора базисов и называется *нормой модуля* M. Она обозначается $N(M)$.

5.1. Доказать, что для любого полного модуля $M = \{\xi, \eta\} \subset K$ существует такое целое число $f > 0$, что $E_M = \{1, f\omega\}$.

Эта задача дает описание всех порядков квадратичного поля.

5.2. Пусть $M = \{1, \gamma\}$, где γ есть корень многочлена $at^2 + bt + c \in \mathbb{Z}[t]$, причем $(a, b, c) = 1, a > 0$. Тогда

$$E_M = \{1, a\gamma\} \qquad D_{E_M} = b^2 - 4ac, \qquad N(M) = \frac{1}{a}.$$

Для каждого $\alpha \in K$ и модуля $M = \{\xi, \eta\}$ будем обозначать αM модуль $\{\alpha\xi, \alpha\eta\}$.

5.3. Пусть M - произвольный полный модуль в поле K и $\alpha \in K, \alpha \neq 0$. Тогда $E_{\alpha M} = E_M$ и $N(\alpha M) = |N(\alpha)| \cdot N(M)$. В частности, $N(\alpha E_M) = |N(\alpha)|$.

Две последние задачи позволяют вычислять кольцо множителей и норму любого модуля.

5.4. Найти кольца множителей для модулей

$$\{1, \sqrt{15}\}, \quad \{2, 1 + \sqrt{15}\}, \quad \{3, \sqrt{15}\}, \quad \{35, 20 + \sqrt{15}\}$$

в поле $\mathbb{Q}(\sqrt{15})$ и их нормы.

5.5. Найти кольца множителей для модулей

$$\{11, 6 + 2i\sqrt{2}\}, \quad \{2, 1 + i\sqrt{2}\}, \quad \{4, i\sqrt{2}\}, \quad \{2, i\sqrt{2}\}$$

в поле $\mathbb{Q}(\sqrt{-2})$ и их нормы.

Дробным идеалом поля K называется модуль M, для которого $E_M = \mathbb{Z}_K$. *Идеалом* называется дробный идеал, содержащийся в $\mathbb{Z}_K$.

5.6. Какие из модулей задач 2.5.4, 2.5.5 являются идеалами в соответствующих кольцах целых чисел.

Два модуля M_1 и M_2 из поля K называются *подобными*, если существует $\alpha \in K, \alpha \neq 0$, для которого $M_1 = \alpha M_2$. Модули подобны в узком смысле, если $N(\alpha) > 0$. Подобие есть отношение эквивалентности.

Модули разбиваются на классы подобных между собой. Из задачи 2.5.3 следует, что кольца множителей подобных модулей совпадают.

5.7. Если $M = \{\xi, \eta\} = \{\alpha, \beta\}$, то с некоторыми целыми числами a, b, c, d выполняется равенство

$$\xi = a\alpha + b\beta, \qquad \eta = c\alpha + d\beta, \tag{2.1}$$

причем $ad - bc = \pm 1$.

5.8. Два модуля $M_1 = \{1, \alpha\}$ и $M_2 = \{1, \beta\}$ подобны тогда и только тогда, когда $\alpha = \frac{a\beta+b}{c\beta+d}$, где $a, b, c, d \in \mathbb{Z}$ и $ad - bc = 1$ (такие числа α и β называются *эквивалентными*). В этом случае $M_1 = \frac{1}{c\beta+d} \cdot M_2$.

В следующих задачах описываются алгоритмы, позволяющие определить, будут данные два модуля поля $K = \mathbb{Q}(\sqrt{d})$ подобны или нет. Эти алгоритмы отличаются в случае комплексного ($d < 0$) и действительного ($d > 0$) поля K. Сначала мы рассмотрим случай комплексных полей.

Определение 34. *Комплексное число γ называется приведенным, если*

1. $\Im\gamma > 0$,

2. $-\frac{1}{2} < \Re\gamma \leq \frac{1}{2}$,

3. При $-\frac{1}{2} < \Re\gamma < 0$ *выполнено неравенство* $|\gamma| > 1$, *а при* $0 \leq \Re\gamma \leq \frac{1}{2}$ *- неравенство* $|\gamma| \geq 1$. *Модуль* $M = \{1, \gamma\}$ *называется приведенным, если* γ *- приведенное число.*

5.9. Для любого $\alpha \in \mathbb{C}$ определим последовательность чисел $\alpha_0 = \alpha$ и $\alpha_{k+1} = -\frac{1}{\alpha_k} + n_k, k \geq 1$, где целое число n_k выбирается так, что $-\frac{1}{2} < \Re\alpha_{k+1} \leq \frac{1}{2}$. Докажите следующие утверждения

2.5.9.1. Каждое из чисел $\alpha_k, k \geq 0$, представимо в виде $\alpha_k = \frac{a\alpha+b}{c\alpha+d}$ с целыми a, b, c, d, удовлетворяющими условию $ad - bc = 1$.

2.5.9.2. В обозначениях предыдущего пункта справедливо равенство

$$\Im\alpha_k = \frac{\Im\alpha}{|c\alpha + d|^2}.$$

2.5.9.3. Существует индекс m для которого выполняется неравенство $\Im\alpha_{m+1} \leq \Im\alpha_m$.

2.5.9.4. По крайней мере одно из двух чисел α_m, α_{m+1} будет приведенным. Таким образом, последовательность α_k, $k \geq 0$, содержит приведенное число.

5.10. Докажите, что если числа α, β приведены и эквивалентны, то $\alpha = \beta$.

5.11. Какие из содержащихся в поле $\mathbb{Q}(\sqrt{-5})$ модулей

$$\{2, 1+\sqrt{-5}\}, \quad \{3, 1-\sqrt{-5}\}, \quad \{1, \sqrt{-5}\}, \quad \{3, 1+\sqrt{-5}\}$$

подобны?

5.12. Какие из содержащихся в поле $\mathbb{Q}(\sqrt{-23})$ модулей

$$\{2, 1+\sqrt{-23}\}, \qquad \{4, 1+\sqrt{-23}\}, \qquad \{4, 3+\sqrt{-23}\}$$

подобны?

5.13. Если

$$\alpha = \frac{a\beta+b}{c\beta+d}, \qquad \beta = \frac{p\gamma+q}{r\gamma+s}, \quad \text{то} \quad \alpha = \frac{u\gamma+v}{w\gamma+t},$$

где коэффициенты u, v, w, t определяются матричным равенством

$$\begin{pmatrix} u & v \\ w & t \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

5.14. Пусть $\omega = \frac{1+\sqrt{-19}}{2} \in \mathbb{Q}(\sqrt{-19})$. Какие из модулей

$$\mathfrak{a}_1 = \{5, \omega-1\}, \qquad \mathfrak{a}_2 = \{7, \omega+1\}, \qquad \mathfrak{a}_3 = \{11, \omega+2\}$$

есть главные идеалы в кольце целых чисел поля $\mathbb{Q}(\sqrt{-19})$? Найти образующие главных идеалов.

5.15. Будут ли идеалами следующие модули

$$\{3, 1+\sqrt{-14}\}, \qquad \{3, 2+\sqrt{-14}\}$$

в поле $\mathbb{Q}(\sqrt{-14})$? Подобны ли они? Чему равны их нормы?

5.16. Установить, что модули

$$\{3, \sqrt{-5}-1\}, \quad \{3, \sqrt{-5}+1\}, \quad \{7, 3+\sqrt{-5}\}, \quad \{7, 3-\sqrt{-5}\}$$

являются идеалами в кольце целых чисел поля $\mathbb{Q}(\sqrt{-5})$. Вычислить их нормы. Доказать, что каждые два из них подобны друг другу. Вычислить коэффициенты подобия.

Следующие далее задачи посвящены подобию модулей в действительных квадратичных полях. Как и в комплексном случае, имеется алгоритм приведения, позволяющий устанавливать подобие модулей и находить коэффициент подобия. Этот алгоритм основан на свойствах цепных дробей. Необходимые теоретические сведения сформулированы ниже в

виде теорем 19-21. Доказательства их можно найти, например, в книге [8].

Пусть $\alpha \in \mathbb{R}$. Положим $\alpha_0 = \alpha$ и определим

$$a_n = [\alpha_n], \qquad \alpha_{n+1} = \frac{1}{\alpha_n - a_n}, \qquad n = 0, 1, 2, \ldots.$$

Если α иррационально, таким способом определяется бесконечная последовательность целых чисел, $[a_0; a_1, a_2, \ldots]$, называемая *цепной дробью* числа α.

Несократимые дроби $\frac{p_n}{q_n}$, определяемые равенствами

$$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}},$$

называются *подходящими дробями* цепной дроби α. Они вычисляются по формулам $q_{-1} = 0, p_{-1} = 1, q_0 = 1, p_0 = a_0$ и

$$p_n = a_n p_{n-1} + p_{n-2}, \qquad q_n = a_n q_{n-1} + q_{n-2}, \qquad n \geq 1.$$

При каждом $n \geq 1$ справедливы равенства

$$\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}, \qquad \alpha_n = \frac{-q_{n-2}\alpha + p_{n-2}}{q_{n-1}\alpha - p_{n-1}},$$

или в символической записи

$$\begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \begin{pmatrix} p_{n-1}, p_{n-2} \\ q_{n-1}, q_{n-2} \end{pmatrix} \begin{pmatrix} \alpha_n \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} \alpha_n \\ 1 \end{pmatrix} = \begin{pmatrix} -q_{n-2}, p_{n-2} \\ q_{n-1}, -p_{n-1} \end{pmatrix} \begin{pmatrix} \alpha \\ 1 \end{pmatrix},$$

удобной с вычислительной точки зрения: при подстановке дробно-линейных выражений друг в друга соответствующие матрицы перемножаются, см. задачу 2.5.13.

Цепная дробь называется *периодической*, если существует такое натуральное k, что для всех достаточно больших n выполняется равенство $a_{n+k} = a_n$, и *чисто периодической*, если последнее равенство выполняется для всех $n \geq 0$.

Теорема 19. *Пусть α - действительное иррациональное число. Цепная дробь числа α периодична тогда и только тогда, когда α - квадратичная иррациональность.*

В действительном случае квадратичная иррациональность α называется *приведенной*, если $\alpha > 1$ и $-1 < \alpha' < 0$.

5.17. Пусть, как и ранее, $\omega = \begin{cases} \sqrt{d} & \text{если, } d \equiv 2,\ 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{если, } d \equiv 1 \pmod 4. \end{cases}$

Докажите, что число $\omega_1 = (\omega - [\omega])^{-1}$ приведено.

5.18. Пусть α - действительное иррациональное число и β определено равенством $\alpha = [\alpha] + \beta^{-1}$. Тогда $D(\alpha) = D(\beta)$.

Теорема 20. *Цепная дробь числа α чисто периодична тогда и только тогда, когда α - приведенная квадратичная иррациональность.*

Теорема 21. *Пусть α, β - действительные иррациональности. Они эквивалентны тогда и только тогда, когда их разложения в цепные дроби, начиная с некоторых мест, совпадают. В частности, для квадратичных иррациональностей эквивалентность равносильна совпадению периодов.*

5.19. Какие из модулей задачи 2.5.4 подобны между собой?

5.20. Доказать, что модули

$$\{2, -1 + \sqrt{7}\}, \qquad \{3, -1 + \sqrt{7}\}$$

в поле $\mathbb{Q}(\sqrt{7})$ есть главные идеалы и найти их образующие.

5.21. Найти в поле $\mathbb{Q}(\sqrt{10})$ два идеала, не подобных друг другу.

2.6 Единицы

Число $\varepsilon \in E$ называется единицей кольца E, если $\varepsilon^{-1} \in E$. Единицы кольца E образуют группу. Число $\varepsilon \in \mathbb{Z}_K$ есть единица в том и только том случае, когда $N(\varepsilon) = \pm 1$.

6.1. Найти единицы в кольцах целых чисел полей $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$ и $\mathbb{Q}(\sqrt{d})$, где $d < 0, d \neq -1, -3$.

При $d > 0$ группа Γ бесконечна и имеет вид $\Gamma = \{\pm\varepsilon_0^n,\ n \in \mathbb{Z}\}$. Для нахождения образующей ε_0 группы Γ применимо следующее утверждение

Теорема 22. *Пусть α приведенная иррациональность дискриминанта $D > 0$ (дискриминант поля $K = \mathbb{Q}(\sqrt{d})$), k - длина наименьшего периода непрерывной дроби, соответствующей числу α. Определим числа u, v равенствами*

$$u = p_{k-1} + q_{k-2}, \qquad v = (q_{k-1}, p_{k-1} - q_{k-2}, p_{k-2}).$$

Тогда число $\varepsilon = \frac{u+v\sqrt{D}}{2}$ *является единицей* $\varepsilon > 1$ *и порождает группу всех единиц кольца* $\mathbb{Z}_K$. *При этом* $N(\varepsilon) = (-1)^k$.

6.2. Найти группы единиц в кольцах целых чисел полей $\mathbb{Q}(\sqrt{d})$ при $d = 2, 11, 14, 58$ и нормы основных единиц.

6.3. Найти группы единиц в кольцах целых чисел полей $\mathbb{Q}(\sqrt{d})$ при $d = 17, 29, 33$ и нормы основных единиц.

2.7 Идеалы, группа классов идеалов

Пусть $K = \mathbb{Q}(\sqrt{d})$, где d - целое число, не делящееся на квадрат простого числа, $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\omega$ и $f(x)$ – минимальный многочлен числа ω. Следующее утверждение есть частный случай теоремы 14.

Теорема 23. *Пусть* p *– простое число. Если многочлен* $f(x) \pmod p$ *неприводим над полем* F_p, *то главный идеал* (p) *– прост в кольце* $\mathbb{Z}_K$ *и имеет степень 2. Если* $f(x) \equiv (x-a)(x-b) \pmod p$, *то идеалы* $\mathfrak{p}_1 = (p, \omega - a)$ *и* $\mathfrak{p}_2 = (p, \omega - b)$ *просты и имеют степень* 1. *При этом* $(p) = \mathfrak{p}_1\mathfrak{p}_2$ *в кольце* $\mathbb{Z}_K$.

Заметим, что в случае $a = b$ справедливо разложение $(p) = \mathfrak{p}_1^2$.

7.1. Разложить простые числа $2, 3, 5, 7$ в произведение простых идеалов в квадратичных полях $\mathbb{Q}(\sqrt{d})$ при $d = -1, 2, -3, 5, -7$.

7.2. Разложить в произведение простых идеалов в поле $\mathbb{Q}(\sqrt{-19})$ числа $2, 3$. Проверить, что все получившиеся при этом простые идеалы будут главными.

Мультипликативная группа дробных идеалов раскладывается в объединение смежных классов по подгруппе главных идеалов. Доказательство следующего утверждения, несколько более сильного, чем теорема 12, можно найти в книге [6], гл. 5, теорема 4.

Теорема 24. *Пусть* $K = \mathbb{Q}(\theta)$ *– конечное расширение поля рациональных чисел. Каждый класс содержит идеал, норма которого не превосходит*

$$\left(\frac{4}{\pi}\right)^t \cdot \frac{n!}{n^n}\sqrt{|D|},$$

где D *– дискриминант поля* K *и* t *– количество пар комплексно сопряженных среди корней минимального многочлена числа* θ. *Множество классов идеалов поля* K *конечно.*

Количество классов идеалов называется числом классов поля K. Число классов поля K равно 1 тогда и только тогда, когда в кольце $\mathbb{Z}_K$ имеет место единственность разложения на неприводимые элементы.

7.3. Доказать, что числа классов полей $\mathbb{Q}(\sqrt{d})$ при

а) $d = 2, 3, 5, 13$;

б) $d = -1, -2, -3, -7$.

равны 1.

7.4. Найти число классов и представителей всех классов идеалов полей $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-23})$.

7.5. Найти число классов и представителей всех классов идеалов полей $\mathbb{Q}(\sqrt{-6})$, $\mathbb{Q}(\sqrt{-14})$.

7.6. Найти число классов и представителей всех классов идеалов полей $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{17})$.

Литература

[1] Боревич З.И., Шафаревич И.Р., Теория чисел, М., Наука, 1972.

[2] ван дер Варден Б.Л., Алгебра, М., Наука, 1976.

[3] Гекке Э., Лекции по теории алгебраических чисел, М., Гостехиздат, 1940.

[4] Зарисский О., Самюэль П., Коммутативная алгебра, т.1, М., Иностранная литература, 1963.

[5] Касселс Дж., Введение в геометрию чисел, М., Мир, 1965.

[6] Ленг С., Алгебраические числа, М., Мир, 1966.

[7] Ленг С., Алгебра, М., Мир, 1968.

[8] Ленг С., Введение в теорию диофантовых приближений, М., Мир, 1970.