Ж.-П. Серр

КУРС АРИФМЕТИКИ

ИЗДАТЕЛЬСТВО «МИР» . Москва 1972

Современный университетский учебник повышенного типа по теории чисел. Сжатое, но весьма содержательное изложение ведется с позиции современной алгебры; развиваются теория конечных полей, теория *p*-адических чисел, локальная теория квадратичных форм, начальные сведения из теории *L*-рядов с теоремой Дирихле о прогрессии, элементы теории модулярных форм.

Автор — выдающийся французский математик; вышедшие в русском переводе его книги: «Алгебраические группы и поля классов», «Когомологии Галуа» («Мир», 1968), «Алгебры Ли и группы Ли» («Мир», 1969), «Линейные представления конечных групп» («Мир», 1970) получили высокую оценку советских ученых. Новый труд Ж.-П. Серра, несомненно, будет пользоваться еще большей популярностью. Он заинтересует математиков различных специальностей и окажется полезным преподавателям, аспирантам и студентам университетов и пединститутов.

ОГЛАВЛЕНИЕ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ИМЕННОЙ УКАЗАТЕЛЬ

ПРЕДИСЛОВИЕ РЕДАКТОРА ПЕРЕВОДА

Читателя не должно ввести в заблуждение название книги: это курс основ теории чисел, предполагающий известной теорию делимости и элементы теории сравнений целых рациональных чисел, а также требующий владения некоторыми терминами и результатами общей алгебры. Для успешного изучения книги Серра в основном достаточно общего курса алгебры, читающегося студентам наших университетов и педагогических институтов в первые два года обучения. Правда, система алгебраического образования во Франции несколько отличается от нашей, но недостающие сведения читатель может найти, например, в соответствующих выпусках «Элементов математики» Н. Бурбаки и в книге С. Ленга «Алгебра» (конечно, систематическое изучение этих сочинений не предполагается).

Ж.-П. Серр известен не только как один из крупнейших современных математиков, но и как автор многих содержательных и ясно написанных книг (некоторые из них переведены на русский язык). Предлагаемая книга — одно из наиболее удачных произведений этого выдающегося автора. Она составлена из записей двух курсов лекций, читанных автором для студентов второго года обучения Высшей нормальной школы.

Нет нужды останавливаться на содержании книги, ибо оно подробно описано в предисловии автора. По тематике ее можно сравнить с известной книгой З. И. Боревича и И. Р. Шафаревича «Теория чисел». Однако книга Серра значительно отличается от последней как по отбору материала, так — и особенно —

по манере изложения. В то время как книга Боревича — Шафаревича представляет собой монографию, небольшая книга Серра является современным университетским учебником.

Выход в свет русского перевода книги Серра тем более актуален, что сейчас идет активная перестройка университетского математического образования. Традиционный обязательный курс теории чисел в ряде университетов ликвидирован. Бóльшая часть его материала включена в курс высшей алгебры, где кольцо целых чисел играет роль модели, на которой демонстрируются абстрактные алгебраические понятия и конструкции, однако при этом ряд важных результатов теории чисел естественно оказывается опущенным. Книга Серра заполняет появившийся пробел. Ее можно рассматривать как первый спецкурс, обязательный для всех, кто хочет специализироваться по теории чисел и смежным с нею дисциплинам. Конечно, отбор материала для такого курса, предлагаемый автором, очень интересен, но не единственно возможен. Представляется, что материал первых трех глав (конечные поля, p-адические поля, символ Гильберта) должен войти в той или иной мере в любой курс основ теории чисел. Содержание же остальных глав может быть развито и в самостоятельные более специализированные курсы арифметики квадратичных форм, теории L-рядов, теории модулярных форм.

Нет сомнения, что предлагаемую книгу Серра будут с пользой и интересом читать студенты средних и старших курсов университетов и педагогических институтов, специализирующиеся в области алгебры, теории чисел и смежных областях математики. Она будет полезна преподавателям и научным работникам — и знающие материал книги читатели с удовольствием познакомятся с изложением Серра.

А. Малышев

ПРЕДИСЛОВИЕ

Эта книга делится на две части.

Первая часть — чисто алгебраическая. Ее целью является классификация квадратичных форм над полем рациональных чисел (теорема Минковского — Хассе); этой теме посвящена глава IV. Предыдущие три главы содержат различные предварительные сведения: квадратичный закон взаимности, p-адические поля, символы Гильберта. В главе V предыдущие результаты прилагаются к квадратичным формам с целыми коэффициентами и определителем ± 1; такие формы используются в различных вопросах: модулярные функции, дифференциальная топология, конечные группы.

Вторая часть (главы VI и VII) использует «аналитические» средства (голоморфные функции). В главе VI дается доказательство теоремы Дирихле об арифметической прогрессии; кстати, эта теорема используется в одном узловом пункте первой части (п. 2.2 гл. III). Глава VII посвящена модулярным формам, в частности, тэта-функциям; здесь вновь появляются некоторые квадратичные формы главы V.

Эти две части соответствуют курсу, прочитанному в 1962 и 1964 гг. студентам второго года обучения Высшей нормальной школы. Предварительная редакция курса, размноженного на ротаторе, принадлежит Сансу (главы I—IV) и Рами и Руже (главы VI—VII). Она была существенно использована мною; я приношу благодарность этим авторам.

Часть первая

АЛГЕБРАИЧЕСКИЕ МЕТОДЫ

Глава I

КОНЕЧНЫЕ ПОЛЯ

Всякое поле, рассматриваемое в дальнейшем, предполагается коммутативным.

§ 1. Общие положения

1.1. *Простые поля. Конечные поля*

Пересечение подполей данного поля K является наименьшим его подполем; оно содержит канонический образ кольца $\mathbf{Z}$, изоморфный $\mathbf{Z}$ или $\mathbf{Z}/p\mathbf{Z}$, где p — некоторое простое число. Следовательно, это подполе будет изоморфно или полю рациональных чисел $\mathbf{Q}$, или полю $\mathbf{Z}/p\mathbf{Z}$.

Определение 1. *Поля* $\mathbf{Q}$ *и* $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, *где* p *— простое число, будем называть простыми полями; характеристикой поля* K *называем число* $\operatorname{caract}(K) = 0$ *или* p *в зависимости от того, является* K *расширением поля* $\mathbf{Q}$ *или поля* $\mathbf{F}_p$.

Поэтому если $\operatorname{caract}(K) = p \neq 0$, то p — наименьшее целое число $n > 0$ такое, что $n \cdot 1 = 0$.

Лемма. *Если* $\operatorname{caract}(K) = p$, *то* $\sigma\colon x \longmapsto x^p$ *есть изоморфное отображение* K *на его подполе*[1]) K^p.

---

[1]) Здесь через K^p автор обозначает совокупность p-х степеней поля K. Аналогичное значение имеют $\mathbf{F}_q^{*2}$ (§ 3) и $\mathbf{Q}_p^{*2}$ (§ 3 гл. II). Обычно же через K^n обозначается прямое произведение n экземпляров множества K (§ 2 этой главы; § 2 гл. II и т. д.). — *Прим. ред.*

Действительно, $\sigma(xy) = \sigma(x)\,\sigma(y)$. Далее, если $1 \leqslant k < p$, то биномиальный коэффициент $\binom{p}{k}$ сравним с $0 \pmod p$; поэтому

$$\sigma(x+y) = \sigma(x) + \sigma(y),$$

так что σ — гомоморфизм. Наконец, очевидно, что σ — инъективное отображение.

Теорема 1. i) *Характеристика конечного поля* K *есть простое число* $p \neq 0$; *если* $f = [\mathrm{K} : \mathbf{F}_p]$, *то число элементов* K *равно* p^f.

ii) *Пусть* p — *простое число и* $q = p^f$ — *степень* p $(f \geqslant 1)$. *Пусть* Ω — *некоторое алгебраически замкнутое поле характеристики* p. *Тогда существует единственное подполе* $\mathbf{F}_q$ *поля* Ω, *состоящее из* q *элементов*; $\mathbf{F}_q$ *есть множество корней полинома* $X^q - X$.

iii) *Любое конечное поле, состоящее из* $q = p^f$ *элементов, изоморфно полю* $\mathbf{F}_q$.

Так как K — конечное поле, то оно не может содержать поля $\mathbf{Q}$; поэтому его характеристика есть простое число p. Если f — степень расширения $\mathrm{K}/\mathbf{F}_p$, то ясно, что $\mathrm{card}(\mathrm{K}) = p^f$, что доказывает i).

Далее, если Ω — алгебраически замкнутое поле характеристики p, то по предыдущей лемме отображение $x \mapsto x^q$ (где $q = p^f$, $f \geqslant 1$) является автоморфизмом; действительно, оно является f-й степенью автоморфизма σ: $x \mapsto x^p$ (заметим, что σ сюръективно в силу алгебраической замкнутости Ω). Элементы x поля Ω, инвариантные относительно отображения $x \mapsto x^q$, образуют некоторое подполе $\mathbf{F}_q$ поля Ω. Это x поле состоит из q элементов. Действительно, производная $X^q - X$, равная

$$qX^{q-1} - 1 = p \cdot p^{f-1}X^{q-1} - 1 = -1,$$

не обращается в нуль; поэтому (в силу алгебраической замкнутости Ω) полином $X^q - X$ имеет q различных корней; таким образом, $\mathrm{card}(\mathbf{F}_q) = q$. Обратно, если K есть подполе поля Ω, состоящее из q элементов, то мультипликативная группа K^* ненулевых

элементов поля K состоит из $q-1$ элемента; поэтому $x^{q-1}=1$, если $x\in K^*$; итак, $x^q-x=0$, если $x\in K$. Отсюда следует, что K содержится в $\mathbf{F}_q$; так как

$$\operatorname{card}(K)=\operatorname{card}(\mathbf{F}_q),$$

то $K=\mathbf{F}_q$, что заканчивает доказательство ii).

Наконец, утверждение iii) следует из ii), если учесть, что всякое поле из p^f элементов может быть вложено в поле Ω, ибо Ω алгебраически замкнуто.

1.2. *Мультипликативная группа конечного поля*

Пусть p — простое число, f — целое число $\geqslant 1$, $q=p^f$.

Теорема 2. *Мультипликативная группа $\mathbf{F}_q^*$ конечного поля $\mathbf{F}_q$ является циклической группой порядка $q-1$.*

Доказательство. Пусть d — целое число $\geqslant 1$; вспомним обозначение $\varphi(d)$ для *функции Эйлера* — числа целых чисел x, удовлетворяющих условию $1\leqslant x\leqslant d$ и *взаимно простых с d* (иначе говоря, чисел x, образы которых в факторгруппе $\mathbf{Z}/d\mathbf{Z}$ являются образующими этой группы).

Ясно, что число образующих циклической группы порядка d равно $\varphi(d)$.

Лемма 1. *Если n — целое число $\geqslant 1$, то*

$$n=\sum_{d\mid n}\varphi(d).$$

(Напоминаем, что $d\mid n$ обозначает, что *n делится на d.*)

Если d — делитель числа n, то пусть C_d — единственная подгруппа факторгруппы $\mathbf{Z}/n\mathbf{Z}$, имеющая порядок d; пусть Φ_d — множество образующих группы C_d. Так как каждый элемент группы $\mathbf{Z}/n\mathbf{Z}$ порождает одну из подгрупп C_d, то $\mathbf{Z}/n\mathbf{Z}$ есть объединение непересекающихся множеств Φ_d, так что

$$n=\operatorname{card}(\mathbf{Z}/n\mathbf{Z})=\sum_{d\mid n}\operatorname{card}(\Phi_d)=\sum_{d\mid n}\varphi(d).$$

Лемма 2. *Пусть* H — *группа конечного порядка* n. *Предположим, что для каждого делителя* d *числа* n *множество всех* $x \in H$, *таких, что* $x^d = 1$, *имеет самое большее* d *элементов. Тогда* H — *циклическая группа.*

Пусть d — делитель числа n. Если существует элемент $x \in H$ порядка d, то подгруппа $(x) = \{1, x, \ldots, x^{d-1}\}$, порожденная элементом x, является циклической группой порядка d; поэтому, по предположению, каждый элемент $y \in H$, такой, что $y^d = 1$, принадлежит (x). В частности, элементы группы H порядка d (и только они) являются образующими подгруппы (x), так что их число равно $\varphi(d)$. Итак, число элементов группы H порядка d равно 0 или $\varphi(d)$. Если хотя бы одному из d отвечало значение 0, то из формулы леммы 1 следовало бы, что число элементов H меньше n; а это противоречит предположению. В частности, существует элемент $x \in H$ порядка n, и H совпадает с циклической группой (x).

Теорема 2 следует из леммы 2, если положить $H = \mathbf{F}_q^*$, $n = q - 1$; действительно, очевидно, что уравнение $x^d = 1$, будучи степени d, имеет не более d решений в F_q.

Замечание. Приведенное выше доказательство позволяет доказать и более общее утверждение: всякая конечная подгруппа мультипликативной группы любого поля является циклической.

§ 2. Уравнения над конечным полем

Пусть q — степень простого числа p, и пусть K — поле, состоящее из q элементов.

2.1. *Суммы степеней*

Лемма. *Пусть* u — *целое число* $\geqslant 0$. *Сумма*

$$S(X^u) = \sum_{x \in K} x^u$$

равна -1, *если* $u \geqslant 1$ *и* $(q-1) \mid u$; *в противном случае эта сумма равна* 0.

(Условимся, что если $u=0$, то $x^u=1$ *даже при* $x=0$.)

Если $u=0$, то каждый член этой суммы равен 1, так что $S(X^u)=q\cdot 1=0$, ибо поле K имеет характеристику p.

Если $u\geqslant 1$ и u делится на $q-1$, то $0^u=0$ и $x^u=1$ для $x\neq 0$; поэтому $S(X^u)=(q-1)\cdot 1=-1$.

Наконец, если $u\geqslant 1$ и u не делится на $q-1$, то, поскольку K^* — циклическая группа порядка $q-1$ (теорема 2), найдется $y\in K^*$, такое, что $y^u\neq 1$. Так как

$$S(X^u)=\sum_{x\in K^*} x^u=\sum_{x\in K^*} y^u x^u=y^u S(X^u),$$

то $(1-y^u)S(X^u)=0$, откуда следует, что $S(X^u)=0$.

(*Вариант.* Использовать то обстоятельство, что при $d\geqslant 2$ сумма корней d-й степени из единицы равна нулю.)

2.2. *Теорема Шевалле*

Теорема 3 (Шевалле — Варнинг). *Пусть*

$$f_\alpha\in K[X_1,\ \ldots,\ X_n]$$

— полиномы от n переменных, причем $\sum \deg(f_\alpha)<n$, *и пусть* V *— множество их общих нулей на* K^n. *Тогда*

$$\operatorname{card}(V)\equiv 0 \pmod p.$$

Положим $P=\prod_\alpha\left(1-f_\alpha^{q-1}\right)$. Пусть $x\in K^n$; если $x\in V$, то все $f_\alpha(x)$ равны нулю и потому $P(x)=1$; если $x\notin V$, то хотя бы один из $f_\alpha(x)$ не равен нулю, так что $f_\alpha^{q-1}(x)=1$, а потому $P(x)=0$. Таким образом, P *— характеристическая функция* множества V. Если для произвольного полинома f

$$S(f)=\sum_{x\in K^n} f(x),$$

то

$$\operatorname{card}(V)\equiv S(P) \pmod p,$$

и остается проверить, что $S(P)=0$.

Действительно, из предположения $\sum \deg(f_\alpha) < n$ вытекает неравенство

$$\deg(P) < n(q-1);$$

поэтому P есть линейная комбинация одночленов

$$X^u = X_1^{u_1} \dots X_n^{u_n},$$

причем $\sum u_i < n(q-1)$. Достаточно доказать, что для такого одночлена X^u имеет место равенство $S(X^u) = 0$. Но это следует из леммы, ибо $u_i < q-1$ хотя бы для одного i. Ч. т. д.

Следствие 1. *Если* $\sum \deg(f_\alpha) < n$ *и полиномы* f_α *не имеют свободных членов, то эти полиномы имеют общий нетривиальный нуль.*

Действительно, если бы V свелось к {0}, то $\mathrm{card}(V) = 1$ и $\mathrm{card}(V)$ не делилось бы на p.

Особенно интересны приложения следствия 1, когда формы f_α *однородны*; в частности

Следствие 2. *Всякая квадратичная форма от трех и более переменных над* K *имеет нетривиальный нуль.*

(На геометрическом языке: всякий конус над конечным полем имеет рациональную точку.)

§ 3. Квадратичный закон взаимности

3.1. *Квадраты поля* $\mathbf{F}_q$

Пусть q — степень простого числа p.

Теорема 4. a) *Если* $p = 2$, *то каждый элемент поля* $\mathbf{F}_q$ *является квадратом.*

b) *Если* $p \neq 2$, *то квадраты группы* $\mathbf{F}_q^*$ *образуют ее подгруппу индекса 2; эта подгруппа есть ядро гомоморфизма* $x \mapsto x^{(q-1)/2}$; *значения* $x^{(q-1)/2}$ *в алгебраическом замыкании* Ω *поля* $\mathbf{F}_q$ *суть* $\{\pm 1\}$.

(В других терминах: последовательность

$$1 \to \mathbf{F}_q^{*2} \to \mathbf{F}_q^* \to \{\pm 1\} \to 1$$

является точной.)

Утверждение a) вытекает из того, что отображение $x \mapsto x^2$ — автоморфизм поля $\mathbf{F}_q$.

Переходим к утверждению b). Пусть Ω — алгебраическое замыкание поля $\mathbf{F}_q$; если $x \in \mathbf{F}_q^*$, то пусть $y \in \Omega$ выбрано так, что $y^2 = x$. Тогда

$$y^{q-1} = x^{(q-1)/2} = \pm 1,$$

ибо $x^{q-1} = 1$.

Для того чтобы x было квадратом поля K, необходимо и достаточно, чтобы y принадлежало $\mathbf{F}_q^*$, т. е. чтобы $y^{q-1} = 1$. Поэтому $\mathbf{F}_q^{*2}$ есть ядро гомоморфизма $x \mapsto x^{(q-1)/2}$. Так как $\mathbf{F}_q^*$ — циклическая группа порядка $q-1$, то индекс $\mathbf{F}_q^{*2}$ равен 2.

3.2. *Символ Лежандра (элементарные свойства)*

Определение. *Пусть p — простое число $\neq 2$ и $x \in \mathbf{F}_p^*$. Символом Лежандра $\left(\frac{x}{p}\right)$ элемента $x \in \mathbf{F}_p^*$ назовем целое число $x^{(p-1)/2} = \pm 1$.*

Удобно распространить этот символ на все поле $\mathbf{F}_p$, полагая $\left(\frac{0}{p}\right) = 0$. Кроме того, если $x \in \mathbf{Z}$ и $x' \in \mathbf{F}_p$ — канонический образ x, то полагаем $\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right)$.

Имеем: $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$, т. е. символ Лежандра является «характером» (см. § 1 гл. VI). По теореме 4 равенство $\left(\frac{x}{p}\right) = 1$ эквивалентно включению $x \in \mathbf{F}_p^{*2}$; если $x \in \mathbf{F}_p^*$ имеет квадратный корень y в некотором алгебраическом замыкании поля $\mathbf{F}_p$, то $\left(\frac{x}{p}\right) = y^{p-1}$.

Вычисление $\left(\frac{x}{p}\right)$ для $x = 1, -1, 2$

Если n — *нечетное* целое число, то определим элементы $\varepsilon(n)$ и $\omega(n)$ факторкольца $\mathbf{Z}/2\mathbf{Z}$ следующим

образом:

$$\varepsilon(n) \equiv \frac{n-1}{2} \pmod 2 = \begin{cases} 0, & \text{если } n \equiv 1 \pmod 4, \\ 1, & \text{если } n \equiv -1 \pmod 4; \end{cases}$$

$$\omega(n) \equiv \frac{n^2-1}{8} \pmod 2 = \begin{cases} 0, & \text{если } n \equiv \pm 1 \pmod 8, \\ 1, & \text{если } n \equiv \pm 5 \pmod 8. \end{cases}$$

[Отображение ε есть гомоморфизм мультипликативной группы $(\mathbf{Z}/4\mathbf{Z})^*$ на $\mathbf{Z}/2\mathbf{Z}$; точно так же ω — гомоморфизм $(\mathbf{Z}/8\mathbf{Z})^*$ на $\mathbf{Z}/2\mathbf{Z}$.]

Теорема 5. *Имеют место формулы*

i) $\left(\frac{1}{p}\right) = 1$;

ii) $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$;

iii) $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$.

Только последняя формула заслуживает доказательства. Если α — примитивный корень восьмой степени из единицы в некотором алгебраическом замыкании Ω поля $\mathbf{F}_p$, то для элемента $y = \alpha + \alpha^{-1}$ имеет место равенство $y^2 = 2$ (действительно, $\alpha^4 = -1$, откуда $\alpha^2 + \alpha^{-2} = 0$). Имеем

$$y^p = \alpha^p + \alpha^{-p}.$$

Если $p \equiv \pm 1 \pmod 8$, то отсюда выводим, что $y^p = y$, так что $\left(\frac{2}{p}\right) = y^{p-1} = 1$.

Если $p \equiv \pm 5 \pmod 8$, то получаем

$$y^p = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -y;$$

это следует из формулы $\alpha + \alpha^3 + \alpha^5 + \alpha^7 = 0$. Отсюда выводим, что $y^{p-1} = -1$, и формула iii) доказана.

Замечание. Теорему 5 можно сформулировать следующим образом:

-1 является квадратом $(\bmod p) \Leftrightarrow p \equiv 1 \pmod 4$;

2 является квадратом $(\bmod p) \Leftrightarrow p \equiv \pm 1 \pmod 8$.

3.3. *Квадратичный закон взаимности*

Пусть l и p — различные простые числа, отличные от 2.

Теорема 6 (Гаусс). *Имеет место равенство*

$$\left(\frac{l}{p}\right)=\left(\frac{p}{l}\right)(-1)^{\varepsilon(l)\varepsilon(p)}.$$

Пусть Ω — некоторое алгебраическое замыкание поля $\mathbf{F}_p$, и пусть $w\in\Omega$ — примитивный корень l-й степени из единицы. Если $x\in\mathbf{F}_l$, то элемент w^x однозначно определен, ибо $w^l=1$. Поэтому может быть определена «сумма Гаусса»

$$y=\sum_{x\in\mathbf{F}_l}\left(\frac{x}{l}\right)w^x.$$

Лемма 1. *Имеет место равенство*

$$y^2=(-1)^{\varepsilon(l)}l.$$

(Злоупотребляя обозначениями, под l мы понимаем образ l в поле $\mathbf{F}_p$.)

Действительно,

$$y^2=\sum_{t,\,z}\left(\frac{tz}{l}\right)w^{t+z}=\sum_{u\in\mathbf{F}_l}w^u\left(\sum_{t\in\mathbf{F}_l}\left(\frac{t(u-t)}{l}\right)\right).$$

Если $t\neq 0$, то

$$\left(\frac{t(u-t)}{l}\right)=\left(\frac{-t^2}{l}\right)\left(\frac{1-ut^{-1}}{l}\right)=(-1)^{\varepsilon(l)}\left(\frac{1-ut^{-1}}{l}\right),$$

откуда

$$(-1)^{\varepsilon(l)}y^2=\sum_{u\in\mathbf{F}_l}C_u w^u,$$

где

$$C_u=\sum_{t\in\mathbf{F}_l^*}\left(\frac{1-ut^{-1}}{l}\right).$$

Если $u=0$, то

$$C_0=\sum_{t\in\mathbf{F}_l^*}\left(\frac{1}{l}\right)=l-1;$$

иначе $s = 1 - ut^{-1}$ пробегает множество $\mathbf{F}_l - \{1\}$, а потому

$$C_u = \sum_{s \in \mathbf{F}_l} \left(\frac{s}{l}\right) - \left(\frac{1}{l}\right) = -\left(\frac{1}{l}\right) = -1,$$

ибо в $\mathbf{F}_l^*$ число элементов, являющихся квадратами, и число элементов, не являющихся квадратами, одинаковы. Поэтому

$$\sum_{u \in \mathbf{F}_l} C_u w^u = (l-1) - \sum_{u \in \mathbf{F}_l^*} w^u = l,$$

что и доказывает лемму.

Лемма 2. *Имеет место равенство*

$$y^{p-1} = \left(\frac{p}{l}\right).$$

Так как Ω имеет характеристику p, то

$$y^p = \sum_{x \in \mathbf{F}_l} \left(\frac{x}{l}\right) w^{xp} = \sum_{z \in \mathbf{F}_l} \left(\frac{zp^{-1}}{l}\right) w^z = \left(\frac{p^{-1}}{l}\right) y = \left(\frac{p}{l}\right) y,$$

откуда следует утверждение леммы.

Теорема 6 теперь получается непосредственно. Действительно, по леммам 1 и 2

$$\left(\frac{(-1)^{\varepsilon(l)} l}{p}\right) = y^{p-1} = \left(\frac{p}{l}\right),$$

а по теореме 5

$$\left(\frac{(-1)^{\varepsilon(l)}}{p}\right) = (-1)^{\varepsilon(l)\varepsilon(p)}.$$

Другая формулировка. Пишем $l\mathrm{R}p$, если l — квадрат (mod p) (иначе говоря, если l — «*квадратичный вычет*» по модулю p); в противном случае пишем $l\mathrm{N}p$. Теорема 6 означает, что

$l\mathrm{R}p \Leftrightarrow p\mathrm{R}l$, когда p или $l \equiv 1 \pmod 4$;

$l\mathrm{R}p \Leftrightarrow p\mathrm{N}l$, когда и p и $l \equiv -1 \pmod 4$,

Замечание. Теорема 6 может быть использована для вычисления символов Лежандра последовательной редукцией; например

$$\left(\frac{29}{43}\right)=\left(\frac{43}{29}\right)=\left(\frac{14}{29}\right)=\left(\frac{2}{29}\right)\left(\frac{7}{29}\right)=$$
$$=-\left(\frac{7}{29}\right)=-\left(\frac{29}{7}\right)=-\left(\frac{1}{7}\right)=-1.$$

Приложение

Другое доказательство квадратичного закона взаимности (по Эйзенштейну [1])

i) *Лемма Гаусса*

Пусть p — простое число $\neq 2$, и пусть S — такое подмножество множества $\mathbf{F}_p^*$, что $\mathbf{F}_p^*$ есть дизъюнктное объединение множеств S и $-$S; например, это множество $S=\left\{1, \ldots, \frac{p-1}{2}\right\}$.

Если $s\in S$ и $a\in\mathbf{F}_p^*$, то as записываем в виде $as=e_s(a)\,s_a$, где $e_s(a)=\pm 1$ и $s_a\in S$.

Лемма (Гаусс). *Имеет место равенство*

$$\left(\frac{a}{p}\right)=\prod_{s\in S} e_s(a).$$

Прежде всего заметим, что если s и s' — два различных элемента множества S, то $s_a\neq s'_a$ (ибо иначе мы получим, что $s=\pm s'$, в противоположность выбору S). Поэтому отображение $s\mapsto s_a$ есть биекция множества S на себя. Перемножая равенства $as=e_s(a)\,s_a$, получаем

$$a^{(p-1)/2}\prod_{s\in S} s=\left(\prod_{s\in S} e_s(a)\right)\prod_{s\in S} s_a=\left(\prod_{s\in S} e_s(a)\right)\prod_{s\in S} s,$$

откуда

$$a^{(p-1)/2}=\prod_{s\in S} e_s(a).$$

Это и доказывает лемму, ибо $\left(\frac{a}{p}\right)=a^{(p-1)/2}$ в $\mathbf{F}_p$.

[1]) Eisenstein G., *J. Crelle*, 29 (1845), 177—184.

Пример. Пусть $a=2$ и $S=\left\{1, \ldots, \frac{p-1}{2}\right\}$. Тогда $e_s(2)=1$, если $2s \leqslant \frac{p-1}{2}$, и $e_s(2)=-1$ в противном случае. Отсюда выводим, что $\left(\frac{2}{p}\right)=(-1)^{n(p)}$, где $n(p)$ — число целых чисел s, таких, что $\frac{p-1}{4}<s \leqslant \frac{p-1}{2}$. Если p имеет вид $1+4k$, то $n(p)=k$; если $p=3+4k$, то $n(p)=k+1$. Поэтому $\left(\frac{2}{p}\right)=1$, если $p \equiv \pm 1 \pmod 8$, и $\left(\frac{2}{p}\right)=-1$, если $p \equiv \pm 5 \pmod 8$; см. теорему 5.

ii) *Тригонометрическая лемма*

Лемма. *Пусть m — нечетное целое положительное число. Тогда*

$$\frac{\sin mx}{\sin x}=(-4)^{(m-1)/2} \prod_{1 \leqslant j \leqslant (m-1)/2}\left(\sin^2 x-\sin^2 \frac{2\pi j}{m}\right).$$

Это тождество проверяется без труда (например, докажем, что левая часть есть полином степени $(m-1)/2$ от $\sin^2 x$, корни которого суть $\sin^2(2\pi j/m)$, где $1 \leqslant j \leqslant (m-1)/2$; множитель $(-4)^{(m-1)/2}$ получается сравнением коэффициентов при $e^{i(m-1)x}$ в левой и правой частях).

iii) *Доказательство закона взаимности*

Пусть l и p — два различных простых числа, отличных от 2. Пусть $S=\{1, \ldots, (p-1)/2\}$ — рассматривавшееся выше множество. По лемме Гаусса

$$\left(\frac{l}{p}\right)=\prod_{s \in S} e_s(l).$$

В силу равенства $ls=e_s(l)\, s_l$

$$\sin \frac{2\pi}{p} ls=e_s(l) \sin \frac{2\pi}{p} s_l.$$

Перемножая эти равенства и учитывая, что отображение $s \mapsto s_l$ биективно, получаем

$$\left(\frac{l}{p}\right) = \prod_{s \in S} e_s(l) = \prod_{s \in S} \left(\sin \frac{2\pi ls}{p} \Big/ \sin \frac{2\pi s}{p}\right).$$

Применяя тригонометрическую лемму при $m = l$, перепишем это равенство следующим образом:

$$\left(\frac{l}{p}\right) = \prod_{s \in S} (-4)^{(l-1)/2} \prod_{t \in T} \left(\sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{l}\right) =$$

$$= (-4)^{(l-1)(p-1)/4} \prod_{s \in S,\ t \in T} \left(\sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{l}\right),$$

где T обозначает множество всех целых чисел t таких, что $1 \leqslant t \leqslant (l-1)/2$. Меняя роли l и p, точно так же получаем

$$\left(\frac{p}{l}\right) = (-4)^{(l-1)(p-1)/4} \prod_{s \in S,\ t \in T} \left(\sin^2 \frac{2\pi t}{l} - \sin^2 \frac{2\pi s}{p}\right).$$

Множители в формулах для (l/p) и (p/l) одинаковы с точностью до знака. Число же противоположных знаков равно $(p-1)(l-1)/4$, а потому

$$\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{(p-1)(l-1)/4},$$

и мы снова доказали квадратичный закон взаимности, см. теорему 6.

Глава II

p-АДИЧЕСКИЕ ПОЛЯ

Во всей этой главе через p обозначается простое число.

§ 1. Кольцо $\mathbf{Z}_p$ и поле $\mathbf{Q}_p$

1.1. *Определения*

Для любого $n \geqslant 1$ положим $\mathbf{A}_n = \mathbf{Z}/p^n\mathbf{Z}$; это — кольцо классов целых чисел (mod p^n). Каждый элемент из $\mathbf{A}_n$ очевидным образом определяет элемент из $\mathbf{A}_{n-1}$; таким образом, мы получаем гомоморфизм

$$\varphi_n\colon \mathbf{A}_n \to \mathbf{A}_{n-1},$$

который сюръективен и имеет ядро $p^{n-1}\mathbf{A}_n$.

Последовательность

$$\ldots \to \mathbf{A}_n \to \mathbf{A}_{n-1} \to \ldots \to \mathbf{A}_2 \to \mathbf{A}_1$$

образует «*проективную систему*», занумерованную целыми числами $\geqslant 1$.

Определение 1. *Проективный предел определенной выше системы* $(\mathbf{A}_n, \varphi_n)$ *называется кольцом целых p-адических чисел и обозначается* $\mathbf{Z}_p$.

По определению, элементом из $\mathbf{Z}_p = \varprojlim (\mathbf{A}_n, \varphi_n)$ является последовательность $x = (\ldots, x_n, \ldots, x_1)$, где

$$x_n \in \mathbf{A}_n \quad \text{и} \quad \varphi_n(x_n) = x_{n-1}, \quad \text{если} \quad n \geqslant 2.$$

Сложение и умножение в $\mathbf{Z}_p$ определены «покоординатно»; иначе говоря, $\mathbf{Z}_p$ является *подкольцом* произведения $\prod_{n \geqslant 1} \mathbf{A}_n$. Если мы снабдим кольца $\mathbf{A}_n$ дискретной топологией, а $\prod \mathbf{A}_n$ — топологией произведе-

ния, то кольцо $\mathbf{Z}_p$ оказывается снабженным топологией, которая делает его *компактным* пространством (так как оно замкнуто в произведении компактных пространств).

1.2. *Свойства кольца* $\mathbf{Z}_p$

Пусть $\varepsilon_n\colon \mathbf{Z}_p \to \mathbf{A}_n$ — отображение, которое сопоставляет целому p-адическому числу x его n-ю составляющую x_n.

Предложение 1. *Последовательность* $0 \to \mathbf{Z}_p \xrightarrow{p^n} \mathbf{Z}_p \xrightarrow{\varepsilon_n} \mathbf{A}_n \to 0$ *точна.*

(Таким образом, можно отождествить $\mathbf{Z}_p/p^n\mathbf{Z}_p$ с $\mathbf{A}_n = \mathbf{Z}/p^n\mathbf{Z}$.)

Умножение на p (и, стало быть, на p^n) инъективно на $\mathbf{Z}_p$; действительно, если $x = (x_n)$ — такое целое p-адическое число, что $px = 0$, то $px_{n+1} = 0$ для любого n, откуда вытекает, что x_{n+1} имеет вид $p^n y_{n+1}$, где $y_{n+1} \in \mathbf{A}_{n+1}$; так как $x_n = \varphi_{n+1}(x_{n+1})$, элемент x_n равен кратному числа p^n, т. е. равен нулю.

Ясно, что ядро гомоморфизма ε_n содержит $p^n\mathbf{Z}_p$; обратно, если $x = (x_m)$ принадлежит ядру $\mathrm{Ker}(\varepsilon_n)$, то $x_m \equiv 0 \pmod{p^n}$ для каждого $m \geqslant n$, а это означает, что существует такой вполне определенный элемент y_{m-n} из $\mathbf{A}_{m-n}$, что $x_m = p^n y_{m-n}$. Элементы y_l определяют элемент y из $\mathbf{Z}_p = \varprojlim \mathbf{A}_i$, и мы сразу же убеждаемся, что $p^n y = x$, а это завершает доказательство предложения.

Предложение 2. a) *Для обратимости элемента из* $\mathbf{Z}_p$ (*соответственно из* $\mathbf{A}_n$) *необходимо и достаточно, чтобы он не делился на* p.

b) *Если через* $\mathbf{U}$ *обозначить группу обратимых элементов из* $\mathbf{Z}_p$, *то любой элемент из* $\mathbf{Z}_p$, *отличный от* 0, *единственным способом запишется в виде* $p^n u$, *где* $u \in \mathbf{U}$ *и* $n \geqslant 0$.

(Элемент из $\mathbf{U}$ называется *p-адической единицей*.)

Достаточно доказать а) для колец $\mathbf{A}_n$: случай кольца $\mathbf{Z}_p$ вытекает отсюда. Итак, если $x \in \mathbf{A}_n$ не принадлежит подкольцу $p\mathbf{A}_n$, то его образ в $\mathbf{A}_1 = \mathbf{F}_p$ отличен от нуля, т. е. обратим; тогда существуют такие $y, z \in \mathbf{A}_n$, что $xy = 1 - pz$, откуда $xy(1+pz+\ldots + p^{n-1}z^{n-1}) = 1$, а это как раз и доказывает, что x обратим.

Далее, если $x \in \mathbf{Z}_p$ не является нулем, то существует такое наибольшее целое число n, что $x_n = \varepsilon_n(x)$ равно нулю; тогда мы имеем $x = p^n u$, где элемент u не делится на p, откуда $u \in \mathbf{U}$ на основании а). Единственность такого разложения очевидна.

Обозначение. Пусть x — ненулевой элемент из $\mathbf{Z}_p$; запишем x в виде $p^n u$, $u \in \mathbf{U}$. Целое число n называется *p-адическим показателем* элемента x и обозначается через $v_p(x)$. Положим $v_p(0) = +\infty$; тогда

$$v_p(xy) = v_p(x) + v_p(y),$$
$$v_p(x+y) \geqslant \operatorname{Inf}(v_p(x), v_p(y)).$$

Из этих формул сразу же получается, что $\mathbf{Z}_p$ является *областью целостности.*

Предложение 3. *На $\mathbf{Z}_p$ можно определить топологию при помощи расстояния*

$$d(x, y) = e^{-v_p(x-y)}.$$

Кольцо $\mathbf{Z}_p$ является полным пространством, в котором $\mathbf{Z}$ всюду плотно.

Идеалы $p^n\mathbf{Z}_p$ образуют базис окрестностей для 0; так как включение $x \in p^n\mathbf{Z}_p$ равносильно неравенству $v_p(x) \geqslant n$, очевидно, что топология на $\mathbf{Z}_p$ определяется расстоянием

$$d(x, y) = e^{-v_p(x-y)}.$$

Так как $\mathbf{Z}_p$ компактно, то оно полно. Наконец, если $x = (x_n)$ — элемент из $\mathbf{Z}_p$ и если $y_n \in \mathbf{Z}$ сравним с $x_n \pmod{p^n}$, то мы имеем $\lim y_n = x$, а это и доказывает, что $\mathbf{Z}$ всюду плотно в $\mathbf{Z}_p$.

1.3. *Поле* $\mathbf{Q}_p$

Определение 2. *Полем p-адических чисел, обозначаемым через* $\mathbf{Q}_p$, *называется поле частных кольца* $\mathbf{Z}_p$.

Сразу же видно, что $\mathbf{Q}_p = \mathbf{Z}_p[p^{-1}]$. Любой элемент x из $\mathbf{Q}_p^*$ единственным способом записывается в виде $p^n u$, где $n \in \mathbf{Z}$, $u \in \mathbf{U}$; число n здесь также называется p-адическим показателем элемента x и обозначается через $v_p(x)$. Неравенство $v_p(x) \geqslant 0$ имеет место в том и только в том случае, когда $x \in \mathbf{Z}_p$.

Предложение 4. *Поле* $\mathbf{Q}_p$, *снабженное топологией, определенной посредством* $d(x, y) = e^{-v_p(x-y)}$, *локально компактно, и* $\mathbf{Z}_p$ *в нем является открытым подкольцом; поле* $\mathbf{Q}$ *всюду плотно в* $\mathbf{Q}_p$.

Это непосредственно ясно.

Замечания. 1) Можно определить $\mathbf{Q}_p$ (соответственно $\mathbf{Z}_p$) как *пополнение* поля $\mathbf{Q}$ (соответственно кольца $\mathbf{Z}$) по p-адическому расстоянию d.

2) Расстояние d удовлетворяет «*ультраметрическому*» неравенству

$$d(x, z) \leqslant \operatorname{Sup}(d(x, y), d(y, z)).$$

Легко доказать, что последовательность u_n имеет предел тогда и только тогда, когда $\lim(u_{n+1} - u_n) = 0$; точно так же, ряд сходится тогда и только тогда, когда его общий член стремится к нулю.

§ 2. p-адические уравнения

2.1. *Решения*

Лемма. *Пусть* $\ldots \to \mathbf{X}_n \to \mathbf{X}_{n-1} \to \ldots \to \mathbf{X}_1$ — *проективная система, и пусть* $\mathbf{X} = \varprojlim \mathbf{X}_n$ — *ее проективный предел. Если множества* $\mathbf{X}_n$ *конечны и не пусты, то* $\mathbf{X}$ *не пусто.*

Тот факт, что $\mathbf{X} \neq \varnothing$, ясен, когда отображения $\mathbf{X}_n \to \mathbf{X}_{n-1}$ сюръективны; сейчас мы сведем доказательство к этому случаю. Для этого обозначим через $\mathbf{X}_{n,p}$ образ множества $\mathbf{X}_{n+p}$ в $\mathbf{X}_n$; для фиксированного n множества $\mathbf{X}_{n,p}$ образуют убывающее семейство конечных непустых множеств; отсюда вытекает, что это семейство *стационарно*, т. е. что $\mathbf{X}_{n,p}$ не зависит от p для достаточно больших p. Пусть $\mathbf{Y}_n$ — это предельное значение для $\mathbf{X}_{n,p}$. Непосредственно убеждаемся, что отображение $\mathbf{X}_n \to \mathbf{X}_{n-1}$ отображает $\mathbf{Y}_n$ *на* $\mathbf{Y}_{n-1}$; так как множества $\mathbf{Y}_n$ не пусты, то на основании сделанного выше замечания $\varprojlim \mathbf{Y}_n \neq \varnothing$; тем более $\varprojlim \mathbf{X}_n \neq \varnothing$.

Обозначение. Если $f \in \mathbf{Z}_p[\mathbf{X}_1, \ldots, \mathbf{X}_m]$ — полином с коэффициентами из $\mathbf{Z}_p$ и если n — целое число $\geqslant 1$, то будем обозначать через f_n полином с коэффициентами из $\mathbf{A}_n$, получаемый из f редукцией $(\mathrm{mod}\ p^n)$.

Предложение 5. *Пусть* $f^{(i)} \in \mathbf{Z}_p[\mathbf{X}_1, \ldots, \mathbf{X}_m]$ — *полиномы с целыми p-адическими коэффициентами. Следующие условия равносильны.*

i) *Полиномы* $f^{(i)}$ *имеют общий нуль в* $(\mathbf{Z}_p)^m$.

ii) *Для всех* $n \geqslant 1$ *полиномы* $f_n^{(i)}$ *имеют общий нуль в* $(\mathbf{A}_n)^m$.

Пусть $\mathbf{X}$ (соответственно $\mathbf{X}_n$) — множество общих нулей для $f^{(i)}$ (соответственно для $f_n^{(i)}$). Множества $\mathbf{X}_n$ конечны, и мы имеем $\mathbf{X} = \varprojlim \mathbf{X}_n$; по предыдущей лемме множество $\mathbf{X}$ не пусто в том и только в том случае, когда не пусты $\mathbf{X}_n$; отсюда вытекает предложение.

Точка $x = (x_1, \ldots, x_m)$ в $(\mathbf{Z}_p)^m$ называется *примитивной*, если хотя бы один из x_i обратим, т. е. если не все x_i делятся на p; аналогичным образом определяем примитивные элементы в $(\mathbf{A}_n)^m$.

Предложение 6. *Пусть* $f^{(i)} \in \mathbf{Z}_p[\mathbf{X}_1, \ldots, \mathbf{X}_m]$ — *однородные полиномы с целыми p-адическими коэффициентами. Следующие условия равносильны.*

a) *Полиномы $f^{(i)}$ имеют общий нетривиальный нуль в $(\mathbf{Q}_p)^m$.*

b) *Полиномы $f^{(i)}$ имеют общий примитивный нуль в $(\mathbf{Z}_p)^m$.*

c) *Для всех $n \geqslant 1$ полиномы $f_n^{(i)}$ имеют общий примитивный нуль в $(\mathbf{A}_n)^m$.*

Импликация b) $\Rightarrow$ a) очевидна. Обратно, если $x = (x_1, \ldots, x_m)$ является общим нетривиальным нулем для $f^{(i)}$, то положим

$$h = \operatorname{Inf}(v_p(x_1), \ldots, v_p(x_m)) \quad \text{и} \quad y = p^{-h}x.$$

Ясно, что y является примитивным элементом в $(\mathbf{Z}_p)^m$ и что это общий нуль для $f^{(i)}$; таким образом, имеем b) $\Leftrightarrow$ a).

Что касается эквивалентности b) и c), то она вытекает из доказанной выше леммы.

2.2. *Улучшение приближенных решений*

Речь идет о том, чтобы перейти от решения (mod p^n) к настоящему решению (т. е. к решению в $\mathbf{Z}_p$). Используется следующая лемма (*p*-адический аналог «метода Ньютона»):

Лемма. *Пусть $f \in \mathbf{Z}_p[\mathbf{X}]$, и пусть f' — его производная. Пусть $x \in \mathbf{Z}_p$, n, $k \in \mathbf{Z}$, таковы, что $0 \leqslant 2k < n$, $f(x) \equiv 0 \pmod{p^n}$, $v_p(f'(x)) = k$. Тогда существует такое $y \in \mathbf{Z}_p$, что*

$$f(y) \equiv 0 \pmod{p^{n+1}},$$
$$v_p(f'(y)) = k \quad и \quad y \equiv x \pmod{p^{n-k}}.$$

Возьмем y в виде $x + p^{n-k}z$, где $z \in \mathbf{Z}_p$. Из формулы Тейлора имеем

$$f(y) = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a, \quad \text{где} \quad a \in \mathbf{Z}_p.$$

По предположению $f(x) = p^n b$ и $f'(x) = p^k c$, где $b \in \mathbf{Z}_p$ и $c \in \mathbf{U}$; это позволяет выбрать z таким образом, что

$$b + zc \equiv 0 \pmod{p}.$$

Тогда

$$f(y) = p^n(b + zc) + p^{2n-2k}a \equiv 0 \pmod{p^{n+1}},$$

поскольку $2n-2k > n$. Наконец, формула Тейлора, примененная к f', показывает, что $f'(y) \equiv p^k c \pmod{p^{n-k}}$; так как $n-k > k$, отсюда легко выводим, что $v_p(f'(y)) = k$.

Теорема 1. *Пусть* $f \in \mathbf{Z}_p[X_1, \ldots, X_m]$, $x = (x_i) \in (\mathbf{Z}_p)^m$, n, $k \in \mathbf{Z}$ *и* j *— целое число, заключенное между* 1 *и* m. *Предположим, что* $0 \leqslant 2k < n$ *и что*

$$f(x) \equiv 0 \pmod{p^n} \quad \text{и} \quad v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k.$$

Тогда в $(\mathbf{Z}_p)^m$ *существует нуль у полинома* f, *который сравним с* x *по модулю* p^{n-k}.

Сначала предположим, что $m = 1$. Применяя предыдущую лемму к $x^{(0)} = x$, получаем элемент $x^{(1)} \in \mathbf{Z}_p$, сравнимый с $x^{(0)} \pmod{p^{n-k}}$, для которого

$$f(x^{(1)}) \equiv 0 \pmod{p^{n+1}}, \quad v_p(f'(x^{(1)})) = k.$$

Можно применить лемму к $x^{(1)}$, заменяя n на $n+1$. Шаг за шагом мы конструируем такую последовательность $x^{(0)}, \ldots, x^{(q)}, \ldots$, что

$$x^{(q+1)} \equiv x^{(q)} \pmod{p^{n+q-k}}, \quad f(x^{(q)}) \equiv 0 \pmod{p^{n+q}}.$$

Это последовательность Коши; если обозначить через y ее предел, то мы, очевидно, получим, что $f(y) = 0$ и $y \equiv x \pmod{p^{n-k}}$, откуда следует случай $m = 1$ теоремы.

Случай $m > 1$ сводится к случаю $m = 1$, так как здесь изменяется лишь x_j. Точнее, пусть $\tilde{f} \in \mathbf{Z}_p[X_j]$ — полином от одной переменной, получаемый заменой X_i, $i \neq j$, на x_i. Можно применить только что доказанное утверждение к $\tilde{f}$ и к x_j; тогда мы выводим существование такого $y_j \equiv x_j \pmod{p^{n-k}}$, что $\tilde{f}(y_j) = 0$. Если положить $y_i = x_i$ для $i \neq j$, то элемент $y = (y_i)$ удовлетворяет условию.

Следствие 1. *Любой простой нуль редуцированного по модулю p полинома f поднимается до нуля полинома f с коэффициентами из $\mathbf{Z}_p$.*

(Если g — полином над полем, то нуль x полинома g называется *простым*, если хотя бы одна частная производная $\partial g/\partial X_j$ отлична от нуля в точке x.)

Это утверждение является частным случаем теоремы при $n=1$, $k=0$.

Следствие 2. *Предположим, что $p \neq 2$. Пусть*

$$f(X) = \sum a_{ij} X_i X_j,$$

где $a_{ij} = a_{ji}$, — квадратичная форма с коэффициентами из $\mathbf{Z}_p$, определитель которой $\det(a_{ij})$ обратим. Пусть $a \in \mathbf{Z}_p$. Тогда всякое примитивное решение уравнения $f(x) \equiv a \pmod{p}$ поднимается до точного решения.

В силу следствия 1 достаточно проверить, что x не обращает в нуль по модулю p хотя бы одну из производных полинома f. Имеем

$$\frac{\partial f}{\partial X_j} = 2 \sum_i a_{ij} X_i.$$

Так как $\det(a_{ij}) \not\equiv 0 \pmod{p}$ и так как нуль x примитивен, совершенно ясно, что одна из этих частных производных $\not\equiv 0 \pmod{p}$.

Следствие 3. *Предположим, что $p = 2$. Пусть*

$$f = \sum a_{ij} X_i X_j,$$

где $a_{ij} = a_{ji}$, — квадратичная форма с коэффициентами из $\mathbf{Z}_2$, и пусть $a \in \mathbf{Z}_2$. Пусть x — примитивное решение уравнения $f(x) \equiv 0 \pmod{8}$. Можно поднять x до точного решения, если только x не обращает в нуль по модулю 4 все производные $\partial f/\partial X_j$; это последнее условие автоматически выполняется, если $\det(a_{ij})$ обратим.

Первое утверждение вытекает из теоремы в случае $n=3$, $k=1$; второе доказывается так же, как и в случае $p \neq 2$ (с точностью до множителя 2).

§ 3. Мультипликативная группа поля $\mathbf{Q}_p$

3.1. *Фильтрация группы единиц*

Пусть $\mathbf{U}=\mathbf{Z}_p^*$ — группа p-адических единиц. Для каждого $n \geqslant 1$ рассмотрим $\mathbf{U}_n = 1 + p^n\mathbf{Z}_p$; ясно, что $\mathbf{U}_n$ является ядром гомоморфизма ε_n: $\mathbf{U} \to (\mathbf{Z}/p^n\mathbf{Z})^*$. В частности, факторгруппа $\mathbf{U}/\mathbf{U}_1$ отождествляется с $\mathbf{F}_p^*$ и, стало быть, является циклической группой порядка $p-1$ (см. теорему 2 гл. I). Группы $\mathbf{U}_n$ образуют убывающую последовательность открытых в $\mathbf{U}$ подгрупп, и мы имеем $\mathbf{U} = \varprojlim \mathbf{U}/\mathbf{U}_n$. Если $n \geqslant 1$, то отображение $(1+p^n x) \longmapsto (x$ по модулю $p)$ определяет изоморфизм

$$\mathbf{U}_n/\mathbf{U}_{n+1} \xrightarrow{\sim} \mathbf{Z}/p\mathbf{Z};$$

это вытекает из формулы

$$(1+p^n x)(1+p^n y) \equiv 1 + p^n(x+y) \pmod{p^{n+1}}.$$

Отсюда индукцией по n выводим, что $\mathbf{U}_1/\mathbf{U}_n$ — группа порядка p^{n-1}.

Лемма. *Пусть* $0 \to \mathrm{A} \to \mathrm{E} \to \mathrm{B} \to 0$ — *точная последовательность коммутативных групп (аддитивно записанных), где* A *и* B *конечны и имеют порядки* a *и* b, *взаимно простые между собой. Пусть* B' — *множество тех* $x \in \mathrm{E}$, *для которых* $bx=0$. *Группа* E *является прямой суммой групп* [1]) A *и* B'; *более того,* B' — *единственная подгруппа группы* E, *изоморфная группе* B.

Так как a и b взаимно просты, существуют такие $r, s \in \mathbf{Z}$, что $ar+bs=1$. Если $x \in \mathrm{A} \cap \mathrm{B}'$, то $ax=bx=0$, откуда $(ar+bs)x=x=0$; таким образом, $\mathrm{A} \cap \mathrm{B}'=0$. Далее, любой $x \in \mathrm{E}$ может быть записан в виде

[1]) Здесь A отождествляется со своим образом в E. — *Прим. ред.*

$x = arx + bsx$; так как $b\mathrm{B} = 0$, то $b\mathrm{E} \subset \mathrm{A}$, откуда $bsx \in \mathrm{A}$; с другой стороны, имеем $ab\mathrm{E} = 0$, откуда $arx \in \mathrm{B}'$. Таким образом, мы видим, что $\mathrm{E} = \mathrm{A} \oplus \mathrm{B}'$, а проекция $\mathrm{E} \to \mathrm{B}$ определяет изоморфизм группы B' на B. Наоборот, если B'' — подгруппа группы E, изоморфная группе B, то $b\mathrm{B}'' = 0$, откуда $\mathrm{B}'' \subset \mathrm{B}'$ и $\mathrm{B}'' = \mathrm{B}'$, поскольку эти группы имеют одинаковые порядки.

Предложение 7. *Имеет место разложение* $\mathbf{U} = \mathbf{V} \times \mathbf{U}_1$, *где*

$$\mathbf{V} = \{x \in \mathbf{U} \mid x^{p-1} = 1\}$$

есть единственная в **U** *подгруппа, изоморфная группе* $\mathbf{F}_p^*$.

Применим лемму к точной последовательности

$$1 \to \mathbf{U}_1/\mathbf{U}_n \to \mathbf{U}/\mathbf{U}_n \to \mathbf{F}_p^* \to 1,$$

что допустимо, поскольку порядок группы $\mathbf{U}_1/\mathbf{U}_{n-1}$ равен p^{n-1}, а порядок группы $\mathbf{F}_p^*$ равен $p-1$. Мы получаем, что $\mathbf{U}/\mathbf{U}_n$ содержит единственную подгруппу $\mathbf{V}_n$, изоморфную группе $\mathbf{F}_p^*$, а проекция

$$\mathbf{U}/\mathbf{U}_n \to \mathbf{U}/\mathbf{U}_{n-1}$$

изоморфно отображает $\mathbf{V}_n$ на $\mathbf{V}_{n-1}$. Из

$$\mathbf{U} = \varprojlim \mathbf{U}/\mathbf{U}_n$$

получаем, переходя к пределу, подгруппу **V** группы **U**, изоморфную группе $\mathbf{F}_p^*$; имеем $\mathbf{U} = \mathbf{V} \times \mathbf{U}_1$; единственность для **V** вытекает из единственности для $\mathbf{V}_n$.

Следствие. *Поле* $\mathbf{Q}_p$ *содержит корни* $(p-1)$*-й степени из единицы.*

Замечания. 1) Группа **V** называется группой *мультипликативных представителей* элементов группы $\mathbf{F}_p^*$.

2) Существование группы **V** может быть доказано применением следствия 1 из теоремы 1 к уравнению

$$X^{p-1} - 1 = 0.$$

3.2. *Строение группы* $\mathbf{U}_1$

Лемма. *Пусть* $x \in \mathbf{U}_n - \mathbf{U}_{n+1}$, *где* $n \geqslant 1$, *если* $p \neq 2$, *и* $n \geqslant 2$, *если* $p = 2$. *Тогда* $x^p \in \mathbf{U}_{n+1} - \mathbf{U}_{n+2}$.

Предпосылка леммы означает, что $x = 1 + kp^n$, где $k \not\equiv 0 \pmod{p}$. На основании формулы бинома имеем

$$x^p = 1 + kp^{n+1} + \ldots + k^p p^{np},$$

и показатели степени p в ненаписанных членах $\geqslant 2n+1$, тем более $\geqslant n+2$. Кроме того, имеем $np \geqslant n+2$ (благодаря тому, что $n \geqslant 2$ при $p = 2$). Отсюда заключаем, что

$$x^p \equiv 1 + kp^{n+1} \pmod{p^{n+2}},$$

откуда $x^p \in \mathbf{U}_{n+1} - \mathbf{U}_{n+2}$.

Предложение 8. *Если* $p \neq 2$, *то группа* $\mathbf{U}_1$ *изоморфна группе* $\mathbf{Z}_p$. *Если* $p = 2$, *то имеет место равенство* $\mathbf{U}_1 = \{\pm 1\} \times \mathbf{U}_2$, *где группа* $\mathbf{U}_2$ *изоморфна группе* $\mathbf{Z}_2$.

Займемся сначала случаем $p \neq 2$. Выберем элемент $\alpha \in \mathbf{U}_1 - \mathbf{U}_2$, например $\alpha = 1 + p$. По предыдущей лемме $\alpha^{p^i} \in \mathbf{U}_{i+1} - \mathbf{U}_{i+2}$. Пусть α_n — образ элемента α в группе $\mathbf{U}_1/\mathbf{U}_n$; в силу предшествующего $(\alpha_n)^{p^{n-2}} \neq 1$ и $(\alpha_n)^{p^{n-1}} = 1$. Но $\mathbf{U}_1/\mathbf{U}_n$ имеет порядок p^{n-1}; отсюда заключаем, что эта группа *циклическая*, порожденная элементом α_n.

Далее, обозначим через $\theta_{n,\alpha}$ изоморфизм $z \mapsto \alpha_n^z$ группы $\mathbf{Z}/p^{n-1}\mathbf{Z}$ на $\mathbf{U}_1/\mathbf{U}_n$. Диаграмма

$$\begin{array}{ccc} \mathbf{Z}/p^n\mathbf{Z} & \xrightarrow{\theta_{n+1,\alpha}} & \mathbf{U}_1/\mathbf{U}_{n+1} \\ \downarrow & & \downarrow \\ \mathbf{Z}/p^{n-1}\mathbf{Z} & \xrightarrow{\theta_{n,\alpha}} & \mathbf{U}_1/\mathbf{U}_n \end{array}$$

коммутативна. Отсюда заключаем, что изоморфизмы $\theta_{n,\alpha}$ определяют изоморфизм θ_α группы $\mathbf{Z}_p = \varprojlim \mathbf{Z}/p^{n-1}\mathbf{Z}$ на

$$\mathbf{U}_1 = \varprojlim \mathbf{U}_1/\mathbf{U}_n,$$

откуда следует предложение для $p \neq 2$.

Теперь предположим, что $p=2$. Тогда выберем $a \in \mathbf{U}_2 - \mathbf{U}_3$, иначе говоря, положим $a \equiv 5 \pmod 8$. Определим, как выше, изоморфизмы

$$\theta_{n,a}\colon \mathbf{Z}/2^{n-2}\mathbf{Z} \to \mathbf{U}_2/\mathbf{U}_n,$$

а отсюда изоморфизм $\theta_a\colon \mathbf{Z}_2 \to \mathbf{U}_2$. Гомоморфизм

$$\mathbf{U}_1 \to \mathbf{U}_1/\mathbf{U}_2 \simeq \mathbf{Z}/2\mathbf{Z}$$

индуцирует изоморфизм групп $\{\pm 1\}$ и $\mathbf{Z}/2\mathbf{Z}$. Поэтому $\mathbf{U}_1 = \{\pm 1\} \times \mathbf{U}_2$. Ч. т. д.

Теорема 2. *Группа* $\mathbf{Q}_p^*$ *изоморфна*

$$\mathbf{Z} \times \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}, \text{ если } p \neq 2,$$

и

$$\mathbf{Z} \times \mathbf{Z}_2 \times \mathbf{Z}/2\mathbf{Z}, \text{ если } p = 2.$$

Каждый элемент $x \in \mathbf{Q}_p^*$ единственным способом записывается в виде $x = p^n u$, где $n \in \mathbf{Z}$ и $u \in \mathbf{U}$. Таким образом, $\mathbf{Q}_p^* \simeq \mathbf{Z} \times \mathbf{U}$. Далее, предложение 7 показывает, что $\mathbf{U} = \mathbf{V} \times \mathbf{U}_1$, где $\mathbf{V}$ — циклическая группа порядка $p-1$; наконец, строение группы $\mathbf{U}_1$ дается предложением 8.

3.3. *Квадраты в* $\mathbf{Q}_p^*$

Теорема 3. *Пусть* $p \neq 2$, *и пусть* $x = p^n u$ — *элемент из* $\mathbf{Q}_p^*$, *где* $n \in \mathbf{Z}$ *и* $u \in \mathbf{U}$. *Для того чтобы элемент* x *был квадратом, необходимо и достаточно, чтобы* n *было четным и чтобы образ* $\bar{u}$ *элемента* u *в* $\mathbf{F}_p^* = \mathbf{U}/\mathbf{U}_1$ *был квадратом.*

(Это последнее условие означает, что *символ Лежандра* $\left(\frac{\bar{u}}{p}\right)$ элемента $\bar{u}$ равен 1; мы будем далее писать $\left(\frac{u}{p}\right)$ вместо $\left(\frac{\bar{u}}{p}\right)$.)

Разложим u в произведение $u = v \cdot u_1$, где $v \in \mathbf{V}$ и $u_1 \in \mathbf{U}_1$. Представление $\mathbf{Q}_p^* \simeq \mathbf{Z} \times \mathbf{V} \times \mathbf{U}_1$ (теорема 2) показывает, что x является квадратом тогда и только тогда, когда n четно, а v и u_1 являются квадратами; но $\mathbf{U}_1$ изоморфна группе $\mathbf{Z}_p$ и число 2 обратимо в $\mathbf{Z}_p$,

стало быть, любой элемент из $\mathbf{U}_1$ является квадратом. Так как $\mathbf{V}$ изоморфна группе $\mathbf{F}_p^*$, то теорема доказана.

Следствие. *Если* $p \neq 2$, *то группа* $\mathbf{Q}_p^*/\mathbf{Q}_p^{*2}$ *есть группа типа* (2, 2); *она допускает систему представителей вида* $\{1, p, u, up\}$, *где* $u \in \mathbf{U}$ *и таково, что* $\left(\frac{u}{p}\right) = -1$.

Это очевидно.

Теорема 4. *Для того чтобы элемент* $x = 2^n u$ *из* $\mathbf{Q}_2^*$ *был квадратом, необходимо и достаточно, чтобы* n *было четным и чтобы* $u \equiv 1 \pmod 8$.

Разложение $\mathbf{U} = \{\pm 1\} \times \mathbf{U}_2$ показывает, что u есть квадрат тогда и только тогда, когда u принадлежит группе $\mathbf{U}_2$ и является там квадратом. Далее, изоморфизм θ_a: $\mathbf{Z}_2 \to \mathbf{U}_2$, построенный в доказательстве предложения 8, отображает $2^n\mathbf{Z}_2$ на $\mathbf{U}_{n+2}$; отсюда заключаем (для $n = 1$), что множество квадратов из $\mathbf{U}_2$ есть $\mathbf{U}_3$. Итак, элемент $u \in \mathbf{U}$ есть квадрат тогда и только тогда, когда он сравним с 1 по модулю 8, откуда следует теорема.

Замечание. Тот факт, что любой элемент из $\mathbf{U}_3$ является квадратом, вытекает также из следствия 3 теоремы 1, примененного к квадратичной форме X^2.

Следствие. *Группа* $\mathbf{Q}_2^*/\mathbf{Q}_2^{*2}$ *есть группа типа* (2, 2, 2). *Она допускает систему представителей* $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.

Это вытекает из того факта, что $\{\pm 1, \pm 5\}$ является системой представителей для $\mathbf{U}/\mathbf{U}_3$.

Замечания. 1) Для $p = 2$ определим гомоморфизмы ε, ω: $\mathbf{U}/\mathbf{U}_3 \to \mathbf{Z}/2\mathbf{Z}$ с помощью формул из п. 3.2 гл. I:

$$\varepsilon(z) \equiv \frac{z-1}{2} \pmod 2 = \begin{cases} 0, & \text{если } z \equiv 1 \pmod 4, \\ 1, & \text{если } z \equiv -1 \pmod 4; \end{cases}$$

$$\omega(z) \equiv \frac{z^2-1}{8} \pmod 2 = \begin{cases} 0, & \text{если } z \equiv \pm 1 \pmod 8, \\ 1, & \text{если } z \equiv \pm 5 \pmod 8. \end{cases}$$

Ясно, что ε определяет изоморфизм группы $\mathbf{U}/\mathbf{U}_2$ на $\mathbf{Z}/2\mathbf{Z}$, а ω определяет изоморфизм группы $\mathbf{U}_2/\mathbf{U}_3$ на $\mathbf{Z}/2\mathbf{Z}$. Пара (ε, ω) определяет, таким образом, *изоморфизм группы* $\mathbf{U}/\mathbf{U}_3$ *на* $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$; в частности, 2-адическая единица z является квадратом тогда и только тогда, когда $\varepsilon(z) = \omega(z) = 0$.

2) Теоремы 3 и 4 показывают, что $\mathbf{Q}_p^{*2}$ есть *открытая* подгруппа группы $\mathbf{Q}_p^*$.

Глава III

СИМВОЛ ГИЛЬБЕРТА

§ 1. Локальные свойства

В этом параграфе буквой k обозначается либо поле $\mathbf{R}$ вещественных чисел, либо поле $\mathbf{Q}_p$ p-адических чисел (p — простое число).

1.1. *Определение и простейшие свойства*

Пусть $a,\ b \in k^*$. Положим

$(a,\ b) = 1$, если $z^2 - ax^2 - by^2 = 0$ имеет решение $\neq (0, 0, 0)$ в k^3;
$(a,\ b) = -1$ в противном случае.

Число $(a,\ b) = \pm 1$ называется *символом Гильберта* элементов a и b относительно поля k. Ясно, что $(a,\ b)$ не изменяется, когда элементы a и b умножаются на *квадраты*; символ Гильберта определяет, таким образом, *отображение группы* $k^*/k^{*2} \times k^*/k^{*2}$ *в* $\{\pm 1\}$.

Предложение 1. *Пусть* $a,\ b \in k^*$, *и пусть* $k_b = k(\sqrt{b})$ *— поле, получаемое присоединением к* k *квадратного корня из* b. *Для* $(a,\ b) = 1$ *необходимо и достаточно, чтобы* a *принадлежало группе* $\mathrm{N}k_b^*$ *норм элементов из* k_b^*.

Если b является квадратом элемента c, то уравнению

$$z^2 - ax^2 - by^2 = 0$$

удовлетворяет решение $(c, 0, 1)$ и мы имеем $(a,\ b) = 1$, откуда вытекает предложение в этом случае, поскольку здесь $k_b = k$ и $\mathrm{N}k_b^* = k_b^*$. Если b не является

квадратом, то k_b — квадратичное расширение поля k; если через β обозначить квадратный корень из b, то любой элемент $\xi \in k_b$ записывается в виде $z + \beta y$, где $y,\ z \in k$, и норма $N(\xi)$ элемента ξ равна $z^2 - by^2$. Если $a \in Nk_b^*$, то существуют такие $y,\ z \in k$, что $a = z^2 - by^2$; поэтому $(z,\ 1,\ y)$ — нуль квадратичной формы $z^2 - ax^2 - by^2$ и мы имеем $(a,\ b) = 1$. Наоборот, если $(a,\ b) = 1$, то эта форма имеет нуль $(z,\ x,\ y) \neq (0,\ 0,\ 0)$. Необходимо, чтобы $x \neq 0$, так как иначе b было бы квадратом; отсюда заключаем, что a есть норма элемента $\frac{z}{x} + \beta \frac{y}{x}$.

Предложение 2. *Символ Гильберта удовлетворяет формулам*

i) $(a,\ b) = (b,\ a),\ (a,\ c^2) = 1$;
ii) $(a,\ -a) = 1,\ (a,\ 1-a) = 1$;
iii) *если* $(a,\ b) = 1$, *то* $(aa',\ b) = (a',\ b)$;
iv) $(a,\ b) = (a,\ -ab) = (a,\ (1-a)\,b)$.

(В этих формулах через $a,\ a',\ b,\ c$ обозначены элементы из k^*; предполагается, что $a \neq 1$, когда формула содержит член $1 - a$.)

Формулы i) очевидны. Если $b = -a$ (соответственно $b = 1 - a$), то квадратичная форма $z^2 - ax^2 - by^2$ имеет нуль $(0,\ 1,\ 1)$ (соответственно $(1,\ 1,\ 1)$); поэтому $(a,\ b) = 1$, что и доказывает ii). Если $(a,\ b) = 1$, то, на основании предложения 1, a принадлежит подгруппе Nk_b^*; поэтому

$$a' \in Nk_b^* \Leftrightarrow aa' \in Nk_b^*,$$

что и доказывает iii). Формула iv) следует из i), ii), iii).

Замечание. Формула iii) является частным случаем формулы

v) $$(aa',\ b) = (a,\ b)(a',\ b),$$

которая выражает *билинейность* символа Гильберта; эта формула будет доказана в следующем пункте.

1.2. *Вычисление символа* (a, b)

Теорема 1. *Если* $k = \mathbf{R}$, *то* $(a, b) = 1$, *когда* a *или* $b > 0$, *и* $(a, b) = -1$, *когда* a *и* $b < 0$.

Если $k = \mathbf{Q}_p$ *и если* a *и* b *записаны в форме* $p^\alpha u$, $p^\beta v$, *где* u *и* v *принадлежат группе* $\mathbf{U}$ *p-адических единиц, то*

$$(a, b) = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha, \quad \text{когда } p \neq 2,$$

$$(a, b) = (-1)^{\varepsilon(u)\,\varepsilon(v) + \alpha\omega(v) + \beta\omega(u)}, \quad \text{когда } p = 2.$$

[Напомним, что через $\left(\frac{u}{p}\right)$ обозначается *символ Лежандра* $\left(\frac{\bar{u}}{p}\right)$, где $\bar{u}$ — образ элемента u при гомоморфизме редуцирования по модулю p: $\mathbf{U} \to \mathbf{F}_p^*$. Что касается $\varepsilon(u)$ и $\omega(u)$, то они обозначают соответственно классы по модулю 2 элементов $\frac{u-1}{2}$ и $\frac{u^2-1}{8}$, см. п. 3.3 гл. II.]

Теорема 2. *Символ Гильберта есть невырожденная билинейная форма на* $\mathbf{F}_2$*-векторном пространстве* k^*/k^{*2}.

[Билинейность символа (a, b) не что иное, как формула v), приведенная в конце п. 1.1; утверждение «(a, b) невырождено» означает, что если $b \in k^*$ таково, что $(a, b) = 1$ для любого $a \in k^*$, то $b \in k^{*2}$.]

Следствие. *Если* b *не является квадратом, то группа* $\mathrm{N}k_b^*$, *определенная в предложении* 1, *является подгруппой индекса* 2 *в* k^*.

По предложению 1 гомоморфизм φ_b: $k^* \to \{\pm 1\}$, определяемый отображением

$$\varphi_b(a) = (a, b),$$

имеет ядром $\mathrm{N}k_b^*$; с другой стороны, φ_b сюръективен из-за невырожденности символа (a, b). Таким образом, φ_b определяет изоморфизм группы $k^*/\mathrm{N}k_b^*$ на $\{\pm 1\}$; отсюда вытекает следствие.

Замечание. В более общей ситуации пусть L—конечное расширение Галуа поля k, группа Галуа G которого *коммутативна*. Можно показать, что группа k^*/NL^* *изоморфна* группе G и что знание группы NL^* *определяет* поле L; в этом заключаются два главных результата так называемой «локальной теории полей классов».

Доказательство теорем 1 *и* 2.

Случай $k = \mathbf{R}$ тривиален; заметим, что здесь k^*/k^{*2} является векторным пространством размерности 1 (над $\mathbf{F}_2$), причем в качестве системы представителей допустим набор $\{1, -1\}$.

Предположим теперь, что $k = \mathbf{Q}_p$.

Лемма. *Пусть* $v \in \mathbf{U}$ *есть* p*-адическая единица. Если уравнение* $z^2 - px^2 - vy^2 = 0$ *имеет нетривиальное решение в* $\mathbf{Q}_p$, *то оно имеет такое решение* (z, x, y), *что* $z, y \in \mathbf{U}$ *и* $x \in \mathbf{Z}_p$.

На основании предложения 6 п. 2.1 гл. II рассматриваемое уравнение имеет *примитивное* решение (z, x, y). Покажем, что это решение отвечает требуемому условию. Если бы это было не так, то мы имели бы либо $y \equiv 0 \pmod p$, либо $z \equiv 0 \pmod p$; поскольку $z^2 - vy^2 \equiv 0 \pmod p$ и $v \not\equiv 0 \pmod p$, мы имели бы одновременно $y \equiv 0 \pmod p$ и $z \equiv 0 \pmod p$, откуда $px^2 \equiv 0 \pmod{p^2}$, т. е. $x \equiv 0 \pmod p$, вопреки примитивности решения (x, y, z).

Вернемся теперь к доказательству теоремы 1 и *предположим сначала, что* $p \neq 2$.

Ясно, что показатели α и β выступают лишь как их вычеты по модулю 2; в силу симметрии символа надлежит рассмотреть три случая.

1) $\alpha = 0$, $\beta = 0$. Надо проверить, что $(u, v) = 1$. Тогда уравнение

$$z^2 - ux^2 - vy^2 = 0$$

имеет нетривиальное решение по модулю p (см. следствие 2 теоремы 3 § 2 гл. I); так как дискриминант рассматриваемой квадратичной формы есть p-адическая единица, то это решение поднимается до

p-адического решения (следствие 2 теоремы 1 п. 2.2 гл. II); таким образом, $(u, v) = 1$.

2) $\alpha = 1$, $\beta = 0$. Надо проверить, что $(pu, v) = \left(\frac{v}{p}\right)$. Так как $(u, v) = 1$, то мы имеем $(pu, v) = (p, v)$ по формуле iii) предложения 2; таким образом, достаточно проверить, что $(p, v) = \left(\frac{v}{p}\right)$. Это ясно, когда v квадрат, ибо тогда оба члена равны 1. В противном случае имеем $\left(\frac{v}{p}\right) = -1$, см. теорему 3 п. 3.3 гл. II; приведенная выше лемма показывает, что здесь форма $z^2 - px^2 - vy^2$ не имеет нетривиального нуля, а потому $(p, v) = -1$.

3) $\alpha = 1$, $\beta = 1$. Надо проверить, что

$$(pu, pv) = (-1)^{(p-1)/2} \left(\frac{u}{p}\right)\left(\frac{v}{p}\right).$$

Однако формула iv) предложения 2 показывает, что

$$(pu, pv) = (pu, -p^2uv) = (pu, -uv).$$

На основании только что доказанного имеем

$$(pu, pv) = \left(\frac{-uv}{p}\right),$$

откуда вытекает искомый результат, поскольку $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Так как теорема 1 установлена (для $p \neq 2$), то из нее выводим (в этом случае) теорему 2; действительно, формула, полученная для (a, b), показывает, что (a, b) — билинейная форма; для доказательства того, что эта форма невырожденная, достаточно предъявить для любого $a \in k^*/k^{*2}$, отличного от нейтрального элемента, такой элемент b, что $(a, b) = -1$. На основании следствия из теоремы 3 п. 3.3 гл. II можно взять $a = p$, u или up, где $u \in \mathbf{U}$ таково, что $\left(\frac{u}{p}\right) = -1$; тогда в качестве b выберем соответственно u, p и u.

Случай $p=2$. Здесь по-прежнему α и β выступают лишь как вычеты по модулю 2 и надо рассмотреть три случая.

1) $\alpha=0$, $\beta=0$. Надо показать, что $(u, v)=1$, когда u или v сравнимы с 1 (mod 4), и что $(u, v)=-1$ в противном случае. Предположим сначала, что $u\equiv 1 \pmod 4$. Тогда либо $u\equiv 1 \pmod 8$, либо $u\equiv 5 \pmod 8$. В первом случае u является квадратом (см. теорему 4 п. 3.3 гл. II) и мы имеем $(u, v)=1$. Во втором случае $u+4v\equiv 1 \pmod 8$ и существует такое $w\in \mathbf{U}$, что $w^2=u+4u$; поэтому форма $z^2-ux^2-vy^2$ имеет в качестве нуля $(w, 1, 2)$ и $(u, v)=1$. Теперь предположим, что $u\equiv v\equiv -1 \pmod 4$; если (z, x, y) является примитивным решением уравнения

$$z^2-ux^2-vy^2=0,$$

то $z^2+x^2+y^2\equiv 0 \pmod 4$; но квадраты в $\mathbf{Z}/4\mathbf{Z}$ суть 0 и 1; из нашего сравнения вытекает, что x, y, z сравнимы с $0 \pmod 2$, вопреки предположенной примитивности решения. Таким образом, в этом случае мы получаем, что $(u, v)=-1$.

2) $\alpha=1$, $\beta=0$. Надо проверить, что

$$(2u, v)=(-1)^{\varepsilon(u)\,\varepsilon(v)+\omega(v)}.$$

Покажем сначала, что $(2, v)=(-1)^{\omega(v)}$, т. е. что равенство $(2, v)=1$ равносильно сравнению $v\equiv \pm 1 \pmod 8$. На основании приведенной выше леммы, если $(2, v)=1$, то существуют такие $x, y, z\in \mathbf{Z}_2$, что $z^2-2x^2-vy^2=0$ и $y, z\not\equiv 0 \pmod 2$. Тогда $y^2\equiv z^2\equiv 1 \pmod 8$, откуда $1-2x^2-v\equiv 0 \pmod 8$. Но единственными квадратами по модулю 8 являются 0, 1 и 4; отсюда вытекает, что $v\equiv \pm 1 \pmod 8$. Обратно, если $v\equiv 1 \pmod 8$, то v является квадратом и $(2, v)=1$; если $v\equiv -1 \pmod 8$, то уравнение $z^2-2x^2-vy^2=0$ допускает $(1, 1, 1)$ в качестве решения по модулю 8, и это приближенное решение поднимается до настоящего решения (см. следствие 3 теоремы 1 п. 2.2 гл. II). Таким образом, $(2, v)=1$.

Остается доказать, что $(2u, v)=(2, v)(u, v)$. Действительно, на основании предложения 2 это верно, если $(2, v)=1$ или $(u, v)=1$. Остается случай

$(2, v)=(u, v)=-1$, т. е. $v\equiv 3 \pmod 8$ и $u\equiv 3$ или $-1 \pmod 8$; допуская умножение элементов u и v на квадраты, можно предположить, что $u=-1$, $v=3$ или $u=3$, $v=-5$; однако уравнения

$$z^2+2x^2-3y^2=0 \quad \text{и} \quad z^2-6x^2+5y^2=0$$

имеют решение (1, 1, 1); таким образом, $(2u, v)=1$.

3) $\alpha=1$, $\beta=1$. Надо проверить, что

$$(2u, 2v)=(-1)^{\varepsilon(u)\,\varepsilon(v)+\omega(u)+\omega(v)}.$$

Однако формула iv) предложения 2 показывает, что

$$(2u, 2v)=(2u, -4uv)=(2u, -uv).$$

На основании только что доказанного

$$(2u, 2v)=(-1)^{\varepsilon(u)\,\varepsilon(-uv)+\omega(-uv)}.$$

Так как $\varepsilon(-1)=1$, $\omega(-1)=0$ и $\varepsilon(u)(1+\varepsilon(u))=0$, то показатель в последней формуле равен $\varepsilon(u)\varepsilon(v)+{}$ $+\omega(u)+\omega(v)$, что и завершает доказательство теоремы 1. Билинейность символа (a, b) вытекает из полученной для него формулы, поскольку ε и ω являются гомоморфизмами. Невырожденность проверяется на мультипликативных представлениях $\{u, 2u\}$, где $u=1, 5, -1$ или -5; действительно, $(5, 2u)=-1$ и $(-1, -1)=(-1, -5)=-1$.

Замечание. Можно явно найти матрицу билинейной формы (a, b) относительно *базиса* пространства k^*/k^{*2}.

Если $k=\mathbf{R}$, то матрица есть (-1).

Если $k=\mathbf{Q}_p$, $p\neq 2$, то в базисе $\{p, u\}$, где $\left(\frac{u}{p}\right)=-1$, матрица имеет вид $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ в случае $p\equiv 1 \pmod 4$ и $\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$ в противном случае.

Если $k=\mathbf{Q}_2$, то в базисе $\{2, -1, 5\}$ матрица имеет вид

$$\begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{pmatrix}.$$

§ 2. Глобальные свойства

Поле рациональных чисел $\mathbf{Q}$ погружается в качестве всюду плотного подполя в каждое из полей $\mathbf{Q}_p$ и $\mathbf{R}$. Если $a, b \in \mathbf{Q}^*$, то мы обозначим через $(a, b)_p$ (соответственно через $(a, b)_\infty$) символ Гильберта их образов в $\mathbf{Q}_p$ (соответственно в $\mathbf{R}$). Обозначим через V объединение множества простых чисел и символа ∞; положим $\mathbf{Q}_\infty = \mathbf{R}$.

2.1. *Формула произведения*

Теорема 3 (Гильберт). *Если* $a, b \in \mathbf{Q}^*$, *то* $(a, b)_v = 1$ *почти для всех* $v \in \mathrm{V}$ *и*

$$\prod_{v \in \mathrm{V}} (a, b)_v = 1.$$

(Выражение «почти для всех $v \in \mathrm{V}$» означает «для всех элементов из V кроме конечного числа».)

Поскольку символ Гильберта билинеен, достаточно доказать теорему в случае, когда a и b равны -1 или простому числу. В каждом случае теорема 1 позволяет вычислить значения $(a, b)_v$.

1) $a = -1$, $b = -1$. Имеем $(-1, -1)_\infty = (-1, -1)_2 = -1$ и $(-1, -1)_p = 1$, если $p \neq 2, \infty$; произведение в точности равно 1.

2) $a = -1$, $b = l$, где l простое. Если $l = 2$, то

$$(-1, 2)_v = 1 \quad \text{для всех} \quad v \in \mathrm{V};$$

если $l \neq 2$, то

$$(-1, l)_v = 1 \quad \text{для} \quad v \neq 2, l$$

и

$$(-1, l)_2 = (-1, l)_l = (-1)^{\varepsilon(l)};$$

произведение в точности равно 1.

3) $a = l$, $b = l'$, где l, l' простые. Если $l = l'$, то формула iv) предложения 2 показывает, что

$$(l, l)_v = (-1, l)_v$$

для всех $v \in \mathrm{V}$, и мы возвращаемся к случаю, описанному выше. Если $l \neq l'$ и $l' = 2$, то имеем $(l, 2)_v = 1$

для $v \neq 2, l$ и $(l, 2)_2 = (-1)^{\omega(l)}$, $(l, 2)_l = \left(\frac{2}{l}\right) = (-1)^{\omega(l)}$, см. теорему 5 п. 3.2 гл. I. Если l и l' различны и отличны от 2, то $(l, l')_v = 1$ для всех $v \neq 2, l, l'$ и $(l, l')_2 = (-1)^{\varepsilon(l)\varepsilon(l')}$, $(l, l')_l = \left(\frac{l'}{l}\right)$, $(l, l')_{l'} = \left(\frac{l}{l'}\right)$; но на основании квадратичного закона взаимности (см. теорему 6 п. 3.3 гл. I) мы имеем

$$\left(\frac{l'}{l}\right)\left(\frac{l}{l'}\right) = (-1)^{\varepsilon(l)\varepsilon(l')};$$

произведение в точности равно 1. Это завершает доказательство.

Замечание. Формула произведения по существу эквивалентна квадратичному закону взаимности. Интерес к ней обеспечивается в значительной степени тем, что ее можно распространить на *любое поле алгебраических чисел* (множество V при этом заменяется множеством дивизоров поля).

2.2. *Существование рациональных чисел с данными символами Гильберта*

Теорема 4. *Пусть* $(a_i)_{i \in I}$ — *конечное семейство элементов из* $\mathbf{Q}^*$, *и пусть* $(\varepsilon_{i,v})_{i \in I,\, v \in V}$ — *семейство чисел, равных* ± 1. *Для того чтобы существовало такое число* $x \in \mathbf{Q}^*$, *что* $(a_i, x)_v = \varepsilon_{i,v}$ *при каждом* $i \in I$ *и при каждом* $v \in V$, *необходимо и достаточно выполнение следующих трех условий*:

(1) *почти все* $\varepsilon_{i,v}$ *равны* 1;

(2) $\prod_{v \in V} \varepsilon_{i,v} = 1$ *для любого* $i \in I$;

(3) *для любого* $v \in V$ *существует такое* $x_v \in \mathbf{Q}_v^*$, *что*

$$(a_i, x_v)_v = \varepsilon_{i,v}$$

при всех $i \in I$.

Необходимость условий (1) и (2) вытекает из теоремы 3; необходимость условия (3) тривиальна (ибо можно взять $x_v = x$).

Для доказательства достаточности этих условий нам понадобятся следующие три леммы.

Лемма 1 («китайская лемма»). *Пусть* $a_1, \ldots, a_n$, $m_1, \ldots, m_n$ — *целые числа, причем числа* m_i *попарно взаимно просты. Тогда существует такое целое* a, *что* $a \equiv a_i \pmod{m_i}$ *для всех* i.

Пусть m есть произведение чисел m_i. Из теоремы Безу выводим, что канонический гомоморфизм

$$\mathbf{Z}/m\mathbf{Z} \to \prod_{i=1}^{n} \mathbf{Z}/m_i\mathbf{Z}$$

является изоморфизмом. Отсюда вытекает лемма.

Лемма 2 («аппроксимационная теорема»). *Пусть* S *есть конечная часть множества* V. *Тогда образ поля* $\mathbf{Q}$ *в* $\prod_{v \in S} \mathbf{Q}_v$ *плотен в этом произведении* (в топологии произведения топологий полей $\mathbf{Q}_v$).

Расширяя в случае надобности множество S, мы можем предполагать, что

$$S = \{\infty, p_1, \ldots, p_n\},$$

где p_i суть различные простые числа, и речь идет о доказательстве того, что $\mathbf{Q}$ плотно в $\mathbf{R} \times \mathbf{Q}_{p_1} \times \ldots \ldots \times \mathbf{Q}_{p_n}$. Пусть $(x_\infty, x_1, \ldots, x_n)$ — точка в этом произведении; докажем, что эта точка является точкой прикосновения для $\mathbf{Q}$. Умножая в случае надобности координаты точки на целое число, мы можем предполагать, что $x_i \in \mathbf{Z}_{p_i}$ для всех $1 \leqslant i \leqslant n$; речь идет о доказательстве того, что для любого $\varepsilon > 0$ и любого $N \geqslant 0$ существует такое $x \in \mathbf{Q}$, что

$$|x - x_\infty| \leqslant \varepsilon \quad \text{и} \quad v_{p_i}(x - x_i) \geqslant N \quad \text{для} \quad i = 1, \ldots, n.$$

На основании леммы 1, примененной к $m_i = p_i^N$, существует такое $x_0 \in \mathbf{Z}$, что $v_{p_i}(x_0 - x_i) \geqslant N$ для всех i. Выберем, с другой стороны, целое $q \geqslant 2$, которое взаимно просто со всеми p_i (например, простое число). Легко видеть, что рациональные числа вида a/q^m, $a \in \mathbf{Z}$, $m \geqslant 0$, *плотны в* $\mathbf{R}$ (это обеспечивается просто тем, что $q^m \to \infty$ при $m \to \infty$). Поэтому можно выбрать такое число $u = a/q^m$, что

$$|x_0 - x_\infty + up_1^N \ldots p_n^N| \leqslant \varepsilon.$$

Тогда рациональное число $x = x_0 + up_1^N \dots p_n^N$ удовлетворяет требуемым условиям.

Лемма 3 («теорема Дирихле»). *Если a и m суть взаимно простые целые положительные числа, то существует бесконечно много таких простых чисел p, что $p \equiv a \pmod m$.*

Доказательство будет дано в главе VI; читатель может проверить, что оно не использует никаких результатов из глав III, IV и V.

Возвратимся теперь к теореме 4; пусть $(\varepsilon_{i,v})$ является семейством чисел, равных ± 1 и удовлетворяющих условиям 1), 2) и 3). Умножая в случае надобности числа a_i на квадраты целых чисел, мы можем предполагать, что все a_i — *целые*. Пусть S является подмножеством множества V, составленным из ∞, 2 и простых делителей чисел a_i; пусть T — множество тех элементов $v \in V$, для которых существует $i \in I$, такие, что $\varepsilon_{i,v} = -1$; эти два множества конечны. Будем различать два случая

1) *Множества* S *и* T *не пересекаются.*

Положим

$$a = \prod_{\substack{l \in T \\ l \neq \infty}} l \quad \text{и} \quad m = 8 \prod_{\substack{l \in S \\ l \neq 2, \infty}} l.$$

Так как $S \cap T = \varnothing$, то целые a и m взаимно просты и по лемме 3 существует такое простое число $p \equiv a \pmod m$, что $p \notin S \cup T$.

Покажем, что число $x = ap$ является искомым, а именно, что $(a_i, x)_v = \varepsilon_{i,v}$ для всех $i \in I$ и всех $v \in V$.

Если $v \in S$, то имеем $\varepsilon_{i,v} = 1$, поскольку $S \cap T = \varnothing$, и нам нужно проверить, что $(a_i, x)_v = 1$. Если $v = \infty$, то это обеспечивается тем, что $x > 0$; если v есть простое число l, то $x \equiv a^2 \pmod m$, откуда $x \equiv a^2 \pmod 8$ для $l = 2$, $x \equiv a^2 \pmod l$ для $l \neq 2$; так как x и a являются l-адическими единицами, то эти сравнения показывают, что x есть квадрат в $\mathbf{Q}_l^*$ (см. п. 3.3 гл. II), а потому $(a_i, x)_v = 1$.

Если $v=l$ не принадлежит множеству S, то a_l является l-адической единицей. Так как $l \neq 2$, то

$$(a_i, b)_l = \left(\frac{a_l}{l}\right)^{v_l(b)} \quad \text{для любого} \quad b \in \mathbf{Q}_l^*;$$

см. теорему 1. Если $l \notin \mathrm{T} \cup \{p\}$, то x является l-адической единицей, откуда $v_l(x)=0$, и написанная выше формула показывает, что $(a_i, x)_l = 1$; с другой стороны, $\varepsilon_{i,l}=1$, ибо $l \notin \mathrm{T}$. Если $l \in \mathrm{T}$, то имеем $v_l(x)=1$; с другой стороны, условие (3) показывает, что существует такое число $x_l \in \mathbf{Q}_l^*$, что $(a_i, x_l)_l = \varepsilon_{i,l}$ для всех $i \in \mathrm{I}$; так как одно из чисел $\varepsilon_{i,l}$ равно -1 (поскольку l принадлежит множеству T), то $v_l(x_l) \equiv 1 \pmod 2$, откуда

$$(a_i, x)_l = \left(\frac{a_l}{l}\right) = (a_i, x_l)_l = \varepsilon_{i,l} \quad \text{для всех} \quad i \in \mathrm{I}.$$

Наконец, остается случай $l=p$, который сводится к остальным в силу формулы произведения:

$$(a_i, x)_p = \prod_{v \neq p} (a_i, x)_v = \prod_{v \neq p} \varepsilon_{i,v} = \varepsilon_{i,p}.$$

Это завершает доказательство теоремы 4 в случае $\mathrm{S} \cap \mathrm{T} = \varnothing$.

2) *Общий случай.*

Известно, что квадраты элементов из $\mathbf{Q}_v^*$ образуют в $\mathbf{Q}_v^*$ открытую подгруппу, см. п. 3.3 гл. II. Поэтому по лемме 2 существует такое $x' \in \mathbf{Q}^*$, что x'/x_v является квадратом в $\mathbf{Q}_v^*$ для всех $v \in \mathrm{S}$. В частности,

$$(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v} \quad \text{для всех} \quad v \in \mathrm{S}.$$

Если положить $\eta_{i,v} = \varepsilon_{i,v}(a_i, x')_v$, то семейство $\eta_{i,v}$ удовлетворяет условиям (1), (2), (3), и кроме того, $\eta_{i,v}=1$ для $v \in \mathrm{S}$. По доказанному в 1) существует такое число $y \in \mathbf{Q}^*$, что

$$(a_i, y)_v = \eta_{i,v}$$

для всех $i \in \mathrm{I}$ и всех $v \in \mathrm{V}$. Если положить $x = yx'$, то ясно, что x удовлетворяет требуемому условию.

Глава IV

КВАДРАТИЧНЫЕ ФОРМЫ НАД $\mathbf{Q}_p$ И НАД $\mathbf{Q}$

§ 1. Квадратичные формы

1.1. *Определения*

Напомним сначала основные понятия теории квадратичных форм (см. Н. Бурбаки, Алгебра, гл. IX, § 3, п. 4).

Определение 1. *Пусть* V — *модуль над коммутативным кольцом* A. *Отображение* $Q\colon V \to A$ *называется квадратичной формой над* V, *если*:

1) *имеет место* $Q(ax) = a^2 Q(x)$, *где* $a \in A$ *и* $x \in V$;

2) *отображение* $(x, y) \mapsto Q(x+y) - Q(x) - Q(y)$ *есть билинейная форма.*

Пара (V, Q) называется *квадратичным модулем.*

Во всей этой главе мы будем ограничиваться случаем, когда кольцо A является *полем k характеристики* $\neq 2$; A-модуль V тогда является векторным k-пространством; мы будем предполагать его *конечномерным.*

Положим

$$x.y = \frac{1}{2}[Q(x+y) - Q(x) - Q(y)];$$

это имеет смысл, поскольку характеристика поля k отлична от 2. Отображение $(x, y) \mapsto x.y$ есть *билинейная симметрическая форма* над V; она называется *скалярным произведением,* ассоциированным с Q. Имеем $Q(x) = x.x$. Этим устанавливается биективное соответствие между *квадратичными формами* и *билинейными симметрическими формами* (такого соответствия нет при характеристике 2).

Если (V, Q) и (V′, Q′) — два квадратичных модуля, то мы назовем *морфизмом* (или *метрическим мор-*

физмом) (V, Q) в (V′, Q′) такое линейное отображение f: $V \to V'$, что $Q' \circ f = Q$; тогда $f(x).f(y) = x.y$, если $x, y \in V$.

Матрица квадратичной формы. Пусть $(e_i)_{1 \leqslant i \leqslant n}$ — базис пространства V. Назовем матрицей квадратичной формы Q относительно этого базиса матрицу $A = (a_{ij})$, где $a_{ij} = e_i . e_j$; эта матрица — симметрическая. Если $x = \sum x_i e_i$ — элемент из V, то

$$Q(x) = \sum_{i,\,j} a_{ij} x_i x_j,$$

а это показывает, что $Q(x)$ является «квадратичной формой» от $x_1, \ldots, x_n$ в обычном смысле.

Если изменить базис (e_i) при помощи обратимой матрицы X, то матрицей A′ квадратичной формы Q по отношению к новому базису будет $X.A.{}^tX$, где через ${}^tX$ обозначается транспонированная к X матрица. В частности,

$$\det(A') = \det(A) \cdot \det(X)^2,$$

а это показывает, что $\det(A)$ *определен с точностью до умножения на элемент из* k^{*2}; его называют *дискриминантом* квадратичной формы Q и обозначают $\operatorname{disc}(Q)$.

1.2. *Ортогональность*

Пусть (V, Q) — квадратичный модуль над k. Два элемента x, y из V называются *ортогональными*, если $x.y = 0$. Множество элементов, ортогональных к подмножеству H пространства V, обозначается [1]) через H^0; это векторное подпространство пространства V. Если V_1 и V_2 два векторных подпространства в V, то говорят, что V_1 и V_2 *ортогональны* в том случае, когда $V_1 \subset V_2^0$, т. е. когда $x \in V_1$, $y \in V_2$ влечет $x.y = 0$.

---

[1]) И в дальнейшем называется *ортогоналом* к H. — *Прим. перев.*

Ортогонал V^0 ко всему пространству V называется *радикалом* (или *ядром*) пространства V и обозначается через rad (V). Его коразмерность называется *рангом* квадратичной формы Q. Если $V^0 = 0$, то говорят, что Q — *невырожденная* форма [1]); это равносильно тому, что Q имеет дискриминант $\neq 0$ (в таком случае дискриминант можно рассматривать как элемент группы k^*/k^{*2}).

Пусть U — векторное подпространство в V, и пусть U^* — подпространство, сопряженное к U. Пусть q_U: $V \to U^*$ — отображение, сопоставляющее каждому $x \in V$ линейную форму ($y \in U \mapsto x.y$). Ядро отображения q_U есть U^0. В частности, ясно, что Q — невырожденная форма тогда и только тогда, когда q_V: $V \to V^*$ есть *изоморфизм.*

Определение 2. *Пусть* $U_1, \ldots, U_m$ — *векторные подпространства пространства* V. *Будем говорить, что* V *есть прямая ортогональная сумма подпространств* U_i, *если эти подпространства попарно ортогональны, а* V *есть их прямая сумма. В этом случае будем писать*

$$V = U_1 \hat{\oplus} \ldots \hat{\oplus} U_m.$$

Замечание. Если $x \in V$ имеет x_i в качестве составляющей в U_i, то

$$Q(x) = Q_1(x_1) + \ldots + Q_m(x_m),$$

где $Q_i = Q|U_i$ обозначает ограничение квадратичной формы Q на U_i. Обратно, если (U_i, Q_i) — семейство квадратичных модулей, то написанная выше формула снабжает пространство $V = \oplus U_i$ квадратичной формой Q, называемой *прямой суммой* квадратичных форм Q_i, причем $V = U_1 \hat{\oplus} \ldots \hat{\oplus} U_m$.

Предложение 1. *Если* U *есть дополнительное подпространство к* rad (V) *в* V, *то* $V = U \hat{\oplus} \mathrm{rad}(V)$.

Это очевидно.

[1]) И что модуль (V, Q) *не вырожден.* — *Прим. перев.*

Предложение 2. *Предположим, что квадратичный модуль* (V, Q) *не вырожден. Тогда:*

i) *Любой метрический морфизм* (V, Q) *в квадратичный модуль* (V′, Q′) *инъективен.*

ii) *Для любого векторного подпространства* U *пространства* V

$$U^{00} = U, \quad \dim U + \dim U^0 = \dim V,$$

$$\operatorname{rad}(U) = \operatorname{rad}(U^0) = U \cap U^0.$$

Для невырожденности U *необходима и достаточна невырожденность* U^0; *в этом случае* $V = U \hat{\oplus} U^0$.

iii) *Если* V *— прямая ортогональная сумма двух подпространств, то они невырождены и каждое из них является ортогоналом к другому.*

Если $f\colon V \to V'$ — метрический морфизм и если $f(x) = 0$, то $x.y = f(x).f(y) = 0$ для каждого $y \in V$; отсюда $x = 0$, поскольку модуль (V, Q) не вырожден.

Если U — векторное подпространство пространства V, то определенный выше гомоморфизм $q_U\colon V \to U^*$ *сюръективен*; действительно, он представляется суперпозицией гомоморфизма $q_V\colon V \to V^*$ и канонической сюръекции $V^* \to U^*$, а по предположению q_V биективно. Поэтому имеет место точная последовательность

$$0 \to U^0 \to V \to U^* \to 0,$$

откуда $\dim V = \dim U^* + \dim U^0 = \dim U + \dim U^0$.

Это показывает, что U и U^{00} имеют одинаковую размерность; так как U содержится в U^{00}, имеем $U = U^{00}$; формула $\operatorname{rad}(U) = U \cap U^0$ очевидна; применяя ее к U^0 и учитывая, что $U^{00} = U$, выводим отсюда, что $\operatorname{rad}(U^0) = \operatorname{rad}(U)$, что дает одновременно последнее утверждение в ii). Наконец, iii) тривиально.

1.3. *Изотропные векторы*

Определение 3. *Говорят, что элемент x квадратичного модуля* (V, Q) *изотропен, если* $Q(x) = 0$. *Говорят, что подпространство* U *пространства* V *изотропно, если все его элементы изотропны.*

Очевидно, что

$$U \text{ изотропно} \Leftrightarrow U \subset U^0 \Leftrightarrow Q \mid U = 0.$$

Определение 4. *Гиперболической плоскостью называется любой квадратичный модуль, имеющий базис, состоящий из двух изотропных элементов x, y, таких, что $x.y \neq 0$.*

Умножая в случае необходимости элемент y на $1/x.y$, можно предполагать, что $x.y = 1$. Матрицей квадратичной формы по отношению к x, y тогда является просто $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; ее дискриминант есть -1 (в частности, она невырожденная).

Предложение 3. *Пусть x — изотропный элемент $\neq 0$ из невырожденного квадратичного модуля* (V, Q). *Тогда существует подпространство U в* V, *которое содержит x и которое является гиперболической плоскостью.*

Так как (V, Q) не вырожден, то существует $z \in V$, такой, что $x.z = 1$. Элемент $y = 2z - (z.z)x$ изотропен, и $x.y = 2$. Подпространство $U = kx + ky$ обладает требуемыми свойствами.

Следствие. *Если модуль* (V, Q) *не вырожден и содержит ненулевой изотропный элемент, то* $Q(V) = k$.

(Иными словами, для всякого $a \in k$ существует такой $v \in V$, что $Q(v) = a$.)

В силу предложения достаточно провести доказательство в случае, когда V — гиперболическая плоскость с базисом x, y, где x, y изотропны и $x.y = 1$. Если $a \in k$, то $a = Q\left(x + \frac{a}{2} y\right)$, откуда $Q(V) = k$.

1.4. *Ортогональные базисы*

Определение 5. *Базис $(e_1, \ldots, e_n)$ квадратичного модуля* (V, Q) *называется ортогональным, если он составлен из попарно ортогональных элементов, т. е. если* $V = ke_1 \widehat{\oplus} \ldots \widehat{\oplus} ke_n$.

Можно сказать также, что матрица квадратичной формы Q по отношению к этому базису является *диагональной матрицей*

$$\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n \end{pmatrix}.$$

Если $x = \sum x_i e_i$, то $Q(x) = a_1 x_1^2 + \dots + a_n x_n^2$.

Теорема 1. *Любой квадратичный модуль* (V, Q) *обладает ортогональным базисом.*

Это доказывается индукцией по $n = \dim V$, причем случай $n = 0$ тривиален. Если V изотропно, то любой его базис ортогонален. Если это не так, то выберем такой элемент $e_1 \in V$, что $e_1 . e_1 \neq 0$. Ортогонал H к e_1 есть гиперплоскость, и так как e_1 не принадлежит ей, то $V = ke_1 \widehat{\oplus} H$; по предположению индукции H обладает ортогональным базисом $(e_2, \dots, e_n)$; ясно, что $(e_1, e_2, \dots, e_n)$ отвечает требуемому условию.

Определение 6. *Будем называть два ортогональных базиса*

$$\mathbf{e} = (e_1, \dots, e_n) \quad \text{и} \quad \mathbf{e}' = (e'_1, \dots, e'_n)$$

пространства V *смежными, если они имеют общий элемент* (т. е. если существуют такие i и j, что $e_i = e'_j$).

Теорема 2. *Пусть* (V, Q) — *невырожденный квадратичный модуль размерности* $\geqslant 3$, *и пусть* $\mathbf{e} = (e_1, \dots, e_n)$, $\mathbf{e}' = (e'_1, \dots, e'_n)$ — *два ортогональных базиса в* V. *Существует такая конечная последовательность* $\mathbf{e}^{(0)}, \mathbf{e}^{(1)}, \dots, \mathbf{e}^{(m)}$ *ортогональных базисов в* V, *что* $\mathbf{e}^{(0)} = \mathbf{e}$, $\mathbf{e}^{(m)} = \mathbf{e}'$ *и что для* $0 \leqslant i < m$ *базисы* $\mathbf{e}^{(i)}$ *и* $\mathbf{e}^{(i+1)}$ — *смежные.*

(Будем говорить, что $\mathbf{e}^{(0)}, \dots, \mathbf{e}^{(m)}$ есть *цепь* смежных ортогональных базисов, связывающих $\mathbf{e}$ с $\mathbf{e}'$.)

Различаем три случая.

i) *Имеет место* $(e_1.e_1)(e_1'.e_1') - (e_1.e_1')^2 \neq 0$.

Это означает, что e_1 и e_1' не пропорциональны и что *плоскость* $\mathrm{P} = ke_1 + ke_1'$ *не вырождена*. Тогда существуют такие ε_2, $\varepsilon_2' \in \mathrm{P}$, что

$$\mathrm{P} = ke_1 \widehat{\oplus} k\varepsilon_2 \quad \text{и} \quad \mathrm{P} = ke_1' \widehat{\oplus} k\varepsilon_2'.$$

Пусть H — ортогонал к P; так как P не вырождена, то $\mathrm{V} = \mathrm{H} \widehat{\oplus} \mathrm{P}$, см. предложение 2. Пусть $(e_3'', \ldots, e_n'')$ — ортогональный базис в H. Тогда можно связать $\mathbf{e}$ с $\mathbf{e}'$ при помощи цепи

$$\mathbf{e} \to (e_1, \varepsilon_2, e_3'', \ldots, e_n'') \to (e_1', \varepsilon_2', e_3'', \ldots, e_n'') \to \mathbf{e}',$$

откуда следует теорема в рассматриваемом случае.

ii) *Имеет место* $(e_1.e_1)(e_2'.e_2') - (e_1.e_2')^2 \neq 0$.

Проверяется тем же способом с заменой e_1' на e_2'.

iii) *Имеет место* $(e_1.e_1)(e_i'.e_i') - (e_1.e_i')^2 = 0$ *для* $i = 1, 2$.

Сначала доказывается

Лемма. *Существует* $x \in k$, *такой, что* $e_x = e_1' + xe_2'$ *не изотропен и порождает с* e_1 *невырожденную плоскость.*

Имеем $e_x.e_x = e_1'.e_1' + x^2(e_2'.e_2')$; мы должны, таким образом, взять x^2 отличным от $-(e_1'.e_1')/(e_2'.e_2')$. С другой стороны, для того чтобы e_x порождал с e_1 невырожденную плоскость, необходимо и достаточно, чтобы

$$(e_1.e_1)(e_x.e_x) - (e_1.e_x)^2 \neq 0.$$

Используя при подсчете условие iii), мы найдем, что левая часть этого неравенства равна $-2x(e_1.e_1')(e_1.e_2')$. Но из условия iii) вытекает, что $e_1.e_i' \neq 0$ для $i = 1, 2$. Мы видим, таким образом, что e_x удовлетворяет условию леммы тогда и только тогда, когда имеет место одновременно и $x \neq 0$, и $x^2 \neq -(e_1'.e_1')/(e_2'.e_2')$. Этим запрещается выбор не более трех значений x; если k содержит 4 элемента, то можно, таким образом, найти нужное x. Остается случай $k = \mathbf{F}_3$ (случай

$k = \mathbf{F}_2$ исключен, поскольку caract $(k) \neq 2$). Но в этом случае все ненулевые квадраты равны 1 и по условию iii) оказывается $(e_1.e_1)(e_i'.e_i') = 1$ для $i = 1, 2$; поэтому $(e_1'.e_1')/(e_2'.e_2') = 1$ и для реализации условия $x^2 \neq 0, -1$ достаточно взять $x = 1$.

Итак, выберем $e_x = e_1' + xe_2'$, удовлетворяющий условию леммы. Так как e_x не изотропен, существует такой элемент e_2'', что (e_x, e_2'') есть ортогональный базис плоскости $ke_1' \widehat{\oplus} ke_2'$. Положим

$$\mathbf{e}'' = (e_x, e_2'', e_3', \ldots, e_n');$$

это ортогональный базис в V. Поскольку $ke_1 + ke_x$ является невырожденной плоскостью, то часть i) нашего доказательства показывает, что $\mathbf{e}$ можно связать с $\mathbf{e}''$ цепью смежных базисов; с другой стороны, $\mathbf{e}'$ и $\mathbf{e}''$ смежны; отсюда следует теорема.

1.5. *Теорема Витта*

Пусть (V, Q) и (V′, Q′) — *невырожденные* квадратичные модули; U — векторное подпространство пространства V;

$$s\colon \mathrm{U} \to \mathrm{V}'$$

— *инъективный* метрический морфизм подпространства U в V′. Отыскивается продолжение морфизма s на подпространство, большее, чем U, а если возможно, то на все пространство V. Начнем со случая, когда U вырождено.

Лемма. *Если* U *вырождено, то можно продолжить* s *до инъективного метрического морфизма* $s_1\colon \mathrm{U}_1 \to \mathrm{V}'$, *где* U_1 *содержит* U *в качестве гиперплоскости.*

Пусть x — ненулевой элемент из rad (U). Поскольку x изотропен, то по предположению 3 существует гиперболическая плоскость в V, которая его содержит; значит, можно найти такой элемент $y \in \mathrm{V}$, что $x.y = 1$ и $y.y = 0$. Так как y не ортогонален к x, то $y \notin \mathrm{U}$ и подпространство $\mathrm{U}_1 = \mathrm{U} \oplus ky$ содержит U

в качестве гиперплоскости. Тем же способом сконструируем такой элемент $y' \in V'$, что $s(x).y' = 1$ и $y'.y' = 0$. Пусть s_1: $U_1 \to V'$ — линейное отображение, которое совпадает с s на U и отображает y на y'. Непосредственно ясно, что s_1 отвечает требуемому условию.

Теорема 3 (Витт). *Если* (V, Q) *и* (V′, Q′) *изоморфны и не вырождены, то любой инъективный метрический морфизм*

$$s\colon U \to V'$$

векторного подпространства U *пространства* V *может быть продолжен до изоморфизма пространства* V *на* V′.

Поскольку V и V′ изоморфны, можно предположить, что $V = V'$. С другой стороны, применяя последнюю лемму, мы видим, что можно ограничиться случаем, когда U *не вырождено*. Теперь разумно применить индукцию по $\dim U$.

Если $\dim U = 1$, то U порождено одним неизотропным элементом x; если $y = s(x)$, то $y.y = x.x$. Можно выбрать такое $\varepsilon = \pm 1$, чтобы $x + \varepsilon y$ не было изотропным; действительно, иначе мы имели бы

$$2x.x + 2x.y = 2x.x - 2x.y = 0,$$

что влекло бы $x.x = 0$. Выберем такое ε, и пусть H — гиперплоскость, ортогональная к $z = x + \varepsilon y$; имеем $V = kz \widehat{\oplus} H$. Пусть σ — «отражение от H», т. е. автоморфизм пространства V, который тождествен на H и переводит z в $-z$. Так как $x - \varepsilon y$ принадлежит гиперплоскости H, то

$$\sigma(x - \varepsilon y) = x - \varepsilon y, \quad \sigma(x + \varepsilon y) = -x - \varepsilon y,$$

откуда $\sigma(x) = -\varepsilon y$. Автоморфизм $-\varepsilon\sigma$ продолжает s.

Если $\dim U > 1$, то разложим U в сумму $U_1 \widehat{\oplus} U_2$, где U_1, $U_2 \neq 0$. По предположению индукции, ограничение s_1 морфизма s на U_1 продолжимо до автоморфизма σ_1 пространства V; допуская замену s на

$\sigma_1^{-1} \circ s$, мы можем, таким образом, предположить, что s тождествен на U_1. Морфизм s отображает U_2 в ортогонал V_1 к U_1; следовательно, по предположению индукции ограничение морфизма s на U_2 продолжимо до автоморфизма σ_2 пространства V_1; автоморфизм σ пространства V, который тождествен на U_1 и совпадает с σ_2 на V_1, отвечает требуемому условию.

Следствие. *Два изоморфных подпространства невырожденного квадратичного модуля имеют изоморфные ортогоналы.*

Продолжим изоморфизм между подпространствами до автоморфизма модуля и ограничим его на ортогоналах.

1.6. *Переформулировки*

Пусть

$$f(X) = \sum_{i=1}^{n} a_{ii} X_i^2 + 2 \sum_{i<j} a_{ij} X_i X_j$$

— квадратичная форма от n переменных над k; положим $a_{ij} = a_{ji}$, если $i > j$, чтобы матрица $A = (a_{ij})$ была симметричной. Пара (k^n, f) есть квадратичный модуль, называемый модулем, *ассоциированным*[1]) *с формой* f (или с матрицей A).

Определение 7. *Две квадратичные формы f и f' называются эквивалентными, если соответствующие модули изоморфны.*

В этом случае будем писать $f \sim f'$. Если A и A′ — матрицы форм f и f', то можно утверждать, что существует такая обратимая матрица X, что $A' = X.A.{}^tX$, см. п. 1.1.

Пусть $f(X_1, \ldots, X_n)$ и $g(X_1, \ldots, X_m)$ — две квадратичные формы; обозначим через $f \dotplus g$ (или проще $f + g$, если невозможны недоразумения) квадратичную форму

$$f(X_1, \ldots, X_n) + g(X_{n+1}, \ldots, X_{n+m})$$

[1]) Или *соответствующим форме* f. — *Прим. перев.*

от $n+m$ переменных. Эта операция соответствует операции взятия *ортогональной суммы* (см. определение 2 п. 1.2). Аналогично, будем писать $f \dot{-} g$ (или просто $f-g$) для $f \dot{+} (-g)$.

Вот некоторые примеры переформулировок.

Определение 4′. *Форма* $f(X_1, X_2)$ *от двух переменных называется гиперболической, если*

$$f \sim X_1X_2 \sim X_1^2 - X_2^2.$$

(Это означает, что соответствующий модуль (k^2, f) является *гиперболической плоскостью*, см. определение 4 п. 1.3.)

Говорят, что форма $f(X_1, \ldots, X_n)$ представляет элемент a в k, если существует такой элемент $x \in k^n$, $x \neq 0$, что $f(x) = a$. В частности, f представляет 0 тогда и только тогда, когда соответствующий квадратичный модуль содержит ненулевой изотропный элемент.

Предложение 3′. *Если* f *представляет* 0 *и не вырождена, то* $f \sim f_2 \dot{+} g$, *где* f_2 *— гиперболическая форма. В этом случае* f *представляет любой элемент в* k.

Это является переформулировкой предложения 3 и его следствия.

Следствие 1. *Пусть* $g = g(X_1, \ldots, X_{n-1})$ *— невырожденная квадратичная форма и* $a \in k^*$. *Тогда равносильны следующие условия*:

i) g *представляет* a;

ii) *имеет место* $g \sim h \dot{+} aZ^2$, *где* h *— форма от* $n-2$ *переменных*;

iii) *форма* $f = g \dot{-} aZ^2$ *представляет* 0.

Ясно, что ii) $\Rightarrow$ i). Обратно, если g представляет a, то квадратичный модуль V, соответствующий форме g, содержит такой элемент x, что $x.x = a$; если обозначить через H ортогонал к x, то $V = H \widehat{\oplus} kx$, откуда $g \sim h \dot{+} aZ^2$, где h — квадратичная форма, связанная с базисом подпространства H.

Импликация ii) $\Rightarrow$ iii) ясна непосредственно. Наконец, если форма $f = g \dot{-} aZ^2$ имеет нетривиальный

нуль $(x_1, \ldots, x_{n-1}, z)$, то либо $z=0$ и g представляет 0, а стало быть, и a, либо $z \neq 0$ и $g(x_1/z, \ldots, x_{n-1}/z) = a$. Поэтому iii) $\Rightarrow$ i).

Следствие 2. *Пусть g и h — невырожденные формы ранга $\geqslant 1$, и пусть $f = g \dotplus h$. Тогда равносильны следующие условия:*

a) *f представляет 0;*

b) *существует $a \in k^*$, представимое обеими формами g и h;*

c) *существует такое $a \in k^*$, что $g \dotplus aZ^2$ и $h \dotplus aZ^2$ представляют 0.*

Эквивалентность b) $\Leftrightarrow$ c) вытекает из следствия 1. Импликация b) $\Rightarrow$ a) тривиальна. Покажем, что a) $\Rightarrow$ b). Нетривиальный нуль формы f можно записать в виде (x, y), где $g(x) = h(y)$. Если элемент $a = g(x) = h(y)$ отличен от 0, то ясно, что b) выполняется. Если $a = 0$, то одна из форм, например g, представляет 0, а стало быть, и любой элемент из k, в частности, любое значение, принимаемое формой h.

Теорема 1 превращается в классическое разложение квадратичной формы на «сумму квадратов»:

Теорема 1′. *Пусть f — квадратичная форма от n переменных. Тогда существуют такие $a_1, \ldots, a_n \in k$, что $f \sim a_1X_1^2 + \ldots + a_nX_n^2$.*

Рангом формы f является число таких индексов i, что $a_i \neq 0$. Он равен n в том и только в том случае, когда *дискриминант* $a_1 \ldots a_n$ формы f отличен от 0 (иными словами, когда f не вырождена).

Наконец, следствие из теоремы Витта дает следующую теорему «упрощения» [1]):

Теорема 4. *Пусть $f = g \dotplus h$ и $f' = g' \dotplus h'$ — невырожденные квадратичные формы. Тогда если $f \sim f'$ и $g \sim g'$, то и $h \sim h'$.*

Следствие. *Если f не вырождена, то*

$$f \sim g_1 \dotplus \ldots \dotplus g_m \dotplus h,$$

[1]) Иначе называемую «теоремой сокращения». — *Прим. перев.*

где $g_1, \ldots, g_m$ являются гиперболическими формами, а h не представляет 0. Это разложение единственно с точностью до эквивалентности.

Существование вытекает из предложения 3′, а единственность из теоремы 4.

[Число m гиперболических слагаемых может быть охарактеризовано как размерность *максимального изотропного подпространства* в квадратичном модуле, соответствующем форме f.]

1.7. *Квадратичные формы над* $\mathbf{F}_q$

Пусть p — простое число $\neq 2$, и пусть $q = p^f$ — степень числа p; пусть $\mathbf{F}_q$ — поле из q элементов (см. § 1 гл. I).

Предложение 4. *Квадратичная форма над* $\mathbf{F}_q$ *ранга* $\geqslant 2$ (*соответственно ранга* $\geqslant 3$) *представляет любой элемент из* $\mathbf{F}_q^*$ (*соответственно из* $\mathbf{F}_q$).

В силу следствия 1 из предложения 3 достаточно доказать, что любая квадратичная форма от 3 переменных представляет 0, а это утверждение доказано в § 2 гл. I как следствие теоремы Шевалле.

[Укажем вскользь, как можно доказать это предложение без использования теоремы Шевалле. Речь идет о доказательстве того, что если $a, b, c \in \mathbf{F}_q$ не являются нулями, то уравнение

$$ax^2 + by^2 = c \qquad (*)$$

имеет решение. Пусть A (соответственно B) есть множество элементов из $\mathbf{F}_q$, имеющих вид ax^2 (соответственно имеющих вид $c - by^2$) при $x \in \mathbf{F}_q$ (соответственно при $y \in \mathbf{F}_q$). Сразу же видно, что каждое из множеств A и B состоит из $(q+1)/2$ элементов; значит, $A \cap B \neq \varnothing$, откуда вытекает разрешимость уравнения (*).]

Напомним далее (см. п. 3.1 гл. I), что группа $\mathbf{F}_q^*/\mathbf{F}_q^{*2}$ состоит из двух элементов. Зафиксируем элемент a из $\mathbf{F}_q^*$, который не является квадратом.

Предложение 5. *Любая невырожденная квадратичная форма ранга n над $\mathbf{F}_q$ эквивалентна либо форме*

$$X_1^2 + \ldots + X_{n-1}^2 + X_n^2,$$

либо форме

$$X_1^2 + \ldots + X_{n-1}^2 + aX_n^2$$

в зависимости от того, является или не является ее дискриминант квадратом.

Это ясно, если $n = 1$. Если $n \geqslant 2$, то предложение 4 показывает, что форма f представляет 1. Поэтому она эквивалентна форме $X_1^2 + g$, где g — форма от $n-1$ переменной, и к g применимо предположение индукции.

Следствие. *Для того чтобы две невырожденные формы над $\mathbf{F}_q$ были эквивалентны, необходимо и достаточно, чтобы они имели одинаковый ранг и одинаковый дискриминант.*

(Разумеется, дискриминант рассматривается как элемент факторгруппы $\mathbf{F}_q^*/\mathbf{F}_q^{*2}$.)

§ 2. Квадратичные формы над $\mathbf{Q}_p$

В этом параграфе (кроме п. 2.4) через p обозначается простое число; через k обозначается p-адическое поле $\mathbf{Q}_p$.

Все рассматриваемые квадратичные модули являются таковыми относительно k и предполагаются невырожденными; такие же условия накладываются на квадратичные формы.

2.1. *Два инварианта*

Пусть (V, Q) — квадратичный модуль ранга n; мы обозначим через $d(Q)$ его дискриминант; это — элемент из k^*/k^{*2}, см. п. 1.1. Если $\mathbf{e} = (e_1, \ldots, e_n)$ является ортогональным базисом в V и $a_i = e_i.e_i$, то

$$d(Q) = a_1 \ldots a_n \quad (\text{в } k^*/k^{*2}).$$

(В дальнейшем мы будем часто позволять себе обозначать одной и той же буквой как элемент из k^*, так и его класс по модулю k^{*2}.)

Напомним далее, что для элементов a и b из k^* мы в п. 1.1 гл. III определили символ Гильберта (a, b), равный ± 1.

Положим

$$\varepsilon(\mathbf{e}) = \prod_{i<j} (a_i, a_j).$$

Имеем $\varepsilon(\mathbf{e}) = \pm 1$. Более того, $\varepsilon(\mathbf{e})$ является *инвариантом* квадратичного модуля (V, Q). Действительно:

Теорема 5. *Число* $\varepsilon(\mathbf{e})$ *не зависит от выбора ортогонального базиса* $\mathbf{e}$.

Если $n = 1$, то $\varepsilon(\mathbf{e}) = 1$. Если $n = 2$, то равенство $\varepsilon(\mathbf{e}) = 1$ имеет место тогда и только тогда, когда форма $Z^2 - a_1X^2 - a_2Y^2$ представляет 0, иными словами (см. следствие 1 из предложения 3′) тогда и только тогда, когда $a_1X^2 + a_2Y^2$ представляет 1; но это последнее условие означает, что существует такой элемент $x \in V$, что $Q(x) = 1$, а это не зависит от $\mathbf{e}$. Для $n \geqslant 3$ проведем индукцию по n. На основании теоремы 2 достаточно доказать, что $\varepsilon(\mathbf{e}) = \varepsilon(\mathbf{e}')$, когда $\mathbf{e}$ и $\mathbf{e}'$ *смежны*. Но из-за симметрии символа Гильберта $\varepsilon(\mathbf{e})$ не меняет значения при перестановке элементов e_i; можно, таким образом, предположить, что базис $\mathbf{e}' = (e_1', \ldots, e_n')$ таков, что $e_1' = e_1$. Если положить $a_i' = e_i' \cdot e_i'$, то $a_1' = a_1$. Можно записать $\varepsilon(\mathbf{e})$ в виде

$$\varepsilon(\mathbf{e}) = (a_1, a_2 \ldots a_n) \prod_{2 \leqslant i < j} (a_i, a_j) =$$

$$= (a_1, d(\mathrm{Q})\, a_1) \prod_{2 \leqslant i < j} (a_i, a_j),$$

поскольку $d(\mathrm{Q}) = a_1 \ldots a_n$.

Аналогично,

$$\varepsilon(\mathbf{e}') = (a_1, d(\mathrm{Q})\, a_1) \prod_{2 \leqslant i < j} (a_i', a_j').$$

Но предположение индукции, примененное к ортогоналу к e_1, показывает, что имеет место

$$\prod_{2\leqslant i<j}(a_i, a_j) = \prod_{2\leqslant i<j}(a'_i, a'_j),$$

откуда вытекает искомый результат.

Отныне мы будем писать $\varepsilon(\mathbf{Q})$ вместо $\varepsilon(\mathbf{e})$.

Переформулировка. Если f — квадратичная форма от n переменных и

$$f \sim a_1 X_1^2 + \ldots + a_n X_n^2,$$

то два элемента

$$d(f) = a_1 \ldots a_n \quad \text{в } (k^*/k^{*2})$$
$$\varepsilon(f) = \prod_{i<j}(a_i, a_j) \quad (\text{в } \{\pm 1\})$$

являются *инвариантами* класса эквивалентности формы f.

2.2. *Представление элемента из k квадратичной формой*

Лемма. a) *Число элементов векторного $\mathbf{F}_2$-пространства k^*/k^{*2} равно 2^r, где $r = 2$, если $p \neq 2$, и $r = 3$, если $p = 2$.*

b) *Пусть для $a \in k^*/k^{*2}$ и $\varepsilon = \pm 1$ через H_a^ε обозначено множество таких $x \in k^*/k^{*2}$, что $(x, a) = \varepsilon$. Тогда если $a = 1$, то H_a^1 состоит из 2^r элементов, а $\mathrm{H}_a^{-1} = \varnothing$; если $a \neq 1$, то H_a^ε состоит из 2^{r-1} элементов.*

c) *Пусть $a, a' \in k^*/k^{*2}$ и $\varepsilon, \varepsilon' = \pm 1$; предположим, что H_a^ε и $\mathrm{H}_{a'}^{\varepsilon'}$ непусты. Тогда для того чтобы $\mathrm{H}_a^\varepsilon \cap \mathrm{H}_{a'}^{\varepsilon'} = \varnothing$, необходимо и достаточно, чтобы $a = a'$ и $\varepsilon = -\varepsilon'$.*

Утверждение a) доказано в п. 3.3 гл. II. В b) случай $a = 1$ тривиален; если $a \neq 1$, то гомоморфизм $b \mapsto (a, b)$ отображает k^*/k^{*2} на $\{\pm 1\}$ (теорема 2

п. 1.2 гл. III); поэтому его ядро H_a^1 есть гиперплоскость в k^*/k^{*2} и состоит из 2^{r-1} элементов; его дополнение H_a^{-1} состоит из 2^{r-1} элементов (это — «аффинная» гиперплоскость, параллельная H_a^1). Наконец, если H_a^ε и $H_{a'}^{\varepsilon'}$ непусты и дизъюнктны, то они обязаны состоять из 2^{r-1} элементов каждое и быть дополнениями друг к другу; поэтому $H_a^1 = H_{a'}^1$, что дает

$$(x, a) = (x, a') \quad \text{для любого} \quad x \in k^*/k^{*2};$$

поскольку символ Гильберта не вырожден, отсюда выводим, что $a = a'$ и, очевидно, $\varepsilon = -\varepsilon'$; обратное утверждение тривиально.

Пусть теперь f — квадратичная форма ранга n; пусть $d = d(f)$ и $\varepsilon = \varepsilon(f)$ — ее инварианты.

Теорема 6. *Для представимости нуля формой f необходимо и достаточно, чтобы выполнялось одно из следующих условий*:

i) $n = 2$ *и* $d = -1$ (*в* k^*/k^{*2});
ii) $n = 3$ *и* $(-1, -d) = \varepsilon$;
iii) $n = 4$ *и либо* $d \neq 1$, *либо* $d = 1$ *и* $\varepsilon = (-1, -1)$;
iv) $n \geqslant 5$.

(В частности, *любая форма от* 5 *и более переменным представляет* 0.)

Прежде чем доказывать эту теорему, укажем одно ее следствие.

Пусть $a \in k^*/k^{*2}$, и пусть $f_a = f \perp aZ^2$ (эта форма определена с точностью до эквивалентности). Известно (см. п. 1.6), что f_a представляет 0 тогда и только тогда, когда f представляет a. Имеем

$$d(f_a) = -ad, \quad \varepsilon(f_a) = (-a, d)\varepsilon,$$

как мы только что вывели. Применяя теорему 6 к f_a и используя эти формулы, получаем

Следствие. *Пусть* $a \in k^*/k^{*2}$. *Тогда для представимости* a *формой* f *необходимо и достаточно, чтобы выполнялось одно из следующих условий:*

i) $n=1$ *и* $a=d$;

ii) $n=2$ и $(a, -d)=\varepsilon$;

iii) $n=3$ *и либо* $a \neq -d$, *либо* $a=-d$ *и* $(-1, -d)=\varepsilon$;

iv) $n \geqslant 4$.

(Уточним, что здесь так же, как в формулировке теоремы 6 и далее, a и $-d$ рассматриваются как элементы из k^*/k^{*2}; например, неравенство $a \neq -d$ означает, что a не равно произведению элемента $-d$ на квадрат.)

Доказательство теоремы 6. Запишем f в виде $f \sim a_1X_1^2 + \ldots + a_nX_n^2$ и рассмотрим отдельно случаи $n=2$, 3, 4 и $\geqslant 5$.

i) *Случай* $n=2$.

Форма f представляет 0 тогда и только тогда, когда $-a_1/a_2$ есть квадрат; но $-a_1/a_2 = -a_1a_2 = -d$ в k^*/k^{*2}; поэтому $-d=1$, т. е. $d=-1$.

ii) *Случай* $n=3$.

Форма f представляет 0 тогда и только тогда, когда форма

$$-a_3f \sim -a_3a_1X_1^2 - a_3a_2X_2^2 - X_3^2$$

представляет 0. По определению символа Гильберта последняя форма представляет 0 в том и только в том случае, когда

$$(-a_3a_1, -a_3a_2)=1.$$

Преобразуя, находим

$$(-1, -1)(-1, a_1)(-1, a_2)(a_3, a_3)(a_1, a_2)(a_1, a_3)(a_2, a_3)=1.$$

Но $(a_3, a_3)=(-1, a_3)$ (см. формулу iv) предложения 2 п. 1.1 гл. III). Поэтому наше условие можно записать в виде

$$(-1, -1)(-1, a_1a_2a_3)(a_1, a_2)(a_1, a_3)(a_2, a_3)=1$$

или $(-1, -d)\varepsilon=1$, т. е. $(-1, -d)=\varepsilon$.

iii) *Случай* $n=4$.

На основании следствия 2 предложения 3′ форма f представляет 0 тогда и только тогда, когда существует $x \in k^*/k^{*2}$, представимый двумя формами

$$a_1X_1^2+a_2X_2^2 \quad \text{и} \quad -a_3X_3^2-a_4X_4^2.$$

В силу ii) приведенного выше следствия [1]) такой элемент x характеризуется условиями

$$(x, -a_1a_2)=(a_1, a_2) \quad \text{и} \quad (x, -a_3a_4)=(-a_3, -a_4).$$

Пусть A — подмножество в k^*/k^{*2}, определенное первым условием, а B — такое же подмножество, определенное вторым условием. Для того чтобы f не представляла нуль, необходимо и достаточно, чтобы $A \cap B=\varnothing$. Очевидно, что A и B не пусты (например, $a_1 \in A$ и $-a_3 \in B$). По части c) леммы, приведенной в начале этого пункта, условие $A \cap B=\varnothing$ эквивалентно следующему:

$$a_1a_2=a_3a_4, \qquad (a_1, a_2)=-(-a_3, -a_4).$$

Первое равенство означает, что $d=1$. Если оно реализовано, то

$$\varepsilon=(a_1, a_2)(a_3, a_4)\ (a_3a_4, a_3a_4);$$

отсюда, используя соотношение $(x, x)=(-1, x)$ (см. формулу iv) предложения 2 п. 1.1 гл. III), получаем

$$\varepsilon=(a_1, a_2)(a_3, a_4)(-1, a_3a_4)=$$
$$=(a_1, a_2)(-a_3, -a_4)(-1, -1).$$

Поэтому второе равенство запишется в виде

$$\varepsilon=-(-1, -1),$$

откуда следует искомый результат.

iv) *Случай* $n \geqslant 5$.

Достаточно рассмотреть случай $n=5$. Используя лемму и часть ii) приведенного выше следствия, видим, что форма ранга 2 представляет не менее 2^{r-1}

[1]) Случай ii) следствия вытекает из уже доказанного случая $n=2$ теоремы 6.— *Прим. ред.*

элементов из k^*/k^{*2}, и тем более это же имеет место для форм ранга $\geqslant 2$. Так как $2^{r-1} \geqslant 2$, то форма f представляет некоторый элемент $a \in k^*/k^{*2}$, *отличный от* d. Имеем

$$f \sim aX^2 + g,$$

где g — форма ранга 4. Дискриминант формы g равен d/a; стало быть, он отличен от 1, и на основании iii) форма g представляет 0. Поэтому то же верно и для f, что завершает доказательство теоремы 6.

Замечания. 1) Пусть f — квадратичная форма, не представляющая 0. Приведенные выше результаты показывают, что число элементов из k^*/k^{*2}, которые представляются посредством f, равно 1, если $n=1$; равно 2^{r-1}, если $n=2$; равно 2^r-1, если $n=3$; равно 2^r, если $n=4$.

2) Мы видели, что каждая квадратичная форма от 5 переменных над $\mathbf{Q}_p$ представляет 0. В связи с этим укажем на гипотезу Артина: *всякий однородный полином степени* d *над* $\mathbf{Q}_p$ *от* d^2+1 *или более переменных имеет нетривиальный нуль.*

В случае $d=3$ эта гипотеза подтверждается (см., например, Springer T., *Koninkl. Nederl. Akad. van Wetenss.*, (1955), 512—516). Общий случай оставался открытым в течение тридцати лет. Только в 1966 году Тержаньян [1]) показал, что *предположение Артина неверно*: существует однородный полином четвертой степени над $\mathbf{Q}_2$ от 18 переменных, который не имеет ни одного нетривиального нуля. Тержаньян исходил из полинома

$$n(X, Y, Z) = X^2YZ + Y^2ZX + Z^2XY + X^2Y^2 + Y^2Z^2 + Z^2X^2 - X^4 - Y^4 - Z^4,$$

который обладает следующим свойством: если (x, y, z) — примитивная точка в $(\mathbf{Z}_2)^3$, то $n(x, y, z) \equiv -1 \pmod 4$. Пусть

$$f(X_1, \ldots, X_9) = n(X_1, X_2, X_3) + n(X_4, X_5, X_6) + n(X_7, X_8, X_9);$$

[1]) Terjanian G., *Comptes Rendus Acad. Sci. Paris*, **262** (1966), № 11, A612. — *Прим. ред.*

тогда $f(x_1, \ldots, x_9) \not\equiv 0 \pmod 4$, если точка $(x_1, \ldots, x_9)$ примитивна. Отсюда легко выводится, что полином

$$F(X_1, \ldots, X_{18}) = f(X_1, \ldots, X_9) + 4f(X_{10}, \ldots, X_{18})$$

не имеет нетривиального нуля. (Существуют аналогичные примеры — но более высоких степеней — для всех полей $\mathbf{Q}_p$.)

Известно все же, что предположение Артина «почти» верно: при фиксированной степени d оно справедливо для всех простых чисел p, кроме конечного числа (Ax J., Kochen S., *Amer. J. Math.*, 87 (1965), 605—648 [1])); однако уже для $d = 4$ неизвестно, как определить множество этих исключительных простых чисел.

2.3. *Классификация*

Теорема 7. *Две квадратичные формы над k эквивалентны тогда и только тогда, когда они имеют одинаковый ранг, одинаковый дискриминант и одинаковый инвариант ε.*

То, что у эквивалентных форм указанные инварианты одинаковы, вытекает из их определения. Обратное доказывается индукцией по рангу n рассматриваемых квадратичных форм f и g (случай $n = 0$ тривиален). Следствие теоремы 6 показывает, что f и g представляют одинаковые элементы из k^*/k^{*2}; поэтому можно найти $a \in k^*$, которое одновременно представимо как формой f, так и формой g; это позволяет записать

$$f \sim aZ^2 + f' \quad \text{и} \quad g \sim aZ^2 + g',$$

где f' и g' являются формами ранга $n - 1$. Имеем

$$d(f') = a\,d(f) = a\,d(g) = d(g'),$$
$$\varepsilon(f') = \varepsilon(f)(a,\ d(f')) = \varepsilon(g)(a,\ d(g')) = \varepsilon(g');$$

это показывает, что f' и g' имеют одинаковые инварианты. По предположению индукции $f' \sim g'$, откуда $f \sim g$.

[1]) См. также сб. *Математика*, 9 : 5 (1965), 3—26. — *Прим. ред.*

Следствие. *Существует единственная с точностью до эквивалентности форма ранга 4, которая не представляет* 0; *если* $(a, b) = -1$, *то такой формой является* $z^2 - ax^2 - by^2 + abt^2$.

Действительно, по теореме 6 такая форма характеризуется инвариантами $d(f) = 1$, $\varepsilon(f) = -(-1, -1)$, и непосредственный подсчет убеждает нас в том, что $z^2 - ax^2 - by^2 + abt^2$ обладает этими свойствами.

Замечание. Эту форму можно трактовать как *редуцированную норму* единственного некоммутативного тела степени 4 над $\mathbf{Q}_p$; если $(a, b) = -1$, то это тело может быть определено как тело «кватернионов» с базисом $\{1, i, j, ij\}$, где $i^2 = a$, $j^2 = b$, $ij = -ji$.

Предложение 6. *Пусть даны* $n \geqslant 1$, $d \in k^*/k^{*2}$ *и* $\varepsilon = \pm 1$. *Тогда для существования квадратичной формы* f *ранга* n *с инвариантами* $d(f) = d$ *и* $\varepsilon(f) = \varepsilon$ *необходимо и достаточно, чтобы имело место одно из следующих условий*:

$n = 1$, $\varepsilon = 1$; *или* $n = 2$, $d \neq -1$;
или $n = 2$, $\varepsilon = 1$; *или* $n \geqslant 3$.

Случай $n = 1$ тривиален. Если $n = 2$, то $f \sim aX^2 + bY^2$, и, если $d(f) = -1$, то $\varepsilon(f) = (a, b) = (a, -ab) = 1$; поэтому не может быть одновременно $d(f) = -1$ и $\varepsilon(f) = -1$. Обратно, если $d = -1$, $\varepsilon = 1$, то возьмем $f = X^2 - Y^2$; если $d \neq -1$, то существует такой элемент $a \in k^*$, что $(a, -d) = \varepsilon$, и мы возьмем $f = aX^2 + adY^2$. Если $n = 3$, то выберем $a \in k^*/k^{*2}$ отличным от $-d$; по только что доказанному существует такая форма g ранга 2, что $d(g) = ad$, $\varepsilon(g) = \varepsilon(a, -d)$; форма $aZ^2 + g$ — искомая. Случай $n \geqslant 4$ сводится к случаю $n = 3$, если в качестве f взять форму $g(X_1, X_2, X_3) + X_4^2 + \ldots + X_n^2$, где g — форма с заданными инвариантами.

Следствие. *Число классов квадратичных форм ранга* n *над* $\mathbf{Q}_p$, $p \neq 2$ (*соответственно* $p = 2$) *равно* 4 (*соответственно* 8), *если* $n = 1$; *равно* 7 (*соответственно* 15), *если* $n = 2$, *и равно* 8 (*соответственно* 16), *если* $n \geqslant 3$.

Действительно, $d(f)$ может принять 4 (соответственно 8) значений, а $\varepsilon(f)$ может принять два значения.

2.4. *Вещественный случай*

Пусть f — квадратичная форма ранга n над полем $\mathbf{R}$ вещественных чисел. Известно, что f эквивалентна форме

$$X_1^2 + \ldots + X_r^2 - Y_1^2 - \ldots - Y_s^2,$$

где r и s — два таких целых неотрицательных числа, что $r+s=n$; пара (r, s) зависит только от f; эта пара называется *сигнатурой* формы f. Говорят, что f — *определенная* форма, если r или $s=0$, иными словами, если f имеет постоянный знак; в противном случае говорят, что f — *неопределенная* форма (это тот случай, когда f представляет 0).

Инвариант $\varepsilon(f)$ определяется так же, как в случае поля $\mathbf{Q}_p$; так как $(-1, -1)=-1$, то

$$\varepsilon(f)=(-1)^{s(s-1)/2}=\begin{cases} 1, & \text{если } s\equiv 0,\ 1 \pmod 4,\\ -1, & \text{если } s\equiv 2,\ 3 \pmod 4.\end{cases}$$

С другой стороны,

$$d(f)=(-1)^s=\begin{cases} 1, & \text{если } s\equiv 0 \pmod 2,\\ -1, & \text{если } s\equiv 1 \pmod 2.\end{cases}$$

Таким образом, мы видим, что задание инвариантов $d(f)$ и $\varepsilon(f)$ равносильно заданию s по модулю 4; в частности, *$d(f)$ и $\varepsilon(f)$ определяют форму f с точностью до эквивалентности при $n\leqslant 3$.*

Таким же образом проверяется, что *части* i), ii), iii) *теоремы* 6 *и ее следствия переносятся на* $\mathbf{R}$ (доказательство их использует только невырожденность символа Гильберта); очевидно, что то же самое можно сказать и о части iv).

§ 3. Квадратичные формы над Q

Мы предполагаем, что все рассматриваемые квадратичные формы имеют коэффициенты в $\mathbf{Q}$ и невырождены.

3.1. *Инварианты формы*

Так же, как и в § 2 гл. III, обозначим через V объединение множества простых чисел и символа ∞ и будем считать, что $\mathbf{Q}_\infty = \mathbf{R}$.

Пусть $f \sim a_1X_1^2 + \ldots + a_nX_n^2$—квадратичная форма ранга n. Свяжем с ней следующие инварианты:

a) *Дискриминант* $d(f) \in \mathbf{Q}^*/\mathbf{Q}^{*2}$, равный произведению $a_1 \ldots a_n$.

b) Пусть $v \in \mathrm{V}$. Инъекция $\mathbf{Q} \to \mathbf{Q}_v$ позволяет рассматривать f как *квадратичную форму* (которую мы обозначим f_v) *над* $\mathbf{Q}_v$. Инварианты формы f_v будем обозначать через $d_v(f)$ и $\varepsilon_v(f)$; ясно, что $d_v(f)$ есть образ дискриминанта $d(f)$ при отображении $\mathbf{Q}^*/\mathbf{Q}^{*2} \to \mathbf{Q}_v^*/\mathbf{Q}_v^{*2}$; имеем

$$\varepsilon_v(f) = \prod_{i<j} (a_i, a_j)_v.$$

Формула произведения (теорема 3 п. 2.1 гл. III) устанавливает соотношение

$$\prod_{v \in \mathrm{V}} \varepsilon_v(f) = 1.$$

c) *Сигнатура* (r, s) вещественной квадратичной формы f_∞ является еще одним инвариантом формы f.

Инварианты $d_v(f)$, $\varepsilon_v(f)$ и (r, s) иногда называются *локальными* инвариантами формы f.

3.2. *Представление числа формой*

Теорема 8 (Хассе — Минковский). *Форма f представляет 0 в $\mathbf{Q}$ тогда и только тогда, когда для любого $v \in \mathrm{V}$ форма f_v представляет 0 (в $\mathbf{Q}_v$).*

(Иными словами, f имеет «глобальный» нуль в том и только в том случае, когда f имеет повсюду «локальный» нуль.)

Необходимость условий теоремы тривиальна. Для доказательства достаточности запишем f в виде

$$f = a_1X_1^2 + \ldots + a_nX_n^2, \quad a_i \in \mathbf{Q}^*.$$

Используя возможность замены f на $a_1 f$, мы можем предположить, что $a_1 = 1$.

Рассмотрим отдельно случаи $n = 2$, 3, 4 и $\geqslant 5$.

i) *Случай* $n = 2$.

Имеем $f = X_1^2 - aX_2^2$; так как f_∞ представляет 0, то $a > 0$. Пусть a записано в виде

$$a = \prod_p p^{v_p(a)};$$

так как f_v представляет 0, то a является квадратом в $\mathbf{Q}_p$, а потому $v_p(a)$ должно быть *четным*. Отсюда вытекает, что a есть квадрат в $\mathbf{Q}$ и f представляет 0.

ii) *Случай* $n = 3$ (Лежандр).

Имеем $f = X_1^2 - aX_2^2 - bX_3^2$; используя возможность умножать a и b на квадраты, мы можем предположить, что a и b являются *целыми числами, не делящимися на квадраты* (т. е. $v_p(a)$, $v_p(b)$ равны 0 или 1 для любого простого числа p). Можно также предположить, что $|a| \leqslant |b|$. Проведем теперь индукцию по целому числу $m = |a| + |b|$. Если $m = 2$, то

$$f = X_1^2 \pm X_2^2 \pm X_3^2;$$

случай формы $X_1^2 + X_2^2 + X_3^2$ исключается, поскольку f_∞ представляет 0; в остальных случаях f действительно представляет 0.

Предположим, что $m > 2$, так что $|b| \geqslant 2$, и запишем b в виде

$$b = \pm p_1 \dots p_k,$$

где p_i суть различные простые числа. Пусть p — одно из чисел p_i; покажем, что *a является квадратом по модулю p*. Это очевидно, если $a \equiv 0 \pmod p$. Если же это не так, то a является p-адической единицей; по условию существует $(x, y, z) \in (\mathbf{Q}_p)^3$, такой, что

$$z^2 - ax^2 - by^2 = 0,$$

и можно предположить, что (x, y, z) примитивен (см. предложение 6 п. 2.1 гл. II). Имеем: $z^2 - ax^2 \equiv 0 \pmod p$. Отсюда заключаем, что если $x \equiv 0 \pmod p$, то это же имеет место для z и by^2 должно делиться

на p^2; но так как $v_p(b)=1$, то это приводит к сравнению $y\equiv 0 \pmod p$ вопреки примитивности (x, y, z). Таким образом, $x \not\equiv 0 \pmod p$, а это и означает, что a является квадратом (mod p). Установив это, мы видим, что *a является квадратом по модулю b*, поскольку $\mathbf{Z}/b\mathbf{Z}=\prod \mathbf{Z}/p_i\mathbf{Z}$. Следовательно, существуют такие целые числа t, b', что

$$t^2 = a + bb',$$

причем t может быть выбрано так, чтобы $|t| \leqslant |b|/2$. Формула $bb' = t^2 - a$ показывает, что bb' есть *норма* в расширении $k(\sqrt{a})/k$, где $k=\mathbf{Q}$ или $\mathbf{Q}_v$; отсюда заключаем (рассуждение, аналогичное выводу предложения 1 гл. III), что f представляет 0 в k тогда и только тогда, когда это имеет место для $f' = \mathrm{X}_1^2 - a\mathrm{X}_2^2 - b'\mathrm{X}_3^2$. В частности, f' представляет 0 в каждом из $\mathbf{Q}_v$. Но $|b'| = \left|\frac{t^2-a}{b}\right| \leqslant \frac{|b|}{4} + 1 < |b|$, поскольку $|b| \geqslant 2$. Запишем b' в виде $b''u^2$, где b'', u — целые числа, причем b'' не делится на квадраты; тогда тем более $|b''| < |b|$. Применим теперь предположение индукции к форме

$$f'' = \mathrm{X}_1^2 - a\mathrm{X}_2^2 - b''\mathrm{X}_3^2,$$

которая эквивалентна форме f'. Мы получаем, что f'' представляет 0 в $\mathbf{Q}$, а отсюда вытекает то же самое и для f.

iii) *Случай* $n=4$.

Имеем

$$f = a\mathrm{X}_1^2 + b\mathrm{X}_2^2 - (c\mathrm{X}_3^2 + d\mathrm{X}_4^2).$$

Пусть $v \in \mathrm{V}$. Так как f_v представляет 0, то следствие 2 предложения 3′ из п. 1.6 показывает, что существует элемент $x_v \in \mathbf{Q}_v^*$, представимый одновременно формами $a\mathrm{X}_1^2 + b\mathrm{X}_2^2$ и $c\mathrm{X}_3^2 + d\mathrm{X}_4^2$; на основании части ii) следствия из теоремы 6 (которое равным образом применимо и к $\mathbf{Q}_\infty = \mathbf{R}$) это позволяет утверждать, что

$$(x_v, -ab)_v = (a, b)_v, \quad (x_v, -cd)_v = (c, d)_v.$$

Так как $\prod_{v\in V}(a, b)_v = \prod_{v\in V}(c, d)_v = 1$, то можно применить теорему 4 п. 2.2 гл. III; мы получаем, что существует такой элемент $x \in \mathbf{Q}^*$, что

$(x, -ab)_v = (a, b)_v$ и

$$(x, -cd)_v = (c, d)_v \quad \text{для каждого} \quad v \in V.$$

Поэтому форма $aX_1^2 + bX_2^2 - xZ^2$ представляет 0 в каждом из $\mathbf{Q}_v$, и следовательно, в $\mathbf{Q}$, на основании ii). Отсюда заключаем, что x представим в $\mathbf{Q}$ формой $aX_1^2 + bX_2^2$, и то же рассуждение применимо к $cX_3^2 + dX_4^2$; из этого следует, что f представляет 0.

iv) *Случай* $n \geqslant 5$.

Применим индукцию по n. Запишем f в виде

$$f = h - g,$$

где $h = a_1X_1^2 + a_2X_2^2$, $g = -(a_3X_3^2 + \ldots + a_nX_n^2)$.

Пусть S обозначает часть множества V, состоящую из ∞, 2 и тех простых чисел p, для которых $v_p(a_i) \neq 0$ при $i \geqslant 3$; это множество конечно. Пусть $v \in S$. Так как f_v представляет 0, то существует элемент $a_v \in \mathbf{Q}_v^*$, который представим в $\mathbf{Q}_v$ формами h и g; тогда существуют такие элементы $x_i^v \in \mathbf{Q}_v$, $i = 1, \ldots, n$, что

$$h(x_1^v, x_2^v) = a_v = g(x_3^v, \ldots, x_n^v).$$

Но квадраты из $\mathbf{Q}_v^*$ образуют *открытое* множество (см. п. 3.3 гл. II). Отсюда при помощи теоремы об аппроксимации (лемма 2 п. 2.2 гл. III) следует, что существуют такие элементы $x_1, x_2 \in \mathbf{Q}$, что если $a = h(x_1, x_2)$, то имеет место $a/a_v \in \mathbf{Q}_v^{*2}$ для каждого $v \in S$. Рассмотрим форму

$$f_1 = aZ^2 - g.$$

Если $v \in S$, то форма g представляет a_v в $\mathbf{Q}_v$; поэтому g представляет также и a в $\mathbf{Q}_v$, ибо $a/a_v \in \mathbf{Q}_v^{*2}$; отсюда заключаем, что f_1 представляет 0 в $\mathbf{Q}_v$. Если $v \notin S$, то коэффициенты $-a_3, \ldots, -a_n$ формы g являются v-адическими единицами; следовательно,

v-адической единицей будет и $d_v(g)$, и так как $v \neq 2$, то $\varepsilon_v(g) = 1$. Так как ранг формы $g \geqslant 3$, то теорема 6 показывает, что g представляет 0 [это может быть также получено из следствия 2 теоремы 1 п. 2.2 гл. II в сочетании с теоремой Шевалле]. Во всех случаях мы видим, что f_1 представляет 0 в $\mathbf{Q}_v$; так как ранг формы f_1 равен $n-1$, предположение индукции показывает, что f_1 представляет 0 в $\mathbf{Q}$, т. е. что g представляет a в $\mathbf{Q}$; так как h представляет a, то отсюда следует, что f представляет 0, что и завершает доказательство.

Следствие 1. *Пусть $a \in \mathbf{Q}^*$. Для представимости элемента a формой f в $\mathbf{Q}$ необходима и достаточна его представимость в каждом из $\mathbf{Q}_v$.*

Это вытекает из теоремы, примененной к форме $aZ^2 - f$.

Следствие 2 (Мейер). *Квадратичная форма ранга $\geqslant 5$ представляет 0 в том и только в том случае, когда она является неопределенной* (т. е. когда она представляет 0 в $\mathbf{R}$).

Действительно, по теореме 6 такая форма представляет 0 в каждом из $\mathbf{Q}_v$.

Следствие 3. *Пусть n — ранг формы f. Предположим, что $n = 3$ (соответственно $n = 4$ и $d(f) = 1$). Тогда, если f представляет 0 во всех $\mathbf{Q}_v$, кроме разве лишь одного, то f представляет* 0.

Предположим, что $n = 3$. По теореме 6 форма f представляет 0 в том и только в том случае, когда

$$(-1, -d(f))_v = \varepsilon_v(f). \qquad (*)_v$$

Но оба семейства $\varepsilon_v(f)$, $(-1, -d(f))_v$ удовлетворяют *формуле произведения* из п. 2.1 гл. III. Отсюда заключаем, что если равенство $(*)_v$ имеет место для всех v, кроме разве лишь одного, то это равенство справедливо для всех v; на основании теоремы 8 форма f представляет 0.

Когда $n = 4$ и $d(f) = 1$, рассуждения проводятся тем же способом с заменой равенства $(*)_v$ равенством

$$(-1, -1)_v = \varepsilon_v(f).$$

Замечания. 1) Предположим, что $n=2$ и что f представляет 0 во всех $\mathbf{Q}_v$, *кроме конечного числа*. Тогда с помощью теоремы об арифметической прогрессии (см. п. 4.4 гл. VI) можно доказать, что f представляет 0.

2) Теорема 8 не распространяется на однородные полиномы степени $\geqslant 3$; например, Селмер [1]) показал, что уравнение

$$3X^3+4Y^3+5Z^3=0$$

имеет нетривиальные решения в каждом из $\mathbf{Q}_v$, но не имеет такого решения в $\mathbf{Q}$.

3.3. *Классификация*

Теорема 9. *Пусть f и f' — квадратичные формы над $\mathbf{Q}$. Для эквивалентности форм f и f' над $\mathbf{Q}$ необходимо и достаточно, чтобы они были эквивалентны над каждым из $\mathbf{Q}_v$.*

Необходимость тривиальна. Для доказательства достаточности проведем индукцию по рангу n форм f и f'. Если $n=0$, то доказывать нечего. Если это не так, то существует элемент $a\in\mathbf{Q}^*$, представимый формой f, а следовательно, представимый и формой f' (см. следствие 1 теоремы 8). Тогда $f\sim aZ^2+g$, $f'\sim aZ^2+g'$. По теореме 4 из п. 1.6 $g\sim g'$ над $\mathbf{Q}_v$ для любого $v\in V$. Предположение индукции показывает, что $g\sim g'$ над $\mathbf{Q}$, откуда $f\sim f'$.

Следствие. *Пусть (r, s) и (r', s') — сигнатуры форм f и f'. Для эквивалентности форм f и f' необходимо и достаточно, чтобы выполнялись следующие условия:*

$$d(f)=d(f'),\quad (r, s)=(r', s')\quad и\quad \varepsilon_v(f)=\varepsilon_v(f')$$

для любого $v\in V$.

Действительно, эти условия как раз и означают, что f и f' эквивалентны над каждым из $\mathbf{Q}_v$.

[1]) Selmer E. S., *Acta mathem.*, **85** (1951), № 3—4, 203—362. — *Прим. ред.*

Замечание. Инварианты $d = d(f)$, $\varepsilon_v = \varepsilon_v(f)$ и (r, s) не произвольны. Они удовлетворяют следующим условиям:

(1) $\varepsilon_v = 1$ почти для всех $v \in V$, $\prod_{v \in V} \varepsilon_v = 1$;

(2) $\varepsilon_v = 1$, если $n = 1$, или если $n = 2$, а образ d_v дискриминанта d в $\mathbf{Q}_v^*/\mathbf{Q}_v^{*2}$ равен -1;

(3) $r, s \geqslant 0$ и $r + s = n$;

(4) $d_\infty = (-1)^s$;

(5) $\varepsilon_\infty = (-1)^{s(s-1)/2}$.

Обратно:

Предложение 7. *Пусть d, $(\varepsilon_v)_{v \in V}$ и (r, s) удовлетворяют приведенным выше условиям* (1) — (5). *Тогда существует квадратичная форма ранга n над $\mathbf{Q}$, имеющая инвариантами d, $(\varepsilon_v)_{v \in V}$ и (r, s).*

Случай $n = 1$ тривиален.

Предположим, что $n = 2$. Пусть $v \in V$. Невырожденность символа Гильберта в сочетании с условием (2) показывает, что существует такой элемент $x_v \in \mathbf{Q}_v^*$, что $(x_v, -d)_v = \varepsilon_v$. Отсюда и из условия (1) выводится существование такого $x \in \mathbf{Q}^*$, что $(x, -d)_v = \varepsilon_v$ для каждого $v \in V$ (см. теорему 4 п. 2.2 гл. III). Форма $xX^2 + x\,dY^2$ — искомая.

Предположим, что $n = 3$. Пусть S — множество таких $v \in V$, что $(-d, -1)_v = -\varepsilon_v$; это множество конечно. Если $v \in S$, то выберем в $\mathbf{Q}_v^*/\mathbf{Q}_v^{*2}$ элемент c_v, отличный от образа $-d_v$ элемента $-d$ в этой группе. Используя теорему об аппроксимации (см. лемму 2 п. 2.2 гл. III), можно доказать, что существует $c \in \mathbf{Q}^*$, образ которого в каждой $\mathbf{Q}_v^*/\mathbf{Q}_v^{*2}$, $v \in S$, равен c_v. На основании только что доказанного существует такая форма g ранга 2, что $d(g) = cd$, $\varepsilon_v(g) = (c, -d)_v \varepsilon_v$ для каждого $v \in V$. Тогда можно утверждать, что форма $f = cZ^2 + g$ — искомая. [Заметим, что для $n \leqslant 3$ не использовалась сигнатура формы, так как условия (3), (4), (5) определяют ее как функцию от d_∞ и ε_∞.]

Для $n \geqslant 4$ применим индукцию по n. Предположим сначала, что $r \geqslant 1$. Тогда на основании предположе-

ния индукции мы видим, что существует форма g ранга $n-1$, которая имеет инвариантами d, $(\varepsilon_v)_{v\in V}$ и $(r-1, s)$; форма $X^2 \dotplus g$ отвечает требуемому условию. Если $r=0$, то построим форму h ранга $n-1$, имеющую инвариантами $-d$, $\varepsilon_v(-1, -d)_v$ и $(0, n-1)$; форма $-X^2 \dotplus h$ — искомая.

Приложение

Суммы трех квадратов

Пусть n и p — положительные целые числа. Говорят, что n *есть сумма* p *квадратов*, если число n представимо *над кольцом* $\mathbf{Z}$ квадратичной формой $X_1^2 + \ldots + X_p^2$, т. е. существуют такие целые числа $n_1, \ldots, n_p$, что

$$n = n_1^2 + \ldots + n_p^2.$$

Теорема (Гаусс). *Для того чтобы целое положительное число* n *было суммой трех квадратов, необходимо и достаточно, чтобы оно не было числом вида* $4^a(8b-1)$, *где* $a, b \in \mathbf{Z}$.

(Например: если n не делится на 4, то оно является суммой трех квадратов в том и только в том случае, когда $n = 1, 2, 3, 5, 6 \pmod 8$.)

Доказательство. Можно предполагать, что n отлично от нуля. Тогда условие «n имеет вид $4^a(8b-1)$» равносильно тому, что $-n$ *является квадратом в* $\mathbf{Q}_2^*$ (см. теорему 4 п. 3.3 гл. II). Имеет место следующее утверждение:

Лемма А. *Пусть* $a \in \mathbf{Q}^*$. *Для того чтобы* a *было представимо в* $\mathbf{Q}$ *формой* $f = X_1^2 + X_2^2 + X_3^2$, *необходимо и достаточно, чтобы* a *было* > 0 *и чтобы* $-a$ *не было квадратом в* $\mathbf{Q}_2$.

На основании следствия 1 из теоремы 8 нам надо выразить условия того, что a представимо формой f в $\mathbf{R}$ и в каждом $\mathbf{Q}_p$. Случай поля $\mathbf{R}$ дает условие положительности. С другой стороны, локальные инва-

рианты $d_p(f)$ и $\varepsilon_p(f)$ равны 1. Если $p \neq 2$, то

$$(-1, -d_p(f))_p = (-1, -1)_p = 1 = \varepsilon_p(f);$$

поэтому следствие из теоремы 6 показывает, что a представимо формой f в $\mathbf{Q}_p$. Если $p = 2$, то

$$(-1, -d_2(f))_2 = -1 \neq \varepsilon_2(f);$$

то же следствие показывает, что a представимо формой f в $\mathbf{Q}_2$ в том и только в том случае, когда a отлично от -1 в $\mathbf{Q}_2^*/\mathbf{Q}_2^{*2}$, т. е. когда $-a$ не является квадратом в $\mathbf{Q}_2$.

Теперь надо перейти от представления *в* $\mathbf{Q}$ к представлению *в* $\mathbf{Z}$. Это делается посредством следующей леммы.

Лемма B (Дэвенпорт — Касселс). *Пусть*

$$f(X) = \sum_{i,\,j=1}^{p} a_{ij} X_i X_j$$

— положительно определенная квадратичная форма, причем (a_{ij}) *— симметрическая матрица с целыми коэффициентами. Сделаем следующее предположение:*

(H). *Для любого элемента* $x = (x_1, \ldots, x_p) \in \mathbf{Q}^p$ *существует такой элемент* $y \in \mathbf{Z}^p$, *что* $f(x - y) < 1$.

Тогда, если число $n \in \mathbf{Z}$ *представимо формой* f *в* $\mathbf{Q}$, *то* n *также представимо формой* f *в* $\mathbf{Z}$.

Если $x = (x_1, \ldots, x_p)$ и $y = (y_1, \ldots, y_p)$ — элементы из $\mathbf{Q}^p$, то мы обозначим через $x.y$ их скалярное произведение $\sum a_{ij} x_i y_j$. Имеем $x.x = f(x)$.

Пусть n — целое число, представимое формой f в $\mathbf{Q}$. Существует такое целое число $t > 0$, что $t^2 n = x.x$, где $x \in \mathbf{Z}^p$. Выберем t и x таким образом, чтобы t было наименьшим; нам надо доказать, что тогда $t = 1$.

По предположению (H) существует такой $y \in \mathbf{Z}^p$, что

$$\frac{x}{t} = y + z, \quad \text{где} \quad z.z < 1.$$

Если $z.z=0$, то $z=0$, и $\frac{x}{t}$ имеет целые компоненты. Из минимальности числа t вытекает, что $t=1$.

Предположим, что $z.z\neq 0$; положим

$$a=y.y-n,$$
$$b=2(nt-x.y),$$
$$t'=at+b,$$
$$x'=ax+by.$$

Имеем $a,\ b,\ t'\in\mathbf{Z}$. Далее,

$$x'.x'=a^2x.x+2abx.y+b^2y.y=$$
$$=a^2t^2n+ab(2nt-b)+b^2(n+a)=$$
$$=n(a^2t^2+2abt+b^2)=t'^2n.$$

С другой стороны,

$$tt'=at^2+bt=t^2y.y-nt^2+2nt^2-2tx.y=$$
$$=t^2y.y-2tx.y+x.x=(ty-x).(ty-x)=t^2z.z,$$

откуда $t'=tz.z$; так как $0<z.z<1$, то $0<t'<t$. Это противоречит минимальности числа t и завершает доказательство леммы.

Для доказательства теоремы теперь достаточно проверить, что форма $f=X_1^2+X_2^2+X_3^2$ удовлетворяет условию (H) леммы B. А это делается непосредственно: если $(x_1, x_2, x_3)\in\mathbf{Q}^3$, то выберем такой элемент $(y_1, y_2, y_3)\in\mathbf{Z}^3$, чтобы $|x_i-y_i|<{}^1/_2$ для всех i; имеем $\sum(x_i-y_i)^2\leqslant{}^3/_4<1$.

Следствие 1 (Лагранж). *Каждое целое положительное число есть сумма четырех квадратов.*

Пусть n — целое число >0. Его можно записать в виде 4^am, где m не делится на 4. Если $m\equiv 1, 2, 3, 5, 6 \pmod 8$, то m есть сумма трех квадратов и это же верно для n. Если это не так, то $m\equiv -1 \pmod 8$ и $m-1$ является суммой трех квадратов; в этом случае m является суммой четырех квадратов и это же верно для n.

Следствие 2 (Гаусс). *Любое целое положительное число есть сумма трех треугольных чисел.*

(«Треугольным числом» называют любое число вида $m(m+1)/2$, где m — целое число.)

Пусть n — целое число $\geqslant 0$. Применяя теорему к $8n+3$, находим целые числа x_1, x_2, x_3, такие, что

$$x_1^2 + x_2^2 + x_3^2 = 8n + 3;$$

имеем

$$x_1^2 + x_2^2 + x_3^2 \equiv 3 \pmod 8.$$

Однако единственными квадратами в $\mathbf{Z}/8\mathbf{Z}$ являются 0, 1 и 4; сумма трех квадратов в $\mathbf{Z}/8\mathbf{Z}$ может быть равна 3 только тогда, когда каждое слагаемое равно 1. Отсюда заключаем, что числа x_i нечетны и их можно записать в виде $2m_i + 1$, где m_i — целые числа. Имеем

$$\sum_{i=1}^{i=3} \frac{m_i(m_i+1)}{2} = \frac{1}{8}\left(\sum_{i=1}^{i=3}(2m_i+1)^2 - 3\right) =$$

$$= \frac{1}{8}(8n + 3 - 3) = n.$$

Глава V

ЦЕЛЫЕ КВАДРАТИЧНЫЕ ФОРМЫ С ДИСКРИМИНАНТОМ ± 1

§ 1. Предварительные сведения

1.1. *Определения*

Пусть n — целое число $\geqslant 0$. Мы будем иметь дело со следующей категорией S_n.

Объектом E в S_n является *свободная абелева группа ранга n* (изоморфная, следовательно, $\mathbf{Z}^n$), снабженная билинейной симметрической формой $E \times E \to \mathbf{Z}$, обозначаемой $(x, y) \mapsto x.y$, такая, что:

i) *Гомоморфизм* E *в* $\mathrm{Hom}(E, \mathbf{Z})$, *определенный формой* $x.y$, *является изоморфизмом.*

Сразу же видно, что это условие равносильно следующему (см. Н. Бурбаки, Алгебра, гл. IX, § 2, предложение 3):

ii) *Если* (e_i) — *базис* E *и* $a_{ij} = e_i.e_j$, *то определитель матрицы* $A = (a_{ij})$ *равен* ± 1.

Понятие *изоморфизма* двух объектов $E, E' \in S_n$ определяется очевидным образом; в этом случае будем писать $E \simeq E'$. Удобно также ввести обозначение $S = \bigcup S_n$, $n = 0, 1, \ldots$.

Если $E \in S_n$, то отображение $x \mapsto x.x$ превращает E в *квадратичный модуль* над $\mathbf{Z}$ (см. определение 1 п. 1.1 гл. IV). Если (e_i) — базис E и $x = \sum x_i e_i$, то квадратичная форма $f(x) = x.x$ задается формулой

$$f(x) = \sum_{i,j} a_{ij} x_i x_j = \sum_i a_{ii} x_i^2 + 2 \sum_{i<j} a_{ij} x_i x_j,$$

где $a_{ij} = e_i.e_j$. Таким образом, коэффициенты ее недиагональных членов четны. Дискриминант формы f (т. е. $\det(a_{ij})$) равен ± 1. Изменение базиса (e_i) приводит к замене матрицы $A = (a_{ij})$ матрицей ${}^tBAB$, где $B \in \mathbf{GL}(n, \mathbf{Z})$. Применительно к форме f это

приводит к осуществлению над переменными (x_i) линейного преобразования с матрицей B; получаемая форма называется формой, *эквивалентной* форме f. (Заметим, что речь идет об эквивалентности *над кольцом* $\mathbf{Z}$ *целых чисел*; это понятие *тоньше*, чем понятие эквивалентности над $\mathbf{Q}$, изученное в предыдущей главе.)

1.2. *Действия на* S

Пусть $E, E' \in S$. Обозначим через $E \oplus E'$ *прямую сумму* E и E', снабженную билинейной формой, являющейся прямой суммой тех билинейных форм, которыми снабжены модули E и E'; по определению (см. Н. Бурбаки, Алгебра, гл. IX, § 1, п° 3):

$$(x + x').(y + y') = x.y + x'.y',$$
$$\text{если } x, y \in E \text{ и } x', y' \in E'.$$

Применительно к квадратичным формам это действие соответствует нахождению *прямой ортогональной суммы*, обозначавшемуся нами в гл. IV через $\widehat{\oplus}$.

Далее можно было бы определить как *тензорное произведение* $E \otimes E'$, так и *внешние степени* $\bigwedge^m E$ (см. Н. Бурбаки, Алгебра, гл. IX, § 1, п° 9); нам эти действия не понадобятся.

1.3. *Инварианты*

1.3.1. Если $E \in S_n$, то целое число n называется *рангом* модуля E и обозначается через $r(E)$.

1.3.2. Пусть $E \in S$, и пусть $V = E \otimes \mathbf{R}$ — векторное $\mathbf{R}$-пространство, получаемое расширением области скаляров $\mathbf{Z}$ до $\mathbf{R}$. Квадратичная форма пространства V имеет некоторую *сигнатуру* (r, s), как это определено ранее (см. п. 2.4 гл. IV). Целое число

$$\tau(E) = r - s$$

называется *индексом* модуля E. Имеем:

$$-r(E) \leqslant \tau(E) \leqslant r(E), \qquad r(E) \equiv \tau(E) \pmod 2.$$

Напомним, что модуль E называется *определенным*, если $\tau(E) = \pm r(E)$, т. е. если $x.x$ имеет постоянный знак; в противном случае E называется *неопределенным*.

1.3.3. *Дискриминант* модуля E относительно базиса (e_i) не зависит от выбора этого базиса; действительно, при изменении базиса (e_i) дискриминант умножается на

$$\det({}^tXX) = \det(X)^2,$$

где X — обратимая над $\mathbf{Z}$ матрица; определитель матрицы X равен ± 1, и его квадрат равен 1.

Дискриминант модуля E обозначается через $d(E)$; при этом $d(E) = \pm 1$.

Если $V = E \otimes \mathbf{R}$ имеет сигнатуру (r, s), то знак числа $d(E)$ тот же, что у $(-1)^s$; так как $d(E) = \pm 1$, отсюда выводится формула

$$d(E) = (-1)^{(r(E)-\tau(E))/2}.$$

1.3.4. Пусть $E \in S$. Говорят, что модуль E *четен* (или есть *модуль второго типа*), если квадратичная форма, ассоциированная с E, принимает лишь четные значения; если A — матрица, соответствующая какому-либо базису в E, то четность модуля E означает, что *все диагональные члены матрицы* A *четны*.

Если модуль E не является четным, то говорят, что он *нечетен* (или есть *модуль первого типа*).

1.3.5. Пусть $E \in S$, и пусть $\bar{E} = E/2E$ — редукция модуля E по модулю 2. Это векторное пространство размерности $r(E)$ над полем $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. При помощи факторизации форма $x.y$ определяет на $\bar{E}$ форму $\bar{x}.\bar{y}$, которая симметрична и имеет дискриминант $\pm 1 = 1$. Ассоциированная квадратичная форма $\bar{x}.\bar{x}$ аддитивна:

$$(\bar{x} + \bar{y}).(\bar{x} + \bar{y}) = \bar{x}.\bar{x} + \bar{y}.\bar{y} + 2\bar{x}.\bar{y} = \bar{x}.\bar{x} + \bar{y}.\bar{y};$$

таким образом, это элемент модуля, *сопряженного* $\bar{E}$. Но билинейная форма $\bar{x}.\bar{y}$ не вырождена: она определяет изоморфизм $\bar{E}$ на сопряженный к нему мо-

дуль. Отсюда заключаем, что существует такой *канонический элемент* $\bar{u} \in \bar{E}$, что

$$\bar{u}.\bar{x} = \bar{x}.\bar{x} \quad \text{для любого} \quad \bar{x} \in \bar{E}.$$

Возвращаясь к E, заключаем, что существует элемент $u \in E$, определенный по модулю $2E$ и такой, что

$$u.x \equiv x.x \pmod 2 \quad \text{для любого} \quad x \in E.$$

Рассмотрим целое число $u.u$. Если заменить u на $u + 2x$, то $u.u$ заменится на

$$(u + 2x).(u + 2x) = u.u + 4(u.x + x.x) \equiv u.u \pmod 8.$$

Образ числа $u.u$ в $\mathbf{Z}/8\mathbf{Z}$ является, следовательно, *инвариантом* модуля E; обозначим его через $\sigma(E)$. Если E — модуль второго типа, то $\bar{x}.\bar{x}$ — нулевая форма (иными словами, форма $\bar{x}.\bar{y}$ *антисимметрична*) и можно взять $\bar{u} = 0$, откуда $\sigma(E) = 0$.

1.3.6. Пусть p — некоторое простое число, и пусть $V_p = E \otimes \mathbf{Q}_p$ — векторное $\mathbf{Q}_p$-пространство, получаемое расширением области скаляров $\mathbf{Z}$ до $\mathbf{Q}_p$. Инвариант $\varepsilon(V_p) = \pm 1$ квадратичного модуля V_p, определенный в п. 2.1 гл. IV, тем более является инвариантом модуля E; обозначим его через $\varepsilon_p(E)$. Можно показать, что

$$\varepsilon_p(E) = 1, \quad \text{если} \quad p \neq 2,$$

$$\varepsilon_2(E) = (-1)^j, \quad \text{где} \quad j = \frac{1}{4}(d(E) + r(E) - \sigma(E) - 1).$$

Это выводится из разложения $E \otimes \mathbf{Z}_p$ в прямую ортогональную сумму $\mathbf{Z}_p$-модулей ранга 1 (соответственно рангов 1 или 2), если $p \neq 2$ (соответственно если $p = 2$). Поскольку нам не придется пользоваться этими формулами, мы оставляем детали проверки читателю (см. также Cassels J., *Comm. Math. Helv.*, **37** (1962), 61—64).

1.3.7. Пусть $E_1, E_2 \in S$, и пусть $E = E_1 \oplus E_2$. Для того чтобы E был модулем второго типа, необхо-

димо и достаточно, чтобы такими были модули E и E_2. Мы имеем

$$r(E) = r(E_1) + r(E_2), \qquad \tau(E) = \tau(E_1) + \tau(E_2),$$
$$\sigma(E) = \sigma(E_1) + \sigma(E_2), \qquad d(E) = d(E_1).d(E_2).$$

1.4. *Примеры*

1.4.1. Обозначим через I_+ (соответственно через I_-) **Z**-модуль **Z**, снабженный билинейной формой xy (соответственно $-xy$); он отвечает квадратичной форме x^2 (соответственно $-x^2$).

Если s и t — целые числа $\geqslant 0$, то через $sI_+ \oplus tI_-$ обозначим прямую сумму s экземпляров модуля I_+ и t экземпляров модуля I_-; соответствующая квадратичная форма имеет вид $\sum_{i=1}^{s} x_i^2 - \sum_{j=1}^{t} y_j^2$. Этот модуль имеет следующие инварианты:

$$r = s + t, \quad \tau = s - t, \quad d = (-1)^t, \quad \sigma \equiv s - t \pmod 8.$$

Исключаем тривиальный случай $(s, t) = (0, 0)$; тогда модуль $sI_+ \oplus tI_-$ является модулем первого типа.

1.4.2. Обозначим через U элемент из S_2, определенный матрицей $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Ассоциированная квадратичная форма имеет вид $2x_1x_2$: U есть форма второго типа. Имеем

$$r(U) = 2, \quad \tau(U) = 0, \quad d(U) = -1, \quad \sigma(U) = 0.$$

1.4.3. Пусть k — целое число $\geqslant 0$, пусть $n = 4k$, и пусть V — векторное пространство $\mathbf{Q}^n$, снабженное стандартной билинейной формой $\sum x_i y_i$, соответствующей единичной матрице. Пусть E_0 — подгруппа в V, состоящая из точек с целыми координатами; будучи снабжен билинейной формой, которая индуцирована формой модуля V, модуль E_0 становится элементом в S_n, изоморфным модулю nI_+. Пусть E_1 — подмодуль модуля E_0, состоящий из таких эле-

ментов x, что $x.x \equiv 0 \pmod 2$, т. е. $\sum x_i \equiv 0 \pmod 2$. Имеем

$$(E_0 : E_1) = 2.$$

Пусть E — подмодуль в V, порожденный модулем E_1 и элементом $e = (1/2, \ldots, 1/2)$. Имеем: $2e \in E_1$ (ибо $n \equiv 0 \pmod 4$) и $e \notin E_1$; поэтому $(E : E_1) = 2$. Для того чтобы элемент $x = (x_i)$ из V принадлежал подмодулю E, необходимо и достаточно, чтобы

$$2x_i \in \mathbf{Z}, \quad x_i - x_j \in \mathbf{Z}, \quad \sum_{i=1}^{n} x_i \in 2\mathbf{Z}.$$

Тогда $x.e = 1/2 \sum x_i \in \mathbf{Z}$; так как $e.e = k$, форма $x.y$ *принимает на* E *целые значения*. Далее, из того, что E_1 имеет тот же индекс в E_0, что и в E, следует, что дискриминант модуля E равен дискриминанту модуля E_0, т. е. числу $+1$. Таким образом, квадратичный модуль E является элементом в $S_n = S_{4k}$; будем его обозначать через Γ_n. Когда k *четно* (т. е. когда $n \equiv 0 \pmod 8$), $e.e = k$ четно, а отсюда вытекает, что $x.x$ четно для любого $x \in E$; таким образом, если $n \equiv 0 \pmod 8$, то Γ_n *есть модуль второго типа*. Имеем

$$r(\Gamma_{8m}) = 8m, \quad \tau(\Gamma_{8m}) = 8m, \quad \sigma(\Gamma_{8m}) = 0, \quad d(\Gamma_{8m}) = 1.$$

Особенно интересен случай Γ_8. Имеется 240 таких элементов [1]) $x \in \Gamma_8$, что $x.x = 2$; если через (e_i) обозначить канонический базис в $\mathbf{Q}^8$, то такими будут векторы

$$\pm e_i \pm e_k \ (i \neq k) \quad \text{и} \quad 1/2 \sum_{i=1}^{8} \varepsilon_i e_i, \ \varepsilon_i = \pm 1, \ \prod_{i=1}^{8} \varepsilon_i = 1.$$

[Скалярные произведения этих векторов друг на друга целые; они образуют то, что в теории групп Ли называют «*системой корней типа* E_8» (см. Н. Бурбаки, Группы Ли и алгебры Ли, гл. VI, § 4, n° 10).]

[1]) Для более общего случая мы увидим в п. 6.6 гл. VII, что если N любое целое число $\geqslant 1$, то количество таких $x \in \Gamma_8$, что $x.x = 2N$, равно умноженной на 240 сумме кубов делителей числа N.

Можно взять в качестве базиса в Γ_8 элементы

$$\tfrac{1}{2}(e_1+e_8)-\tfrac{1}{2}(e_2+\ \dots\ +e_7),$$
$$e_1+e_2 \quad \text{и} \quad e_i-e_{i-1} \quad (2\leqslant i\leqslant 7).$$

Соответствующая матрица имеет вид

$$\Gamma_8=\begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0\\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0\\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0\\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0\\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0\\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0\\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1\\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}.$$

Для $m\geqslant 2$ векторы $x\in\Gamma_{8m}$, удовлетворяющие условию $x.x=2$, исчерпываются совокупностью $\pm e_i\pm e_k$ $(i\neq k)$; мы увидим, что они *не порождают* Γ_{8m} в отличие от того, что имеет место в случае $m=1$. В частности, $\Gamma_8\oplus\Gamma_8$ *не изоморфно* Γ_{16}.

1.5. *Группа* K(S)

Пусть E, E′ ∈ S. Будем говорить, что E и E′ *стабильно изоморфны*, если существует F ∈ S такой, что $E\oplus F\simeq E'\oplus F$; это отношение является отношением эквивалентности. Мы обозначим через $K_+(S)$ результат факторизации множества S по этому отношению, и если E ∈ S, то будем обозначать через (E) класс объекта E в $K_+(S)$. При факторизации действие $\oplus$ определяет некоторый закон композиции на $K_+(S)$, обозначаемый $+$; этот закон коммутативен, ассоциативен и имеет в качестве нейтрального элемента класс 0 модуля $0\in S$. Имеем

$$(E\oplus E')=(E)+(E').$$

Кроме того, если $x, y, z\in K_+(S)$ таковы, что $x+z=y+z$, то $x=y$, что проверяется непосредственно.

Это позволяет определить *группу* $K(S)$, исходя из $K_+(S)$ (точно так же, как определяется $\mathbf{Z}$, исходя из множества $\mathbf{Z}_+$ целых чисел $\geqslant 0$): по определению элементом в $K(S)$ является пара (x, y), где $x, y \in K_+(S)$; при этом две пары (x, y), (x', y') отождествляются в том и только в том случае, когда $x + y' = y + x'$. Закон композиции в $K(S)$ определяется посредством формулы

$$(x, y) + (x', y') = (x + x', y + y').$$

Он превращает $K(S)$ в коммутативную группу с нейтральным элементом $(0, 0)$. Отождествим $K_+(S)$ с подмножеством в $K(S)$ при помощи отображения $x \mapsto (x, 0)$. Любой элемент из $K(S)$ есть разность двух элементов из $K_+(S)$, которая может быть записана в виде $(E) - (F)$, где $E, F \in S$. Имеем

$$(E) - (F) = (E') - (F') \quad \text{в} \quad K(S)$$

тогда и только тогда, когда существует такой $G \in S$, что

$$E \oplus F' \oplus G \simeq E' \oplus F \oplus G,$$

т. е. тогда и только тогда, когда $E \oplus F'$ и $E' \oplus F$ стабильно изоморфны.

Свойство универсальности группы $K(S)$. Пусть A — коммутативная группа, и пусть $f\colon S \to A$ — такое отображение, что

$$f(E) = f(E_1) + f(E_2), \quad \text{если} \quad E \simeq E_1 \oplus E_2;$$

тогда будем говорить, что отображение f *аддитивно*. Если $x = (E) - (F)$ — элемент из $K(S)$, то положим $f(x) = f(E) - f(F)$; это определение не зависит от выбора разложения для x. Непосредственно ясно, что так определенное отображение $f\colon K(S) \to A$ есть *гомоморфизм*. Обратно, каждый гомоморфизм $f\colon K(S) \to A$ при помощи композиции с вложением $S \to K(S)$ дает аддитивную функцию на S. Чтобы выразить это свойство «универсальности» группы $K(S)$, говорят, что $K(S)$ есть *группа Гротендика* категории S относительно действия $\oplus$.

В частности, инварианты r, τ, d, σ из п. 1.3 определяют гомоморфизмы

$$r\colon K(S)\to\mathbf{Z}, \qquad \tau\colon K(S)\to\mathbf{Z},$$
$$d\colon K(S)\to\{\pm 1\}, \qquad \sigma\colon K(S)\to\mathbf{Z}/8\mathbf{Z}.$$

Кроме того, мы здесь имеем $\tau\equiv r \pmod 2$, $d=(-1)^{(r-\tau)/2}$.

§ 2. Формулировки результатов

2.1. *Описание группы* $K(S)$

Теорема 1. *Группа* $K(S)$ *есть свободная абелева группа с базисом* (I_+) *и* (I_-).

(Доказательство будет дано в п. 3.4.)

Иными словами, каждое $f\in K(S)$ единственным образом записывается в виде

$$f=s.(I_+)+t.(I_-), \quad \text{где} \quad s,\ t\in\mathbf{Z}.$$

Мы имеем $r(f)=s+t$, $\tau(f)=s-t$, а это показывает, что s и t вполне определяются через r и τ. Отсюда заключаем, что имеет место

Следствие 1. *Пара* (r, τ) *определяет изоморфизм группы* $K(S)$ *на подгруппу группы* $\mathbf{Z}\times\mathbf{Z}$, *состоящую из таких элементов* (a, b), *что* $a\equiv b \pmod 2$.

Отсюда вытекает

Следствие 2. *Для того чтобы два элемента* E *и* E′ *из* S *были стабильно изоморфными, необходимо и достаточно, чтобы они имели одинаковые ранги и одинаковые индексы.*

[Заметим, что это никоим образом не обеспечивает $E\simeq E'$. Например, $U=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ определяет в $K(S)$ тот же элемент, что и $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=I_+\oplus I_-$, хотя U и $I_+\oplus I_-$ являются модулями разного типа.]

Теорема 2. *Имеет место* $\sigma(E)\equiv\tau(E) \pmod 8$ *для любого* $E\in S$.

Действительно, τ, редуцированное по модулю 8, и σ являются гомоморфизмами группы $K(S)$ в $\mathbf{Z}/8\mathbf{Z}$, которые совпадают на образующих I_+ и I_- группы $K(S)$; следовательно, они совпадают на всей группе $K(S)$.

Следствие 1. *Если* E *является модулем второго типа, то* $\tau(E) \equiv 0 \pmod 8$.

Действительно, $\sigma(E) = 0$.

[Заметим, что это влечет $r(E) \equiv 0 \pmod 2$ и $d(E) = (-1)^{r(E)/2}$.]

Следствие 2. *Если* E *— определенный модуль второго типа, то* $r(E) \equiv 0 \pmod 8$.

Действительно, в этом случае $\tau(E) = \pm r(E)$.

Замечания. 1) Обратно, мы видели в п. 1.4, что для любого n, кратного 8, существует $E \in S_n$, который положительно определен и является модулем второго типа.

2) Сравнение $\sigma(E) \equiv \tau(E) \pmod 8$ может быть также выведено из формулы произведения $\prod \varepsilon_v(E) = 1$ (см. п. 3.1 гл. IV) с использованием значений $\varepsilon_p(E)$, данных (без доказательства) в п. 1.3.6.

2.2. *Структурные теоремы (случай неопределенного модуля)*

Пусть $E \in S$. Мы говорим, что E *представляет нуль*, если существует такой элемент $x \in E$, $x \neq 0$, что $x.x = 0$. Это равносильно тому, что соответствующая квадратичная форма $Q(x)$ *представляет* 0 *над* $\mathbf{Q}$ в смысле п. 1.6 гл. IV; действительно, от рационального нуля можно перейти к целому нулю при помощи гомотетии.

Теорема 3. *Если модуль* $E \in S$ *неопределенный, то* E *представляет нуль.*

(Доказательство будет дано в п. 3.1.)

Теорема 4. *Если* $E \in S$ *— неопределенный модуль первого типа, то* E *изоморфен прямой сумме* $sI_+ \oplus tI_-$, *где* s *и* t *— целые числа* $\geqslant 1$.

[Соответствующая квадратичная форма эквивалентна над $\mathbf{Z}$ форме $\sum_{i=1}^{s} x_i^2 - \sum_{j=1}^{t} y_j^2$.]

(Доказательство будет дано в п. 3.3.)

Следствие. *Пусть* E *и* E′ *— два элемента из* S *одинакового ранга и одинакового индекса. Тогда*

$$E \oplus I_+ \simeq E' \oplus I_+ \quad \textit{или} \quad E \oplus I_- \simeq E' \oplus I_-.$$

Это ясно, если $E = 0$. Если это не так, то один из двух модулей $E \oplus I_+$, $E \oplus I_-$ — неопределенный. Предположим, что таким является первый. Так как E и E′ имеют одинаковую сигнатуру, модуль $E' \oplus I_+$ также является неопределенным. Применяя теорему 4, мы видим, что $E \oplus I_+$ и $E' \oplus I_+$ изоморфны модулям $sI_+ \oplus tI_-$ и $s'I_+ \oplus t'I_-$ соответственно. Так как E и E′ имеют одинаковую сигнатуру, то $s = s'$, $t = t'$, откуда следует искомое.

Теорема 5. *Если* $E \in S$ *— неопределенный модуль второго типа и если* $\tau(E) \geqslant 0$, *то* E *изоморфен модулю* $pU \oplus q\Gamma_8$, *где* p *и* q *суть некоторые подходящие целые числа* $\geqslant 0$.

[Когда $\tau(E) \leqslant 0$, имеет место аналогичный результат, который достигается применением теоремы к модулю, получаемому из E изменением знака квадратичной формы.]

(Доказательство будет дано в п. 3.5.)

Заметим, что $q = \frac{1}{8}\tau(E)$ и $p = \frac{1}{2}(r(E) - \tau(E))$. Поэтому модуль E определяется с точностью до изоморфизма своим рангом и своим индексом. Поскольку то же самое имеет место для модулей первого типа (см. теорему 4), отсюда вытекает

Теорема 6. *Если модули* $E, E' \in S$ *неопределенные, имеют одинаковые ранги, одинаковые индексы и одинаковые типы, то они изоморфны.*

2.3. *Случай определенного модуля*

Здесь нет структурных теорем, имеется лишь *теорема конечности*: для любого целого числа n категория S_n содержит лишь конечное число положительно определенных классов. Это следует, например, из теории «приведения» квадратичных форм. Явное перечисление этих классов сделано лишь для малых значений ранга n (для $n \leqslant 16$ см. Kneser M., *Archiv der Math.*, 8 (1957), 241—250). Для доказательства теоремы конечности можно применить *формулу Минковского — Зигеля* (Кнезер пользовался другим методом). Вот в чем заключается эта формула (я ограничусь для простоты вторым типом; имеются аналогичные результаты для первого типа).

Пусть $n = 8k$ — некоторое целое число, делящееся на 8. Обозначим через C_n множество классов, т. е. взятых с точностью до изоморфизма элементов $E \in S_n$, являющихся положительно определенными модулями второго типа. Пусть G_E — *группа автоморфизмов* модуля $E \in C_n$; это — конечная группа, поскольку она является дискретной подгруппой ортогональной группы, которая компактна; пусть g_E — порядок группы G_E. Положим

$$M_n = \sum_{E \in C_n} 1/g_E.$$

Это — «масса» [1]) множества C_n в смысле Эйзенштейна, т. е. число элементов E из C_n, подсчитанных каждый с множителем $1/g_E$. Формула Минковского — Зигеля [2]) дает

$$M_n = 2^{1-8k} \frac{B_{2k}}{(4k)!} \prod_{j=1}^{j=4k-1} B_j \qquad (n = 8k), \qquad (*)$$

где через B_j обозначены *числа Бернулли* ($B_1 = 1/6$, $B_2 = 1/30$, ...; см. п. 4.1 гл. VII).

[1]) Иначе называемая «весом» или «мерой». — *Прим. ред.*

[2]) Доказательство этой формулы имеется у Зигеля (Siegel C. L., Gesamm. Abh., I, п. 20; III, п. 79).

(Вот несколько приближенных значений для M_n:

$$M_8 = 10^{-9} \times 1{,}4352\ldots; \quad M_{16} = 10^{-18} \times 2{,}4885\ldots;$$
$$M_{24} = 10^{-15} \times 7{,}9369\ldots; \quad M_{32} = 10^{7} \times 4{,}0309\ldots;$$
$$M_{40} = 10^{51} \times 4{,}3930\ldots.)$$

Эта формула позволяет устанавливать, что подмножество C' множества C_n *совпадает с* C_n: достаточно проверить, что сумма значений $1/g_E$ для $E \in C'$ равна величине M_n (если $C' \neq C_n$, то эта сумма $< M_n$).

Примеры

i) $n = 8$, т. е. $k = 1$. Выше (п. 1.4.3) был дан один пример модуля Γ_8 из C_8. Можно проверить (см., например, Н. Бурбаки, Группы Ли и алгебры Ли, гл. VI, § 4, n° 10), что группа автоморфизмов модуля Γ_8 имеет порядок $2^{14}3^5 5^2 7$. С другой стороны, формула (*) дает значение $M_8 = 2^{-14}3^{-5}5^{-2}7^{-1}$. Сравнивая, мы видим, что C_8 *сводится к одному элементу* Γ_8, что является результатом Морделла.

ii) $n = 16$. Известны два элемента из C_{16}: Γ_{16} и $\Gamma_8 \oplus \Gamma_8$. Можно показать, что относящиеся к ним порядки g_E соответственно равны $2^{15}(16!)$ и $2^{29}3^{10}5^4 7^2$. С другой стороны, $M_{16} = 691 \cdot 2^{-30}3^{-10}5^{-4}7^{-2}11^{-1}13^{-1}$, и нетрудно проверить, что

$$691/2^{30}3^{10}5^4 7^2 11 \cdot 13 = 1/2^{15}(16!) + 1/2^{29}3^{10}5^4 7^2.$$

Таким образом, $C_{16} = \{\Gamma_{16},\ \Gamma_8 \oplus \Gamma_8\}$, что является результатом Витта.

iii) $n = 24$. Определение множества C_{24} было дано в 1968 г. Нимейером (H. Niemeier); это множество состоит из 24 элементов. Один из них (открытый Личем в связи с проблемой упаковки сфер в $\mathbf{R}^{24}$) особенно замечателен; это единственный элемент из C_{24}, который не содержит ни одного вектора x такого, что $x.x = 2$. Его группа автоморфизмов G имеет порядок

$$2^{23}3^9 5^4 7^2 11 \cdot 13 \cdot 23 = 8\,315\,553\,613\,086\,720\,000.$$

Факторгруппа $G/\{\pm 1\}$ есть новая простая группа, найденная Конвеем [1]).

iv) $n=32$. Так как $M_{32} > 4 \cdot 10^7$ и так как $g_E \geqslant 2$ для всех E, то C_{32} имеет более 80 миллионов элементов; их списка еще нет.

§ 3. Доказательства

3.1. *Доказательство теоремы 3*

Пусть $E \in S_n$, и пусть $V = E \otimes \mathbf{Q}$ — соответствующее векторное $\mathbf{Q}$-пространство. Предполагается, что E — неопределенный модуль, и нам надо доказать, что E (или V, что приводит к тому же) представляет 0. Будем различать ряд случаев.

i) $n=2$. В этом случае пространство V имеет сигнатуру (1, 1), откуда $d(E) = -1$. Так как $-d(E)$ есть квадрат в $\mathbf{Q}$, то V представляет 0.

ii) $n=3$. Пусть $f(X_1, X_2, X_3) = \sum a_{ij} X_i X_j$ — *квадратичная форма, соответствующая некоторому базису* модуля E; мы имеем $a_{ij} \in \mathbf{Z}$ и $\det(a_{ij}) = \pm 1$. Если p — простое число $\neq 2$, то форма, полученная из f редукцией по модулю p, имеет нетривиальный нуль (п. 2.2 гл. I) и этот нуль поднимается до p-адического нуля (следствие 2 теоремы 1 п. 2.2 гл. II). Таким образом, f представляет 0 в каждом из $\mathbf{Q}_p$ ($p \neq 2$), так же как и в $\mathbf{R}$; на основании следствия 3 теоремы 8 п. 3.2 гл. IV отсюда вытекает, что f представляет 0 в $\mathbf{Q}$.

iii) $n=4$. Такие же соображения, как и приведенные выше, показывают, что квадратичная форма f представляет 0 в каждом из $\mathbf{Q}_p$, $p \neq 2$, так же как и в $\mathbf{R}$. Если дискриминант $d(E)$ формы f равен 1, то этого достаточно для установления того, что f представляет 0 в $\mathbf{Q}$ (следствие 3 теоремы 8 п. 3.2 гл. IV). В противном случае

$$d(E) = -1$$

[1]) См. Conway J. H., *Proc. Nat. Acad. Sci. USA*, **61** (1968), 398—400; ср. также *Invent. Math.*, **7** (1969), 137—142.

и $d(E)$ не является квадратом в $\mathbf{Q}_2$; на основании теоремы 6 п. 2.2 гл. IV отсюда вытекает, что f представляет 0 в $\mathbf{Q}$.

iv) $n \geqslant 5$. Применяется теорема Мейера (следствие 2 теоремы 8 п. 3.2 гл. IV).

3.2. *Леммы*

Пусть $E \in S$, и пусть F — некоторый подмодуль в E; пусть F' — множество элементов из E, ортогональных элементам из F.

Лемма 1. *Для того чтобы модуль* F, *снабженный формой* $x.y$, *которая индуцирована формой модуля* E, *принадлежал категории* S, *необходимо и достаточно, чтобы* E *был прямой суммой модулей* F *и* F'.

Если $E = F \oplus F'$, то имеем $d(E) = d(F).d(F')$, откуда $d(F) = \pm 1$. Обратно, если $d(F) = \pm 1$, то, очевидно, $F \cap F' = 0$; кроме того, если $x \in E$, то линейная форма $y \mapsto x.y$ ($y \in F$) определяется некоторым элементом $x_0 \in F$. Тогда $x = x_0 + x_1$, где $x_0 \in F$ и $x_1 \in F'$, откуда $E = F \oplus F'$.

Лемма 2. *Пусть* $x \in E$, *причем* $x.x = \pm 1$, *и пусть* X — *ортогонал к* x *в* E. *Тогда, если* $D = \mathbf{Z}x$, *то* $E = D \oplus X$.

Утверждение вытекает из леммы 1 при $F = D$. (Если, например, $x.x = 1$, то $D \simeq I_+$, откуда $E \simeq I_+ \oplus X$.)

Элемент $x \in E$ называется *неделимым*, если он не принадлежит подгруппе nE ($n \geqslant 2$), иными словами, если он не делится ни на какое целое число $\geqslant 2$. Каждый ненулевой элемент из E единственным способом записывается в виде mx, где $m \geqslant 1$, а x неделим.

Лемма 3. *Если* x — *неделимый элемент из* E, *то существует* $y \in E$, *такой, что* $x.y = 1$.

Пусть f_x — линейная форма $y \mapsto x.y$, определяемая элементом x. Это гомоморфизм модуля E в $\mathbf{Z}$.

Более того, f_x *неделим*, так как x неделим и так как $x.y$ определяет изоморфизм модуля E на сопряженный к нему модуль $\mathrm{Hom}(E, \mathbf{Z})$. Отсюда заключаем, что f_x сюръективен (иначе его можно было бы разделить на целое число $\geqslant 2$), а потому существует $y \in E$, такой, что $x.y = 1$.

3.3. *Структурная теорема (случай нечетного неопределенного модуля*[1])

Лемма 4. *Пусть* $E \in S_n$. *Предположим, что* E — *неопределенный модуль первого типа. Тогда существует такой модуль* $F \in S_{n-2}$, *что* $E \simeq I_+ \oplus I_- \oplus F$.

По теореме 3 существует такой $x \in E$, $x \neq 0$, что $x.x = 0$. Деля в случае надобности элемент x на подходящее целое число, мы можем предполагать, что x неделим; на основании изложенной выше леммы 3 тогда существует такой $y \in E$, что $x.y = 1$. Элемент y может быть выбран так, чтобы $y.y$ было *нечетным*. Действительно, предположим, что $y.y$ четно; поскольку E — модуль первого типа, существует такой элемент $t \in E$, что $t.t$ нечетно. Положим $y' = t + ky$ и выберем k так, чтобы $x.y = 1$, т. е. $k = 1 - x.t$; мы имеем $y'.y' \equiv t.t \pmod 2$, и $y'.y'$ нечетно. Таким образом, можно предположить, что $y.y = 2m + 1$. Положим тогда

$$e_1 = y - mx, \quad e_2 = y - (m+1)x.$$

Непосредственно устанавливаем, что $e_1.e_1 = 1$, $e_1.e_2 = 0$, $e_2.e_2 = -1$. Подмодуль G модуля E, порожденный элементами (e_1, e_2), изоморфен сумме $I_+ \oplus I_-$; поэтому по лемме 1 $E \simeq I_+ \oplus I_- \oplus F$, где $F \in S_{n-2}$.

Доказательство теоремы 4. Ведем рассуждения индукцией по n. Пусть $E \in S_n$, где E — неопределенный модуль первого типа. По лемме 4 $E \simeq I_+ \oplus I_- \oplus F$. Если $n = 2$, то $F = 0$, и теорема доказана. Если $n > 2$,

---

[1]) Метод, которому следует данный пункт, подсказан мне Милнором, так же как и идея введения группы $\tilde{K}(S)$.

то $F \neq 0$, и один из модулей $I_+ \oplus F$, $I_- \oplus F$ — неопределенный; предположим, например, что имеет место первый случай. Так как I_+ является модулем первого типа, то таким же является и модуль $I_+ \oplus F$, и предположение индукции показывает, что $I_+ \oplus F$ имеет вид $aI_+ \oplus bI_-$; отсюда

$$E \simeq aI_+ \oplus (b+1)I_-.$$

3.4. *Описание группы* $K(S)$

Пусть $E \in S$, $E \neq 0$. Тогда или $E \oplus I_+$, или $E \oplus I_-$ — неопределенный модуль первого типа. Применяя теорему 4, отсюда выводим, что образ модуля E в $K(S)$ есть линейная комбинация классов (I_+) и (I_-). Поэтому (I_+) и (I_-) порождают $K(S)$. Так как их образы при гомоморфизме

$$(r, \tau)\colon K(S) \to \mathbf{Z} \times \mathbf{Z}$$

линейно независимы, то классы (I_+) и (I_-) составляют базис в $K(S)$.

3.5. *Структурная теорема (случай четного неопределенного модуля)*

Лемма 5. *Пусть* $E \in S$. *Предположим, что* E — *неопределенный модуль второго типа. Тогда существует такой модуль* $F \in S$, *что* $E \simeq U \oplus F$.

Рассуждаем, как в доказательстве леммы 4. Сначала выберем $x \in E$, $x \neq 0$, x — неделимый элемент, $x.x = 0$; затем выберем такой элемент $y \in E$, что $x.y = 1$. Если $y.y = 2m$, то заменим y на $y - mx$, так что для нового элемента $y.y = 0$. Тогда подмодуль G модуля E, порожденный элементами (x, y), изоморфен модулю U; по лемме 1 $E \simeq U \oplus F$, где $F \in S$.

Лемма 6. *Пусть* $F_1, F_2 \in S$. *Предположим, что* F_1 *и* F_2 — *модули второго типа и что* $I_+ \oplus I_- \oplus F_1 \simeq I_+ \oplus I_- \oplus F_2$. *Тогда* $U \oplus F_1 \simeq U \oplus F_2$.

Чтобы упростить обозначения, положим $W = I_+ \oplus I_-$, $E_i = W \oplus F_i$, $V_i = E_i \oplus \mathbf{Q}$. Пусть E_i^0 — подгруппа в E_i, образованная такими элементами x, что $x.x \equiv 0 \pmod 2$; эта подгруппа имеет индекс 2 в E_i. Сразу же видно, что имеет место $E_i^0 = W^0 \oplus F_i$, где W^0 — множество таких элементов $x = (x_1, x_2)$ из W, что $x_1 \equiv x_2 \pmod 2$. Пусть E_i^+ — «сопряженный» к E_i^0 в V_i модуль, т. е. множество таких $y \in V_i$, что $x.y \in \mathbf{Z}$ для всех $x \in E_i^0$. Ясно, что $E_i^+ = W^+ \oplus F_i$, где W^+ — множество таких (x_1, x_2), что $2x_1 \in \mathbf{Z}$, $2x_2 \in \mathbf{Z}$, $x_1 - x_2 \in \mathbf{Z}$. Имеем $E_i^0 \subset E_i \subset E_i^+$, и факторгруппа E_i^+/E_i^0 изоморфна факторгруппе W^+/W^0; это группа типа (2, 2). Поэтому существуют три подгруппы, строго содержащиеся между E_i^0 и E_i^+; они соответствуют трем подгруппам порядка 2 группы типа (2, 2). Одна из них есть сама E_i; две другие будем обозначать через E_i' и E_i''. Имеем

$$E_i' = W' \oplus F_i, \quad E_i'' = W'' \oplus F_i,$$

где W' и W'' определяются очевидным образом. Непосредственно проверяется, что W' и W'' изоморфны модулю U (можно, например, в качестве базиса W' взять векторы $a = (1/2, 1/2)$, $b = (1, -1)$; тогда $a.a = b.b = 0$, $a.b = 1$; для W'' возьмем $(1/2, -1/2)$ и $(1, 1)$). Пусть теперь f: $W \oplus F_1 \to W \oplus F_2$ — изоморфизм. Он продолжается до изоморфизма пространства V_1 на V_2; этот изоморфизм отображает E_1 на E_2, а следовательно, E_1^0 на E_2^0 и E_1^+ на E_2^+ по определению этих подгрупп. Поэтому он отображает также (E_1', E_1'') либо на (E_2', E_2''), либо на (E_2'', E_2'). Поскольку модули E_i' и E_i'' изоморфны модулю $U \oplus F_i$, совершенно ясно, что $U \oplus F_1 \simeq U \oplus F_2$.

Доказательство теоремы 5. Сначала докажем, что *если* $E_1, E_2 \in S$ — *неопределенные модули второго типа, имеющие одинаковые ранги и одинаковые индексы, то они изоморфны.* По лемме 5 $E_1 = U \oplus F_1$, $E_2 = U \oplus F_2$; ясно, что F_1 и F_2 — модули второго типа, имеющие одинаковые ранги и одинаковые индексы.

Модули $I_+ \oplus I_- \oplus F_1$ и $I_+ \oplus I_- \oplus F_2$ являются неопределенными модулями первого типа, имеющими одинаковые ранги и одинаковые индексы. По теореме 4 они изоморфны. Тогда, применяя лемму 6, мы видим, что E_1 и E_2 изоморфны, в чем и состоит наше утверждение.

Теперь теорема 5 получается непосредственно: если E — определенный модуль второго типа и если $\tau(E) \geqslant 0$, то определим целые числа p и q по формулам

$$q = \frac{1}{8}\tau(E), \quad p = \frac{1}{2}(r(E) - \tau(E)).$$

Применяя только что полученный результат к модулям E и $pU \oplus q\Gamma_8$, мы видим, что эти модули изоморфны.

Часть вторая

АНАЛИТИЧЕСКИЕ МЕТОДЫ

Глава VI

ТЕОРЕМА ОБ АРИФМЕТИЧЕСКОЙ ПРОГРЕССИИ

Целью этой главы является доказательство следующей теоремы, которую сформулировал (и использовал) Лежандр, а доказал Дирихле.

Теорема. *Пусть a и m — целые числа $\geqslant 1$, взаимно простые между собой. Существует бесконечно много таких простых чисел p, что $p \equiv a \pmod{m}$.*

Мы следуем методу (который является методом самого Дирихле), использующему свойства L-*функции*.

§ 1. Характеры конечных абелевых групп

1.1. *Двойственность*

Пусть G — мультипликативно записанная конечная абелева группа.

Определение 1. *Характером группы* G *называется любой гомоморфизм группы* G *в мультипликативную группу* $\mathbf{C}^*$ *комплексных чисел.*

Характеры группы G образуют группу Hom (G, $\mathbf{C}^*$), которая обозначается $\hat{\mathrm{G}}$ и называется группой, *дуальной* группе G.

Пример. Предположим, что G — *циклическая группа порядка* n с образующей s. Если χ: $\mathrm{G} \to \mathbf{C}^*$ — характер группы G, то элемент $w = \chi(s)$ удовлетворяет уравнению $w^n = 1$, т. е. является корнем n-й

степени из единицы. Обратно, любой корень n-й степени из единицы w определяет характер группы G посредством отображения $s^a \mapsto w^a$. Таким образом, отображение $\chi \mapsto \chi(s)$ есть *изоморфизм группы* $\hat{G}$ *на группу* μ_n *корней* n*-й степени из единицы*; в частности, $\hat{G}$ есть циклическая группа порядка n.

Предложение 1. *Пусть* H — *подгруппа группы* G. *Всякий характер группы* H *может быть продолжен до характера группы* G.

Доказываем индукцией по *индексу* $(G : H)$ подгруппы H в G. Если $(G : H) = 1$, то $H = G$ и доказывать нечего. Если это не так, то пусть x — элемент из G, не принадлежащий подгруппе H, и пусть n — такое наименьшее целое число > 1, что $x^n \in H$. Пусть χ — характер группы H, и пусть $t = \chi(x^n)$. Поскольку $\mathbf{C}^*$ — *бесконечно делимая* группа, можно выбрать такой элемент $w \in \mathbf{C}^*$, что $w^n = t$. Пусть H′ — подгруппа группы G, порожденная подгруппой H и элементом x; любой элемент из H′ записывается в виде $h' = hx^a$, где $a \in \mathbf{Z}$ и $h \in H$. Положим

$$\chi'(h') = \chi(h)\, w^a.$$

Легко проверить, что это число не зависит от разложения hx^a элемента h' и что χ': $H' \to \mathbf{C}^*$ — характер группы H′, продолжающий χ. Так как $(G : H') < (G : H)$, предположение индукции позволяет продолжить χ' до характера всей группы G.

Замечание. Операция *ограничения* определяет гомоморфизм

$$\rho\colon \hat{G} \to \hat{H},$$

и предложение 1 означает, что ρ сюръективен. С другой стороны, ядро гомоморфизма ρ состоит из тех характеров группы G, которые тривиальны на H; поэтому оно изоморфно группе $(G/H)^\wedge$, дуальной группе G/H. Отсюда получаем *точную последовательность*

$$\{1\} \to (G/H)^\wedge \to \hat{G} \to \hat{H} \to \{1\}.$$

Предложение 2. *Группа* $\hat{G}$ *есть конечная абелева группа того же порядка, что и* G.

Доказываем индукцией по порядку n группы G, причем случай $n=1$ тривиален. Если $n\geqslant 2$, то выберем нетривиальную циклическую подгруппу H группы G. На основании приведенного выше замечания порядок группы $\hat{G}$ есть произведение порядков группы $\hat{H}$ и $(G/H)\hat{}$. Но порядок группы H (соответственно группы G/H) равен порядку дуальной ей группы, поскольку H циклична (соответственно поскольку порядок группы G/H строго меньше, чем n). Отсюда заключаем, что порядок группы $\hat{G}$ есть произведение порядков групп H и G/H и поэтому равен порядку группы G.

Замечание. Можно доказать несколько более точный результат: $\hat{G}$ *изоморфна* (вообще говоря, не канонически) группе G. Это показывается разложением группы G в произведение циклических групп.

Если $x\in G$, то отображение $\chi\longmapsto\chi(x)$ есть характер группы $\hat{G}$. Таким образом, мы получаем гомоморфизм $\varepsilon\colon G\to\hat{\hat{G}}$.

Предложение 3. *Гомоморфизм* ε *есть изоморфизм группы* G *на бидуальную ей группу* $\hat{\hat{G}}$.

Так как G и $\hat{\hat{G}}$ имеют один и тот же порядок, то достаточно показать, что ε инъективен, т. е. что если x есть элемент $\neq 1$ из G, то существует такой характер χ группы G, что $\chi(x)\neq 1$. Итак, пусть H — циклическая подгруппа в G, порожденная элементом x. Ясно (см. приведенный выше пример), что существует характер χ группы H, такой, что $\chi(x)\neq 1$; предложение 1 позволяет продолжить χ до характера группы G. Отсюда вытекает искомый результат.

1.2. *Соотношения ортогональности*

Предложение 4. *Пусть* $n=\operatorname{card}(G)$, *и пусть* $\chi\in\hat{G}$. *Тогда*

$$\sum_{x\in G}\chi(x)=\begin{cases} n, & \text{если } \chi=1,\\ 0, & \text{если } \chi\neq 1.\end{cases}$$

Первая формула очевидна. Чтобы доказать вторую, выберем такой $y \in G$, что $\chi(y) \neq 1$. Имеем

$$\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x),$$

откуда

$$(\chi(y) - 1) \sum_{x \in G} \chi(x) = 0.$$

Так как $\chi(y) \neq 1$, то отсюда $\sum_{x \in G} \chi(x) = 0$.

Следствие. *Пусть* $x \in G$. *Тогда*

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n, & \text{если } x = 1, \\ 0, & \text{если } x \neq 1. \end{cases}$$

Это вытекает из предложения 4, примененного к группе $\hat{G}$.

Замечание. Приведенные результаты являются частными случаями «соотношений ортогональности» из теории характеров конечных групп (не обязательно абелевых).

1.3. *Модулярные характеры*

Пусть m — целое число $\geqslant 1$. Обозначим через $G(m)$ мультипликативную группу $(\mathbf{Z}/m\mathbf{Z})^*$ обратимых элементов кольца $\mathbf{Z}/m\mathbf{Z}$. Это — конечная абелева группа порядка $\varphi(m)$, где $\varphi(m)$ — функция Эйлера, см. п. 1.2 гл. I. Элемент χ из группы, дуальной группе $G(m)$, называется *характером по модулю* m; его можно рассматривать как функцию, определенную на множестве взаимно простых с m целых чисел, имеющую значения в $\mathbf{C}^*$ и удовлетворяющую соотношению $\chi(ab) = \chi(a)\chi(b)$; удобно продолжить эту функцию на множество $\mathbf{Z}$ всех целых чисел, полагая $\chi(a) = 0$, если a не взаимно просто с m.

Примеры.

1) $m = 4$; группа $G(4)$ состоит из двух элементов и, следовательно, имеет единственный нетривиальный характер, которым является $x \longmapsto (-1)^{\varepsilon(x)}$; см. п. 3.2 гл. I.

2) $m=8$; группа $G(8)$ состоит из четырех элементов. Она имеет три нетривиальных характера, которыми являются

$$x \mapsto (-1)^{\varepsilon(x)}, \quad (-1)^{\omega(x)}, \quad (-1)^{\varepsilon(x)+\omega(x)},$$

см. п. 3.2 гл. I.

3) $m=p$, где p — простое число $\neq 2$. Группа $G(p)$ — циклическая порядка $p-1$; следовательно, она имеет единственный характер порядка 2 — характер Лежандра $x \mapsto \left(\frac{x}{p}\right)$.

4) $m=7$. Группа $G(7)$ — циклическая порядка 6; следовательно, она имеет два характера порядка 3, которые комплексно сопряжены. Один из них задается посредством

$$\chi(x)=\begin{cases} 1, & \text{если } x \equiv \pm 1 \pmod 7, \\ e^{2\pi i/3}, & \text{если } x \equiv \pm 2 \pmod 7, \\ e^{4\pi i/3}, & \text{если } x \equiv \pm 3 \pmod 7. \end{cases}$$

Характеры порядка 2 тесно связаны с характерами Лежандра. Более точно:

Предложение 5. *Пусть a — отличное от нуля целое число, не делящееся на квадраты* (см. п. 3.2 гл. IV), *и пусть $m=4|a|$. Тогда существует такой характер χ_a по модулю m, что $\chi_a(p)=\left(\frac{a}{p}\right)$ для любого простого числа p, не делящего m. Характер с такими свойствами единственный. При этом $\chi_a^2=1$ и $\chi_a \neq 1$, если $a \neq 1$.*

Единственность характера χ_a очевидна, поскольку любое взаимно простое с m целое число является произведением простых чисел, не делящих числа m; ясно также, что $\chi_a^2=1$.

Для доказательства существования характера χ_a предположим сначала, что a имеет вид $l_1 \dots l_k$, где l_i — различные простые числа, отличные от 2. В качестве χ_a возьмем характер

$$\chi_a(x)=(-1)^{\varepsilon(x)\varepsilon(a)}\left(\frac{x}{l_1}\right)\dots\left(\frac{x}{l_k}\right).$$

Если p — простое число, отличное от 2 и от l_i, то квадратичный закон взаимности показывает, что

$$\chi_a(p) = \left(\frac{l_1}{p}\right) \dots \left(\frac{l_k}{p}\right) = \left(\frac{a}{p}\right),$$

и, стало быть, χ_a отвечает требуемому условию.

В случае, когда a имеет вид $-b$ (или $2b$, или $-2b$), где $b = l_1 \dots l_k$ в смысле, указанном выше, мы возьмем в качестве χ_a произведение характера χ_b на характер $(-1)^{\varepsilon(x)}$ (или на $(-1)^{\omega(x)}$, или на $(-1)^{\varepsilon(x)+\omega(x)}$). Это явное построение характера χ_a в то же время показывает, что $\chi_a \neq 1$, если $a \neq 1$.

Замечание. Можно доказать, что если x — целое число > 0, взаимно простое с m, то

$$\chi_a(x) = \prod_{l \mid m} (a, x)_l = \prod_{(l, m)=1} (a, x)_l,$$

где $(a, x)_l$ обозначает символ Гильберта чисел a и x в поле $\mathbf{Q}_l$. Впрочем, можно было бы использовать эту формулу для определения χ_a.

§ 2. Ряды Дирихле

2.1. *Леммы*

Лемма 1. *Пусть* U — *открытое подмножество множества* **C**, *и пусть* f_n — *последовательность функций, голоморфных на* U, *которая равномерно сходится на любом компакте к функции* f. *Тогда функция* f *голоморфна на* U, *а производные* f'_n *функций* f_n *равномерно сходятся на любом компакте к производной* f' *функции* f.

Напомним вкратце доказательство.

Пусть D — замкнутый круг, содержащийся в U, и пусть C — его граница, ориентированная обычным образом. По формуле Коши

$$f_n(z_0) = \frac{1}{2i\pi} \int_C \frac{f_n(z)}{z - z_0}\, dz$$

для любой точки z_0, внутренней для D. Переходя к пределу, отсюда получаем

$$f(z_0)=\frac{1}{2i\pi}\int\limits_C \frac{f(z)}{z-z_0}dz,$$

а это и показывает, что f голоморфна внутри D, т. е. мы доказали первую часть леммы. Вторая доказывается таким же способом с использованием формулы

$$f'(z_0)=-\frac{1}{2i\pi}\int\limits_C \frac{f(z)}{(z-z_0)^2}dz.$$

Лемма 2 (лемма Абеля). *Пусть* (a_n) *и* (b_n) — *две последовательности. Положим*

$$A_{m,\,p}=\sum_{n=m}^{n=p} a_n \quad \text{и} \quad S_{m,\,m'}=\sum_{n=m}^{n=m'} a_n b_n;$$

тогда

$$S_{m,\,m'}=\sum_{n=m}^{n=m'-1} A_{m,\,n}(b_n-b_{n+1})+A_{m,\,m'}b_{m'}.$$

Доказательство. Заменим a_n на $A_{m,\,n}-A_{m,\,n-1}$ и перегруппируем члены.

Лемма 3. *Пусть* α *и* β — *вещественные числа, причем* $0<\alpha<\beta$. *Пусть* $z=x+iy$, *где* $x,\ y\in\mathbf{R}$ *и* $x>0$. *Тогда*

$$|e^{-\alpha z}-e^{-\beta z}|\leqslant\left|\frac{z}{x}\right|(e^{-\alpha x}-e^{-\beta x}).$$

Доказательство. Запишем

$$e^{-\alpha z}-e^{-\beta z}=-z\int\limits_\alpha^\beta e^{-tz}\,dt;$$

отсюда, переходя к абсолютным величинам, получаем

$$|e^{-\alpha z}-e^{-\beta z}|\leqslant|z|\int\limits_\alpha^\beta e^{-tx}\,dt=\frac{|z|}{x}(e^{-\alpha x}-e^{-\beta x}).$$

2.2. *Ряды Дирихле*

Зададим строго возрастающую последовательность (λ_n) вещественных чисел, стремящуюся к $+\infty$. Для упрощения мы предположим, что все λ_n положительны (это предположение несущественно, так как всегда можно вернуться к общему случаю, добавляя конечное число членов рассматриваемого ряда).

Мы назовем *рядом Дирихле с показателями* (λ_n) ряд вида

$$\sum a_n e^{-\lambda_n z} \quad (a_n \in \mathbf{C},\ z \in \mathbf{C}).$$

Примеры

a) $\lambda_n = \log n$ (ряд Дирихле в собственном смысле). Тогда ряд запишется в виде $\sum a_n/n^z$, см. п. 2.4.

b) $\lambda_n = n$. Полагая $t = e^{-z}$, мы придем к целым относительно t рядам.

Замечание. Понятие ряда Дирихле является частным случаем понятия преобразования Лапласа с мерой μ. Так называют функцию

$$\int_0^\infty e^{-zt}\mu(t)\,dt.$$

Рассматриваемый случай является таким случаем, в котором μ — дискретная мера. (Для более детального ознакомления см., например, Widder D., The Laplace Transform, Princeton Univ. Press, 1946.)

Предложение 6. *Если ряд* $f(z) = \sum a_n e^{-\lambda_n z}$ *сходится при* $z = z_0$, *то он равномерно сходится во всей области вида* $\mathrm{R}(z - z_0) \geqslant 0$, $|\mathrm{Arg}(z - z_0)| \leqslant \alpha$, *где* $\alpha < \pi/2$.

(Здесь и везде в дальнейшем через $\mathrm{R}(z)$ обозначается *вещественная часть* комплексного числа z.)

Производя, если это необходимо, замену переменной z, мы можем предполагать, что $z_0 = 0$. Наше условие тогда означает, что ряд $\sum a_n$ сходится. Нам надо доказать, что имеет место равномерная сходи-

мость в области вида $\mathrm{R}(z) \geqslant 0$, $|z|/\mathrm{R}(z) \leqslant k$. Пусть $\varepsilon > 0$. Поскольку ряд $\sum a_n$ сходится, существует такое число N, что если $m, m' \geqslant \mathrm{N}$, то $|\mathrm{A}_{m,m'}| \leqslant \varepsilon$ (обозначения те же, что и в лемме 2). Применяя лемму, положив $b_n = e^{-\lambda_n z}$, получаем

$$\mathrm{S}_{m,m'} = \sum_{m}^{m'-1} \mathrm{A}_{m,n}\left(e^{-\lambda_n z} - e^{-\lambda_{n+1} z}\right) + A_{m,m'} e^{-\lambda_{m'} z}.$$

Полагая $z = x + iy$ и применяя лемму 3, находим (для $m, m' \geqslant \mathrm{N}$)

$$|\mathrm{S}_{m,m'}| \leqslant \varepsilon\left(1 + \frac{|z|}{x}\sum_{m}^{m'-1}\left(e^{-\lambda_n x} - e^{-\lambda_{n+1} x}\right)\right),$$

или

$$|\mathrm{S}_{m,m'}| \leqslant \varepsilon\left(1 + k\left(e^{-\lambda_m x} - e^{-\lambda_{m'} x}\right)\right),$$

откуда

$$|\mathrm{S}_{m,m'}| \leqslant \varepsilon(1 + k),$$

и равномерная сходимость очевидна.

Следствие 1. *Если ряд f сходится для $z = z_0$, то он сходится для $\mathrm{R}(z) > \mathrm{R}(z_0)$, и так определенная функция голоморфна.*

Это вытекает из предложения 6 и из леммы 1.

Следствие 2. *Область сходимости ряда f представляет собой максимальную открытую полуплоскость* (называемую *полуплоскостью сходимости*).

(Допуская вольность языка, рассматривают $\varnothing$ и $\mathbf{C}$ как открытые полуплоскости.)

Если полуплоскость сходимости задается неравенством $\mathrm{R}(z) > \rho$, то ρ называют *абсциссой сходимости* рассматриваемого ряда.

(Случаям $\varnothing$ и $\mathbf{C}$ отвечают соответственно $\rho = +\infty$ и $\rho = -\infty$.)

Полуплоскость сходимости ряда $\sum |a_n| e^{-\lambda_n z}$ называется (по понятным соображениям) *полуплоскостью абсолютной сходимости* ряда f; абсцисса его сходимости обозначается через ρ^+. Если $\lambda_n = n$ (случай целых рядов), то, как известно, $\rho = \rho^+$. Однако, вообще говоря, это не имеет места.

Например, один из наиболее простых L-рядов

$$L(z) = 1 - 1/3^z + 1/5^z - 1/7^z + \ldots$$

соответствует случаю $\rho = 0$ и $\rho^+ = 1$, как мы увидим дальше.

Следствие 3. *$f(z)$ сходится к $f(z_0)$, когда $z \to z_0$, оставаясь в области $\mathrm{R}(z - z_0) \geqslant 0$, $|\operatorname{Arg}(z - z_0)| \leqslant \alpha$, где $\alpha < \pi/2$.*

Это следует из равномерной сходимости и из того, что $e^{-\lambda_n z}$ стремится к $e^{-\lambda_n z_0}$.

Следствие 4. *Функция f может быть тождественно равной нулю только в том случае, когда все коэффициенты a_n равны нулю.*

Покажем, что a_0 есть нуль. Умножим f на $e^{\lambda_0 z}$ и устремим z к $+\infty$ (например, вдоль вещественной оси). Равномерная сходимость обеспечит тогда, что $e^{\lambda_0 z} f$ стремится к a_0; отсюда $a_0 = 0$. Проделаем то же самое с a_1 и т. д.

2.3. *Ряды Дирихле с положительными коэффициентами*

Предложение 7. *Пусть $f = \sum a_n e^{-\lambda_n z}$ — ряд Дирихле, коэффициенты a_n которого являются вещественными числами $\geqslant 0$. Предположим, что f сходится для $\mathrm{R}(z) > \rho$, где $\rho \in \mathbf{R}$, и что функция f может быть аналитически продолжена до функции, голоморфной в окрестности точки $z = \rho$. Тогда существует такое $\varepsilon > 0$, что f сходится для $\mathrm{R}(z) > \rho - \varepsilon$.*

(Иначе говоря: область сходимости ряда f ограничивается *особенностью* функции f, расположенной на вещественной оси.)

Доказательство. Допуская замену z на $z - \rho$, мы можем предположить, что $\rho = 0$. Так как f голоморфна одновременно и для $\mathrm{R}(z) > 0$ и в окрестности точки 0, то она голоморфна в круге $|z - 1| \leqslant 1 + \varepsilon$, где $\varepsilon > 0$. В частности, в этом круге сходится ряд Тейлора. Таким образом, на основании леммы 1 p-я

производная функции f задается формулой

$$f^{(p)}(z) = \sum_n a_n (-\lambda_n)^p e^{-\lambda_n z} \quad \text{для} \quad R(z) > 0;$$

отсюда

$$f^{(p)}(1) = (-1)^p \sum_n (\lambda_n)^p a_n e^{-\lambda_n}.$$

Ряд Тейлора в рассматриваемом случае записывается так:

$$f(z) = \sum_{p=0}^{\infty} \frac{1}{p!} (z-1)^p f^{(p)}(1), \quad |z-1| \leqslant 1+\varepsilon.$$

В частности, для $z = -\varepsilon$ имеем

$$f(-\varepsilon) = \sum_{p=0}^{\infty} \frac{1}{p!} (1+\varepsilon)^p (-1)^p f^{(p)}(1),$$

причем этот ряд сходится.

Но $(-1)^p f^{(p)}(1) = \sum_n \lambda_n^p a_n e^{-\lambda_n}$ — сходящийся ряд с членами $\geqslant 0$. Следовательно, двойной ряд с положительными членами

$$f(-\varepsilon) = \sum_{p,n} a_n \frac{1}{p!} (1+\varepsilon)^p \lambda_n^p e^{-\lambda_n}$$

сходится. Перегруппировывая члены этого ряда, получаем

$$f(-\varepsilon) = \sum_n a_n e^{-\lambda_n} \sum_{p=0}^{\infty} \frac{1}{p!} (1+\varepsilon)^p \lambda_n^p =$$

$$= \sum_n a_n e^{-\lambda_n} e^{\lambda_n (1+\varepsilon)} = \sum_n a_n e^{\lambda_n \varepsilon},$$

так что данный ряд Дирихле сходится для $z = -\varepsilon$, а следовательно, и для $R(z) > -\varepsilon$. Ч. т. д.

2.4. *Ряды Дирихле в собственном смысле*

В этом случае $\lambda_n = \log n$. Соответствующие ряды записываются так:

$$f(s) = \sum_{n=1}^{\infty} a_n / n^s,$$

при этом буква s здесь традиционна для обозначения переменной.

Предложение 8. *Если a_n ограничены, то ряд абсолютно сходится для* $\mathrm{R}(s) > 1$.

Это следует из общеизвестной сходимости ряда $\sum_{n=1}^{\infty} 1/n^{\alpha}$ для $\alpha > 1$.

Предложение 9. *Если частные суммы* $\mathrm{A}_{m,p} = \sum_{m}^{p} a_n$ *ограничены, то ряд сходится (не обязательно абсолютно) для* $\mathrm{R}(s) > 0$.

Предположим, что $|\mathrm{A}_{m,p}| \leqslant \mathrm{K}$. Применяя лемму Абеля (лемма 2), находим, что

$$|\mathrm{S}_{m,m'}| \leqslant \mathrm{K}\left(\sum_{m}^{m'-1} \left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| + \left|\frac{1}{m'^s}\right|\right).$$

Можно предположить, что s вещественно (в силу предложения 6). Это позволяет записать предыдущее неравенство в более простой форме

$$|\mathrm{S}_{m,m'}| \leqslant \mathrm{K}/m^s,$$

и сходимость очевидна.

§ 3. Дзета-функция и L-функции

3.1. *Эйлеровское произведение*

Определение 2. *Функция* $f\colon \mathbf{N} \to \mathbf{C}$ *называется мультипликативной, если*

$$f(nm) = f(n)f(m)$$

каждый раз, когда n и m взаимно просты.

Примеры. Функция Эйлера (п. 1.2 гл. I), *функция Рамануджана* (п. 4.5 гл. VII) являются мультипликативными функциями.

Пусть f — мультипликативная и ограниченная функция.

Лемма 4. *Ряд Дирихле* $\sum_{n=1}^{\infty} f(n)/n^s$ *абсолютно сходится для* $\mathrm{R}(s) > 1$, *а его сумма в этой области равна сходящемуся бесконечному произведению*

$$\prod_{p \in \mathrm{P}} (1 + f(p)\, p^{-s} + \ldots + f(p^m)\, p^{-ms} + \ldots).$$

(Здесь и в дальнейшем через P обозначается множество простых чисел.)

Абсолютная сходимость ряда вытекает из ограниченности функции f (см. предложение 8). Пусть S — конечное множество простых чисел, и пусть $\mathbf{N}(\mathrm{S})$ — множество целых чисел $\geqslant 1$, все простые делители которых принадлежат множеству S.

Непосредственно ясно следующее равенство:

$$\sum_{n \in \mathbf{N}(\mathrm{S})} f(n)/n^s = \prod_{p \in \mathrm{S}} \left(\sum_{m=0}^{\infty} f(p^m)\, p^{-ms} \right).$$

Когда S растет, левая часть равенства стремится к $\sum_{n=1}^{\infty} f(n)/n^s$. Отсюда вытекает, что бесконечное произведение сходится и что его значение действительно равно $\sum f(n)/n^s$.

Лемма 5. *Если* f *мультипликативна в строгом смысле* (*т. е. если* $f(nn') = f(n) f(n')$ *для любой пары* $n,\ n' \in \mathbf{N}$), *то*

$$\sum_{n=1}^{\infty} f(n)/n^s = \prod_{p \in \mathrm{P}} \frac{1}{1 - f(p)/p^s}.$$

Это вытекает из предыдущей леммы в сочетании с тождеством $f(p^m) = f(p)^m$.

3.2. *Дзета-функция*

Применим предыдущий пункт к $f = 1$. Мы получаем функцию

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathrm{P}} \frac{1}{1 - 1/p^s};$$

эта формула имеет смысл для $\mathrm{R}(s) > 1$.

Предложение 10. a) *Функция* ζ *голоморфна и* $\neq 0$ *в полуплоскости* $\mathrm{R}(s) > 1$.

b) *Имеет место*

$$\zeta(s) = \frac{1}{s-1} + \varphi(s),$$

где $\varphi(s)$ *голоморфна для* $\mathrm{R}(s) > 0$.

Утверждение a) очевидно. Для b) заметим, что

$$\frac{1}{s-1} = \int_1^\infty t^{-s}\,dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s}\,dt.$$

Можно, следовательно, записать:

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \int_n^{n+1} t^{-s}\,dt \right) =$$

$$= \frac{1}{s-1} + \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s})\,dt.$$

Положим

$$\varphi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s})\,dt \quad \text{и} \quad \varphi(s) = \sum_{n=1}^{\infty} \varphi_n(s).$$

Нам остается проверить, что $\varphi(s)$ определена и голоморфна для $\mathrm{R}(s) > 0$. Но ясно, что каждая $\varphi_n(s)$ удовлетворяет этому условию; таким образом, достаточно доказать, что ряд $\sum \varphi_n$ равномерно сходится на любом компакте при $\mathrm{R}(s) > 0$. Имеем

$$|\varphi_n(s)| \leqslant \sup_{n \leqslant t \leqslant n+1} |n^{-s} - t^{-s}|.$$

Но производная функции $n^{-s} - t^{-s}$ равна s/t^{s+1}. Отсюда

$$|\varphi_n(s)| \leqslant \frac{|s|}{n^{x+1}}, \text{ где } x = \mathrm{R}(s),$$

и мы действительно получаем ряд, который равномерно сходится для $\mathrm{R}(s) \geqslant \varepsilon$, каково бы ни было $\varepsilon > 0$.

Следствие 1. *Дзета-функция имеет простой полюс в точке* $s=1$.

Это ясно.

Следствие 2. *При* $s\to 1$

$$\sum_{p} p^{-s}\sim \log 1/(s-1),$$

тогда как $\sum\limits_{p,\ k\geqslant 2} 1/p^{ks}$ *остается ограниченной.*

Мы имеем

$$\log\zeta(s)=\sum_{\substack{p\in P\\ k\geqslant 1}} 1/k\cdot p^{ks}=\sum_{p\in P} 1/p^{s}+\psi(s),$$

где $\psi(s)=\sum\limits_{p\in P}\sum\limits_{k\geqslant 2} 1/k\cdot p^{ks}$. Ряд ψ мажорируется рядом

$$\sum 1/p^{ks}=\sum 1/p^{s}(p^{s}-1)\leqslant \sum 1/p(p-1)\leqslant$$
$$\leqslant\sum_{n=2}^{\infty} 1/n(n-1)=1.$$

Отсюда заключаем, что ψ остается ограниченной, и так как по следствию 1 $\log\zeta(s)\sim\log 1/(s-1)$, следствие 2 доказано.

Замечание. Хотя это и не используется в дальнейшем, отметим, что $\zeta(s)$ аналитически продолжается до мероморфной функции на всю комплексную плоскость с единственным полюсом $s=1$. Функция

$$\xi(s)=\pi^{-s/2}\Gamma(s/2)\zeta(s)$$

удовлетворяет *функциональному уравнению* $\xi(s)=\xi(1-s)$. При этом дзета-функция принимает *рациональные* значения на отрицательных целых числах:

$$\zeta(-2n)=0, \qquad \text{если } n>0,$$
$$\zeta(1-2n)=(-1)^{n}B_{n}/2n, \qquad \text{если } n>0;$$

здесь B_n обозначает n-е число Бернулли (см. п. 4.1 гл. VII).

Предполагается (гипотеза Римана), что *остальные нули функции* ζ *находятся на прямой* $R(s)=1/2$; это численно проверено для очень большого их числа (более трех миллионов).

3.3. L-*функции*

Пусть m — целое число $\geqslant 1$, и пусть χ — характер mod m (см. п. 3.1). L-*функция* по этому характеру определяется рядом Дирихле

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)/n^s.$$

Заметим, что в этой сумме можно ограничиться лишь теми целыми числами n, которые *взаимно просты с* m, ибо остальные соответствуют нулевому значению характера χ.

Случай единичного характера не дает ничего существенно нового.

Предложение 11. *Для* $\chi = 1$ *имеет место*

$$L(s, 1) = F(s)\zeta(s), \quad \textit{где} \quad F(s) = \prod_{p \mid m} (1 - p^{-s}).$$

В частности, $L(s, 1)$ *аналитически продолжима для* $R(s) > 0$ *и имеет простой полюс в точке* $s = 1$.

Проверяется непосредственно.

Предложение 12. *Для* $\chi \neq 1$ *ряд* $L(s, \chi)$ *сходится (соответственно абсолютно сходится) в полуплоскости* $R(s) > 0$ (*соответственно* $R(s) > 1$). *Имеет место равенство*

$$L(s, \chi) = \prod_{p \in P} \frac{1}{1 - \chi(p)/p^s} \quad \textit{для} \quad R(s) > 1.$$

Утверждение, касающееся $R(s) > 1$, следует из того, что было сказано в п. 3.1. Остается показать сходимость ряда для $R(s) > 0$. В силу предложения 9 достаточно проверить, что сумма

$$A_{u, v} = \sum_{u}^{v} \chi(n), \quad u \leqslant v$$

ограничена. Но по предложению 4

$$\sum_{u}^{u+m-1} \chi(n) = 0.$$

Отсюда заключаем, что достаточно мажорировать суммы $A_{u, v}$ для $v - u < m$, а это делается непосред-

ственно:

$$|A_{u,v}| \leqslant \varphi(m),$$

что и доказывает предложение.

Замечание. В частности, $L(1, \chi)$ *конечна*, когда $\chi \neq 1$. *Существенным моментом* в доказательстве Дирихле является проверка того, что $L(1, \chi)$ *отлична от нуля*. Это является предметом следующего пункта.

3.4. *Произведение* L-*функций, относящихся к одному и тому же целому числу* m

В этом пункте m предполагается фиксированным целым числом $\geqslant 1$. Если p не делит m, то обозначим через $\bar{p}$ его образ в $G(m) = (\mathbf{Z}/m\mathbf{Z})^*$ и через $f(p)$ порядок элемента $\bar{p}$ в группе $G(m)$. По определению $f(p)$ есть наименьшее целое число $f \geqslant 1$, для которого $p^f \equiv 1 \pmod{m}$. Пусть

$$g(p) = \varphi(m)/f(p);$$

это порядок факторгруппы группы $G(m)$ по подгруппе $(\bar{p})$, порожденной элементом $\bar{p}$.

Лемма 6. *Если* $p \nmid m$, *то*

$$\prod (1 - \chi(p)T) = (1 - T^{f(p)})^{g(p)};$$

при этом произведение берется по всем характерам χ *группы* $G(m)$.

Пусть W — множество корней $f(p)$-й степени из единицы. Имеем тождество

$$\prod_{w \in W} (1 - wT) = 1 - T^{f(p)}.$$

Отсюда следует лемма 6, если учесть, что для любого $w \in W$ существует $g(p)$ характеров χ группы $G(m)$, таких, что $\chi(\bar{p}) = w$.

Определим новую функцию $\zeta_m(s)$ формулой

$$\zeta_m(s) = \prod_{\chi} L(s, \chi),$$

где произведение берется по всем характерам χ группы $G(m)$.

Предложение 13. *Имеет место равенство*

$$\zeta_m(s) = \prod_{p \nmid m} \frac{1}{\left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}}.$$

Это — ряд Дирихле с целыми коэффициентами $\geqslant 0$, *сходящийся в полуплоскости* $R(s) > 1$.

Заменяя каждую L-функцию ее разложением в произведение и применяя лемму 6 (при $T = p^{-s}$), получаем разложение в произведение для $\zeta_m(s)$. Это разложение делает очевидным то, что мы имеем дело с рядом, имеющим целые коэффициенты $\geqslant 0$; его сходимость для $R(s) > 1$ видна непосредственно.

Теорема 1. a) ζ_m *имеет простой полюс в точке* $s = 1$.

b) $L(1, \chi) \neq 0$ *для любого* $\chi \neq 1$.

Если $L(1, \chi) \neq 0$ для любого $\chi \neq 1$, то из того, что $L(s, 1)$ имеет в точке $s = 1$ простой полюс, это же вытекает и для ζ_m. Таким образом, b) $\Rightarrow$ a). Предположим теперь, что $L(1, \chi) = 0$ для некоторого $\chi \neq 1$. Функция ζ_m была бы тогда голоморфной в точке $s = 1$, а следовательно, и при всех s таких, что $R(s) > 0$ (см. предложения 11 и 12). Так как эта функция является рядом Дирихле с положительными коэффициентами, то этот ряд сходился бы при всех s из той же области (см. предложение 7). Но это невозможно. Действительно, p-й сомножитель в ζ_m равен

$$\frac{1}{(1 - p^{-f(p)s})^{g(p)}} = (1 + p^{-f(p)s} + p^{-2f(p)s} + \ldots)^{g(p)}$$

и превосходит ряд

$$1 + p^{-\varphi(m)s} + p^{-2\varphi(m)s} + \ldots.$$

Поэтому коэффициенты ряда для ζ_m больше, чем соответствующие коэффициенты ряда

$$\sum_{(n, m)=1} n^{-\varphi(m)s},$$

который, очевидно, расходится при $s = 1/\varphi(m)$. Отсюда следует искомый результат.

Замечание. Функция ζ_m равна (с точностью до конечного числа сомножителей) дзета-функции поля корней m-й степени из единицы. Тот факт, что ζ_m имеет простой полюс в точке $s=1$, может быть, следовательно, также получен из общих результатов, относящихся к дзета-функциям полей алгебраических чисел.

§ 4. Плотность и теорема Дирихле

4.1. *Плотность*

Пусть P — множество простых чисел. Мы видели (следствие 2 предложения 10), что когда s стремится к 1 (причем можно для определенности считать s вещественным числом >1), имеет место

$$\sum_{p\in \mathrm{P}} \frac{1}{p^s} \sim \log \frac{1}{s-1}.$$

Пусть A — часть множества P. Будем говорить, что вещественное число k есть *плотность* множества A, если отношение

$$\left(\sum_{p\in \mathrm{A}} \frac{1}{p^s}\right) \Big/ \left(\log \frac{1}{s-1}\right)$$

стремится к k при $s\to 1$. (Разумеется, необходимо, чтобы $0\leqslant k\leqslant 1$.) Теорема об арифметической прогрессии может быть уточнена следующим образом:

Теорема 2. *Пусть* $m\geqslant 1$, *и пусть* a *таково, что* $(a, m)=1$. *Пусть* P_a — *множество простых чисел* p, *таких, что* $p\equiv a \pmod m$. *Тогда плотность множества* P_a *равна* $1/\varphi(m)$.

(Иными словами, простые числа «равномерно распределены» между различными взаимно простыми с m классами по модулю m.)

Следствие. *Множество* P_a *бесконечно.*

Действительно, конечное множество имеет нулевую плотность.

4.2. *Леммы*

Пусть χ — характер группы $G(m)$. Положим

$$f_\chi(s) = \sum_{p \nmid m} \chi(p)/p^s;$$

этот ряд сходится при $s > 1$.

Лемма 7. *Если* $\chi = 1$, *то* $f_\chi \sim \log(1/(s-1))$ *при* $s \to 1$.

Действительно, f отличается от ряда $\sum 1/p^s$ лишь конечным числом членов.

Лемма 8. *Если* $\chi \neq 1$, *то при* $s \to 1$ *функция* f_χ *ограничена.*

Сейчас мы воспользуемся логарифмом функции $L(s, \chi)$. Нужно несколько уточнить, что под этим понимается (исходя из того, что log не является функцией в собственном смысле этого слова):

$L(s, \chi)$ определяется произведением $\prod 1/(1-\chi(p)/p^s)$. При $R(s) > 1$ каждый сомножитель имеет вид $1/(1-\alpha)$, где $|\alpha| < 1$. Мы определим $\log(1/(1-\alpha))$ как $\sum_{n=1}^{\infty} \alpha^n/n$ («главное» значение логарифма) и определим $\log L(s, \chi)$ рядом (очевидно, сходящимся)

$$\log L(s, \chi) = \sum \log \frac{1}{1-\chi(p)\,p^{-s}} = \sum_{n,\,p} \chi(p)^n/np^{sn}$$
$$(R(s) > 1).$$

(Другое эквивалентное определение: берем ту «ветвь» $\log L(s, \chi)$ при $R(s) > 1$, которая стремится к нулю, когда $s \to \infty$ вдоль вещественной оси.)

Можно разложить $\log L(s, \chi)$ на две части:

$$\log L(s, \chi) = f_\chi(s) + F_\chi(s),$$

где

$$F_\chi(s) = \sum_{p,\ n \geqslant 2} \chi(p)^n/np^{ns}.$$

Теорема 1 совместно со следствием 2 предложения 10 показывает, что $\log L(s, \chi)$ и $F_\chi(s)$ остаются ограниченными, когда $s \to 1$. Поэтому то же самое верно и для $f_\chi(s)$, что доказывает лемму.

4.3. *Доказательство теоремы* 2

Изучим поведение функции

$$g_a(s) = \sum_{p \in P_a} 1/p^s$$

при $s \to 1$.

Лемма 9. *Имеет место равенство*

$$g_a(s) = \frac{1}{\varphi(m)} \sum_{\chi} \chi(a)^{-1} f_\chi(s),$$

где суммирование распространено на все характеры χ *группы* $G(m)$.

Запишем функцию $\sum \chi(a)^{-1} f_\chi(s)$, заменив f_χ по ее определению:

$$\sum_{p \nmid m} \left(\sum_{\chi} \chi(a^{-1}) \chi(p) \right) \Big/ p^s.$$

Но $\chi(a^{-1})\chi(p) = \chi(a^{-1}p)$. На основании следствия предложения 4 имеем

$$\sum_{\chi} \chi(a^{-1}p) = \begin{cases} \varphi(m), & \text{если } a^{-1}p \equiv 1 \pmod m, \\ 0 & \text{в противном случае.} \end{cases}$$

Так что мы нашли как раз функцию $\varphi(m)\, g_a(s)$.

Теорема 2 теперь очевидна. В самом деле, лемма 7 показывает, что $f_\chi(s) \sim \log(1/(1-s))$ для $\chi = 1$, а лемма 8 показывает, что остальные f_χ остаются ограниченными. Учитывая лемму 9, отсюда выводим, что

$$g_a(s) \sim \frac{1}{\varphi(m)} \log \frac{1}{s-1},$$

а это и означает, что плотность множества P_a есть $1/\varphi(m)$.

4.4. *Приложения*

Предложение 14. *Пусть* a *— целое число, не являющееся квадратом. Тогда плотность множества простых чисел* p, *для которых* $\left(\frac{a}{p}\right) = 1$, *равна* $1/2$.

Можно предположить, что a не делится на квадраты. Пусть $m = 4|a|$, пусть χ_a — характер $(\mathrm{mod}\, m)$, определенный в предложении 5 из п. 1.3, и пусть $H \subset G(m)$ — ядро характера χ_a в $G(m)$. Если p — простое число, не делящее m, то пусть $\bar{p}$ — его образ в $G(m)$. Мы имеем $\left(\frac{a}{p}\right) = 1$ тогда и только тогда, когда $\bar{p}$ принадлежит ядру H. Поэтому по теореме 3 плотность множества простых чисел, удовлетворяющих этому условию, есть число, обратное индексу подгруппы H в $G(m)$, т. е. $1/2$.

Следствие. *Пусть a — целое число. Если уравнение $X^2 - a = 0$ имеет решение по модулю p почти для каждого $p \in P$, то оно имеет решение в* $\mathbf{Z}$.

Замечание. Имеются аналогичные результаты для других типов уравнений. Приведем примеры.

i) Пусть $f(X) = a_0X^n + \ldots + a_n$ — полином степени n с целыми коэффициентами, неприводимый над $\mathbf{Q}$. Пусть K — поле, порожденное корнями полинома f (в некотором алгебраически замкнутом расширении поля $\mathbf{Q}$), и пусть $N = [K : \mathbf{Q}]$; имеем $N \geqslant n$. Пусть P_f — множество таких простых чисел p, что f «полностью раскладывается по модулю p», т. е. таких p, для которых все корни полинома $f(\mathrm{mod}\, p)$ принадлежат полю $\mathbf{F}_p$. Можно доказать, что *плотность множества* P_f *есть* $1/N$. (Метод теоремы Дирихле — используется тот факт, что дзета-функция поля K имеет простой полюс в точке $s = 1$.) Можно также найти плотность множества P_f' таких p, для которых редукция полинома $f(\mathrm{mod}\, p)$ имеет по крайней мере один корень в $\mathbf{F}_p$; это число имеет вид q/N, где $1 \leqslant q \leqslant N$ (начиная с тривиального случая при $n = 1$).

ii) В более общей ситуации пусть $\{f_\alpha(X_1, \ldots, X_n)\}$ — семейство полиномов с целыми коэффициентами, и пусть Q — множество таких $p \in P$, для которых редукции полиномов $f_\alpha(\mathrm{mod}\, p)$ имеют общий нуль в $(\mathbf{F}_p)^n$. Можно показать (см. Ax J., *Ann. of Math.*, **85** (1967), 161—183), что Q имеет плотность; более того, эта плотность есть рациональное число, равное нулю только тогда, когда Q конечно.

4.5. *Натуральная плотность*

Понятие плотности, используемое в этом параграфе, есть понятие «аналитическое» (или плотность «по Дирихле»). Несмотря на достаточную сложность этого понятия, оно удобно в применениях.

Имеется другое понятие, понятие «натуральной» плотности: подмножество A множества P имеет в качестве натуральной плотности число k, если отношение

$$\frac{\text{Число элементов из A, которые} \leqslant n}{\text{Число элементов из P, которые} \leqslant n}$$

стремится к k при $n \to \infty$.

Можно показать, что если A имеет натуральную плотность k, то аналитическая плотность множества A существует и равна k. Наоборот, существуют множества, имеющие аналитическую плотность, но не имеющие натуральной плотности. Таким, например, является множество P^1 простых чисел, первая цифра которых (в десятичной системе) равна 1: легко видеть, используя теорему о простых числах, что P^1 не имеет натуральной плотности, но, с другой стороны, Бомбьери сообщил мне доказательство того, что аналитическая плотность множества P^1 существует (она равна $\log_{10} 2 = 0{,}3010300\ldots$).

Однако этой «патологии» не происходит с множествами простых чисел, рассмотренными выше: *множество таких* $p \in P$, *что* $p \equiv a \pmod m$, *имеет натуральную плотность* (равную $1/\varphi(m)$, если a взаимно просто с m); то же самое можно сказать о множествах, обозначенных через P_f, P'_f и Q в предыдущем пункте.

Доказательство (и оценку остаточного члена) см. в книге К. Прахара «Распределение простых чисел», гл. V, § 7.

Глава VII

МОДУЛЯРНЫЕ ФОРМЫ

§ 1. Модулярная группа

1.1. *Определения*

Обозначим через H *верхнюю полуплоскость в* **C**, т. е. множество комплексных чисел z, мнимая часть которых $\mathrm{Im}(z) > 0$.

Пусть $\mathbf{SL}_2(\mathbf{R})$ — группа матриц $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ с вещественными элементами, таких, что $ad - bc = 1$. Заставим $\mathbf{SL}_2(\mathbf{R})$ действовать на $\tilde{\mathbf{C}} = \mathbf{C} \cup \{\infty\}$ следующим образом:

если $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ — элемент из $\mathbf{SL}_2(\mathbf{R})$ и $z \in \tilde{\mathbf{C}}$, то положим

$$gz = \frac{az + b}{cz + d}.$$

Легко проверяется формула

$$\mathrm{Im}(gz) = \frac{\mathrm{Im}(z)}{|cz + d|^2}. \tag{1}$$

Отсюда вытекает, что H *инвариантна* относительно $\mathbf{SL}_2(\mathbf{R})$. Заметим, что элемент $-1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ из $\mathbf{SL}_2(\mathbf{R})$ действует тривиально на H; поэтому мы можем считать, что на самом деле действует группа $\mathbf{PSL}_2(\mathbf{R}) = \mathbf{SL}_2(\mathbf{R})/\{\pm 1\}$ (и действие этой группы *точное* — можно показать, что она является группой всех аналитических автоморфизмов полуплоскости H).

Пусть $\mathbf{SL}_2(\mathbf{Z})$ — подгруппа в $\mathbf{SL}_2(\mathbf{R})$, образованная матрицами с элементами из $\mathbf{Z}$. Это — *дискретная* подгруппа группы $\mathbf{SL}_2(\mathbf{R})$.

Определение 1. *Модулярной группой называется группа*

$$G = \mathbf{SL}_2(\mathbf{Z})/\{\pm 1\},$$

являющаяся образом группы $\mathbf{SL}_2(\mathbf{Z})$ *в* $\mathbf{PSL}_2(\mathbf{R})$.

Если $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ — элемент из $\mathbf{SL}_2(\mathbf{Z})$, то часто мы будем позволять себе обозначать через g и его образ в модулярной группе G.

1.2. *Фундаментальная область модулярной группы*

Пусть S и T — элементы группы G, определенные соответственно матрицами $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ и $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Тогда

$$Sz = -1/z, \quad Tz = z + 1,$$
$$S^2 = 1, \quad (ST)^3 = 1.$$

Пусть, с другой стороны, D — подмножество в H, состоящее из таких точек z, что $|z| \geqslant 1$ и $|R(z)| \leqslant 1/2$. Рисунок 1 показывает преобразования области D под действием элементов

$$\{1, T, TS, ST^{-1}S, ST^{-1}, S, ST, STS, T^{-1}S, T^{-1}\}$$

из группы G.

Мы сейчас увидим, что D есть *фундаментальная область* действия группы G на полуплоскости H. Точнее, имеет место следующая теорема.

Теорема 1. 1) *Для каждого* $z \in H$ *существует* $g \in G$, *такой, что* $gz \in D$.

2) *Пусть* z, z' — *две различные точки из* D, *сравнимые по модулю* G. *Тогда либо* $R(z) = \pm 1/2$ *и* $z = z' \pm 1$, *либо* $|z| = 1$ *и* $z' = -1/z$.

3) *Пусть* $z \in D$, *и пусть* $I(z) = \{g \mid g \in G, gz = z\}$ — *стабилизатор в* G *точки* z. *Тогда* $I(z) = \{1\}$ *за исключением следующих трех случаев*:

$z = i$; *в этом случае* $I(z)$ — *группа второго порядка, порожденная элементом* S;

$z = \rho = e^{2\pi i/3}$; *в этом случае* $I(z)$ — *группа третьего порядка, порожденная элементом* ST;

$z = -\bar{\rho} = e^{\pi i/3}$; *в этом случае* $I(z)$ — *группа третьего порядка, порожденная элементом* TS.

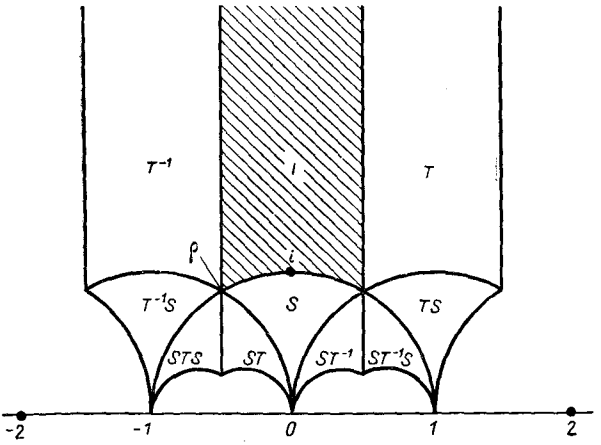

Рис. 1.

Из утверждений 1) и 2) вытекает

Следствие. *Каноническое отображение*[1]) $D \to H/G$ *сюръективно; его ограничение на внутренность области* D *инъективно.*

Теорема 2. *Группа* G *порождается элементами* S *и* T.

Доказательство теорем 1 *и* 2. Пусть G' — подгруппа в G, порожденная элементами S и T, и пусть $z \in H$. Покажем, что *существует такой элемент* $g' \in G'$, *что* $g'z \in D$; это и доказывает утверждение 1) теоремы 1. Если $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ — элемент из G', то

$$\operatorname{Im}(gz) = \frac{\operatorname{Im}(z)}{|cz+d|^2}; \qquad (1)$$

[1]) Т. е. сопоставление элементу из D его G-орбиты в H.— *Прим. перев.*

так как c и d суть целые числа, то число пар (c, d), для которых $|cz+d|$ ограничено сверху данным числом, *конечно*. Отсюда заключаем, что существует такой $g \in G'$, что $\mathrm{Im}(gz)$ максимально. С другой стороны, существует такое целое число n, что вещественная часть значения $T^n gz$ заключена между $-1/2$ и $+1/2$. Элемент $z' = T^n gz$ *принадлежит* D; действительно, нам достаточно убедиться в том, что $|z'| \geqslant 1$; но если бы имело место $|z'| < 1$, то элемент $-1/z'$ имел бы мнимую часть, строго *большую*, чем $\mathrm{Im}(z')$, а это невозможно. Таким образом, элемент $g' = T^n g$ отвечает требуемому условию.

Докажем далее утверждения 2) и 3) теоремы 1. Пусть $z \in D$ и $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ таковы, что $gz \in D$. Заменяя в случае необходимости (z, g) на (gz, g^{-1}), мы можем считать, что $\mathrm{Im}(gz) \geqslant \mathrm{Im}(z)$, т. е. что $|cz+d| \leqslant 1$. Это, очевидно, невозможно, если $|c| \geqslant 2$. Таким образом, остаются случаи $c = 0, 1, -1$.

Если $c = 0$, то $d = \pm 1$ и g является сдвигом на $\pm b$. Так как оба числа $R(z)$ и $R(gz)$ расположены между $-1/2$ и $1/2$, то либо $b = 0$ и $g = 1$, либо $b = \pm 1$ и одно из чисел $R(z)$ и $R(gz)$ равно $-1/2$, а другое $1/2$.

Если $c = 1$, то из $|z+d| \leqslant 1$ следует, что $d = 0$, кроме случая $z = \rho$ (соответственно $z = -\bar{\rho}$); в последнем случае мы можем иметь $d = 0, 1$ (соответственно $d = 0, -1$). Случай $d = 0$ дает $gz = a - 1/z$, и первая часть рассуждения показывает, что $a = 0$, кроме случая $R(z) = \pm 1/2$, т. е. $z = \rho$ или $-\bar{\rho}$, когда $a = 0, -1$ или $0, 1$. Случай $z = \rho$, $d = 1$ дает $gz = a - 1/(1+\rho) = a + \rho$, откуда $a = 0, 1$; аналогично исследуется случай $z = -\bar{\rho}$, $d = -1$.

Наконец, случай $c = -1$ сводится к случаю $c = 1$ изменением знаков у a, b, c, d (что не меняет g, рассматриваемого как элемент из G). Это завершает проверку утверждений 2) и 3).

Нам остается доказать, что $G' = G$. Пусть g — элемент из G. Выберем *внутреннюю* точку z_0 области D (например, $z_0 = 2i$) и положим $z = gz_0$. Выше

мы видели, что существует такой элемент $g' \in G'$, что $g'z \in D$. Точки z_0 и $g'z = g'gz_0$ из D сравнимы по модулю G и одна из них является внутренней в D. На основании 2) и 3) отсюда вытекает, что эти точки совпадают и что $g'g = 1$. А это и означает, что $g \in G'$, что завершает доказательство.

Замечание. Можно показать, что $\langle S, T; S^2, (ST)^3\rangle$ есть представление группы G или (что равносильно) что G есть свободное произведение циклической группы порядка 2, порожденной элементом S, и циклической группы порядка 3, порожденной элементом ST.

§ 2. Модулярные функции

2.1. *Определения*

Определение 2. *Пусть k — целое число. Слабо модулярной функцией веса $2k$* [1]) *называется мероморфная на полуплоскости* H *функция f, которая удовлетворяет соотношению*

$$f(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right), \tag{2}$$

для любой матрицы $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z})$.

Пусть g — образ в G матрицы $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; тогда

$$d(gz)/dz = (cz + d)^{-2}.$$

Соотношение (2) может быть, разумеется, записано так:

$$\frac{f(gz)}{f(z)} = \left(\frac{d(gz)}{dz}\right)^{-k},$$

или так:

$$f(gz)\, d(gz)^k = f(z)\, dz^k. \tag{3}$$

---

[1]) Некоторые авторы говорят, что f «веса $-2k$», другие, что f «веса k».

Это означает, что «дифференциальная форма веса k» $f(z)\,dz^k$ *инвариантна* относительно G. Так как G порождается элементами S и T (см. теорему 2), достаточно чтобы эта форма была инвариантна относительно S и T. Отсюда следует

Предложение 1. *Пусть f — мероморфная на* H *функция. Для того чтобы f была слабо модулярной функцией веса $2k$, необходимо и достаточно, чтобы выполнялись два соотношения*:

$$f(z+1)=f(z), \tag{4}$$

$$f(-1/z)=z^{2k}f(z). \tag{5}$$

Предположим, что выполнено соотношение (4). Тогда мы можем представить f как функцию от $q=e^{2\pi iz}$, функцию, которую мы обозначим через $\tilde{f}$; она мероморфна в круге $|q|<1$ с исключенным началом. Если $\tilde{f}$ продолжается до функции, мероморфной (соответственно голоморфной) в начале, то мы будем говорить, допуская вольность языка, что f *мероморфна* (соответственно *голоморфна*) *на бесконечности*. Это означает, что $\tilde{f}$ допускает разложение в ряд Лорана в окрестности начала

$$\tilde{f}(q)=\sum_{-\infty}^{\infty} a_n q^n,$$

где a_n равны нулю для достаточно малых n (соответственно для $n<0$).

Определение 3. *Слабо модулярная функция называется модулярной, если она мероморфна на бесконечности.*

Когда f голоморфна на бесконечности, полагаем $f(\infty)=\tilde{f}(0)$; это является *значением* функции f на бесконечности.

Определение 4. *Модулярной формой называется всякая модулярная функция, которая голоморфна всюду (включая бесконечность); если такая функция обращается в нуль на бесконечности, то*

говорят, что она является параболической формой (Spitzenform — по-немецки, cusp-form — по-английски).

Таким образом, модулярная форма веса $2k$ задается рядом

$$f(z) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}, \qquad (6)$$

который сходится для $|q|<1$ (т. е. для $\mathrm{Im}(z) > 0$) и удовлетворяет тождеству

$$f(-1/z) = z^{2k} f(z). \qquad (5)$$

Эта форма является параболической формой, если $a_0 = 0$.

Примеры

1) Если f и f' — модулярные формы веса $2k$ и $2k'$ соответственно, то произведение ff' есть модулярная форма веса $2k + 2k'$.

2) Мы увидим дальше, что функция

$$q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \ldots$$

есть параболическая форма веса 12.

2.2. *Функции решеток и модулярные функции*

Напомним сначала, что такое *решетка* в вещественном векторном пространстве V конечной размерности: это подгруппа Γ в V, удовлетворяющая следующим трем равносильным условиям:

i) Γ дискретна и V/Γ компактна;

ii) Γ дискретна и порождает векторное $\mathbf{R}$-пространство V;

iii) существует $\mathbf{R}$-базис $(e_1, \ldots, e_n)$ в V, который является $\mathbf{Z}$-базисом в Γ (т. е. $\Gamma = \mathbf{Z}e_1 \oplus \ldots \oplus \mathbf{Z}e_n$).

Пусть $\mathscr{R}$ — *множество решеток в* $\mathbf{C}$, рассматриваемом как векторное $\mathbf{R}$-пространство. Пусть M — множество таких пар (ω_1, ω_2) элементов из $\mathbf{C}^*$, что $\mathrm{Im}(\omega_1/\omega_2) > 0$; такой паре мы сопоставим решетку

$$\Gamma(\omega_1, \omega_2) = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2.$$

с базисом $\{\omega_1, \omega_2\}$. Таким образом, мы получаем отображение $M \to \mathcal{R}$, которое, очевидно, *сюръективно*.

Пусть $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z})$, и пусть $(\omega_1, \omega_2) \in M$. Положим

$$\omega_1' = a\omega_1 + b\omega_2 \quad \text{и} \quad \omega_2' = c\omega_1 + d\omega_2.$$

Ясно, что $\{\omega_1', \omega_2'\}$ есть базис в $\Gamma(\omega_1, \omega_2)$. Кроме того, если положить $z = \omega_1/\omega_2$ и $z' = \omega_1'/\omega_2'$, то

$$z' = \frac{az + b}{cz + d} = gz.$$

Отсюда заключаем, что $\operatorname{Im}(z') > 0$, и, следовательно, (ω_1', ω_2') принадлежит множеству M.

Предложение 2. *Для того чтобы два элемента из* M *определяли одну и ту же решетку, необходимо и достаточно, чтобы они были конгруентны по модулю* $\mathbf{SL}_2(\mathbf{Z})$.

Мы только что увидели, что это условие достаточно. Обратно, если (ω_1, ω_2) и (ω_1', ω_2') два элемента из M, которые порождают одну и ту же решетку, то существует матрица $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ с определителем ± 1, которая переводит первый базис во второй. Если бы $\det(g)$ был < 0, то знак числа $\operatorname{Im}(\omega_1/\omega_2)$ был бы *противоположным* знаку числа $\operatorname{Im}(\omega_1'/\omega_2')$, как это видно из непосредственного подсчета. Так как эти два знака одинаковы, то необходимо, чтобы $\det(g) = 1$, что и доказывает предложение.

Таким образом, можно отождествить *множество* $\mathcal{R}$ *решеток в* $\mathbf{C}$ с *фактормножеством множества* M *по действию группы* $\mathbf{SL}_2(\mathbf{Z})$.

Заставим теперь $\mathbf{C}^*$ действовать на $\mathcal{R}$ (соответственно на M) посредством отображения $\Gamma \mapsto \lambda\Gamma$ (соответственно $(\omega_1, \omega_2) \mapsto (\lambda\omega_1, \lambda\omega_2)$), $\lambda \in \mathbf{C}^*$. Фактормножество $M/\mathbf{C}^*$ отождествляется с H посредством $(\omega_1, \omega_2) \mapsto z = \omega_1/\omega_2$, и это отождествление индуцирует действие группы $\mathbf{SL}_2(\mathbf{Z})$ на M и действие группы $G = \mathbf{SL}_2(\mathbf{Z})/\{\pm 1\}$ на H (см. п. 1.1). Из этого получаем

Предложение 3. *Отображение* $(\omega_1, \omega_2) \mapsto \omega_1/\omega_2$ *при факторизации индуцирует биекцию фактормножества* $\mathscr{R}/\mathbf{C}^*$ *на* H/G.

(Таким образом, элемент из H/G отождествляется с решеткой в $\mathbf{C}$, определенной с точностью до гомотетии.)

Замечание. Сопоставим решетке Γ в $\mathbf{C}$ *эллиптическую кривую* $E_\Gamma = \mathbf{C}/\Gamma$; легко видеть, что две решетки Γ и Γ' определяют изоморфные эллиптические кривые в том и только том случае, когда они пропорциональны. Таким образом получается третья интерпретация для $H/G = \mathscr{R}/\mathbf{C}^*$: это множество *классов изоморфных эллиптических кривых*.

Перейдем теперь к *модулярным функциям*. Пусть F — функция на $\mathscr{R}$ с комплексными значениями, и пусть $k \in \mathbf{Z}$. Мы будем говорить, что F есть функция *веса* $2k$, если

$$F(\lambda\Gamma) = \lambda^{-2k} F(\Gamma) \tag{7}$$

для любой решетки Γ и любого $\lambda \in \mathbf{C}^*$.

Пусть F — такая функция. Если $(\omega_1, \omega_2) \in M$, то мы обозначим через $F(\omega_1, \omega_2)$ значение функции F на решетке $\Gamma(\omega_1, \omega_2)$. Формула (7) принимает вид

$$F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-2k} F(\omega_1, \omega_2); \tag{8}$$

кроме того, $F(\omega_1, \omega_2)$ инвариантна при действии $\mathbf{SL}_2(\mathbf{Z})$ на M.

Формула (8) показывает, что произведение $\omega_2^{2k} F(\omega_1, \omega_2)$ зависит только от $z = \omega_1/\omega_2$. Следовательно, существует функция f на H, такая, что

$$F(\omega_1, \omega_2) = \omega_2^{-2k} f(\omega_1/\omega_2). \tag{9}$$

Учитывая инвариантность F относительно $\mathbf{SL}_2(\mathbf{Z})$, мы видим, что f удовлетворяет тождеству

$$f(z) = (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right) \tag{2}$$

для всех $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z})$.

Наоборот, если для функции f выполняется (2), то формула (9) сопоставляет ей функцию F на $\mathcal{R}$ веса $2k$. Таким образом, можно отождествить *модулярные функции веса* $2k$ с некоторыми *функциями решеток веса* $2k$.

2.3. *Примеры модулярных функций: ряды Эйзенштейна*

Лемма 1. *Пусть* Γ — *решетка в* $\mathbf{C}$. *Ряд* $\sum'_{\gamma\in\Gamma} 1/|\gamma|^\sigma$ *сходится для* $\sigma > 2$.

(Символ $\sum'$ обозначает, что суммирование распространяется на *ненулевые* элементы из Γ.)

Можно рассуждать так же, как в случае ряда $\sum 1/n^\alpha$, т. е. мажорировать рассматриваемый ряд с точностью до постоянного множителя двойным интегралом $\int\int \frac{dx\,dy}{(x^2+y^2)^{\sigma/2}}$, распространенным на плоскость без круга с центром 0. Двойной интеграл вычисляется без труда переходом к «полярным координатам». Другой, совершенно равносильный метод состоит в следующем: заметим, что число элементов из Γ, таких, что $|\gamma|$ заключен между последовательными целыми числами n и $n+1$, есть $O(n)$; тогда сходимость нашего ряда сводится к сходимости ряда $\sum 1/n^{\sigma-1}$.

Пусть далее k — целое число > 1. Если Γ — решетка в $\mathbf{C}$, то положим

$$G_k(\Gamma) = \sum'_{\gamma\in\Gamma} 1/\gamma^{2k}. \tag{10}$$

На основании леммы 1 этот ряд абсолютно сходится. Ясно, что G_k — функция *веса* $2k$; она называется *рядом Эйзенштейна индекса* k (или, у других авторов, индекса $2k$). Как и в предыдущем пункте, можно рассматривать G_k как функцию на M, задаваемую равенством

$$G_k(\omega_1, \omega_2) = \sum'_{m,n} \frac{1}{(m\omega_1 + n\omega_2)^{2k}}; \tag{11}$$

здесь, как и прежде, символ $\sum'$ обозначает, что суммирование распространяется на пары (m, n), *отличные от* $(0, 0)$. Функция на H, сопоставляемая (способом, описанным в предыдущем пункте) функции G_k, обозначается также через G_k. На основании формул (9) и (11) мы имеем

$$G_k(z) = \sum_{m,\,n}{}' \frac{1}{(mz+n)^{2k}}. \tag{12}$$

Предложение 4. *Пусть* k *— целое число* > 1. *Ряд Эйзенштейна* $G_k(z)$ *есть модулярная форма веса* $2k$. *Имеет место равенство*

$$G_k(\infty) = 2\zeta(2k),$$

где ζ *— дзета-функция Римана.*

Приведенные выше рассуждения показывают, что $G_k(z)$ — слабо модулярная функция веса $2k$. Покажем, что G_k везде голоморфна (включая бесконечность). Сначала предположим, что z принадлежит фундаментальной области D (см. п. 1.2). Тогда мы имеем

$$|mz+n|^2 = m^2z\bar{z} + 2mn\mathrm{R}(z) + n^2 \geqslant$$
$$\geqslant m^2 - mn + n^2 = |m\rho - n|^2.$$

По лемме 1 ряд $\sum' 1/|m\rho - n|^{2k}$ сходится. Отсюда вытекает, что ряд $G_k(z)$ *сходится равномерно на* D, а следовательно, и (применяя результат к $G_k(g^{-1}z)$ при $g \in G$) на любом сдвиге gD области D элементом $g \in G$. Поскольку эти сдвиги покрывают H (теорема 1), функция G_k голоморфна на H. Остается убедиться в голоморфности G_k на бесконечности (и найти ее значение в этой точке). Это сводится к доказательству того, что G_k имеет предел при $\mathrm{Im}(z) \to \infty$. Итак, можно предположить, что z остается в фундаментальной области D; ввиду равномерной сходимости на D, мы можем перейти к пределу почленно. Члены $1/(mz+n)^{2k}$, соответствующие $m \neq 0$, дают 0; остальные дают $1/n^{2k}$. Таким образом, мы

получаем

$$\lim G_k(z) = \sum{}' 1/n^{2k} = 2\sum_{n=1}^{\infty} 1/n^{2k} = 2\zeta(2k),$$

что и завершает доказательство.

Замечание. В п. 4.2 мы дадим разложение для G_k в ряд по степеням переменной $q = e^{2\pi i z}$.

Примеры. Ряды Эйзенштейна наиболее низких значений веса суть G_2 и G_3, имеющие вес 4 и 6. Удобно (по соображениям теории эллиптических кривых) домножить их на некоторые коэффициенты:

$$g_2 = 60G_2, \quad g_3 = 140G_3. \tag{13}$$

Имеем: $g_2(\infty) = 120\zeta(4)$ и $g_3(\infty) = 280\zeta(6)$. Подставляя известные значения для $\zeta(4)$ и $\zeta(6)$ (см., например, ниже п. 4.1), находим

$$g_2(\infty) = \frac{4}{3}\pi^4 \quad \text{и} \quad g_3(\infty) = \frac{8}{27}\pi^6. \tag{14}$$

Если положить

$$\Delta = g_2^3 - 27g_3^2, \tag{15}$$

то отсюда вытекает, что $\Delta(\infty) = 0$; иными словами, Δ *есть параболическая форма веса* 12.

Связь с эллиптическими кривыми. Пусть Γ — решетка в $\mathbf{C}$, и пусть

$$\wp_\Gamma(u) = \frac{1}{u^2} + \sum_{\gamma\in\Gamma}{}' \left(\frac{1}{(u-\gamma)^2} - \frac{1}{\gamma^2}\right) \tag{16}$$

— соответствующая функция Вейерштрасса [1]). Функции $G_k(\Gamma)$ входят в разложение Лорана для $\wp_\Gamma$:

$$\wp_\Gamma(u) = \frac{1}{u^2} + \sum_{k=2}^{\infty} (2k-1)\,G_k(\Gamma)\,u^{2k-2}. \tag{17}$$

---

[1]) См., например, Картан А., Элементарная теория аналитических функций одного и нескольких комплексных переменных, М., 1963, гл. V, § 2, п. 5,

Если положить $x = \wp_\Gamma(u)$, $y = \wp'_\Gamma(u)$, то

$$y^2 = 4x^3 - g_2 x - g_3, \tag{18}$$

где $g_2 = 60\mathrm{G}_2(\Gamma)$, $g_3 = 140\mathrm{G}_3(\Gamma)$, как и выше. С точностью до числового множителя $\Delta = g_2^3 - 27g_3^2$ равен дискриминанту полинома $4X^3 - g_2X - g_3$.

Можно доказать, что кубика (проективная), определенная уравнением (18), изоморфна эллиптической кривой $\mathbf{C}/\Gamma$; в частности, эта кривая *неособая*, откуда вытекает, что $\Delta \neq 0$.

§ 3. Пространство модулярных форм

3.1. *Нули и полюсы модулярной функции*

Пусть f — функция, мероморфная на H, не совпадающая с тождественным нулем, и пусть p — точка из H. Назовем *порядком функции f в p* и обозначим через $v_p(f)$ такое целое число n, что $f/(z-p)^n$ голоморфна и не обращается в нуль в точке p.

Если f — *модулярная функция* веса $2k$, то тождество

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right)$$

показывает, что $v_p(f) = v_{g(p)}(f)$ при $g \in \mathrm{G}$; иными словами, $v_p(f)$ зависит только от образа точки p в фактормножестве H/G. Дополнительно определим $v_\infty(f)$ как порядок в точке $q = 0$ функции $\tilde{f}(q)$, ассоциированной с f (см. п. 2.1).

Наконец, мы обозначим через e_p порядок стабилизатора точки p; таким образом, $e_p = 2$ (соответственно $e_p = 3$), если p конгруентна по модулю G точке i (соответственно точке ρ), и $e_p = 1$ для всех других точек — см. теорему 1.

Теорема 3. *Пусть f — модулярная функция веса $2k$, не равная тождественно нулю. Тогда*

$$v_\infty(f) + \sum_{p \in \mathrm{H/G}} \frac{1}{e_p} v_p(f) = \frac{k}{6}. \tag{19}$$

[Можно также записать эту формулу в виде

$$v_\infty(f)+\frac{1}{2}v_i(f)+\frac{1}{3}v_\rho(f)+\sum_{p\in \mathrm{H/G}}{}^{*}\, v_p(f)=\frac{k}{6}, \quad (20)$$

где символ $\sum^{*}$ обозначает, что суммирование распространяется на точки множества H/G, отличные от классов точки i и точки ρ.]

Заметим сначала, что записанная в теореме 3 сумма имеет смысл, т. е. что f *имеет лишь конечное число нулей и полюсов по модулю* G. Действительно, поскольку $\tilde{f}$ мероморфна, существует такое $r>0$, что $\tilde{f}$ не имеет ни нулей, ни полюсов для $0<q<r$; это означает, что f не имеет ни нулей,

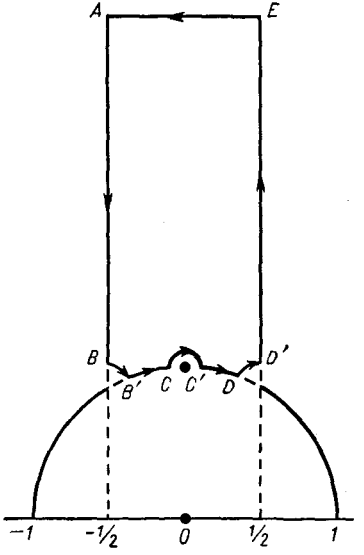

Рис. 2.

ни полюсов для $\mathrm{Im}(z)>e^{2\pi r}$. Подмножество D_r фундаментальной области D, определенное неравенством $\mathrm{Im}(z)\leqslant e^{2\pi r}$, *компактно*; так как f мероморфна в H, она имеет лишь конечное число нулей и полюсов в D_r, откуда вытекает наше утверждение.

Чтобы доказать теорему 3, проинтегрируем $\frac{1}{2\pi i}\frac{df}{f}$ по границе области D. Более точно:

1) Предположим, что f на границе области D не имеет нулей и полюсов, кроме разве лишь i, ρ, $-\bar{\rho}$. Существует контур $\mathscr{C}$ (как показано на рис. 2), внутренность которого содержит представитель каждого нуля и полюса функции f, не конгруентного i

или ρ. По теореме о вычетах имеем

$$\frac{1}{2i\pi}\int_{\mathcal{C}}\frac{df}{f}=\sum_{p\in H/G}^{*}v_p(f).$$

С другой стороны:

a) Замена переменной $q=e^{2\pi iz}$ преобразует путь EA в окружность ω с центром в точке $q=0$, пробегаемую в обратном направлении и не содержащую нулей и полюсов $\tilde{f}$, кроме разве лишь 0. Отсюда

$$\frac{1}{2i\pi}\int_{E}^{A}\frac{df}{f}=\frac{1}{2i\pi}\int_{\omega}\frac{d\tilde{f}}{\tilde{f}}=-v_\infty(f).$$

b) Интеграл от $\frac{1}{2i\pi}\frac{df}{f}$ по окружности, на которой лежит дуга BB′, пробегаемой в обратном направлении, равен $-v_\rho(f)$. Когда радиус этой окружности стремится к нулю, угол $\widehat{B\rho B'}$ стремится к $\frac{2\pi}{6}$, откуда

$$\frac{1}{2i\pi}\int_{B}^{B'}\frac{df}{f}\to-\frac{1}{6}v_\rho(f).$$

Точно так же, когда радиус дуг CC′ и DD′ стремится к 0, мы получаем

$$\frac{1}{2i\pi}\int_{C}^{C'}\frac{df}{f}\to-\frac{1}{2}v_i(f),\qquad\frac{1}{2i\pi}\int_{D}^{D'}\frac{df}{f}\to-\frac{1}{6}v_\rho(f).$$

c) T преобразует путь AB в путь ED′, и $f(Tz)$ равно $f(z)$; поэтому получаем

$$\frac{1}{2i\pi}\int_{A}^{B}\frac{df}{f}+\frac{1}{2i\pi}\int_{D'}^{E}\frac{df}{f}=0.$$

d) S преобразует дугу B′C в дугу DC′, и $f(Sz)$ равно $z^{2k}f(z)$, поэтому получаем

$$\frac{df(Sz)}{f(Sz)}=2k\frac{dz}{z}+\frac{df(z)}{f(z)},$$

откуда

$$\frac{1}{2i\pi}\int_{B'}^{C}\frac{df}{f}+\frac{1}{2i\pi}\int_{C'}^{D}\frac{df}{f}=\frac{1}{2i\pi}\int_{B'}^{C}\left(\frac{df(z)}{f(z)}-\frac{df(Sz)}{f(Sz)}\right)=$$

$$=\frac{1}{2i\pi}\int_{B'}^{C}\left(-2k\frac{dz}{z}\right)\to-2k\left(-\frac{1}{12}\right)=\frac{k}{6},$$

когда радиусы дуг BB′, CC′, DD′ стремятся к 0.

Записывая равенство двух найденных выражений для $\frac{1}{2i\pi}\int_{\mathscr{C}}\frac{df}{f}$ и переходя к пределу, мы получаем формулу (20).

2) Предположим, что f имеет нуль или полюс λ на полупрямой $\left\{z\mid \mathrm{R}(z)=-\frac{1}{2},\ \mathrm{Im}(z)>\frac{\sqrt{3}}{2}\right\}$. Повторим такое же доказательство с контуром, полученным из $\mathscr{C}$ изменением его в окрестностях точек λ и $T\lambda$, как это показано на рис. 3 (дуга окружности, окружающей точку $T\lambda$, является сдвигом при помощи T дуги окружности, окружающей точку λ).

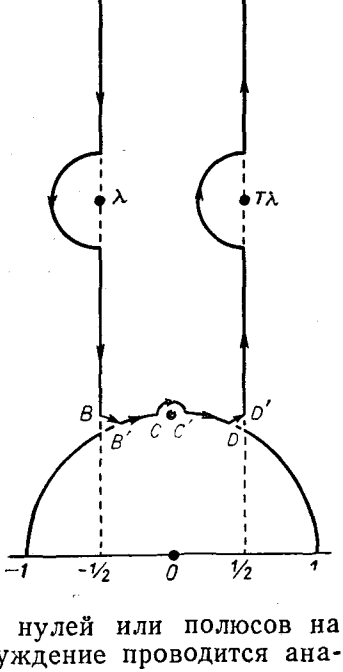

Рис. 3.

Если f имеет несколько нулей или полюсов на границе области D, то рассуждение проводится аналогично.

Замечание. Можно было бы избежать этого несколько утомительного доказательства, если определить комплексную аналитическую структуру на

компактификации множества H/G (см., например, Семинар по комплексному умножению, сб. *Математика*, 12 : 1 (1968), Лекция 2).

3.2. *Алгебра модулярных форм*

Если k — целое число, то мы обозначим через M_k (соответственно через M_k^0) векторное $\mathbf{C}$-пространство модулярных форм веса $2k$ (соответственно параболических форм веса $2k$), см. определение 4 п. 2.1. Напомним, что M_k^0 есть ядро линейной формы $f \mapsto f(\infty)$ на M_k; таким образом, мы имеем $\dim M_k/M_k^0 \leqslant 1$. Более того, для $k \geqslant 2$ ряд Эйзенштейна G_k является таким элементом из M_k, что $G_k(\infty) \neq 0$, см. предложение 4 п. 2.3; следовательно, мы имеем

$$M_k = M_k^0 \oplus \mathbf{C} \cdot G_k \qquad (\text{для } k \geqslant 2).$$

Наконец, напомним, что через Δ мы обозначаем элемент $g_2^3 - 27g_3^2$ из M_6^0, где $g_2 = 60G_2$ и $g_3 = 140G_3$.

Теорема 4. i) $M_k = 0$ *при* $k < 0$ *и* $k = 1$.

ii) *При* $k = 0$, 2, 3, 4, 5 *пространство* M_k *имеет размерность* 1; *его базисным элементом соответственно является* 1, G_2, G_3, G_4, G_5; *при этом* $M_k^0 = 0$.

iii) *Умножение на* Δ *определяет изоморфизм* M_{k-6} *на* M_k^0.

Пусть f — ненулевой элемент из M_k. Тогда все слагаемые в левой части формулы

$$v_\infty(f) + \tfrac{1}{2} v_i(f) + \tfrac{1}{3} v_\rho(f) + \sum_{p \in H/G}^{*} v_p(f) = \frac{k}{6} \qquad (20)$$

неотрицательны. Таким образом, $k \geqslant 0$ и одновременно $k \neq 1$, поскольку $1/6$ не может быть записана в виде $n + n'/2 + n''/3$ при n, n', $n'' \geqslant 0$. Это доказывает i).

Применим теперь (20) к $f = G_2$, $k = 2$. Можно записать $2/6$ в виде $n + n'/2 + n''/3$, n, n', $n'' \geqslant 0$, только при $n = 0$, $n' = 0$, $n'' = 1$; отсюда заключаем, что $v_\rho(G_2) = 1$ и что $v_p(G_2) = 0$ при $p \neq \rho$ по мо-

дулю G. Те же соображения, примененные к G_3, показывают, что $v_i(G_3)=1$ и что остальные $v_p(G_3)$ равны нулю. Этого уже достаточно для доказательства того, что Δ не обращается в нуль в точке i и, следовательно, не является тождественным нулем. Так как вес формы Δ есть 12 и так как $v_\infty(\Delta)\geqslant 1$, формула (20) показывает, что $v_p(\Delta)=0$ при $p\neq\infty$ и что $v_\infty(\Delta)=1$; иначе говоря, Δ *не обращается в нуль на* H *и имеет простой нуль в бесконечности.* Если f — элемент из M_k^0 и если положить $g=f/\Delta$, то ясно, что g имеет вес $k-6$; кроме того, формула

$$v_p(g)=v_p(f)-v_p(\Delta)=\begin{cases} v_p(f), & \text{если } p\neq\infty,\\ v_p(f)-1, & \text{если } p=\infty,\end{cases}$$

показывает, что $v_p(g)\geqslant 0$ при всех p и, следовательно, что g принадлежит пространству M_{k-6}, а это доказывает iii).

Наконец, если $k\leqslant 5$, то $k-6<0$, откуда $M_k^0=0$ на основании i) и iii); отсюда заключаем, что $\dim M_k\leqslant 1$. Так как 1, G_2, G_3, G_4, G_5 суть ненулевые элементы из M_0, M_2, M_3, M_4, M_5, то $\dim M_k=1$ при $k=0$, 2, 3, 4, 5, что и доказывает ii).

Следствие 1. *Имеет место формула*

$$\dim M_k=\begin{cases}[k/6], & \text{если } k\equiv 1 \pmod 6,\ k\geqslant 0,\\ [k/6]+1, & \text{если } k\not\equiv 1 \pmod 6,\ k\geqslant 0.\end{cases} \tag{21}$$

(Напоминаем, что $[x]$ обозначает *целую часть* числа x, т. е. наибольшее целое число n, такое, что $n\leqslant x$.)

Формула (21) верна при $0\leqslant k<6$ на основании i) и ii). С другой стороны, обе части равенства возрастают на единицу при замене k на $k+6$ (см. iii)). Таким образом формула верна при всех $k\geqslant 0$.

Следствие 2. *Пространство* M_k *допускает в качестве базиса семейство одночленов* $G_2^\alpha G_3^\beta$ *при* α, β *целых* $\geqslant 0$ *и* $2\alpha+3\beta=k$.

Покажем, сначала, что эти одночлены *порождают* M_k. Это ясно для $k\leqslant 3$ на основании i) и ii). Для $k\geqslant 4$ рассуждаем по индукции. Выбираем пару (γ, δ)

таких целых неотрицательных чисел, что $2\gamma + 3\delta = k$ (это возможно для любого $k \geqslant 2$). Модулярная форма $g = G_2^{\gamma} G_3^{\delta}$ отлична от нуля на бесконечности. Если $f \in M_k$, то существует такое $\lambda \in \mathbf{C}$, что модулярная форма $f - \lambda g$ является параболической и, следовательно, имеет вид Δh, где $h \in M_{k-6}$, см. iii). Теперь применим предположение индукции к h.

Нам остается показать, что указанные одночлены линейно независимы; если это не так, то функция G_2^3/G_3^2 удовлетворяет нетривиальному алгебраическому уравнению с коэффициентами из $\mathbf{C}$ и, значит, является константой, что невозможно, поскольку G_2 обращается в нуль в точке ρ, а G_3 в ней в нуль не обращается.

Замечание. Пусть $M = \sum_{-\infty}^{+\infty} M_k$ — градуированная алгебра, построенная на *прямой сумме* пространств M_k, и пусть ε: $\mathbf{C}[X, Y] \to M$ — гомоморфизм, переводящий X в G_2 и Y в G_3. Следствие 2 равносильно тому, что ε есть изоморфизм; можно, таким образом, отождествить M с алгеброй полиномов $\mathbf{C}[G_2, G_3]$.

3.3. *Модулярный инвариант*

Положим

$$j = 1728 g_2^3/\Delta. \tag{22}$$

Предложение 5. a) *Функция j есть модулярная функция веса* 0.

b) *Она голоморфна на* H *и имеет простой полюс в бесконечности.*

c) *Она определяет при факторизации биекцию множества* H/G *на* $\mathbf{C}$.

Утверждение a) обеспечивается тем, что обе функции g_2^3 и Δ являются функциями веса 12; b) обеспечивается тем, что Δ везде $\neq 0$ на H и имеет простой нуль в бесконечности, тогда как g_2 отлично от нуля в бесконечности. Для доказательства c) нужно показать, что если $\lambda \in \mathbf{C}$, то модулярная форма $f_\lambda = 1728 g_2^3 - \lambda\Delta$ имеет нуль, и притом един-

ственный, по модулю G. Для этого применим формулу (20) при $f = f_\lambda$ и $k = 6$. Единственные разложения числа $k/6 = 1$ в виде $n + n'/2 + n''/3$ при $n, n', n'' \geqslant 0$ соответствуют тройкам

$$(n, n', n'') = (1, 0, 0) \quad \text{или} \quad (0, 2, 0) \quad \text{или} \quad (0, 0, 3).$$

Это как раз и означает, что f обращается в нуль в одной и только одной точке множества H/G.

Предложение 6. *Пусть f — мероморфная на* H *функция. Следующие свойства равносильны:*

i) *f есть модулярная функция веса* 0;

ii) *f есть частное двух модулярных форм одинакового веса*;

iii) *f есть рациональная функция от j.*

Импликации iii) $\Rightarrow$ ii) $\Rightarrow$ i) ясны непосредственно. Покажем, что i) $\Rightarrow$ iii). Пусть f — модулярная функция. Умножая f, если нужно, на подходящий полином от j, мы можем предполагать, что f голоморфна на H. Так как Δ обращается в 0 на бесконечности, существует такое целое $n \geqslant 0$, что $g = \Delta^n f$ голоморфна на бесконечности. Тогда g является модулярной формой веса $12n$; по следствию 2 из теоремы 4 ее можно записать как линейную комбинацию одночленов $G_2^\alpha G_3^\beta$, где $2\alpha + 3\beta = 6n$. Ввиду линейности, мы сводим задачу к случаю, когда $g = G_2^\alpha G_3^\beta$, т. е. $f = G_2^\alpha G_3^\beta/\Delta^n$. Но соотношение $2\alpha + 3\beta = 6n$ показывает, что числа $p = \alpha/3$ и $q = \beta/2$ *целые*, и тогда $f = G_2^{3p} G_3^{2q}/\Delta^{p+q}$. Таким образом, мы свели вопрос к установлению того, что G_2^3/Δ и G_3^2/Δ суть рациональные функции от j, а это очевидно.

Замечания. 1) Как мы указали выше, возможно определить естественным образом структуру *комплексного аналитического многообразия* на компактификации $\widehat{H/G}$ множества H/G. Предложение 5 утверждает тогда, что j определяет *изоморфизм* многообразия $\widehat{H/G}$ на сферу Римана

$$S_2 = C \cup \{\infty\};$$

что же касается предложения 6, то оно сводится к хорошо известному факту, что единственными мероморфными на $\mathbf{S}_2$ функциями являются рациональные функции.

2) Коэффициент $1728 = 2^6 3^3$ вводится для того, чтобы j имела в бесконечности вычет равный 1. Более точно, разложения в ряды из § 4 показывают, что

$$j(z) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n)\, q^n, \quad z \in \mathrm{H}, \quad q = e^{2\pi i z}. \tag{23}$$

При этом

$$c(1) = 2^2 \cdot 3^3 \cdot 1823 = 196\,884,$$
$$c(2) = 2^{11} \cdot 5 \cdot 2099 = 21\,493\,760.$$

Коэффициенты $c(n)$ являются целыми числами, обладающими замечательными свойствами делимости [1]):

$$n \equiv 0 \pmod{2^a} \Rightarrow c(n) \equiv 0 \pmod{2^{3a+8}},$$
$$n \equiv 0 \pmod{3^a} \Rightarrow c(n) \equiv 0 \pmod{3^{2a+3}},$$
$$n \equiv 0 \pmod{5^a} \Rightarrow c(n) \equiv 0 \pmod{5^{a+1}},$$
$$n \equiv 0 \pmod{7^a} \Rightarrow c(n) \equiv 0 \pmod{7^a},$$
$$n \equiv 0 \pmod{11^a} \Rightarrow c(n) \equiv 0 \pmod{11^a}.$$

§ 4. Разложения в бесконечные ряды

4.1. *Числа Бернулли* B_k

Эти числа определяются разложением в ряд

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} \mathrm{B}_k \frac{x^{2k}}{(2k)!}. \tag{24}$$

---

[1]) См. по этому поводу Atkin A. O. L., O'Brien J. N., *Trans. Amer. Math. Soc.*, **126** (1967), а также статью Аткина в сборнике Computers in mathematical research, North Holland, 1968.

Таблица чисел:

$$B_1=\frac{1}{6},\quad B_2=\frac{1}{30},\quad B_3=\frac{1}{42},\quad B_4=\frac{1}{30},\quad B_5=\frac{5}{66},$$

$$B_6=\frac{691}{2730},\quad B_7=\frac{7}{6},\quad B_8=\frac{3617}{510},\quad B_9=\frac{43\,867}{798},$$

$$B_{10}=\frac{174\,611}{330},\quad B_{11}=\frac{854\,513}{138},\quad B_{12}=\frac{236\,364\,091}{2730},$$

$$B_{13}=\frac{8\,553\,103}{6},\quad B_{14}=\frac{23\,749\,461\,029}{870}.$$

Числа B_k позволяют вычислять значения дзета-функции Римана для целых четных $\geqslant 0$ (а также для целых нечетных $\leqslant 0$) значений аргумента.

Предложение 7. *Если k — целое число $\geqslant 1$, то*

$$\zeta(2k)=\frac{2^{2k-1}}{(2k)!}B_k\pi^{2k}. \tag{25}$$

Тождество

$$z\operatorname{ctg}z=1-\sum_{k=1}^{\infty}B_k\frac{2^{2k}z^{2k}}{(2k)!} \tag{26}$$

вытекает из определения чисел B_k, если положить $x=2iz$. С другой стороны, взяв логарифмическую производную от

$$\sin z=z\prod_{n=1}^{\infty}\left(1-\frac{z^2}{n^2z^2}\right), \tag{27}$$

мы получим

$$z\operatorname{ctg}z=1+2\sum_{n=1}^{\infty}\frac{z^2}{z^2-n^2\pi^2}=1-2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{z^{2k}}{n^{2k}\pi^{2k}}. \tag{28}$$

Сравнивая (26) и (28), мы получаем (25).

Примеры.

$$\zeta(2)=\frac{\pi^2}{2\cdot3},\quad \zeta(4)=\frac{\pi^4}{2\cdot3^2\cdot5},\quad \zeta(6)=\frac{\pi^6}{3^3\cdot5\cdot7},$$

$$\zeta(8)=\frac{\pi^8}{2\cdot3^3\cdot5^2\cdot7},\quad \zeta(10)=\frac{\pi^{10}}{3^5\cdot5\cdot7\cdot11},$$

$$\zeta(12)=\frac{691\pi^{12}}{3^6\cdot5^3\cdot7^2\cdot11\cdot13},\quad \zeta(14)=\frac{2\pi^{14}}{3^6\cdot5^2\cdot7\cdot11\cdot13}.$$

4.2. *Разложения в ряды функций* G_k

Мы сейчас дадим разложение Тейлора ряда Эйзенштейна $G_k(z)$ по степеням $q = e^{2\pi i z}$.

Исходим из хорошо известной формулы

$$\pi \operatorname{ctg} \pi z = \frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z+n} + \frac{1}{z-n} \right). \tag{29}$$

Кроме этого, мы имеем

$$\pi \operatorname{ctg} \pi z = \pi \frac{\cos \pi z}{\sin \pi z} = i\pi \frac{q+1}{q-1} =$$

$$= i\pi - \frac{2i\pi}{1-q} = i\pi - 2i\pi \sum_{n=1}^{\infty} q^n. \tag{30}$$

Отсюда, сравнивая, получаем

$$\frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z+n} + \frac{1}{z-n} \right) = i\pi - 2i\pi \sum_{n=1}^{\infty} q^n. \tag{31}$$

Последовательным дифференцированием равенства (31) получается следующая формула (имеющая смысл при $k \geqslant 2$):

$$\sum_{n \in \mathbf{Z}} \frac{1}{(n+z)^k} = \frac{1}{(k-1)!} (-2i\pi)^k \sum_{n=1}^{\infty} n^{k-1} q^n. \tag{32}$$

Условимся обозначать через $\sigma_k(n)$ сумму $\sum_{d \mid n} d^k$ k-х степеней положительных делителей числа n.

Предложение 8. *Если k — целое число $\geqslant 2$, то*

$$G_k(z) = 2\zeta(2k) + 2 \frac{(2i\pi)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n. \tag{33}$$

Действительно,

$$G_k(z) = \sum_{(n,\,m)\neq(0,\,0)} \frac{1}{(nz+m)^{2k}} =$$

$$= 2\zeta(2k) + 2\sum_{n=1}^{\infty}\sum_{m\in Z}\frac{1}{(nz+m)^{2k}} =$$

$$= 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sum_{a=1}^{\infty} a^{2k-1}q^{an} =$$

$$= 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)\,q^n.$$

Следствие. $G_k(z) = 2\zeta(2k)\,E_k(z)$, *где*

$$E_k(z) = 1 + \gamma_k\sum_{n=1}^{\infty}\sigma_{2k-1}(n)\,q^n \qquad (34)$$

и

$$\gamma_k = (-1)^k\frac{4k}{B_k}. \qquad (35)$$

Определим $E_k(z)$ как частное от деления $G_k(z)$ на $2\zeta(2k)$; ясно, что $E_k(z)$ имеет вид (34). Коэффициент γ_k вычисляется при помощи предложения 7:

$$\gamma_k = \frac{(2i\pi)^{2k}}{(2k-1)!}\frac{1}{\zeta(2k)} =$$

$$= \frac{(2\pi)^{2k}(-1)^k}{(2k-1)!}\frac{(2k)!}{2^{2k-1}B_k\pi^{2k}} = (-1)^k\frac{4k}{B_k}.$$

Примеры

$$E_2 = 1 + 240\sum_{n=1}\sigma_3(n)\,q^n, \qquad g_2 = (2\pi)^4\frac{1}{2^2\cdot 3}E_2,$$

$$E_3 = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)\,q^n, \qquad g_3 = (2\pi)^6\frac{1}{2^3\cdot 3^3}E_3,$$

$$E_4 = 1 + 480\sum_{n=1}^{\infty}\sigma_7(n)\,q^n,$$

$$E_5 = 1 - 264 \sum_{n=1}^{\infty} \sigma_9(n)\, q^n,$$

$$E_6 = 1 + \frac{65\,520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n)\, q^n \quad (65\,520 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13),$$

$$E_7 = 1 - 24 \sum_{n=1}^{\infty} \sigma_{13}(n)\, q^n.$$

Замечание. Мы видели в п. 3.2, что пространство модулярных форм веса 8 (соответственно 10) имеет размерность 1. Поэтому

$$E_2^2 = E_4, \quad E_2 E_3 = E_5. \tag{36}$$

Отсюда получаются тождества

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m),$$

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040 \sum_{m=1}^{n-1} \sigma_3(n)\,\sigma_5(n-m).$$

Более общо, каждую форму E_k можно представить как *полином* от E_2 и E_3.

4.3. *Порядок роста коэффициентов модулярных форм*

Пусть

$$f(z) = \sum_{n=0}^{\infty} a_n q^n \quad (q = e^{2\pi i z}) \tag{37}$$

есть модулярная форма веса $2k$, $k \geqslant 2$. Нас интересует, как растут a_n.

Предложение 9. *Если* $f = G_k$, *то порядок роста* a_n *есть* n^{2k-1}. *Точнее, существуют две такие постоянные* A, $B > 0$, *что*

$$An^{2k-1} \leqslant |a_n| \leqslant Bn^{2k-1}. \tag{38}$$

Предложение 8 показывает, что существует такая постоянная $A > 0$, что $a_n = (-1)^k A\sigma_{2k-1}(n)$, откуда

$$|a_n| = A\sigma_{2k-1}(n) \geqslant An^{2k-1}.$$

С другой стороны:

$$\frac{|a_n|}{n^{2k-1}} = A \sum_{d|n} \frac{1}{d^{2k-1}} \leqslant A \sum_{d=1}^{\infty} \frac{1}{d^{2k-1}} = A\zeta(2k-1) < +\infty.$$

Теорема 5 (Гекке). *Если f — параболическая форма, то*

$$a_n = O(n^k). \tag{39}$$

(Иначе говоря, частное $|a_n|/n^k$ остается ограниченным при $n \to \infty$.)

Поскольку f — параболическая форма, то $a_0 = 0$, и в разложении (37) для f можно выделить множитель q. Поэтому

$$|f(z)| = O(q) = O(e^{-2\pi y}), \tag{40}$$

где $y = \operatorname{Im}(z)$, когда q стремится к 0.

Пусть $\varphi(z) = |f(z)|\, y^k$. Формулы (1) и (2) показывают, что φ *инвариантна* при действии модулярной группы G. Более того, φ продолжается на фундаментальную область D, и формула (40) показывает, что φ стремится к 0 при $y \to \infty$. Отсюда заключаем, что φ *ограничена*, иначе говоря, что существует такая постоянная M, что

$$|f(z)| \leqslant My^{-k} \quad \text{для} \quad z \in H. \tag{41}$$

Зафиксируем y и заставим x изменяться между 0 и 1. Точка $q = e^{2\pi i(x+yi)}$ описывает окружность C_y с центром 0. По формуле вычетов

$$a_n = \frac{1}{2i\pi} \int_{C_y} f(z)\, q^{-n-1}\, dq = \int_0^1 f(x+iy)\, q^{-n}\, dx.$$

(Эту формулу можно было бы вывести и из формулы для коэффициентов Фурье периодической функции.)

Используя (41), получаем

$$|a_n| \leqslant My^{-k} e^{2\pi n y}.$$

Это неравенство имеет смысл при всех $y > 0$. При $y = 1/n$ оно дает $|a_n| \leqslant e^{2\pi} M n^k$, откуда следует теорема.

Следствие. *Если f не является параболической формой, то порядок роста коэффициента a_n есть n^{2k-1}.*

Запишем f в виде $\lambda G_k + h$, где $\lambda \neq 0$ и h — параболическая форма, и применим предложение 9 и теорему 5, учитывая, что n^k «бесконечно мало» по сравнению с n^{2k-1}.

Замечание. Показатель k в теореме 5 может быть улучшен: имеет место оценка

$$a_n = O(n^{k-1/4+\varepsilon})$$

при любом $\varepsilon > 0$ (см. Selberg A., Proc. Symp. Pure Math., VIII, Amer. Math. Soc., 1965 [1])).

Предполагается, что k может быть заменено на $k - 1/2 + \varepsilon$ при любом $\varepsilon > 0$ или даже что

$$a_n = O(n^{k-1/2}\sigma_0(n)),$$

где $\sigma_0(n)$ — число делителей числа n. Мы вернемся к этому в п. 5.6.

4.4. *Разложение формы* Δ

Напомним, что

$$\Delta = g_2^3 - 27g_3^2 = (2\pi)^{12} 2^{-6} 3^{-3} (E_2^3 - E_3^2) = \\ = (2\pi)^{12} (q - 24q^2 + 252q^3 - 1472q^4 + \ldots). \quad (42)$$

Теорема 6 (Якоби). $\Delta = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24}$.

[Эта формула доказывается естественным образом средствами теории эллиптических функций. Так как мы займемся этим методом несколько позже, мы укажем сейчас другое доказательство, которое «элементарно», но несколько искусственно; для более детального знакомства читатель сможет обратиться к работе Гурвица (Hurwitz A., Math. Werke, Bd. I, 578—595).]

[1]) См. также Исследования по теории чисел (Записки научных семинаров ЛОМИ), т. 1, 1966, 140—163. — *Прим. ред.*

Положим

$$F(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}. \tag{43}$$

Для того чтобы доказать, что F и Δ пропорциональны, достаточно показать, что F — модулярная форма веса 12; действительно, тот факт, что разложение функции F имеет нулевой свободный член, показывает, что F — параболическая форма, а известно (теорема 4), что пространство M_{12}^0 параболических форм веса 12 имеет размерность 1. На основании предложения 1 из п. 2.1 все сводится к доказательству того, что

$$F(-1/z) = z^{12}F(z). \tag{44}$$

Используем для этого двойные ряды

$$G_1(z) = \sum_n{\sum_m}' \frac{1}{(m+nz)^2},$$

$$G(z) = \sum_m{\sum_n}' \frac{1}{(m+nz)^2},$$

$$H_1(z) = \sum_n{\sum_m}' \frac{1}{(m-1+nz)(m+nz)},$$

$$H(z) = \sum_m{\sum_n}' \frac{1}{(m-1+nz)(m+nz)},$$

где символ $\sum'$ означает, что при суммировании исключается пара (0, 0). (Обратить внимание на порядок суммирований!)

Ряды H_1 и H легко вычислить непосредственно с помощью формулы

$$\frac{1}{(m-1+nz)(m+nz)} = \frac{1}{m-1+nz} - \frac{1}{m+nz}.$$

Мы видим, что они сходятся и что

$$H_1 = 0, \quad H = -2\pi i/z.$$

С другой стороны, двойной ряд с общим членом

$$\frac{1}{(m-1+nz)(m+nz)} - \frac{1}{(m+nz)^2} = \frac{1}{(m+nz)^2(m-1+nz)}$$

абсолютно сходится. Отсюда вытекает, что $G_1 - H_1$ и $G - H$ совпадают, следовательно, ряды G и G_1 сходятся (с указанным порядком суммирования), и что

$$G_1(z) - G(z) = H_1(z) - H(z) = 2\pi i/z.$$

Кроме того, ясно, что $G_1(-1/z) = z^2 G(-1/z)$. Из этого заключаем

$$G_1(-1/z) = z^2 G_1(z) - 2\pi i z. \tag{45}$$

С другой стороны, проводя вычисления, аналогичные тем, что проводились при доказательстве предложения 8, получаем

$$G_1(z) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) q^n. \tag{46}$$

Возвратимся к функции F, определенной равенством (43). Ее логарифмический дифференциал равен

$$\frac{dF}{F} = \frac{dq}{q}\left(1 - 24 \sum_{n,m=1}^{\infty} n q^{nm}\right) = \\ = \frac{dq}{q}\left(1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n\right). \tag{47}$$

Отсюда, сравнивая с (46), находим

$$\frac{dF}{F} = \frac{6i}{\pi} G_1(z)\, dz. \tag{48}$$

Комбинируя (45) и (48), получаем

$$\frac{dF(-1/z)}{d(-1/z)} = \frac{6i}{\pi} G_1(-1/z) \frac{dz}{z^2} = \\ = \frac{6i}{\pi} \frac{dz}{z^2}(z^2 G_1(z) - 2\pi i z) = \frac{dF(z)}{dz} + 12\frac{dz}{z}. \tag{49}$$

Таким образом, функции $F(-1/z)$ и $z^{12}F(z)$ имеют одинаковый логарифмический дифференциал. Следовательно, существует такая постоянная k, что $F(-1/z) = kz^{12}F(z)$ для всех $z \in H$. При $z = 1$ мы

имеем $z^{12}=1$, $-1/z=z$ и $F(z)\neq 0$, откуда $k=1$, что устанавливает (44) и завершает доказательство.

Замечание. Другое «элементарное» доказательство тождества (44) см. Siegel C. L., Gesamm. Abh., III, n° 62. См. также Семинар по комплексному умножению, сб. *Математика*, 12 : 1 (1968), лекция 6 [1]).

4.5. *Функция Рамануджана*

Обозначим n-й коэффициент параболической формы $F(z)=(2\pi)^{12}\Delta(z)$ через $\tau(n)$. Тогда

$$\sum_{n=1}^{\infty}\tau(n)\,q^n=q\prod_{n=1}^{\infty}(1-q^n)^{24}. \tag{50}$$

Функция $n\longmapsto\tau(n)$ называется *функцией Рамануджана*.

Таблица численных значений [2])

$$\tau(1)=1,\quad \tau(2)=-24,\quad \tau(3)=252,\quad \tau(4)=-1472,$$
$$\tau(5)=4830,\quad \tau(6)=-6048,\quad \tau(7)=-16\,744,$$
$$\tau(8)=84\,480,\quad \tau(9)=-113\,643,\quad \tau(10)=-115\,920,$$
$$\tau(11)=534\,612,\quad \tau(12)=-370\,944.$$

Свойства $\tau(n)$

$$\tau(n)=O(n^6), \tag{51}$$

поскольку Δ имеет вес 12, см. теорему 5 п. 4.3.

$$\tau(nm)=\tau(n)\,\tau(m),\quad \text{если } (n,m)=1, \tag{52}$$

$$\tau(p^{n+1})=\tau(p)\,\tau(p^n)-p^{11}\tau(p^{n-1})$$
$$\text{для простых } p \text{ и } n\geqslant 1, \tag{53}$$

см. далее п. 5.5.

---

[1]) По-видимому, наиболее естественное доказательство формулы (44) дал А. Вейль (Weil A., Sur une formule classique, *J. Math. Soc. Japan*, **20** (1968), № 1—2, 400—402). — *Прим. перев.*

[2]) Эта таблица заимствована из статьи Лемера (Lehmer D. H., Ramanujan's function $\tau(n)$, *Duke Math. J.*, **10** (1943)), где приведены значения $\tau(n)$ для $n\leqslant 300$.

Другой способ выражения свойств (52) и (53) состоит в утверждении, что ряд Дирихле $L_\tau(s) = \sum_{n=1}^{\infty} \tau(n)/n^s$ допускает следующее эйлеровское разложение:

$$L_\tau(s) = \prod_{p \in P} \frac{1}{1 - \tau(p)\, p^{-s} + p^{11-2s}}, \tag{54}$$

см. п. 5.4.

По Гекке (см. п. 5.4) функция L_τ продолжается до *целой* на всей комплексной плоскости функции, причем функция

$$(2\pi)^{-s}\, \Gamma(s)\, L_\tau(s)$$

инвариантна относительно преобразования $s \longmapsto 12 - s$.

Значения $\tau(n)$ удовлетворяют различным *сравнениям* по модулям 2^{12}, 3^6, 5^3, 7, 23, 691. Приведем, в частности (без доказательства), следующие:

$$\tau(n) \equiv n^2 \sigma_7(n) \pmod{3^3}, \tag{55}$$

$$\tau(n) \equiv n \sigma_3(n) \pmod{7}, \tag{56}$$

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}. \tag{57}$$

Другие примеры и их интерпретацию в терминах «l-адических представлений» см. Sém. Delange — Pisot — Poitou, 1967/68, exposé 14 [1]), и Sém. Bourbaki, 1968/69, exposé 355.

В заключение укажем на два *открытых вопроса*:

a) (гипотеза Рамануджана, см. п. 5.6) *верно ли, что* $|\tau(p)| < 2p^{11/2}$ *для любого простого числа* p?

b) (Lehmer) *верно ли, что* $\tau(n) \neq 0$ *для любого* n?

§ 5. Операторы Гекке

5.1. *Определение* $T(n)$

Понятие соответствия на множестве. Пусть E — множество, и пусть X_E — свободная абелева группа, порожденная множеством E. *Соответствием на* E

[1]) Русский перевод: сб. *Математика*, 13 : 4 (1969), 3 — 15. — *Прим. перев.*

(с целыми коэффициентами) мы называем любой гомоморфизм T группы X_E в себя. Гомоморфизм T может задаваться его значениями на элементах x из E:

$$T(x) = \sum_{y \in E} n_y(x)\, y, \quad n_y(x) \in \mathbf{Z}; \tag{58}$$

при этом $n_y(x)$ являются нулями почти для всех y.

Пусть F — *числовая функция на* E. Она продолжается по $\mathbf{Z}$-линейности до функции, обозначаемой также через F, на $\mathbf{X}_E$. Ограничение на E функции $F \circ T$ мы назовем трансформацией функции F посредством T и будем ее обозначать через TF. В обозначениях (58)

$$TF(x) = F(T(x)) = \sum_{y \in E} n_y(x)\, F(y). \tag{59}$$

T(n). Пусть $\mathscr{R}$—множество решеток в $\mathbf{C}$ (см. п. 2.2), и пусть n — целое число $\geqslant 1$. Через T(n) мы обозначим *соответствие на* $\mathscr{R}$, *которое преобразует решетку в сумму* (*в* $X_{\mathscr{R}}$) *ее подрешеток индекса* n. Таким образом,

$$T(n)\,\Gamma = \sum_{(\Gamma : \Gamma') = n} \Gamma', \quad \text{если} \quad \Gamma \in \mathscr{R}. \tag{60}$$

Сумма в правой части равенства конечна: действительно, все Γ' содержат $n\Gamma$; их число совпадает с числом подгрупп порядка n группы $\Gamma/n\Gamma = (\mathbf{Z}/n\mathbf{Z})^2$. Если n — простое число, то легко видеть, что это число равно $n+1$ (*число точек проективной прямой над полем из* n *элементов*).

Мы будем использовать также операторы гомотетии R_λ ($\lambda \in \mathbf{C}^*$), определенные так:

$$R_\lambda \Gamma = \lambda\Gamma, \quad \text{если} \quad \Gamma \in \mathscr{R}. \tag{61}$$

Перечень формул. Можно составить *композиции* соответствий T(n) и R_λ между собой, поскольку они являются эндоморфизмами абелевой группы $X_{\mathscr{R}}$.

Предложение 10. *Соответствия* $T(n)$ *и* R_λ *удовлетворяют тождествам*

$$R_\lambda R_\mu = R_{\lambda\mu} \qquad (\lambda, \mu \in \mathbf{C}^*), \tag{62}$$

$$R_\lambda T(n) = T(n) R_\lambda \quad (n \geqslant 1, \lambda \in \mathbf{C}^*), \tag{63}$$

$$T(m) T(n) = T(mn), \quad \textit{если} \quad (m, n) = 1, \tag{64}$$

$$T(p^n) T(p) = T(p^{n+1}) + pT(p^{n-1}) R_p \quad (p - \textit{простое число}, n \geqslant 1). \tag{65}$$

Формулы (62) и (63) тривиальны.

Формула (64) равносильна следующему утверждению: пусть m, n — два целых $\geqslant 1$ взаимно простых числа, и пусть Γ'' — подрешетка решетки Γ индекса mn; тогда в Γ существует единственная подрешетка Γ', содержащая Γ'', причем $(\Gamma : \Gamma') = n$ и $(\Gamma' : \Gamma'') = m$. Само же это утверждение вытекает из того факта, что группа Γ/Γ'', порядок которой равен mn, единственным образом раскладывается в прямую сумму группы порядка m и группы порядка n (теорема Безу).

Докажем равенство (65). Пусть Γ — решетка. Тогда $T(p^n) T(p) \Gamma$, $T(p^{n+1}) \Gamma$ и $T(p^{n-1}) R_p \Gamma$ являются линейными комбинациями решеток, содержащихся в Γ и имеющих в Γ индекс p^{n+1} (заметим, что $R_p\Gamma$ имеет индекс p^2 в Γ). Пусть Γ'' — одна из таких решеток; ей отвечают в указанном выше смысле коэффициенты a, b, c; нам остается показать, что $a = b + pc$, т. е. что

$$a = 1 + pc,$$

так как b, очевидно, равно 1.

Будем различать два случая.

i) Γ'' не содержится в $p\Gamma$. Тогда $c = 0$ и a является числом решеток Γ', промежуточных между Γ и Γ'' и имеющих индекс p в Γ; такая решетка Γ' содержит $p\Gamma$. В $\Gamma/p\Gamma$ образ решетки Γ' имеет индекс p и содержит образ решетки Γ'', который имеет порядок p (и индекс p, поскольку порядок $\Gamma/p\Gamma$ равен p^2); таким образом, существует единственная решетка Γ', которая отвечает требуемому условию; отсюда $a = 1$, и равенство $a = 1 + pc$ выполняется

ii) $\Gamma'' \subset p\Gamma$. Здесь $c = 1$; произвольная решетка Γ', имеющая индекс p в Γ, содержит $p\Gamma$, следовательно, она тем более содержит Γ''. Отсюда $a = p + 1$, и формула $a = 1 + pc$ опять выполняется.

Следствие 1. $T(p^n)$, $n \geqslant 1$, *суть полиномы от* $T(p)$ *и* R_p.

Это получается из (65) индукцией по n.

Следствие 2. *Алгебра, порожденная всеми* R_λ *и* $T(p)$, p — *простое, коммутативна; она содержит все* $T(n)$.

Это следует из предложения 10 и следствия 1.

Действие $T(n)$ *на функциях веса* $2k$. Пусть F — функция на $\mathcal{R}$ веса $2k$ (см. п. 2.2); по определению имеем

$$R_\lambda F = \lambda^{-2k} F \quad \text{для любого} \quad \lambda \in \mathbf{C}^*. \tag{66}$$

Пусть n — целое число $\geqslant 1$. Формула (63) показывает, что

$$R_\lambda (T(n) F) = T(n) (R_\lambda F) = \lambda^{-2k} T(n) F,$$

иными словами, что $T(n) F$ *есть также функция веса* $2k$. Формулы (64) и (65) дают

$$T(m) T(n) F = T(mn) F, \quad \text{если} \quad (m, n) = 1; \tag{67}$$

$$T(p) T(p^n) F = T(p^{n+1}) F + p^{1-2k} T(p^{n-1}) F,$$
$$p \text{ — простое}, \quad n \geqslant 1. \tag{68}$$

5.2. *Матричная лемма*

Пусть Γ — решетка с базисом (ω_1, ω_2), и пусть n — целое число $\geqslant 1$. Следующая лемма дает способ построения подрешеток решетки Γ индекса n.

Лемма 2. *Пусть* S_n — *множество целых матриц* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *где* $ad = n$, $a \geqslant 1$, $0 \leqslant b < d$. *Для* $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_n$ *обозначим через* Γ_σ *подрешетку решетки* Γ, *определяемую базисом*

$$\omega_1' = a\omega_1 + b\omega_2, \quad \omega_2' = d\omega_2.$$

Тогда отображение $\sigma \longrightarrow \Gamma_\sigma$ *есть биекция множества* S_n *на множество* $\Gamma(n)$ *подрешеток решетки* Γ *индекса* n.

Непосредственно ясно, что Γ_σ порождают $\Gamma(n)$. Обратно, пусть $\Gamma' \in \Gamma(n)$. Положим

$$Y_1 = \Gamma/(\Gamma' + \mathbf{Z}\omega_2) \quad \text{и} \quad Y_2 = \mathbf{Z}\omega_2/(\Gamma' \cap \mathbf{Z}\omega_2).$$

Это циклические группы, порожденные соответственно образами ω_1 и ω_2. Пусть a и d — их порядки. Точная последовательность

$$0 \to Y_2 \to \Gamma/\Gamma' \to Y_1 \to 0$$

показывает, что $ad = n$. Если $\omega_2' = d\omega_2$, то $\omega_2' \in \Gamma'$.

С другой стороны, существует такое $\omega_1' \in \Gamma'$, что

$$\omega_1' \equiv a\omega_1 \pmod{\mathbf{Z}\omega_2}.$$

Ясно, что ω_1' и ω_2' образуют базис решетки Γ'. Далее, ω_1' может быть записано в виде

$$\omega_1' = a\omega_1 + b\omega_2, \quad \text{где} \quad b \in \mathbf{Z},$$

при этом b определено единственным образом по модулю d; если потребовать, чтобы b удовлетворяло неравенству $0 \leqslant b < d$, то это определит b, а следовательно, и ω_1'. Таким образом, каждому $\Gamma' \in \Gamma(n)$ поставлена в соответствие матрица $\sigma(\Gamma') \in S_n$; сразу же проверяется, что соответствия $\sigma \longmapsto \Gamma_\sigma$ и $\Gamma' \longmapsto \sigma(\Gamma')$ обратны друг другу, что и доказывает лемму.

Пример. Если p — простое число, то S_p состоит из матрицы $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ и p матриц $\begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}$, где $0 \leqslant b < p$.

5.3. *Действие* $\mathrm{T}(n)$ *на модулярные функции*

Пусть k — целое число, и пусть f — слабо модулярная функция веса $2k$, см. п. 2.1. Как мы видели в п. 2.2, ей соответствует функция F веса $2k$ на $\mathscr{R}$, для которой

$$\mathrm{F}(\Gamma(\omega_1, \omega_2)) = \omega_2^{-2k} f(\omega_1/\omega_2). \tag{69}$$

Определим $T(n)f$ как *функцию на* H, *ассоциированную с функцией* $n^{2k-1}T(n)F$ *на* $\mathcal{R}$ (отметим числовой коэффициент n^{2k-1}, который позволит впоследствии получать формулы «без знаменателя»). Таким образом, по определению

$$T(n)f(z) = n^{2k-1}T(n)F(\Gamma(z,\ 1)), \tag{70}$$

или иначе, на основании леммы 2,

$$T(n)f(z) = n^{2k-1}\sum_{\substack{a\geqslant 1,\ ad=n\\ 0\leqslant b<d}} d^{-2k}f\left(\frac{az+b}{d}\right). \tag{71}$$

Предложение 11. *Функция* $T(n)f$ *есть слабо модулярная функция веса* $2k$; *она голоморфна на* H, *если такова* f. *Справедливы формулы*

$$T(m)T(n)f = T(mn)f, \text{ если } (m,\ n) = 1, \tag{72}$$

$$T(p)T(p^n)f = T(p^{n+1})f + p^{2k-1}T(p^{n-1})f,$$

$$p \text{ — простое, } n \geqslant 1. \tag{73}$$

Формула (71) показывает, что $T(n)f$ мероморфна на H и, стало быть, слабо модулярна; если помимо этого f голоморфна, то это же имеет место и для $T(n)f$. Формулы (72) и (73) следуют из формул (67) и (68) с учетом числового коэффициента n^{2k-1}, введенного при определении $T(n)f$.

Поведение на бесконечности. Предположим, что f — *модулярная функция*, т. е. она мероморфна в бесконечности. Пусть

$$f(z) = \sum_{m\in\mathbb{Z}} c(m)q^m \tag{74}$$

— ее разложение в ряд Лорана по степеням $q = e^{2\pi iz}$.

Предложение 12. *Функция* $T(n)f$ *есть модулярная функция. При этом*

$$T(n)f(z) = \sum_{m\in\mathbb{Z}} \gamma(m)q^m, \tag{75}$$

где

$$\gamma(m) = \sum_{\substack{a\mid(m,\ n)\\ a\geqslant 1}} a^{2k-1}c(mn/a^2). \tag{76}$$

По определению

$$\mathrm{T}(n)f(z) = \\ = n^{2k-1} \sum_{\substack{ad=n,\ a\geqslant 1 \\ 0\leqslant b<d}} d^{-2k} \sum_{m\in\mathbf{Z}} c(m)\, e^{2\pi i\,[(az+b)/d]\,m}.$$

Заметим, что

$$\sum_{0\leqslant b<d} e^{2\pi i b m/d}$$

равно d, если d делит m, и равно 0, если это не так. Поэтому, полагая $m/d = m'$, можно записать

$$\mathrm{T}(n)f(z) = n^{2k-1} \sum_{\substack{ad=n \\ a\geqslant 1,\ m'\in\mathbf{Z}}} d^{-2k+1}\, c(m'd)\, q^{am'}.$$

Упорядочим по степеням q:

$$\mathrm{T}(n)f(z) = \sum_{\mu\in\mathbf{Z}} q^{\mu} \sum_{a\,|\,(n,\,\mu)\\ a\geqslant 1} (n/d)^{2k-1}\, c(\mu d/a).$$

Так как f мероморфна в бесконечности, существует такое целое число $\mathrm{N}\geqslant 0$, что $c(m) = 0$, если $m\leqslant -\mathrm{N}$. Поэтому коэффициенты $c(\mu d/a)$ равны нулю для $\mu\leqslant -n\mathrm{N}$, что и означает, что функция $\mathrm{T}(n)f$ также мероморфна на бесконечности; так как она уже является слабо модулярной, то этим установлено, что $\mathrm{T}(n)f$ есть модулярная функция. Тот факт, что ее коэффициенты задаются формулой (76) вытекает из приведенного выше подсчета.

Следствие 1. $\gamma(0) = \sigma_{2k-1}(n)\, c(0)$ *и* $\gamma(1) = c(n)$.

Следствие 2. *Если* $n = p$, *где* p — *простое, то*

$$\gamma(m) = c(pm), \qquad \text{если } m \not\equiv 0 \pmod p,$$

$$\gamma(m) = c(pm) + p^{2k-1}\, c(m/p), \qquad \text{если } m \equiv 0 \pmod p.$$

Следствие 3. *Если* f — *модулярная форма (соответственно параболическая форма), то таковой же является и* $\mathrm{T}(n)f$.

Это ясно.

Таким образом, $\mathrm{T}(n)$ действуют на пространствах M_k и M_k^0, определенных в п. 3.2. На основании того,

что мы видели выше, таким образом определенные операторы *коммутируют* между собой и удовлетворяют следующим тождествам:

$$T(m)\,T(n) = T(mn), \text{ если } (m, n) = 1, \tag{72}$$

$$T(p)\,T(p^n) = T(p^{n+1}) + p^{2k-1}\,T(p^{n-1}),$$
$$\text{если } p \text{ — простое, } n \geqslant 1. \tag{73}$$

5.4. *Собственные функции операторов* $T(n)$

Пусть $f(z) = \sum_{n=0}^{\infty} c(n)\,q^n$ — модулярная форма веса $2k$, $k > 0$, не равная тождественно нулю. Предположим, что f — *собственная функция* всех $T(n)$, т. е. существует последовательность комплексных чисел $\lambda(n)$, такая, что

$$T(n)f = \lambda(n)f \text{ для каждого } n \geqslant 1. \tag{77}$$

Теорема 7. a) *Коэффициент* $c(1)$ *при* q *в* f *отличен от* 0.

b) *Если* f *так нормализована, что* $c(1) = 1$, *то*

$$c(n) = \lambda(n) \text{ для каждого } n \geqslant 1. \tag{78}$$

Следствие 1 предложения 12 показывает, что коэффициент при q в $T(n)f$ равен $c(n)$. С другой стороны, на основании (77) он же равен $\lambda(n)\,c(1)$, следовательно

$$c(n) = \lambda(n)\,c(1).$$

Если бы $c(1)$ был нулем, то все $c(n)$, $n > 0$, также были бы нулями, и f была бы постоянной, что невозможно. Отсюда получаем a) и b).

Следствие 1. *Две модулярные формы веса* $2k$, $k > 0$, *которые являются собственными функциями операторов* $T(n)$ *с одинаковыми собственными значениями* $\lambda(n)$ *и которые нормализованы, совпадают.*

Это следует из утверждения a), примененного к разности двух указанных в формулировке функций.

Следствие 2. *Если утверждение* b) *теоремы 7 выполняется, то*

$$c(m)\,c(n) = c(mn), \text{ если } (m, n) = 1, \tag{79}$$

$$c(p)\,c(p^n) = c(p^{n+1}) + p^{2k-1}\,c(p^{n-1}),$$

$$\text{если } p - \text{простое}, \; n \geqslant 1. \tag{80}$$

Действительно, собственные значения $\lambda(n) = c(n)$ удовлетворяют тем же тождествам (72) и (73), что и операторы $\mathrm{T}(n)$.

Формулы (79) и (80) могут быть переформулированы аналитически следующим образом.

Пусть

$$\Phi_f(s) = \sum_{n=1}^{\infty} c(n)/n^s \tag{81}$$

— ряд Дирихле, определенный коэффициентами $c(n)$; на основании следствия из теоремы 5 этот ряд абсолютно сходится для $\mathrm{R}(s) > 2k$.

Следствие 3. *Имеет место разложение*

$$\Phi_f(s) = \prod_{p \in \mathrm{P}} \frac{1}{1 - c(p)\,p^{-s} + p^{2k-1-2s}}. \tag{82}$$

В силу (79) функция $n \longmapsto c(n)$ мультипликативна. Поэтому лемма 4 п. 3.1 гл. VI показывает, что $\Phi_f(s)$ есть произведение рядов $\sum_{n=0}^{\infty} c(p^n)\,p^{-ns}$. Полагая $p^{-s} = \mathrm{T}$, мы замечаем, что вопрос сводится к доказательству тождества

$$\sum_{n=0}^{\infty} c(p^n)\,\mathrm{T}^n = 1/\Phi_{f,\,p}(\mathrm{T}), \tag{83}$$

где

$$\Phi_{f,\,p}(\mathrm{T}) = 1 - c(p)\,\mathrm{T} + p^{2k-1}\mathrm{T}^2.$$

Составим ряд

$$\psi(\mathrm{T}) = \left(\sum_{n=0}^{\infty} c(p^n)\,\mathrm{T}^n\right)(1 - c(p)\,\mathrm{T} + p^{2k-1}\mathrm{T}^2),$$

Коэффициент при T в ψ есть $c(p) - c(p) = 0$; коэффициент при T^{n+1}, $n \geqslant 1$, есть

$$c(p^{n+1}) - c(p)\,c(p^n) + c^{2k-1}\,c(p^{n-1}),$$

что равно нулю в силу (80). Таким образом, ряд ψ сводится к своему постоянному члену $c(1) = 1$, что и доказывает (83).

Замечания. 1) Обратно, из формул (81) и (82) следуют (79) и (80).

2) Гекке доказал, что Φ_f аналитически продолжима до мероморфной на всей комплексной плоскости функции (которая оказывается голоморфной, если f параболична) и что функция

$$X_f(s) = (2\pi)^{-s}\,\Gamma(s)\,\Phi_f(s) \tag{84}$$

удовлетворяет *функциональному уравнению*

$$X_f(s) = (-1)^k\,X_f(2k - s). \tag{85}$$

Доказательство использует *формулу Меллина*

$$X_f(s) = \int_0^\infty (f(iy) - f(\infty))\,y^s\,dy/y$$

в сочетании с тождеством $f(-1/z) = z^{2k} f(z)$. Гекке также доказал и обратное утверждение: каждый ряд Дирихле Φ, который удовлетворяет функциональному уравнению этого типа, а также некоторым требованиям регулярности и возрастания, порождается модулярной формой f веса $2k$; более того, f тогда и только тогда является нормализованной собственной функцией операторов $T(n)$, когда Φ является эйлеровским произведением типа (82). По поводу этого см. Hecke E., Math. Werke, n° 33, а также Weil A., *Math. Annalen,* **168** (1967), 149—156 [1]).

[1]) Русский перевод: сб. *Математика*, 14:6 (1970), 138—145.— *Прим. перев.*

5.5. *Примеры*

а) *Ряды Эйзенштейна.* Пусть k — целое число $\geqslant 2$.

Предложение 13. *Ряд Эйзенштейна* G_k *есть собственная функция операторов* $T(n)$; *соответственные собственные значения суть* $\sigma_{2k-1}(n)$, *а нормализованной собственной функцией является*

$$(-1)^k \frac{B_k}{4k} E_k = (-1)^k \frac{B_k}{4k} + \sum_{n=1}^{\infty} \sigma_{2k-1}(n)\, q^n. \qquad (86)$$

Соответствующий ряд Дирихле есть $\zeta(s)\zeta(s-2k+1)$.

Сначала докажем, что G_k есть собственная функция для $T(n)$; достаточно это сделать для $T(p)$, p — простое число. Рассмотрим G_k как функцию на множестве $\mathscr{R}$ решеток в $\mathbf{C}$; мы имеем

$$G_k(\Gamma) = \sum_{\gamma \in \Gamma}{}' 1/\gamma^{2k}$$

(см. п. 2.3) и

$$T(p)\, G_k(\Gamma) = \sum_{(\Gamma : \Gamma') = p} \sum_{\gamma \in \Gamma'}{}' 1/\gamma^{2k}.$$

Пусть $\gamma \in \Gamma$. Если $\gamma \in p\Gamma$, то γ принадлежит каждой из $p+1$ подрешеток решетки Γ индекса p; сумма соответствующих членов в $T(p)\, G_k(\Gamma)$ есть $(p+1)/\gamma^{2k}$. Если $\gamma \in \Gamma - p\Gamma$, то γ принадлежит точно одной подрешетке индекса p и ему соответствует слагаемое $1/\gamma^{2k}$. Таким образом,

$$T(p)\, G_k(\Gamma) = G_k(\Gamma) + p \sum_{\gamma \in p\Gamma} 1/\gamma^{2k} = G_k(\Gamma) + pG_k(p\Gamma) =$$
$$= (1 + p^{1-2k})\, G_k(\Gamma),$$

а это показывает, что G_k (рассматриваемая как *функция на* $\mathscr{R}$) есть собственная функция для $T(p)$ с собственным значением $1 + p^{1-2k}$; если G_k рассматривать как модулярную форму, то она является собственной функцией для $T(p)$ с собственным значением

$$p^{2k-1}(1 + p^{1-2k}) = \sigma_{2k-1}(p).$$

Формулы (34) и (36) из п. 4.2 показывают, что *нормализованная* собственная функция, ассоциированная с G_k, есть

$$(-1)^k \frac{B_k}{4k} + \sum_{n=1}^{\infty} \sigma_{2k-1}(n)\, q^n.$$

Из этого заключаем, что собственные значения для $T(n)$ равны $\sigma_{2k-1}(n)$.

Наконец,

$$\sum_{n=1}^{\infty} \sigma_{2k-1}(n)/n^s = \sum_{a,\, d \geqslant 1} a^{2k-1}/a^s d^s =$$

$$= \Big(\sum_{d \geqslant 1} 1/d^s\Big)\Big(\sum_{a \geqslant 1} 1/a^{s+1-2k}\Big) = \zeta(s)\,\zeta(s-2k+1).$$

b) *Функция* Δ.

Предложение 14. *Функция* Δ *есть собственная функция операторов* $T(n)$; *соответствующие собственные значения суть* $\tau(n)$, *а нормализованной собственной функцией является*

$$(2\pi)^{-12}\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)\,q^n.$$

Это очевидно, поскольку пространство параболических форм веса 12 имеет размерность 1, так что оно инвариантно относительно $T(n)$.

Следствие. *Имеют место следующие соотношения*:

$$\tau(nm) = \tau(n)\,\tau(m), \quad \textit{если} \quad (n,\, m) = 1, \tag{52}$$

$$\tau(p)\,\tau(p^n) = \tau(p^{n+1}) + p^{11}\tau(p^{n-1}),$$

$$\textit{если } p - \textit{простое}, \; n \geqslant 1. \tag{53}$$

Это вытекает из следствия 2 теоремы 7.

Замечание. Аналогичный результат имеет место в каждом случае, когда пространство M_k^0 параболических форм веса $2k$ имеет размерность 1, как это происходит для $k = 6$, 8, 9, 10, 11 со следующими соответственно базисными элементами: Δ, ΔG_2, ΔG_3, ΔG_4, ΔG_5.

5.6. *Дополнения*

5.6.1. *Скалярное произведение Петерссона*

Пусть f, g — две параболические формы веса $2k$, причем $k > 0$. Легко проверить, что мера

$$\mu(f, g) = f(z)\overline{g(z)}\, y^{2k}\, dx\, dy/y^2 \qquad (x = \mathrm{R}(z),\ y = \mathrm{Im}(z))$$

инвариантна относительно G и *ограничена* на фактормножестве H/G. Полагая

$$\langle f, g\rangle = \int\limits_{\mathrm{H/G}} \mu(f, g) = \int\limits_{\mathrm{D}} f(z)\overline{g(z)}\, y^{2k-2}\, dx\, dy, \qquad (87)$$

мы получаем *эрмитово скалярное произведение* на M_k^0, которое является *положительно определенным* и *невырожденным*. Помимо этого проверяется, что выполняется равенство

$$\langle \mathrm{T}(n) f, g\rangle = \langle f, \mathrm{T}(n) g\rangle, \qquad (88)$$

т. е. $\mathrm{T}(n)$ являются эрмитовыми относительно $\langle f, g\rangle$. Поскольку $\mathrm{T}(n)$ коммутируют между собой, из этого известным способом выводится, что *существует ортогональный базис в* M_k^0, *составленный из собственных векторов операторов* $\mathrm{T}(n)$, и что собственные значения для $\mathrm{T}(n)$ *вещественны*.

5.6.2. *Свойства целости*

Пусть $\mathrm{M}_k(\mathbf{Z})$ — множество модулярных форм

$$f = \sum_{n=0}^{\infty} c(n)\, q^n$$

веса $2k$ с *целыми* коэффициентами $c(n)$. Можно доказать, что существует $\mathbf{Z}$-базис в $\mathrm{M}_k(\mathbf{Z})$, который является $\mathbf{C}$-базисом в M_k (поскольку $\mathrm{M}_k(\mathbf{Z})$ содержит одночлены $\mathrm{E}_2^{\alpha}\mathrm{E}_3^{\beta}$ при $2\alpha + 3\beta = k$). Предложение 12 показывает, что $\mathrm{M}_k(\mathbf{Z})$ инвариантно относительно $\mathrm{T}(n)$, $n \geqslant 1$. Отсюда заключаем, что *коэффициенты характеристического полинома оператора* $\mathrm{T}(n)$, действующего

на M_k, *целые* [1]); в частности, собственные значения операторов $T(n)$ являются *целыми алгебраическими числами* («вполне вещественными» по 5.6.1).

5.6.3. *Гипотеза Рамануджана — Петерссона*

Пусть $f = \sum_{n \geqslant 1} c(n) q^n$, $c(1) = 1$, — параболическая форма веса $2k$, и пусть она является нормализованной собственной функцией операторов $T(n)$. Пусть

$$\Phi_{f,p}(T) = 1 - c(p)T + p^{2k-1}T^2$$

(где p — простое число) — полином, определенный формулой (83) п. 5.4. Можно записать

$$\Phi_{f,p}(T) = (1 - \alpha_p T)(1 - \alpha'_p T), \tag{89}$$

где

$$\alpha_p + \alpha'_p = c(p), \qquad \alpha_p \alpha'_p = p^{2k-1}. \tag{90}$$

Гипотеза Петерссона состоит в том, что α_p *и* α'_p *комплексно сопряжены*; это же самое можно выразить, сказав, что

$$|\alpha_p| = |\alpha'_p| = p^{k-1/2},$$

или что

$$|c(p)| \leqslant 2p^{k-1/2},$$

или что

$$|c(n)| \leqslant n^{k-1/2}\sigma_0(n) \quad \text{для всех} \quad n \geqslant 1.$$

Для $k = 6$ это гипотеза Рамануджана

$$|\tau(p)| \leqslant 2p^{11/2}.$$

(Гипотеза Петерссона может быть сведена к более общим гипотезам Вейля об алгебраических многообразиях над конечным полем; по этому поводу см. Deligne P., Sém. Bourbaki 1968/69, exposé 355.)

---

[1]) Отметим, что существует *явная формула*, дающая след операторов $T(n)$, см. Eichler M., Selberg A., *Journ. Indian Math. Soc.*, 20 (1956). (Русский перевод: сб. *Математика*, 1:4 1957), 3—28.)

§ 6. Тэта-функции

6.1. *Формула Пуассона*

Пусть V — вещественное векторное пространство конечной размерности n, снабженное инвариантной мерой μ. Пусть V′ — пространство, *сопряженное* к V. Пусть f — бесконечно дифференцируемая функция быстрого убывания на V (см. Schwartz L., Théorie des Distributions, гл. VII, § 3 [1]). *Преобразование Фурье* f' функции f определяется формулой

$$f'(y) = \int_V e^{-2i\pi\langle x,\, y\rangle} f(x)\,\mu(x). \tag{91}$$

Это бесконечно дифференцируемая функция быстрого убывания на V′.

Пусть, далее, Γ — *решетка* в V (см. п. 2.2). Мы обозначим через Γ' решетку в V′, *сопряженную* к Γ; под этим понимается множество таких $y \in V'$, что $\langle x, y\rangle \in \mathbf{Z}$ для всех $x \in \Gamma$. Сразу же проверяется, что Γ' отождествима с решеткой, **Z**-сопряженной к решетке Γ (отсюда — название).

Предложение 15. *Пусть* $v = \mu(V/\Gamma)$. *Тогда*

$$\sum_{x\in\Gamma} f(x) = v^{-1} \sum_{y\in\Gamma'} f'(y). \tag{92}$$

Заменяя при необходимости μ на $v^{-1}\mu$, мы можем предполагать, что $\mu(V/\Gamma) = 1$. Взяв базис $e_1, \ldots, e_n$ решетки Γ, отождествим V с $\mathbf{R}^n$, Γ с $\mathbf{Z}^n$ и μ с мерой произведения $dx_1 \ldots dx_n$; тогда $V' = \mathbf{R}^n$, $\Gamma' = \mathbf{Z}^n$, и мы возвращаемся к классической формуле Пуассона (Schwartz L., цит. соч., формула (VII, 7; 5)).

6.2. *Приложение к квадратичным формам*

Далее мы предполагаем, что V снабжено симметрической билинейной формой $x.y$, которая является *положительно определенной* и *невырожденной* (т. е. если $x \neq 0$, то $x.x > 0$).

---

[1]) См. также § 19 гл. VI работы Ганнинга, включенной в список литературы. — *Прим. перев.*

Отождествим V с V′ при помощи только что упомянутой билинейной формы. Решетка Γ′ становится тогда *решеткой* в V; $y \in \Gamma'$ тогда и только тогда, когда $x.y \in \mathbf{Z}$ для любого $x \in \Gamma$.

Решетке Γ мы поставим в соответствие следующую функцию, определенную на $\mathbf{R}_+^*$:

$$\Theta_\Gamma(t) = \sum_{x \in \Gamma} e^{-\pi t x.x}. \tag{93}$$

Наконец, выберем в пространстве V такую инвариантную меру μ, что для ортонормального базиса $\varepsilon_1, \ldots, \varepsilon_n$ объем единичного куба, определенного этим базисом, равен 1. Объем v решетки Γ определяется тогда величиной $v = \mu(V/\Gamma)$, см. п. 6.1.

Предложение 16. *Справедливо тождество*

$$\Theta_\Gamma(t) = t^{-n/2} v^{-1} \Theta_{\Gamma'}(t^{-1}). \tag{94}$$

Пусть $f = e^{-\pi x.x}$. Это бесконечно дифференцируемая функция быстрого убывания на V. Ее преобразование Фурье f' *равно* f. Действительно, выберем ортогональный базис в V и используем его для отождествления V с $\mathbf{R}^n$; мера μ становится мерой $dx = dx_1 \ldots dx_n$, а функция f записывается в виде

$$f = e^{-\pi\left(x_1^2 + \ldots + x_n^2\right)}.$$

Тогда вопрос сводится к доказательству того, что преобразование Фурье от $e^{-\pi x^2}$ есть $e^{-\pi x^2}$, а это общеизвестно.

Теперь можно применить предложение 15 к функции f и к решетке $t^{1/2}\Gamma$; объем этой решетки равен $t^{n/2}v$, а сопряженная к ней решетка есть $t^{-1/2}\Gamma'$; отсюда и следует требуемая формула.

6.3. *Матричная интерпретация*

Пусть $e_1, \ldots, e_n$ — базис решетки Γ, и пусть $a_{ij} = e_i.e_j$. Тогда $A = (a_{ij})$ — симметрическая положительно определенная невырожденная матрица. Если $x = \sum x_i e_i$ — элемент из V, то

$$x.x = \sum a_{ij} x_i x_j.$$

Функция Θ_Γ записывается в виде

$$\Theta_\Gamma(t) = \sum_{x_i \in Z} e^{-\pi i \sum a_{ij} x_i x_j}. \tag{95}$$

Объем v решетки Γ задается формулой

$$v = \det(A)^{1/2}. \tag{96}$$

Это может быть показано следующим образом. Пусть $\varepsilon_1, \ldots, \varepsilon_n$ — ортогональный базис в V; положим

$$\varepsilon = \varepsilon_1 \wedge \ldots \wedge \varepsilon_n, \qquad e = e_1 \wedge \ldots \wedge e_n.$$

Тогда $e = \lambda\varepsilon$, где $\lambda = |v|$. С другой стороны,

$$e.e = \det(A)\,\varepsilon.\varepsilon;$$

сравнивая эти равенства, получаем $v^2 = \det(A)$.

Пусть $B = (b_{ij})$ — матрица, обратная к A. Непосредственно проверяется, что базис (e'_i), сопряженный к базису (e_i), задается формулой

$$e'_i = \sum b_{ij} e_j.$$

Элементы (e'_i) образуют базис решетки Γ'. Матрица $e'_i.e'_j$ равна B. Отсюда заключаем, в частности, что если положить $v' = \mu(V/\Gamma')$, то $vv' = 1$.

6.4. *Частный случай*

Сейчас нас будет интересовать пара (V, Γ), удовлетворяющая следующим двум условиям.

i) *Решетка* Γ', *сопряженная к решетке* Γ, *совпадает с* Γ.

Это утверждение сводится к тому, что $x.y \in \mathbf{Z}$ для $x, y \in \Gamma$ и что форма $x.y$ определяет *изоморфизм* решетки Γ на сопряженную к ней решетку. На матричном языке это сводится к тому, что матрица $A = (e_i.e_j)$ имеет *целые элементы* и что *ее определитель равен* 1; на основании (96) последнее условие равносильно тому, что $v = 1$.

Если $n = \dim V$, то это условие позволяет утверждать, что квадратичный модуль Γ принадлежит

категории S_n, определенной в п. 1.1 гл. V. Обратно, если модуль $\Gamma \in S_n$ положительно определен и если положить $V = \Gamma \otimes \mathbf{R}$, то пара (V, Γ) удовлетворяет i).

ii) *Имеет место сравнение* $x.x \equiv 0 \pmod 2$ *для всех* $x \in \Gamma$.

Это означает, что Γ — *модуль второго типа* в смысле п. 1.3.4 гл. V, или иначе, что диагональные элементы $e_i.e_i$ матрицы A *четны*.

В гл. V мы приводили примеры таких решеток Γ.

6.5. *Тэта-функции*

В этом пункте, равно как и в следующем, мы будем предполагать, что пара (V, Γ) удовлетворяет условиям i) и ii) предыдущего пункта.

Пусть m — целое число $\geqslant 0$; обозначим через $r_\Gamma(m)$ число таких элементов x из Γ, что $x.x = 2m$. Легко видеть, что $r_\Gamma(m)$ мажорируется полиномом от m (точнее, что $r_\Gamma(m) = O(m^{n/2})$). Отсюда вытекает, что целый ряд

$$\sum_{m=0}^{\infty} r_\Gamma(m)\, q^m = 1 + r_\Gamma(1)\, q + \ldots$$

сходится при $|q| < 1$. Поэтому можно определить функцию θ_Γ на полуплоскости H формулой

$$\theta_\Gamma(z) = \sum_{m=0}^{\infty} r_\Gamma(m)\, q^m \qquad (\text{где } q = e^{2\pi i z}). \tag{97}$$

Мы имеем

$$\theta_\Gamma(z) = \sum_{x \in \Gamma} q^{(x.x)/2} = \sum_{x \in \Gamma} e^{\pi i z (x.x)}. \tag{98}$$

Функция θ_Γ называется *тэта-функцией* квадратичного модуля Γ. Она является функцией, голоморфной на H.

Теорема 8. a) *Размерность n пространства* V *делится на* 8.

b) *Функция* θ_Γ *есть модулярная форма веса* $n/2$.

Утверждение a) уже было доказано (следствие 2 теоремы 2 п. 2.1 гл. V).

Покажем, что θ_Γ удовлетворяет тождеству

$$\theta_\Gamma(-1/z) = (-iz)^{n/2}\,\theta_\Gamma(z). \qquad (99)$$

Так как обе части равенства аналитичны по z, то достаточно доказать эту формулу для $z = it$ при вещественном $t > 0$. Итак,

$$\theta_\Gamma(it) = \sum_{x \in \Gamma} e^{-\pi t (x,\,x)} = \Theta_\Gamma(t).$$

Точно так же $\theta_\Gamma(-1/it) = \Theta_\Gamma(t^{-1})$. Поэтому формула (99) следует из (94), если учесть, что $v = 1$ и $\Gamma' = \Gamma$.

Так как n делится на 8, то (99) можно переписать в виде

$$\theta_\Gamma(-1/z) = z^{n/2}\theta_\Gamma(z), \qquad (100)$$

а это и показывает, что θ_Γ есть модулярная форма веса $n/2$.

[Укажем вкратце другое доказательство утверждения а). Предположим, что n не делится на 8; заменяя, если это нужно, Γ на $\Gamma \oplus \Gamma$ или $\Gamma \oplus \Gamma \oplus \Gamma \oplus \Gamma$, можно предполагать, что $n \equiv 0 \pmod 4$. Формула (99) запишется тогда следующим образом:

$$\theta_\Gamma(-1/z) = (-1)^{n/4} z^{n/2}\theta_\Gamma(z) = -z^{n/2}\theta_\Gamma(z).$$

Если положить $\omega(z) = \theta_\Gamma(z)\,dz^{n/4}$, то мы видим, что дифференциальная форма ω получается из $-\omega$ посредством преобразования S: $z \mapsto -1/z$. Так как ω инвариантна относительно T: $z \mapsto z + 1$, то отсюда следует, что ST переводит ω в $-\omega$, что невозможно, поскольку $(ST)^3 = 1$.]

Следствие 1. *Существует такая параболическая форма f_Γ веса $n/2$, что*

$$\theta_\Gamma = E_k + f_\Gamma, \quad \textit{где } k = n/4. \qquad (101)$$

Это вытекает из того факта, что $\theta_\Gamma(\infty) = 1$ и, следовательно, $\theta_\Gamma - E_k$ — параболическая форма.

Следствие 2. *Справедливо равенство* $r_\Gamma(m) = \frac{4k}{B_k}\,\sigma_{2k-1}(m) + O(m^k)$, *где* $k = n/4$.

Это вытекает из следствия 1, формулы (34) и теоремы 5.

Замечание. „Поправочный член" f_Γ, вообще говоря, отличен от нуля. Однако Зигель доказал, что *усреднение* (надлежащим образом взвешенное) *функции* f_Γ *есть нуль.* Точнее, пусть C_n — множество классов (с точностью до изоморфизма) решеток Γ, удовлетворяющих условиям i) и ii), и пусть g_Γ — порядок группы автоморфизмов элемента Γ из C_n (см. п. 3.3 гл. V). Тогда

$$\sum_{\Gamma \in C_n} \frac{1}{g_\Gamma} f_\Gamma = 0, \tag{102}$$

или, иначе,

$$\sum_{\Gamma \in C_n} \frac{1}{g_\Gamma} \theta_\Gamma = M_n \cdot E_k, \quad \text{где} \quad M_n = \sum_{\Gamma \in C_n} \frac{1}{g_\Gamma}. \tag{103}$$

Заметим, что это равносильно тому, что усреднение функции θ_Γ есть *собственная функция* для $T(n)$.

Доказательство формул (102) и (103) см. Siegel C. L., Gesam. Abh., n° 20.

6.6. *Примеры*

i) *Случай* $n = 8$.

Любая параболическая форма веса $n/2 = 4$ — нулевая. Следствие 1 теоремы 8 показывает, что тогда $\theta_\Gamma = E_2$, иными словами

$$r_\Gamma(m) = 240\,\sigma_3(m) \text{ для любого целого числа } m \geqslant 1. \tag{104}$$

Это относится к решетке Γ_8, построенной в п. 1.4.3 гл. V, решетке, которая является единственным элементом в C_8.

ii) *Случай* $n = 16$.

Как и в предыдущем случае получаем

$$\theta_\Gamma = E_4 = 1 + 480 \sum_{m=1}^{\infty} \sigma_7(m)\, q^m. \tag{105}$$

Здесь можно взять $\Gamma = \Gamma_8 \oplus \Gamma_8$ или $\Gamma = \Gamma_{16}$ (в обозначениях п. 1.4.3 гл. V); хотя эти решетки и не изо-

морфны, они имеют одинаковые тэта-функции (они представляют одинаковое число раз каждое целое число).

Заметим, что θ-функция решетки $\Gamma_8 \oplus \Gamma_8$ является *квадратом* θ-функции решетки Γ_8. Мы приходим, таким образом, к тождеству

$$\left(1 + 240 \sum_{m=1}^{\infty} \sigma_3(m)\, q^m\right)^2 = 1 + 480 \sum_{m=1}^{\infty} \sigma_7(m)\, q^m.$$

iii) *Случай* $n = 24$.

Пространство модулярных форм веса 12 имеет размерность 2. Его базис составляют

$$\mathrm{E}_6 = 1 + \frac{65\,520}{691} \sum_{m=1}^{\infty} \sigma_{11}(m)\, q^m,$$

$$\mathrm{F} = (2\pi)^{-12}\Delta = q \prod_{m=1}^{\infty} (1 - q^m)^{24} = \sum_{m=1}^{\infty} \tau(m)\, q^m.$$

Тэта-функция, ассоциированная с решеткой Γ, таким образом, записывается в виде

$$\theta_\Gamma = \mathrm{E}_6 + c_\Gamma \mathrm{F}, \text{ где } c_\Gamma \in \mathbf{Q}. \tag{106}$$

Мы имеем

$$r_\Gamma(m) = \frac{65\,520}{691}\sigma_{11}(m) + c_\Gamma \tau(m) \text{ при } m \geqslant 1. \tag{107}$$

Для определения коэффициента c_Γ положим $m = 1$:

$$c_\Gamma = r_\Gamma(1) - \frac{65\,520}{691}. \tag{108}$$

Заметим, что он $\neq 0$, поскольку 65 520/691 не является целым числом.

Примеры

а) Решетка Γ, построенная Личем (Leech J., *Canad. J. Math.*, **16** (1964)), такова, что $r_\Gamma(1) = 0$. Тогда

$$c_\Gamma = -\frac{65\,520}{691} = -2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13/691.$$

b) Для $\Gamma = \Gamma_8 \oplus \Gamma_8 \oplus \Gamma_8$, $r_\Gamma(1) = 3 \cdot 240$, откуда

$$c_\Gamma = \frac{432\,000}{691} = 2^7 \cdot 3^3 \cdot 5^3/691.$$

c) Для $\Gamma = \Gamma_{24}$, $r_\Gamma(1) = 2 \cdot 24 \cdot 23$, откуда

$$c_\Gamma = \frac{697\,344}{691} = 2^{10} \cdot 3 \cdot 227/691.$$

6.7. *Дополнения*

Тот факт, что мы занимались только самой модулярной группой $G = \mathbf{PSL}_2(\mathbf{Z})$, обязывал нас ограничиваться решетками, удовлетворяющими очень жестким условиям из п. 6.4. В частности, мы не могли даже рассмотреть наиболее естественный случай квадратичной формы

$$X_1^2 + \ldots + X_n^2,$$

которая удовлетворяет условию i) и не удовлетворяет условию ii). Соответствующие тэта-функции являются «модулярными формами веса $n/2$» (заметим, что $n/2$ не обязательно четное и даже не обязательно целое число) относительно подгруппы группы G, порожденной элементами S и T^2. Эта группа имеет индекс 3 в G; ее фундаментальная область имеет две «точки» [1]), которым соответствуют два типа «рядов Эйзенштейна»; этими средствами получаются формулы для числа представлений целого числа в виде суммы n квадратов; за подробностями отсылаем к работам, приведенным в прилагаемом далее списке литературы

[1]) В русской литературе они называются *параболическими вершинами. — Прим. перев.*

ЛИТЕРАТУРА

Некоторые классические произведения

Gauss C. F., Disquisitiones arithmeticae, Werke, Bd. I, 1801. [Русский перевод: Гаусс К. Ф., Труды по теории чисел, М., 1959.]

Jacobi C., Fundamenta nova theoriae functionum ellipticarum, 1829, Gesammelte Werke, Bd. I.

Lejeune-Dirichlet G., Démonstration d'un théorème sur la progression arithmétique, 1834, Werke, Bd. I.

Eisenstein G., Mathematische Abhandlungen, Berlin, 1847.

Riemann B., Gesammelte mathematische Werke, Teubner, 1892. [Русский перевод: Риман Б., Сочинения, М. — Л., 1948.]

Hilbert D., Die Theorie der algebraischer Zahlkörper, Gesammelte Abhandlungen, Bd. I.

Minkowski H., Gesammelte Abhandlungen, Teubner, 1911.

Hecke E., Mathematische Werke, Göttingen, 1959.

Siegel C. L., Gesammelte Abhandlungen, Springer-Verlag, 1966.

Числовые и локальные поля

Hecke E., Algebraische Zahlen, Leipzig, 1923. [Русский перевод: Гекке Э., Лекции по теории алгебраических чисел, М. — Л., 1940.]

Боревич З. И., Шафаревич И. Р., Теория чисел, М., 1964 (2-е изд., 1972).

Eichler M., Einführung in die Theorie der algebraischen Zahlen und Funktionen, Birkhäuser Verlag, 1963.

Serre J.-P., Corps locaux, Hermann, 1962.

Samuel P., Théorie algébrique des nombres, Hermann, 1967.

Artin E., Tate J., Class Field Theory, Benjamin, 1968.

Cassels J., Fröhlich A. (Ed.), Algebraic Number Theory, Acad. Press, 1967. [Русский перевод: Алгебраическая теория чисел, М., 1969.]

Weil A., Basic Number Theory, Springer-Verlag, 1967. [Русский перевод: Вейль А., Основы теории чисел, М., 1972.]

(Последние три книги содержат изложение теории так называемых «полей классов»).

Квадратичные формы

a) *Общая теория, теорема Витта*

Witt E., Theorie der quadratischen Formen in beliebigen Körpern, *J. Crelle*, **176** (1937), 31—44.
Bourbaki N., Algèbre, chap. IX, Hermann, 1959. [Русский перевод: Бурбаки Н., Алгебра. Модули, кольца, формы, М., 1966.]
Artin E., Geometric Algebra, Interscience Publ., 1957. [Русский перевод: Артин Э., Геометрическая алгебра, М., 1969.]

b) *Арифметические свойства*

Jones B., The arithmetic theory of quadratic forms, Wiley, 1950.
Eichler M., Quadratische Formen und orthogonale Gruppen, Springer-Verlag, 1952.
Watson G. L., Integral quadratic forms, Cambridge, 1960.
O'Meara O. T., Introduction to quadratic forms, Springer-Verlag, 1963.

c) *Целые квадратичные формы с дискриминантом* ± 1

Witt E., Eine Identität zwischen Modulformen zweiten Grades, *Abh. math. Sem. Univ. Hamburg*, **14** (1941), 323—337.
Kneser M., Klassenzahlen definiter quadratischer Formen, *Arch. der Math.*, 8 (1957), 241—250.
Milnor J., On simply connected manifolds, *Symp. Mexico*, 1958, 122—128.
Milnor J., A procedure for killing homotopy groups of differentiable manifolds, *Symp. Amer. Math. Soc.*, n° 3, 1961, 39—55.

Теорема Дирихле, дзета-функция и L-функции

Hadamard J., Sur la distribution des zeros de la fonction $\zeta(s)$ et ses conséquences arithmétiques, 1896, Œuvres, C. N. R. S., t. I, 189—210.
Landau E., Handbuch der Lehre von der Verteilung der Primzahlen, Teubner, 1909.
Selberg A., An elementary proof of the prime number theorem for arithmetic progressions, *Canad. J. Math.*, **2** (1950), 66—78.
Prachar K., Primzahlverteilung, Springer-Verlag, 1957. [Русский перевод: Прахар К., Распределение простых чисел, М., 1967.]
Davenport H., Multiplicative number theory, Chicago, Markham, 1968. [Русский перевод: Дэвенпорт Г., Мультипликативная теория чисел, М., 1971.]
Chandrasekharan K., Introduction to analytic number theory, Springer-Verlag, 1968.
Blanchard A., Initiation a la théorie analytique des nombres premiers, Dunod, 1969.

Модулярные функции

Klein F., Vorlesungen über die Theorie der elliptischen Modulfunktionen, Leipzig, 1890.
Ramanujan S., On certain arithmetical functions, *Trans. Cambridge Phil. Soc.*, 22 (1916), 159—184.
Hardy G., Ramanujan, Cambridge, 1940.
Godement R., Travaux de Hecke, *Sém. Bourbaki*, 1952—1953, exposés 74—80.
Gunning R. C., Lectures on modular forms (notes by A. Brumer), Princeton, 1962. [Русский перевод: сб. *Математика*, 8 : 6 (1964), 3—68.]
Borel A. et al., Seminar on complex multiplication, Lecture Notes in Math., n° 21, Springer-Verlag, 1966. [Русский перевод: сб. *Математика*, 12 : 1 (1968), 55—95.]
Weil A., Sur la formule de Siegel dans la théorie des groups classiques, *Acta Math.*, 113 (1965), 1—87. [Русский перевод: сб. *Математика*, 13 : 6 (1969), 18—98.]
Ogg A., Modular forms and Dirichlet series, Benjamin, 1969.

(См. также сочинения Гекке и Зигеля, указанные выше.)

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ

$\mathbf{Z}$, $\mathbf{N}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ — множество целых, неотрицательных целых, рациональных, вещественных, комплексных чисел.

$\mathbf{A}^*$ — множество обратимых элементов кольца $\mathbf{A}$.

$\mathbf{F}_q$ (поле из q элементов) I.1.1

$\left(\frac{x}{p}\right)$ (символ Лежандра) I.3.2, II.3.3

$\varepsilon(n)$, $\omega(n)$ I.3.2, II.3.3

$\mathbf{Z}_p$ (кольцо целых p-адических чисел) II.1.1

v_p (p-адический показатель) II.1.2

$\mathbf{U} = \mathbf{Z}_p^*$ (группа p-адических единиц) II.1.3

$\mathbf{Q}_p$ (поле p-адических чисел) II.1.2

(a, b), $(a, b)_v$ (символ Гильберта) III.1.1, III.2.1

$\mathrm{V} = \mathrm{P} \cup \{\infty\}$ III.2.1, IV.3.1

$\widehat{\oplus}$, $\oplus$ (прямая ортогональная сумма) IV.1.2, V.1.2

$f \sim g$ IV.1.6

$f + g$, $f \dot{-} g$ IV.1.6

$d(f)$ (дискриминант формы f) IV.2.1, IV.3.1

$\varepsilon(f)$, $\varepsilon_v(f)$ (локальный инвариант формы f) IV.2.1, IV.3.1

S, S_n V.1.1

$d(\mathrm{E})$, $r(\mathrm{E})$, $\sigma(\mathrm{E})$, $\tau(\mathrm{E})$ (инварианты элемента из S) V.1.3

I_+, I_-, U, Γ_8, Γ_{8m} (элементы из S) V.1.4

$\mathrm{K}(\mathrm{S})$ (группа Гротендика категории S) V.1.5

$\hat{\mathrm{G}}$ (группа, дуальная конечной абелевой группе G) VI.1.1

$\mathrm{G}(m) = (\mathbf{Z}/m\mathbf{Z})^*$ VI.1.3

P (множество простых чисел) VI.3.1

$\zeta(s)$ (дзета-функция Римана) VI.3.2

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ИМЕННОЙ УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ

УВАЖАЕМЫЙ ЧИТАТЕЛЬ!

Ваши замечания о содержании книги, ее оформлении, качестве перевода и другие просим присылать по адресу: 129820, Москва, И-110, ГСП, 1-й Рижский пер., д. 2, издательство „Мир“.

СЕРР Ж.-П.

КУРС АРИФМЕТИКИ

Редактор *Г. М. Ильичева*
Художник *И. Я. Вовк*
Художественный редактор *В. И. Шаповалов*
Технический редактор *Л. П. Бирюкова*

Сдано в набор 10/XII 1971 г. Подписано к печати 23/V 1972 г.
Бумага кн.-журн. 84 × 108¹/₃₂=2,88 бум. л. 9,66 усл. печ. л.,
Уч.-изд. л. 7,34. Изд. № 1/6449. Цена 51 коп. Зак. 1381

ИЗДАТЕЛЬСТВО «МИР»
Москва, 1-й Рижский пер., 2

Ордена Трудового Красного Знамени Ленинградская типография № 2 имени Евгении Соколовой Главполиграфпрома Комитета по печати при Совете Министров СССР, Измайловский проспект, 29