Дж. МИЛНОР, Д. ХЬЮЗМОЛЛЕР

СИММЕТРИЧЕСКИЕ БИЛИНЕЙНЫЕ ФОРМЫ

Перевод с английского **А.И. НЕМЫТОВА**

Под редакцией **А.В. МИХАЛЕВА**

МОСКВА "НАУКА"
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1986

ББК 22.14
М60
УДК 515.14

J. Milnor, D. Husemoller
Symmetric bilinear forms
Springer-Verlag
Berlin Heidelberg New York
1973

Милнор Дж., Хьюзмоллер Д. Симметрические билинейные формы: Пер. с англ./Под ред. А.В. Михалева. – М.: Наука. Гл. ред. физ.-мат. лит., 1986. – 176 с.

Посвящена теории симметрических билинейных форм. В ней удачно сочетаются черты учебника и монографии. Изложение материала построено таким образом, что получился интересный сплав классических результатов с результатами последних десятилетий.

Для математиков различных специальностей, особенно алгебраистов, геометров и топологов. Доступна студентам старших курсов университетов.

Ил. 13. Библиогр. 85 назв.

Джон Милнор, Дэйл Хьюзмоллер

БИЛИНЕЙНЫЕ СИММЕТРИЧЕСКИЕ ФОРМЫ

Редактор *Т.А. Панькова*
Художественный редактор *Т.Н. Кольченко*
Технический редактор *С.В. Геворкян*
Корректор *Т.В. Обод*

Набор осуществлен в издательстве
на наборно-печатающих автоматах

ИБ № 12309

Сдано в набор 20.01.86. Подписано к печати 14.04.86
Формат 84 X 108 1/32. Бумага офсетная № 1
Гарнитура Пресс-Роман. Печать офсетная. Усл.печ.л. 9,24
Усл.кр.-отт. 9,45. Уч.-изд.л. 9,61. Тираж 6400 экз.
Тип. зак. 24 Цена 95 коп.

Ордена Трудового Красного Знамени
издательство "Наука"
Главная редакция физико-математической литературы
117071 Москва, В-71, Ленинский проспект, 15

4-я типография издательства "Наука"
630077 г. Новосибирск-77, ул. Станиславского, 25

М 1702030000-091 / 053 (02)-86 17-86

ОГЛАВЛЕНИЕ

ОТ РЕДАКТОРА ПЕРЕВОДА

Книга известных математиков Дж. Милнора и Д. Хьюзмоллера, хорошо знакомых советскому читателю по переводам их трудов, посвящена теории симметрических билинейных форм над коммутативными кольцами. Книга успешно выдержала два издания. Ее отличительная особенность – удачное сочетание черт учебника и монографии. Авторам удалось построить изложение материала таким образом, что получился чрезвычайно интересный сплав классических результатов с результатами последних десятилетий. Книга написана в характерном для авторов четком и ясном стиле. Она будет интересна широкому кругу советских читателей.

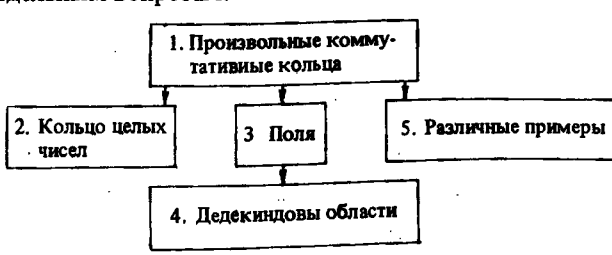
А. Михалев

ВВЕДЕНИЕ

Теория квадратичных форм и тесно связанная с ней теория симметрических билинейных форм имеют длинную и богатую историю, озаренную работами Лежандра, Гаусса, Минковского и Хассе (см. [23] и [10, с. 524]). Наше изложение будет сосредоточено на относительно недавних результатах, начатых и вдохновленных работой Витта "Теория квадратичных форм над произвольными полями" (1937). В наибольшей степени нас будут интересовать работы Пфистера и Кнебуша. Однако будет изложен и более традиционный материал, в частности, в гл. 2. Основой книги послужили лекции Милнора в Институте перспективных исследований (Institute for Advanced Study) и в колледже г. Хейверфорда в рамках лекционной программы Филлипса в 1970 г., а также лекции в Принстонском университете в 1966 г. Нам хотелось бы выразить благодарность Дж. Каннингхэму, М. Кнебушу, М. Кнезеру, А. Розенбергу, В. Шарлау и Ж.-П. Серру за полезные предложения и замечания.

Предполагаемая подготовка читателя. Желательно знакомство с основами алгебры, включая, например, понятие тензорного произведения модулей над коммутативным кольцом. Для чтения некоторых параграфов оно должно быть чуть более глубоким.

Логические связи между различными главами могут быть грубо описаны приведенной ниже диаграммой. Имеются также пять приложений, в значительной степени замкнутых в себе и посвященных отдельным вопросам.



Глава 1

ОСНОВНЫЕ ПОНЯТИЯ

В этой главе будет определено понятие *пространства с внутренним произведением* над коммутативным кольцом R и описаны основные конструкции, не зависящие от специфики кольца R. В частности, вводится *кольцо Витта* $W(R)$, которое будет играть центральную роль в последующих главах. Кольцо $W(R)$ является, грубо говоря, набором всех симметрических пространств с внутренним произведением X над кольцом R по модулю набора "расщепляющихся" пространств с внутренним произведением. Про пространство с внутренним произведением X говорят, что оно *расщепляется*, если $X = X_1 + X_2$, где подмодули X_1 и X_2 двойственно спарены внутренним произведением и $X_1 \cdot X_1 = 0$.

§ 1. Билинейные формы и внутренние произведения

Пусть R — коммутативное кольцо с 1 и X — левый R-модуль.

1.1. Определение. *Билинейной формой* на модуле X называется функция $\beta(x, y)$,

$$\beta\colon X \times X \to R,$$

R-линейная как функция от x при фиксированном y и как функция от y при фиксированном x. Билинейная форма β называется *внутренним произведением* на модуле X, если выполнено следующее сильное условие невырожденности: для каждого R-линейного отображения

$$\varphi\colon X \to R$$

существует и только один элемент $x_0 \in X$, для которого гомоморфизм

$$y \mapsto \beta(x_0, y)$$

из X в R совпадает с отображением φ, и существует и только один элемент $y_0 \in X$, для которого гомоморфизм

$$x \mapsto \beta(x, y_0)$$

совпадает с отображением φ. (Другими словами, каждый из двух гомоморфизмов

$$x_0 \mapsto \beta(x_0,), \quad y_0 \mapsto \beta(, y_0)$$

из модуля X в двойственный модуль $\mathrm{Hom}_R(X, R)$ является изоморфизмом.)

Для внутреннего произведения обычно будет использоваться следующее обозначение: $\beta(x, y) = x \cdot y$.

Если β является билинейной формой или внутренним произведением на модуле X, то пара (X, β) называется *модулем с билинейной формой* или *модулем с внутренним произведением* над кольцом R. Два модуля с билинейными формами называются *изоморфными*, если существует изоморфизм R-модулей f: $X \to X'$, для которого $\beta'(f(x), f(y)) = \beta(x, y)$ при любых $x, y \in X$.

В тех случаях, когда можно не опасаться двусмысленности, для модуля с билинейной формой (X, β) будем использовать сокращенную запись X.

Нас будут интересовать в первую очередь конечно порожденные проективные [1]) R-модули.

1.2. Определение. Если R-модуль X конечно порожден и проективен, то модуль с внутренним произведеним (X, β) будет называться *пространством* с внутренним произведением.

Нас будут особенно интересовать симметрические внутренние произведения.

1.3. Определение. Билинейная форма или внутреннее произведение β называется *симметрическим*, если для любых элементов x и y

$$\beta(x, y) = \beta(y, x).$$

Аналогично, оно называется *кососимметрическим*, если для любых элементов x и y

$$\beta(x, y) = -\beta(y, x),$$

и *симплектическим* (или знакопеременным), если для каждого элемента x

$$\beta(x, x) = 0.$$

Из равенства $\beta(x, y) + \beta(y, x) = \beta(x + y, x + y) - \beta(x, x) - \beta(y, y)$ следует, что каждое симплектическое внутреннее произведение является кососимметрическим. Над кольцом R, в котором 2 –

---

[1]) Модуль P называется *проективным*, если существует такой модуль Q, что прямая сумма $P \oplus Q$ является свободным модулем (т.е. изоморфна прямой сумме экземпляров R-модуля R).

обратимый элемент, верно и обратное, поскольку над ним из равенства $\beta(x, x) = -\beta(x, x)$ следует, что $\beta(x, x) = 0$.

Элементы x и y модуля с билинейной формой β называются *ортогональными*, если $\beta(x, y) = 0$. При использовании понятия ортогональности всегда будем предполагать, что форма β является либо симметрической, либо кососимметрической. Таким образом, из равенства $\beta(x, y) = 0$ следует, что $\beta(y, x) = 0$ (см. [4, с. 152]).

Отметим, что если X является модулем с внутренним произведением, то элемент x ортогонален каждому элементу $y \in X$ тогда и только тогда, когда $x = 0$. В том случае, когда R – поле, верно и обратное утверждение: если (X, β) является пространством с билинейной формой, в котором лишь нулевой вектор ортогонален каждому вектору $y \in X$, то β является внутренним произведением на X.

§ 2. Билинейные формы на свободном модуле

Если X является свободным конечно порожденным R-модулем с базисом $e_1, \ldots, e_n$, то число n называется *рангом* или *размерностью* модуля X и обозначается $\mathrm{rk}(X)$. Поскольку кольцо R коммутативно, то ранг определен однозначно.

Если модуль X имеет базис $e_1, \ldots, e_n$, то любой билинейной форме β на модуле X сопоставляется матрица $B = (\beta_{ij})$ размером $n \times n$, где

$$\beta_{ij} = \beta(e_i, e_j).$$

Эта матрица однозначно определяет билинейную форму, поскольку из $x = \Sigma \xi_i e_i$ и $y = \Sigma \eta_j e_j$ следует, что

$$\beta(x, y) = \Sigma \beta_{ij} \xi_i \eta_j.$$

2.1. Определение. Для матрицы $B = (\beta_{ij})$ с элементами из R символом

$$\langle B \rangle = \langle B \rangle_R$$

обозначим свободное пространство с билинейной формой (X, β) над R с базисом $e_1, \ldots, e_n$, в котором $\beta(e_i, e_j) = \beta_{ij}$.

2.2. Лемма. *Введенная билинейная форма является внутренним произведением тогда и только тогда, когда матрица Γ обратима (т.е. имеет двустороннюю обратную матрицу).*

Утверждение непосредственно вытекает из того, что гомоморфизм $x \mapsto \beta(x,)$ из модуля X в двойственный ему модуль $\mathrm{Hom}_R(X, R)$, снабженный двойственным базисом $e_1^*, \ldots, e_n^*$, задается соответствием $e_i \mapsto \sum_j \beta_{ij} e_j^*$. □

Отметим, что пространство с билинейной формой $\langle B \rangle$ является: симметрическим тогда и только тогда, когда $B = B^t$; кососимметрическим тогда и только тогда, когда $B^t = -B$; симплектическим тогда и только тогда, когда $B^t = -B$ и на диагонали матрицы B стоят нули. (Здесь B^t обозначает, как обычно, транспонированную к матрице B матрицу.)

Рассмотрим теперь замену базиса.

2.3. Лемма. *Пространства с билинейными формами* $\langle B \rangle$ *и* $\langle B' \rangle$ *изоморфны тогда и только тогда, когда*

$$B' = ABA^t$$

для некоторой обратимой матрицы A *размером* $n \times n$.

Если $e'_1, \ldots, e'_n$ — новый базис, то

$$e'_i = \alpha_{i1} e_1 + \ldots + \alpha_{in} e_n$$

для некоторой обратимой матрицы (α_{ik}). Отсюда следует, что

$$B(e'_i, e'_j) = \Sigma\, \alpha_{ik}\, \beta_{kl}\, \alpha_{jl},$$

где суммирование ведется по $1 \leqslant k \leqslant n$, $1 \leqslant l \leqslant n$. □

Следующий частный случай представляет особый интерес.

2.4. Пример. Пусть u — произвольный элемент группы R^* обратимых элементов кольца R. Тогда через $\langle u \rangle$ обозначим пространство с симметрическим внутренним произведением, имеющее один базисный элемент e_1, такой, что $e_1 \cdot e_1 = u$. Отметим, что

$$\langle u \rangle \cong \langle u' \rangle$$

тогда и только тогда, когда $u' = \alpha^2 u$ для некоторого элемента $\alpha \in R^*$.

Полезным инвариантом свободного пространства с внутренним произведением является его определитель. Пусть R^{*2} обозначает подгруппу группы R^*, состоящую из всех квадратов обратимых элементов кольца R.

2.5. Определение. *Определителем* свободного пространства с внутренним произведением X называется элемент факторгруппы R^*/R^{*2}, порожденный элементом $\det(B)$, где B — любая матрица, такая, что $\langle B \rangle \cong X$.

В более общей ситуации, если X — свободный модуль с билинейной формой, то $\det(X)$ является элементом факторполугруппы R/R^{*2}, порожденным элементом $\det(B)$, где B — любая матрица, такая, что $\langle B \rangle \cong X$. Из леммы 2.3 следует, что определитель определен корректно.

В заключение параграфа приведем одну классическую конструкцию. Пусть в свободном пространстве X с внутренним произведением задан базис $e_1, \ldots, e_n$. Тогда *дуальный*, или *двойственный*,

базис $e_1^{\#}, \ldots, e_n^{\#}$ пространства X определяется соотношениями:

$e_i \cdot e_k^{\#} = 0$ при $i \neq k$;

$e_i \cdot e_i^{\#} = 1$.

2.6. Л е м м а. *Каждому базису свободного пространства с внутренним произведением соответствует, и притом единственный, дуальный базис.*

Так как матрица $(\beta_{ij}) = (e_i \cdot e_j)$ обратима, то через (γ_{ij}) обозначим обратную к ней матрицу. Тогда элементы

$$e_k^{\#} = \gamma_{1k} e_1 + \ldots + \gamma_{nk} e_n$$

образуют требуемый дуальный базис. □

§ 3. Ортогональные суммы

Пусть $X_1, \ldots, X_n$ – модули с билинейными формами $\beta_1, \ldots, \beta_n$ соответственно. *Ортогональная сумма* $X_1 \oplus \ldots \oplus X_n$ определяется как прямая сумма модулей X_i с билинейной формой β, для которой

$$\beta(x_1 \oplus \ldots \oplus x_n, y_1 \oplus \ldots \oplus y_n) = \Sigma \beta_i(x_i, y_i),$$

где $x_i, y_i \in X_i$, и суммирование ведется по $1 \leqslant i \leqslant n$.

Очевидно, что ортогональная сумма $X_1 \oplus \ldots \oplus X_n$ является модулем (или пространством) с внутренним произведением тогда и только тогда, когда каждое слагаемое X_i является модулем (или пространством) с внутренним произведением. Отметим, что если модули X_i свободны и конечно порождены, то

$$\mathrm{rk}(X_1 \oplus \ldots \oplus X_n) = \Sigma \, \mathrm{rk}(X_i)$$

и

$$\det(X_1 \oplus \ldots \oplus X_n) = \Pi \det(X_i).$$

Следующая лемма чрезвычайно важна, хотя и легко доказывается. Пусть X – модуль с билинейной формой β, а M – подмодуль в X. *Будем предполагать, что билинейная форма β либо симметрическая, либо кососимметрическая, так что из $\beta(x, y) = 0$ следует, что $\beta(y, x) = 0$.*

3.1. Л е м м а (об ортогональном разложении). *Если ограничение билинейной формы β на произведение $M \times M$ является внутренним произведением на M, то модуль с билинейной формой X изоморфен ортогональной сумме $M \oplus M^{\perp}$.*

Здесь через $M^{\perp}$ обозначено *ортогональное дополнение* подмодуля M, состоящее из всех элементов $x \in X$, таких, что $\beta(x, M) = 0$.

Доказательство. Если $m \in M \cap M^{\perp}$, то $\beta(m, m') = 0$ для любого $m' \in M$ и, следовательно, $m = 0$. Таким образом, для доказательства утверждения 3.1 достаточно показать, что каждый элемент $x \in X$ может быть записан в виде суммы $m + y$, где $m \in M$ и $y \in M^{\perp}$.

Пусть $x \in X$. Рассмотрим на модуле M линейную форму $m' \mapsto \beta(x, m')$. По определению внутреннего произведения существует ровно один элемент $m \in M$, такой, что

$$\beta(m, m') = \beta(x, m')$$

для любого элемента m'. Тогда $x - m \in M^{\perp}$ и поэтому

$$x = m + (x - m).$$

Этим завершается доказательство леммы. □

3.2. Теорема. *Пусть X – модуль с симметрической или кососимметрической билинейной формой β, $x_1, \ldots, x_k \in X$ и $k \times k$-матрица $(\beta(x_i, x_j))$ обратима. Тогда элементы $x_1, \ldots, x_k$ линейно независимы и*

$$X \cong M \oplus M^{\perp},$$

где M – свободный модуль, порожденный элементами x_i.

Доказательство. Поскольку любое нетривиальное соотношение $\rho_1 x_1 + \ldots + \rho_k x_k = 0$ противоречило бы гипотезе об обратимости матрицы $(\beta(x_i, x_j))$, теорема легко выводится из предыдущей леммы. □

Эта теорема имеет многочисленные приложения. Приведем некоторые из них.

3.3. Следствие. *Если X – конечно порожденный модуль с симметрической билинейной формой, то*

$$X \cong \langle u_1 \rangle \oplus \ldots \oplus \langle u_k \rangle \oplus N,$$

где $u_1, \ldots, u_k$ – обратимые элементы, а значение $\beta(x, x)$ необратимо для любого $x \in N$.

Если X содержит некоторый элемент x_1, такой, что элемент $\beta(x_1, x_1) = u_1$ обратим, то по теореме 3.2

$$X \cong (Rx_1) \oplus (Rx_1)^{\perp},$$

где подмодуль

$$Rx_1 \cong \langle u_1 \rangle$$

свободен. Теперь применим то же построение к модулю $(Rx_1)^{\perp}$ и продолжим далее по индукции.

После конечного числа шагов эта процедура должна окончиться. Предположим, что модуль X порожден n элементами. Если бы по-

строение продолжалось более чем n шагов, то мы могли бы построить гомоморфизм свободного модуля ранга n на свободный модуль ранга $n+1$. Поскольку кольцо R коммутативно, то это невозможно. Этим завершается доказательство. □

Если R – поле, то отсюда следует, что $\beta(x, x) = 0$ для любого $x \in N$ и, таким образом, модуль N симплектический. В действительности, если характеристика поля R не равна 2, то ограничение формы β на $N \times N$, будучи одновременно симметрической и симплектической формой, должно в действительности быть нулевой формой. В случае внутреннего произведения это означает, что модуль N сам должен быть нулевым.

В качестве более общего случая рассмотрим *локальное кольцо* (т.е. кольцо с единственным максимальным идеалом).

3.4. Следствие. *Если R – локальное кольцо, в котором 2 – обратимый элемент, то каждое пространство с симметрическим внутренним произведением над R обладает ортогональным базисом.*

Это означает, что модуль X обладает базисом $e_1, \ldots, e_k$, таким, что $e_i \cdot e_j = 0$ для любых $i \neq j$. Другими словами,

$$X \cong \langle u_1 \rangle \oplus \ldots \oplus \langle u_k \rangle$$

для подходящих обратимых элементов $u_1, \ldots, u_k$.

Доказательство следствия 3.4. Рассмотрим подмодуль N в следствии 3.3. Как ортогональное слагаемое пространства с внутренним произведением подмодуль N сам должен быть пространством с внутренним произведением. Предположим, что модуль N ненулевой. Поскольку каждый конечно порожденный проективный модуль над локальным кольцом свободен ([71] или [59]), мы можем выбрать базис $e_1, \ldots, e_n$ модуля N, где $n \geqslant 1$. Пусть $e_1^\#, \ldots, e_n^\#$ – дуальный базис. Тогда вычисление

$$2 = 2e_1 \cdot e_1^\# = (e_1 + e_1^\#) \cdot (e_1 + e_1^\#) - e_1 \cdot e_1 - e_1^\# \cdot e_1^\#$$

показывает, что элемент 2 принадлежит идеалу необратимых элементов, что противоречит нашему предположению. Таким образом, $N = 0$, что завершает доказательство. □

Рассмотрим, наконец, следующий пример. Пусть X – пространство с симплектическим внутренним произведением. Под *симплектическим базисом* пространства X мы будем понимать такой базис $e_1, \ldots, e_n$, что ассоциированная матрица $(e_i \cdot e_j)$ внутреннего произведения имеет вид $\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$.

3.5. Следствие. *Если R является либо дедекиндовой областью* (см. определение на с. 111), *либо локальным кольцом,*

то каждое пространство с симплектическим внутренним произведением над R свободно и обладает симплектическим базисом.

Таким образом, ранг такого пространства всегда четный, а определитель всегда равен единице в $R^{\times}/R^{\cdot 2}$. (В более общем случае определитель в $R/R^{\cdot 2}$ любого свободного пространства с симплектическим внутренним произведением имеет канонический квадратный корень в $R/R^{\cdot}$, называемый "пфаффианом" (см. [11, с. 409]).)

Доказательство следствия 3.5. Сначала мы должны построить в пространстве X элементы x_1 и x_2, такие, что $x_1 \cdot x_2 = 1$. Если R – локальное кольцо, то проективный модуль X обязательно свободен, так что, выбирая базис $e_1, \ldots, e_n$ и дуальный базис $e_1^{\#}, \ldots, e^{\#}$, мы получим подходящую пару векторов e_1 и $e_1^{\#}$.

В случае дедекиндова кольца классическая теорема Штейница [1]) утверждает, что проективный модуль X является прямой суммой свободного модуля с базисом $e_1, \ldots, e_n$ и идеала $\mathfrak{a} \subset R$. Если $n \geqslant 1$, то мы опять можем выбрать элемент $e_1^{\#}$, такой, что $e_1 \cdot e_1^{\#} = 1$. Если же $n = 0$, то $X \cong \mathfrak{a}$ и ясно, что симплектическая форма $\beta\colon \mathfrak{a} \times \mathfrak{a} \to R$ должна быть нулевой. Следовательно, случай $X \cong \mathfrak{a} \neq 0$ не может встретиться.

Таким образом, если $X \neq 0$, то существуют элементы x_1 и x_2, такие, что $x_1 \cdot x_2 = 1$. Очевидно, что 2×2-матрица

$$(x_i \cdot x_j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

обратима, и по теореме 3.2 эти два элемента порождают свободное ортогональное слагаемое. Теперь доказательство легко завершается по индукции. □

Пример пространства с симплектическим внутренним произведением, не имеющего симплектического базиса, будет построен в § 2 гл. 5.

§ 4. Теорема Витта

Пусть X – модуль с симметрической билинейной формой над кольцом R. Предположим, что дано разложение в ортогональную сумму $X = M \oplus N$.

4.1. Определение. *Отражением* модуля X относительно пары (M, N) называется линейное преобразование $r\colon X \to X$, которое оставляет подмодуль M поэлементно неподвижным, а каждый элемент подмодуля N переводит в противоположный.

---

[1]) См., например, [59, с. 21–24].

Таким образом, преобразование r отображает каждую сумму $x = m + n$ в модуле X в $r(x) = m - n$. Очевидно, что преобразование r является инволюцией:

$$r(r(x)) = x,$$

и что оно сохраняет билинейную форму, т.е.

$$\beta(r(x), r(y)) = \beta(x, y)$$

для любых x и y. Если элемент 2 обратим в кольце R, то легко показать и обратное, т.е. что любая сохраняющая билинейную форму линейная инволюция на модуле X является отражением.

4.2. Л е м м а. *Предположим, что R – локальное кольцо, в котором элемент 2 обратим. Если x и y являются элементами модуля с симметрической билинейной формой X, такими, что элемент*

$$\beta(x, x) = \beta(y, y)$$

обратим в R, то существует отражение модуля X, переводящее элемент x в элемент y.

Д о к а з а т е л ь с т в о. Представим x в виде суммы двух взаимно ортогональных векторов $u = (x + y)/2$ и $v = (x - y)/2$. Тогда

$$\beta(x, x) = \beta(u, u) + \beta(v, v).$$

Поскольку кольцо R локально, по крайней мере один из элементов $\beta(u, u)$ и $\beta(v, v)$ кольца должен быть обратим. Если обратим элемент $\beta(u, u)$, то $X = (Ru) \oplus (Ru)^{\perp}$ и отражение относительно пары $((Ru), (Ru)^{\perp})$ переводит элемент $u + v = x$ в элемент $u - v = y$. Аналогично, если обратим элемент $\beta(v, v)$, то отражение относительно пары $((Rv)^{\perp}, (Rv))$ переводит элемент x в элемент y. Это завершает доказательство леммы. □

4.2. С л е д с т в и е. *Пусть кольцо R удовлетворяет условиям леммы. Если X – пространство с внутренним произведением ранга n над кольцом R, то любой автоморфизм f пространства X может быть представлен в виде композиции n отражений.*

Д о к а з а т е л ь с т в о проведем по индукции. Из следствия 3.4 следует, что существует ортогональный базис $e_1, \ldots, e_n$ модуля X. Выберем отражение r_1, переводящее элемент $f(e_1)$ в элемент e_1. Тогда отображение $r_1 f$ оставляет элемент e_1 на месте и, следовательно, переводит в себя подпространство $(Re_1)^{\perp}$ ранга $n - 1$. Следовательно, ограничение на $(Re_1)^{\perp}$ отображения $r_1 f$ является композицией отражений $r_2 \ldots r_n$. Полагая $r_i(e_1) = e_1$ при $i > 1$, мы продолжаем каждое отражение r_i на модуль X и получаем разложение $f = r_1 \ldots r_n$, что и требовалось. □

Более важным для наших приложений результатом, вытекающим из леммы 4.2, является следующая теорема. (Мы продолжаем считать, что R – локальное кольцо, в котором элемент 2 обратим.)

4.4. Теорема Витта. *Пусть X, Y, Z – пространства с внутренним произведением над R. Тогда если $X \oplus Y \cong X \oplus Z$, то $Y \cong Z$.*

Доказательство. Поскольку, в силу следствия 3.4, пространство X является прямой суммой пространств ранга 1, то теорему достаточно доказать в случае, когда X – свободный модуль ранга 1. Пусть e – базисный элемент модуля X и пусть

$$f\colon X \oplus Y \to X \oplus Z$$

– произвольный изоморфизм. Чтобы избежать недоразумений, через 0_X, 0_Y и 0_Z обозначим нулевые элементы пространств X, Y и Z соответственно. Тогда пара элементов $f(e \oplus 0_Y)$ и $e \oplus 0_Z$ в пространстве $X \oplus Z$ удовлетворяет условиям леммы 4.2 и, следовательно, существует отражение r пространства $X \oplus Z$, переводящее элемент $f(e \oplus 0_Y)$ в элемент $e \oplus 0_Z$. Теперь изоморфизм

$$rf\colon X \oplus Y \to X \oplus Z$$

переводит элемент $e \oplus 0_Y$ в элемент $e \oplus 0_Z$ и, следовательно, переводит его ортогональное дополнение $0_X \oplus Y$ в $0_X \oplus Z$. Этим завершается доказательство теоремы. □

Отметим, что теорема Витта заведомо неверна в том случае, когда элемент 2 необратим в кольце R. Для доказательства этого рассмотрим изоморфизм

$$\langle -1 \rangle \oplus \langle -1 \rangle \oplus \langle 1 \rangle \cong \langle -1 \rangle \oplus H,$$

где через H обозначена *гиперболическая плоскость* – свободный модуль ранга 2 с внутренним произведением, заданным матрицей $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Действительно, если e_1, e_2, e_3 – ортогональные векторы, такие, что $e_1 \cdot e_1 = e_2 \cdot e_2 = -1$ и $e_3 \cdot e_3 = 1$, то векторы

$$e_1 + e_2 + e_3, \quad e_1 + e_3, \quad e_2 + e_3$$

образуют новый базис с матрицей внутреннего произведения

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Но если элемент 2 необратим, то

$$\langle -1 \rangle \oplus \langle 1 \rangle \ncong H,$$

поскольку каждый элемент $h \in H$, очевидно, удовлетворяет условию

$$h \cdot h \equiv 0 \mod 2R$$

(см. также обсуждение в § 1 гл. 5).

Интересно отметить, что теорема Витта остается справедливой для *квадратичных форм* над полем характеристики 2 (см. приложение 1).

§ 5. Тензорные произведения и внешние степени

Пусть $X_1, \ldots, X_n$ – модули над кольцом R с билинейными формами $\beta_1, \ldots, \beta_n$ соответственно. Тогда тензорное произведение $X_1 \otimes \ldots \otimes X_n$ над кольцом R может быть превращено в модуль с билинейной формой следующим образом.

5.1. Л е м м а. *Существует единственная билинейная форма β на модуле $X_1 \otimes \ldots \otimes X_n$, удовлетворяющая равенству*

$$\beta(x_1 \otimes \ldots \otimes x_n, y_1 \otimes \ldots \otimes y_n) = \prod_{i=1}^{n} \beta_i(x_i, y_i)$$

для всех элементов x_i и y_i из модулей X_i, где $1 \leqslant i \leqslant n$.

Д о к а з а т е л ь с т в о. Заметим, что $2n$-линейная функция $(x_1, \ldots, x_n, y_1, \ldots, y_n) \mapsto \beta(x_1, y_1) \ldots \beta(x_n, y_n)$ из модуля $X_1 \times \ldots \times X_n \times X_1 \times \ldots \times X_n$ в кольцо R поднимается до ассоциированного линейного отображения

$$X_1 \otimes \ldots \otimes X_n \otimes X_1 \otimes \ldots \otimes X_n \to R.$$

Рассматривая композицию с канонической билинейной функцией

$$(X_1 \otimes \ldots \otimes X_n) \times (X_1 \otimes \ldots \otimes X_n) \to$$

$$\to X_1 \otimes \ldots \otimes X_n \otimes X_1 \otimes \ldots \otimes X_n,$$

получаем требуемую билинейную форму β. □

5.2. З а м е ч а н и е. Если каждый модуль X_i является симметрическим, то, очевидно, и тензорное произведение является симметрическим. В более общем случае, если каждый модуль X_i является ϵ_i-симметрическим, где "1-симметрический" означает "симметрический", а "-1-симметрический" означает "кососимметрический", то тензорное произведение $X_1 \otimes \ldots \otimes X_n$ является $(\epsilon_1 \ldots \epsilon_n)$-симметрическим. Аналогично, если модуль X_1 симметрический, а модуль X_2 симплектический, то произведение $X_1 \otimes X_2$ будет симплектическим.

Теперь предположим, что каждый сомножитель X_i является пространством с внутренним произведением.

5.3. Л е м м а. *Если $X_1, \ldots, X_n$ – пространства с внутренним произведением над кольцом R, то $X_1 \otimes \ldots \otimes X_n$ – пространство с внутренним произведением над кольцом R.*

Д о к а з а т е л ь с т в о. Поскольку каждый модуль X_i является прямым слагаемым в свободном конечно порождением R-модуле, то легко выводится, что тензорное произведение $X_1 \otimes \ldots \otimes X_n$ является прямым слагаемым в свободном конечно порожденном R-модуле.

Через X^* обозначим модуль $\mathrm{Hom}(X, R)$, дуальный к модулю X. Каждому внутреннему произведению β_i сопоставим ассоциированный изоморфизм

$$\overline{\beta}_i\colon X_i \to X_i^*,$$

где $\overline{\beta}_i(x)(y) = \beta_i(x, y)$. Ассоциированный с билинейной формой β гомоморфизм

$$\overline{\beta}\colon X_1 \otimes \ldots \otimes X_n \to (X_1 \otimes \ldots \otimes X_n)^*$$

может быть выражен как композиция

$$\overline{\beta} = \eta \circ (\overline{\beta}_1 \otimes \ldots \otimes \overline{\beta}_n),$$

где η – гомоморфизм из модуля $X_1^* \otimes \ldots \otimes X_n^*$ в модуль $(X_1 \otimes \ldots \otimes X_n)^*$, отображающий каждый образующий $f_1 \otimes \ldots \otimes f_n$ в гомоморфизм $x_1 \otimes \ldots \otimes x_n \mapsto f(x_1) \ldots f(x_n)$. Но каждый модуль X_i конечно порожден и проективен. Поэтому легко проверяется, что η – изоморфизм. Это завершает доказательство.

В этой лемме предположение о проективности модулей X_i является существенным. В качестве контрпримера в непроективном случае можно рассмотреть модули порядка 3 над кольцом $\mathbf{Z}/9\mathbf{Z}$.

Отметим, что для любых элементов u и v из группы R^*

$$\langle u \rangle \otimes \langle v \rangle \cong \langle uv \rangle$$

и для любого модуля X

$$\langle 1 \rangle \otimes X \cong X.$$

Если X и Y – свободные модули, то

$$\mathrm{rk}(X \otimes Y) = \mathrm{rk}(X)\,\mathrm{rk}(Y).$$

Тензорное произведение будет играть важную роль в последующих разделах. В частности, оно используется при построении операции умножения в кольце Витта (§ 7). Далее приводится основан-

ная на тензорном произведении конструкция замены колец, которая также будет играть существенную роль.

5.4. Замена колец. Пусть $f\colon R \to R'$ — кольцевой гомоморфизм. Тогда любое пространство с внутренним произведением X над кольцом R порождает пространство с внутренним произведением

$$f_{\#}(X) = R' \otimes_R X$$

над кольцом R', где внутреннее произведение на модуле $f_{\#}(X)$ определяется формулой

$$(\alpha \otimes x) \cdot (\beta \otimes y) = \alpha\beta f(x \cdot y).$$

Например, если X — свободный R-модуль с базисом $e_1, \ldots, e_n$ и матрицей внутреннего произведения $(e_i \cdot e_j)$, то модуль $f_{\#}(X)$ свободен над кольцом R' и имеет матрицу внутреннего произведения $(f(e_i \cdot e_j))$. Соответствие $X \mapsto f_{\#}(X)$ сохраняет ортогональные суммы и тензорные произведения.

Завершая настоящий параграф, кратко опишем три близких конструкции, которые, однако, не будут играть заметной роли в нашем изложении.

5.5. Ранг проективного модуля. Аналогичная конструкция используется при определении *ранга* конечно порожденного проективного модуля P над кольцом R (см., например, [71, с. 136]). Через $\operatorname{Spec}(R)$ обозначим снабженное топологией Зарисского множество простых идеалов кольца R, а через $\mathbf{Z}^{\operatorname{Spec}(R)}$ — группу непрерывных целочисленных функций на пространстве $\operatorname{Spec}(R)$. Тогда по определению

$$\operatorname{rank}(P) \in \mathbf{Z}^{\operatorname{Spec}(R)}$$

является функцией, сопоставляющей каждому простому идеалу $\mathfrak{p}$ размерность векторного пространства $F \otimes_R P$, где F — факторполе $R/\mathfrak{p}$. В том случае, когда модуль P свободен, это совпадает с нашим предыдущим определением.

5.6. Внешние степени. Если X — модуль с билинейной формой над кольцом R, то его внешняя степень $\bigwedge^k X$ над кольцом R обладает единственной билинейной формой $\hat{\beta}$, удовлетворяющей равенству

$$\hat{\beta}(x_1 \wedge \ldots \wedge x_k, y_1 \wedge \ldots \wedge y_k) = \det(\beta(x_i, y_j))$$

(см. [11, с. 348]). Если модуль X симметричен, то модуль $\bigwedge^k X$ ϵ^k-симметричен. Если X — пространство с внутренним произведением, то $\bigwedge^k X$ — также является пространством с внутренним произведением.

5.7. Определитель. Пусть X – пространство с билинейной формой над кольцом R, заданной на таком проективном модуле, ранг которого равен n по каждому простому идеалу. Тогда пространство с билинейной формой $\wedge^n X$ ранга 1 называется "определителем" пространства X (см. [24]). В эту схему входит и наша предыдущая конструкция определителя, поскольку если X – свободный модуль с базисом $e_1, \ldots, e_n$, то $\wedge^n X$ – свободный модуль с базисом $e = e_1 \wedge \ldots \wedge e_n$ и, следовательно,

$$\wedge^n X \cong \langle d_0 \rangle,$$

где элемент

$$d_0 = \hat{\beta}(e, e) = \det(\beta(e_i, e_j))$$

корректно определен с точностью до умножения на квадрат обратимого элемента.

В § 3 гл. 5 будет приведена иллюстрация "определителя" пространства.

§ 6. Расщепляемые пространства с внутренним произведением

6.1. Определение. Пространство с симметрическим внутренним произведением S над кольцом R называется *расщепляемым*, если существует подмодуль $N \subset S$, являющийся прямым слагаемым в S и совпадающий со своим ортогональным дополнением $N^{\perp}$.

Этим понятием мы обязаны Кнебушу, использовавшему термин "метаболическое" вместо "расщепляемое".

Отметим эквивалентную форму этого определения. Пространство S расщепляемо, если оно является прямой суммой двух подмодулей M и N, которые дуально спарены над кольцом R с помощью внутреннего произведения,

$$M \xrightarrow{\cong} \mathrm{Hom}_R(N, R),$$

$$N \xrightarrow{\cong} \mathrm{Hom}_R(M, R),$$

причем подмодуль N ортогонален самому себе, т.е. $N \cdot N = 0$. (Еще одной переформулировкой была бы такая:

пространство S расщепляемо, если оно содержит ортогональное самому себе прямое слагаемое N, ранг которого в смысле п. 5.5 равен $\frac{1}{2}\,\mathrm{rank}(S)$.)

Приведем два примера. *Гиперболическая плоскость* с матрицей $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, очевидно, расщепляема. Кроме того, для любого обратимого элемента u ортогональная сумма

$$\langle u \rangle \oplus \langle -u \rangle$$

расщепляема, поскольку если e_1, e_2 – ортогональный базис, в котором внутреннее произведение имеет матрицу $\begin{pmatrix} u & 0 \\ 0 & -u \end{pmatrix}$, то элемент $e_1 + e_2$ порождает требуемое прямое слагаемое N, для которого $N = N^{\perp}$.

6.2. Л е м м а. *Пусть S и S' – расщепляемые пространства с внутренним произведением и пусть $X = (X, \beta)$ – произвольное пространство с внутренним произведением. Тогда расщепляемы ортогональная сумма $S \oplus S'$ и тензорное произведение $S \otimes X$. Кроме того, расщепляема ортогональная сумма*

$$(X, \beta) \oplus (X, -\beta).$$

Легко приводятся доказательства первых двух утверждений. Для доказательства третьего утверждения рассмотрим расщепляемое пространство с внутренним произведением $\langle 1 \rangle \oplus \langle -1 \rangle$ и заметим, что тензорное произведение

$$\begin{aligned} (\langle 1 \rangle \oplus \langle -1 \rangle) \otimes (X, \beta) &\cong \\ &\cong (\langle 1 \rangle \otimes (X, \beta)) \oplus (\langle -1 \rangle \oplus (X, \beta)) \\ &\cong (X, \beta) \otimes (X, -\beta) \end{aligned}$$

также расщепляемо.

В отдельных случаях удается получить более точное описание расщепляемых пространств.

6.3. Л е м м а. *Пусть над кольцом R каждый конечно порожденный проективный модуль свободен. Тогда пространство с внутренним произведением над R расщепляемо в том и только в том случае, когда оно обладает таким базисом, в котором матрица внутреннего произведения имеет вид* $\begin{pmatrix} 0 & I \\ I & A \end{pmatrix}$. *Если элемент* 2 *обратим в R, то любое расщепляемое пространство с внутренним произведением в подходящем базисе будет иметь матрицу* $\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$.

Таким образом, если выполнены все предположения леммы 6.3, то каждое расщепляемое пространство изоморфно ортогональной сумме гиперболических плоскостей. В частности, это имеет место, если R – поле характеристики, отличной от 2.

Доказательство леммы 6.3. Если N – прямое слагаемое в X, то выберем в подмодуле N базис $e_1, \ldots, e_n$ и расширим его до базиса $e_1, \ldots, e_k$ модуля X. Пусть $e_1^\#, \ldots, e_k^\#$ – дуальный базис. Ясно, что элементы $e_{n+1}^\#, \ldots, e_k^\#$ образуют базис ортогонального дополнения $N^\perp$

Предположим, что $N = N^\perp$. Тогда, подставляя элементы $e_1, \ldots, e_n$ вместо элементов $e_{n+1}^\#, \ldots, e_k^\#$, мы увидим, что элементы

$$e_1, \ldots, e_n, \quad e_1^\#, \ldots, e_n^\#$$

образуют базис модуля X. (В частности, ранг k модуля X должен равняться $2n$.) В этом новом базисе матрица внутреннего произведения X примет вид $\begin{pmatrix} 0 & I \\ I & A \end{pmatrix}$, где A – некоторая симметрическая матрица. Обратное утверждение очевидно.

Предположим теперь, что элемент 2 обратим в кольце R. Положим $B = -\frac{1}{2}A$. Непосредственное вычисление показывает, что

$$\begin{pmatrix} I & 0 \\ B & I \end{pmatrix}\begin{pmatrix} 0 & I \\ I & A \end{pmatrix}\begin{pmatrix} I & 0 \\ B & I \end{pmatrix}^t = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

Этим завершается доказательство леммы. □

§ 7. Кольцо Витта

Следуя Кнебушу, на множестве всех пространств с внутренним произведением над кольцом R введем следующее отношение эквивалентности (см. также [78]).

7.1. Определение. Пространства с симметрическим внутренним произведением X и X' над кольцом R принадлежат одному *классу Витта*, что записывается $X \sim X'$, если существуют расщепляемые пространства с внутренним произведением S и S', такие, что пространство $X \oplus S$ изоморфно пространству $X' \oplus S'$.

Очевидно, что это отношение является отношением эквивалентности. Кроме того:

7.2. Лемма. *Если* $X \sim X'$ *и* $Y \sim Y'$, *то* $X \oplus Y \sim X' \oplus Y'$ *и* $X \otimes Y \sim X' \otimes Y'$.

Доказательство. Эти утверждения легко следуют из леммы 6.2. □

Вспоминая теперь, что $(X, \beta) \oplus (X, -\beta) \sim 0$ и $\langle 1 \rangle \otimes X \cong X$, получаем следующее утверждение.

7.3. Теорема. *Множество $W(R)$ всех классов Витта пространств с симметрическим внутренним произведением над кольцом R образует коммутативное кольцо с 1, если использовать ортогональную сумму в качестве операции сложения и тензорное произведение в качестве операции умножения.*

Следуя Кнебушу, назовем $W(R)$ *кольцом Витта* кольца R. Используя результат п. 5.4, видим, что любой кольцевой гомоморфизм $R \to R'$ индуцирует кольцевой гомоморфизм $W(R) \to W(R')$. Строение кольца $W(R)$ будет исследовано в следующих главах.

7.4. Лемма. *Если R – локальное кольцо, в котором элемент 2 обратим, то пространства с симметрическими внутренними произведениями над R изоморфны тогда и только тогда, когда они принадлежат одному и тому же классу Витта и имеют один и тот же ранг.*

Доказательство. Это легко следует из теоремы 4.4 и леммы 6.3. □

Глава 2

ПРОСТРАНСТВА С СИММЕТРИЧЕСКИМ ВНУТРЕННИМ ПРОИЗВЕДЕНИЕМ НАД КОЛЬЦОМ Z

В этой главе будет обсуждена задача классификации пространств с внутренним произведением над кольцом $\mathbf{Z}$ целых чисел. Все внешние произведения будут симметрическими. Наше изложение основано на классической теореме Минковского о точках решетки в выпуклом симметричном подмножестве пространства $\mathbf{R}^n$. В первую очередь эта теорема используется для классификации пространств с внутренним произведением ранга $\leqslant 4$ над кольцом $\mathbf{Z}$. С использованием теоремы Хассе – Минковского (доказательство которой мы не приводим) показывается, что неопределенные пространства с внутренним произведением над кольцом $\mathbf{Z}$ полностью определяются своими рангом, типом и сигнатурой (пространство называется *пространством типа* I или *типа* II в зависимости от того, содержит пространство или нет вектор с нечетной нормой). Из этого следует, что кольцо Витта $W(\mathbf{Z})$ изоморфно кольцу $\mathbf{Z}$.

С другой стороны, задача классификации положительно определенных пространств с внутренним произведением чрезвычайно сложна. После обсуждения этой задачи и связанной с ней задачи о плотной упаковке шаров в евклидовом пространстве мы приведем классические результаты о суммах двух или четырех квадратов в кольце $\mathbf{Z}$. Главу завершит краткое изложение работы Зигеля о положительно определенных билинейных формах над кольцом $\mathbf{Z}$.

§ 1. Теорема Минковского о выпуклом теле

Пусть $\mathbf{R}^n$ – пространство строк $x = (x_1, \ldots, x_n)$ из n действительных чисел, наделенное стандартной мерой Лебега $dx_1 \ldots dx_n$.

1.1. Определение. *Решеткой* в пространстве $\mathbf{R}^n$ называется аддитивная подгруппа $L \subset \mathbf{R}^n$, которая аддитивно порождается некоторым базисом $b_1, \ldots, b_n$ действительного векторного пространства $\mathbf{R}^n$.

Выбрав в решетке L некоторый базис $b_1, \ldots, b_n$, мы можем образовать фундаментальную область P, состоящую из всех элементов $\xi_1 b_1 + \ldots + \xi_n b_n$, таких, что $0 \leqslant \xi_i < 1$. Очевидно, что каждая

точка пространства $\mathbf{R}^n$ конгруэнтна по модулю решетки L ровно одной точке области P. Объем (т.е. мера Лебега)

$$\mathrm{vol}(P) = \int_P dx_1 \ldots dx_n$$

может быть отождествлен с объемом тора $\mathbf{R}^n/L$. Этот объем, конечно, равен абсолютной величине определителя матрицы со строками $b_1, \ldots, b_n$ (см., например, [7]). Мы запишем это кратко в виде

$$\mathrm{vol}(\mathbf{R}^n/L) = |\det(b_1, \ldots, b_n)|.$$

Решетка называется *унимодулярной*, если объем тора $\mathbf{R}^n/L$ равен 1.

1.2. Примеры. Очевидно, что $\mathbf{Z}^n$ является решеткой в $\mathbf{R}^n$, для которой $\mathrm{vol}(\mathbf{R}^n/\mathbf{Z}^n) = 1$. Если L и L' — такие решетки, что $L \supset L'$, то очевидно, что индекс $|L/L'|$ конечен и

$$\mathrm{vol}(\mathbf{R}^n/L') = \mathrm{vol}(\mathbf{R}^n/L)\,|L/L'|.$$

Если рассматривать $\mathbf{R}^n$ как евклидово пространство с внутренним произведением $x \cdot y = \Sigma x_i y_i$, то объем $|\det(b_1, \ldots, b_n)|$ может быть также записан в виде $\sqrt{\det(b_i \cdot b_j)} = \sqrt{\det(L)}$. Отметим, что любое пространство с внутренним произведением X над кольцом $\mathbf{Z}$ канонически вкладывается в качестве решетки в действительное пространство с внутренним произведением $\mathbf{R} \otimes X$. Если пространство X положительно определено (т.е. если $x \cdot x > 0$ при $x \neq 0$), то пространство $\mathbf{R} \otimes X$ изоморфно евклидову пространству $\mathbf{R}^n$, а пространство X соответствует унимодулярной решетке в пространстве $\mathbf{R}^n$

Напомним, что подмножество $K \subseteq \mathbf{R}^n$ является *выпуклым*, если из $x, x' \in K$ следует, что $\lambda x + (1 - \lambda)x' \in K$ для всех действительных чисел λ, таких, что $0 \leqslant \lambda \leqslant 1$. Подмножество K называется *симметричным относительно* 0, если из $x \in K$ следует, что $-x \in K$.

1.3. Теорема Минковского. *Пусть K – симметричное относительно 0 выпуклое подмножество в пространстве $\mathbf{R}^n$. Если объем (мера Лебега) множества K превосходит объем фундаментальной области решетки L более, чем в 2^n раз, то множество K содержит ненулевую точку решетки.*

Доказательство. Подмножество K', состоящее из всех элементов вида $\frac{1}{2}x$, $x \in K$, очевидно, удовлетворяет неравенству

$$\mathrm{vol}(K') > \mathrm{vol}(\mathbf{R}^n/L).$$

Следовательно, каноническое отображение $K' \to \mathbf{R}^n/L$, которое локально является вложением, сохраняющим объем, не может

быть взаимно одиозначным. Поэтому в K' должны существовать две различные точки, скажем $\frac{1}{2}x$ и $\frac{1}{2}y$, с одним и тем же образом в $\mathbf{R}^n/L$, т.е.

$$0 \neq \frac{1}{2}x - \frac{1}{2}y \in L.$$

Но точка $\frac{1}{2}(x - y)$ является серединой отрезка, соединяющего точки x и y множества K, и, следовательно, сама принадлежит множеству K. Этим завершается доказательство теоремы. □

Пример. Пусть $D(r)$ обозначает замкнутый диск радиусом r в евклидовом пространстве $\mathbf{R}^n$. Тогда объем диска $D(r)$ равен $\omega_n r^n$, где числа

$$\omega_1 = 2, \quad \omega_2 = \pi, \quad \omega_3 = \frac{4}{3}\pi, \quad \omega_4 = \frac{\pi^2}{2}, \ \ldots$$

могут быть вычислены по индукции с помощью формулы

$$\omega_n = \int_0^{2\pi} \int_0^1 \omega_{n-2} (\sqrt{1 - r^2})^{n-2} r \, dr \, d\vartheta = 2\pi\omega_{n-2}/n.$$

Отсюда следует, что $\omega_n = \pi^{n/2}/(n/2)!$ для четных значений n. Используя гамма-функцию, получаем, что $\omega_n = \pi^{n/2}/\Gamma\left(1 + \frac{1}{2}n\right)$ для любых значений n. Применяя теорему Минковского к диску $D(r)$, приходим к следующему утверждению.

1.4. Следствие. *Если* $r^n \geqslant (2^n/\omega_n)\,\mathrm{vol}(\mathbf{R}^n/L)$, *то диск* $D(r)$ *содержит ненулевую точку решетки.*

Доказательство. Если число r^n строго больше $(2^n/\omega_n) \times \mathrm{vol}(\mathbf{R}^n/L)$, то утверждение непосредственно вытекает из теоремы 1.3. Если же имеет место равенство, то заметим, что для любого $\epsilon > 0$ диск $D(r + \epsilon)$ содержит ненулевую точку решетки. Однако компактное множество $D(r + \epsilon)$ может содержать только конечное число ненулевых точек решетки. Следовательно, ближайшая к началу координат точка должна лежать в $D(r)$.

Полагая r_0 равным корню n-й степени из $(2^n/\omega_n)\,\mathrm{vol}(\mathbf{R}^n/L)$, получаем следующее

1.5. Следствие. *Любая решетка* $L \subset \mathbf{R}^n$ *содержит такую точку* $(x_1, \ldots, x_n)$, *что*

$$0 < x_1^2 + \ldots + x_n^2 \leqslant r_0^2 = 4(\omega_n^{-1}\,\mathrm{vol}(\mathbf{R}^n/L))^{2/n}.$$

В частности, любая унимодулярная решетка в пространстве $\mathbf{R}^n$

содержит такую точку, что

$$0 < x_1^2 + \ldots + x_n^2 \leqslant 4/(\omega_n)^{2/n}.$$

По формуле Стирлинга эта верхняя оценка $4/(\omega_n)^{2/n}$ при $n \to \infty$ асимптотически стремится к $2n/\pi e$ (см. § 7). В следующей таблице приводятся значения $4/(\omega_n)^{2/n}$, округленные до сотых.

n	1	2	3	4	5	6
$4/(\omega_n)^{2/n}$	1	1,27	1,54	1,80	2,06	2,31

n	7	8	9	10	11
$4/(\omega_n)^{2/n}$	2,57	2,82	3,07	3,32	3,56

Отметим, в частности, что $4/(\omega_n)^{2/n} < 2$ при $n \leqslant 4$.

З а м е ч а н и е. В более общем случае для любого положительного целого числа n имеет место следующая оценка:

$$4/(\omega_n)^{2/n} < 1 + \frac{1}{4}\, n.$$

Для $n < 12$ это можно проверить по таблице, а для $n \geqslant 12$ можно доказать следующим образом. Полагая $A_n = \left(1 + \frac{1}{4}\, n\right)^{n/2} \omega_n / 2^n$ и $n = 2u - 2$, имеем

$$A_n / A_{n-2} = \frac{\pi}{8}\, \frac{u^2}{u^2 - 1} \left(1 + \frac{1}{u}\right)^u,$$

где выражение $\frac{\pi}{8}\left(1 + \frac{1}{u}\right)^u$ монотонно возрастает при $u \geqslant 2$ и больше 1 при $u = 7$. По индукции $A_n > A_{n-2} > 1$ при $n \geqslant 12$. □

Некоторые нетривиальные примеры будут приведены в § 6. Более точная верхняя граница чисел

$$\min_{\substack{x \in L \\ x \neq 0}} (x_1^2 + \ldots + x_n^2)$$

будет описана в § 7.

Имеет место важный качественный результат, вытекающий из утверждения 1.5.

1.6. Л е м м а (Эйзенштейн, Эрмит). *Над кольцом* $\mathbf{Z}$ *для каждого целого числа* n *существует лишь конечное число классов изоморфных положительно определенных пространств с внутренним произведением ранга* n.

Действительно, если даны положительные целые числа n и d, то существует лишь конечное число различных положительно определенных пространств с билинейной формой над $\mathbf{Z}$, имеющих ранг n и определитель d (см. п. 7.4). Доказательство этого факта можно провести индукцией по n по следующей схеме. Очевидно, что любое такое пространство может быть изометрично вложено в качестве решетки L в пространство $\mathbf{R}^n$ с евклидовым внутренним произведением. Объем фундаментальной области решетки L будет равен $\sqrt{d}$. Используя следствие 1.5, получаем, что в любой такой решетке L содержится вектор x, для которого

$$0 < x \cdot x \leqslant c(n, d) = 4\sqrt[n]{d/\omega_n^2}.$$

Пусть L_0 – подрешетка в L, состоящая из всех таких $y \in L$, что

$$x \cdot y \equiv 0 \pmod{x \cdot x}.$$

Тогда ее индекс не превосходит $x \cdot x$ и она разлагается в ортогональную сумму подгруппы, порожденной элементом x и ее ортогонального дополнения. В силу индуктивного предположения для подрешетки L существует, с точностью до изоморфизма, лишь конечное число возможностей. □

Аналогичные рассуждения могут быть проведены и для неопределенных билинейных форм.

§ 2. Пространства с внутренним произведением над кольцом Z, ранг которых не превосходит 4

2.1. Лемма. *Если* L *– пространство с внутренним произведением ранга* n *над кольцом* $\mathbf{Z}$, *то оно содержит вектор* $x \neq 0$, *для которого*

$$|x \cdot x| \leqslant 4/(\omega_n)^{2/n}.$$

В частности, если $n \leqslant 4$, *то пространство* L *содержит вектор* $x \neq 0$, *такой, что* $|x \cdot x| < 2$.

Д о к а з а т е л ь с т в о. Отметим, что пространство L изометрично вкладывается в качестве решетки в действительное пространство с внутренним произведением $\mathbf{R} \otimes L$. Если пространство L положительно определено, то мы можем отождествить $\mathbf{R} \otimes L$ с n-мерным евклидовым пространством и непосредственно применить следствие 1.5. В любом случае, можно выбрать такой ортогональный базис $e_1, \ldots, e_n$ в $\mathbf{R} \otimes L$, что $e_i \cdot e_i = \pm 1$. Используя этот базис для отождествления пространства $\mathbf{R} \otimes L$ с декартовым пространст-

вом $\mathbf{R}^n$ и для введения элемента объема $dx_1 \ldots dx_n$, отметим, что объем тора $(\mathbf{R} \otimes L)/L$ равен 1. Если $b_1, \ldots, b_n$ – базис решетки L, то из матричного равенства

$$(b_i \cdot b_j) = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \begin{pmatrix} \pm 1 & & \\ & \ddots & \\ & & \pm 1 \end{pmatrix} (b_1^t \ldots b_n^t)$$

следует, что определитель $\det(b_i \cdot b_j)$, равный ± 1, совпадает с $\pm \det(b_1, \ldots, b_n)^2$.

Следовательно, в силу следствия 1.5, существует элемент решетки $x = x_1 e_1 + \ldots + x_n e_n \neq 0$, для которого

$$x_1^2 + \ldots + x_n^2 \leqslant 4/(\omega_n)^{2/n}.$$

Отсюда, очевидно, следует, что

$$|x \cdot x| = |\pm x_1^2 \pm \ldots \pm x_n^2| \leqslant 4/(\omega_n)^{2/n}.$$

Поскольку $4/(\omega_n)^{2/n} < 2$ при $n \leqslant 4$, то этим самым доказательство леммы завершено. □

2.2. Т е о р е м а. *Любое пространство с внутренним произведением над кольцом* $\mathbf{Z}$, *ранг которого не превосходит* 4, *либо обладает ортогональным базисом и, следовательно, изоморфно сумме экземпляров пространств* $\langle 1 \rangle$ *и* $\langle -1 \rangle$, *либо является "гиперболическим" пространством с матрицей внутреннего произведения вида* $\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$.

Д о к а з а т е л ь с т в о проведем индукцией. Утверждение заведомо верно в случае ранга 1. Предположим теперь, что ранг равен $n > 1$. Если существует вектор x в пространстве X, для которого $x \cdot x = \pm 1$, то очевидно, что

$$X \cong \langle \pm 1 \rangle \oplus X'.$$

Если подпространство X' имеет ортогональный базис, то мы завершили доказательство. Если же X' – гиперболическое подпространство, порожденное элементами y и z, для которых $y \cdot y = z \cdot z = 0$, $y \cdot z = 1$, то векторы $x + y$, $x \mp z$ и $x + y \mp z$ образуют требуемый ортогональный базис.

С другой стороны, предположим, что мы смогли найти вектор $x_1 \neq 0$, для которого $x_1 \cdot x_1 = 0$. Без потери общности можно считать, что x_1 – неделимый вектор и, таким образом, x_1 является элементом базиса $x_1, \ldots, x_n$ в пространстве X. Пусть $y_1, \ldots, y_n$ – дуальный базис. Тогда порожденное векторами x_1 и y_1 подпространство имеет матрицу внутреннего произведения вида $\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}$. Имеются две возможности.

Случай 1. Если число $a = y_1 \cdot y_1$ четно, то подпространство, порожденное элементами x_1 и y_1, гиперболическое с базисом из элементов x_1 и $y_1 - \frac{1}{2}ax_1$, которые ортогональны самим себе. Относительно нового базиса внутреннее произведение имеет матрицу $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Таким образом, пространство X изоморфно ортогональной сумме

$$\left\langle\!\!\left\langle \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \right\rangle\!\!\right\rangle \oplus X'.$$

Применение индуктивного предположения завершает доказательство.

Случай 2. Если число $a = 2k + 1$ нечетно, то векторы

$$x' = y_1 - kx_1, \quad y' = y_1 - (k+1)x_1$$

взаимно ортогональны и имеют матрицу внутреннего произведения $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Таким образом, опять можем отщепить ортогональное слагаемое и продолжить доказательство по индукции.

Так как в силу леммы 2.1 всегда существует вектор $x \in X$, для которого либо $x \cdot x = \pm 1$, либо $x \cdot x = 0$, то этим завершается доказательство теоремы. □

2.3. Замечание. Теорема 2.2 в действительности верна для значений ранга 5, 6 и 7. Как мы увидим в § 6, она неверна, если ранг больше или равен 8.

§ 3. Теорема Хассе–Минковского и теорема Мейера

Этот параграф посвящен основной теореме алгебраической теории чисел, которую мы не будем доказывать. Пусть дано пространство с внутренним произведением X над полем рациональных чисел $\mathbf{Q}$ и нам надо найти ненулевой вектор x, такой, что $x \cdot x = 0$. Выбирая ортогональный базис, для которого

$$X \cong \langle a_1 \rangle \oplus \ldots \oplus \langle a_n \rangle,$$

мы видим, что задача эквивалентна нахождению нетривиального решения уравнения

$$a_1\xi_1^2 + \ldots + a_n\xi_n^2 = 0.$$

3.1. Теорема (Хассе – Минковского). *Уравнение* $a_1\xi_1^2 + \ldots + a_n\xi_n^2 = 0$ *с ненулевыми рациональными коэффициентами*

имеет нетривиальное рациональное решение тогда и только тогда, когда:

1) *оно имеет нетривиальное действительное решение*;

2) *для каждого простого числа p оно имеет нетривиальное решение в поле p-адических чисел* $\mathbf{Q}_p$.

Доказательства приведены, например, в [9], [61] и [66]. Набросок доказательства дается в приложении 3.

3.2. Следствие (теорема Мейера). *Неопределенное пространство с внутренним произведением ранга* $n \geqslant 5$ *над полем* $\mathbf{Q}$ *всегда содержит вектор* $x \neq 0$, *для которого* $x \cdot x = 0$.

(Здесь термин "неопределенное" означает, что норма $x \cdot x$ принимает как положительные, так и отрицательные значения. Ограничение $n \geqslant 5$ существенно. Например, уравнение $\xi_1^2 + \xi_2^2 + \xi_3^2 - 7\xi_4^2 = 0$ не имеет нетривиальных рациональных решений. Это можно легко проверить, если избавиться от знаменателей, а затем привести уравнение по модулю 8).

Для вывода следствия из теоремы нам требуется только показать, что уравнение

$$a_1\xi_1^2 + \ldots + a_5\xi_5^2 = 0$$

имеет нетривиальное p-адическое решение. Мы воспользуемся следующими леммами, на которые будем также ссылаться и впоследствии.

3.3. Лемма. *Если* F – *конечное поле, то для любых элементов* $a, b, c \in F^*$ *уравнение*

$$a\xi^2 + b\eta^2 = c$$

имеет решение в F.

Доказательство будет основываться на принципе Дирихле. Пусть q – число элементов поля F. Можно считать что число q нечетное, поскольку в противном случае уравнение $a\xi^2 = c$ уже имеет решение.

Отметим, что поскольку переменная ξ пробегает элементы поля F, то $a\xi^2$ принимает $\frac{1}{2}(q+1)$ различных значений. Аналогично, выражение $c - b\eta^2$ принимает $\frac{1}{2}(q+1)$ различных значений. Поскольку

$$\frac{1}{2}(q+1) + \frac{1}{2}(q+1) > q,$$

отсюда следует, что по крайней мере одно из значений выражения $a\xi^2$ должно равняться одному из значений выражения $c - b\eta^2$. Следовательно, $a\xi^2 + b\eta^2 = c$, что и требовалось доказать. □

3.4. Л е м м а. *Пусть p – нечетное простое число, u, v, w – обратимые элементы кольца целых p-адических чисел $\mathbf{Z}_p$. Тогда уравнение $u\xi^2 + v\eta^2 + w\zeta^2 = 0$ имеет нетривиальное решение $\xi, \eta, \zeta \in \mathbf{Z}_p$.*

Д о к а з а т е л ь с т в о. Поскольку p нечетно, то любое число, сравнимое с 1 по модулю p, является квадратом p-адического числа. Действительно, пусть через U_k обозначена подгруппа группы $\mathbf{Z}_p^*$, состоящая из всех обратимых элементов, конгруэнтных 1 по модулю $p^k\mathbf{Z}_p$. Тогда факторгруппа U_1/U_k является конечной абелевой группой нечетного порядка p^{k-1}. Таким образом, ясно, что любой элемент группы U_1 имеет единственный квадратный корень по модулю подгруппы U_k. Предел этих квадратных корней по модулю подгрупп U_k при $k \to \infty$ дает квадратный корень в подгруппе U_1.

Теперь для данных обратимых чисел u, v, w по лемме 3.3 можно найти p-адические целые числа ξ и η, для которых

$$u\xi^2 + v\eta^2 \equiv -w \pmod{p},$$

или, другими словами,

$$-(u\xi^2 + v\eta^2)/w \equiv 1 \pmod{p}.$$

Полагая

$$\zeta = \sqrt{-(u\xi^2 + v\eta^2)/w},$$

получаем, что $u\xi^2 + v\eta^2 + w\zeta^2 = 0$, что и требовалось в утверждении леммы. □

Д о к а з а т е л ь с т в о с л е д с т в и я 3.2. Если даны числа $a_1, \ldots, a_5 \in \mathbf{Q}_p$, то можно считать, что каждое число a_i является либо целым обратимым p-адическим числом, либо целым обратимым p-адическим числом, умноженным на p. Если по крайней мере три числа a_i обратимы, то доказательство завершается с помощью леммы 3.4. В противном случае, по крайней мере три числа a_i равны целым обратимым p-адическим числам, умноженным на p. Из леммы 3.4 опять следует существование p-адического решения.

При $p = 2$ доказательство аналогично, но необходимо использовать сравнение по модулю 8, так как сравнимость с 1 по модулю 8 обеспечивает существование квадратного корня. После перестановки коэффициентов и домножения на константу можно считать, что: $a_1 = 1$; a_2 и a_3 – обратимые p-адические числа; a_4 и a_5 делятся по крайней мере на 2. Затем нетрудно проверить, что уравнение

$$a_2\xi_2^2 + a_3\xi_3^2 + a_4\xi_4^2 + a_5\xi_5^2 \equiv -1 \pmod{8}$$

имеет решение, и провести те же рассуждения, что и выше. □

§ 4. Неопределенные пространства над кольцом Z

4.1. Лемма. *Каждое неопределенное пространство с внутренним произведением над кольцом* Z *содержит такой ненулевой вектор* x, *что* $x \cdot x = 0$.

Доказательство. Если ранг пространства больше или равен 5, то утверждение следует из теоремы Мейера (3.5). Если же ранг не превосходит 4, то оно следует из теоремы 2.2. □

Замечание. Проведенные рассуждения, конечно, опираются на теорему Хассе – Минковского, которая не доказывалась. Другое, замкнутое в себе доказательство будет дано в гл. 4.

4.2. Определение. Пространство с внутренним произведением над кольцом Z имеет *тип* I, если оно содержит вектор x, для которого $x \cdot x$ нечетно, и имеет *тип* II, если оно не содержит такого вектора.

Очевидно, что пространство X имеет тип II в том и только в том случае, если квадратичная функция $q(x) = x \cdot x/2$ принимает значения в кольце Z. Таким образом, пространствами с внутренним произведением типа II являются в точности те, которые получаются из квадратичных пространств с внутренним произведением над кольцом Z (см. приложение 1).

4.3. Теорема. *Каждое неопределенное пространство с внутренним произведением типа* I *над кольцом* Z *обладает ортогональным базисом и, следовательно, изоморфно ортогональной сумме экземпляров пространств* $\langle 1 \rangle$ *и* $\langle -1 \rangle$.

(Отсюда следует, что такое пространство однозначно определяется своими рангом и сигнатурой. Это утверждение стоит сравнить с последующим обсуждением.)

Доказательство теоремы 4.3 проведем по индукции. Утверждение уже доказано для малых значений ранга. Выберем такой вектор $x_1 \neq 0$, что $x_1 \cdot x_1 = 0$. Без потери общности можно считать, что элемент x_1 неделим и, следовательно, является частью базиса $x_1, \ldots, x_n$ пространства X. Пусть $y_1, \ldots, y_n$ – дуальный базис. Тогда $x_1 \cdot y_1 = 1$.

По предположению, существует вектор y, норма $y \cdot y$ которого нечетная. Следовательно, один из базисных векторов y_k должен иметь нечетную норму. Выберем подпространство $X_0 \subset X$ следующим образом. Если норма $y_1 \cdot y_1$ нечетная, то в качестве подпространства X_0 возьмем подпространство, порожденное векторами x_1 и y_1. Если же норма $y_1 \cdot y_1$ четная, то в качестве подпространства X_0 возьмем подпространство, порожденное векторами x_1 и $y_1 + y_k$, где k выбрано так, что

$$(y_1 + y_k) \cdot (y_1 + y_k) \equiv y_k \quad y_k \equiv 1 \pmod 2.$$

Тогда пространство X_0 имеет матрицу внутреннего произведения вида

$$\begin{pmatrix} 0 & 1 \\ 1 & \text{нечетное} \end{pmatrix}.$$

Как и в случае 2 доказательства теоремы 2.2, мы видим, что

$$X_0 \cong \langle 1 \rangle \oplus \langle -1 \rangle.$$

Очевидно, что пространство X разлагается в ортогональную прямую сумму

$$X \cong X_0 \oplus X_0^{\perp} \cong \langle 1 \rangle \oplus \langle -1 \rangle \oplus X_0^{\perp}.$$

Выберем ± 1 так, чтобы пространство $\langle \pm 1 \rangle \oplus X_0^{\perp}$ было неопределенным. Тогда по индуктивному предположению пространство $\langle \pm 1 \rangle \oplus X_0^{\perp}$ обладает ортогональным базисом. Следовательно, таково же и пространство X, что завершает доказательство теоремы. □

Сигнатура пространства с внутренним произведением X над кольцом $\mathbf{Z}$ определяется следующим образом. Выберем ортогональный базис $b_1, \ldots, b_n$ для рационального пространства с внутренним произведением $\mathbf{Q} \otimes X$. Тогда сигнатура

$$\sigma(X) = \sigma(\mathbf{Q} \otimes X) \in \mathbf{Z}$$

является разностью между числом базисных элементов b_i, для которых $b_i \cdot b_i > 0$, и числом базисных элементов b_j, для которых $b_j \cdot b_j < 0$. В силу теоремы Якоби – Сильвестра об инерции сигнатура является инвариантом (см. п. 2.5 гл. 3). Отметим, что $\sigma(X \oplus Y) = \sigma(X) + \sigma(Y)$.

Теперь кольцо Витта $W(\mathbf{Z})$ может быть вычислено следующим образом.

4.4. Следствие. *Кольцо $W(\mathbf{Z})$ канонически изоморфно кольцу $\mathbf{Z}$.*

В действительности, мы покажем, что соответствие $X \mapsto \sigma(X)$ дает кольцевой изоморфизм $W(\mathbf{Z}) \to \mathbf{Z}$. (Сравните как с п. 2.6 гл. 3, так и с § 2 гл. 4.)

Если S – расщепляемое пространство с внутренним произведением над кольцом $\mathbf{Z}$, то сигнатура $\sigma(S)$ равна нулю. В силу п. 6.3 гл. 1 рациональное пространство с внутренним произведением $\mathbf{Q} \otimes S$ изоморфно сумме копий пространства $\langle 1 \rangle \oplus \langle -1 \rangle$, следовательно,

$$\sigma(S) = \sigma(\mathbf{Q} \otimes S) = 0.$$

Отсюда легко выводится, что соответствие $X \mapsto \sigma(X)$ задает аддитивный гомоморфизм из кольца $W(\mathbf{Z})$ в кольцо $\mathbf{Z}$.

Этот гомоморфизм сюръективен, поскольку $\sigma(\langle 1\rangle) = 1$. Он имеет нулевое ядро, поскольку если $\sigma(X) = 0$, то, в силу теоремы 4.3, сумма $X \oplus \langle 1\rangle \oplus \langle -1\rangle$ изоморфна сумме экземпляров пространства $\langle 1\rangle \oplus \langle -1\rangle$ и, следовательно,

$$X \sim X \oplus \langle 1\rangle \oplus \langle -1\rangle \sim 0.$$

Таким образом, два пространства с внутренним произведением над кольцом $\mathbf{Z}$ *имеют одну и ту же сигнатуру тогда и только тогда, когда они принадлежат одному классу Витта.* Поскольку из равенства $\sigma(\langle 1\rangle) = 1$ следует, что биекция $W(\mathbf{Z}) \to \mathbf{Z}$ является кольцевым изоморфизмом, то этим завершается доказательство. □

§ 5. Пространства типа II

Сначала докажем следующее утверждение.

5.1. Теорема. *Сигнатура пространства с внутренним произведением типа* II *делится на* 8.

В § 6 будет описан пример пространства, имеющего сигнатуру, равную 8.

Для доказательства теоремы 5.1, рассмотрим сначала произвольное пространство с внутренним произведением над кольцом $\mathbf{Z}$. Элемент $u \in X$ назовем *характеристическим*, если

$$u \cdot x \equiv x \cdot x \pmod 2$$

для любого элемента x.

5.2. Лемма (ван дер Блий). *Любое пространство с внутренним произведением* X *над кольцом* $\mathbf{Z}$ *содержит характеристический элемент. Более того, если* $u \in X$ *– характеристический элемент, то*

$$u \cdot u \equiv \sigma(X) \pmod 8.$$

Доказательство. Образуем индуцированное пространство с внутренним произведением $X \otimes \mathbf{F}_2 = X/2X$ над полем из двух элементов. Через $\overline{x}$ обозначим образ элемента x в пространстве $X/2X$. Тогда ясно, что внутреннее произведение $x \cdot y$ на пространстве X индуцирует $\mathbf{F}_2$-значное внутреннее произведение

$$\overline{x} \cdot \overline{y} = (\text{класс элемента } x \cdot y \text{ по модулю } 2)$$

на пространстве $X/2X$.

Функция $\overline{x} \mapsto \overline{x} \cdot \overline{x}$ из пространства $X/2X$ в поле $\mathbf{F}_2$ является $\mathbf{F}_2$-линейной, следовательно, существует единственный элемент $\overline{u} \in X/2X$, удовлетворяющий уравнению $\overline{u} \cdot \overline{x} = \overline{x} \cdot \overline{x}$ для любого элемента $\overline{x}$. Выбирая любой прообраз $u \in X$ элемента $\overline{u}$, мы получаем требуемый характеристический элемент.

Заметим далее, что класс числа $u \cdot u$ по модулю 8 является инвариантом пространства X, поскольку если u' – другой характеристический элемент, то $u' = u + 2x$ и, следовательно,

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

Ясно, что инвариант $u \cdot u$ аддитивен относительно прямых сумм. Отметим, что $u \cdot u \equiv 1 \pmod 8$ для пространства с внутренним произведением $\langle 1 \rangle$, и что $u \cdot u \equiv -1 \pmod 8$ для пространства $\langle -1 \rangle$. Таким образом, мы видим, что для ортогональной суммы p экземпляров пространства $\langle 1 \rangle$ и q экземпляров пространства $\langle -1 \rangle$ значение $u \cdot u$ сравнимо с сигнатурой $\sigma = p - q$ по модулю 8.

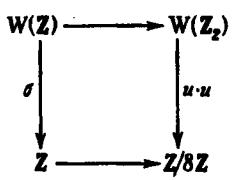
Для любого пространства с внутренним произведением X ортогональная сумма $X \oplus \langle 1 \rangle \oplus \langle -1 \rangle$ является неопределенным пространством типа I и, следовательно, изоморфна сумме экземпляров пространств $\langle 1 \rangle$ и $\langle -1 \rangle$. Поскольку ассоциированный с пространством $X \oplus \langle 1 \rangle \oplus \langle -1 \rangle$ инвариант $u \cdot u \pmod 8$ есть класс вычетов $\sigma(X \oplus \langle 1 \rangle \oplus \langle -1 \rangle) = \sigma(X) \pmod 8$, а ассоциированный с пространством $\langle 1 \rangle \oplus \langle -1 \rangle$ инвариант равен нулю, то этим завершается доказательство леммы. □

Доказательство теоремы 5.1. Если X – пространство типа II, то можно выбрать $u = 0$. Следовательно,

$$\sigma(X) \equiv 0 \cdot 0 \pmod 8,$$

что завершает доказательство теоремы. □

Замечание 1. Инвариант $u \cdot u$ по модулю 8 определен также для пространств с внутренним произведением над кольцом 2-адических чисел $\mathbf{Z}_2$. Он порождает гомоморфизм из кольца Витта $W(\mathbf{Z}_2)$ в кольцо $\mathbf{Z}/8\mathbf{Z}$. Очевидно, что диаграмма



является коммутативной диаграммой кольцевых гомоморфизмов.

Замечание 2. Отличная от приведенной и весьма интригующая формула для сигнатуры по модулю 8 была недавно дана Дж. Милгрэмом в связи с одной задачей в топологии. Пусть V – любое пространство с внутренним произведением сигнатуры σ над рациональными числами и пусть L – решетка в V, настолько малая, что $l \cdot l \in 2\mathbf{Z}$ для любого $l \in L$. Если через $L^{\#} \subset V$ обозначить "двойственную решетку", состоящую из всех элементов $v \in V$, для которых $v \cdot L \subset \mathbf{Z}$, и если $v_1, \ldots, v_d$ – полный набор представите-

лей смежных классов решетки $L^{\#}$ по модулю решетки L, то Милгрэм доказал, что

$$\exp(2\pi i\sigma/8) = \sum_{j=1}^{d} \exp(\pi i\, v_j \cdot v_j)/\sqrt{d}.$$

Дальнейшие подробности можно найти в приложенни 4. Пусть, например, решетка L унимодулярна. Тогда $L = L^{\#}$ и $d = 1$, так что правая часть равенства равна 1 и отсюда опять же следует, что $\sigma \equiv 0 \pmod 8$. Это рассуждение блнзко к исходному доказательству в [8].

В заключение параграфа докажем следующее.

5.3. Т е о р е м а. *Если два неопределенных пространства с внутренним произведением над кольцом* $\mathbf{Z}$ *имеют одни и те же ранг, тип и сигнатуру, то они изоморфны.*

Для типа I зто было доказано в § 4, так что нам осталось рассмотреть только тип II.

Д о к а з а т е л ь с т в о (следует Серру [66]). Сначала рассмотрим следующую конструкцию. Если дано пространство с внутренним произведением X типа I, то можно образовать подмножество X_0, состоящее из всех элементов x, для которых $x \cdot x \equiv 0 \pmod 2$. Очевидно, это подрешетка индекса 2 в решетке X. Нам хотелось бы построить пространство с внутренним произведением типа II, которое также содержало бы множество X_0 в качестве подрешетки индекса 2. Если такое пространство существует, то оно, очевидно, должно содержаться в "дуальной решетке",

$$X_0^{\#} \subset \mathbf{Q} \otimes X,$$

состоящей из всех векторов $x^{\#}$ векторного пространства $\mathbf{Q} \otimes X$, которые для любого вектора $x \in X_0$ удовлетворяют условию

$$x^{\#} \cdot x \in \mathbf{Z}.$$

(Можно сравнить с § 3 гл. 4.) Поскольку $X_0^{\#}$ содержит X_0 в качестве подрешетки индекса 4, то существует не более трех различных решеток, строго содержащих решетку X_0 и строго содержащихся в решетке $X_0^{\#}$. Одной из них является сама решетка X. Мы будем интересоваться двумя другими.

В качестве примера давайте применим эту конструкцию к пространству с внутренним произведением $W = \langle 1 \rangle \oplus \langle -1 \rangle$ с ортогональным базисом e_1, e_2. Проверка показывает, что решетка W_0 имеет базис $e_1 + e_2, e_1 - e_2$ и что $W_0^{\#}$ имеет двойственный базис $\frac{1}{2}(e_1 - e_2), \frac{1}{2}(e_1 + e_2)$. В этом случае имеются три решетки, лежащие между W_0 и $W_0^{\#}$. Одной из них является решетка W, а две

другие решетки, очевидно, изоморфны гиперболической плоскости H.

Теперь рассмотрим сумму $Y \oplus W = Y \oplus \langle 1 \rangle \oplus \langle -1 \rangle$, где Y – произвольное пространство с внутренним произведением типа II. Тогда подпространство $(Y \oplus W)_0$ векторов четной нормы равно $Y \oplus W_0$ и, следовательно, $(Y \oplus W)_0^{\#} = Y \oplus W_0^{\#}$. Ясно, что существуют три решетки, лежащие между $(Y \oplus W)_0$ и $(Y \oplus W)_0^{\#}$. Одной из них является решетка $Y \oplus W$, а каждая из двух других изоморфна $Y \oplus H$.

Пусть Y' – другое пространство с внутренним произведением типа II, имеющее те же ранг, сигнатуру, что и пространство Y. Тогда, в силу теоремы 4.3,

$$Y \oplus W \cong Y' \oplus W.$$

Применяя в обе стороны описанную выше конструкцию, получаем, что $Y \oplus H \cong Y' \oplus H$.

Но простые рассуждения показывают, что любое неопределенное пространство с внутренним произведением типа II изоморфно ортогональной сумме $Y \oplus H$ для некоторого пространства Y (см. § 2 и 4). Это завершает доказательство. □

§ 6. Задача классификации для положительно определенных пространств

Сначала опишем некоторые примеры положительно определенных пространств с внутренним произведением над кольцом $\mathbf{Z}$. Пусть через $\mathbf{R}^{4m}$ обозначено евклидово пространство с ортогональным базисом $e_1, \ldots, e_{4m}$.

6.1. Л е м м а. *Векторы* $e_i + e_j$ *и* $\frac{1}{2}(e_1 + \ldots + e_{4m})$ *порождают решетку* $\Gamma_{4m} \subset \mathbf{R}^{4m}$, *являющуюся пространством с внутренним произведением над кольцом* $\mathbf{Z}$.

Д о к а з а т е л ь с т в о. Пусть L_0 – подрешетка индекса 2, порожденная векторами $e_i + e_j$. Очевидно, что решетка L_0 может рассматриваться также как подрешетка индекса 2 в порожденной векторами $e_1, \ldots, e_{4m}$ решетке. Следовательно, фундаментальная область решетки Γ_{4m} имеет объем 1. Проверка показывает, что внутреннее произведение любых двух элементов решетки Γ_{4m} является целым числом, что завершает доказательство. □

(Решетка Γ_{4m} может быть явно описана как множество всех таких линейных комбинаций $\xi_1 e_1 + \ldots + \xi_{4m} e_{4m}$, что $2\xi_i \in \mathbf{Z}$, $\xi_1 \equiv \xi_2 \equiv \ldots \equiv \xi_{4m} \pmod{\mathbf{Z}}$ и $\xi_1 + \ldots + \xi_{4m} \equiv 0 \pmod{2\mathbf{Z}}$.)

6.2. Л е м м а. *Построенное пространство с внутренним произведением* Γ_{4m} *имеет тип* I *при нечетном* m *и тип* II *при четном* m.

Доказательство. Поскольку каждый из векторов $e_i + e_j$ имеет норму 2, то из этого легко следует утверждение леммы. □

Решетки $\Gamma_8, \Gamma_{16}, \Gamma_{24}, \ldots$ дают примеры положительно определенных пространств с внутренним произведением типа II с сигнатурами 8, 16, 24, ...

Предпримем теперь попытку продвинуться в исследовании строения множества всех положительно определенных пространств с внутренним произведением над кольцом $\mathbf{Z}$.

6.3. Определение. Пространство с внутренним произведением X называется *неразложимым,* если оно не разлагается в ортогональную сумму двух нетривиальных подпространств.

6.4. Теорема (Эйхлер). *Каждое положительно определенное пространство с внутренним произведением над кольцом* $\mathbf{Z}$ *однозначно разлагается в ортогональную сумму неразложимых пространств.*

Доказательство (см. [36]). Вектор $x \neq 0$ из пространства X назовем *минимальным,* если он не может быть выражен в виде суммы $y + z$ двух векторов y и z строго меньшей длины (т.е. таких векторов, что $y \cdot y < x \cdot x$ и $z \cdot z < x \cdot x$). Очевидно, что после конечного числа шагов процедура представления вектора в виде суммы более коротких векторов должна завершиться. Следовательно, пространство X порождается множеством своих минимальных векторов. Отметим, что если пространство X разлагается в ортогональную сумму $X_1 \oplus X_2$, то каждый минимальный вектор пространства X должен принадлежать либо подпространству X_1, либо подпространству X_2.

Скажем, что минимальные вектора x и x' *эквивалентны,* если существует конечная последовательность $x = x_0, x_1, \ldots, x_k = x'$ минимальных векторов, для которых $x_{i-1} \cdot x_i \neq 0$ при $1 \leqslant i \leqslant k$. Тогда каждый класс эквивалентности порождает подпространство в пространстве X. Ясно, что пространство X является ортогональной прямой суммой построенных подпространств. Отметим, что это разложение определено однозначно, чем завершено доказательство теоремы. □

Заметим, что описанное выше построение легко выполнить практически. Приведем пример, подробное рассмотрение которого предоставляется читателю.

6.5. Предложение. *При* $m \geqslant 2$ *пространство* Γ_{4m} *неразложимо. Минимальными векторами в пространстве* Γ_{4m} *являются все вектора вида* $\pm e_i \pm e_j$ *или* $\frac{1}{2}(\pm e_1 \pm \ldots \pm e_{4m})$ *и только они.*

Конечно, пространство Γ_4 не является неразложимым, поскольку, в силу теоремы 2.2, каждое положительно определенное прост-

ранство ранга 4 над кольцом $\mathbf{Z}$ должно быть изоморфно пространству $\langle 1\rangle \oplus \langle 1\rangle \oplus \langle 1\rangle \oplus \langle 1\rangle$.

Замечание 1. Кнезер нашел все неразложимые пространства, ранг которых не превосходит 16. Он показал, что кроме описанных пространств существует по одному дополнительному неприводимому пространству (типа I) в каждой из размерностей 14, 15, 16. Однако едва ли можно надеяться продвинуться далеко вперед в вычислениях, поскольку с увеличением ранга число различных пространств очень быстро растет. Например, при рассмотрении только положительно определенных пространств типа II получается следующая таблица. (Сравните с обсуждением, следующим за теоремой 9.7, и с заключительным замечанием в приложении 5, а также с [66, с.93].)

Размерность	8	16	24	32	40
Число различных пространств	1	2	24	$\geqslant 10^7$	$\geqslant 10^{51}$

Замечание 2. Два неизоморфных пространства $\Gamma_8 \oplus \Gamma_8$ и Γ_{16} в размерности 16 обладают следующими замечательными свойствами. Для каждого положительного целого числа k число решений уравнения $x \cdot x = 2k$ при $x \in \Gamma_8 \oplus \Gamma_8$ в точности равно числу решений того же уравнения при $x \in \Gamma_{16}$. (См. [17], [66].) В любом случае число решений равно $480 \sum_{d \mid k} d^7$.

Замечание 3. Впервые открытая А.Н. Коркиным и Е.И. Золотаревым в 1873 г.[1]) решетка Γ_8 встречается также при изучении исключительной группы Ли E_8. Эта решетка более симметрична, чем высшие решетки Γ_{4m}, в следующем смысле. Все минимальные векторы решетки Γ_8 имеют одну и ту же длину и, в действительности, группа автоморфизмов решетки Γ_8 транзитивно переставляет 240 минимальных векторов. Факторгруппа группы, состоящей из сохраняющих ориентацию автоморфизмов, по ее центру является простой группой порядка $174\,182\,400 = 2^{12} \cdot 3^5 \cdot 5^2 \cdot 7$ (см. [12, с. 221, 265]).

Замечание 4. Эта решетка в размерности 8 имеет чрезвычайно интересный аналог, открытый в 1967 г. Джоном Личем. Решетка Лича является положительно определенным пространством с внутренним произведением типа II с тем свойством, что $x \cdot x \geqslant 4$ при любом $x \neq 0$ (см. приложение 5). Группа автоморфизмов ре-

[1]) Ее существование было неконструктивно доказано Смитом в 1867 г.

шетки L транзитивно переставляет 196 560 минимальных векторов, а факторгруппа этой группы автоморфизмов по ее центру является простой группой порядка $4\,157\,776\,806\,543\,360\,000 = 2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$ ([38–40]).

Неизвестно, существуют ли такие симметричные решетки в более высоких размерностях. Было бы естественным искать следующую решетку в размерности 48, поскольку теория модулярных форм ([66, с. 168–175]) указывает на то, что пространство с внутренним произведением типа II, для которого $x \cdot x \geqslant 6$ при любом $x \neq 0$, должно иметь размерность не менее 48. (Интересно отметить, что $8 = 3^2 - 1$, $24 = 5^2 - 1$, $48 = 7^2 - 1$.)

§ 7. Упаковка одинаковых шаров в пространстве $\mathbf{R}^n$

Унимодулярная решетка Γ_8 обладает тем свойством, что $x \cdot x \geqslant 2$ для любого ненулевого элемента x решетки Γ_8, в то время как решетка Лича обладает тем свойством, что $x \cdot x \geqslant 4$ для любого ненулевого элемента. Пример унимодулярной решетки, для которой $x \cdot x \geqslant 2^n$ при любом элементе $x \neq 0$, дает n-кратное тензорное произведение $\Gamma_8 \otimes \ldots \otimes \Gamma_8$ (см. п. 9.6). Эти примеры приводят к следующему вопросу. *Если фиксирована размерность n, то каково наибольшее возможное значение для минимума ненулевых норм*

$$\min_{x \in L \setminus \{0\}} (x \cdot x)$$

по унимодулярной решетке L в пространстве $\mathbf{R}^n$?

Другой эквивалентной переформулировкой является следующая: *каково максимальное возможное значение для отношения*

$$\mu(L) = \Big(\min_{x \in L \setminus \{0\}} x \cdot x\Big) / \sqrt[n]{\det L},$$

где L теперь пробегает множество всех решеток пространства $\mathbf{R}^n$? Это действительно эквивалентный вариант, поскольку любая решетка максимального ранга в пространстве $\mathbf{R}^n$ может быть преобразована в унимодулярную решетку преобразованием подобия $x \mapsto x / \sqrt[2n]{\det L}$, не изменяющим отношения $\mu(L)$.

Следующее утверждение хорошо известно (см. [74, с. 29–31]).

7.1. Л е м м а. *Для каждой размерности n существует решетка L_n, максимизирующая отношение* $\mu(L) = \Big(\min_{x \in L \setminus \{0\}} x \cdot x\Big) / \sqrt[n]{\det L}$. *Кроме того, если выбрать базис в решетке L_n, то матрица внутреннего произведения в нем (возможно, домноженная на действительное число) является матрицей рациональных чисел.*

Следовательно, максимальное отношение $\mu(L_n)$ является корнем n-й степени из рационального числа. Доказательство леммы 7.1 будет дано в конце этого параграфа.

Максимальное значение функции $\mu(L)$ при $n \leqslant 5$ было определено А.Н. Коркиным и Е.И. Золотаревым, а при $n \leqslant 8$ – Блихфельдтом. Эти максимальные значения при $1 \leqslant n \leqslant 8$ равны $1, \sqrt{4/3}, \sqrt[3]{2}, \sqrt[4]{4}, \sqrt[5]{8}, \sqrt[6]{64/3}$ и 2 соответственно. Округленные до трех десятичных знаков, эти величины имеют следующие значения (сравните с рис. 3 на с. 49.)

n	1	2	3	4
$\mu(L_n)$	1	1,155	1,260	1,414

n	5	6	7	8
$\mu(L_n)$	1,516	1,665	1,811	2

При $n = 2$ максимальное значение $\mu(L_2) = \sqrt{4/3}$ достигается на решетке, изображенной на рис. 1, с матрицей внутреннего произведения $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Мы будем называть *ее правильной шестиугольной решеткой*, поскольку связанный с ней "многогранник Вороного", состоящий из двух точек пространства $\mathbf{R}^2$, которые отстоят от начала координат не дальше, чем от любой другой точки решетки, является правильным шестиугольником.

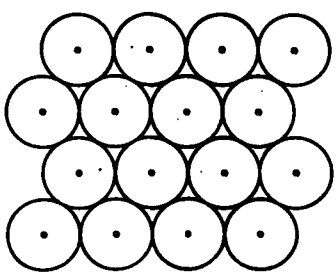


Рис. 1. Правильная шестиугольная решетка и ассоциированная с ней упаковка в пространстве $\mathbf{R}^2$

При $n = 3, 4, 5$ максимальное значение функции $\mu(L)$ достигается на решетке, построенной следующим образом. Пусть $\mathbf{Z}^n$ – решетка, порожденная ортонормированным базисом $e_1, \ldots, e_n$ в

пространстве $\mathbf{R}^n$, и пусть L_n – подрешетка индекса 2, порожденная элементами $e_i + e_j$. В случае $n = 3$ она известна как *кубическая гранецентрированная решетка,* поскольку она получается из "кубической" решетки с базисом $2e_1, 2e_2, 2e_3$ добавлением центральных точек граней всех кубов. (Сравните как с рис. 2, так и с [19].) Матрицей внутреннего произведения относительно базиса $e_1 + e_2$, $e_1 + e_3, e_2 + e_3$ является матрица

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

Эта решетка встречается в природе как конфигурация атомов в кристаллах (например) золота, серебра, алюминия.

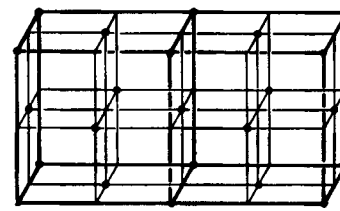


Рис. 2. Кубическая гранецентрированная решетка в пространстве $\mathbf{R}^3$

Ассоциированный с решеткой L_3 многогранник является ромбическим додекаэдром, т.е. телом, ограниченным двенадцатью ромбами.

При $n = 6, 7, 8$ функция $\mu(L)$ достигает максимума на решетке L_n, построенной следующим образом. Пусть L_8 – это решетка Γ_8 из § 6, L_7 – ортогональное дополнение к минимальному вектору в решетке Γ_8, L_6 – ортогональное дополнение к правильной шестиугольной решетке в Γ_8

Эти три решетки можно отождествить с решетками, порожденными системами корней исключительных групп Ли E_6, E_7 и E_8. (Подобным образом решетки L_2, L_3, L_4 и L_5 порождены системами корней A_2, A_3, D_4, D_5. Сравните это с материалом на с. 166–167.)

При $n > 8$ точное значение $\mu(L_n) = \max_{L \subset \mathbf{R}^n} \mu(L)$ неизвестно. Однако оно может быть вычислено с точностью до множителя 4 следующим образом. Напомним, что $\omega_n = \pi^{n/2}/\Gamma(1 + n/2)$ – объем единичного диска в $\mathbf{R}^n$.

7.2. Теорема Минковского. *Для любой размерности n справедливо неравенство*

$$\omega_n^{-2/n} < \mu(L_n) \leqslant 4\omega_n^{-2/n}.$$

Действительно, верхняя оценка $\mu(L) \leqslant 4\omega_n^{-2/n}$ является точной переформулировкой следствия 1.5. Используя формулу Стирлинга

$\Gamma(1+x) \sim x^x e^{-x}\sqrt{2\pi x}$ при $x \to \infty$, видим, что [1])

$$4\omega_n^{-2/n} \sim 2n/\pi e \quad \text{при } n \to \infty.$$

Роджерсом была получена более сильная верхняя оценка вида

$$\mu(L) \leqslant 4(\sigma_n/\omega_n)^{2/n} \sim n/\pi e.$$

Ее мы обсудим несколько позже в этом параграфе (сравните с рис. 3).

Нижняя оценка

$$\mu(L) > \omega_n^{-2/n} \sim n/2\pi e$$

(или чуть более сильная оценка $\mu(L_n) \geqslant (2\zeta(n)/\omega_n)^{2/n}$) была получена Минковским в 1905 г. С этим неравенством часто связывается имя Главки, поскольку им доказано сформулированное Минковским обобщение этого неравенства. Более сильные неравенства этого вида были даны Шмидтом, Роджерсом и другими, но все они имеют то же самое асимптотическое поведение при $n \to \infty$. (Сравните с [64].) Вариант с самодвойственными решетками будет доказан в п. 9.5.

Доказательство неравенства $\mu(L_n) \geqslant (2/\omega_n)^{2/n} > \omega_n^{-2/n}$. Пусть $f(x) = f(\xi_1, \ldots, \xi_n) \geqslant 0$ — непрерывная действительная функция с компактным носителем. Интеграл $\int_{-\infty}^{\infty} \ldots \int_{-\infty}^{\infty} f(\xi_1, \ldots, \xi_n)\, d\xi_1 \ldots d\xi_n$ будем кратко записывать в виде $\int f(x)dx$. Сначала докажем следующее утверждение. Предположим, далее, что $n \geqslant 2$.

7.3. Лемма. *Для любого действительного числа $\beta > \int f(x)dx$ существует унимодулярная решетка $L \subset \mathbf{R}^n$, для которой сумма $\sum_{x \in L \setminus \{0\}} f(x)$ меньше β.*

Доказательство. Пусть $e_1, \ldots, e_n$ — стандартный ортонормированный базис пространства $\mathbf{R}^n$. Пусть $\epsilon > 0$ — фиксированное достаточно малое число, которое будет выбрано позже. Определим число $\lambda > 0$ из уравнения $\epsilon\lambda^{n-1} = 1$. Для данных вещественных параметров $\tau_1, \ldots, \tau_{n-1}$ рассмотрим унимодулярную решетку $L = L(\tau_1, \ldots, \tau_{n-1})$, порожденную базисом

$$\lambda e_1, \ldots, \lambda e_{n-1}, \tau_1 \lambda e_1 + \ldots + \tau_{n-1}\lambda e_{n-1} + \epsilon e_n.$$

Таким образом, типичным элементом решетки является n-ка

$$(\lambda(i_1 + j\tau_1), \ldots, \lambda(i_{n-1} + j\tau_{n-1}), j\epsilon),$$

---

[1]) Или, более точно, $\omega_n^{2/n} = n/2\pi e + \ln(\pi n)/2\pi e + o(1)$.

где коэффициенты $i_1, \ldots, i_{n-1}$ и j принимают независимые значения из кольца $\mathbf{Z}$. Ясно, что если к любому из параметров τ_ν добавим целое число, то решетка $L(\tau_1, \ldots, \tau_{n-1})$ не изменится.

При фиксированном ϵ для каждого набора параметров $\tau_1, \ldots, \tau_{n-1}$ (по модулю 1), рассмотрим сумму

$$(1) \qquad \sum_{x \in L(\tau_1, \ldots, \tau_{n-1}) \setminus \{0\}} f(x) = \sum{}' f(\lambda(i_1 + j\tau_1), \ldots, \lambda(i_{n-1} + j\tau_{n-1}), j\epsilon),$$

где второе суммирование ведется по всем n-кам $i_1, \ldots, i_{n-1}, j$ целых чисел, не равных одновременно нулю. Поскольку функция f имеет компактный носитель, можно выбрать ϵ таким малым, что

$$f(\lambda i_1, \ldots, \lambda i_{n-1}, 0) = 0$$

при $(i_1, \ldots, i_{n-1}) \neq (0, \ldots, 0)$. Если параметр ϵ выбран таким образом, то члены с $j = 0$ не вносят вклада в сумму, так что мы можем переписать сумму (1) в виде

$$(1') \qquad \sum_{j \neq 0} S_j(\tau_1, \ldots, \tau_{n-1}),$$

где слагаемое

$$S_j(\tau_1, \ldots, \tau_{n-1}) = \sum_{i_1, \ldots, i_{n-1}} f(\lambda(i_1 + j\tau_1, \ldots, \lambda(i_{n-1} + j\tau_{n-1}), j\epsilon)$$

равно нулю при больших $|j|$. Затем рассмотрим среднее

$$(2) \qquad \int_0^1 \ldots \int_0^1 \sum_{j \neq 0} S_j(\tau_1, \ldots, \tau_{n-1})\, d\tau_1 \ldots d\tau_{n-1} = \sum_{j \neq 0} \int_0^1 \ldots \int_0^1 S_j(\tau_1, \ldots, \tau_{n-1})\, d\tau_1 \ldots d\tau_{n-1}$$

при изменении параметров $\tau_1, \ldots, \tau_{n-1}$ от 0 до 1. Если $j > 0$, то подстановка $\eta_\nu = j\tau_\nu$ преобразует последний интеграл в

$$j^{1-n} \int_0^j \ldots \int_0^j \sum_{i_1 \ldots i_{n-1}} f(\lambda(i_1 + \eta_1), \ldots, \lambda(i_{n-1} + \eta_{n-1}), j\epsilon)\, d\eta_1 \ldots d\eta_{n-1}.$$

Проверка показывает, что мы интегрируем ровно j^{n-1} раз по каждому единичному кубу в $\mathbf{R}^{n-1}$, так что наше выражение в точности равно

$$\int_{-\infty}^{\infty} \ldots \int_{-\infty}^{\infty} f(\lambda\eta_1, \ldots, \lambda\eta_{n-1}, j\epsilon)\, d\eta_1 \ldots d\eta_{n-1}.$$

Аналогичным образом формула доказывается при $j < 0$. Если положить

$$g(\eta) = \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} f(\xi_1, \dots, \xi_{n-1}\ \eta)\, d\xi_1 \dots d\xi_{n-1},$$

то последнее выражение равно

$$\lambda^{1-n}\, g(j\epsilon) = \epsilon g(j\epsilon).$$

Следовательно, среднее (2) равно

$$(3) \qquad \sum_{j \neq 0} \epsilon g(j\epsilon).$$

Но $g(\eta)$ — непрерывная функция с компактным носителем. Поэтому при $\epsilon \to 0$ сумма (3) сходится к интегралу Римана

$$\int_{-\infty}^{\infty} g(\eta)\, d\eta = \int f(x)\, dx < \beta.$$

Если выбрать сумму Римана (3) меньше β, то отсюда следует, что среднее (2) также меньше β. Следовательно, найдутся значения параметров $\tau_1, \dots, \tau_{n-1}$, такие, что сумма (1) = (1′) меньше β. Этим завершается доказательство леммы 7.3. □

Для доказательства теоремы 7.2 мы специальным образом подберем функцию f. Пусть $r < s$ — положительные действительные числа, которые меньше $(2/\omega_n)^{1/n}$. Выберем функцию f так, что

$$f(x) = 1 \quad \text{при} \quad x \cdot x \leqslant r^2,$$

$$f(x) = 0 \quad \text{при} \quad x \cdot x \geqslant s^2$$

и всюду $0 \leqslant f(x) \leqslant 1$. Тогда очевидно, что

$$\int f(x)\, dx < \omega_n s^n < 2.$$

Следовательно, по лемме 7.2 существует унимодулярная решетка $L \subset \mathbf{R}^n$, для которой

$$(4) \qquad \sum_{x \in L \setminus \{0\}} f(x) < 2.$$

Эта решетка L не может содержать такого вектора x_0, что

$$0 < x_0 \cdot x_0 < r^2$$

(поскольку если бы такой вектор x_0 существовал, то сумма (4) содержала бы члены $f(x_0) + f(-x_0) \geqslant 2$, что невозможно).

Следовательно,

$$\mu(L) = \min_{x \in L \setminus \{0\}} x \cdot x > r^2.$$

Поскольку r^2 может быть любым числом, меньшим $(2/\omega_n)^{2/n}$, то

этим доказано, что

$$\mu(L_n) = \sup_{L \subset \mathbf{R}^n} \mu(L) \geqslant (2/\omega_n)^{2/n},$$

чем и завершается доказательство теоремы 7.2. □

Однако и после этих замечаний многие вопросы остались без ответа. Стремится ли отношение $\mu(L_n)/n$ к пределу при $n \to \infty$? Если — да, то каков этот предел? Возрастает ли последовательность $\mu(L_1)$, $\mu(L_2), \ldots$ монотонно? Каковы точные значения $\mu(L_9), \mu(L_{10}), \ldots$?

С задачей о вычислении значения $\mu(L)$ тесно связана следующая классическая задача. *Какова максимальная возможная плотность объединения непересекающихся шаров фиксированного радиуса в евклидовом пространстве* $\mathbf{R}^n$?

Такое объединение P непересекающихся шаров одинакового радиуса будет кратко называться *упаковкой* в пространстве $\mathbf{R}^n$. Про упаковку P говорят, что она имеет *плотность* ρ, если отношение

$$\mathrm{vol}(P \cap C)/\mathrm{vol}(C),$$

где через C обозначен большой куб, равномерно стремится к пределу ρ, когда ребро куба стремится к бесконечности.

Любая решетка $L \subset \mathbf{R}^n$ приводит к упаковке в пространстве $\mathbf{R}^n$ следующим образом. Определим радиус r из уравнения

$$(2r)^2 = \min_{x \in L \setminus \{0\}} x \cdot x.$$

Если расположить центры шаров с радиусами r в каждой точке решетки, то множества внутренних точек шаров, очевидно, не будут пересекаться. Плотность этой упаковки задается формулой

$$\rho = \omega_n r^n / \sqrt{\det L} = \omega_n (\mu(L)/4)^{n/2}.$$

Следовательно,

$$\mu(L) = 4(\rho/\omega_n)^{2/n}.$$

Отметим, что оценка Минковского (п. 1.5) в точности совпадает с неравенством $\rho \leqslant 1$.

Туэ доказал, что максимальная возможная плотность упаковки в пространстве $\mathbf{R}^2$ равна плотности $\rho = \pi/\sqrt{12}$, связанной с правильной шестиугольной решеткой, изображенной на рис. 1. При $n = 3$ кубическая гранецентрированная решетка дает упаковку с плотностью $\pi/\sqrt{18}$. Что касается произвольной упаковки в пространстве $\mathbf{R}^3$, то, согласно Роджерсу, "большинство математиков верит, а все физики знают, что ее плотность не может превосходить $\pi/\sqrt{18}$". Однако это никем не было доказано. В действительности, задача остается нерешенной для всех $n \geqslant 3$. Примечательно, что Лич и Слоун недавно описали примеры нерешеточных упаковок в размер-

ностях 10, 11, 13, имеющие большую плотность, чем для упаковок, связанных с любой из известных в этих размерностях решетках.

Роджерсом была доказана прекрасная верхняя оценка для плотности любой упаковки в пространстве $\mathbf{R}^n$, основывающаяся на более ранней работе Блихфельдта. Пусть Δ_n – равносторонний n-симплекс в евклидовом пространстве с ребрами длины 2. Пусть подмножество B состоит из всех точек симплекса Δ_n, отстоящих от какой-нибудь из его вершин не более чем на 1,

$$\sigma_n = \mathrm{vol}\,(B)/\mathrm{vol}\,(\Delta_n).$$

Роджерс доказал, что для любой упаковки в пространстве $\mathbf{R}^n$, *обладающей плотностью* ρ, *выполняется неравенство*

$$\rho \leqslant \sigma_n.$$

(В таблице приведены некоторые примеры с округлением десятичных дробей до ближайших десятитысячных.)

Размерность	Решетка	Плотность ассоциированной упаковки	Верхняя оценка σ_n
2	правильная шестиугольная	0,9069 $= \pi/\sqrt{12}$	0,9069 $= \pi/\sqrt{12}$
3	кубическая гранецентрированная	0,7405	0,7796
8	Γ_8	0,2537	0,2568
24	решетка Лича	0,0019	0,0025

Следовательно, для любой решетки L

$$\mu(L) = 4\,(\rho/\omega_n)^{2/n} \leqslant 4\,(\sigma_n/\omega_n)^{2/n}.$$

Это представляет существенное улучшение верхней оценки $4\,(1/\omega_n)^{2/n}$ из § 1, что становится очевидным, если использовать асимптотическую формулу Роджерса

$$\sigma_n \sim n/e\sqrt{2^n} \quad \text{при } n \to \infty.$$

Числовые значения при $n \leqslant 24$ изображены на рис. 3. Все использованные в этом графике данные взяты из работ [46] и [47]. Отметим, что при $n = 8$ верхняя оценка Роджерса $4\,(\sigma_8/\omega_8)^{1/4} \approx \approx 2{,}006$ так близка к $\mu(L_8) = 2$, что две точки на графике кажутся совпадающими.

Для того чтобы завершить этот параграф, нам осталось доказать лемму 7.1. Доказательство будет основываться на следующем утверждении.

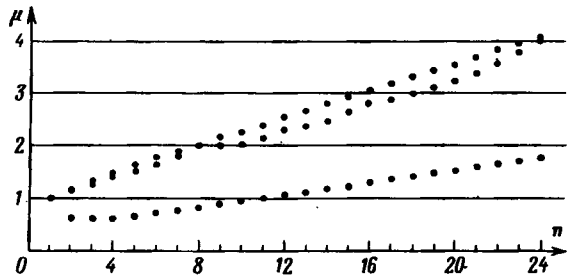


Рис. 3. **Средний ряд точек дает наибольшее возможное значение $\mu(L) = \min(x \cdot x)/\sqrt[n]{\det L}$ для решетки L в каждой из размерностей $n \leqslant 8$ и наибольшее известное значение – в каждой из размерностей n в диапазоне от 9 до 24. Верхний ряд точек дает верхнюю оценку Роджерса $4(\sigma_n/\omega_n)^{2/n}$, а нижний ряд – грубую оценку Минковского $(2/\omega_n)^{2/n}$**

7.4. Л е м м а. *Существует такая константа $c_n > 0$, что любая решетка в пространстве $\mathbf{R}^n$ обладает базисом $b_1, \ldots, b_n$, для которого*

$$|b_i \cdot b_j| \leqslant c_n \det(L)/(\min_{L \setminus \{0\}} x \cdot x)^{n-1}$$

при любых i, j.

В действительности мы покажем, что константа c_n может быть определена индуктивно по формуле

$$(5) \qquad c_n = \left(\frac{4}{3}\right)^{n-2} c_{n-1} + 4^n \omega_n^{-2},$$

где $c_1 = 1$.

Чтобы начать доказательство леммы 7.4, выберем в решетке L вектор $b_n \neq 0$, для которого

$$(6) \qquad b_n \cdot b_n = \min_{x \in L \setminus \{0\}} x \cdot x.$$

Тогда, в силу следствия 1.5 или теоремы 7.2,

$$(7) \qquad b_n \cdot b_n \leqslant 4\,\omega_n^{-2/n} (\det L)^{1/n}.$$

Деля n-ю степень неравенства (7) на $(n-1)$-ю степень равенства (6), получаем неравенство

$$(8) \qquad b_n \cdot b_n \leqslant (4^n \omega_n^{-2}) \det L/(\min_{L \setminus \{0\}} x \cdot x)^{n-1},$$

где коэффициенты $4^n \omega_n^{-2}$, очевидно, удовлетворяют неравенству $4^n \omega_n^{-2} \leqslant c_n$.

Этим завершается доказательство при $n = 1$. Предположим теперь, что $n \geqslant 2$. Пусть через L' обозначен образ решетки L при орто-

гональном проектировании из пространства $\mathbf{R}^n$ на гиперплоскость $(b_n)^{\perp}$. Тогда любой вектор $x' \in L'$ может быть выражен в виде разности

$$x' = x - \lambda b_n,$$

где $x \in L$, и мы можем выбрать вектор x так, чтобы $|\lambda| \leqslant 1/2$. Если $x' \neq 0$, то

$$b_n \cdot b_n \leqslant x \cdot x = x' \cdot x' + \lambda^2 b_n \cdot b_n \leqslant x' \cdot x' + \frac{1}{4} b_n \cdot b_n$$

и, следовательно,

$$x' \cdot x' \geqslant \frac{3}{4} b_n \cdot b_n = \frac{3}{4} \min_{L \setminus \{0\}} x \cdot x.$$

Теперь, используя формулы

$$\min_{L' \setminus \{0\}} x' \cdot x' \geqslant \frac{3}{4} \min_{L \setminus \{0\}} x \cdot x$$

и

$$\det(L') = \det(L)/b_n \cdot b_n,$$

получаем по индукции, что решетка L' обладает базисом $b'_1, \ldots, b'_{n-1}$, для которого

(9) $b'_i \cdot b'_i \leqslant$

$$\leqslant c_{n-1} \det(L')/(\min_{L \setminus \{0\}} x' \cdot x')^{n-2} \leqslant$$

$$\leqslant \left(\frac{4}{3}\right)^{n-2} c_{n-1} \det(L)/(\min_{L \setminus \{0\}} x \cdot x)^{n-1}$$

Полагая $b'_i = b_i - \lambda_i b_n$, где $|\lambda_i| < 1$, мы получим требуемые элементы $b_1, \ldots, b_{n-1}$, удовлетворяющие, в силу формул (5), (8), (9), неравенству

$$b_i \cdot b_i < b'_i \cdot b'_i + b_n \cdot b_n \leqslant c_n \det L/(\min_{L \setminus \{0\}} x \cdot x)^{n-1}$$

Очевидно, что векторы $b_1, \ldots, b_n$ образуют базис решетки L. Требуемая верхняя оценка для выражения $|b_i \cdot b_j|$ при $i \neq j$ следует теперь из неравенства Шварца, чем завершается доказательство леммы 7.4. □

Доказательство леммы 7.1. Пусть множество K состоит из всех действительных симметрических матриц $A = (a_{ij})$ размером $n \times n$, которые для любого набора $(\zeta_1, \ldots, \zeta_n)$ из n целых чисел, не равных одновременно нулю, удовлетворяют неравенству

(10) $\Sigma a_{ij} \zeta_i \zeta_j \geqslant 1.$

Очевидно, множество K можно представлять себе как замкнутое выпуклое подмножество в действительном $n(n+1)/2$-мерном пространстве.

Отметим, что каждая матрица из множества K положительно определена. Действительно, из следствия 1.5 или теоремы 7.2 следует, что любая положительно определенная матрица A из множества K удовлетворяет неравенству

$$\det(A) \geqslant \omega_n^2/4^n > 0.$$

Отсюда легко выводится, что подмножество множества K, состоящее из положительно определенных матриц, не только открыто, но также и замкнуто. Следовательно, это подмножество совпадает с множеством K.

Мы докажем, что функция определителя $A \mapsto \det(A)$ из множества K в поле $\mathbf{R}$ действительно достигает минимального значения в некоторой точке $A_0 \in K$. Пусть K_0 – компактное подмножество в K, состоящее из всех матриц $A = (a_{ij})$ множества K, элементы a_{ij} которых удовлетворяют неравенству

$$|a_{ij}| \leqslant c_n.$$

Из леммы 7.4 следует, что для любой матрицы $A \in K$, такой, что $\det(A) \leqslant 1$, существует обратимая целочисленная матрица $P \in \mathrm{GL}(n, \mathbf{Z})$, такая, что $PAP^t \in K_0$. Очевидно, что

$$\det(PAP^t) = \det(A).$$

Но функция определителя, ограниченная на компактное множество K_0, достигает минимума. Следовательно, можно выбрать матрицу $A_0 \in K_0$, такую, что $\det(A_0) \leqslant \det(A)$ для всех матриц $A \in K_0$, и, следовательно, для всех матриц $A \in K$.

Если L_n является решеткой с матрицей внутреннего произведения A_0, то отсюда, очевидно, следует, что

$$\mu(L_n) = 1/\sqrt[n]{\det A_0}$$

равно $\max\limits_{L \subset \mathbf{R}^n} \mu(L)$.

Теперь мы должны доказать, что элементы матрицы A_0 являются рациональными числами. В более общем случае назовем, следуя А.Н. Коркину и Е.И. Золотареву, матрицу $A_0 \in K$ *экстремальной*, если функция $\det: K \to R$ имеет в A_0 локальный минимум. *Отметим, что экстремальная матрица A_0 не может лежать внутри отрезка матриц*

$$A_\xi = A_0 + \xi B \quad (-\epsilon < \xi < \epsilon),$$

целиком принадлежащего множеству K, где $B \neq 0$. (На языке теории выпуклых множеств экстремальная матрица обязательно является "экстремальной точкой" выпуклого множества K.) Действительно,

выбирая такую вещественную матрицу P, что $PA_0P^t = I$, и полагая $PBP^t = C = (c_{ij})$, простыми вычислениями показываем, что

$$\det(A_\xi)/\det(A_0) = \det(I + \xi C) =$$

$$= \frac{1}{2} + \frac{1}{2}(1 + \xi \sum_i c_{ii})^2 - \frac{1}{2}\xi^2 \sum_i \sum_j c_{ij}^2 + \ldots$$

где опущены члены с ξ^3 и более старшими степенями. Поскольку $C \neq 0$, то легко показать, что существуют как угодно малые значения ξ, для которых $\det(A_\xi) < \det(A_0)$.

Если A_0 – экстремальная матрица, то пусть $\pm z_{(1)}, \ldots, \pm z_{(N)}$ – полный список всех n-к целых чисел (рассматриваемых как матрицы размера $1 \times n$), удовлетворяющих матричному уравнению

$$(11)\quad z_{(i)} A_0 z_{(i)}^t = 1.$$

Мы будем рассматривать уравнение (11) как систему из N линейных уравнений относительно $n(n+1)/2$ элементов матрицы A_0. *Утверждается, что матрица A_0 является единственным решением этой системы.* В противном случае, если решение не единственно, то существовало бы однопараметрическое семейство симметрических матриц $A_\xi = A_0 + \xi B$, удовлетворяющих уравнению (11). Мы докажем, что $A_\xi \in K$ при достаточно малом ξ. Если z – ненулевая n-ка целых чисел, то либо $zA_0z^t = 1$ и, следовательно, $zA_\xi z^t = 1$, либо $zA_0z^t \geqslant c$ для некоторой константы $c > 1$. Выбирая в последнем случае такую константу, что для любого $x \in \mathbf{R}^n$

$$|xBx^t| \leqslant \epsilon^{-1} xA_0x^t,$$

получаем, что

$$zA_\xi z^t \geqslant zA_0z^t - \epsilon^{-1}|\xi| zA_0z^t > 1$$

при $|\xi| < (1 - c^{-1})\epsilon$. Таким образом, $A_\xi \in K$ при $|\xi| < (1 - c^{-1})\epsilon$, что противоречит предположению об экстремальности матрицы A_0.

Поскольку единственное решение системы линейных рациональных уравнений всегда рационально, то этим доказано, что элементы матрицы A_0 рациональны, чем завершено доказательство леммы 7.1. □

§ 8. Суммы двух и четырех квадратов

В этом параграфе теорема Минковского о выпуклом теле будет использована для доказательства двух теорем. Первая из них была сформулирована Ферма в семнадцатом столетии и доказана Эйлером в восемнадцатом.

8.1. Т е о р е м а. *Если p – простое число вида $4k+1$, то уравнение $a^2+b^2=p$ имеет решение $a, b \in \mathbf{Z}$.*

В терминах кольца $\mathbf{Z}[i]$ целых гауссовых чисел эта теорема утверждает, что любое такое простое число разлагается в произведение $(a+bi)(a-bi)$.

Д о к а з а т е л ь с т в о. Пусть p – любое нечетное простое число. Отметим сначала, что сравнение $u^2 \equiv -1 \pmod{p}$ имеет решение $u \in \mathbf{Z}$ тогда и только тогда, когда $p \equiv 1 \pmod 4$. Действительно, группа $(\mathbf{Z}/p\mathbf{Z})^*$ взаимно простых классов вычетов по модулю p является циклической группой порядка $p-1$. Образом элемента -1 в группе $(\mathbf{Z}/p\mathbf{Z})^*$ является единственный элемент порядка 2. Очевидно, что элемент порядка 4 существует в этой группе тогда и только тогда, когда 4 делит $p-1$, т.е. тогда и только тогда, когда $p \equiv 1 \pmod 4$.

Предположим теперь, что число p сравнимо с 1 по модулю 4, и выберем некоторое целое число u, удовлетворяющее сравнению $u^2 \equiv -1 \pmod p$. Зафиксировав число u, определим $L \subset \mathbf{Z} \oplus \mathbf{Z}$ как решетку в пространстве $\mathbf{R}^2$, состоящую из всех пар (a, b) целых чисел, для которых

$$b \equiv ua \pmod p.$$

Тогда решетка L является подгруппой индекса p в группе $\mathbf{Z}^2$. Следовательно, объем фундаментальной области решетки L равен p. В силу следствия 1.5 существует точка $x \neq 0$ решетки L, для которой

$$x \cdot x \leqslant 4p/\pi.$$

Полагая $x = (a, b)$, получаем, что

$$0 < a^2 + b^2 \leqslant 4p/\pi < 2p.$$

Но по модулю p имеем

$$a^2 + b^2 \equiv a^2 + (ua)^2 \equiv (1+u^2)a^2 \equiv 0.$$

Следовательно, $a^2 + b^2$ должно в точности равняться p. Этим завершается доказательство. □

8.2. С л е д с т в и е. *Подмножество группы $\mathbf{Q}^*$, состоящее из всех ненулевых рациональных чисел, которые можно выразить в виде суммы двух квадратов, является свободной мультипликативной абелевой группой с базисом* $2, 3^2, 5, 7^2, 11^2, 13, 17, \ldots$

(Сравните с п. 4.4 гл. 3.)

Д о к а з а т е л ь с т в о. Сначала рассмотрим над полем $\mathbf{Q}$ какое-нибудь уравнение вида $\alpha^2 + \beta^2 = \gamma \neq 0$. После домножения на квадрат достаточно большого числа можно предполагать, что $\alpha, \beta, \gamma \in \mathbf{Z}$. Мы должны показать, что любое нечетное простое число p, которое входит делителем в γ в нечетной степени, должно

иметь вид $4k + 1$. Пусть p^{2l} — наибольшая степень p, делящая одновременно α^2 и β^2. Тогда, очевидно,

$$(\alpha/p^l)^2 \equiv -(\beta/p^l)^2 \not\equiv 0 \pmod{p}.$$

Следовательно, -1 является квадратом по модулю p и из первого замечания в доказательстве теоремы 8.1 следует, что $p \equiv 1 \pmod 4$. Таким образом, если $\gamma = \alpha^2 + \beta^2$, то γ должен принадлежать мультипликативной группе, порожденной числами $2, 3^2, 5, 7^2, \ldots$. Обратно, используя тождество

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad \mp bc)^2,$$

легко получаем, что любой элемент мультипликативной группы является суммой квадратов. □

Упражнение для читателя: доказать, что целое число является суммой двух квадратов рациональных чисел тогда и только тогда, когда оно является суммой двух квадратов целых чисел.

Вторая теорема была сформулирована Баше де Мезирьяком в семнадцатом столетии, а доказана Лагранжем в восемнадцатом.

8.3. Т е о р е м а. *Любое положительное целое число является суммой четырех квадратов.*

Из этой теоремы сразу следует, что любое положительное рациональное число является суммой квадратов четырех рациональных чисел. (Это можно рассматривать как частный случай теоремы Мейера, соответствующий пространствам с внутренним произведением вида $\langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle -r \rangle$.)

Д о к а з а т е л ь с т в о т е о р е м ы 8.3. Пусть p — любое нечетное простое число. Из леммы 3.3 мы видим, что сравнение

$$u^2 + v^2 + 1 \equiv 0 \pmod{p}$$

имеет решение $u, v \in \mathbf{Z}$. (Принцип Дирихле показывает, что одно из $(p + 1)/2$ различных значений члена u^2 по модулю p должно совпадать с одним из $(p + 1)/2$ различных значений члена $-1 - v^2$.) Зафиксировав u и v, определим $L \subseteq \mathbf{Z} \oplus \mathbf{Z} \oplus \mathbf{Z} \oplus \mathbf{Z}$ как решетку, состоящую из всех четверок (a, b, c, d), для которых

$$c \equiv ua + vb, \quad d \equiv ub - va \pmod{p}.$$

Тогда L — подгруппа индекса p^2 в группе $\mathbf{Z}^4$ и, следовательно, объем фундаментальной области решетки L равен p^2. Поэтому, в силу утверждения 1.5, существует точка $x \neq 0$ решетки L, для которой

$$x \cdot x \leqslant 4\sqrt{p^2/\omega_4} = 4p\sqrt{2}/\pi.$$

Полагая $x = (a, b, c, d)$, получаем, что

$$0 < a^2 + b^2 + c^2 + d^2 \leqslant 4p\sqrt{2}/\pi < 2p.$$

Но, сравнивая по модулю p, имеем

$$\begin{aligned} a^2+b^2+c^2+d^2 &\equiv \\ &\equiv a^2+b^2+(ua+vb)^2+(ub-va)^2= \\ &=(1+u^2+v^2)a^2+(1+u^2+v^2)b^2\equiv \\ &\equiv 0 \pmod p. \end{aligned}$$

Следовательно, сумма $a^2+b^2+c^2+d^2$ должна в точности равняться p.

Для распространения этого результата на произвольное произведение простых чисел заметим, что сумма $a^2+b^2+c^2+d^2$ является нормой кватерниона $a+bi+cj+dk$. Поскольку функция нормы из кватернионов в действительные числа мультипликативна, то отсюда следует, что любое произведение $(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2)$ сумм четырех квадратов может само быть выражено в виде суммы

$$\begin{aligned} &(aA-bB-cC-dD)^2+(aB+bA+cD-dC)^2+ \\ &\qquad +(aC-bD+cA+dB)^2+(aD+bC-cB+dA)^2 \end{aligned}$$

четырех квадратов. Очевидно, что этим завершается доказательство. □

Характеристику сумм трех квадратов можно найти, например, в [66, с. 78].

§ 9. Теорема Зигеля

В этом параграфе будет описана принадлежащая К.Л. Зигелю основная формула для положительно определенных билинейных форм над кольцом $\mathbf{Z}$. Никакого доказательства формулы дано не будет, но будут подробно описаны некоторые интересные приложения. За доказательствами читатель отсылается к работам [25, 15, 52].

Одна из классических задач теории чисел состоит в том, чтобы дать удовлетворительную формулу для числа решений квадратного уравнения с несколькими целыми переменными. Например, сколько n-к $x_1, \ldots, x_n \in \mathbf{Z}$ удовлетворяет уравнению $x_1^2+\ldots+x_n^2=k$ при данном положительном целом числе k? В 1881 г. Парижская академия объявила, что ее большая премия будет присуждена автору лучшей работы на тему "Теория разложения целых чисел в сумму пяти квадратов". Двумя годами позже французская печать была возмущена тем, что половина[1]) премии была

[1]) Другим лауреатом премии был Г.Дж. Смит из Оксфорда, который в действительности опубликовал решение поставленной задачи многими годами раньше.

присуждена немецкому студенту, еще не достигшему двадцати лет, который из-за недостатка времени даже не следовал правилам и не представил свою рукопись на французском языке. Тем не менее французская академия была непоколебима. В своей работе, удостоенной премии, Герман Минковский заложил фундамент современной теории квадратичных форм над целыми и рациональными числами.

В этом параграфе пойдет речь о формуле Зигеля для "среднего" числа решений квадратного уравнения. Для ее формулировки понадобится несколько определений.

Пусть X и Y – топологические пространства, каждое из которых снабжено мерой на σ-кольце, порожденном открытыми множествами. Мера множества U будет обозначаться $\mathrm{vol}\,(U)$. Для любого непрерывного отображения $f\colon X \to Y$ плотность решений уравнения $f(x) = y_0$ может быть измерена следующим образом. Рассмотрим малые окрестности U точки y_0 и образуем предел

$$\lim_{U \to y_0} \mathrm{vol}\, f^{-1}(U)/\mathrm{vol}\,(U).$$

Если этот предел существует, то он будет называться *плотностью* для f^{-1} в точке y_0 и обозначаться $Df^{-1}(y_0)$. Если эта плотность непрерывна как функция от y_0, то очевидно, что для любого измеримого множества $U \subset Y$

$$\int_U Df^{-1}(y)\,dy = \mathrm{vol}\, f^{-1}(U).$$

(Это топологическая версия теоремы Радона–Никодима.)

Пример 1. Пусть $f : \mathbf{R}^n \to \mathbf{R}$ – квадратичная функция $f(x_1, \ldots, x_n) = x_1^2 + \ldots + x_n^2$. Используя обычную меру Лебега в пространствах $\mathbf{R}^n$ и $\mathbf{R}$, мы видим, что при $y > 0$ интеграл

$$\int_0^y Df^{-1}(\eta)\,d\eta = \mathrm{vol}\, f^{-1}[0, y]$$

равен объему шара радиусом $\sqrt{y}$. Следовательно, плотность $Df^{-1}(y)$ равна производной

$$\frac{d}{dy}\left(\omega_n \sqrt{y^n}\right) = \frac{1}{2}\, n\omega_n y^{n/2-1}.$$

Например,

$Df^{-1}(y) = 1/\sqrt{y}$, если $n = 1$,

$= \pi$, если $n = 2$,

$= 2\pi\sqrt{y}$, если $n = 3$,

$= \pi^2 y$, если $n = 4$,

и так далее, при условии, что $y > 0$. Очевидно, что $Df^{-1}(y) = 0$ при $y < 0$. Функция Df^{-1} непрерывна в 0 при $n \geqslant 3$ и разрывна при $n = 1, 2$.

Пример 2. Через $\mathbf{Z}_p$ обозначим кольцо p-адических целых чисел. Это кольцо имеет каноническую меру Хаара, в которой объем каждого из p^k различных классов вычетов по модулю p^k равен p^{-k}. Тогда n-кратное декартово произведение $\mathbf{Z}_p \times \ldots \times \mathbf{Z}_p$ имеет соответствующую меру Хаара. Определяя функцию f_p: $\mathbf{Z}_p \times \ldots \times \mathbf{Z}_p \to \mathbf{Z}_p$ по формуле $f_p(x_1, \ldots, x_n) = x_1^2 + \ldots + x_n^2$, мы опять можем образовать плотность Df_p^{-1}: $\mathbf{Z}_p \to \mathbf{R}$.

Пусть u — любое обратимое p-адическое число. Тогда преобразование $(x_1, \ldots, x_n) \mapsto (ux_1, \ldots, ux_n)$ непрерывно и сохраняет объем. Поскольку

$$f_p(ux_1, \ldots, ux_n) = u^2 f_p(x_1, \ldots, x_n),$$

то плотность $Df^{-1}(u^2 y)$ равняется плотности $Df^{-1}(y)$. *В частности, для любого элемента $y \neq 0$ из кольца $\mathbf{Z}_p$ функция Df^{-1} постоянна в окрестности точки y.*

Далее для функции Df_p^{-1} дается точная формула. Для упрощения рассуждений мы рассмотрим только случай четного n, скажем $n = 2m$. Напомним, что любой элемент $y \neq 0$ из кольца $\mathbf{Z}_p$ может быть однозначно записан в виде произведения $p^v u$, где v — неотрицательное целое число, а u — обратимое p-адическое число.

9.1. Лемма. *Пусть f_p: $\mathbf{Z}_p \times \ldots \times \mathbf{Z}_p \to \mathbf{Z}_p$ — функция от $2m$ p-адических переменных, для которой $f_p(x_1, \ldots, x_{2m}) = x_1^2 + \ldots + x_{2m}^2$. Пусть $r = p^{1-m}$, а для нечетного p пусть $\epsilon = \left(\frac{-1}{p}\right)^m$, так что ϵ равно $+1$ или -1 в соответствии с тем, $p^m \equiv 1$ или $p^m \equiv -1 \pmod 4$. Если p нечетно, то ассоциированная функция плотности $Df_p^{-1}(p^v u)$ равна*

$$(1 - \epsilon r/p)(1 + \epsilon r + \epsilon^2 r^2 + \ldots + \epsilon^v r^v).$$

При $p = 2$ и четном m она равна

$$1 + (-1)^{m/2}(r + r^2 + \ldots + r^{v-1} - r^v),$$

тогда как при нечетном m она равна $1 + r^{v+1}$ или $1 - r^{v+1}$ в зависимости от того, $m \equiv$ и или $m \equiv -$и $\pmod 4$.

Доказательство будет дано в конце этого параграфа. При нечетном n формула несколько сложнее.

Отметим, что при $m \to \infty$ плотность $Df_p^{-1}(y)$ стремится к 1. Более того, заметим, что при $m \geqslant 2$ плотность $Df_p^{-1}(y)$ равномерно стремится к 1 при $p \to \infty$.

Для единообразия записи будем использовать обозначение $\mathbf{Z}_\infty$ для поля действительных чисел $\mathbf{R}$. Тогда имеем каноническое вложение $\mathbf{Z} \to \mathbf{Z}_p$ при $p = 2, 3, 5, 7, \ldots, \infty$.

О п р е д е л е н и е (Гаусс, Минковский). Пространства с билинейными формами X и Y над целыми числами принадлежат одному и тому же *роду*, если для любого $p = 2, 3, \ldots, \infty$ индуцированное пространство с билинейной формой $X \otimes \mathbf{Z}_p$ над кольцом $\mathbf{Z}_p$ изоморфно пространству $Y \otimes \mathbf{Z}_p$.

Если пространства X и Y имеют один и тот же род, то нетрудно проверить, что они также имеют один и тот же определитель. Следовательно, используя лемму 1.6, мы видим, что *каждый род содержит лишь конечное число различных, с точностью до изоморфизма, пространств.*

П р и м е р 3. Пространства с билинейными формами $\langle 5 \rangle \oplus \langle 11 \rangle$ и $\langle 1 \rangle \oplus \langle 55 \rangle$ положительно определены, и нетрудно показать, что для любого простого числа p вложение $\mathbf{Z} \to \mathbf{Z}_p$ переводит их в изоморфные пространства. Следовательно, эти два пространства принадлежат одному и тому же роду. Они не изоморфны, поскольку уравнение $5x^2 + 11y^2 = 1$ не имеет целочисленных решений.

Аналогично, пространства с внутренним произведением $\langle 1 \rangle \oplus \Gamma_8$ и $\langle 1 \rangle \oplus \ldots \oplus \langle 1 \rangle$, имеющие ранг 9, принадлежат одному роду, но не изоморфны.

Теперь мы готовы привести одну из формулировок теоремы Зигеля. Пусть X – пространство с положительно определенной билинейной формой ранга $n \geqslant 2$ над кольцом $\mathbf{Z}$.

О п р е д е л е н и е. Пусть для каждого целого числа k через $r_X(k)$ обозначено число различных элементов $x \in X$, удовлетворяющих уравнению $x \cdot x = k$.

Для любого простого числа p мы можем образовать индуцированное пространство $X \otimes \mathbf{Z}_p$ над кольцом $\mathbf{Z}_p$. Пусть через

$$f_p\colon X \otimes \mathbf{Z}_p \to \mathbf{Z}_p$$

обозначена квадратичная функция $f_p(\xi) = \xi \cdot \xi$.

9.2. Т е о р е м а З и г е л я (предварительный вариант). *Если род пространства X содержит только один класс изоморфных форм, то для любого целого числа $k \neq 0$*

$$r_X(k) = \epsilon \prod_{p=2,3,\ldots,\infty} Df_p^{-1}(k),$$

где коэффициент ϵ полагается равным 1/2 *или* 1 *в соответствии с тем, что $n = 2$ или $n > 2$.*

За доказательством, которое не является легким, мы отошлем к работе [25, с. 326–366]. Эта теорема остается верной и в неопре-

деленном случае, но она не столь интересна, поскольку обе стороны равенства обычно бесконечны.

Произведение в правой части абсолютно сходится при $n \geqslant 4$. В случаях $n = 2, 3$ необходимо позаботиться о перемножении множителей в обычном порядке.

Пример 4. Пространство с внутренним произведением $\langle 1 \rangle \oplus \langle 1 \rangle \oplus \ldots \oplus \langle 1 \rangle$ ранга 8 удовлетворяет предположениям теоремы 9.2. Пусть через $v_p = v_p(k)$ обозначен показатель наибольшей степени числа p, делящий число k. Тогда по теореме 9.2

$$Df_p^{-1}(k) = (1-p^4)(1+p^{-3}+p^{-6}+\ldots+p^{-3v_p})$$

при нечетном p и

$$Df_2^{-1}(k) = 1+2^{-3}+2^{-6}+\ldots+2^{-3(v_2-1)}-2^{-3v_2}$$

при $p = 2$. (Если $v_2 = 0$, то эта формула читается как $Df_2^{-1}(k) = 1$.) Кроме того, из примера 1

$$Df_\infty^{-1}(k) = 4\omega_8 k^3 = \pi^4 k^3/6.$$

Перемножая выражения при $p = 2, 3, \ldots, \infty$, получаем не зависящее от k бесконечное произведение

$$C = \frac{1}{6}\pi^4(1-3^{-4})(1-5^{-4})(1-7^{-4})\ldots,$$

умноженное на конечное произведение

$$k^3 \prod_{p \mid k} (1+p^{-3}+p^{-6}+\ldots \pm p^{-3v_p}),$$

явно зависящее от k. Вычисляя произведение в последнем выражении, получаем

$$k^3 \sum_{d \mid k} \pm d^{-3} = \sum_{d \mid k} \pm d^3,$$

где знак слагаемого d^3 оказывается равным $(-1)^{d+k}$.

Поскольку C – константа, то, вычисляя $r_X(k)$ при $k = 1$, видим, что $C = 16$. С другой стороны, можно записать в терминах дзета-функции Римана

$$C = \frac{1}{6}\pi^4(1-2^{-4})^{-1} \prod_{p \text{ конечное}} (1-p^{-4}) = \frac{1}{6}\pi^4 \frac{16}{15}\zeta(4)^{-1}.$$

Подставляя известное равенство

$$\zeta(4) = \pi^4/90$$

(см., например, [66, с. 145]), опять получаем $C = 16$. Таким образом, выведено следующее утверждение.

Формула Якоби. *Для любого положительного целого числа k число представлений числа k в виде суммы восьми квадратов равно* $16 \sum_{d \mid k} (-1)^{d+k} d^3$.

Оставляем читателю в качестве упражнений соответствующие формулы для двух, четырех или шести квадратов.

Теперь рассмотрим произвольный род G положительно определенных пространств с билинейными формами. Пусть род G содержит g различных классов изоморфных форм, где g – положительное целое число, $X_1, \ldots, X_g$ – представители этих различных классов. Следуя Эйзенштейну, присвоим веса различным классам изоморфных форм в зависимости от нехватки в них симметрий. Точнее, пусть $|O(X_i)|$ обозначает порядок ортогональной группы, состоящей из всех автоморфизмов пространства X_i. Определяя

$$w_i = |O(X_i)|^{-1} / \sum_{j=1}^{g} |O(X_j)|^{-1},$$

получаем положительные рациональные числа $w_1, \ldots, w_g$, для которых $w_1 + \ldots + w_g = 1$.

Пусть, как и выше, f_p: $X_1 \otimes \mathbf{Z}_p \to \mathbf{Z}_p$ – квадратичные функции, для которых $f_p(x) = x \cdot x$.

9.3. Теорема Зигеля (второй вариант). *Для любого целого числа $k \neq 0$ взвешенное среднее $w_1 r_{X_1}(k) + \ldots + w_g r_{X_g}(k)$ равняется $\epsilon \prod_{p=2,3,\ldots,\infty} Df_p^{-1}(k)$, где ϵ равно 1/2 или 1 в зависимости от того, равен ранг 2 или больше 2.*

Предположим, например, что X_1 – пространство с внутренним произведением $\langle 1 \rangle \oplus \ldots \oplus \langle 1 \rangle$ ранга n. Тогда род G состоит из всех положительно определенных пространств с внутренним произведением типа I и ранга n. Мы обозначим этот род символом I_n.

Если число n велико, то вклад конечных простых чисел в произведение $\prod Df_p^{-1}(k)$ мал. Преобладает сомножитель

$$Df_\infty^{-1}(k) = \frac{1}{2} n \omega_n k^{n/2-1}.$$

Далее приводится весьма грубая оценка.

9.4. Лемма. *Если $f_p(x_1, \ldots, x_n) = \sum x_i^2$, где $n \geqslant 8$, то произведение плотностей $Df_p^{-1}(k)$ по всем конечным простым числам лежит между 5/6 и 6/5.*

Доказательство будет дано позже.

Следовательно, среднее $w_1 r_{X_1}(k) + \ldots + w_g r_{X_g}(k)$ лежит между $\frac{5}{12} n \omega_n k^{n/2-1}$ и $\frac{6}{10} n \omega_n k^{n/2-1}$.

Конвей и Дж.Томпсон отметили (не опубликовано), что теорема Зигеля может быть использована для доказательства аналога теоремы Минковского–Главки (7.2) для пространств с внутренним произведением (т.е. самодвойственных решеток) над кольцом $\mathbf{Z}$.

Пусть для каждого $n > 0$ через $k(n)$ обозначено ближайшее к $\left(\frac{5}{3}\omega_n^{-1}\right)^{2/n}$ целое число. Ясно, что эта целочисленная функция $k(n)$ асимптотически ведет себя, как $\omega_n^{-2/n} \sim n/2\pi e$ при $n \to \infty$.

9.5. Теорема (Конвей, Томпсон). *Для любой размерности n существует положительно определенное пространство с внутренним произведением X типа* I *и ранга n, для которого*

$$\min_{x \in X \setminus \{0\}} x \cdot x \geqslant k(n).$$

Доказательство. Пусть $k = k(n)$. Можно считать, что $n \geqslant 8$, поскольку $k \leqslant 1$ для меньших значений n. Следовательно, применима лемма 9.4. Если $X_1, \ldots, X_g$ – различные пространства с внутренним произведением рода I_n, то, суммируя по $j = 1, 2, \ldots, k-1$ и используя неравенство

$$j^m \leqslant \int_{m-\frac{1}{2}}^{m+\frac{1}{2}} t^m dt,$$

справедливое при $m \geqslant 1$, мы видим, что взвешенное среднее

$$\sum_{i=1}^{g} w_i(r_{X_i}(1) + r_{X_i}(2) + \ldots + r_{X_i}(k-1))$$

меньше

$$\frac{6}{10} n\omega_n \int_0^{k-\frac{1}{2}} t^{n/2-1} dt = \frac{6}{5}\omega_n\left(k-\frac{1}{2}\right)^{n/2}.$$

Но число $k = k(n)$ было выбрано таким образом, что

$$k - \frac{1}{2} \leqslant \left(\frac{5}{3}\omega_n^{-1}\right)^{2/n}.$$

Следовательно, эта верхняя оценка меньше или равна $\frac{6}{5}\omega_n \frac{5}{3}\omega_n^{-1} = 2$. Поскольку взвешенное среднее меньше 2, то должно существовать некоторое пространство с внутренним произведением $X = X_i$, для которого

$$r_X(1) + r_X(2) + \ldots + r_X(k-1) < 2.$$

Каждое слагаемое $r_X(j)$ является четным неотрицательным це-

лым числом, поэтому неравенство имеет место только в том случае, если

$$r_X(1) = r_X(2) = \ldots = r_X(k-1) = 0.$$

Следовательно,

$$\min_{x \in X \setminus \{0\}} x \cdot x \geqslant k = k(n),$$

что завершает доказательство. □

Приведем некоторые числовые значения. Вычисления показывают, что $k(20) = 2$, $k(37) = 3$, $k(54) = 4$, $k(71) = 5$. Отсюда, например, следует, что при всех $n \geqslant 37$ род I_n содержит пространство X, для которого $\min_{X \setminus \{0\}} x \cdot x \geqslant 3$.

Для пространств типа II могут быть приведены аналогичные рассуждения (см., [66, с. 173]). В этом случае при $n \equiv 0 \pmod 8$ существует пространство X типа II, для которого $\min_{X \setminus \{0\}} x \cdot x$ больше или равен, чем ближайшее к $\left(\frac{5}{3}\omega_n^{-1}\right)^{2/n}$ четное целое число. Например, если $n = 8m \geqslant 48$, то существует пространство ранга n и типа II, для которого $\min_{X \setminus \{0\}} x \cdot x \geqslant 4$.

Интересное приложение теоремы 9.5 было отмечено Стейнбергом (не опубликовано). Для любой решетки L в пространстве $\mathbf{R}^n$ положим

$$m(L) = \min_{x \in X \setminus \{0\}} x \cdot x.$$

Если $L \subset \mathbf{R}^n$ и $L' \subset \mathbf{R}^k$ – решетки, то можно образовать тензорное произведение

$$L \otimes L' \subset \mathbf{R}^n \otimes \mathbf{R}^k \cong \mathbf{R}^{nk}.$$

Ясно, что

$$m(L \otimes L') \leqslant m(L)\, m(L'),$$

и было бы заманчиво предположить, что имеет место равенство.

9.6. Теорема (Стейнберг). *Если в качестве решетки L' взята решетка Γ_8 из § 6, то для любой решетки $L \subset \mathbf{R}^n$ справедливо равенство*

$$m(L \otimes \Gamma_8) = m(L)\, m(\Gamma_8) = 2m(L).$$

С другой стороны, для любой размерности $n \geqslant 292$ существуют

самодвойственные решетки L и L' в пространстве $\mathbf{R}^n$, для которых

$$m(L \otimes L') < m(L)\, m(L').$$

Для доказательства первого утверждения заметим, что решетка $L \otimes \Gamma_8$ может быть описана как множество всех элементов $u_1 \otimes e_1 + \ \ldots \ + u_8 \otimes e_8$ в пространстве $\mathbf{R}^n \otimes \mathbf{R}^8$, для которых $u_i \in \frac{1}{2} L$, $u_1 \equiv u_2 \equiv \ldots \equiv u_8 \pmod{L}$ и $u_1 + \ldots + u_8 \in 2L$. Предположим, что $x = \Sigma u_i \otimes e_i$ является ненулевым элементом в решетке $L \otimes \Gamma_8$. Если $u_1, \ldots, u_8 \in 2L$, то

$$x \cdot x = \Sigma\, u_i \cdot u_i \geqslant m(2L) = 4m(L).$$

Если один из элементов u_i принадлежит решетке L, но не принадлежит подрешетке $2L$, то некоторый другой элемент, скажем u_j, должен также принадлежать решетке L, но не принадлежать подрешетке $2L$. Следовательно, $u_i \neq 0$, $u_j \neq 0$ и

$$x \cdot x \geqslant u_i \cdot u_i + u_j \cdot u_j \geqslant 2m(L).$$

Наконец, если некоторый элемент u_i не принадлежит решетке L, то $u_j \neq 0$ для всех j и, следовательно,

$$x \cdot x \geqslant 8m\left(\frac{1}{2} L\right) = 2\, m(L).$$

Таким образом, $m(L \otimes \Gamma_8) \geqslant 2m(L)$, откуда сразу следует, что имеет место равенство.

Рассмотрим в качестве примера тензорное произведение k экземпляров решетки Γ_8. По индукции легко получаем, что $m(\Gamma_8 \otimes \ldots \otimes \Gamma_8) = 2^k$.

Для доказательства второго утверждения пусть L будет некоторой решеткой в пространстве $\mathbf{R}^n$ и пусть через $L^{\#}$ обозначена двойственная решетка, состоящая из всех элементов $x \in \mathbf{R}^n$, для которых $x \cdot L \subset \mathbf{Z}$. Тензорное произведение $L \otimes L^{\#}$ канонически изоморфно группе $\mathrm{Hom}\,(L, L)$, поэтому решетка $L \otimes L^{\#}$ содержит выделенный элемент e, соответствующий тождественному отображению в L.

В терминах базиса $b_1, \ldots, b_n$ и дуального базиса $b_1^{\#}, \ldots, b_n^{\#}$ имеем

$$e = b_1 \otimes b_1^{\#} + \ldots + b_n \otimes b_n^{\#}.$$

Несложное вычисление показывает, что $e \cdot e = n$. Следовательно,

$$m(L \otimes L^{\#}) \leqslant n.$$

Применим теперь теорему 9.5. Для любой размерности существует пространство с внутренним произведением (т.е. самодвойственная решетка) $L = L^{\#}$, для которой

$$m(L) \geqslant k(n) \sim n/2\pi e.$$

Для больших чисел n это, очевидно, больше $\sqrt{n}$. Действительно, если $n > (2\pi e)^2 = 291{,}708\ldots$, то вычисления показывают, что $k(n) > \sqrt{n}$. Таким образом, выбирая решетку L, для которой

$$m(L) = m(L^{\#}) > \sqrt{n},$$

получаем, что

$$m(L)\,m(L^{\#}) > n \geqslant m(L \otimes L^{\#}),$$

чем и завершается доказательство. □

Теперь опишем еще более общий вариант формулы Зигеля. Вместо того чтобы решать одно уравнение $x \cdot x = k$, предположим, что мы пытаемся решить систему из $t(t+1)/2$ однородных уравнений вида

$$x_i \cdot x_j = K_{ij},$$

где $K = (K_{ij})$ – фиксированная симметрическая $t \times t$-матрица целых чисел, а $x_1, \ldots, x_t$ – неизвестные элементы из пространства X. Мы предполагаем, что $1 \leqslant t \leqslant n$. Пусть через $r_X(k)$ обозначено число решений. Другими словами, $r_X(k)$ является числом элементов в прообразе $f^{-1}(K)$, где

$$f\colon X \times \ldots \times X \quad \to$$

$$\to \text{(аддитивная группа симметрических } t \times t\text{-матриц)}$$

является квадратичной функцией $f(x_1, \ldots, x_n) = (x_i \cdot x_j)$. Как и выше, тензорно домножим все на кольцо $\mathbf{Z}_p$ и образуем соответствующую p-адическую функцию f_p.

9.7. Теорема Зигеля (последний вариант). *Взвешенное среднее*

$$w_1 r_{X_1}(K) + \ldots + w_g r_{X_g}(K),$$

где пространства $X_1, \ldots, X_g$ *представляют различные классы рода пространства* $X = X_1$, *равно*

$$(\epsilon_{n-t-1}/\epsilon_{n-1}) \prod_{p = 2, 3, \ldots, \infty} \epsilon_{n-t}\, Df_p^{-1}(K),$$

где коэффициент ϵ_i *равен* $1/2$ *при* $i = 0$ *и равен* 1 *при* $i \neq 0$.

Очевидно, что эта теорема сводится к предыдущей в случае $n > t = 1$.

Рассмотрим другой крайний случай $n = t > 1$. Выберем базис $b_1, \ldots, b_n$ в пространстве X_1 и предположим, что K_1 является матрицей $(b_i \cdot b_j)$. Тогда $r_{X_1}(K_1)$, очевидно, является числом $|O(X_1)|$ автоморфизмов пространства X_1, тогда как $r_{X_i}(K_1) = 0$ при $i > 1$. Но по определению

$$w_1 = |O(X_1)|^{-1} / \sum_j |O(X_j)|^{-1}$$

Следовательно, взвешенное среднее равно выражению

$$\left(\sum_{j=1}^{g} |O(X_j)|^{-1} \right)^{-1},$$

зависящему только от рода G. Обратная величина

$$M(G) = \sum_{j=1}^{g} |O(X_j)|^{-1}$$

называется обычно *массой*, ассоциированной с родом G. Таким образом, для вычисления массы, ассоцинированной с родом G положительно определенного пространства над кольцом $\mathbf{Z}$, мы имеем более или менее эффективную формулу:

$$M(G) = \prod_{p = 2, \ldots, \infty} \left(\frac{1}{2} D f_p^{-1}(K_1) \right)^{-1}$$

Отметим основное неравенство $g \geqslant 2M(G)$, *где* g *является числом различных классов изоморфных форм в роде* G. Это очевидно,

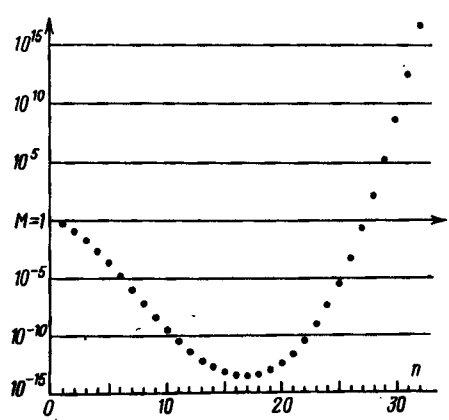


Рис. 4. Масса $M(I_n)$ рода I_n, изображенная в логарифмическом масштабе как функция от ранга n

поскольку каждая группа автоморфизмов $O(X)$ содержит по крайней мере два различных элемента (а именно: 1 и -1).

В качестве примера рассмотрим род I_n, состоящий из всех положительно определенных пространств с внутренним произведением типа I и ранга n. Тогда функция $M(I_n)$ изображена на рис. 4 в быстро сгущающемся логарифмическом масштабе. Для малых значений ранга n масса $M(I_n)$ очень близка к нулю. Например, если $n \leqslant 8$, то масса $M(I_n)$ в точности обратна числу $n! \cdot 2^n$ автоморфизмов n-кратной суммы $\langle 1 \rangle \oplus \ldots \oplus \langle 1 \rangle$. Но для больших значений ранга n масса $M(I_n)$ является очень большим числом. Так, вычисления показывают, что

$$2M(I_{27}) = 0{,}3048\ldots,$$

$$2M(I_{28}) = 208{,}06\ldots,$$

$$2M(I_{29}) = 297\,184{,}9\ldots,$$

$$2M(I_{30}) = 904\,093\,985{,}9\ldots$$

Следовательно, существует по крайней мере 209 различных классов в роде I_{28}, 297 185 – в роде I_{29} и т.д. При $n \to \infty$ число $M(I_n)$ имеет асимптотику

$$C(n/2\pi e\sqrt{e})^{n^2/4}(8\pi e/n)^{n/4}/\sqrt[24]{n},$$

где константа C равна приблизительно 0,705, а $2\pi e\sqrt{e} = 28{,}159\ldots$

Подробности вычисления массы $M(I_n)$ довольно утомительны. Упомянем лишь о том, что множители $\frac{1}{2}Df_p^{-1}(I)$, соответствующие конечным простым числам, достаточно близки к 1 и вносят очень небольшой вклад в окончательный результат.

Поведение функции $n \mapsto M(n)$ целиком обусловлено единственным множителем $\frac{1}{2}Df_\infty^{-1}(I)$. Этот множитель может быть вычислен по формуле

$$Df_\infty^{-1}(I) = \frac{1}{2}\omega_1\,\frac{2}{2}\omega_2\,\frac{3}{2}\omega_3\ldots\frac{n}{2}\omega_n.$$

Дальнейшие подробности будут опущены.

Аналогичные вычисления могут быть выполнены для пространств типа II (см. [66, с. 93]).

Завершая этот параграф, докажем леммы 9.1 и 9.4.

Через $N_n(a)$ обозначим число решений сравнения

$$x_1^2 + \ldots + x_n^2 \equiv a \pmod{p},$$

где p – фиксированное нечетное простое число. В работе Зигеля [25, с. 344] эти числа вычислялись непосредственно с помощью остроумного соображения о гауссовых суммах. Мы используем другой метод.

Пусть (a/p) – символ Лежандра, равный +1 или –1 в зависимости от того, является ли число a квадратом по модулю p или нет. Обычное определение будет удобно расширить соглашением о том, что $(a/p) = 0$ при $a \equiv 0 \pmod p$. При таком соглашении число $N_1(a)$ решений сравнения

$$x^2 \equiv a \pmod p$$

равно в точности $1 + (a/p)$.

Для вычисления числа $N_2(a)$ используем тождество

$$N_2(a) = \sum_{x+y \equiv a \pmod p} N_1(x) N_1(y).$$

Подстановка $1 + (x/p)$ вместо $N_1(x)$ дает

$$N_2(a) = \sum_{x+y \equiv a} \left(1 + \left(\frac{x}{p}\right) + \left(\frac{y}{p}\right) + \left(\frac{xy}{p}\right)\right).$$

Но ясно, что сумма символов (x/p) по всем классам x вычетов по модулю p равна нулю. Следовательно,

$$N_2(a) = p + 0 + 0 + \sum_{x+y \equiv a} \left(\frac{xy}{p}\right).$$

Предположим сначала, что $a = 0$. Тогда каждое слагаемое $\left(\frac{xy}{p}\right) = \left(\frac{-x^2}{p}\right)$ равно либо $\left(\frac{-1}{p}\right)$ при $x \not\equiv 0 \pmod p$, либо нулю при $x \equiv 0 \pmod p$. Следовательно,

$$(1) \quad N_2(0) = p + (p-1)\left(\frac{-1}{p}\right).$$

С другой стороны, если a взаимно просто с p, то сумма

$$\sum_{x+y \equiv a} \left(\frac{xy}{p}\right)$$

не зависит от a, поскольку если $x + y \equiv a$, то для любого взаимно простого с p числа u имеем $ux + uy \equiv ua$ и

$$\left(\frac{uxuy}{p}\right) = \left(\frac{xy}{p}\right).$$

Таким образом,

$$N_2(1) = N_2(2) = \ldots = N_2(p-1).$$

Но очевидно, что сумма

$$N_2(0) + N_2(1) + \ldots + N_2(p-1)$$

равна p^2, т.е. общему числу пар (x_1, x_2) по модулю p. Следовательно, для любого взаимно простого с p числа u

$$N_2(u) = N_2(1) = (p^2 - N_2(0))/(p-1).$$

Подставляя равенство (1), получаем

$$(2) \quad N_2(u) = p - \left(\frac{-1}{p}\right).$$

Удобно ввести сокращение $s = \left(\frac{-1}{p}\right)p^{-1}$ и записать обе формулы следующим образом:

$$N_2(u) = p(1-s),$$

и

$$N_2(0) = N_2(u) + p^2 s.$$

Теперь, используя тождество

$$N_{2m+2}(a) = \sum_{x+y=a} N_{2m}(x) N_2(y)$$

и индукцию по m, покажем, что для любого положительного целого числа m

$$(3) \quad N_{2m}(u) = p^{2m-1}(1 - s^m)$$

и

$$(4) \quad N_{2m}(0) = N_{2m}(u) + p^{2m} s^m.$$

В более общем случае, пусть через $N_n(a \bmod p^k)$ обозначено число n-к $x_1, \ldots, x_n$ из вычетов по модулю p^k, удовлетворяющих сравнению

$$(5) \quad x_1^2 + \ldots + x_n^2 \equiv a \pmod{p^k}.$$

Эти числа могут быть вычислены следующим образом. Предположим, что $a = p^v u$, где $v < k$ и u взаимно просты с p.

Случай 1. Если $v = 0$, т.е. $a = u$ является обратимым p-адическим числом, то число $N_n(u \bmod p^k)$ равно

$$p^{(n-1)(k-1)} N_n(u),$$

поскольку каждое решение сравнения

$$\xi_1^2 + \ldots + \xi_n^2 \equiv u \pmod{p}$$

поднимается в точности до $p^{(n-1)(k-1)}$ решений по модулю p^k. Чтобы увидеть это, отметим, что компоненты ξ_i не могут все делиться на p. Если, скажем, $\xi_1 \not\equiv 0 \pmod{p}$, то легко выводится, что для любых выбранных вычетов $x_1, \ldots, x_n$ по модулю p^k, таких, что

$$x_2 \equiv \xi_2, \ldots, x_n \equiv \xi_n \pmod{p},$$

вычет x_1 по модулю p^k определяется однозначно.

Случай 2. Даже при $v \geqslant 1$ сравнение

$$\xi_1^2 + \ldots + \xi_n^2 \equiv p^v u \equiv 0 \pmod{p}$$

все еще может иметь решения, для которых не все ξ_i делятся на p. Общее число таких решений равно $N_n(0) - 1$. Повторяя рассуждения случая 1, получаем, что число решений уравнения (5), в которых не все компоненты x_i делятся на p, равно $p^{(n-1)(k-1)}(N_n(0) - 1)$.

Случай 3. Если $v \geqslant 2$, то уравнение (5) может иметь решения, для которых все компоненты x_i делятся на p. Общее число таких решений равно

$$p^n N_n(p^{v-2}u \pmod{p^{k-2}}),$$

поскольку каждое решение сравнения

$$\xi_1^2 + \ldots + \xi_n^2 \equiv p^{v-2}u \pmod{p^{k-2}}$$

поднимается в точности до p^n решений уравнения (5), удовлетворяющих условиям

$$x_1 \equiv p\xi_1, \ldots, x_n \equiv p\xi_n \pmod{p^{k-1}}.$$

Комбинируя случаи 1, 2, 3 с явными формулами (3) и (4) для $N_{2m}(u)$ и $N_{2m}(0)$ индукцией по v получаем теперь следующий результат.

9.8. Лемма. *Если* $0 \leqslant v < k$, *то число* $N_{2m}(p^v u \bmod p^k)$ *решений сравнения*

$$x_1^2 + \ldots + x_{2m}^2 \equiv p^v u \pmod{p^k}$$

равно

$$p^{(2m-1)k}(1-s^m)(1+ps^m+p^2s^{2m}+\ldots+p^v s^{vm}),$$

где $s = \left(\frac{-1}{p}\right) p^{-1}$.

Доказательство леммы 9.1 для нечетных p.

Пусть $Df_p^{-1}\colon \mathbf{Z}_p \to \mathbf{R}$ – плотность, ассоциированная с отображением $f_p(x_1, \ldots, x_{2m}) = x_1^2 + \ldots + x_{2m}^2$. Сравнивая определение плотности Df_p^{-1} с леммой 9.8, легко выводим, что

$$Df_p^{-1}(p^v u) = (1-s^m)(1+ps^m+p^2s^{2m}+\ldots+p^v s^{vm}).$$

Проверка показывает, что это выражение равно выражению, используемому в формулировке леммы 9.1.

В случае $p = 2$ доказательство аналогично. Отметим сначала, что число решений $N_n(a \bmod 8)$ сравнения $x_1^2 + \ldots + x_n^2 \equiv a \pmod 8$ равно сумме числа

$$2^{3n-3} + 2^{5n/2-2}\cos\left(\frac{\pi}{4}(2a-n)\right)$$

и поправочного члена

$$(-1)^{(a-n)/4}2^{2n-1} \quad \text{при } a \equiv n \pmod 4.$$

Действительно, легко видеть, что число решений сравнения, для которых нечетны ровно t чисел из $x_1, \ldots, x_n$, равно:

$$\binom{n}{t}2^{2n-1} \quad \text{при } 0 \leqslant t < n \text{ и } t \equiv a \pmod 4;$$

$$2^{2n} \quad \text{при } t = n \equiv a \pmod 8;$$

$$0 \quad \text{при } t \not\equiv a \pmod 4 \text{ или } t = n \not\equiv a \pmod 8.$$

Сумма биномиальных коэффициентов $\binom{n}{t}$ по всем $t \equiv a \pmod 4$ может быть вычислена через биномиальные разложения для выражений $(1 \pm 1)^n$ и $(1 + i)^n$. Отсюда легко выводится приведенное выражение для $N_n(a \bmod 8)$.

Точно так же, как и в случае нечетного числа p, теперь для больших k можно вычислить число

$$N_n(a \bmod 2^k)$$

и, следовательно, можно вычислить плотность 2-адических решений. Подробности оставлены читателю. □

Доказательство леммы 9.4. Будет удобно подчеркнуть, используя символ $\delta_n = \delta_{n,p}$, зависимость от n функции плотности $Df_p^{-1}\colon \mathbf{Z}_p \to \mathbf{R}$, связанной с суммой n квадратов. Мы должны найти верхнюю и нижнюю оценки для произведения $\prod_p \delta_{n,p}(k)$.

Сначала рассмотрим случай $n = 8$, когда

$$\delta_8(p^v u) = (1 - p^u)(1 + p^{-3} + p^{-6} + \ldots + p^{-3v})$$

при нечетных p. Очевидно, функция δ_8 достигает минимума $1 - p^{-4}$ при $v = 0$ и стремится к максимуму

$$(1 - p^{-4})(1 + p^{-3} + p^{-6} + \ldots) = (1 - p^{-4})/(1 - p^{-3})$$

при $v \to \infty$ (или при $p^v u \to 0$). Аналогично, при $p = 2$ функция

$$\delta_{8,2}(2^v u) = 1 + 8^{-1} + 8^{-2} + \ldots + 8^{1-v} - 8^v$$

достигает минимума 7/8 при $v = 1$ и стремится к максимуму 8/7 при $v \to \infty$. Следовательно, произведение

$$\prod_{p \text{ конечно}} \delta_{8,p}(k),$$

где переменная k принимает значения в кольце $\mathbf{Z}$, достигает минимума

$$\frac{7}{8} \prod_{p \text{ нечетно}} (1 - p^{-4}) = \frac{14}{15}\zeta(4)^{-1} = 0{,}862\ldots$$

при $k = 2$ и максимума

$$\frac{8}{7} \prod_{p \text{ нечетно}} (1 - p^{-4})/(1 - p^{-3}) =$$

$$= \frac{16}{15}\zeta(3)/\zeta(4) = 1{,}184\ldots.$$

при $k = 0$. Поскольку эти оценки лежат между 5/6 и 6/5, то этим завершается доказательство леммы 9.4 в случае $n = 8$.

Но любая верхняя или нижняя оценка для $\delta_{8,p}$ автоматически является верхней или нижней оценкой для $\delta_{n,p}$ при любом $n \geqslant 8$. Действительно, деля обе части тождества

$$N_{m+n}(a \bmod p^k) =$$

$$= \sum_{x+y \equiv a \,(\mathrm{mod}\, p^k)} N_m(x \bmod p^k) N_n(y \bmod p^k)$$

на $p^{(m+n-1)k}$ и переходя к пределу при $k \to \infty$, мы получаем формулу свертки:

$$\delta_{m+n}(a) = \int \delta_m(x)\,\delta_n(a - x)\,dx.$$

Таким образом, если $\delta_8(x) \leqslant c$ при любом x, то отсюда сразу следует, что для любого a

$$\delta_{m+8}(a) \leqslant \int \delta_m(x) c\,dx = c.$$

Этим завершается доказательство леммы. □

Глава 3

ПРОСТРАНСТВА С ВНУТРЕННИМ ПРОИЗВЕДЕНИЕМ НАД ПОЛЕМ

В этой главе будет описан ряд наиболее ярких результатов из теории колец Витта $W(F)$ над произвольным полем F. Наиболее тщательно будут проводиться доказательства, справедливые также и в характеристике 2. Классическая теория для числовых полей, описанная, например, в [61], в значительной степени остается вне нашего рассмотрения.

§ 1. Анизотропные пространства с внутренним произведением

Пространство с внутренним произведением X является *анизотропным*, если из $x \cdot x = 0$ следует $x = 0$. В этом параграфе будет показано, что каждый элемент кольца Витта $W(F)$ представляется анизотропным пространством с внутренним произведением, определяемым однозначно с точностью до изоморфизма. Сначала отметим следующее утверждение.

1.1. Лемма. *Любое пространство с внутренним произведением X над полем F изоморфно ортогональной сумме $S \oplus A$, где пространство S расщепляемо, а пространство A анизотропно.*

Доказательство. Если пространство X само анизотропно, то можно просто положить $S = 0$. В противном случае существует вектор $x \neq 0$, такой, что $x \cdot x = 0$, и можно выбрать вектор y, для которого $x \cdot y = 1$. Тогда векторы x и y порождают подпространство $S_1 \subset X$ с матрицей внутреннего произведения $\begin{pmatrix} 0 & 1 \\ 1 & * \end{pmatrix}$. Ясно, что подпространство S_1 расщепляемо и

$$X \cong S_1 \oplus S_1^{\perp}.$$

Применяя эту же конструкцию к пространству $S_1^{\perp}$ и проводя индукцию, легко завершить доказательство. □

Выбирая такое разложение $X \cong S \oplus A$, мы хотим показать, что анизотропное слагаемое определено однозначно с точностью до изоморфизма. Если характеристика поля F не равна 2, то это легко

доказывается с помощью теоремы 4.4 и леммы 6.3 гл. 1. Приведем другие соображения, работающие также и в случае характеристики 2.

Определим *индекс изотропии* $i(X)$ пространства с внутренним произведением X как максимальную размерность самоортогональных подпространств $N \subset X$, т.е. таких подпространств, что $N \cdot N = 0$.

1.2. Лемма. *Для любого пространства с внутренним произведением X индекс изотропии удовлетворяет неравенству*

$$0 \leqslant 2i(X) \leqslant \mathrm{rk}(X),$$

где в первом случае равенство имеет место тогда и только тогда, когда пространство X анизотропно, а во втором – когда пространство X расщепляемо.

Доказательство. Если $N \cdot N = 0$, то $N \subset N^{\perp}$ и, следовательно,

$$\mathrm{rk}(N) \leqslant \mathrm{rk}(N^{\perp}) = \mathrm{rk}(X) - \mathrm{rk}(N),$$

где равенство имеет место тогда и только тогда, когда $N = N^{\perp}$. Дальнейшие рассуждения очевидны. □

Нам понадобится следующая оценка сверху.

1.3. Основная лемма. *Если пространство A анизотропно, а X – произвольное пространство с внутренним произведением, то*

$$i(X \oplus A) + i(X) \leqslant \mathrm{rk}(X).$$

Доказательство основывается на следующей интерпретации индекса $i(X \oplus A)$. Назовем линейное отображение

$$f: X \to Y$$

антиизометрией, если $f(x) \cdot f(x') = -x \cdot x'$ для любых элементов x и x' из пространства X.

1.4. Лемма. *Если пространства X и A такие, как описано выше, то самоортогональное подпространство $N \subset X \oplus A$ ранга n существует тогда и только тогда, когда существуют подпространство $M \subset X$ ранга n и антиизометрия $f: M \to A$.*

Доказательство. Если дана такая антиизометрия f, то через $N \subset X \oplus A$ обозначим график отображения f, состоящий из всех пар (x, a), где $x \in M$ и $f(x) = a$. Для любых двух пар $(x, f(x))$ и $(x', f(x'))$ из графика имеем

$$(x, f(x)) \cdot (x', f(x')) = x \cdot x' + f(x) \cdot f(x') = 0.$$

Таким образом, N – самоортогональное подпространство ранга n, что и требовалось показать.

Обратно, если дано подпространство $N \subset X \oplus A$, для которого $N \cdot N = 0$, то отметим, что подпространство N пересекается с анизотропным подпространством $0 \oplus A$ только по нулевому вектору. Если каждая из пар (x, a) и (x, a') принадлежит подпространству N, то отсюда следует, что $a = a'$. Таким образом, подпространство

N может быть отождествлено с графиком линейного отображения $f: M \to A$ некоторого подпространства $M \subset X$. Поскольку подмодуль N самоортогонален, то отображение f является антиизометрией. □

Доказательство леммы 1.3 проводится индукцией по рангу пространства $X \oplus A$. Можем предполагать, что $A \neq 0$, поскольку при $A = 0$ неравенство следует из леммы 1.2.

Для данной антиизометрии $f: M \to A$, где $M \subset X$, надо найти верхнюю оценку для ранга подпространства M. Через M_0 обозначим ядро отображения f, а через M_1 обозначим дополняющее его прямое слагаемое, т.е.

$$M = M_0 + M_1, \qquad 0 = M_0 \cap M_1.$$

Тогда подпространство M_1 вкладывается в подпространство A и, таким образом, подпространство M_1 анизотропно. Следовательно, ограничение внутреннего произведения на подпространство M_1 является внутренним произведением и

$$X \cong M_1^{\perp} \oplus M_1.$$

Применяя предположение индукции, заключаем, что

$$i(X) + i(M_1^{\perp}) \leqslant \mathrm{rk}(M_1^{\perp}).$$

Но $M_0 \cdot M = 0$, так что M_0 является самоортогональным подпространством в пространстве $M_1^{\perp}$ и

$$\mathrm{rk}(M_0) \leqslant i(M_1^{\perp}).$$

Складывая эти два неравенства и добавляя к обеим частям $\mathrm{rk}(M_1) - i(M_1^{\perp})$, получаем

$$i(X) + \mathrm{rk}(M) \leqslant \mathrm{rk}(X).$$

Следовательно, по лемме 1.4

$$i(X) + i(X \oplus A) \leqslant \mathrm{rk}(X),$$

что завершает доказательство. □

В качестве примера рассмотрим случай, когда пространство $X = S$ расщепляемо. Тогда неравенство $i(S \oplus A) \leqslant \mathrm{rk}(S) - i(S) = i(S)$ влечет равенство $i(S \oplus A) = i(S)$.

1.5. Следствие. *Предположим, что ортогональная сумма $S \oplus A$ расщепляема, где пространство S расщепляемо, а пространство A анизотропно. Тогда $A = 0$.*

Подставляя $i(S \oplus A) = \frac{1}{2}\mathrm{rk}(S \oplus A)$ в неравенство $i(S \oplus A) + i(S) \leqslant \mathrm{rk}(S)$, получаем, что $\frac{1}{2}\mathrm{rk}(S \oplus A) \leqslant \mathrm{rk}(S) - i(S) = \frac{1}{2}\mathrm{rk}(S)$, и поэтому $\mathrm{rk}(A) \leqslant 0$.

1.6. Следствие. *Пространство с внутренним произведением X представляет нулевой элемент в кольце Витта тогда и только тогда, когда пространство X расщепляемо.*

Действительно, если пространство X принадлежит классу Витта пространства 0, то существуют расщепляемые пространства S' и S'', такие, что

$$X \oplus S' \cong 0 \oplus S''$$

В силу леммы 1.1

$$X \cong A \oplus S$$

и поэтому пространство $A \oplus S \oplus S'$ расщепляемо. Следовательно $A = 0$ и пространство X расщепляемо.

1.7. Теорема. *Каждый элемент кольца Витта $W(F)$ представляется единственным, с точностью до изоморфизма, анизотропным пространством с внутренним произведением.*

Доказательство. Если два анизотропных пространства с внутренним произведением A и A' принадлежат одному и тому же классу Витта, $A \sim A'$, то мы должны доказать, что $A \cong A'$. Рассмотрим пространство с внутренним произведением $B' = \langle -1 \rangle \otimes A'$. Тогда пространство $A' \oplus B'$ расщепляемо, так что из следствия 1.6 следует, что пространство $A \oplus B' \sim A' \oplus B'$ расщепляемо. Поэтому, согласно лемме 1.4, существуют подпространство $M \subset A$ и антиизометрия

$$f: M \to B',$$

такие, что

$$\operatorname{rk}(M) = i(A \oplus B') = \frac{1}{2} \operatorname{rk}(A \oplus B').$$

Но подпространство M анизотропно, поэтому отображение f имеет тривиальное ядро и

$$\operatorname{rk}(M) \leqslant \operatorname{rk}(A), \quad \operatorname{rk}(M) \leqslant \operatorname{rk}(B').$$

Отсюда вытекает, что $\operatorname{rk}(M) = \operatorname{rk}(A) = \operatorname{rk}(B')$. Следовательно, $M = A$, а f является антиизометрией из пространства A на пространство B'. Таким образом, пространство A антиизометрично пространству B' и, следовательно, изоморфно пространству A', что завершает доказательство. □

Таким образом, кольцо Витта $W(F)$ может быть отождествлено с множеством классов изоморфных анизотропных пространств с внутренним произведением над полем F. Для полного завершения картины необходим еще один фрагмент.

1.8. Определение. Пусть для каждого элемента w кольца Витта $W(F)$ через $\| w \|$ обозначается ранг единственного анизотропного представителя элемента w.

Иначе говоря, выбирая произвольного представителя X класса Витта w, мы можем положить

$$\| w \| = \mathrm{rk}(X) - 2i(X).$$

Очевидно, что

$$\| w \| \geqslant 0,$$

причем равенство выполняется только при $w = 0$. Отметим также неравенства

$$\| w \pm w' \| \leqslant \| w \| + \| w' \|,$$

$$\| ww' \| \leqslant \| w \| \ \| w' \|$$

и

$$\| 1 \| = 1.$$

§ 2. Упорядоченные поля

В основном этот параграф является обзором результатов об упорядоченных полях. В нем изучается "полная сигнатура" $\sigma(X)$ пространства с внутренним произведением над полем F. Это некоторый Ω-набор целых чисел, где Ω является множеством всех упорядочений поля F.

2.1. Определение. *Упорядочением* поля F называется подмножество $P \subset F^*$, замкнутое относительно сложения и умножения и удовлетворяющее равенству

$$P \cup (-P) = F^*.$$

Элементы подмножества P называются *положительными* (или *строго положительными*). Если $\xi - \eta \in P$, то используется обозначение $\xi > \eta$.

Отметим, что подмножества P и $-P$ обязательно не пересекаются, поскольку если бы элемент ξ и элемент $-\xi$ принадлежали подмножеству P, то сумма $\xi + (-\xi)$ должна была бы принадлежать подмножеству P. Но это противоречит предположению о том, что $P \subset F^*$.

В упорядоченном поле каждый ненулевой квадрат положителен. Действительно, если $\xi \neq 0$, то либо $\xi \in P$, либо $-\xi \in P$, и в любом случае отсюда следует, что $\xi^2 = (-\xi)^2 \in P$.

Характеристика упорядоченного поля всегда равна 0. Действительно, поскольку $1 = 1^2 \in P$, то любая сумма $1 + 1 + \ldots + 1$ принадлежит подмножеству P. Следовательно, никакая из таких сумм не может равняться 0 в поле F.

2.2. Теорема Артина–Шрейера. *Поле F обладает упорядочением тогда и только тогда, когда -1 не является суммой квадратов в поле F.*

Поле, в котором -1 не является суммой квадратов, называется "формально вещественным" полем, а иногда просто "вещественным" полем.

Доказательство. Если поле F обладает упорядочением P, то $1 \in P$. Следовательно, $-1 \notin P$ и -1 не может быть суммой квадратов.

Обратно, пусть F – поле, в котором -1 не является суммой квадратов. Под *частичным упорядочением* поля F мы будем подразумевать любое подмножество множества F^*, замкнутое относительно сложения и умножения. Одно частичное упорядочение P_0 может быть построено следующим образом. Пусть P_0 – множество всех сумм ненулевых квадратов в поле F. Тогда подмножество P_0, очевидно, замкнуто относительно сложения и умножения, а если бы 0 принадлежал подмножеству P_0, то из уравнения

$$0 = \xi_1^2 + \ldots + \xi_n^2$$

с $\xi_1 \neq 0$ следовало бы

$$-1 = (\xi_2/\xi_1)^2 + \ldots + (\xi_n/\xi_1)^2,$$

что противоречит нашему предположению.

По лемме Цорна частичное упорядочение P_0 содержится в некотором максимальном (относительно включения) частичном упорядочении P поля F.

Мы докажем, что если $\xi \neq 0$, *то либо* $\xi \in P$, *либо* $-\xi \in P$. Этим будет показано, что P является упорядочением поля F. Рассмотрим подмножество

$$Q = P \cup \xi P \cup (P + \xi P)$$

поля F, аддитивно порожденное подмножествами P и ξP. Если подмножество Q содержит 0, то, полагая $0 = \pi' + \xi\pi$, где элементы π и π' из подмножества P, мы получим

$$-\xi = \pi'/\pi = \pi'\pi(\pi^{-1})^2 \in P.$$

(Каждый ненулевой квадрат принадлежит подмножеству P, поскольку $P \supset P_0$.) С другой стороны, если подмножество Q не содержит 0, то оно, очевидно, является частичным упорядочением поля F. Но подмножество Q содержит максимальное частичное упорядочение P. Поэтому $Q = P$ и, следовательно, $\xi \in P$. Это показывает, что P является упорядочением поля F, чем и завершается доказательство. □

Читателю предлагается несколько отклониться от основной линии изложения.

2.3. Упражнение. Пусть F – поле характеристики, отличной от 2. Используя аналогичные методы, докажите, что элемент поля $\xi \neq 0$ может быть представлен в виде суммы квадратов в том и только в том случае, если $\xi \in P$ для любого упорядочения P поля F. (Такой элемент ξ называется "вполне положительным".) В частности, если поле F вообще не имеет упорядочений, то любой элемент поля F является суммой квадратов.

Классический случай может быть описан следующим образом

2.4. Пример. *Если F – алгебраическое расширение поля рациональных чисел $\mathbf{Q}$, то любое упорядочение поля F индуцируется вложением $\varphi\colon F \to \mathbf{R}$. Если расширение F имеет конечную степень n над полем $\mathbf{Q}$, то поле F имеет не более n различных упорядочений.*

С другой стороны, для полей бесконечной степени над $\mathbf{Q}$, таких как $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)$, может существовать бесконечное число различных упорядочений.

Доказательство утверждения 2.4. Поле рациональных чисел имеет только одно упорядочение, поскольку любое положительное число m/n может быть представлено как mn-кратная сумма квадратов $n^{-2} + \ldots + n^{-2}$. Таким образом, любое упорядочение поля F индуцирует обычное упорядочение на подполе $\mathbf{Q} \subset F$. Отметим, что ни один элемент ξ поля F не может для всех элементов $q \in \mathbf{Q}$ удовлетворять условию $\xi > q$. Если бы такой элемент ξ существовал, то, проводя индукцию, легко показать, что при любом $n \geqslant 1$ и любых коэффициентах $q_1, \ldots, q_n \in \mathbf{Q}$

$$\xi^n + q_1 \xi^{n-1} + \ldots + q_n > 1.$$

(Шаг индукции состоит в домножении неравенства на элемент ξ и учете того, что $\xi > 1 - q_{n+1}$.) Следовательно, элемент ξ не мог бы быть алгебраическим, что противоречит нашему предположению.

Таким образом, любой элемент ξ поля F задает дедекиндово сечение в поле $\mathbf{Q}$. Если положить

$$\varphi(\xi) = \sup\{q \in \mathbf{Q} \mid q < \xi\} = \inf\{q \in \mathbf{Q} \mid q > \xi\},$$

то ясно, что функция φ аддитивна и что $\varphi(\xi\eta) = \varphi(\xi)\,\varphi(\eta)$, по крайней мере когда $\xi > 0$ и $\eta > 0$. Но тождества $\varphi(-\xi) = -\varphi(\xi)$ и $\varphi(1) = 1$ также очевидны. Следовательно, отображение $\varphi\colon F \to \mathbf{R}$ является кольцевым гомоморфизмом. Его ядро равно нулю, поскольку F – поле.

Если расширение F конечно над полем $\mathbf{Q}$ и имеет степень n, то $F = \mathbf{Q}(\xi)$ для некоторого элемента ξ, а неприводимое уравнение для элемента ξ над полем $\mathbf{Q}$ может иметь не более чем n вещественных корней. Этим завершается доказательство утверждения 2.4. □

Теперь давайте посмотрим на пространства с внутренним произведением над полем F, на которых заданы некоторые упорядочения (сравните со с. 34).

Определение. Пространство с внутренним произведением X над полем F называется *положительно определенным*, если $x \cdot x \in P$ для любого ненулевого вектора x из пространства X, и *отрицательно определенным*, если $x \cdot x \in -P$ для любого ненулевого вектора x из пространства X.

2.5. Теорема инерции (Якоби, Сильвестр). *Любое пространство с внутренним произведением X изоморфно ортогональной сумме $X^+ \oplus X^-$, где подпространство X^+ положительно определено, а подпространство X^- отрицательно определено. Ранги подпространств X^+ и X^- являются инвариантами при изоморфизмах пространства X.*

Это значит, что эти ранги не зависят от конкретного выбора подпространств X^+ и X^-.

Доказательство. Выбрав ортогональный базис $e_1, \ldots, e_r$ в пространстве X, возьмем в качестве подпространства X^+ подпространство, порожденное теми из векторов e_i, для которых $e_i \cdot e_i > 0$, а в качестве подпространства X^- — подпространство, порожденное теми из векторов e_i, для которых $e_i \cdot e_i < 0$. Тогда, очевидно, что $X \cong X^+ \oplus X^-$, где подпространство X^+ положительно определено, а подпространство X^- отрицательно определено.

Пусть теперь Y — произвольное положительно определенное подпространство пространства X. Тогда $Y \cap X^- = 0$ и, значит,

$$\mathrm{rk}(Y) \leqslant \mathrm{rk}(X) - \mathrm{rk}(X^-) = \mathrm{rk}(X^+).$$

Следовательно, $\mathrm{rk}(X^+)$ может быть охарактеризован как максимальная возможная размерность положительно определенного подпространства пространства X. Это показывает, что он является инвариантом относительно изоморфизмов, и завершает доказательство. □

Определение. Разность $\mathrm{rk}(X^+) - \mathrm{rk}(X^-)$ называется *сигнатурой* пространства с внутренним произведением X относительно упорядочения P. Для этой сигнатуры мы будем использовать обозначение

$$\sigma_P(X) \in \mathbf{Z}.$$

Очевидно, что сигнатура $\sigma_P(X)$ также является инвариантом пространства X относительно изоморфизмов.

Отметим, что в случае пространства с внутренним произведением $\langle \alpha \rangle$ ранга 1 сигнатура $\sigma_P\langle \alpha \rangle$ является в точности тем, что обычно называется *знаком* элемента поля α в упорядочении P, т.е.

сигнатура $\sigma_P\langle\alpha\rangle$ равна +1 или −1 в соответствии с тем, положителен или отрицателен элемент α.

2.6. Лемма. *Сигнатура $\sigma_P(X)$ зависит только от класса Витта пространства X. Кроме того,*

$$\sigma_P(X \oplus Y) = \sigma_P(X) + \sigma_P(Y),$$

$$\sigma_P(X \otimes Y) = \sigma_P(X)\,\sigma_P(Y)$$

и

$$\sigma_P\langle 1\rangle = 1.$$

Таким образом, сигнатура σ_P задает корректно определенный гомоморфизм из кольца Витта $W(F)$ в кольцо целых чисел $\mathbf{Z}$.

Доказательство леммы 2.6. Если S – расщепляемое пространство с внутренним произведением, то из леммы 6.3 гл. 1 следует, что пространство S изоморфно ортогональной сумме экземпляров пространства $\langle 1\rangle \oplus \langle -1\rangle$. Следовательно, сигнатура $\sigma_P(S)$ равна нулю. (Или, более прямо, если подпространство $N \subset S$ самоортогонально, то использовавшиеся в доказательстве теоремы 2.5 рассуждения показывают также, что $\operatorname{rk}(N) \leqslant \operatorname{rk}(S^+)$ и $\operatorname{rk}(N) \leqslant \operatorname{rk}(S^-)$. Поэтому если $\operatorname{rk}(N) = \frac{1}{2}\operatorname{rk}(S)$, то отсюда следует, что $\operatorname{rk}(N) = \operatorname{rk}(S^+) = \operatorname{rk}(S^-)$, а сигнатура равна нулю.)

Представляя теперь пространства X и Y в виде суммы пространств ранга 1 и используя очевидное тождество

$$\sigma_P(\langle\alpha_1\rangle \oplus \ldots \oplus \langle\alpha_r\rangle) = \sigma_P\langle\alpha_1\rangle + \ldots + \sigma_P\langle\alpha_r\rangle,$$

мы сводим оставшуюся часть доказательства к простым вычислениям. □

2.7. Следствие. *Предположим, что F – упорядоченное поле, в котором каждый положительный элемент – квадрат. Тогда отображение σ_P: $W(F) \to \mathbf{Z}$ является изоморфизмом.*

Например, кольцо Витта поля действительных чисел $\mathbf{R}$ изоморфно кольцу $\mathbf{Z}$. Доказательство непосредственно следует из теоремы 2.5 и леммы 2.6.

Замечание. В стандартных учебниках по алгебре показывается, что имеется взаимно однозначное соответствие между упорядочениями поля F и классами изоморфных "вещественных замыканий" поля F. Вещественное замыкание F_P, связанное с некоторым упорядочением P, может быть охарактеризовано как максимальное согласованно упорядоченное алгебраическое расширение поля F. Любой положительный элемент поля F_P является квадратом, и, следовательно, кольцо Витта $W(F_P)$ изоморфно кольцу $\mathbf{Z}$. Легко выводится, что гомоморфизм сигнатуры σ_P: $W(F) \to \mathbf{Z}$ мо-

жет быть отождествлен с естественным кольцевым гомоморфизмом $W(F) \to W(F_P)$.

Рассмотрим теперь множество $\Omega = \Omega(F)$, состоящее из всех возможных упорядочений данного поля F. На множестве Ω введем топологию следующим образом.

Определение. Для каждого элемента $\xi \in F^*$ пусть $U_\xi \subset \Omega$ – множество всех упорядочений P, для которых $\xi \in P$. Тогда множества U_ξ порождают требуемую топологию. (Другими словами, подмножество пространства Ω открыто тогда и только тогда, когда оно является объединением конечных пересечений множеств U_ξ.)

2.8. Лемма. *Топологическое пространство Ω компактно и вполне несвязно. Для любого пространства с внутренним произведением X над полем F функция*

$$P \mapsto \sigma_P(X)$$

из пространства Ω в кольцо $\mathbf{Z}$ непрерывна.

Определение. Эта функция $P \mapsto \sigma_P(X)$ будет называться *полной сигнатурой* $\sigma(X)$ пространства с внутренним произведением X.

Доказательство леммы 2.8. Сначала рассмотрим пространство с внутренним произведением $\langle \xi \rangle$ ранга 1. Тогда прообразом $+1$ для функции полной сигнатуры

$$P \mapsto \sigma_P\langle \xi \rangle$$

является открытое множество $U_\xi \subset \Omega$, а прообразом -1 – дополнительное открытое множество $U_{-\xi}$. Таким образом, функция полной сигнатуры пространства $\langle \xi \rangle$ непрерывна, откуда легко выводится непрерывность функции полной сигнатуры, ассоциированной с любым пространством с внутренним произведением $X \cong \langle \xi_1 \rangle \oplus \ldots \oplus \langle \xi_r \rangle$.

Поскольку пространство Ω при любом $\xi \in F^*$ является объединением непересекающихся открытых множеств U_ξ и $U_{-\xi}$, то легко проверить, что пространство Ω хаусдорфово и вполне несвязно. Для доказательства компактности мы введем пространство 2^F, состоящее из всех подмножеств пространства F. На нем введем топологию декартова произведения. Для этого отождествим каждое подмножество пространства F с его характеристической функцией $F \to \{0, 1\}$ и, следовательно, отождествим пространство 2^F с декартовым произведением экземпляров пространства $\{0, 1\}$ по одному экземпляру на каждый элемент пространства F. Это произведение компактно по теореме А.Н. Тихонова.

Любое упорядочение пространства F может рассматриваться как элемент пространства 2^F, поэтому пространство Ω вложено как подмножество в пространство 2^F. Очевидно, что построенная нами

на пространстве Ω топология является в точности топологией ограничения, которую пространство Ω получает как подмножество пространства 2^F. В действительности пространство Ω является замкнутым подмножеством пространства 2^F, поскольку если подмножество $Q \subset F$ не является упорядочением, то в пространстве 2^F легко построить окрестность множества Q, не содержащую ни одного упорядочения. Это доказывает, что пространство Ω компактно, и завершает доказательство леммы 2.8. □

2.9. Определение. Через $\mathbf{Z}^\Omega$ обозначим кольцо, состоящее из всех непрерывных функций из пространства Ω в кольцо $\mathbf{Z}$. Очевидно, что для любого пространства с внутренним произведением X над полем F функция полной сигнатуры $\sigma(X)$ является элементом этого кольца $\mathbf{Z}^\Omega$. Поскольку функция σ аддитивна и мультипликативна, а значение $\sigma(X)$ зависит только от класса Витта пространства X, мы получим корректно определенный кольцевой гомоморфизм

$$\sigma\colon W(F) \to \mathbf{Z}^\Omega.$$

(Конечно, если множество Ω пусто, то $\mathbf{Z}^\Omega$ – нулевое кольцо и эта конструкция не особенно интересна.)

Замечание. Если пространство Ω содержит более одного элемента, то гомоморфизм σ не является эпиморфизмом. Действительно, для любого пространства с внутренним произведением X и любого упорядочения P выполняется сравнение

$$\sigma_P(X) \equiv \operatorname{rk}(X) \pmod 2.$$

Следовательно, в зависимости от того, четен ранг пространства X или нет, полная сигнатура

$$\sigma(X) \in \mathbf{Z}^\Omega$$

должна быть конгруэнтна либо 0, либо 1.

Для того чтобы определить точный образ отображения $\sigma\colon W(F) \to \mathbf{Z}^\Omega$, необходимо знать, в какой степени возможно задать знаки элемента в различных упорядочениях поля F.

2.10. Пример. Если F – алгебраическое расширение поля рациональных чисел и задано произвольное подмножество $U \subset \Omega$, открытое и замкнутое одновременно, то в поле существует элемент α, удовлетворяющий условию

$$\alpha \in P \Leftrightarrow P \in U.$$

Таким образом, сигнатура $\sigma(\langle 1 \rangle + \langle \alpha \rangle) \in \mathbf{Z}^\Omega$ является удвоенной характеристической функцией подмножества U. Добавляя такие характеристические функции, мы видим, что *любой элемент идеала* $2\mathbf{Z}^\Omega$ *принадлежит образу отображения* σ. (Соответствующее утверждение для произвольного поля уже не имеет места.)

Доказательство утверждения 2.10. В начале предположим, что поле F имеет конечную степень над полем $\mathbf{Q}$. Тогда существует лишь конечное число вложений

$$\varphi_1, \ldots, \varphi_m \colon F \to \mathbf{R}$$

и ясно, что достаточно построить элементы $\alpha_1, \ldots, \alpha_m$ поля F, такие, что значения $\varphi_i(\alpha_j)$ положительны при $i \neq j$ и отрицательны при $i = j$. Тогда подходящие произведения элементов α_i будут иметь произвольные заранее заданные знаки.

Выберем в поле элемент ξ, такой, что $F = \mathbf{Q}(\xi)$. Затем выберем такое рациональное число $\epsilon > 0$, что при $i \neq j$

$$2\epsilon < |\varphi_i(\xi) - \varphi_j(\xi)|,$$

и такие рациональные числа $q_1, \ldots, q_m$, что

$$|\varphi_i(\xi) - q_i| < \epsilon.$$

Тогда разности

$$\alpha_i = (\xi - q_i)^2 - \epsilon^2$$

будут обладать требуемым свойством.

Теперь предположим, что поле F имеет бесконечную степень над полем $\mathbf{Q}$. Открыто-замкнутое множество $U \subset \Omega$ может быть покрыто конечным числом базовых открытых множеств $U_{\xi_1} \cap \ldots \cap U_{\xi_k}$, не пересекающихся с дополнением множества U. Собирая в поле все элементы $\xi_1, \ldots, \xi_k$, потребовавшиеся для всех базовых открытых множеств, мы порождаем ими некоторое подполе $F_0 \subset F$, которое конечно над полем $\mathbf{Q}$. Ясно, что данное множество $U \subset \Omega(F)$ равно прообразу подходящего подмножества $U_0 \subset \Omega(F_0)$ относительно морфизма ограничения

$$\Omega(F) \to \Omega(F_0).$$

Выбирая элемент $\alpha \in F_0$, положительный в упорядочениях из подмножества U_0 и отрицательный в упорядочениях из дополнения к подмножеству U_0, мы завершаем доказательство. □

Дальнейшую информацию по этому вопросу можно найти в [30].

§ 3. Простые идеалы кольца Витта

В этом параграфе будет изучено строение кольца Витта над произвольным полем F. Результаты принадлежат Пфистеру, а упрощенные доказательства – Лоренцу и Лейхту.

3.1. Лемма. *Кольцо Витта $W(F)$ аддитивно порождено элементами $\langle \alpha \rangle$, где α пробегает группу F^*.*

Доказательство непосредственно следует из § 3 гл. 1. □

3.2. Лемма. *Если* $\mathfrak{p}$ *– произвольный простой идеал кольца* $W(F)$, *то для любого элемента* $\alpha \in F^*$ *либо*

$$\langle \alpha \rangle \equiv \langle 1 \rangle \pmod{\mathfrak{p}},$$

либо

$$\langle \alpha \rangle \equiv \langle -1 \rangle \pmod{\mathfrak{p}}.$$

Следовательно, факторкольцо $W(F)/\mathfrak{p}$ *изоморфно либо кольцу* $\mathbf{Z}$, *либо полю* $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ *при некотором простом* p.

Доказательство. Поскольку элемент $\langle \alpha^2 \rangle$ в кольце $W(F)$ равен 1, то имеем

$$(\langle \alpha \rangle - \langle 1 \rangle)(\langle \alpha \rangle + \langle 1 \rangle) = 0$$

в кольце $W(F)$. Следовательно, элемент $\langle \alpha \rangle$ конгруэнтен либо $\langle 1 \rangle$, либо $\langle -1 \rangle$ по модулю любого простого идеала $\mathfrak{p}$. Отсюда следует, что однозначно определяемый кольцевой гомоморфизм

$$Z \to W(F) \to W(F)/\mathfrak{p}$$

сюръективен. Этим завершается доказательство, поскольку ядро должно быть простым идеалом в кольце $\mathbf{Z}$. □

Сначала рассмотрим случай $p = 2$.

3.3. Лемма. *Для любого поля* F *в кольце* $W(F)$ *существует ровно один идеал* I, *для которого* $W(F)/I \cong \mathbf{F}_2$.

Таким образом, идеал $I = I(F)$ является ядром единственного кольцевого гомоморфизма $W(F) \to \mathbf{F}_2$. Будем называть идеал I *фундаментальным идеалом* кольца Витта.

Доказательство леммы 3.3. Если $W(F)/I \cong \mathbf{F}_2$, то

$$\langle 1 \rangle \equiv \langle -1 \rangle \pmod{I}$$

и, следовательно,

$$\langle \alpha \rangle \equiv \langle 1 \rangle \pmod{I}$$

для любого элемента α. Поэтому идеал I состоит в точности из всех сумм $\langle \alpha_1 \rangle + \ldots + \langle \alpha_r \rangle$, для которых ранг r четен.

Обратно, поскольку любое расщепляемое пространство с внутренним произведением имеет четный ранг, то соответствие

$$X \mapsto \operatorname{rk}(X) \pmod 2$$

порождает гомоморфизм $W(F) \to \mathbf{F}_2$, ядро которого является требуемым фундаментальным идеалом I.

3.4. Замечание. *Кольцо Витта* $W(F)$ *изоморфно полю* $\mathbf{F}_2$ *тогда и только тогда, когда каждый элемент группы* F^* *является квадратом.*

Примерами являются алгебраически замкнутые поля и совершенные поля в характеристике 2.

Доказательство. Если $W(F) \cong \mathbf{F}_2$, то для любого элемента $\alpha \in F^*$ анизотропное пространство с внутренним произведением $\langle \alpha \rangle$ принадлежит тому же классу Витта, что и пространство $\langle 1 \rangle$, и, значит изоморфно пространству $\langle 1 \rangle$. Следовательно, элемент α – квадрат. Поскольку обратное очевидно, то этим завершается доказательство. □

Теперь давайте рассмотрим остальные простые идеалы.

3.5. Основная лемма. *Если* $\mathfrak{p} \subset W(F)$ *– любой простой идеал, для которого*

$$W(F)/\mathfrak{p} \ncong \mathbf{F}_2,$$

то множество $P \subset F^*$, *состоящее из всех элементов* $\alpha \neq 0$ *поля* F, *для которых*

$$\langle \alpha \rangle \equiv \langle 1 \rangle \pmod{\mathfrak{p}},$$

образует упорядочение поля F. *Связанный с ним гомоморфизм сигнатуры*

$$\sigma_P\colon W(F) \to \mathbf{Z}$$

для любого элемента w *из кольца Витта удовлетворяет сравнению*

$$w \equiv \sigma_P(w)\langle 1 \rangle \pmod{\mathfrak{p}}.$$

Следовательно, данный простой идеал $\mathfrak{p}$ является либо ядром отображения σ_P, либо ядром композиции

$$W(F) \xrightarrow{\sigma_P} \mathbf{Z} \to \mathbf{F}_p$$

в зависимости от того, изоморфно ли факторкольцо $W(F)/\mathfrak{p}$ кольцу Z или полю $\mathbf{F}_p$.

Доказательство леммы 3.5. Ясно, что множество P замкнуто относительно умножения и что

$$P \cup (-P) = F^*.$$

Поэтому достаточно доказать, что множество P замкнуто относительно сложения. Если $\alpha, \beta \in P$ и $\alpha + \beta = \gamma \neq 0$, то очевидно, что для некоторого δ

$$\langle \alpha \rangle \oplus \langle \beta \rangle \cong \langle \gamma \rangle \oplus \langle \delta \rangle.$$

Переходя к факторкольцу кольца Витта по идеалу $\mathfrak{p}$, получаем, что

$$\langle 1 \rangle + \langle 1 \rangle \equiv \langle \gamma \rangle + \langle \delta \rangle \pmod{\mathfrak{p}},$$

где $\langle \gamma \rangle \equiv \langle \pm 1 \rangle$ и $\langle \delta \rangle \equiv \langle \pm 1 \rangle$. Но из предположения, что $W(F)/\mathfrak{p} \ncong \mathbf{F}_2$, следует, что сумма $\langle 1 \rangle + \langle 1 \rangle$ не сравнима по модулю идеала $\mathfrak{p}$ ни с суммой $\langle -1 \rangle + \langle 1 \rangle$, ни с суммой $\langle -1 \rangle + \langle -1 \rangle$.

Следовательно,

$$\langle \gamma \rangle \equiv \langle 1 \rangle \pmod{\mathfrak{P}}$$

и, значит, $\gamma = \alpha + \beta \in P$. Случай $\alpha, \beta \in P$ и $\alpha + \beta = 0$ встретиться не может, поскольку тогда пространство с внутренним произведением $\langle \alpha \rangle \oplus \langle \beta \rangle$ было бы расщепляемым, откуда

$$\langle 1 \rangle + \langle 1 \rangle \equiv \langle \alpha \rangle + \langle \beta \rangle = 0,$$

что противоречит предположению. Таким образом, P является упорядочением поля F.

Теперь для любого элемента α из группы F^* сравнение

$$\langle \alpha \rangle \equiv \sigma_P(\langle \alpha \rangle)\langle 1 \rangle \pmod{\mathfrak{P}}$$

следует из определения упорядочения P. Ясно, что отсюда вытекает

$$w \equiv \sigma_P(w)\langle 1 \rangle \pmod{\mathfrak{P}}$$

для любого элемента $w = \langle \alpha_1 \rangle + \ldots + \langle \alpha_r \rangle$ из кольца Витта. Этим завершается доказательство. □

Замечание. Отсюда легко выводится, что топологическое пространство $\mathrm{Spec}\,(W(F))$, состоящее из всех простых идеалов кольца $W(F)$ с топологией Зарисского, гомеоморфно факторпространству, получающемуся из декартова произведения $\Omega \times \mathrm{Spec}\,(\mathbf{Z})$ стягиванием в точку замкнутого подмножества $\Omega \times (2)$. Каждой паре $(P, \mathfrak{q})$ в пространстве $\Omega \times \mathrm{Spec}\,(\mathbf{Z})$ соответствует, конечно, ядро отображения $(\sigma_P \bmod \mathfrak{q}) : W(F) \to \mathbf{Z}/\mathfrak{q}$.

Одним из непосредственных следствий леммы 3.5 является следующая

3.6. Теорема. *Если -1 является суммой квадратов в поле F, то $W(F)$ является локальным кольцом, содержащим единственный простой идеал I. Любой элемент идеала I нильпотентен, а порядок любого элемента аддитивной группы $W(F)$ является степенью числа 2.*

Прежде чем привести доказательство, изложим некоторые элементарные факты из теории колец.

3.7. Лемма. *Для любого коммутативного кольца R пересечение всех простых идеалов кольца R в точности равно идеалу $\mathfrak{N}$, состоящему из всех нильпотентных элементов кольца R.*

Действительно, если $\xi^n = 0$, то, конечно, элемент ξ принадлежит каждому простому идеалу в кольце R. Обратно, предположим, что элемент ξ не нильпотентен. Рассмотрим все идеалы $\mathfrak{a} \subset R$, обладающие тем свойством, что никакая степень элемента ξ не лежит в идеале $\mathfrak{a}$. Множество таких идеалов не пусто, поскольку нулевой идеал обладает этим свойством. По лемме Цорна в этом

множестве существует максимальный (относительно включения) идеал $\mathfrak{a}$. Тогда $\mathfrak{a}$ – простой идеал. Действительно, если $\alpha \notin \mathfrak{a}$ и $\beta \notin \mathfrak{a}$, то идеалы $\mathfrak{a} + R\alpha$ и $\mathfrak{a} + R\beta$ строго больше идеала $\mathfrak{a}$. Следовательно, при некоторых m и n

$$\xi^m \in \mathfrak{a} + R\alpha, \quad \xi^n \in \mathfrak{a} + R\beta.$$

Поэтому

$$\xi^{m+n} \in (\mathfrak{a} + R\alpha)(\mathfrak{a} + R\beta) \subset \mathfrak{a} + R\alpha\beta.$$

Но никакая степень элемента ξ не лежит в идеале $\mathfrak{a}$, так что этим доказано, что $\alpha\beta \notin \mathfrak{a}$. Таким образом, идеал $\mathfrak{a}$ простой. Следовательно, данный элемент $\xi \notin \mathfrak{a}$ не лежит в пересечении всех простых идеалов. Этим завершается доказательство леммы 3.7. □

Доказательство теоремы 3.6. Поскольку поле F не может быть упорядочено, кольцо Витта $W(F)$ не может иметь никаких простых идеалов $\mathfrak{p}$, кроме фундаментального идеала I. Следовательно, идеал $\mathfrak{N}$ нильпотентных элементов, являющийся пересечением всех простых идеалов, равен I.

В частности, поскольку $\langle 1 \rangle + \langle 1 \rangle \in I$, некоторая степень $(\langle 1 \rangle + \langle 1 \rangle)^n = 2^n \langle 1 \rangle$ равна нулю $W(F)$. (Здесь через $2^n\langle 1 \rangle$ обозначена сумма 2^n экземпляров пространства $\langle 1 \rangle$.) Следовательно, для любого элемента w в кольце Витта $2^n w = 0$. Этим завершается доказательство. □

Замечание. Это доказательство явно использует лемму Цорна. Более конструктивное рассуждение будет приведено в § 4.6.

Рассмотрим теперь поле, в котором -1 не является суммой квадратов. Через $\mathfrak{N}$ обозначим идеал, состоящий из всех нильпотентных элементов кольца Витта.

3.8. Теорема. *Если -1 не является суммой квадратов в поле F, то нильрадикал $\mathfrak{N}$ в точности равен ядру гомоморфизма полной сигнатуры*

$$\sigma\colon W(F) \to \mathbf{Z}^{\Omega}$$

(см. п. 2.8). *Элемент w из кольца Витта обратим тогда и только тогда, когда его образ обратим в кольце $\mathbf{Z}^{\Omega}$.*

Доказательство. Если $\sigma(w) = 0$, то, конечно, элемент w принадлежит фундаментальному идеалу I, состоящему из классов Витта четного ранга. Но из леммы 3.5 следует, что элемент w принадлежит также каждому другому простому идеалу. Следовательно, $w \in \mathfrak{N}$. Обратно, если $w \in \mathfrak{N}$, то элемент $\sigma(w)$ нильпотентен и, значит, $\sigma(w) = 0$.

Теперь предположим, что элемент $\sigma(w)$ обратим. Тогда $\sigma(w)^2 = 1$, откуда $w^2 \equiv 1 \pmod{\mathfrak{N}}$ и, следовательно, элемент w обратим. Этим завершается доказательство. □

3.9. Следствие. *Кольцо Витта $W(F)$ изоморфно кольцу* $\mathbf{Z}$ *тогда и только тогда, когда F является упорядоченным полем, в котором каждый положительный элемент – квадрат.*

Действительно, если $W(F) \cong \mathbf{Z}$, то поле F может быть упорядочено и для любого элемента $\alpha > 0$ анизотропное пространство с внутренним произведением $\langle \alpha \rangle$ принадлежит тому же классу Витта, что и пространство $\langle 1 \rangle$, и, значит, изоморфно пространству $\langle 1 \rangle$. Следовательно, элемент α – квадрат. Вместе со следствием 2.7 это завершает доказательство. □

3.10. Теорема. *Для любого поля F периодическая подгруппа кольца $W(F)$ в точности совпадает с ядром гомоморфизма полной сигнатуры*

$$\sigma\colon W(F) \to \mathbf{Z}^{\Omega}.$$

Порядок каждого периодического элемента является степенью числа 2.

Замечание. Если поле F имеет только одно упорядочение, то это можно совсем просто доказать следующим образом. Ясно, что ядро гомоморфизма $\sigma\colon W(F) \to \mathbf{Z}$ аддитивно порождается элементами вида $\langle 1 \rangle - \langle \alpha \rangle$, где $\alpha > 0$. Но

$$(\langle 1 \rangle - \langle \alpha \rangle)^2 = 2(\langle 1 \rangle - \langle \alpha \rangle)$$

и, следовательно,

$$(\langle 1 \rangle - \langle \alpha \rangle)^n = 2^{n-1}(\langle 1 \rangle - \langle \alpha \rangle).$$

Поскольку известно, что элемент $\langle 1 \rangle - \langle \alpha \rangle$ нильпотентен, то отсюда следует, что его порядок является степенью числа 2.

В общем случае доказательство будет основываться на следующем. Пусть K – любое расширение поля F. Напомним из п. 5.4 гл. 1, что любое пространство с внутренним произведением X ранга r над полем F порождает пространство с внутренним произведением $K \otimes_F X$ ранга r над полем F. Ясно, что это соответствие индуцирует кольцевой гомоморфизм

$$i_*\colon W(F) \to W(K).$$

Для квадратичных расширений ядро этого гомоморфизма вычисляется следующим образом (предполагаем, что поле F имеет характеристику, отличную от 2):

3.11. Лемма. *Для любого элемента $\alpha \in F^*$ ядро естественного гомоморфизма $W(F) \to W(F(\sqrt{\alpha}))$ равно главному идеалу $(\langle 1 \rangle - \langle \alpha \rangle)W(F)$. Каждый элемент w ядра удовлетворяет равенству $w = -\langle \alpha \rangle w$.*

Доказательство. Ясно, что элемент α отображается в квадрат в поле $F(\sqrt{\alpha})$, и следовательно, идеал $(\langle 1 \rangle - \langle \alpha \rangle)W(F)$ отображается в нуль. Но если анизотропное пространство с внут-

ренним произведением $X \neq 0$ над полем F представляет класс Витта из ядра, то, конечно, в пространстве $F(\sqrt{\alpha}) \otimes_F X$ существует вектор $z \neq 0$, для которого $z \cdot z = 0$. Полагая $z = x + \sqrt{\alpha}y$, где элементы x и y лежат в пространстве X, из уравнения $z \cdot z = 0$ получаем, что

$$x \cdot x + ay \cdot y = 0, \quad x \cdot y = 0.$$

Поскольку пространство X анизотропно, то по крайней мере один из элементов $x \cdot x$ и $y \cdot y$ поля F не нулевой и, значит, оба они не нулевые. Полагая $y \cdot y = \eta_1$ и $x \cdot x = -\alpha\eta_1$, мы видим, что пространство X разлагается в ортогональную сумму

$$\langle \eta_1 \rangle \oplus \langle -\alpha\eta_1 \rangle \oplus X',$$

где пространство X' также анизотропно и также представляет собой элемент ядра. Теперь легко показать по индукции, что для подходящих элементов $\eta_1, \ldots, \eta_k$

$$X \cong (\langle 1 \rangle \oplus \langle -\alpha \rangle) \otimes (\langle \eta_1 \rangle \oplus \ldots \oplus \langle \eta_k \rangle).$$

Отсюда следует, что

$$X \cong \langle -\alpha \rangle \otimes X,$$

чем и завершается доказательство. □

Доказательство теоремы 3.10. Предположим, что некоторый нильпотентный элемент w кольца $W(F)$ для всех n удовлетворяет неравенству $2^n w \neq 0$. Рассмотрим такие алгебраические расширения полей $K \supset F$, что для всех n образ $w' = i_*(w)$ в кольце $W(K)$ удовлетворяет неравенству $2^n w' \neq 0$. Отметим, что любое объединение вложенных полей, обладающих этим свойством, будет опять обладать этим свойством. Следовательно, по лемме Цорна существует максимальное расширение поля K с этим свойством. Если элемент $\alpha \in K$ не является квадратом, то поле $K(\sqrt{\alpha})$ строго содержит поле K. Следовательно, образ элемента $2^n w'$ в кольце $W(K(\sqrt{\alpha}))$ равен нулю для больших n. Из леммы 3.1 следует теперь, что при больших n

$$2^n w' = \langle \alpha \rangle 2^n w'.$$

Поскольку группа $W(K)$ не 2-периодична, то из теоремы 3.6 следует, что поле K может быть упорядочено. Поскольку кольцо $W(K)$ обладает нильпотентными элементами, то из утверждения 3.9 вытекает, что не каждый положительный элемент в поле K является квадратом. Следовательно, факторгруппа $K^\cdot/K^{\cdot 2}$ содержит не меньше четырех различных элементов. Пусть $1, \alpha, \beta$ и $\alpha\beta$ – элементы группы $K^\cdot$, различные по модулю подгруппы $K^{\cdot 2}$. Тогда для

больших n

$$2^n w' = \langle -\alpha \rangle 2^n w' = \langle -\alpha \rangle \langle -\beta \rangle 2^n w' =$$

$$= \langle \alpha \rangle \langle \beta \rangle \langle -\alpha\beta \rangle 2^n w'.$$

Это доказывает, что $2^n w' = -2^n w'$ или $2^{n+1} w' = 0$, что противоречит нашему предположению. Этим завершается доказательство. □

3.12. Следствие. *Пусть для каждого упорядочения P через F_P обозначено связанное с ним вещественное замыкание поля F. Тогда ядро естественного гомоморфизма*

$$W(F) \to \prod_P W(F_P)$$

равно периодической подгруппе кольца $W(F)$.

Доказательство проводится непосредственно.

Завершая этот параграф, мы наметим другое описание периодической подгруппы кольца $W(F)$, принадлежащее Шарлау [81], [82]. Пусть F – поле характеристики, отличной от 2.

Определение. Поле F называется *пифагоровым,* если подмножество F^2 замкнуто относительно сложения (другими словами, если любая сумма квадратов является квадратом в поле F).

Для любого поля F характеристики, отличной от 2, с алгебраическим замыканием $\bar{F}$ существует единственное иаименьшее пифагорово расширение $F_{\text{пиф}} \subset \bar{F}$. Действительно, расширение $F_{\text{пиф}}$ является объединением всех итерированных квадратичных расширений вида

$$F \subset \ldots \subset K \subset K(\sqrt{\alpha^2 + \beta^2})$$

в поле $\bar{F}$. Назовем это единственное поле $F_{\text{пиф}}$ *пифагоровым замыканием* поля F.

Кольцо Витта $W(F_{\text{пиф}})$ пифагорова поля может быть описано следующим образом. Если -1 является суммой квадратов в поле $F_{\text{пиф}}$, то любой элемент поля $F_{\text{пиф}}$ является квадратом и, следовательно, $W(F_{\text{пиф}}) = \mathbb{Z}/2\mathbb{Z}$. (Сравните с упражнением 2.3 и замечанием 3.4.) *С другой стороны, если -1 не является суммой квадратов, то кольцо $W(F_{\text{пиф}})$ не имеет кручения.* Действительно, для элемента $w \neq 0$ в кольце $W(F_{\text{пиф}})$ выберем анизотропного представителя $A \cong \langle \alpha_1 \rangle \oplus \ldots \oplus \langle \alpha_n \rangle$ элемента w. Тогда для любого $k > 0$ k-кратная сумма $A \oplus \ldots \oplus A$ также анизотропна. Если бы уравнение $\sum_{j=1}^{k} \sum_{i=1}^{n} \alpha_i \xi_{ij}^2 = 0$ имело нетривиальное решение, то, полагая $\sum_j \xi_{ij}^2 = \eta_i^2$, можно было бы вывести, что уравнение $\sum \alpha_i \eta_i^2 = 0$ также имеет нетривиальное решение, что невозможно.

3.13. Утверждение. *Если* $F_{\text{пиф}}$ *– пифагорово замыкание поля* F, *то точна последовательность*

$$0 \to \operatorname{Tors} IW(F) \to W(F) \to W(F_{\text{пиф}}).$$

Здесь через $\operatorname{Tors} IW(F)$ обозначена периодическая подгруппа фундаментального идеала $I \subset W(F)$, рассматриваемого как аддитивная группа.

Доказательство утверждения 3.13. Сначала рассмотрим квадратичное расширение вида

$$K \subset K(\sqrt{\alpha^2 + \beta^2}).$$

В силу леммы 3.11 ядро ассоциированного с ним гомоморфизма

$$W(K) \to W(K(\sqrt{\alpha^2 + \beta^2}))$$

равно идеалу $(\langle 1 \rangle - \langle \alpha^2 + \beta^2 \rangle) W(K)$. Используя изоморфизм

$$\langle 1 \rangle \oplus \langle 1 \rangle \cong \langle \alpha^2 + \beta^2 \rangle \oplus \langle \alpha^2 + \beta^2 \rangle,$$

мы видим, что любой элемент этого идеала имеет порядок 2. Для итерированного расширения $F \subset \ldots \subset K \subset K(\sqrt{\alpha^2 + \beta^2})$ степени 2^n над полем F по индукции доказывается, что ядро ассоциированного с ним гомоморфизма колец Витта имеет показатель 2^n. Переходя к прямому пределу (индуктивному пределу) по всем таким итерированным расширениям, получаем, что ядро гомоморфизма

$$W(F) \to W(F_{\text{пиф}})$$

является 2-примарной периодической группой. Но группа $W(F_{\text{пиф}})$ без кручения, так что это ядро должно в точности совпадать с периодической подгруппой кольца $W(F)$.

Между прочим, это рассуждение дает более простое доказательство того, что кольцо Витта над полем не содержит кручения нечетного порядка.

Отметим, что для любого поля (даже характеристики 2) подгруппа $\operatorname{Tors} IW(F)$ в точности равна нильрадикалу кольца $W(F)$.

§ 4. Мультипликативные пространства с внутренним произведением

Результаты этого параграфа принадлежат Пфистеру (сравните с [81] и [48]). Однако для удобства изложения мы несколько модифицируем определения Пфистера.

Если элемент x принадлежит пространству с внутренним произведением X, то будет удобно называть значение $x \cdot x$ *нормой* элемента x. Таким образом, элемент α из поля является *нормой в пространстве* X, если $\alpha = x \cdot x$ для некоторого элемента $x \in X$.

4.1. О п р е д е л е н и е. Пространство с внутренним произведением X называется *мультипликативным,* если для любого элемента α из поля, являющегося нормой в пространстве X,

$$X \cong \langle \alpha \rangle \otimes X.$$

(Это определение не является общепринятым.)

Одним из важных свойств мультипликативных пространств является следующее.

4.2. Л е м м а. *Если пространство X мультипликативно, то множество всех элементов $\alpha \neq 0$ поля, являющихся нормами в пространстве X, образует подгруппу в группе F^*.*

Д о к а з а т е л ь с т в о. Если $\alpha = x \cdot x \neq 0$ и $\beta = y \cdot y \neq 0$, то рассмотрим изоморфизм

$$f\colon X \to \langle \beta \rangle \otimes X.$$

Полагая $f(x) = e \otimes z$, где $e \cdot e = \beta$, получим, что

$$x \cdot x = f(x) \cdot f(x) = \beta z \cdot z.$$

Следовательно, частное $\alpha/\beta = z \cdot z$ также является нормой в пространстве X, что завершает доказательство. □

В качестве примера рассмотрим пространство с внутренним произведением $\langle 1 \rangle$, которое, конечно, мультипликативно, а его группа ненулевых норм равна подгруппе $F^{\cdot 2}$.

4.3. Т е о р е м а. *Любое тензорное произведение форм*

$$(\langle 1 \rangle \oplus \langle \alpha_1 \rangle) \otimes \ldots \otimes (\langle 1 \rangle \oplus \langle \alpha_n \rangle)$$

мультипликативно. Кроме того, любое такое тензорное произведение либо анизотропно, либо расщепляемо.

Д о к а з а т е л ь с т в о. Сначала рассмотрим случай $n = 1$. Если элемент $\beta \neq 0$ является нормой в пространстве $\langle 1 \rangle \oplus \langle \alpha \rangle$, то ясно, что для некоторого элемента γ

$$\langle 1 \rangle \oplus \langle \alpha \rangle \cong \langle \beta \rangle \oplus \langle \gamma \rangle.$$

Сравнивая определители, мы видим, что $\langle \gamma \rangle \cong \langle \beta\alpha \rangle$, откуда, как и требовалось,

$$\langle 1 \rangle \oplus \langle \alpha \rangle \cong \langle \beta \rangle \otimes (\langle 1 \rangle \oplus \langle \alpha \rangle).$$

Поскольку любое пространство ранга 2 либо анизотропно, либо расщепляемо, то этим рассмотрен случай $n = 1$.

Далее продолжим доказательство по индукции. Предположив, что пространство X мультипликативно, покажем, что мультипликативно пространство

$$(\langle 1 \rangle \oplus \langle \alpha \rangle)X \cong X \oplus \langle \alpha \rangle X.$$

Здесь для упрощения записи опущены знаки тензорного произве-

дения. Пусть элемент $\beta \neq 0$ является нормой в пространстве $X \oplus \langle \alpha \rangle X$. Тогда элемент β, очевидно, имеет вид

$$\beta = x \cdot x + \alpha y \cdot y = \xi + \alpha\eta,$$

где элементы ξ и η – нормы в пространстве X. Если $\xi = 0$, то $\eta \neq 0$, откуда $\langle \eta \rangle X \cong X$ и $\langle \alpha\eta \rangle (X \oplus \langle \alpha \rangle X) \cong \langle \alpha \rangle X \oplus \langle \alpha \rangle^2 X \cong X \oplus \langle \alpha \rangle X$, что и требовалось показать. Случай $\eta = 0$ рассматривается аналогично. Предположим теперь, что оба элемента ξ и η не равны нулю. Тогда $X \cong \langle \xi \rangle X \cong \langle \eta/\xi \rangle X$, откуда следует, что

$$\langle \xi + \alpha\eta \rangle (X \oplus \langle \alpha \rangle X) \cong \langle 1 + \alpha\eta/\xi \rangle (X \oplus \langle \alpha\eta/\xi \rangle X) \cong$$

$$\cong \langle 1 + \alpha\eta/\xi \rangle (\langle 1 \rangle \oplus \langle \alpha\eta/\xi \rangle) X.$$

Но уже установлено, что пространство с внутренним произведением

$$\langle 1 \rangle \oplus \langle \alpha\eta/\xi \rangle$$

мультипликативно. Поскольку элемент $1 + \alpha\eta/\xi$ является ненулевой нормой в этом пространстве, то видим, что множитель $\langle 1 + \alpha\eta/\xi \rangle$ можно сократить и оставить

$$(\langle 1 \rangle \oplus \langle \alpha\eta/\xi \rangle) X \cong X \oplus \langle \alpha \rangle X,$$

что и требовалось показать.

Нужно доказать, что пространство $X \oplus \langle \alpha \rangle X$ либо анизотропно, либо расщепляемо, предполагая по индукции, что само пространство X либо анизотропно, либо расщепляемо. Если пространство $X \oplus \langle \alpha \rangle X$ не анизотропно, то в пространстве X существуют векторы x и y, не равные нулю одновременно и такие, что

$$x \cdot x + \alpha y \cdot y = \xi + \alpha\eta = 0.$$

Если $\xi = \eta = 0$, то пространство X должно быть расщепляемым, откуда, конечно, следует расщепляемость пространства $X \oplus \langle \alpha \rangle X$. В противном случае, элемент $\xi/\eta = -\alpha$ является ненулевой нормой в пространстве X. Следовательно, $X \cong \langle -\alpha \rangle X$, откуда опять же следует, что пространство $X \oplus \langle \alpha \rangle X$ расщепляемо. Этим завершается доказательство. □

Особенно интересным частным случаем теоремы 4.3 является случай, когда $\alpha_1 = \ldots = \alpha_n = 1$. Тензорное произведение

$$(\langle 1 \rangle \oplus \langle 1 \rangle) \otimes \ldots \otimes (\langle 1 \rangle \oplus \langle 1 \rangle)$$

является в этой ситуации 2^n-кратной суммой экземпляров пространства $\langle 1 \rangle$. Запишем это кратко как $2^n \langle 1 \rangle$.

4.4. Следствие. *Для любого поля F и любого $n \geqslant 0$ подмножество, состоящее из всех элементов $\xi \neq 0$ поля, которые могут быть выражены в виде суммы 2^n квадратов, является мультипликативной группой.*

Это следует из леммы 4.2 и теоремы 4.3, поскольку элемент поля является нормой в пространстве $2^n\langle 1\rangle$ тогда и только тогда, когда он является суммой 2^n квадратов.

Например, для поля Q рациональных чисел из возможности представить числа $5 = 1^2 + 2^2$ и $13 = 2^2 + 3^2$ в виде суммы двух квадратов следует, что число 65 $(= 4^2 + 7^2)$ также можно представить в таком виде (сравните с § 8 гл. 2). Напротив, оба числа $3 = 1^2 + 1^2 + 1^2$ и $5 = 0^2 + 1^2 + 2^2$ можно представить в виде суммы трех квадратов, а их произведение уже нельзя. Если бы 15 равнялось $\alpha^2 + \beta^2 + \gamma^2$, то, освобождаясь от знаменателей и переходя к вычетам по модулю 8, получили бы, что

$$-d^2 \equiv a^2 + b^2 + c^2 \pmod 8,$$

где по крайней мере одно из целых чисел a, b, c, d нечетно, что, как легко видеть, невозможно.

Имеется важное приложение теоремы 4.3.

О п р е д е л е н и е. Если -1 является суммой квадратов в поле F, то *уровнем* поля F называется наименьшее целое число s, такое, что -1 является суммой s квадратов. Если -1 не является суммой квадратов, то полагаем $s = \infty$.

4.5. Т е о р е м а. *Для любого поля F порядок элемента $\langle 1\rangle$ в аддитивной группе кольца $W(F)$ равен в точности $2s$. Уровень s всегда равен либо ∞, либо степени числа 2.*

З а м е ч а н и е. В классическом случае числового поля уровень всегда равен ∞, 1, 2 или 4. Примеры дают поля Q, $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-2})$ и $\mathbf{Q}(\sqrt{-7})$ соответственно. Поскольку порядок элемента $\langle 1\rangle$ сравнительно легко вычисляется, эта теорема предоставляет прекрасное средство для вычисления уровня s.

Д о к а з а т е л ь с т в о т е о р е м ы 4.5. Если $s = \infty$, то утверждение очевидно. Поэтому можно предполагать, что $s < \infty$. Отметим сначала, что s-кратная ортогональная сумма $\langle 1\rangle \oplus \ldots \oplus \langle 1\rangle = s\langle 1\rangle$ анизотропна. Если бы уравнение

$$\xi_1^2 + \ldots + \xi_s^2 = 0$$

имело решение, скажем, с $\xi_1 \neq 0$, то из этого следовало бы, что

$$-1 = (\xi_2/\xi_1)^2 + \ldots + (\xi_s/\xi_1)^2.$$

Но это противоречит определению уровня s. Аналогичные рассуждения показывают, что $(s+1)$-кратная ортогональная сумма $(s+1)\langle 1\rangle$ *не* анизотропна.

Теперь определим целое число $n \geqslant 0$ из неравенства $2^n \leqslant s < 2^{n+1}$. Заведомо известно, что ортогональная сумма $2^n\langle 1\rangle$ анизотропна, а сумма $2^{n+1}\langle 1\rangle$ — нет. Давайте применим теорему 4.3.

Поскольку пространство $2^{n+1}\langle 1\rangle$ может быть представлено в виде тензорного произведения

$$(\langle 1\rangle \oplus \langle 1\rangle) \otimes \ldots \otimes (\langle 1\rangle \oplus \langle 1\rangle)$$

и не анизотропно, то отсюда следует, что пространство $2^{n+1}\langle 1\rangle$ расщепляемо. Из соотношений

$$2^n\langle 1\rangle \neq 0, \quad 2^{n+1}\langle 1\rangle \sim 0$$

теперь, очевидно, вытекает, что порядок элемента $\langle 1\rangle$ в кольце Витта равен в точности 2^{n+1}.

Нужно доказать, что $s = 2^n$. Добавляя 2^n экземпляров пространства $\langle -1\rangle$ к обеим сторонам соотношения $2^{n+1}\langle 1\rangle \sim 0$, выводим, что

$$2^n\langle 1\rangle \sim 2^n\langle -1\rangle.$$

Но эти пространства анизотропны, и из теоремы 1.7 следует, что

$$2^n\langle 1\rangle \cong 2^n\langle -1\rangle.$$

Следовательно, -1 является суммой 2^n квадратов, откуда $s \leqslant 2^n$ и, значит, $s = 2^n$. Этим завершается доказательство. □

4.6. З а м е ч а н и е. Теперь можно дать более конструктивное доказательство того факта, что любой элемент фундаментального идеала $I \subset W(F)$ нильпотентен, если $s = 2^n < \infty$ (сравните с теоремой 3.6). Действительно, для любого элемента w из кольца Витта положим

$$w = \langle \alpha_1\rangle + \ldots + \langle \alpha_r\rangle.$$

Тогда

$$w^2 \equiv \langle \alpha_1\rangle^2 + \ldots + \langle \alpha_r\rangle^2 = r\langle 1\rangle \pmod{2W(F)}.$$

Если ранг r четен, то отсюда вытекает, что

$$w^2 \equiv 0 \pmod{2W(F)}$$

и, следовательно,

$$w^{2(n+1)} \equiv 0 \pmod{2^{n+1}W(F)}.$$

Поскольку умножение на $2^{n+1} = 2s$ аннулирует любой элемент кольца Витта, то это доказывает, что $w^{2(n+1)} = 0$. □

Завершим параграф следующей задачей для читателя. (В ней F-линейная биекция $f\colon X \to X$ называется *преобразованием подобия*, если в поле существует элемент $\lambda \neq 0$, такой, что для любых x и y

$$f(x) \cdot f(y) = \lambda x \cdot y.)$$

У п р а ж н е н и е. Предположим, что 1 является нормой в пространстве X. Докажите, что группа преобразований подобия пространства X действует транзитивно на множестве $X\setminus\{0\}$ тогда и только тогда, когда пространство X мультипликативно и анизотропно.

§ 5. Степени фундаментального идеала

В этом параграфе будет изучаться цепочка идеалов $I \supset I^2 \supset I^3 \supset \ldots$ в кольце Витта $W(F)$, где I – фундаментальный идеал, состоящий из всех классов Витта четного ранга. Основная теорема об этих идеалах была недавно доказана Арасоном и Пфистером. Приведем ее здесь без доказательства.

5.1. Т е о р е м а. *Если* $w \in I^n$ *и* $w \neq 0$, *то* $\|w\| \geqslant 2^n$.

(Здесь через $\|w\|$ обозначен ранг анизотропного представителя класса Витта w.) Отсюда сразу следует, что пересечение идеалов I^n равно нулю.

Каждый фактормодуль I^n/I^{n+1}, очевидно, является векторным пространством над полем

$$W(F)/I \cong \mathbf{F}_2.$$

Следующее наблюдение принадлежит Пфистеру.

5.2. Т е о р е м а. *Факторгруппа* I/I^2 *канонически изоморфна факторгруппе* F^*/F^{*2}.

Доказательство основывается на использовании определителя, введенного в § 2 гл. 1. Напомним, что для любого пространства с внутренним произведением X определитель $\det(X)$ является корректно определенным элемеитом в группе F^*/F^{*2}. Однако нужно быть осторожными, поскольку определитель расщепляемого пространства с внутренним произведением не обязательно тривиален. Чтобы исправить это, проведем следующую модификацию.

О п р е д е л е н и е. Для любого пространства с внутренним произведением X *дискриминант*

$$d(X) \in F^*/F^{*2}$$

определяется как элемент $(-1)^{r(r-1)/2}\det(X)$.

Давайте вычислим дискриминант ортогональной суммы $X \oplus Y$. Полагая $r = \mathrm{rk}(X)$, $s = \mathrm{rk}(Y)$ и $f(r) = r(r-1)/2$, легко проверим тождество

$$f(r+s) = f(r) + f(s) + rs.$$

Отсюда следует, что

$$d(X \oplus Y) = (-1)^{rs} d(X) d(Y).$$

В частности, если либо пространство X, либо пространство Y имеет четный ранг, то $d(X \oplus Y) = d(X) \cdot d(Y)$.

5.3. Л е м м а. *Дискриминант $d(X)$ зависит только от класса Витта пространства X.*

Если S — расщепляемое пространство ранга $2n$, то, согласно лемме 6.3 из гл. 1, матрица внутреннего произведения пространства S в подходящем базисе имеет вид $\begin{pmatrix} 0 & I \\ I & * \end{pmatrix}$. Следовательно,

$$\det S = (-1)^n F^{\cdot 2},$$

откуда вытекает, что $d(S)$ единичный элемент в группе $F^{\cdot}/F^{\cdot 2}$. Далее доказательство леммы 5.3 не вызывает трудностей. □

Д о к а з а т е л ь с т в о т е о р е м ы 5.2. Очевидно, что соответствие $w \mapsto d(w)$ задает гомоморфизм из аддитивной группы идеала I в группу $F^{\cdot}/F^{\cdot 2}$ Этот гомоморфизм сюръективен, поскольку

$$d(\langle \xi \rangle \oplus \langle -1 \rangle) = \xi F^{\cdot 2};$$

и аннулирует идеал I^2, поскольку идеал I^2 аддитивно порожден произведениями вида

$$(\langle \alpha \rangle + \langle 1 \rangle)(\langle \beta \rangle + \langle 1 \rangle) = \langle \alpha\beta \rangle + \langle \alpha \rangle + \langle \beta \rangle + \langle 1 \rangle,$$

каждое из которых имеет тривиальный дискриминант. Пусть теперь $w = \langle \alpha_1 \rangle + \ldots + \langle \alpha_{2r} \rangle$ — произвольный элемент идеала I. Используя сравнения

$$\langle \alpha \rangle + \langle \beta \rangle \equiv \langle -\alpha\beta \rangle + \langle -1 \rangle \pmod{I^2}$$

и

$$\langle -1 \rangle + \langle -1 \rangle + \langle -1 \rangle \equiv \langle 1 \rangle \pmod{I^2},$$

получаем, проводя индукцию по r, что элемент w сравним по модулю I^2 с выражением вида $\langle \xi \rangle + \langle -1 \rangle$. Если

$$d(w) = d(\langle \xi \rangle + \langle -1 \rangle) = \xi F^{\cdot 2}$$

является единичным элементом группы $F^{\cdot}/F^{\cdot 2}$, то $\langle \xi \rangle + \langle -1 \rangle = 0$ и, следовательно, $w \in I^2$. Таким образом, последовательность $0 \to I^2 \to I \to F^{\cdot}/F^{\cdot 2} \to 0$ точна. Этим завершается доказательство. □

На следующем шаге естественно рассмотреть фактормодуль I^2/I^3.

5.4. О п р е д е л е н и е. *Символом* на поле F со значениями в группе $\mathbf{Z}^{\cdot}$ называется бимультипликативная функция

$$\varphi\colon F^{\cdot} \times F^{\cdot} \to \mathbf{Z}^{\cdot},$$

удовлетворяющая тождеству $\varphi(\alpha, 1 - \alpha) = 1$ для всех элементов $\alpha \neq 0, 1$.

Слово "бимультипликативная" означает, что функция $\varphi(\alpha, \beta)$ мультипликативна и как функция от α при фиксированном β, и как функция от β при фиксированном α. В частности, $\varphi(\alpha, 1) = 1$.

З а м е ч а н и е. Прототипом для такого объекта является "символ Гильберта". Для локального поля F характеристики, отличной от 2, Гильберт показал, что существует ровно один нетривиальный символ на поле F со значениями в группе $\mathbf{Z}^{\cdot}$. В более позднее время символы со значениями в произвольной коммутативной группе возникли при анализе Стейнбергом центральных расширений классических групп. (Сравните с [59].)

5.5. Л е м м а. *Если задан некоторый фиксированный символ φ на поле F со значениями в группе $\mathbf{Z}^{\cdot}$, то образ $\varphi(\alpha, \beta)$ зависит только от класса Витта пространства с внутренним произведением $\langle \alpha \rangle \oplus \langle \beta \rangle$.*

Д о к а з а т е л ь с т в о. Поскольку группа $\mathbf{Z}$ имеет показатель 2, то образ $\varphi(\alpha, \beta)$ не изменится, если умножить α или β на квадрат. Используя тождество

$$-\alpha = (1-\alpha)/(1-\alpha^{-1}),$$

легко получаем, что

$$\varphi(\alpha, -\alpha) = 1.$$

Поэтому образ $\varphi(\alpha, \beta)$ тривиален, если пространство с внутренним произведением $\langle \alpha \rangle \oplus \langle \beta \rangle$ расщепляемо.

Предположим, что пространства с внутренним произведением $\langle \alpha \rangle \oplus \langle \beta \rangle \sim \langle \gamma \rangle \oplus \langle \delta \rangle$ не расщепляемы. Тогда эти пространства изоморфны и, значит, уравнение

$$\gamma = \alpha\xi^2 + \beta\eta^2$$

имеет решение. Отметим соотношение

$$\alpha\beta \equiv \gamma\delta \pmod{F^{\cdot 2}}.$$

Если $\eta = 0$, то $\alpha = \gamma$, $\beta = \delta \pmod{F^{\cdot 2}}$, откуда, конечно, $\varphi(\alpha, \beta) = \varphi(\gamma, \delta)$. Если $\xi = 0$, то аналогичные рассуждения показывают, что

$$\varphi(\gamma, \delta) = \varphi(\beta, \alpha).$$

Но соотношение симметрии

$$\varphi(\beta, \alpha) = \varphi(\alpha, \beta)^{-1} = \varphi(\alpha, \beta)$$

легко установить, если раскрыть тождество $\varphi(\alpha\beta, -\alpha\beta) = 1$. Наконец, предположим, что $\xi \neq 0$ и $\eta \neq 0$. Тогда

$$\alpha\xi^2/\gamma + \beta\eta^2/\gamma = 1$$

и, следовательно,

$$\varphi(\alpha\gamma, \beta\gamma) = \varphi(\alpha\xi^2/\gamma, \beta\eta^2/\gamma) = 1.$$

Преобразуя выражение, получаем

$$\varphi(\alpha, \beta) = \varphi(\gamma, \alpha\beta\gamma),$$

что завершает доказательство, поскольку $\alpha\beta\gamma \equiv \delta \pmod{F^{\cdot 2}}$. □

5.6. Л е м м а. *Предположим, что два пространства с внутренним произведением*

$$\langle \alpha_1 \rangle \oplus \ldots \oplus \langle \alpha_n \rangle \quad \text{и} \quad \langle \beta_1 \rangle \oplus \ldots \oplus \langle \beta_n \rangle$$

имеют один и тот же ранг и класс Витта. Тогда можно перейти от последовательности $\alpha_1, \ldots, \alpha_n$ *к последовательности* $\beta_1, \ldots, \beta_n$, *изменяя одновременно ровно по два коэффициента и сохраняя на каждом шаге класс Витта.*

Доказательство этой классической леммы будет отложено до конца § 5.

Теперь для любого пространства с внутренним произведением X, обладающего ортогональным базисом,

$$X \cong \langle \alpha_1 \rangle \oplus \ldots \oplus \langle \alpha_n \rangle,$$

определим *инвариант Хассе* $H_\varphi(X) \in \mathbf{Z}$ как произведение $\prod_{i<j} \varphi(\alpha_i, \alpha_j)$. Если пространство X не обладает ортогональным базисом, то оно должно быть симплектическим пространством над полем F характеристики 2. Для него положим $H_\varphi(X) = 1$.

5.7. Т е о р е м а. *Инвариант Хассе* $H_\varphi(X)$ *не зависит от выбора ортогонального разложения. Если два пространства* X *и* X' *имеют одни и те же ранг и класс Витта, то* $H_\varphi(X) = H_\varphi(X')$. *Тождество*

$$H_\varphi(X \oplus Y) = H_\varphi(X) H_\varphi(Y) \varphi(\det X, \det Y)$$

выполняется для любых пространств X *и* Y.

Доказательство, использующее леммы 5.5 и 5.6, проводится непосредственно и предоставляется читателю. □

Пусть S – расщепляемое пространство с внутренним произведением ранга $n = 2m$. Тогда пространство S имеет тот же ранг и класс Витта, что и m-кратная сумма $m(\langle 1 \rangle \oplus \langle -1 \rangle)$. Легко выводится, что

$$H_\varphi(S) = \varphi(-1, 1)^{m(m-1)/2}.$$

Этот инвариант не всегда равен 1, но если $n = 2m \equiv 0 \pmod 8$, то, конечно, $H_\varphi(S) = 1$.

О п р е д е л е н и е. Для любого класса Витта w из фундаментального идеала I *инвариант Хассе – Витта* $h_\varphi(w)$ определяется следующим образом. Выберем пространство с внутренним произве-

дением X, представляющее класс Витта w, таким образом, что

$$\mathrm{rk}(X) \equiv 0 \pmod 8,$$

и положим $h_\varphi(w)$ равным инварианту Хассе $H_\varphi(X)$.

Эта функция корректно определена, поскольку если $X \sim X'$ и $\mathrm{rk}(X) \equiv \mathrm{rk}(X') \equiv 0 \pmod 8$, то $X \oplus S \cong X' \oplus S'$, где $\mathrm{rk}(S) \equiv \mathrm{rk}(S') \equiv 0 \pmod 8$ и, следовательно,

$$H_\varphi(X) = H_\varphi(X \oplus S) = H_\varphi(X' \oplus S') = H_\varphi(X').$$

5.8. Теорема. *Для любого символа φ ограничение функции Хассе – Витта h_φ на идеал I^2 дает корректно определенный гомоморфизм*

$$h_\varphi\colon I^2 \to \mathbf{Z}^*.$$

Элемент w из идеала I^2 аннулируется любым из этих гомоморфизмов h_φ тогда и только тогда, когда $w \in I^3$.

(Сравните с [67].) В действительности в доказательстве будет показано, что группа всех символов φ на поле F со значениями в $\mathbf{Z}^*$ канонически изоморфна группе $\mathrm{Hom}(I^2/I^3, \mathbf{Z}^*)$.

Доказательство теоремы 5.8. Тождество

$$h_\varphi(w + w') = h_\varphi(w)\, h(w')\, \varphi(d(w), d(w')),$$

очевидно, выполняется для любых элементов w и w' фундаментального идеала I. Если $w \in I^2$, то $d(w) = 1$, откуда

$$h_\varphi(w + w') = h_\varphi(w)\, h_\varphi(w').$$

Следующим шагом вычислим инвариант Хассе – Витта от произведения $w\langle\beta\rangle$. Полагая $w = \langle\alpha_1\rangle + \ldots + \langle\alpha_m\rangle$, где $m \equiv 0 \pmod 8$, имеем

$$h_\varphi(w\langle\beta\rangle) = \prod_{i<j} \varphi(\alpha_i\beta, \alpha_j\beta) =$$

$$= h_\varphi(w)\, \varphi(\alpha_1 \ldots \alpha_m, \beta)^{m-1} \varphi(\beta, \beta)^{m(m-1)/2} =$$

$$= h_\varphi(w)\, \varphi(d(w), \beta).$$

Для любого элемента $w' \in I$, полагая $w' = \langle\beta_1\rangle + \ldots + \langle\beta_n\rangle$, где $n \equiv 0 \pmod 4$, получаем, что

$$h_\varphi(ww') = h_\varphi(w)^n \varphi(d(w), \beta_1 \ldots \beta_n)\, \varphi(d(w), d(w))^{n(n-1)/2} =$$

$$= \varphi(d(w), d(w')).$$

В частности, если $w \in I$ и $w' \in I^2$, то $h_\varphi(ww') = 1$. Следовательно, каждая функция h_φ аннулирует идеал I^3 и индуцирует гомо-

морфизм

$$h_\varphi\colon I^2/I^3 \to \mathbf{Z}^*.$$

Обратно, если дан произвольный гомоморфизм $g\colon I^2/I^3 \to \mathbf{Z}^*$, то обозначим через φ символ

$$\varphi(\alpha,\beta) = g((\langle\alpha\rangle - \langle 1\rangle)(\langle\beta\rangle - \langle 1\rangle)).$$

Используя сравнение

$$\langle\alpha\alpha'\rangle - \langle 1\rangle \equiv \langle\alpha\rangle - \langle 1\rangle + \langle\alpha'\rangle - \langle 1\rangle \pmod{I^2},$$

видим, что функция φ бимультипликативна. Если $\alpha + \beta = 1$, то изоморфизм

$$\langle\alpha\rangle \oplus \langle\beta\rangle \cong \langle 1\rangle \oplus \langle\alpha\beta\rangle$$

влечет $\varphi(\alpha, \beta) = 1$. Поскольку ассоциированный гомоморфизм

$$h_\varphi\colon I^2/I^3 \to \mathbf{Z}^*$$

совпадает с гомоморфизмом g на каждом образующем $(\langle\alpha\rangle - \langle 1\rangle)(\langle\beta\rangle - \langle 1\rangle)$ идеала I^2, то отсюда следует, что $h_\varphi = g$. Если элемент $w \in I^2$ аннулируется любой функцией h_φ, то он аннулируется любым гомоморфизмом из группы I^2/I^3 в группу $\mathbf{Z}^*$ и, следовательно, $w \in I^3$. □

5.9. Классические примеры. Если F – конечное поле, то элементарные рассуждения, принадлежащие Стейнбергу, показывают, что любой символ на поле F тривиален и, следовательно, идеал $I^2 \subset W(F)$ нулевой. (Сравните с леммой 1.5 гл. 4.)

Если F – конечное расширение поля p-адических чисел, то существует в точности один нетривиальный символ на поле F со значениями в группе $\mathbf{Z}^*$. Следовательно, группа I^2/I^3 циклическая порядка 2. В действительности ранг, определитель и инвариант Хассе образуют полную систему инвариантов пространства с внутренним произведением над полем F. (См. [61, с. 170].) Легко выводится, что идеал I^2 – циклическая группа порядка 2 и что $I^3 = 0$.

Теперь предположим, что F – конечное расширение поля рациональных чисел. В этом случае полный инвариант для пространства с внутренним произведением над полем F дается рангом, определителем, полной сигнатурой вместе с инвариантами Хассе, связанными со всеми различными локальными пополнениями поля F ([61, с. 189]). Для элемента w идеала $I^3 \subset W(F)$ легко выводится, что сигнатура $\sigma(w)$ дает полный инвариант. В действительности гомоморфизм σ биективно отображает идеал I^3 на идеал $8\mathbf{Z}^\Omega$ В частности, во вполне мнимом случае отсюда следует, что $I^3 = 0$.

Отметим, что "длина" цепочки идеалов $I \supset I^2 \supset I^3 \supset \ldots$ в случае числового поля равна либо 2, либо ∞ в соответствии с тем, является ли -1 суммой квадратов или нет. Однако вычисление "длины" в этом случае – это совершенно другой вопрос.

Пусть F – поле характеристики 2. Тогда гомоморфизм $\xi \mapsto \xi^2$ отображает поле F изоморфно на подполе F^2. Степень поля F над подполем F^2 является числом вида 2^ι, где ι принимает значения $0, 1, 2, \ldots, \infty$. Отметим, что поле F совершенно тогда и только тогда, когда $\iota = 0$. Если E – конечное расширение степени n поля F, то поле E^2 имеет степень n над подполем F^2 и, следовательно, поле E имеет степень 2^ι над подполем E^2. Другими словами, мера ι несовершенности поля является инвариантом относительно конечных расширений поля F. Она также является инвариантом относительно сепарабельных расширений. Однако мера ι возрастает на 1 при простом трансцендентном расширении. (Другую характеризацию меры ι см. в [24, с. 154].)

5.10. Т е о р е м а. *Если поле F характеристики 2 имеет степень 2^ι над подполем F^2, то идеал $I^n \subset W(F)$ равен нулю при $n > \iota$ и не равен нулю при $n \leqslant \iota$.*

Например, если поле F конечно, то $\iota = 0$ и поэтому фундаментальный идеал $I = I^1$ нулевой.

Д о к а з а т е л ь с т в о. Идеал I^n аддитивно порождается произведениями вида

$$X = (\langle 1 \rangle \oplus \langle \alpha_1 \rangle) \otimes \ldots \otimes (\langle 1 \rangle \oplus \langle \alpha_n \rangle).$$

По теореме 4.3 Пфистера каждое такое произведение либо анизотропно, либо расщепляемо. Но если $n > \iota$, то 2^n произведений $\alpha_{j_1}\alpha_{j_2} \ldots \alpha_{j_k}$, где набор $\{j_1, \ldots, j_k\}$ пробегает все подмножества множества $\{1, \ldots, n\}$, не могут быть линейно независимыми над полем F^2. Следовательно, пространство X, будучи ортогональной суммой пространств $\langle \alpha_{j_1} \ldots \alpha_{j_k} \rangle$, не может быть анизотропным. Следовательно, $X \sim 0$, откуда вытекает, что $I^n = 0$.

Обратно, если $n \leqslant \iota$, то можем построить по индукции элементы $\alpha_1, \ldots, \alpha_n$ поля F, такие, что элемент α_{j+1} не принадлежит подполю $F^2(\alpha_1, \ldots, \alpha_j)$. Отсюда следует, что 2^n произведений $\alpha_{j_1} \ldots \alpha_{j_k}$ линейно независимы над полем F^2. Значит, описанное выше пространство с внутренним произведением X анизотропно и, следовательно, $I^n \neq 0$. Этим завершается доказательство. (Сравните с [58].) □

Завершая § 5, д о к а ж е м л е м м у 5.6. Предположим, что

$$\langle \alpha_1 \rangle \oplus \ldots \oplus \langle \alpha_n \rangle \sim \langle \beta_1 \rangle \oplus \ldots \oplus \langle \beta_n \rangle.$$

Проводя индукцию по n, надо показать, что можно так изменять парами коэффициенты α_i, чтобы, сохраняя класс Витта, преобразовать одну последовательность в другую. Конечно, любая перестановка коэффициентов α_i может быть получена как композиция перестановок, затрагивающих только два элемента. Начиная индукцию, отметим, что утверждение, безусловно, верно при $n = 2$.

Предположим сначала, что два пространства анизотропны и, значит, изоморфны. Тогда уравнение

$$\beta_1 = \alpha_1 \xi_1^2 + \ldots + \alpha_n \xi_n^2$$

имеет решение. Пусть k — число индексов i, для которых $\xi_i \neq 0$. Доказательство будет основываться на дополнительной индукции по числу k.

Если $k = 1$, скажем, $\beta_1 = \alpha_1 \xi_1$, то $\langle \alpha_1 \rangle \cong \langle \beta_1 \rangle$, следовательно, $\langle \alpha_2 \rangle \oplus \ldots \oplus \langle \alpha_n \rangle \sim \langle \beta_2 \rangle \oplus \ldots \oplus \langle \beta_n \rangle$ и заключение получается индукцией по n. Если $k \geqslant 2$, то пусть $\xi_1 \neq 0$ и $\xi_2 \neq 0$. Можно предположить, что элемент поля

$$\gamma = \alpha_1 \xi_1^2 + \alpha_2 \xi_2^2$$

ненулевой. Следовательно, $\langle \alpha_1 \rangle \oplus \langle \alpha_2 \rangle \cong \langle \gamma \rangle \oplus \langle \delta \rangle$ для некоторого элемента δ. Подставляя элементы γ и δ вместо элементов α_1 и α_2, выводим заключение индукцией по k.

Предположим теперь, что эти два пространства не анизотропны. Тогда уравнение

$$0 = \alpha_1 \xi_1^2 + \ldots + \alpha_n \xi_n^2$$

имеет нетривиальное решение. Пусть $k \geqslant 2$ будет числом коэффициентов $\xi_i \neq 0$. Докажем индукцией по k, что данную последовательность можно преобразовать в последовательность, в которой $\langle \alpha_1 \rangle \oplus \langle \alpha_2 \rangle \sim 0$, заменяя только по два коэффициента α_i одновременно. Если $k = 2$, то это ясно. Если $k > 2$, то, скажем,

$$\alpha_1 \xi_1^2 + \ldots + \alpha_k \xi_k^2 = 0,$$

где $\alpha_1 \xi_1^2 + \alpha_2 \xi_2^2 = \gamma \neq 0$ и, значит, $\langle \alpha_1 \rangle \oplus \langle \alpha_2 \rangle \cong \langle \gamma \rangle \oplus \langle \delta \rangle$. Как и ранее, можем подставить элементы γ и δ вместо элементов α_1 и α_2. Следовательно, индукцией по k, можем преобразовать последовательность $\alpha_1, \ldots, \alpha_n$ в последовательность, в которой $\langle \alpha_1 \rangle \oplus \langle \alpha_2 \rangle \sim 0$. Аналогично, можем преобразовать последовательность $\beta_1, \ldots, \beta_n$ в последовательность, в которой $\langle \beta_1 \rangle \oplus \langle \beta_2 \rangle \sim 0$. Тогда

$$\langle \alpha_3 \rangle \oplus \ldots \oplus \langle \alpha_n \rangle \sim \langle \beta_3 \rangle \oplus \ldots \oplus \langle \beta_n \rangle,$$

и требуемое утверждение получается индукцией по n. Этим завершается доказательство. □

Глава 4

ДИСКРЕТНЫЕ НОРМИРОВАНИЯ И ДЕДЕКИНДОВЫ ОБЛАСТИ

В § 1 этой главы определяются два гомоморфизма из кольца Витта поля, связанные с полями дискретного нормирования, в кольцо Витта его поля вычетов. В § 2 один из них используется для вычисления кольца Витта $W(\mathbf{Q})$ поля рациональных чисел $\mathbf{Q}$ и для получения нового доказательства утверждения о том, что $W(\mathbf{Z}) \cong \mathbf{Z}$. В § 3 аналогичная конструкция применяется к произвольной дедекиндовой области D с полем частных F для построения точной последовательности

$$0 \to W(D) \to W(F) \to W(D/\oplus W(D/\mathfrak{P}),$$

где прямая сумма взята по всем максимальным идеалам $\mathfrak{P}$ области D. В § 4 эта последовательность применяется в частном случае кольца целых величин числового поля.

§ 1. Гомоморфизм ∂_v: $W(F) \to W(\bar{F})$

Напомним, что *дискретным нормированием* v поля F называется гомоморфизм из группы F^* в аддитивную группу $\mathbf{Z}$, удовлетворяющий неравенству

$$v(\alpha+\beta) \geqslant \min(v(\alpha), v(\beta))$$

при α, β, $\alpha+\beta \neq 0$. Удобно положить $v(0) = +\infty$. Ассоциированное *кольцо нормирования* $\mathfrak{O}$ состоит из всех элементов $\alpha \in F$, для которых $v(\alpha) \geqslant 0$. Это кольцо имеет единственный максимальный идеал $\mathfrak{P}$, состоящий из всех элементов α, для которых $v(\alpha) > 0$. Факторкольцо $\bar{F} = \mathfrak{O}/\mathfrak{P}$ называется *полем вычетов*. Образ любого элемента $u \in \mathfrak{O}^*$ будет обозначаться как $\bar{u} \in \bar{F}^*$.

Построим аддитивный гомоморфизм ∂_v: $W(F) \to W(\bar{F})$, корректно определенный с точностью до домножения на обратимые элементы вида $\langle \bar{u} \rangle$ в $W(\bar{F})$. Для того чтобы определить гомоморфизм ∂_v, удобно задать группу $W(F)$ образующими и соотношениями.

1.1. Лемма (Витт). *Аддитивная группа $W(F)$ порождается элементами $\langle \alpha \rangle$, $\alpha \in F^*$, удовлетворяющими следующим соот-*

ношениям:

1) $\langle\alpha\rangle = \langle\alpha\xi^2\rangle$ *при* $\xi \neq 0$,

2) $\langle\alpha\rangle + \langle -\alpha\rangle = 0$,

3) $\langle\alpha\rangle + \langle\beta\rangle = \langle\alpha+\beta\rangle + \langle\alpha\beta(\alpha+\beta)\rangle$ *при* $\alpha+\beta \neq 0$;

любое соотношение между образующими является их следствием.

Доказательство. Ясно, что эти три соотношения выполняются в группе $W(F)$, а то, что любое соотношение между образующими выводится из них, легко следует из леммы 5.6 гл. 3.

Выберем теперь простой элемент $\pi \in \mathfrak{D}$, т.е. такой элемент π, что $v(\pi) = 1$ и, таким образом, $\pi\mathfrak{D} = \mathfrak{P}$. Тогда любой элемент группы F^* может быть однозначно записан в виде произведения $\pi^i u$, где $u \in \mathfrak{D}^*$.

1.2. Лемма (Спрингер, Кнебуш). *При фиксированных элементе* π *и целом числе* k, *равном* 0 *или* 1, *существует ровно один аддитивный гомоморфизм*

$$\psi^k: \quad W(F) \to W(\bar{F}),$$

отображающий каждый образующий $\langle\pi^i u\rangle$ *либо в* $\langle u\rangle$, *либо в* 0 *в зависимости от того, выполняется сравнение* $i \equiv k \pmod 2$ *или* $i \not\equiv k \pmod 2$.

Доказательство. В силу леммы 1.1 нам надо лишь проверить, что каждое определяющее соотношение группы $W(F)$ отображается в соотношение, справедливое в группе $W(\bar{F})$. Удобно положить символ ϵ_i равным 1 или 0 в зависимости от того, $i \equiv k$ или $i \not\equiv k \pmod 2$. Если

$$\pi^h u_1 + \pi^i u_2 = \pi^j u_3,$$

то нужно доказать, что в группе $W(\bar{F})$

$$\epsilon_h\langle\bar{u}_1\rangle + \epsilon_i\langle\bar{u}_2\rangle = \epsilon_j\langle\bar{u}_3\rangle + \epsilon_{h+i+j}\langle\bar{u}_1\bar{u}_2\bar{u}_3\rangle$$

После деления на подходящую степень элемента π (и перемены, если необходимо, ролей отображений ψ^0 и ψ^1) можем предположить, что два из трех чисел h, i и j равны 0, а третье больше или равно 0.

Случай 1. Если $h = i = j = 0$, то $\bar{u}_1 + \bar{u}_2 = \bar{u}_3$ и требуемое соотношение, конечно, выполняется.

Случай 2. Если $h > i = j = 0$, то $\bar{u}_2 = \bar{u}_3$, значит, $\langle\bar{u}_1\rangle = \langle\bar{u}_1\bar{u}_2\bar{u}_3\rangle$ и соотношение выполняется. Случай $i > 0$ полностью аналогичен.

Случай 3. Если $0 = h = i < j$, то $\bar{u}_2 = \bar{u}_3$, значит

$$\langle\bar{u}_1\rangle + \langle\bar{u}_2\rangle = 0, \quad \langle\bar{u}_3\rangle + \langle\bar{u}_1\bar{u}_2\bar{u}_3\rangle = 0,$$

и опять же требуемое соотношение выполняется. Этим завершается доказательство. □

О п р е д е л е н и е. Построенные гомоморфизмы ψ^0 и ψ^1 из группы $W(F)$ в группу $W(\bar{F})$ называются *гомоморфизмами, ассоциированными с нормированием* v. Нас, в первую очередь, интересует гомоморфизм ψ^1; для него будем использовать также и обозначение

$$\partial_v\colon W(F) \to W(\bar{F}).$$

Отметим, что гомоморфизм ψ^0 корректно определен, тогда как гомоморфизм $\psi^1 = \partial_v$ зависит от выбора элемента π.

Пусть $\mathfrak{O} \subset F$ – ассоциированное с нормированием v кольцо нормирования, и пусть $W(\mathfrak{O}) \to W(F)$ – естественный кольцевой гомоморфизм.

1.3. Л е м м а. *Композиция отображений* $W(\mathfrak{O}) \to W(F) \xrightarrow{\psi^1} W(\bar{F})$ *равна нулю.*

В действительности, в § 3 увидим, что последовательность $W(\mathfrak{O}) \to W(F) \to W(\bar{F}) \to 0$ точна.

Д о к а з а т е л ь с т в о л е м м ы 1.3. Поскольку кольцо $\mathfrak{O}$ локально, любое пространство с внутренним произведением над кольцом $\mathfrak{O}$ может быть легко представлено в виде суммы пространств с внутренним произведением ранга 1 с матрицами внутреннего произведения вида (u) и пространств с внутренним произведением ранга 2 с матрицами внутреннего произведения вида

$$\begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix},$$

где $\alpha \equiv 0 \pmod{\mathfrak{P}}$. В первом случае соответствующий элемент $\langle u \rangle$ в кольце $W(F)$, конечно, удовлетворяет равенству $\psi^1\langle u \rangle = 0$. Во втором случае при $\alpha \neq 0$ соответствующий элемент в кольце $W(F)$ может быть записан как сумма $\langle \alpha \rangle + \langle \alpha(\alpha\beta - 1) \rangle$, где $\alpha\beta - 1 \equiv -1 \pmod{\mathfrak{P}}$. Очевидно, что гомоморфизм ψ^1 аннулирует любую такую сумму. Наконец, при $\alpha = 0$ данное слагаемое расщепляется и, следовательно, соответствует нулевому элементу в кольце Витта. Таким образом, каждое ортогональное слагаемое отображается в нуль в кольце $W(\bar{F})$, откуда следует наше утверждение. □

1.4. Л е м м а. *Каждый из гомоморфизмов* $\psi^k\colon W(F) \to W(\bar{F})$ *отображает идеал* $I^n(F)$ *на идеал* $I^{n-1}(\bar{F})$ *при* $n \geqslant 1$.

Д о к а з а т е л ь с т в о. Проверка показывает, что сумма $\psi^0 + \psi^1$ является кольцевым гомоморфизмом, отображающим идеал $I(F)$ на идеал $I(\bar{F})$ и, следовательно, отображающим идеал $I^n(F)$ на идеал $I^n(\bar{F})$. Таким образом, для любого элемента $w_n \in I^n(F)$ имеем

$$\psi^1(w_n) = -\psi^0(w_n) \pmod{I^n(\bar{F})}.$$

Проводя индукцию, предположим, что $\psi^0(w_n) \equiv 0 \pmod{I^{n-1}(\bar{F})}$.

Тогда для любого элемента $w \in I(F)$ имеем

$$\psi^0(ww_n) = \psi^0(w)\psi^0(w_n) + \psi^1(w)\psi^1(w_n) \equiv$$
$$\equiv \psi^0(w)\psi^0(w_n) - \psi^1(w)\psi^1(w_n) \equiv$$
$$\equiv 0 \,(\mathrm{mod}\, I^n(\bar{F})),$$

поскольку ясно, что разность $\psi^0(w) - \psi^1(w)$ принадлежит идеалу $I(\bar{F})$. Этим завершается индукция и доказательство леммы, поскольку каждый образующий $(\langle\bar{1}\rangle - \langle\bar{u}_1\rangle) \ldots (\langle\bar{1}\rangle - \langle\bar{u}_{n-1}\rangle)$ идеала $I^{n-1}(\bar{F})$ является образом при отображении ψ^0 или ψ^1 образующего

$$(\langle 1\rangle + \langle\pi\rangle)(\langle 1\rangle + \langle u_1\rangle) \ldots (\langle 1\rangle + \langle u_{n-1}\rangle)$$

идеала $I^n(F)$. □

Нас будет особенно интересовать поле вычетов $\bar{F}$ в том случае, когда оно конечно. Через $\mathbf{F}_q$ обозначим поле из q элементов.

1.5. Л е м м а. *Для любого конечного поля* $\mathbf{F}_q$ *идеал* $I(\mathbf{F}_q)$ *либо равен нулю, либо является циклической группой порядка* 2 *в зависимости от того, четное* q *или нечетное. Аддитивная группа* $W(\mathbf{F}_q)$ *является либо циклической группой порядка* 2, *либо циклической группой порядка* 4, *либо нециклической группой порядка* 4 *в зависимости от того, является ли число* q *четным,* $q \equiv 3 \,(\mathrm{mod}\, 4)$ *или* $q \equiv 1 \,(\mathrm{mod}\, 4)$.

Д о к а з а т е л ь с т в о. Для заданных элементов $\alpha, \beta \in \mathbf{F}_q^*$, согласно лемме 3.3 из гл. 2, уравнение

$$\alpha\xi^2 + \beta\eta^2 = 1$$

имеет решение. Следовательно,

$$\langle\alpha\rangle \oplus \langle\beta\rangle \cong \langle 1\rangle \oplus \langle\alpha\beta\rangle,$$

откуда вытекает, что идеал $I^2(\mathbf{F}_q)$ равен нулю. Используя теорему 5.2 гл. 3, получаем, что

$$I(\mathbf{F}_q) \cong \mathbf{F}_q^*/\mathbf{F}_q^{*2},$$

где группа $\mathbf{F}_q^*$ – циклическая порядка $q-1$. Следовательно, идеал $I(\mathbf{F}_q)$ имеет порядок 2 или 1 в зависимости от того, четно число $q-1$ или нечетно.

Если $q \equiv 3 \,(\mathrm{mod}\, 4)$, то -1 не является квадратом в поле $\mathbf{F}_q$ (сравните с теоремой 8.1 гл. 2). Следовательно, $\langle -1\rangle \neq \langle 1\rangle$, откуда $\langle 1\rangle \oplus \langle 1\rangle \neq 0$, и тогда легко выводится, что $W(\mathbf{F}_q) = \mathbf{Z}/4\mathbf{Z}$. С другой стороны, если $q \equiv 3 \,(\mathrm{mod}\, 4)$, то $\langle -1\rangle \cong \langle 1\rangle$, откуда получаем, что $W(\mathbf{F}_q)$ – алгебра над $\mathbf{Z}/2\mathbf{Z}$. Этим завершается доказательство. □

§ 2. Вычисление группы $W(\mathbf{Q})$

В этом параграфе будет полностью описано аддитивное строение кольца Витта $W(\mathbf{Q})$. Будет также дано другое доказательство того факта, что $W(\mathbf{Z}) \cong \mathbf{Z}$ (не использующее теоремы Хассе—Минковского).

Отметим, что p-адическое нормирование поля $\mathbf{Q}$ для каждого простого числа p порождает гомоморфизм

$$\psi^1 = \partial_p \colon W(\mathbf{Q}) \to W(\mathbf{F}_p).$$

Ясно, что при любом фиксированном элементе $w \in W(\mathbf{Q})$ имеем $\partial_p(w) = 0$ для почти всех p. Следовательно, можем объединить эти гомоморфизмы ∂_p в один гомоморфизм ∂: $W(\mathbf{Q}) \to \oplus W(\mathbf{F}_p)$. Через i обозначим единственный кольцевой гомоморфизм из кольца $\mathbf{Z}$ в кольцо $W(\mathbf{Q})$.

2.1. Теорема. *Последовательность*

$$0 \to \mathbf{Z} \xrightarrow{i} W(\mathbf{Q}) \xrightarrow{\partial} \oplus W(\mathbf{F}_p) \to 0$$

точна и расщепляется.

Здесь прямая сумма взята по всем простым числам p. (Таким образом, для того чтобы описать наиболее классическое из колец Витта $W(\mathbf{Q})$ нам надо рассмотреть пространства с внутренним произведением над конечными полями, включая поле $\mathbf{F}_2$, которое исключено из классической теории.) Строение колец $W(\mathbf{F}_p)$ см. в лемме 1.5.

Доказательство теоремы 2.1. Пусть для каждого целого числа $k \geqslant 1$ через L_k обозначено подкольцо кольца $W(\mathbf{Q})$, порожденное элементами $\langle 1 \rangle, \langle 2 \rangle, \ldots, \langle k \rangle$. Тогда ясно, что

$$L_1 \subset L_2 \subset L_3 \subset \ldots$$

и их объединение равно $W(\mathbf{Q})$. Кольцо L_1, очевидно, изоморфно кольцу $\mathbf{Z}$. Отметим, что если k не является простым числом, то $L_k = L_{k-1}$.

С этого момента будем игнорировать кольцевую структуру и думать о подкольце L_k как об аддитивной группе.

2.2. Лемма. *Для каждого простого числа p аддитивный гомоморфизм* ∂_p: $W(\mathbf{Q}) \to W(\mathbf{F}_p)$ *индуцирует изоморфизм*

$$L_p/L_{p-1} \to W(\mathbf{F}_p).$$

Доказательство. Ясно, что гомоморфизм ∂_p аннулирует подгруппу L_{p-1} и отображает группу L_p на группу $W(\mathbf{F}_p)$. Нам потребуется следующее вспомогательное утверждение.

2.3. Лемма. *Если числа n_i и n удовлетворяют соотношениям* $0 < |n_i| < p$, $0 < |n| < p$ *и*

$$n_1 \ldots n_r \equiv n \pmod{p},$$

то

$$\langle pn_1 \dots n_r \rangle \equiv \langle pn \rangle \pmod{L_{p-1}}.$$

Доказательство. Сначала рассмотрим случай $r = 2$. Тогда

$$n_1 n_2 = n + kp,$$

где

$$|k| \leqslant ((p-1)^2 + (p-1))/p < p.$$

Если $k = 0$, то все доказано. В противном случае, домножая тензорно изоморфизм

$$\langle n \rangle \oplus \langle kp \rangle \cong \langle n_1 n_2 \rangle \oplus \langle n_1 n_2 nkp \rangle$$

на элемент $\langle p \rangle$, получаем

$$\langle pn \rangle \oplus \langle k \rangle \cong \langle pn_1 n_2 \rangle \oplus \langle n_1 n_2 nk \rangle$$

и, следовательно, $\langle pn \rangle \equiv \langle pn_1 n_2 \rangle \pmod{L_{p-1}}$. Для любых чисел $n_3, \dots, n_r$, которые меньше по абсолютной величине, чем число p, отсюда следует, что

$$\langle pnn_3 \dots n_r \rangle \equiv \langle pn_1 n_2 n_3 \dots n_r \rangle \pmod{L_{p-1}}.$$

Непосредственная индукция завершает доказательство леммы 2.3. □

Доказательство леммы 2.2. Для каждого образующего $\langle \bar{n} \rangle$ группы $W(\mathbf{F}_p)$ можем выбрать представитель n, для которого $|n| < p$, и поднять образующий $\langle \bar{n} \rangle$ до образующего $\langle pn \rangle$ группы L_p/L_{p-1}. Проверим, что эти поднятые элементы удовлетворяют всем определяющим соотношениям группы $W(\mathbf{F}_p)$. (Сравните с леммой 1.1.) Таким образом, если

$$n' \equiv nm^2 \pmod{p},$$

где n', n, m меньше по абсолютной величине, чем число p, то из леммы 2.3 следует, что

$$\langle pn' \rangle \equiv \langle pnm^2 \rangle = \langle pn \rangle \pmod{L_{p-1}}.$$

Ясно, что $\langle pn \rangle + \langle p(-n) \rangle = 0$, и если $n_1 + n_2 = n$, где можно предполагать, что $-p < n_1 < 0 < n_2 < p$, то

$$\langle pn_1 \rangle \oplus \langle pn_2 \rangle \cong \langle pn \rangle \oplus \langle pnn_1 n_2 \rangle.$$

Таким образом, эти элементы $\langle pn \rangle$ удовлетворяют по модулю подгруппы L_{p-1} всем определяющим соотношениям группы $W(\mathbf{F}_p)$. Это завершает доказательство, поскольку из леммы 2.3 следует, что элементы $\langle pn \rangle$ порождают группу L_p по модулю подгруппы L_{p-1}. □

Доказательство теоремы 2.1. Проводя индукцию по k, покажем, что гомоморфизм

$$L_k \to \bigoplus_{p<k} W(\mathbf{F}_p)$$

сюръективен и его ядро равно $L_1 \cong \mathbf{Z}$. Это утверждение, конечно, верно при $k = 1$. Предположим, что оно верно для $k - 1$. Можно предполагать, что число k простое. По лемме 2.2 для данного элемента в прямой сумме существует элемент w из подгруппы L_k, образ которого имеет нужную k-ю координату. Вычитая образ элемента w, сюръективность получаем по индукции.

Аналогично, если элемент $w \in L_k$ отображается в нуль, то из леммы 2.2 следует, что $w \in L_{k-1}$, и по индукции получаем, что $w \in L_1 \cong \mathbf{Z}$.

Теперь, переходя к прямому пределу при $k \to \infty$, видим, что требуемая последовательность

$$0 \to \mathbf{Z} \to W(\mathbf{Q}) \to \oplus W(\mathbf{F}_p) \to 0$$

точна. Используя гомоморфизм сигнатуры $W(\mathbf{Q}) \to \mathbf{Z}$, получаем, что она расщепляется. В действительности, расщепление единственно, поскольку все группы $W(\mathbf{F}_p)$ периодические. Этим завершается доказательство теоремы 2.1. □

Как одно из следствий теоремы 2.1 мы получаем слабую форму теоремы Хассе–Минковского.

2.4. Следствие. *Если элемент w в кольце Витта $W(\mathbf{Q})$ для любого простого p отображается в нуль в кольце Витта $W(\mathbf{Q}_p)$ поля p-адических чисел и, кроме того, отображается в нуль в кольце $W(\mathbf{R})$, то $w = 0$.*

Доказательство. Это следует из того, что гомоморфизм $\partial_p\colon W(\mathbf{Q}) \to W(\mathbf{F}_p)$ может быть пропущен через группу $W(\mathbf{Q}_p)$. □

2.5. Следствие. *Пусть I – фундаментальный идеал кольца $W(\mathbf{Q})$. Тогда идеал I^3 является свободной аддитивной группой, порожденной элементом $8\langle 1\rangle$.*

Доказательство. Если $w \in I^3(\mathbf{Q})$, то, в силу лемм 1.4 и 1.5, $\partial_p(w) \in I^2(\mathbf{F}_p) = 0$. Следовательно, элемент w является кратным элемента $\langle 1\rangle$. В действительности, элемент w должен быть кратным элемента $8\langle 1\rangle$, поскольку гомоморфизм сигнатуры отображает идеал $I^n(\mathbf{Q})$ в идеал $2^n\mathbf{Z}$. □

Теперь рассмотрим другое доказательство леммы 4.1 из гл. 2.

2.6. Следствие. *Пусть X – произвольное пространство с внутренним произведением над кольцом $\mathbf{Z}$. Тогда индуцированное пространство с внутренним произведением $\mathbf{Q} \otimes X$ над полем $\mathbf{Q}$ изоморфно ортогональной сумме экземпляров пространств $\langle 1\rangle$ и $\langle -1\rangle$.*

Доказательство. Через $Z_{(p)} \subset \mathbf{Q}$ обозначим кольцо нормирования, ассоциированное p-адическим нормированием по-

ля $\mathbf{Q}$. Поскольку естественный гомоморфизм $W(\mathbf{Z}) \to W(\mathbf{Q})$ пропускается через $W(\mathbf{Z}_{(p)})$, из леммы 1.3 следует, что композиция

$$W(\mathbf{Z}) \to W(\mathbf{Q}) \to \oplus W(\mathbf{F}_p)$$

равна нулю. Следовательно, образ кольца $W(\mathbf{Z})$ в кольце $W(\mathbf{Q})$ состоит в точности из всех положительных и отрицательных кратных элемента $\langle 1 \rangle$. Вместе с леммой 7.4 гл. 1 это завершает доказательство. □

В частности, если пространство X неопределенное, отсюда следует существование в пространстве $\mathbf{Q} \otimes X$ ненулевого вектора y, для которого $y \cdot y = 0$. После домножения на подходящее положительное целое число m это дает в решетке X ненулевой вектор $x = my$, для которого $x \cdot x = 0$. Таким образом, мы вновь доказали лемму 4.1 гл. 2.

2.7. Следствие. *Кольцо Витта $W(\mathbf{Z})$ изоморфно кольцу $\mathbf{Z}$.*

Доказательство. Если пространство X является представителем элемента ядра естественного гомоморфизма $W(\mathbf{Z}) \to W(\mathbf{Q})$, то, конечно, пространство X содержит вектор $x \neq 0$, для которого $x \cdot x = 0$. Продолжая доказательство, как в теореме 2.2 гл. 2, можно разложить пространство X в ортогональную сумму $X_0 \oplus X_0^{\perp}$, где пространство X_0 имеет матрицу внутреннего произведения $\begin{pmatrix} 0 & 1 \\ 1 & * \end{pmatrix}$. По индукцин получаем, что пространство X расщепляемо. (Сравните дальше с п. 3.3.) Следовательно, кольцо $W(\mathbf{Z})$ отображается изоморфно на кольцо $\mathbf{Z} \subset W(\mathbf{Q})$. □

Объединяя теорему 2.1 со следствием 2.7, видим, что последовательность

$$0 \to W(\mathbf{Z}) \to W(\mathbf{Q}) \to \oplus W(\mathbf{Z}/p\mathbf{Z}) \to 0$$

точна. В этом виде последовательность допускает значительное обобщение, которое будет обсуждаться в следующем параграфе.

§ 3. Дедекиндовы области

Пусть D – дедекиндова область, т.е. коммутативное кольцо без делителей 0, в котором любой ненулевой идеал может быть однозначно представлен в виде произведения максимальных идеалов. Поле частных области D будет обозначаться через $F \supset D$. Каждый максимальный идеал $\mathfrak{p} \subset D$ порождает $\mathfrak{p}$-адическое нормирование поля F с полем вычетов $D/\mathfrak{p}$ и, следовательно, ему сопоставляется гомоморфизм

$$\partial_{\mathfrak{p}} : W(F) \to W(D/\mathfrak{p}).$$

Будем называть такие максимальные идеалы *простыми* точками. Пусть X – пространство с внутренним произведением над полем F

Если дан конечный набор элементов $x_1, \ldots, x_k$, включающий базис пространства X над полем F, то можно образовать D-подмодуль

$$L = Dx_1 + \ldots + Dx_k \subset X,$$

порожденный элементами $x_1, \ldots, x_k$.

Определение. Любой такой конечно порожденный D-подмодуль, содержащий базис пространства X, называется *решеткой* (или *D-решеткой*) в пространстве X.

Для решетки $L \subset X$ *дуальная* (или *двойственная*) решетка $L^{\#} \subset X$ определяется как множество всех элементов $x \in X$, таких, что $x \cdot l \in D$ для всех элементов $l \in L$.

Отметим, что решетка $L^{\#}$ является в действительности D-модулем, канонически изоморфным модулю $\mathrm{Hom}_D(L, D)$, поскольку любое D-линейное отображение однозначно продолжается до F-линейного отображения $X \to F$, которое должно иметь вид $x \mapsto x \cdot x_0$ для некоторого единственного элемента $x_0 \in L^{\#}$. Используя теорему о том, что каждый конечно порожденный модуль без кручения над кольцом D проективен[1)], видим, что модуль L и, следовательно, модуль $L^{\#}$, конечно порождены и проективны. Очевидно, что модуль $L^{\#}$ содержит базис пространства X над F.

3.1. Теорема. *Пространство с внутренним произведением X над полем F содержит самодвойственную решетку $L = L^{\#}$ тогда и только тогда, когда для любого максимального идеала $\mathfrak{p}$ кольца D класс Витта пространства X принадлежит ядру гомоморфизма*

$$\partial_{\mathfrak{p}} : W(F) \to W(D/\mathfrak{p}).$$

Очевидно, что решетка L самодвойственна тогда и только тогда, когда ограничение данного внутреннего произведения с пространства X на решетку L превращает решетку L в пространство с внутренним произведением над кольцом D.

Доказательство теоремы 3.1. Предположим, что в кольце D существует только один максимальный идеал $\mathfrak{p}$, т.е. кольцо D является кольцом нормирования, ассоциированным с $\mathfrak{p}$-адическим нормированием поля F. Пусть X – пространство с внутренним произведением над полем F. Предположим, что

$$X \cong \langle \pi u_1 \rangle \oplus \ldots \oplus \langle \pi u_m \rangle \oplus \langle u_{m+1} \rangle \oplus \ldots \oplus \langle u_n \rangle.$$

Если класс Витта пространства X принадлежит ядру гомоморфизма $\partial_{\mathfrak{p}}$, то пространство с внутренним произведением

$$\langle \bar{u}_1 \rangle \oplus \ldots \oplus \langle \bar{u}_m \rangle$$

над полем $D/\mathfrak{p}$ расщепляемо. Следовательно, это пространство с

[1)] См., например, [26] или [59]

внутренним произведением в подходящем базисе имеет матрицу внутреннего произведения вида $\begin{pmatrix} 0 & I \\ I & * \end{pmatrix}$. Поднимаясь в локальное кольцо D, легко получаем, что пространство с внутренним произведением $\langle u_1 \rangle \oplus \ldots \oplus \langle u_m \rangle$ над кольцом D имеет в подходящем базисе матрицу внутреннего произведения вида $\begin{pmatrix} A & I \\ I & B \end{pmatrix}$, где каждый элемент матрицы A принадлежит идеалу $\mathfrak{p}$. Следовательно, это же самое утверждение применимо к пространству с внутренним произведением $\langle u_1 \rangle \oplus \ldots \oplus \langle u_m \rangle$ над полем F. Тензорно домножая на пространство $\langle \pi \rangle$, получаем, что пространство с внутренним произведением $\langle \pi u_1 \rangle \oplus \ldots \oplus \langle \pi u_m \rangle$ имеет матрицу внутреннего произведения

$$\begin{pmatrix} \pi A & \pi I \\ \pi I & \pi B \end{pmatrix}.$$

После деления первых $m/2$ базисных векторов на π эта матрица внутреннего произведения заменяется на

$$\begin{pmatrix} \pi^{-1} A & I \\ I & \pi B \end{pmatrix}.$$

Очевидно, что элементы этой матрицы лежат в кольце D, а определитель обратим в кольце D. Значит, этот модифицированный базис порождает требуемую самодвойственную решетку в пространстве $\langle \pi u_1 \rangle \oplus \ldots \oplus \langle \pi u_m \rangle$. Образуя прямую сумму с очевидной самодвойственной решеткой в пространстве $\langle u_{m+1} \rangle \oplus \ldots \oplus \langle u_n \rangle$, получаем требуемую самодвойственную решетку в пространстве X.

Теперь предположим, что дедекиндова область D обладает более чем одним, максимальным идеалом $\mathfrak{p}$. Для каждого такого идеала $\mathfrak{p}$ пусть $D_{\mathfrak{p}} \subset F$ – ассоциированное кольцо нормирования. Выбрав базис $e_1, \ldots, e_n$ пространства X, отметим, что каждое внутреннее произведение $e_i \cdot e_j$ принадлежит кольцу $D_{\mathfrak{p}}$ для почти всех (всех, за исключением конечного числа) простых точек $\mathfrak{p}$. Аналогично, определитель $\det(e_i \cdot e_j)$ обратим в кольце $D_{\mathfrak{p}}$ для почти всех простых точек. Таким образом, существует конечное множество S простых точек, таких, что $D_{\mathfrak{p}}$-решетка

$$D_{\mathfrak{p}} e_1 + \ldots + D_{\mathfrak{p}} e_n$$

самодвойственна при всех $\mathfrak{p} \notin S$.

Теперь предположим, что $\partial_{\mathfrak{p}}(X) \sim 0$ при всех $\mathfrak{p}$. Тогда для каждой простой точки $\mathfrak{p} \in S$ можем, в силу приведенных выше соображений, выбрать самодвойственную $D_{\mathfrak{p}}$-решетку. Нам понадобится следующее утверждение.

3.2. Лемма. *Пусть X – векторное пространство над полем F с базисом $e_1, \ldots, e_n$ и для каждой простой точки $\mathfrak{p}$ задана $D_{\mathfrak{p}}$-решетка $L_{\mathfrak{p}}$ в пространстве X, при этом*

$$L_{\mathfrak{p}} = D_{\mathfrak{p}} e_1 + \ldots + D_{\mathfrak{p}} e_n$$

для почти всех $\mathfrak{p}$. Тогда существует ровно одна такая D-решетка

$$L = \cap L_{\mathfrak{p}},$$

что порожденная решеткой L $D_{\mathfrak{p}}$-решетка, равна решетке $L_{\mathfrak{p}}$ для любой простой точки $\mathfrak{p}$.

Это утверждение доказано, например, в [61, § 81:14].

Объединяя лемму 3.2 с приведенным выше рассуждением, построим такую D-решетку L, что индуцированные $D_{\mathfrak{p}}$-решетки $D_{\mathfrak{p}}L$ самодвойственны для каждого максимального идеала $\mathfrak{p}$. Таким образом, если $x, y \in L$, то $x \cdot y \in D_{\mathfrak{p}}$ для каждого $\mathfrak{p}$ и, следовательно, $x \cdot y \in D$. Это доказывает, что $L \subset L^{\#}$. Обратно, если $x \in L^{\#}$, то $x \cdot D_{\mathfrak{p}}L \subset D_{\mathfrak{p}}$ для каждой простой точки $\mathfrak{p}$ и, следовательно,

$$x \in \cap (D_{\mathfrak{p}} L)^{\#} = \cap D_{\mathfrak{p}} L = L.$$

Таким образом, решетка L самодвойственная.

Обратно, если пространство X содержит самодвойственную решетку, то из леммы 1.3 легко выводится, что образ пространства X в кольце $W(D/\mathfrak{p})$ равен нулю при любом $\mathfrak{p}$. Этим завершается доказательство. □

3.3. Следствие. *Для любой дедекиндовой области D точна последовательность*

$$0 \to W(D) \to W(F) \to \oplus W(D/\mathfrak{p})$$

(здесь сумма берется по всем ненулевым простым идеалам).

Доказательство. Если пространство с внутренним произведением L над кольцом D соответствует расщепляемому пространству с внутренним произведением над полем F, то надо доказать, что пространство L само расщепляемо. Будем считать, что пространство L является самодвойственной решеткой в пространстве с внутренним произведением $X = F \otimes_D L$. Пусть $N \subset X$ – пространство половинной размерности, для которого $N \cdot N = 0$, т.е. $N = N^{\perp}$. Тогда пересечение $N \cap L$, очевидно, является самоортогональным подпространством в пространстве L. Это пересечение является прямым слагаемым в решетке L, поскольку фактормодуль

$$L/(N \cap L) \subset X/N$$

конечно порожден и не имеет кручения, а следовательно, проек-

тивен. Оно равно $(N \cap L)^{\perp}$, поскольку если элемент $x \in L$ ортогонален $N \cap L$, то он ортогонален и всему подпространству N и, следовательно, принадлежит подмодулю $N^{\perp} \cap L = N \cap L$.

Таким образом, пространство L расщепляемо, и последовательность $0 \to W(D) \to W(F)$ точна. Оставшаяся часть доказательства проводится непосредственно с использованием теоремы 3.1. □

З а м е ч а н и е. В отличие от ситуации в § 2 не утверждается, что гомоморфизм ∂: $W(F) \to \oplus W(D/\mathfrak{p})$ обязательно сюръективен.

3.4. П р и м е р. Если F – конечное расширение поля рациональных чисел, то коядро гомоморфизма ∂ может быть вычислено следующим образом. Пусть через $\mathscr{C}$ обозначена группа классов идеалов дедекиндовой области $D \subset F$. Тогда существует однозначно определяемый гомоморфизм

$$W(D/\mathfrak{p}) \to \mathscr{C}/\mathscr{C}^2,$$

переводящий каждый образующий $\langle u \rangle$ кольца $W(D/\mathfrak{p})$ в класс идеала $\mathfrak{p}$ по модулю $\mathscr{C}^2$. Теперь нетрудно проверить, что точна последовательность

$$W(F) \xrightarrow{\partial} \oplus W(D/\mathfrak{p}) \to \mathscr{C}/\mathscr{C}^2 \to 0.$$

(Использование приведенной ниже леммы 4.4 вместе с предшествующими ей рассуждениями показывает, что любой элемент из $\oplus I(D/\mathfrak{p})$ поднимается в $I^2(F)$. После этого достаточно только проверить, что коядро гомоморфизма из $I(F)/I^2(F) \cong F^*/F^{*2}$ в $\oplus W(D/\mathfrak{p})/I(D/\mathfrak{p}) \cong \mathbf{Z}/2\mathbf{Z}$, индуцированного гомоморфизмом ∂, изоморфно группе $\mathscr{C}/\mathscr{C}^2$.)

3.5. П р и м е р. Пусть $D = \mathbf{R}[x, y]/(x^2 + y^2 - 1)$ – кольцо, состоящее из всех полиномиальных функций на окружности. Тогда каждая точка $(\cos\theta, \sin\theta)$ единичной окружности задает идеал $\mathfrak{p}_\theta$, состоящий из многочленов $f(x, y)$, равных нулю в точке $(\cos\theta, \sin\theta)$. Ясно, что факторкольцо $D/\mathfrak{p}_\theta$ является полем вещественных чисел и, следовательно, $W(D/\mathfrak{p}_\theta) \cong \mathbf{Z}$. Ассоциированный гомоморфизм

$$\partial_\theta : \ W(F) \to W(D/\mathfrak{p}_\theta) \cong \mathbf{Z}$$

корректно определен с точностью до знака. Ясно, что гомоморфизм ∂_{θ_0} переводит каждый образующий $\langle f \rangle$ кольца $W(F)$ либо в ± 1, либо в 0 в зависимости от того, изменяет или нет функция $f(\cos\theta, \sin\theta)$ свой знак при переходе переменной θ через θ_0. Выбор знака для гомоморфизма ∂_θ эквивалентен выбору локальной ориентации окружности. Согласованно выбирая ориентации, мы получаем соотношение

$$\sum_\theta \partial_\theta \langle f \rangle = 0$$

при любом $f \in F^*$. Теперь нетрудно проверить, что коядро отображения

$$\partial\colon\ W(F) \to \oplus W(D/\mathfrak{p})$$

является бесконечной циклической группой.

§ 4. Числовые поля

Пусть F — конечное расширение поля рациональных чисел и D — кольцо всех алгебраических целых чисел в поле F. (См., например, [44, с. 20].) Поскольку строение кольца $W(F)$ прозрачно (сравните с п. 5.9 гл. 3), можно использовать точную последовательность из следствия 3.3 для описания кольца $W(D)$.

Сначала приведем некоторые обозначения.

Пусть d — число диадических простых идеалов в кольце D (т.е. число таких простых идеалов $\mathfrak{p}$, что факторкольцо $D/\mathfrak{p}$ имеет характеристику 2). Пусть r — число вложений поля F в поле вещественных чисел и c — число пар сопряженных вложений поля F в качестве плотного подмножества в поле комплексных чисел. Таким образом, $r + 2c$ равно степени поля F над полем $\mathbf{Q}$.

Два ненулевых идеала $\mathfrak{a}$ и $\mathfrak{b}$ в кольце D называются *строго эквивалентными*, если $\mathfrak{a} = \tau\mathfrak{b}$ для некоторого элемента поля τ, являющегося *вполне положительным*. (т.е. положительным при любом вложении поля F в поле $\mathbf{R}$). Пусть $\hat{\mathscr{C}}$ — группа всех классов строго эквивалентных ненулевых идеалов. Это — конечное расширение обычной группы классов идеалов, которую мы обозначаем $\mathscr{C}$.

4.1. Теорема[1]. *Радикал $\mathfrak{N}$, состоящий из всех нильпотентных элементов кольца Витта $W(D)$, является конечной группой, порядок которой равен числу 2^{c+d-1}, умноженному на число элементов в группе $\mathscr{C}$, порядок которых не превосходит 2.*

Ясно, что элемент в кольце $W(D)$ нильпотентен тогда и только тогда, когда нильпотентен его образ в кольце $W(F)$. Сравнивая с п. 3.6 и п. 3.8 гл. 3, получаем, что последовательность

$$0 \to \mathfrak{N}_D \to W(D) \to \mathbf{F}_2 \to 0$$

точна в том случае, когда F — вполне мнимое поле ($r = 0$). В противном случае точна последовательность

$$0 \to \mathfrak{N}_D \to W(D) \xrightarrow{\sigma} \mathbf{Z}^{\Omega}.$$

---

[1]) Мы благодарны Кнебушу, указавшему на ошибку в первоначальной формулировке этого результата.

Ниже увидим (см. следствие 4.5), что образ $\sigma(W(D))$ всегда является подгруппой конечного индекса в кольце $\mathbf{Z}^{\Omega}$.

4.2. Следствие. *Если F – вполне мнимое поле, то кольцо $W(F)$ конечно и его порядок равен числу 2^{c+d}, умноженному на число элементов порядка 2 в группе классов идеалов.*

Приведем некоторые примеры. Для мнимого квадратичного поля $\mathbf{Q}(\sqrt{-2})$ или $\mathbf{Q}(\sqrt{-3})$ имеем $W(D) \cong \mathbf{Z}/4\mathbf{Z}$, тогда как для поля $\mathbf{Q}(\sqrt{-7})$ кольцо $W(D)$ изоморфно кольцу $\mathbf{Z}/8\mathbf{Z}$. Для поля $\mathbf{Q}(\sqrt{-1})$ это нециклическая группа порядка 4 с базисом $\langle 1 \rangle$ и $\langle i \rangle$. Наконец, для поля $\mathbf{Q}(\sqrt{-5})$ кольцо $W(D)$ является суммой кольца $\mathbf{Z}/4\mathbf{Z}$ и подгруппы порядка 2, соответствующей не являющемуся свободным пространству с внутренним произведением над кольцом D. (См. приведенную ниже таблицу.)

4.3. Следствие. *Радикал $\mathfrak{R}_D$ равен нулю тогда и только тогда, когда кольцо D вполне вещественно, имеет только одну диадическую простую точку, имеет нечетное число классов и содержит обратимые элементы, имеющие произвольно заданные наборы знаков. Если эти условия выполнены, то аддитивная группа кольца $W(F)$ свободна и имеет базис $\langle 1 \rangle, \langle u_1 \rangle, \ldots, \langle u_{r-1} \rangle$, где элемент u_j отрицателен в j-м упорядочении поля F и положителен в оставшихся $r-1$ упорядочениях.*

Этим условиям удовлетворяют, например, поля $\mathbf{Q}$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{5})$ и $\mathbf{Q}(\sqrt{13})$. (Сравните как с приводимой ниже таблицей, так и с таблицами в [9].)

Доказательства следствий 4.2 и 4.3 достаточно просты. □

Таблица описывает аддитивную структуру кольца $W(D)$ для квадратичного поля $\mathbf{Q}(\sqrt{n})$. Циклическая группа порядка m обозначается кратко числом m.

$n=$	$W(D) \cong$	$n=$	$W(D) \cong$
2	$\mathbf{Z} \oplus \mathbf{Z}$	-1	$2 \oplus 2$
3	$\mathbf{Z} \oplus \mathbf{Z} \oplus 2$	-2	4
5	$\mathbf{Z} \oplus \mathbf{Z}$	-3	4
6	$\mathbf{Z} \oplus \mathbf{Z} \oplus 2$	-5	$4 \oplus 2$
7	$\mathbf{Z} \oplus \mathbf{Z} \oplus 2$	-6	$4 \oplus 2$
10	$\mathbf{Z} \oplus \mathbf{Z} \oplus 2$	-7	8
11	$\mathbf{Z} \oplus \mathbf{Z} \oplus 2$	-10	$4 \oplus 2$
13	$\mathbf{Z} \oplus \mathbf{Z}$	-11	4
14	$\mathbf{Z} \oplus \mathbf{Z} \oplus 2$	-13	$4 \oplus 2$
15	$\mathbf{Z} \oplus \mathbf{Z} \oplus 2 \oplus 2$	-14	$4 \oplus 2 \oplus 2$
		-15	$8 \oplus 2$

Эти результаты легко проверяются, если использовать [9, с. 481–485] вместе с доказательством теоремы 4.1.

Доказательство теоремы 4.1. Будем считать кольцо $W(D)$ подкольцом кольца $W(F)$. Следовательно, можно рассмотреть пересечение радикала $\mathfrak{R}_D$ с идеалом $I^2(F)$. В качестве первого шага доказательства покажем, что это пересечение $\mathfrak{R}_D \cap I^2(F)$ является элементарной 2-группой порядка 2^{d-1}.

Пусть через $F_\mathfrak{p}$ обозначено $\mathfrak{p}$-адическое пополнение поля F. Классическая теория, описанная, например, в [61], показывает, что пространство с внутренним произведением над полем $F_\mathfrak{p}$ однозначно определяется своими рангом, определителем и инвариантом Хассе. Если ранг больше или равен 3, то определитель в $F_\mathfrak{p}^*/F_\mathfrak{p}^{*2}$ и инвариант Хассе в $\mathbf{Z}^*$ могут быть заданы произвольно. Отсюда легко выводится, что идеал $I^2(F_\mathfrak{p})$ циклический порядка 2, а гомоморфизм Хассе–Витта.

$$h_\mathfrak{p}: I^2(F_\mathfrak{p}) \to Z^*$$

биективен. (Сравните с пп. 5.4–5.9 гл. 3.)

Теперь вспомним, что гомоморфизм $\partial_\mathfrak{p}: I^2(F_\mathfrak{p}) \to I(D/\mathfrak{p})$ из § 1 сюръективен. Если простой идеал $\mathfrak{p}$ не диадический, то в силу леммы 1.5 группа $I(D/\mathfrak{p})$ состоит из двух элементов, откуда следует, что гомоморфизм

$$\partial_\mathfrak{p}: I^2(F_\mathfrak{p}) \to I(D/\mathfrak{p})$$

также биективен. *После отождествления группы $I(D/\mathfrak{p})$ с группой $\mathbf{Z}^*$ получаем, что для любого простого недиадического идеала $\mathfrak{p}$ гомоморфизм*

$$\partial_\mathfrak{p}: I(F) \to I(D/\mathfrak{p}) \cong \mathbf{Z}^*$$

может быть отождествлен с $\mathfrak{p}$-м инвариантом Хассе–Витта.

Классическая теория дает следующее описание идеала $I^2(F)$.

4.4. Лемма. *Элемент w идеала $I^2(F)$ однозначно определяется своими инвариантами Хассе–Витта $h_\mathfrak{p}(w) \in \mathbf{Z}^*$ для различных простых идеалов $\mathfrak{p}$ и значениями своей сигнатуры $\sigma_p(w) \in 4\mathbf{Z}$ на различных упорядочениях поля F. Эти инварианты удовлетворяют лишь соотношениям $h_\mathfrak{p}(w) = 1$ для почти всех $\mathfrak{p}$ и $\prod_\mathfrak{p} h_\mathfrak{p}(w) = \prod_P (-1)^{\sigma_P(w)/4}$.*

Доказательство. Это утверждение выводится из классического описания пространств с внутренним произведением над полем F (сравните с [61, § 72]) и рассуждений § 5 гл. 3. □

Рассмотрим теперь вопрос о том, какие элементы w из идеала $I^2(F)$ принадлежат подкольцу $W(D)$. Необходимым и достаточным является условие, что элемент $\partial_\mathfrak{p}(w)$ должен равняться нулю для всех простых идеалов $\mathfrak{p}$. Мы видели, что если простой идеал $\mathfrak{p}$ не диадический, то элемент $\partial_\mathfrak{p}(w)$ может быть отождествлен с $\mathfrak{p}$-м инвариантом Хассе–Витта. Если же идеал $\mathfrak{p}$ диади-

ческий, то $\partial_{\mathfrak{p}} I^2(F) = 0$. Очевидно, это доказывает следующее утверждение.

4.5. Следствие. *Элемент w из пересечения $W(D) \cap I^2(F)$ однозначно задается своими инвариантами Хассе для d диадических простых точек и своими сигнатурами $\sigma_P(w) \in 4\mathbf{Z}$ относительно r упорядочений поля F. Эти инварианты подчиняются лишь соотношению* $\prod_{\mathfrak{p}} h_{\mathfrak{p}}(w) = \prod_P (-1)^{\sigma_P(w)/4}$

В частности, образ $\sigma(W(D) \cap I^2(F))$ в точности равен идеалу $4\mathbf{Z}^{\Omega}$, поскольку всегда существует по крайней мере одна диадическая простая точка. *Следовательно, $\sigma(W(D))$ является подкольцом конечного индекса в кольце $\mathbf{Z}^{\Omega}$.*

Отсюда следует, что группа $W(D) \cap I^2(F)$ является прямой суммой свободной абелевой группы ранга r и элементарной 2-группы порядка 2^{d-1}. Рассматривая ограничение на ядро отображения σ, *получаем, что подгруппа $\mathfrak{N}_D \cap I^2(F)$ является элементарной 2-группой порядка 2^{d-1}.*

Далее, нам нужно изучить факторгруппу $\mathfrak{N}_D/\mathfrak{N}_D \cap I^2(F)$. Ясно, что она вкладывается в факторгруппу

$$I(F)/I^2(F) \cong F^*/F^{*2}$$

и, следовательно, является элементарной 2-группой. Ее образ в группе F^*/F^{*2} может быть явно описан следующим образом. Пусть через $F_+^* \subset F^*$ обозначена подгруппа индекса 2^r, состоящая из вполне положительных элементов, а через $F^*_{\text{чет}}$ обозначена подгруппа, состоящая из таких элементов α, $\mathfrak{p}$-адическая норма которых четна для всех простых идеалов $\mathfrak{p}$. Другими словами, подгруппа $F_{\text{чет}}$ состоит из всех элементов α, для которых дробный идеал $D\alpha$ равен квадрату $\mathfrak{a}^2$ некоторого дробного идеала $\mathfrak{a}$.

4.6. Лемма. *Факторгруппа $\mathfrak{N}_D/\mathfrak{N}_D \cap I^2(F)$ канонически изоморфна факторгруппе $(F_+^* \cap F^*_{\text{чет}})/F^{*2}$.*

Доказательство. Нужно решить, какие элементы α группы F^* по модулю подгруппы F^{*2} могут встречаться в качестве дискриминанта пространств с внутренним произведением над кольцом D с сигнатурой нуль. Если элемент α вполне положителен и

$$D\alpha = \mathfrak{a}^2$$

для некоторого дробного идеала $\mathfrak{a}$, то можем превратить дробный идеал $\mathfrak{a}$ в пространство с внутренним произведением, введя внутреннее произведение

$$x \cdot y = xy/\alpha$$

при $x, y \in \mathfrak{a}$. Очевидно, пространство $\mathfrak{a}$ положительно определено в любом упорядочении P поля F. Следовательно, пространство

с внутренним произведением

$$\mathfrak{a} \oplus \langle -1 \rangle$$

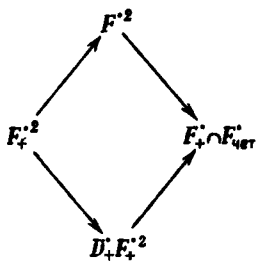
над кольцом D представляет элемент кольца $W(D) \subset W(F)$ с сигнатурой нуль и дискриминантом $\alpha F^{\cdot 2}$.

Обратно, если дано пространство с внутренним произведением X над кольцом D, имеющее четный ранг и нулевую сигнатуру, то можно считать (добавляя, если необходимо, гиперболическую плоскость) что ранг n делится на 4. Внешняя степень $\wedge^n X$ имеет ранг 1 и положительно определена в любом упорядочении. Поэтому легко проверяется, что $\wedge^n X$ изоморфно идеалу $\mathfrak{a}$ с внутренним произведением

$$x \cdot y = xy/\alpha,$$

где элемент α вполне положителен, порождает идеал $\mathfrak{a}^2$ и $d(X) = \alpha F^{\cdot 2}$.

Рассмотрим теперь вложения



Предположим сначала, что $r \geqslant 1$. Обходя диаграмму сверху и учитывая, что подгруппа $F_+^{\cdot}$ в группе $F^{\cdot}$ имеет индекс 2^r, легко выводим, что подгруппа $F^{\cdot 2}$ имеет индекс 2^{r-1} в $F^{\cdot 2}$. Ранее заметили, что индекс подгруппы $F^{\cdot 2}$ в группе $F_+^{\cdot} \cap F_{\text{чет}}^{\cdot}$ равен порядку группы $\mathfrak{N}_D / \mathfrak{N}_D \cap I^2(F)$.

Обходя диаграмму снизу, по теореме Дирихле об обратимых элементах получаем, что факторгруппа

$$D_+^{\cdot} F_+^{\cdot 2} / F_+^{\cdot 2} \cong D_+^{\cdot} / D_+^{\cdot 2}$$

имеет порядок 2^{r+c-1} (все еще в предположении о том, что $r \geqslant 1$). Утверждаем, что факторгруппа

$$(F_+^{\cdot} \cap F_{\text{чет}}^{\cdot}) / D_+^{\cdot} F_+^{\cdot 2}$$

канонически изоморфна подгруппе элементов порядка 2 в группе $\hat{\mathscr{C}}$. Действительно, каждый элемент α из подгруппы $F_+^{\cdot} \cap F_{\text{чет}}^{\cdot}$ определяет единственный дробный идел $\mathfrak{a}$,

$$\mathfrak{a}^2 = D\alpha,$$

представляющий элемент второго порядка в группе $\hat{\mathscr{C}}$, а этот

идеал $\mathfrak{a}$ представляет единичный элемент группы $\hat{\mathscr{C}}$ тогда и только тогда, когда элемент α является произведением обратимого элемента и квадрата вполне положительного элемента поля.

Сравнивая теперь обходы сверху и снизу диаграммы, получаем равенство

$$2^{r-1} \mid \mathfrak{N}_D/\mathfrak{N}_D \cap I^2(F) \mid = 2^{r+c-1} \mid \hat{\mathscr{C}}_2 \mid$$

при $r \geqslant 1$ [1]. Если $r = 0$, то можно провести аналогичные рассуждения, но потребуется заменить числа 2^{r-1} и 2^{r+c-1} на числа 1 и 2^c соответственно. Таким образом, в любом случае

$$\mid \mathfrak{N}_D/\mathfrak{N}_D \cap I^2(F) \mid = 2^c \mid \hat{\mathscr{C}}_2 \mid .$$

Домножая это равенство на $\mid \mathfrak{N}_D \cap I^2(F) \mid = 2^{d-1}$, получаем требуемую формулу. □

В завершение приведем еще одно следствие теоремы 4.1. Пусть D – кольцо целых чисел произвольного числового поля F.

4.7. Следствие. *Аддитивная группа $W(D)$ циклична тогда и только тогда, когда поле F является одним из следующих полей:* $\mathbf{Q}$, $\mathbf{Q}(\sqrt{-2})$ *или* $\mathbf{Q}(\sqrt{-p})$, *где p – простое число вида $4k+3$.*

Доказательство. Если $W(D)$ – бесконечная циклическая группа, то из следствия 4.3 легко выводится, что $F = \mathbf{Q}$. Таким образом, можно считать, что группа $W(D)$ конечна и, следовательно, поле F вполне мнимо. Напомним, что из доказательства теоремы 4.1 нам известно, что факторгруппа

$$\mathfrak{N}_D/\mathfrak{N}_D \cap I^2(F)$$

является элементарной 2-группой, порядок которой равен числу элементов второго порядка в группе классов идеалов, умноженному на 2^c. Если группа $W(D)$ циклична, то, очевидно, факторгруппа должна быть циклической и, следовательно, число c должно равняться 1, а число классов кольца D должно быть нечетным.

Таким образом, поле F является мнимым квадратичным полем. Точная формула для числа классов мнимого квадратичного поля $\mathbf{Q}(\sqrt{-n})$ приводится, например, в [9, гл. V, § 4.1]. Из этой формулы видно, что число классов нечетно тогда и только тогда, когда не содержащее квадратов целое число n равно 1, 2 или простому числу вида $4k+3$. Случаи $n = 1, 2$ легко разбираются, поэтому предположим, что $n \geqslant 3$.

Если n – простое число вида $8k+3$, то существует только одна диадическая простая точка (а именно: $\mathfrak{p} = 2D$), поэтому из следствия 4.2 следует, что группа $W(D)$ имеет порядок 4. Но эле-

---

[1] Здесь $\mid X \mid$ – число элементов множества X.

мент -1 не является квадратом в поле F. Поэтому элемент $\langle 1 \rangle \in$ $\in W(D)$ имеет порядок не меньше 4. Это доказывает, что $W(D)$ – циклическая группа порядка 4.

С другой стороны, если n – простое число вида $8k + 7$, то 2 разлагается в кольце D и, следовательно, порядок группы $W(D)$ равен 8. Используя инвариант Хассе–Витта, связанный с одной из двух диадических простых точек, видим, что

$$\langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle 1 \rangle \neq 0,$$

поэтому элемент $\langle 1 \rangle$ имеет порядок не меньше 8. Это показывает, что $W(D)$ – циклическая группа порядка 8, чем завершается доказательство. □

Глава 5

НЕКОТОРЫЕ ПРИМЕРЫ

В этой заключительной главе мы кратко опишем некоторые примеры билинейных форм, естественно возникающих в топологии, дифференциальной геометрии и в теории чисел. Три параграфа этой главы совершенно независимы друг от друга.

§ 1. Гомологическая теория многообразий

Нам будет удобно пользоваться старомодной терминологией и называть *замкнутым* компактное многообразие без края.

Пусть $M = M^{2n}$ – замкнутое многообразие размерности $2n$, и пусть $\mathbf{F}_2$ – поле из двух элементов. Если x и y – классы гомологий в $H_n(M; \mathbf{F}_2)$, то определен их индекс пересечения

$$x \cdot y = y \cdot x \in \mathbf{F}_2.$$

Теорема о двойственности Пуанкаре показывает (см., например, [67]), что группа $H_n(M; \mathbf{F}_2)$ является пространством с внутренним произведением над полем $\mathbf{F}_2$, где в качестве внутреннего произведения используется индекс пересечения.

Рассмотрим теперь частный случай поверхности, т.е. предположим, что $n = 1$. Если многообразие M связно, то любой класс

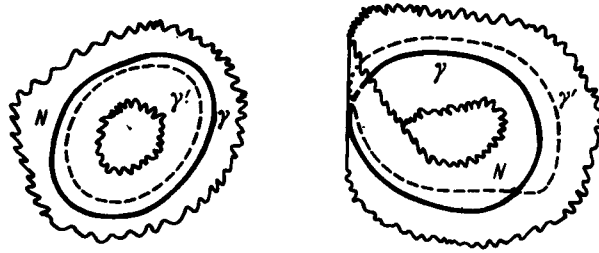


Рис. 5

гомологий $x \in H_1(M; \mathbf{F}_2)$ может быть представлен простой замкнутой кривой $\gamma \subset M$. *Отметим, что индекс пересечения $x \cdot x$ равен нулю тогда и только тогда, когда ориентируема некоторая малая*

окрестность N кривой γ. Действительно, если окрестность N ориентируема, то можно гладкой гомотопией деформировать кривую γ в кривую $\gamma' \subset N$, непересекающуюся с кривой γ (рис. 5). Если же кривая γ не обладает ориентируемой окрестностью, то у нее есть окрестность, являющаяся листом Мёбиуса. В этом случае, продеформировав кривую γ в кривую γ', трансверсально пересекающую кривую γ, получим нечетное число точек пересечений. Этим доказано следующее утверждение.

1.1. Л е м м а. *Поверхность M ориентируема тогда и только тогда, когда $x \cdot x = 0$ для каждого $x \in H_1(M; \mathbf{F}_2)$.*

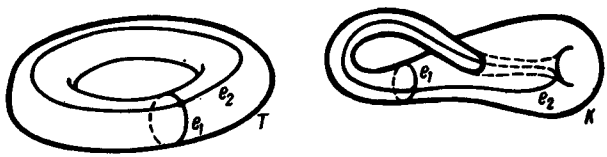


Рис. 6. Тор и бутылка Клейна

Поскольку замкнутая связная поверхность полностью определяется своей ориентируемостью или неориентируемостью и своим первым числом Бетти (см., например, [53]), получается такое утверждение.

1.2. С л е д с т в и е. *Замкнутые связные поверхности M и M' гомеоморфны тогда и только тогда, когда изоморфны пространства с внутренними произведениями $H_1(M; \mathbf{F}_2)$ и $H_1(M'; \mathbf{F}_2)$.*

Приведем некоторые примеры. Для тора T пространство $H_1(T; \mathbf{F}_2)$ является гиперболической плоскостью с базисом e_1, e_2 и матрицей внутреннего произведения $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (рис. 6). Для проективной плоскости P имеется единственный базисный вектор e, для которого $e \cdot e = 1$. Поэтому

$$H_1(P; \mathbf{F}_2) \cong \langle 1 \rangle.$$

Наконец, для бутылки Клейна K имеется базис e_1, e_2 с матрицей внутреннего произведения $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Иначе, используя ортогональный базис $e_1 + e_2, e_2$, видим, что

$$H_1(K; \mathbf{F}_2) \cong \langle 1 \rangle \oplus \langle 1 \rangle.$$

Это разложение, конечно, соответствует геометрическому соотношению

$$K \cong P \# P,$$

где знак $\#$ обозначает операцию связной суммы: в каждом сла-

гаемом вырезается маленькое отверстие и края склеиваются между собой. Аналогично, соотношению $\langle 1\rangle \oplus \langle 1\rangle \oplus \langle 1\rangle \cong \langle 1\rangle \oplus$ (гиперболическая плоскость) из § 4 гл. 1 соответствует геометрическое соотношение

$$P \# K \cong P \# T.$$

1.3. Л е м м а. *Каждое пространство с внутренним произведением над полем* $\mathbf{F}_2$ *изоморфно пространству* $H_1(M; \mathbf{F}_2)$ *для некоторой замкнутой связной поверхности* M.

Действительно, в силу п. 3.3 гл. 1 данное пространство с внутренним произведением изоморфно пространству

$$\langle 1\rangle \oplus \ldots \oplus \langle 1\rangle \oplus S,$$

где пространство S симплектично. В силу п. 3.5 гл. 1 любое симплектическое пространство с внутренним произведением над полем $\mathbf{F}_2$ изоморфно ортогональной сумме гиперболических плоскостей. Таким образом, наше пространство с внутренним произведением может быть реализовано как пространство $H_1(M; \mathbf{F}_2)$, где поверхность M является подходящей связной суммой $P \# \ldots \# P \# T \# \ldots \# T$. □

Эти результаты остаются справедливыми, если вместо поля $\mathbf{F}_2$ взять любое совершенное поле характеристики 2.

Понятие расщепляемого пространства с внутренним произведением тесно связано с теорией кобордизмов.

1.4. У т в е р ж д е н и е. *Поверхность* M *является краем компактного трехмерного многообразия тогда и только тогда, когда пространство с внутренним произведением* $H_1(M; \mathbf{F}_2)$ *расщепляемо.*

В самом деле, если замкнутое многообразие M^{2n} является краем компактного многообразия P^{2n+1}, то, согласно теореме Тома, ядро N гомоморфизма вложения края

$$H_n(M^{2n}; \mathbf{F}_2) \to H_n(P^{2n+1}; \mathbf{F}_2)$$

удовлетворяет условиям $N \cdot N = 0$ и $\operatorname{rk}(N) = \frac{1}{2} \operatorname{rk} H_n(M^{2n}; \mathbf{F}_2)$ (сравните с [79, § 8]). Следовательно, $N = N^{\perp}$ и, значит, пространство с внутренним произведением $H_n(M^{2n}; \mathbf{F}_2)$ расщепляемо.

В случае поверхности легко выводится и обратное утверждение, поскольку тор и бутылка Клейна, очевидно, являются краями некоторых многообразий.. (Ясно, что пространство с внутренним произведением над полем $\mathbf{F}_2$ расщепляемо тогда и только тогда, когда оно имеет четный ранг.)

З а м е ч а н и е. Для некоторых целей лучше работать с бо́льшим пространством с внутренним произведением, содержащим все группы гомологий $H_i(M; \mathbf{F}_2)$. Если $x \in H_i(M; \mathbf{F}_2)$ и $y \in H_j(M; \mathbf{F}_2)$, то индекс пересечения определен при $i + j = \dim M$. Если положить

$x \cdot y = 0$ при $i + j \neq \dim M$, то прямая сумма

$$H_*(M; \mathbf{F}_2) = \oplus H_i(M; \mathbf{F}_2).$$

превращается в пространство с внутренним произведением над полем $\mathbf{F}_2$. Ясно, что это пространство с внутренним произведением расщепляемо при нечетной размерности многообразия M и является ортогональной суммой пространства $H_n(M; \mathbf{F}_2)$ и расщепляемого пространства с внутренним произведением в том случае, когда размерность M равна $2n$. Тензорное произведение

$$H_*(M; \mathbf{F}_2) \otimes H_*(M'; \mathbf{F}_2)$$

канонически изоморфно пространству с внутренним произведением $H_*(M \times M'; \mathbf{F}_2)$.

Пусть теперь M^{2n} – замкнутое *ориентируемое* многообразие и F – произвольное поле коэффициентов. *Тогда пространство* $H_n(M^{2n}; F)$ *является пространством с внутренним произведением над полем* F, *где в качестве внутреннего произведения используется индекс пересечения.* Это пространство с внутренним произведением симметрично или кососимметрично в зависимости от того, четно или нечетно число n. Если многообразие M^{2n} является краем ориентируемого $2n + 1$-мерного многообразия, то пространство с внутренним произведением $H_n(M^{2n}; F)$ расщепляемо.

Аналогичным образом можно работать с целыми коэффициентами. Заметим, что $\mathbf{Z}$-модуль $H_n(M^{2n}; \mathbf{Z})/$(периодическая часть) является пространством с внутренним произведением над кольцом $\mathbf{Z}$. Особенно интересен случай односвязного четырехмерного многообразия.

1.5. Т е о р е м а. *Пусть* M *и* M' *– замкнутые ориентируемые односвязные четырехмерные многообразия. Сохраняющая ориентацию гомотопическая эквивалентность* $M \to M'$ *существует тогда и только тогда, когда симметрическое пространство с внутренним произведением* $H_2(M; \mathbf{Z})$ *изоморфно пространству* $H_2(M'; \mathbf{Z})$.

З а м е ч а н и е. Неизвестно, каждое ли пространство с внутренним произведением над кольцом $\mathbf{Z}$ может быть реализовано как пространство $H_2(M; \mathbf{Z})$ для подходящего замкнутого односвязного четырехмерного многообразия M. В гл. 2 мы описали положительно определенное пространство Γ_8 над кольцом $\mathbf{Z}$, имеющее ранг 8 и удовлетворяющее условию

$$x \cdot x \equiv 0 \pmod 2$$

для каждого $x \in \Gamma_8$. Было бы чрезвычайно интересно выяснить, существует ли изоморфизм $\Gamma_8 \cong H_2(M; \mathbf{Z})$ для некоторого многообразия M. Если такое многообразие M существует, то по теореме Рохлина оно не может быть задано какой-либо кусочно-линейной структурой (сравните с [55]).

Наши частные примеры поверхностей имеют довольно точные аналоги среди четырехмерных многообразий. Например, если через P обозначить комплексную проективную плоскость, то

$$H_2(P; \mathbf{Z}) \cong \langle 1 \rangle .$$

Если через $\bar{P}$ обозначить то же самое многообразие с обратной ориентацией, то

$$H_2(\bar{P}; \mathbf{Z}) \cong \langle -1 \rangle .$$

Аналогом тора является произведение $T = S^2 \times S^2$, имеющее в подходящем базисе e_1, e_2 матрицу внутреннего произведения $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Отметим, что индекс самопересечения $(e_1 + e_2) \cdot (e_1 + e_2)$ диагонального класса гомологий $e_1 + e_2$ равен 2. Аналогом бутылки Клейна является тотальное пространство нетривиального S^2-расслоения K над сферой S^2. Геометрическими рассуждениями можно показать, что

$$K \cong P \# \bar{P}$$

и что

$$K \# \bar{P} \cong T \# \bar{P},$$

хотя ясно, что пространство с внутренним произведением $H_2(K; \mathbf{Z})$ не изоморфно пространству $H_2(T; \mathbf{Z})$. (Сравните с § 4 гл. 1.)

Доказательство теоремы 1.5. Пусть E – внутренность четырехмерного диска, вложенного в многообразие M. Используя точную гомологическую последовательность пары $(M, M \setminus E)$ с коэффициентами в кольце $\mathbf{Z}$ вместе с двойственностью Пуанкаре, легко получаем, что

$$H_i(M \setminus E) \tilde{=} H_i(pt) \text{ при } i \neq 2.$$

Группа

$$H_2(M \setminus E) \cong H_2(M)$$

является свободной абелевой группой ранга r. Изоморфизм двойственности Пуанкаре

$$H_2(M) \cong H^2(M) \cong \mathrm{Hom}(H_2(M); \mathbf{Z})$$

показывает, что индекс пересечения задает внутреннее произведение на пространстве $H_2(M)$.

Поскольку $\pi_1(M \setminus E) = 0$, то по теореме Гуревича

$$\pi_2(M \setminus E) \cong H_2(M \setminus E) \cong H_2(M).$$

Следовательно, существует отображение

$$f\colon S^2 \vee \ldots \vee S^2 \to M \setminus E$$

из r-кратного букета двумерных сфер, индуцирующее изомор-

физм групп гомологий

$$H_*(S^2\vee\ldots\vee S^2)\to H_*(M\setminus E).$$

Поскольку пространство $M\setminus E$ является абсолютным окрестностным ретрактом, оно имеет гомотопический тип CW-комплекса. Следовательно, по теореме Уайтхеда отображение f является гомотопической эквивалентностью (см. [67, с. 507–523]).

Но пространство M получается из $M\setminus E$ приклеиванием четырехмерной клетки ([67, с. 191]). Следовательно, пространство M имеет гомотопический тип пространства, получающегося из r-кратного букета $S^2\vee\ldots\vee S^2$ приклеиванием четырехмерной клетки по некоторому отображению

$$g\colon S^3\to S^2\vee\ldots\vee S^2.$$

Обозначим через $(S^2\vee\ldots\vee S^2)\underset{g}{\cup}E^4$ пространство, получающееся в результате такой склейки. Гомотопический тип пространства M полностью определяется гомотопическим классом отображения g в группе $\pi_3(S^2\vee\ldots\vee S^2)$.

Для вычисления группы $\pi_3(S^2\vee\ldots\vee S^2)$ поместим $S^2=P_1(\mathbf{C})$ в бесконечномерное комплексное проективное пространство $P_\infty(\mathbf{C})$ и воспользуемся вложением

$$S^2\vee\ldots\vee S^2\subset S^2\times\ldots\times S^2\subset P_\infty(\mathbf{C})\times\ldots\times P_\infty(\mathbf{C}).$$

Обозначим r-кратный букет через B, а r-кратное произведение проективных пространств — через K. Вложение $B\subset K$ индуцирует изоморфизм

$$H_4(K)\cong H_4(K,B)\cong\pi_4(K,B)\cong\pi_3(B).$$

Действительно, первый из этих изоморфизмов получается из точной гомологической последовательности пары (K,B), второй — из относительной теоремы Гуревича, и третий — из точной гомотопической последовательности пары.

Ясно, что группа $H_4(K)$ является свободным $\mathbf{Z}$-модулем. Двойственный модуль

$$H^4(K)\cong\operatorname{Hom}(H_4(K),\mathbf{Z})$$

имеет базис, состоящий из произведений u_iu_j, где $i\leqslant j$, а элементы $u_1,\ldots,u_r$ образуют базис группы когомологий

$$H^2(K)\cong H^2(B)\cong H^2(M\setminus E)\cong H^2(M)$$

([67, с. 341]). Продолжим вложение $B\to K$ до отображения

$$B\underset{g}{\cup}E^4\to K.$$

Поднимая произведения $u_iu_j\in H^4(K)$ в $H^4(B\underset{g}{\cup}E^4)\cong H^4(M)$,

а затем вычисляя класс ориентации $[M] \in H_4(M) \cong \mathbf{Z}$, получаем симметрическую матрицу целых чисел $u_i u_j [M]$, полностью описывающую пространство с внутренним произведением $H^2(M) \cong H_2(M)$. Но очевидно, что эти числа описывают также гомотопический класс отображения приклеивания клетки в группе $\pi_3(B) \cong \pi_4(K, B) \cong H_4(K)$. Этим завершается доказательство. □

§ 2. Кольца гладких вещественнозначных функций

Слово *гладкий* будет означать k раз непрерывно дифференцируемый, где k – фиксированное число, $0 \leqslant k \leqslant \infty$.

Для данного гладкого паракомпактного многообразия M обозначим $R(M)$ кольцо всех гладких вещественнозначных функций на многообразии M. Тогда конечнопорожденный проективный модуль над кольцом $R(M)$ может быть отождествлен с модулем $\Gamma(\xi)$, состоящим из всех гладких сечений некоторого вещественного расслоения ξ над M (см. [70]). Проективный модуль $\Gamma(\xi)$ свободен тогда и только тогда, когда ξ является тривиальным векторным расслоением.

Внутренним произведением на модуле $\Gamma(\xi)$ (принимающим значения в кольце $R(M)$) называется гладкая функция, ставящая в соответствие каждой точке x многообразия M вещественнозначное внутреннее произведение на слое расслоения ξ в точке x.

Сначала рассмотрим симплектический случай. Векторные расслоения с симплектическим внутренним произведением естественно возникают в теории гамильтоновых дифференциальных уравнений (см., например, [51]). Такие расслоения классифицируются отображениями базы M в классифицирующее пространство $BSp(2n, \mathbf{R})$, имеющее тот же гомотопический тип, что и пространство $BU(n)$ (см., [69, § 19.8, 41.15]). Здесь через $Sp(2n, \mathbf{R})$ обозначена группа изометрий $2n$-мерного вещественного симплектического пространства с внутренним произведением. *Таким образом, существует взаимно однозначное соответствие между симплектическими пространствами с внутренним произведением ранга $2n$ над кольцом $R(M)$ и комплексными n-мерными векторными расслоениями над многообразием M* ([69, § 41]). Симплектическое пространство с внутренним произведением обладает симплектическим базисом тогда и только тогда, когда соответствующее комплексное векторное расслоение тривиально.

Одним из наиболее прозрачных примеров является ориентированное двумерное векторное расслоение. В этом случае $\Lambda^2 \xi$ – тривиальное линейное расслоение и поэтому модуль $\Gamma(\xi)$ обладает единственным симплектическим внутренним произведением. Если расслоение ξ не тривиально (например, если ξ – касательное рас-

слоение двумерной сферы), то модуль $\Gamma(\xi)$, конечно, не может обладать симплектическим базисом.

Рассмотрим теперь симметрический случай. Векторные расслоения с симметрическим внутренним произведением естественно возникают в римановой геометрии и общей теории относительности. Следующее утверждение принадлежит Г. Люстигу (см. как [69], так и [18]).

Теорема. *Кольцо Витта $W(R(M))$ классов симметрических пространств с внутренним произведением над $R(M)$ канонически изоморфно кольцу $KO(M)$ виртуальных вещественных векторных расслоений над многообразием M.*

Приведем набросок доказательства. Пусть ξ — вещественное векторное расслоение над многообразием M с симметрическим внутренним произведением. Прежде всего, покажем, что расслоение ξ изоморфно ортогональной сумме $\xi^+ \oplus \xi^-$, где на каждом слое расслоения ξ^+ внутреннее произведение положительно определено, а на каждом слое расслоения ξ^- — отрицательно определено. Для каждого слоя ξ_x расслоения ξ через $P(\xi_x)$ обозначим множество, состоящее из всех положительно определенных подпространств максимального ранга в пространстве ξ_x. Тогда $P(\xi_x)$ имеет естественную топологию и в действительности является топологической клеткой. Чтобы доказать это, выберем отмеченную точку $\eta_x^0 \in P(\xi_x)$. Ясно, что вещественное пространство с внутренним произведением ξ_x разлагается в прямую сумму

$$\xi_x = \eta_x^0 \oplus \eta_x^{0\perp}.$$

Произвольный элемент $\eta_x \in P(\xi_x)$ может быть реализован как график линейного отображения $f \in \mathrm{Hom}(\eta_x^0, \eta_x^{0\perp})$, принадлежащего открытому выпуклому множеству, определенному неравенством

$$|f(v) \cdot f(v)| < v \cdot v$$

при всех $v \in \eta_x^0$, $v \neq 0$.

Очевидно, что клетки $P(\xi_x)$ образуют слои нового расслоения над многообразием M. Это новое расслоение обладает сечением

$$x \mapsto \xi_x^+ \in P(\xi_x)$$

(см. [79, с. 51]). Получающиеся в результате пространства ξ_x^+ образуют слои требуемого подрасслоения $\xi^+ \subset \xi$, для которого $\xi = \xi^+ \oplus \xi^{+\perp} = \xi^+ \oplus \xi^-$, что и требовалось доказать. □

Векторные расслоения ξ^+ и ξ^- определены однозначно (с точностью до изоморфизма). Действительно, если расслоение ξ разлагается еще в одну прямую сумму $\eta^+ \oplus \eta^-$, то $\eta^+ \cap \xi^- = 0$ и, сле-

довательно, композиция отображений

$$\eta^+ \subset \xi \to \xi/\xi^- \cong \xi^+$$

является изоморфизмом векторных расслоений.

Нетрудно показать, что пространство с внутренним произведением $\Gamma(\xi^+ \oplus \xi^-)$ расщепляется тогда и только тогда, когда векторные расслоения ξ^+ и ξ^- изоморфны. Дальнейшие подробности оставляются читателю.

§ 3. Дискриминант расширения поля

Пусть $F \subset F'$ – конечное расширение поля рациональных чисел. Тогда кольцо R, состоящее из всех целых алгебраических чисел поля F, является дедекиндовой областью ([44, с. 20]), так же как и кольцо R', состоящее из всех целых алгебраических чисел поля F'. Забывая о кольцевой структуре, будем рассматривать бо́льшее кольцо R' как модуль над кольцом R. Этот R-модуль конечно порожден и не имеет кручения ([44, с. 6]). Следовательно, по классической теореме Штейница, модуль R' проективен, поскольку он R-линейно изоморфен прямой сумме вида $R \oplus \ldots \oplus R \oplus \mathfrak{a}$, где $\mathfrak{a}$ – ненулевой идеал в кольце R (см., например, [59, с. 21]). Очевидно, что число слагаемых n (включая $\mathfrak{a}$) равно степени поля F' над полем F.

Модуль R' обладает канонической R-значной симметрической билинейной формой

$$\beta(x, y) = \operatorname{trace}_{F'|F}(xy).$$

Таким образом, пара (R', β) является пространством с билинейной формой над кольцом R.

Как и в п. 5.7 гл. 1, рассмотрим n-ю внешнюю степень $\bigwedge_R^n R'$. Эта внешняя степень, будучи изоморфной как R-модуль идеалу $\mathfrak{a}$, является проективным модулем ранга 1. На нем имеется каноническая симметрическая билинейная форма $\hat{\beta}$, заданная равенством

$$\hat{\beta}(x_1 \wedge \ldots \wedge x_n, y_1 \wedge \ldots \wedge y_n) = \det(\beta(x_i, y_j)).$$

"Дискриминант" расширения $R' \supset R$ обычно определяется как некоторый идеал $\mathfrak{b}$ в R ([44, с. 65]). Например, $\mathfrak{b}$ может быть описан как идеал, порожденный образом функции

$$\hat{\beta}: \bigwedge_R^n R' \times \bigwedge_R^n R' \to R.$$

Определяя *дискриминант* модуля R' над кольцом R как класс изоморфных объектов, содержащий пространство с билинейной формой $(\bigwedge_R^n R', \hat{\beta})$ над кольцом R, получаем несколько более чувствительный инвариант (см. [75]).

Например, предположим, что модуль R' оказался свободным над кольцом R с базисом $e_1, \ldots, e_n$. Тогда модуль $\wedge_R^n R'$ свободен над кольцом R и имеет единственный базисный элемент $e = e_1 \wedge \ldots \ldots \wedge e_n$. Полагая

$$d_0 = \hat{\beta}(e, e) = \det(\operatorname{trace}(e_i e_j)) \in R,$$

получаем, что пространство $(\wedge_R^n R', \hat{\beta})$ изоморфно свободному пространству с билинейной формой $\langle d_0 \rangle = \langle d_0 \rangle_R$. Этот элемент d_0 корректно определен с точностью до умножения на квадрат обратимого элемента. Очевидно, что идеал дискриминанта $\mathfrak{d}$, порожденный образом функции $\hat{\beta}$, равен главному идеалу $d_0 R$.

Даже если модуль R' не свободен над кольцом R, поле F', очевидно, свободно над полем F. При работе над полем F соответствующая внешняя степень $\wedge_F^n F'$ снабжается соответствующей билинейной формой $\hat{\beta}$. Очевидно, что

$$(\wedge_F^n F', \hat{\beta}) \cong \langle d \rangle_F$$

для некоторого элемента поля $d \neq 0$, причем элемент d корректно определен с точностью до умножения на подгруппу F^{*2}. Следующий результат принадлежит Артину [3] и Фрёлиху [70].

3.1. Лемма. *Если d и $\mathfrak{d}$ определены, как описано выше, то существует ровно один дробный идеал $\mathfrak{a}$ в поле F, удовлетворяющий уравнению*

$$(1)\quad \mathfrak{d} = d\mathfrak{a}^2.$$

Внешняя степень $\wedge_R^n R'$ R-линейно изоморфна идеалу $\mathfrak{a}$. Следовательно, кольцо R' свободно над кольцом R тогда и только тогда, когда идеал $\mathfrak{a}$ главный.

В действительности будет показано, что пространство с билинейной формой $(\wedge_R^n R', \hat{\beta})$ изоморфно пространству $(\mathfrak{a}, \beta d)$, где

$$(2)\quad \beta_d(a_1, a_2) = da_1a_2$$

для всех $a_1, a_2 \in \mathfrak{a}$. Мы уже отмечали, что модуль R' R-линейно изоморфен сумме $R \oplus \ldots \oplus R \oplus \mathfrak{a}_1$ для некоторого идеала $\mathfrak{a}_1$ и, следовательно, $\wedge_R^n R' \cong \mathfrak{a}_1$. Очевидно, что любая R-значная билинейная форма на идеале $\mathfrak{a}_1$ равна для некоторого элемента $d_1 \in \mathfrak{a}_1^{-2}$ форме βd, определенной формулой (2). Таким образом,

$$(3)\quad (\wedge_R^n R', \hat{\beta}) \cong (\mathfrak{a}_1, \beta_{d_1}),$$

откуда следует, что $\mathfrak{d} = d_1 \mathfrak{a}_1^2$. Тензорно домножая изоморфизм (3) на поле F, видим, что $d_1 = df^2$ для некоторого $f \in F^*$. Определяя теперь $\mathfrak{a} = f\mathfrak{a}_1$, получаем, что $\mathfrak{d} = d\mathfrak{a}^2$ и

$$(\mathfrak{a}_1, \beta_{d_1}) \cong (\mathfrak{a}, \beta_d).$$

Этим завершается доказательство. □

3.2. Пример. *Предположим, что* $R = \mathbf{Z}[\sqrt{-5}]$ *– кольцо целых чисел поля* $\mathbf{Q}(\sqrt{-5})$ *и что* R' *– кольцо целых чисел в квадратичном расширении* $\mathbf{Q}(\sqrt{-5}, \sqrt{2})$. *Тогда дискриминант* $(\Lambda_R^2 R', \hat{\beta})$ *этого расширения изоморфен пространству* $(\mathfrak{p}, \beta_2)$, *где через* $\mathfrak{p}$ *обозначен простой идеал* $2R + (1+\sqrt{-5})R$, *для которого* $\mathfrak{p}^2 = 2R$, *и* $\beta_2(a_1, a_2) = 2a_1a_2$ *при* $a_1, a_2 \in \mathfrak{p}$. *Идеал* $\mathfrak{p}$ *не является главным, поэтому кольцо* R' *не является свободным* R*-модулем.*

Доказательство. Кольцо R' может быть описано явно, если отметить, что элементы $1, \sqrt{-5}, \sqrt{2}, (\sqrt{2}+\sqrt{-10})/2$ образуют базис кольца R' над $\mathbf{Z}$. Это может быть установлено, например, вложением поля $F' = \mathbf{Q}(\sqrt{-5}, \sqrt{2})$ в круговое поле $\mathbf{Q}(e^{2\pi i/40})$ и использованием того факта, что кольцо R' является пересечением поля F' и кольца $\mathbf{Z}[e^{2\pi i/40}]$ круговых целых чисел ([44, с. 75]). Подробности вычислений оставляются читателю. Идеал $\mathfrak{d} = \mathfrak{d}_{R'/R}$ теперь может быть вычислен непосредственно. Другой способ заключается в том, что сначала вычисляются два дискриминанта

$$(\Lambda_{\mathbf{Z}}^2 R, \hat{\beta}) \cong \langle -20 \rangle_{\mathbf{Z}},$$

$$(\Lambda_{\mathbf{Z}}^4 R', \hat{\beta}) \cong \langle 6400 \rangle_{\mathbf{Z}},$$

а затем используется тождество (где число n является степенью поля F' над полем F)

$$\mathfrak{d}_{R'/\mathbf{Z}} = \mathfrak{d}_{R/\mathbf{Z}}^{\,n} \operatorname{norm}_{R/\mathbf{Z}}(\mathfrak{d}_{R'/R}),$$

которое следует из [44, с. 60, 66]. В любом случае, находим, что идеал $\mathfrak{d}_{R'/R}$ равен $\mathfrak{p}^4 = 4R$.

Выбирая базис e_1, e_2 в расширении $F' = F(\sqrt{2})$ поля F и проводя несложные вычисления, получаем, что

$$\det(\operatorname{trace}(e_i e_j)) \equiv 2 \pmod{F^{\cdot 2}}.$$

Таким образом, в лемме 3.1 можно выбрать $d = 2$. Теперь из уравнения $\mathfrak{d} = 2\mathfrak{a}^2$ выводим, что $\mathfrak{a} = \mathfrak{p}$. Это завершает доказательство. □

Аналогичный пример описан в [50].

Приложение 1

КВАДРАТИЧНЫЕ ФОРМЫ

Теория симметрических билинейных форм тесно связана с теорией квадратичных форм. В действительности, над кольцом, в котором 2 – обратимый элемент, эти две теории неразличимы. Поэтому, хотя мы и сосредоточили основное внимание на билинейных формах, представляется целесообразным дать краткое описание квадратичных форм. Пусть X – R-модуль. Как всегда, мы предполагаем, что кольцо R коммутативно и имеет 1.

О п р е д е л е н и е. *Квадратичной формой на модуле* X называется такая функция $q : X \to R$, что для всех $\alpha \in R$

$$q(\alpha x) = \alpha^2 q(x),$$

а функция $(x \mid y)$ на $X \times X$, определенная равенством

$$(x \mid y) = q(x + y) - q(x) - q(y),$$

билинейна над кольцом R.

Например, если β – билинейная форма (не обязательно симметрическая), то очевидно, что функция

$$q(x) = \beta(x, x)$$

является квадратичной формой с ассоциированной симметрической билинейной формой

$$(x \mid y) = \beta(x, y) + \beta(y, x).$$

Если X – проективный модуль, то любая квадратичная форма на нем может быть получена таким путем из (несимметрической) билинейной формы. Две билинейные формы β и β' порождают одну и ту же квадратичную форму тогда и только тогда, когда разность $\beta - \beta'$ симплектична.

Отметим тождество $(x \mid x) = 2q(x)$. Таким образом, ассоциированная с квадратичной формой симметрическая билинейная форма $(x \mid y)$ должна для всех x удовлетворять сравнению

$$(x \mid x) \equiv 0 \pmod{2R}.$$

Если элемент 2 не является делителем нуля в кольце R, то любая удовлетворяющая этому сравнению симметрическая билинейная

форма ассоциирована с единственной квадратичной формой

$$q(x)=\frac{1}{2}(x\mid x).$$

В частности, если 2 – *обратимый элемент, то каждая симметрическая билинейная форма получается из однозначно определенной квадратичной формы* $\frac{1}{2}(x\mid x)$.

Определение. Пусть $(X_1,q_1),\ldots,(X_n,q_n)$ – модули с квадратичными формами над произвольным коммутативным кольцом R. *Ортогональная сумма* $X_1\oplus\ldots\oplus X_n$ определяется как прямая сумма модулей X_i с квадратичной формой, определенной равенством

$$q(x_1\oplus\ldots\oplus x_n)=\Sigma\, q_i(x_i),$$

где суммирование ведется по $1\leqslant i\leqslant n$.

Ассоциированная билинейная форма $(x\mid y)$ на модуле $X=X_1\oplus\ldots\ldots\oplus X_n$ является ортогональной суммой ассоциированных билинейных форм на модулях X_i. Следовательно, форма $(x\mid y)$ является внутренним произведением тогда и только тогда, когда каждая форма $(x\mid y)_i$ является внутренним произведением.

Определение. Назовем пару (X,q) *квадратичным пространством с внутренним произведением*, если модуль X конечно порожден и проективен, а ассоциированная с квадратичной формой q билинейная форма $(x\mid y)$ является внутренним произведением на пространстве X (см. п. 1.1 гл. 1).

В § 4 гл. 1 видели, что в случае характеристики, равной 2, теорема Витта о сокращении неверна для пространств с внутренним произведением. Интересно отметить, что аналог этой теоремы для *квадратичных* пространств с внутренним произведением верен при любой характеристике поля. Это означает, что если

$$(X_1,q_1)\oplus(X,q)\cong(X_2,q_2)\oplus(X,q),$$

где (X_1,q_1), (X_2,q_2) и (X,q) – квадратичные пространства с внутренним произведением над полем, то $(X_1,q_1)\cong(X_2,q_2)$. Это доказано, например, в [85] или [11].

Следующее важное замечание было сделано Фрёлихом [76] и независимо Сахом [65]. *Если* X_1 – *симметрический модуль с билинейной формой, а* X_2 – *модуль с квадратичной формой, то тензорное произведение* $X_1\otimes X_2$ *является модулем с квадратичной формой.* Действительно, если заданы симметрическая билинейная форма β_1 на модуле X_1 и квадратичная форма q_2 на модуле X_2, то существует, и притом единственная, квадратичная

форма q на модуле $X_1 \otimes X_2$, удовлетворяющая равенствам

$$q(x_1 \otimes x_2) = \beta(x_1, x_1)\, q_2(x_2)$$

и

$$(x_1 \otimes x_2 \mid y_1 \otimes y_2) = \beta(x_1, y_1)\,(x_2 \mid y_2)$$

(каждое из этих равенств необходимо для определения формы q).

Отметим изоморфизм

$$\langle 1 \rangle \otimes X_2 \cong X_2.$$

Если X_1 и X_2 являются модулями с квадратичными формами, то, используя ассоциированную билинейную форму $(x_1 \mid y_1)$ в качестве формы β_1, получаем, что $X_1 \otimes X_2$ также является модулем с квадратичной формой. Квадратичная форма q на модуле $X_1 \otimes X_2$ определяется равенствами

$$q(x_1 \otimes x_2) = 2q_1(x_1)\, q_2(x_2)$$

и

$$(x_1 \otimes x_2 \mid y_1 \otimes y_2) = (x_1 \mid y_1)(x_2 \mid y_2).$$

Множитель 2 несколько неожидан, но он необходим. Этот множитель ошибочно опущен в [11].

Алгебра Витта $WQ(R)$ квадратичных пространств с внутренним произведением над кольцом R теперь может быть определена следующим образом. (Сравните с [6], [65].) Квадратичное пространство с внутренним произведением (X, q) называется *расщепляемым* тогда и только тогда, когда модуль X содержит прямое слагаемое N, для которого $N = N^{\perp}$ и $q(N) = 0$. Квадратичные пространства с внутренним произведением (X_1, q_1) и (X_2, q_2) принадлежат одному и тому же *классу Витта*, если

$$(X_1, q_1) \oplus (S_1, q_1') \cong (X_2, q_2) \oplus (S_2, q_2'),$$

где пространства (S_1, q_1') расщепляемые. Классы Витта квадратичных пространств с внутренним произведением над кольцом R образуют требуемую алгебру $WQ(R)$. Ясно, что $WQ(R)$ является коммутативной ассоциативной алгеброй над кольцом Витта $W(R)$. В общем случае эта алгебра не обладает единицей. Имеется каноническое пополнение

$$a\colon WQ(R) \to W(R),$$

а произведение двух произвольных элементов w_1 и w_2 в алгебре $WQ(R)$ определяется равенством $w_1 w_2 = a(w_1) w_2$. Если элемент 2 обратим в кольце R, то отображение a, конечно, является изоморфизмом.

В случае поля F легко проверяется, что любое квадратичное пространство с внутренним произведением над полем F является

ортогональной суммой расщепляемого квадратичного пространства с внутренним произведением и анизотропного квадратичного пространства с внутренним произведением (т.е. такого, что $q(x) \neq 0$ при $x \neq 0$). Кроме того, любые два расщепляемых пространства одного и того же ранга изоморфны. *Применяя теперь теорему Витта, получаем, что любой класс Витта в алгебре $WQ(F)$ обладает ровно одним, с точностью до изоморфизма, анизотропным представителем.*

Предположим, в частности, что F является полем характеристики 2. Тогда билинейная форма $(x \mid y)$, ассоциированная с квадратичной формой, обязательно симплектична:

$$(x \mid x) = 2q(x) = 0.$$

Следовательно, гомоморфизм пополнения

$$WQ(F) \to W(F)$$

тождественно равен нулю. Действительно, если (X, p) — квадратичное пространство с внутренним произведением, то оно обладает симплектическим базисом (п. 3.5 гл. 1) и, следовательно, представляет нулевой элемент в кольце Витта $W(F)$.

Важный инвариант квадратичного пространства с внутренним произведением в случае характеристики 2 был определен Арфом. Через

$$\wp: F \to F$$

обозначим аддитивный гомоморфизм, для которого $\wp(\xi) = \xi^2 + \xi$. Выбрав симплектический базис $x_1, \ldots, x_n, y_1, \ldots, y_n$ в пространстве X, Арф показал, что класс вычетов

$$q(x_1)q(y_1) + \ldots + q(x_n)q(y_n)$$

по модулю подгруппы $\wp$ является инвариантом пространства (X, q). Этот инвариант Арфа зависит лишь от класса Витта пространства (X, q) и, следовательно, порождает аддитивный эпиморфизм

$$\Delta: WQ(F) \to F/\wp F.$$

Ядро гомоморфизма Δ было вычислено Сахом следующим образом. Пусть $I \subset W(F)$ — фундаментальный идеал. Тогда

$$\ker \Delta = I \cdot WQ(F).$$

Получающийся в результате аддитивный изоморфизм

$$WQ(F)/I \cdot WQ(F) \cong F/\wp F,$$

возможно, следовало бы считать аналогом изоморфизма Пфистера

$$I/I^2 \cong F^*/F^{*2}$$

(сравните с п. 5.2 гл. 3).

Рассмотрим теперь простой пример, поясняющий роль инварианта Арфа. Пусть (X, q) – квадратичное пространство с внутренним произведением ранга 2. Продолжаем считать, что характеристика поля F равна 2. Любому базису x, y, для которого $(x \mid y) = 1$, сопоставим класс вычетов

$$q(x)q(y) \pmod{\wp(F)}.$$

Это инвариант пространства (X, q). Действительно, при элементарном изменении базиса $\overline{x} = x + \alpha y$ имеем $q(\overline{x}) = q(x) + \alpha + \alpha^2 q(y)$ и, следовательно,

$$q(\overline{x})\, q(y) = q(x)q(y) + \wp(\alpha q(y)).$$

Из этой формулы видно, что *квадратичная форма q представляет* 0 *тогда и только тогда, когда* $q(x)q(y) \equiv 0 \pmod{\wp(F)}$. В самом деле, если $q(x)\, q(y) \equiv 0$ и $q(y) \neq 0$, то можно выбрать элемент α таким образом, что $q(\overline{x})\, q(y) = 0$. В действительности, можно выбрать симплектический базис $\overline{x}, \overline{y}$, для которого $q(\overline{x}) = q(\overline{y}) = 0$, полагая $\overline{y} = \beta\overline{x} + y$ и подбирая подходящее β.

Если поле F совершенно, то смежный класс $q(x)\, q(y) \pmod{\wp(F)}$ всегда является полным инвариантом квадратичного пространства с внутренним произведением.

Доказательство. Можно считать, что $q(x) \neq 0$. Выбирая произвольного представителя $\Delta_0 = q(x)\, q(y) + \wp(\alpha)$ инварианта Арфа, получаем, что симплектический базис

$$\overline{x} = x/\sqrt{q(x)}, \qquad \overline{y} = \alpha\overline{x} + y\sqrt{q(x)}$$

удовлетворяет равенствам

$$q(\overline{x}) = 1, \qquad q(\overline{y}) = \Delta_0.$$

Таким образом, Δ_0 определяет класс изоморфности формы (X, q). □

В частности, если F – конечное поле характеристики 2, то отсюда следует, что имеется ровно два квадратичных пространства с внутренним произведением ранга 2 над полем F. Рассматривая аддитивную точную последовательность $0 \to \mathbf{F}_2 \to F \xrightarrow{\wp} F$, видим, что коядро $F/\wp(F)$ имеет порядок 2.

Приложение 2

ЭРМИТОВЫ ФОРМЫ

Пусть R — ассоциативное, не обязательно коммутативное кольцо с 1. *Инволюцией* в кольце R (или, более точно, "инволютивным антиавтоморфизмом") называется аддитивный гомоморфизм $\alpha \to \alpha^J$ из кольца R в себя, удовлетворяющий условиям

$$(\alpha\beta)^J = \beta^J \alpha^J$$

и

$$(\alpha^J)^J = \alpha$$

для всех α и β. Отметим, что $1^J = 1$.

Примеры. Если кольцо R коммутативно, то тождественное отображение кольца R является инволюцией. Для любой мультипликативной группы Π целочисленное групповое кольцо $\mathbf{Z}\Pi$ обладает канонической инволюцией, отображающей каждый элемент группы σ в σ^{-1} (см. [18] или [73, § 5]). Кольцо $n \times n$-матриц над коммутативным кольцом имеет каноническую инволюцию, отображающую каждую матрицу в транспонированную к ней.

Пусть R — некоторое кольцо, а X — левый R-модуль.

Определение. *Эрмитовой формой* на модуле X называется функция

$$\varphi: X \times X \to R,$$

R-линейная по первой переменной и удовлетворяющая условию

$$\varphi(y, x) = \varphi(x, y)^J.$$

Отсюда вытекает, что функция $\varphi(x, y)$ билинейна над $\mathbf{Z}$ и

$$\varphi(\alpha x, \beta y) = \alpha\varphi(x, y)\beta^J.$$

Если отображение

$$y \mapsto \varphi(\ , y)$$

из X в $\mathrm{Hom}(X, R)$ биективно, то функция φ называется эрмитовым *внутренним произведением*, а пара (X, φ) — *эрмитовым модулем с внутренним произведением*.

Так же, как и для симметрических или квадратичных пространств с внутренним произведением, можно определить понятие

расщепляемого эрмитова пространства с внутренним произведением. Работая по модулю этих расщепляемых пространств, получим *группу Витта* $W(R,J)$ эрмитовых пространств с внутренним произведеннем над кольцом R. В коммутативном случае группа $W(R,J)$ имеет естественную кольцевую структуру. Если J – тождественная инволюция, то кольцо совпадает с обычным кольцом Витта $W(R)$.

Если X – свободный R-модуль с базисом $e_1, \ldots, e_n$, то очевидно, что любая эрмитова форма φ на пространстве X полностью характеризуется матрицей $(\varphi(e_i, e_k))$ с единственным ограничением

$$\varphi(e_k, e_i) = \varphi(e_i, e_k)^J$$

Форма φ является эрмитовым внутренним произведением тогда и только тогда, когда матрица $(\varphi(e_i, e_j))$ обратима.

Предположим теперь, что кольцо R коммутативно. Тогда множество неподвижных точек

$$R_0 = \{\alpha \in R \mid \alpha^J = \alpha\}$$

образует подкольцо кольца R. Определитель матрицы $(\varphi(e_i, e_j))$, очевидно, является элементом подкольца R_0. Если перейти к новому базису $e'_1, \ldots, e'_n$ в модуле X, то определитель умножится на некоторый элемент из образа гомоморфизма

$$\text{norm}\colon R^* \to R_0^*,$$

где $\text{norm}(\alpha) = \alpha\alpha^J$.

Определение. Смежный класс (мультипликативный) элемента $\det(\varphi(e_i, e_j))$ по подгруппе $\text{norm}(R^*)$ называется *определителем* эрмитова пространства X. Этот определитель является удивительно мощным инвариантом (см. приводимые ниже примеры 2 и 3).

В коммутативном случае каждой эрмитовой форме над кольцом R сопоставляется квадратичная форма

$$Q(x) = \varphi(x, x)$$

над кольцом R_0. В частности, функция Q принимает значения в кольце R_0 и ассоциированная с ней форма

$$(x \mid y) = Q(x+y) - Q(x) - Q(y) = \varphi(x, y) + \varphi(y, x)$$

билинейна над кольцом R_0.

Предположим теперь, что F – поле с нетривиальной инволюцией. Из теории Галуа следует, что поле F является квадратичным расширением Галуа поля F_0 неподвижных элементов.

Теорема Джекобсона. *Два эрмитовых пространства с внутренним произведением над полем F изоморфны тогда и только тогда, когда соответствующие им квадратичные пространства изоморфны над полем F_0.*

Другими словами, пространство X изоморфно пространству Y как эрмитово пространство над полем F в том случае, если существует F_0-линейное отображение из X в Y, сохраняющее квадратичную функцию $Q(x) = \varphi(x, x)$. Таким образом, классификация эрмитовых пространств с внутренним произведением над полем F сводится к классификации квадратичных пространств с внутренним произведением над полем F_0.

Доказательство проведем индукцией по рангу. Отметим сначала, что поле F содержит такой элемент α_0, что $\alpha_0 + \alpha_0^J \neq 0$. В случае поля характеристики 2 в качестве элемента α_0 можно взять любой элемент из дополнения к подкольцу F_0; в случае характеристики, отличной от 2, можно положить $\alpha_0 = 1$.

Далее, отметим, что для любого эрмитова пространства с внутренним произведением X над полем F ассоциированная билинейная форма

$$(x \mid y) = \varphi(x, y) + \varphi(y, x)$$

является внутренним произведением над полем F_0. Действительно, если дан элемент $x \neq 0$, то, конечно, можно выбрать такой элемент x', что $\varphi(x, x') \neq 0$. После домножения элемента x' на подходящий элемент поля, можно считать, что $\varphi(x, x') = \alpha_0$ и, следовательно,

$$(x \mid x') = \alpha_0 + \alpha_0^J \neq 0.$$

Предположим теперь, что эрмитовы пространства с внутренним произведением X и Y изоморфны как F_0-квадратичные пространства. Поскольку ассоциированная билинейная форма $(x \mid x')$ не равна тождественно нулю, конечно, можно выбрать вектор $x \in X'$ и соответствующий ему вектор $y \in Y$, для которых $Q(x) = Q(y) \neq 0$.

Поскольку $\varphi(x, x) \neq 0$, то так же, как и в § 3 гл. 1, выводим, что эрмитово пространство X изоморфно ортогональной сумме $(Fx) \oplus (Fx)^{\perp}$. Аналогично, пространство Y изморфио $(Fy) \oplus (Fy)^{\perp}$. Но очевидно, что $(Fx) \cong (Fy)$.

Перейдем теперь к соответствующим квадратичным пространствам над полем F_0 и применим теорему Витта о сокращении (см. § 4 гл. 1 и приложение 1). Получим, что пространство $(Fx)^{\perp}$ изоморфио как квадратичное пространство пространству $(Fy)^{\perp}$. Используя индуктивное предположение, получаем, что $(Fx)^{\perp} \cong (Fy)^{\perp}$ как эрмитовы пространства и, следовательно, $X \cong Y$. □

Следствие. *Для полей $F \supset F_0$, рассмотренных выше, последовательность $W(F_0)$-модулей*

$$0 \to W(F, J) \to WQ(F_0) \to WQ(F)$$

точна.

Доказательство. Если задан ненулевой элемент в группе $W(F, J)$, то, очевидно, среди представляющих его эрмитовых пространств можно выбрать анизотропное пространство X:

$$\varphi(x, x) \neq 0 \quad \text{при} \quad x \neq 0.$$

Тогда соответствующее ему квадратичное пространство также анизотропно и, следовательно, представляет ненулевой элемент в $WQ(F_0)$. Таким образом, естественный гомоморфизм $W(F, J) \to WQ(F_0)$ инъективен.

Рассмотрим затем композицию $W(F, J) \to WQ(F_0) \to WQ(F)$. Выберем базис $\{1, \alpha\}$ в пространстве F над полем F_0. Сначала рассмотрим эрмитово пространство X размерности 1 над полем F. Оно имеет базисный вектор e_1, такой, что $\varphi(e_1, e_1) \in F_0^*$. Следовательно, пространство X двумерно над полем F_0, имеет базис $\{e_1, e_2\}$, где $e_2 = \alpha e_1$, и

$$Q(e_2) = \alpha\alpha^J Q(e_1), \qquad (e_1 \mid e_2) = (\alpha + \alpha^J) Q(e_1).$$

(Было бы удобно выбрать элемент α таким, что $\alpha + \alpha^J = 1$ в случае характеристики 2 или $\alpha + \alpha^J = 0$ в противном случае, но это не обязательно.)

Перейдем теперь к индуцированному квадратичному пространству $F \otimes_{F_0} X$ размерности 2 над полем F. Рассмотрим в этом пространстве ненулевой вектор $\alpha \otimes e_1 - 1 \otimes e_2$. Очевидно, что

$$Q(\alpha \otimes e_1 - 1 \otimes e_2) = \alpha^2 Q(e_1) + Q(e_2) - \alpha(e_1 \mid e_2) =$$
$$= (\alpha^2 + \alpha\alpha^J - \alpha(\alpha + \alpha^J)) Q(e_1) = 0.$$

Следовательно, индуцированное квадратичное пространство расщепляемо. Поскольку ясно, что любое эрмитово пространство с внутренним произведением является ортогональной суммой одномерных пространств, то этим доказано, что композиция отображений $W(F, J) \to WQ(F_0) \to WQ(F)$ равна нулю.

Обратно, пусть Y — квадратичное пространство над полем F_0, отображающееся в нулевой элемент группы $WQ(F)$. Исключив расщепляемое ортогональное слагаемое, можно считать, что пространство Y анизотропно. Поскольку пространство $F \otimes_{F_0} Y$ расщепляемо, оно, конечно, содержит такой вектор $y \neq 0$, что $Q(y) = 0$. Полагая

$$y = \alpha \otimes y_1 - 1 \otimes y_2,$$

где $y_1, y_2 \in Y$, получаем, что

$$Q(y) = \alpha^2 Q(y_1) + Q(y_2) - \alpha(y_1 \mid y_2) = 0.$$

Подставляя

$$\alpha^2 = \alpha(\alpha + \alpha^J) - \alpha\alpha^J$$

и вспоминая, что элементы 1 и α линейно независимы над полем F_0, получаем, что

$$(y_1 \mid y_2) = (\alpha + \alpha^J) Q(y_1),$$

$$Q(y_2) = \alpha\alpha^J Q(y_1),$$

где $Q(y_1) \neq 0$, поскольку пространство Y анизотропно. Это доказывает, что подпространство пространства Y, порожденное элементами y_1 и y_2, изоморфно квадратичному пространству, соответствующему эрмитову пространству над полем F, порожденному вектором y_1, для которого $\varphi(y_1, y_1) = Q(y_1)$, причем вектор αy_1 соответствует вектору y_2.

Представим теперь пространство Y в виде ортогональной суммы $(F_0 y_1 \oplus F_0 y_2) \oplus (F_0 y_1 \oplus F_0 y_2)^{\perp}$. Второе слагаемое имеет меньший ранг, так же анизотропно и так же представляет элемент из ядра. Индукция по рангу завершает доказательство. □

Разберем более подробно ряд примеров (см. [56]). *В каждом из них мы предполагаем, что инволюция J отлична от тождественной.*

Пример 1. Если F – конечное поле, то эрмитово пространство с внутренним произведением расщепляемо тогда и только тогда, когда оно имеет четный ранг. Ранг является полным инвариантом, и $W(F, J) \cong \mathbf{Z}/2\mathbf{Z}$.

Отметим, что это описание не зависит от того, равна ли характеристика 2 или нет. Доказательство оставляется читателю.

Пример 2. Если F – локальное поле или поле функций от одной переменной над конечным полем, то ранг и определитель эрмитова пространства с внутренним произведением образуют полную систему инвариантов. Ядро гомоморфизма $W(F, J) \to \mathbf{Z}/2\mathbf{Z}$, индуцированного рангом, является идеалом, который аддитивно изоморфен группе $F_0^{\cdot}/\mathrm{norm}\, F_0^{\cdot}$ и квадрат которого равен 0.

Случай характеристики 2 в этом примере опять ничем не отличается от остальных случаев. Доказательство можно наметить следующим образом. Достаточно заметить, что для любого пространства X, ранг которого над полем F не меньше 2, его ранг над полем F_0 не меньше 4, и, следовательно квадратичное уравнение $Q(e_1) = 1$ имеет в нем решение. (В глобальном случае используется теорема Хассе – Минковского; сравните с § 3 гл. 2. Случай характеристики 2 см. в [5].) Следовательно, пространство X изо-

морфно ортогональной сумме $(Fe_1) \oplus (Fe_1)^{\perp}$. Продолжая по индукции, находим ортогональный базис $e_1, \ldots, e_n$, для которого $\varphi(e_i, e_i) = Q(e_i) = 1$ при $i < n$. Следовательно, определитель $\varphi(e_n, e_n)$ однозначно определяет строение пространства X.

Пример 3. Если F – поле С комплексных чисел с комплексным сопряжением в качестве инволюции, то очевидно, что ранг и сигнатура квадратичного пространства образуют полную систему инвариантов. Следовательно, W(С, сопряжение) $\cong \mathbf{Z}$.

Пример 4. Если F – алгебраическое расширение поля рациональных чисел, то любое сохраняющее сопряжение вложение $\omega: F \to$ $\to$С порождает гомоморфизм сигнатуры

$$\omega_*: W(F, J) \to W(\mathrm{C}, \text{сопряжение}) \cong \mathbf{Z}.$$

Ранг, определитель и этот набор сигнатур образуют полную систему инвариантов эрмитова пространства с внутренним произведением над полем F. За подробностями читатель отсылается к [43].

Завершая параграф, отметим, что теорема Джекобсона применима также и в некоторых некоммутативных ситуациях. Однако для того, чтобы утверждение имело смысл, нужно предположить, что множество R_0 неподвижных точек инволюции J является подкольцом, содержащимся в центре кольца R. Именно так обстоит дело в том случае, когда R является *алгеброй кватернионов* с базисом $1, i, j$ и $ij = -ji$ над кольцом R_0, где элементы i^2 и j^2 лежат в $R_0^{\cdot}$. Кольцо R_0 здесь должно было бы быть полем, характеристика которого отлична от 2. Инволюция определяется равенствами $i^J = -i$, $j^J = -j$. Отметим, что норма $\xi\xi^J$ элемента $\xi = \alpha + \beta i + \gamma j + \delta ij$ равна $\alpha^2 - \beta^2 i^2 - \gamma^2 j^2 + \delta^2 i^2 j^2$. Если $\xi\xi^J \neq 0$ при $\xi \neq 0$, или, другими словами, если ассоциированное пространство с внутренним произведением

$$\langle 1 \rangle \oplus \langle -i^2 \rangle \oplus \langle -j^2 \rangle \oplus \langle i^2 j^2 \rangle$$

над кольцом R_0 анизотропно, то очевидно, что R – тело. В этом случае, применимы рассуждения теоремы Джекобсона. Имеется каноническое вложение

$$0 \to W(R, J) \to WQ(R_0),$$

и два эрмитовых пространства с внутренним произведением изоморфны тогда и только тогда, когда соответствующие им квадратичные пространства изоморфны над полем R_0.

Джекобсон также заметил, что "определитель" эрмитова пространства может быть определен и в неабелевом случае как элемент факторгруппы $R_0^{\cdot}/\mathrm{norm}(R^{\cdot})$. Определение основано на работе Мура (см. [20]).

Приложение 3

ТЕОРЕМА ХАССЕ – МИНКОВСКОГО

Теорема Хассе – Минковского является одним из красивейших результатов в алгебраической теории чисел. Приводимое ниже доказательство предполагает некоторое знакомство с теорией полей классов (например, по [44] или [1]). В случае поля рациональных чисел можно дать более элементарное доказательство (см. [66] или [9]). Полное и замкнутое в себе доказательство общего случая содержится в [61].

Сначала дадим некоторые определения. Пусть X – пространство с внутренним произведением над полем F. Тогда говорят, что пространство X *представляет* элемент α поля, если существует ненулевой вектор $x \in X$, для которого $x \cdot x = \alpha$.

Далее, мы предполагаем, что характеристика поля F не равна 2.

Л е м м а 1. *Если пространство X над полем F представляет* 0, *то оно представляет любой элемент поля F.*

Действительно, если пространство X представляет 0, то оно допускает выделение прямым слагаемым гиперболической плоскости (§ 6 гл. 1), которая, очевидно, представляет все элементы поля. □

С л е д с т в и е. *Пространство X представляет элемент $\alpha \neq 0$ тогда и только тогда, когда ортогональная сумма $X \oplus \langle -\alpha \rangle$ представляет* 0.

(Другими словами, неоднородное уравнение от n переменных может быть представлено как однородное уравнение от $n + 1$ переменной.) Доказательство очевидно. □

Предположим теперь, что F – *глобальное поле*. Это означает, что поле F является либо конечным расширением поля рациональных чисел, либо конечно порожденным расширением конечного поля, степень трансцедентности которого равна 1.

Мы продолжаем предполагать, что характеристика поля F не равна 2.

Пусть для любого (нетривиального) нормирования v поля F через F_v обозначается пополнение, а через $X_v = F_v \otimes X$ – индуцированное пространство с внутренним произведением над полем F_v. Пусть α – некоторый фиксированный элемент поля F.

Теорема Хассе – Минковского. *Пространство с внутренним произведением X представляет элемент α тогда и только тогда, когда для каждого (нетривиального) нормирования v поля F пространство X_v представляет элемент α.*

Отметим, что здесь должны учитываться как архимедовы, так и неархимедовы нормирования.

Доказательство этой теоремы будет удобно разбить на две части, соответствующие случаям нулевого и ненулевого элемента α.

Утверждение A_n. *Пусть $\alpha \in F^*$. Пространство X ранга n над полем F представляет элемент α тогда и только тогда, когда пространство X_v представляет элемент α для каждого нормирования v.*

В силу следствия леммы 1 это утверждение полностью эквивалентно следующему высказыванию.

Утверждение A'_n. *Пространство Y ранга $n+1$ над полем F представляет 0 тогда и только тогда, когда для каждого нормирования v пополнение Y_v представляет 0.*

Отметим сдвиг размерности с n на $n+1$ в утверждении A'_n.

Для доказательства справедливости этих двух утверждений будем переходить от одной формы утверждения к другой, доказывая сначала A_2, а затем показывая, что

$$A'_2 \Rightarrow A_3 \Rightarrow A'_n$$

при $n \geqslant 4$. Доказательство утверждения A_1 будет дано позже, поскольку оно совершенно не зависит от остальных рассуждений.

Доказательство утверждения A_2. Предположим, что $X \cong \langle u_1 \rangle \oplus \langle u_2 \rangle$. Попытаемся решить уравнение

$$u_1\xi^2 + u_2\eta^2 = \alpha$$

при $\alpha \neq 0$. Полагая $u = -u_2/u_1$ и $\beta = \alpha/u_1$, это можно записать в виде

$$(1) \quad \xi^2 - u\eta^2 = \beta.$$

Пусть через K обозначено расширение $F(\sqrt{u}) = F(\sqrt{-u_2/u_1})$. Уравнение (1) обладает решением $\xi, \eta \in F$ тогда и только тогда, когда элемент β принадлежит образу гомоморфизма нормы

$$\mathrm{norm}_{K/F}\colon K^* \to F^*.$$

При $K \neq F$ это ясно, поскольку $\mathrm{norm}(\xi + \eta\sqrt{u}) = \xi^2 - \eta^2 u$. При $K = F$ это верно потому, что $u_2 \in -u_1F^{*2}$. Поэтому пространство с внутренним произведением X расщепляется и уравнение (1) всегда имеет решение.

Теперь напомним следующее утверждение.

Теорема Хассе о норме. *Пусть K – циклическое расширение Галуа глобального поля F. Элемент $\alpha \in F^*$ принадлежит образу гомоморфизма* $\mathrm{norm} = \mathrm{norm}_{K|F}\colon K^* \to F^*$ *тогда и только тогда, когда для любого нормирования w поля K элемент α принадлежит образу гомоморфизма*

$$\mathrm{norm}\colon K_w^* \to F_{w|F}^*.$$

Эта теорема доказывается, например, в [44, с. 195] и в [1, с. 282].

Если уравнение (1) имеет решение в F_v для каждого нормирования v, то элемент β является нормой элемента из K_w^* для каждого нормирования w. Следовательно, в силу теоремы Хассе о норме, элемент β является нормой элемента поля K. Этим завершается доказательство утверждения A_2.

Для доказательства утверждения A_3 понадобится следующее утверждение.

Лемма 2. *Пусть X – пространство с внутренним произведением ранга 3 и определителем d над полем K, характеристика которого отлична от 2. Любому элементу α из поля сопоставим расширение $K = F(\sqrt{-\alpha d})$. Тогда для представления элемента α пространством X необходимо и достаточно, чтобы индуцированное пространство с внутренним произведением $K \otimes_F X$ над полем K представляло* 0.

Доказательство. Если пространство X представляет элемент α, то $X \cong \langle \alpha \rangle \oplus \langle \beta \rangle \oplus \langle \gamma \rangle$ для некоторых элементов β, γ, таких, что

$$d \in \alpha\beta\gamma F^{*2}.$$

Мы видим, что в расширении $K = F(\sqrt{-\alpha d}) = F(\sqrt{-\beta\gamma})$ элемент γ равен элементу $-\beta$, умноженному на квадрат. Следовательно, пространство $K \otimes (\langle \beta \rangle \oplus \langle \gamma \rangle)$ расщепляемо и, значит, пространство $K \otimes X$ представляет 0.

Обратно, предположим, что пространство $K \otimes X$ представляет 0. Можно предположить, что поле K является собственным расширением поля F, поскольку если $K = F$, то пространство X само представляет 0, и, следовательно, оно представляет элемент α. Таким образом, существуют два вектора $x, y \in X$, не равные нулю одновременно и для которых

$$(x + \sqrt{-\alpha d}\,y) \cdot (x + \sqrt{-\alpha d}\,y) = 0.$$

Другими словами,

$$x \cdot x - \alpha d y \cdot y = 0, \qquad x \cdot y = 0.$$

Можно предполагать, что внутреннее произведение $x \cdot x = \alpha d y \cdot y$ не равно 0, поскольку в противном случае пространство X пред-

ставляло бы 0. Следовательно, ортогональные векторы x и y образуют часть ортогоиального базиса $x, y, z,$ для которого

$$X \cong \langle x \cdot x \rangle \oplus \langle y \cdot y \rangle \oplus \langle z \cdot z \rangle$$

и

$$d \in (x \cdot x)(y \cdot y)(z \cdot z) F^{\cdot 2}.$$

Подставляя $x \cdot x = \alpha d y \cdot y$, видим, что $z \cdot z$ равно элементу α, умноженному на элемент из группы $F^{\cdot 2}$. Это доказывает лемму 2. □

Доказательство импликации $A_2' \Rightarrow A_3$. Зафиксируем пространство X ранга 3 и элемент $\alpha \neq 0$ из поля F. Положим, как и в лемме, $K = F(\sqrt{-\alpha d})$. Для каждого нормирования w поля K очевидно, что

$$K_w = F_v(\sqrt{-\alpha d}),$$

где $v = w|F$. Таким образом, если для любого нормирования v пространство X_v представляет элемент α, то пространство $(K \otimes X)_w$ представляет 0 для любого номирования w. Используя уже доказанное утверждение A_2', получаем, что пространство $K \otimes X$ представляет 0. Следовательно, пространство X представляет элемент α.

Доказательство импликации $A_3 \Rightarrow A_n'$ при $n \geqslant 4$. Пусть X – пространство ранга $n+1 \geqslant 5$. Тогда X изоморфно сумме $Y \oplus Z$, где пространство $Z \cong \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \langle u_3 \rangle$ имеет ранг 3, а ранг пространства $Y \cong \langle u_1' \rangle \oplus \ldots \oplus \langle u_{n-2}' \rangle$ больше или равен 2.

Через $T = T(u_1, u_2, u_3)$ обозначим конечное множество, состоящее из всех (классов эквивалентности) нормирований v, для которых выполнено одно из следующих утверждений:

1) нормирование v архимедово или диадическое;

2) $|u_1|_v \neq 1$, или $|u_2|_v \neq 1$, или $|u_3|_v \neq 1$.

Как и в п. 3.4 гл. 2, видим, что при $v \in T$ пополненное пространство Z_v обязательно представляет 0.

Предположим теперь, что пространство X_v представляет 0. Тогда, конечно, можно выбрать векторы $y_v \in Y_v$ и $z_v \in Z_v$, не равные одновременно нулю и такие, что $y_v \cdot y_v + z_v \cdot z_v = 0$. *В действительности эти векторы можно выбрать таким образом, что*

$$y_v \cdot y_v = -z_v \cdot z_v \neq 0.$$

Действительно, если при нашем первом выборе векторы y_v и z_v дают $y_v \cdot y_v = z_v \cdot z_v = 0$, то либо пространство Y представляет 0 (и в этом случае можно выбрать произвольный элемент z_v', для которого $z_v' \cdot z_v' \neq 0$, и применить лемму 1), либо пространство Z представляет 0 (и в этом случае годится любой элемент y_v', для которого $y_v' \cdot y_v' \neq 0$).

Нам также придется использовать следующее утверждение.

Слабая теорема об аппроксимации. *Если дано конечное число неэквивалентных нормирований $v_1, \ldots, v_t$ поля F, то образ диагонального вложения*

$$F \to F_{v_1} \times \ldots \times F_{v_t}$$

всюду плотен.

Доказательство теоремы содержится, например, в [45, с. 324].

Рассмотрим теперь $(n-2)$-мерное векторное пространство Y над полем F и множество $T = \{v_1, \ldots, v_t\}$. Применяя теорему об аппроксимации к каждой из $n-2$ координат, видим, что образ диагонального вложения $Y \to Y_{v_1} \times \ldots \times Y_{v_t}$ плотен. В частности, можно выбрать элемент $y \in Y$, который настолько близок к элементу y_v в каждом нормировании $v \in T$, что отношение $(y \cdot y)/(y_v \cdot y_v)$ является квадратом в F_v^*.

Применим к пространству Z утверждение A_3. Для каждого нормирования $v \in T$ пополнение Z_v представляет элемент $-y_v \cdot y_v$ и, следовательно, представляет элемент $-y \cdot y$. В силу утверждения A_3 получаем, что пространство Z само представляет элемент $-y \cdot y$ и, следовательно, пространство $X = Y \oplus Z$ представляет 0. Этим завершается доказательство утверждений A_n и A_n' при $n \geqslant 2$.

Для окончания доказательства теоремы Хассе – Минковского нужно доказать утверждение A_1. Для данного пространства $X \cong \cong \langle u \rangle$ и данного элемента $\alpha \neq 0$ поля F необходимо решить уравнение

$$u\xi^2 = \alpha.$$

Положив $\alpha/u = \beta$, его можно переписать в виде $\xi^2 = \beta$. Таким образом, нужно доказать следующее утверждение.

Теорема о квадратах. *Если элемент $\beta \in F^*$ для любого нормирования v является квадратом в поле F_v, то элемент β является квадратом в поле F.*

Эта теорема легко выводится из основных неравенств глобальной теории полей классов. Напомним, что *группой иделей* A_F^* называется группа обратимых элементов кольца $A_F \subset \prod_v F_v$, состоящего из всех элементов (a_v) декартова произведения, удовлетворяющих условию $|a_v|_v \leqslant 1$ для почти всех нормирований v. (При образовании этого декартова произведения, конечно, выбрано ровно по одному нормированию v в каждом нетривиальном классе эквивалентных нормирований.) Факторгруппа A_F^*/F^* называется *группой классов иделей* C_F. Для любого конечного расширения $K \supset F$ локальные гомоморфизмы нормы $K_w^* \to F_{w|F}^*$ порождают

глобальные гомоморфизмы нормы $A_K^{\cdot} \to A_F^{\cdot}$ и $C_K \to C_F$. Если K · циклическое расширение степени m поля F, то неравенства из теории полей классов утверждают, что *индекс подгруппы* $\operatorname{norm}_{K|F} C_K \subset C_F$ *равен* m. (см., [44, с. 192] или [1, с. 275].)

Доказательство теоремы о квадратах. Пусть $\beta \in F^{\cdot}$. Положим $K = F(\sqrt{\beta})$. Если для любого нормирования v элемент β является квадратом в поле F_v, то $K_w = F_{w|F}$ для любого нормирования w поля K. Поэтому гомоморфизм нормы $A_K^{\cdot} \to A_F^{\cdot}$ сюръективен. Следовательно, сюръективен гомоморфизм нормы $C_K \to C_F$, а степень m должна равняться 1. Таким образом, $\sqrt{\beta} \in F$, что завершает доказательство теоремы о квадратах и теоремы Хассе – Минковского. □

Рассмотрим теперь более общую ситуацию. Пусть X и Y – пространства с внутренним произведением над полем F, причем $\operatorname{rk}(X) \geqslant \operatorname{rk}(Y)$.

Определение. Пространство X *представляет* пространство Y, если $X \cong Y \oplus Z$ для некоторого пространства Z.

Если ранг пространства Y равен 1, скажем $Y \cong \langle u \rangle$, то очевидно, что пространство X представляет пространство Y тогда и только тогда, когда пространство X представляет элемент u.

Следствие 1. *Пусть F – глобальное поле. Если для любого нормирования v пополнение X_v представляет Y_v, то пространство X представляет пространство Y.*

Доказательство. Это, конечно, верно в том случае, когда ранг пространства Y равен 1. Если ранг пространства Y больше 1, то, полагая $Y = Y \oplus \langle u \rangle$, можем по индукции считать, что пространство X представляет пространство Y', скажем

$$X \cong Y' \oplus Z'. \tag{2}$$

По нашему предположению, для каждого нормирования v существует пространство $Z(v)$ над полем F_v, для которого

$$X_v \cong Y_v \oplus Z(v) \cong$$
$$\cong Y_v' \oplus \langle u \rangle_v \oplus Z(v).$$

Сравнивая этот изоморфизм с пополнением изоморфизма (2) и применяя теорему Витта о сокращении, получаем

$$Z_v' \cong \langle u \rangle_v \oplus Z(v).$$

Таким образом, для любого нормирования v пространство Z_v' представляет элемент u. По теореме Хассе – Минковского из этого следует, что пространство Z' представляет элемент u, скажем

$$Z' \cong \langle u \rangle \oplus Z''.$$

Вместе с изоморфизмом (2) это завершает доказательство следствия. □

Следствие 2. *Пространства X и Y над полем F изоморфны тогда и только тогда, когда для любого нормирования v пространство X_v изоморфно пространству Y_v. В частности, пространство X расщепляемо тогда и только тогда, когда для любого нормирования v расщепляемо пространство X_v.*

Доказательство. Используя лемму 6.3 гл. 1, видим, что наше утверждение является частным случаем следствия 1 при $\mathrm{rk}(X) = \mathrm{rk}(Y)$. □

Далее приводится еще одна формулировка теоремы Хассе – Минковского.

Следствие 3. *Рассмотрим квадратичное уравнение $\Sigma\alpha_{ij}\xi_i\xi_j + \Sigma\beta_k\xi_k + \gamma = 0$ от n переменных с коэффициентами из глобального поля F. Если для любого нормирования v это уравнение имеет решение в поле F_v, то оно имеет решение и в поле F.*

Отметим, что соответствующее утверждение для уравнений более высокой степени или для систем квадратичных уравнений уже было бы неверным. Приведем простейший пример. Уравнение шестой степени

$$(\xi^2 + 1)(\xi^2 + 17)(\xi^2 - 17) = 0$$

имеет решение в поле $\mathbf{Q}_v$ при любом нормировании v, но оно не имеет рациональных решений. Аналогично, рассмотрим систему квадратичных уравнений

$$\xi^2 + \eta = 0,$$
$$(\eta - \zeta)(\eta - \zeta + 16) = 0,$$
$$\zeta^2 = 17^2$$

Для любого решения (ξ, η, ζ) необходимо иметь $\zeta = \pm 17$, следовательно, $\eta = 1, 17, -17, -33$ и $\xi^2 + \eta = 0$. Опять же, для каждого нормирования v существует решение над полем $\mathbf{Q}_v$, но нет решений над полем $\mathbf{Q}$.

Доказательство следствия 3. Запишем данное уравнение в виде

$$(3) \qquad \alpha(x, x) + \beta(x) + \gamma = 0,$$

где α – симметрическая билинейная форма на векторном пространстве $X = F^n$, а β является элементом дуального векторного пространства $\mathrm{Hom}(X, F)$. Пусть N – ядро линейного отображения $x \mapsto \alpha(x, \ )$ из X в $\mathrm{Hom}(X, F)$. Подсчитывая размерности, видим, что точна последовательность

$$0 \to N \to X \to \mathrm{Hom}(X, F) \to \mathrm{Hom}(N, F) \to 0.$$

Если отображение $\beta \in \mathrm{Hom}(X, F)$ имеет ненулевое ограничение в пространстве $\mathrm{Hom}(N, F)$, то легко выбрать элемент $x \in N$, удовлетворяющий требуемому уравнению:

(3′) $\quad 0 + \beta(x) + \gamma = 0.$

Предположим теперь, что элемент β имеет нулевой образ в пространстве $\mathrm{Hom}(N, F)$. Тогда элемент β поднимается до элемента из пространства X, скажем

$$\beta(x) = 2\alpha(x_0, x)$$

при некотором $x \in X$. Подстановка $x = y - x_0$ приводит теперь уравнение (3) к виду

(4) $\quad \alpha(y, y) = \gamma',$

где $\gamma' = \beta(x_0) - \alpha(x_0, x_0) - \gamma$. Если $N = 0$ (т.е. X является пространством с внутренним произведением), то можно применить к уравнению (4) теорему Хассе – Минковского и получить решение. Если $N \neq 0$, то нужно просто выбрать дополнительное прямое слагаемое

$$X = N \oplus X'.$$

Тогда ограничение формы α на подпространство X является внутренним произведением. Поэтому применима теорема Хассе – Минковского, и уравнение (4) имеет решение $y \in X' \subset X$. Этим завершается доказательство следствия 3. □

Приложение 4

ГАУССОВЫ СУММЫ, СИГНАТУРА ПО МОДУЛЮ 8 И КВАДРАТИЧНАЯ ВЗАИМНОСТЬ

Пусть L – свободный $\mathbf{Z}$-модуль ранга n, снабженный $\mathbf{Z}$-значной симметрической билинейной формой $x \cdot y$ с ненулевым определителем. Через σ обозначим сигнатуру этой формы, а через d – абсолютное значение ее определителя. Представление выражения $\exp(2\pi i\sigma/8)$ в виде конечной экспоненциальной суммы было дано Браун в 1940 г. (Точнее, она показала, что

$$(2a)^{n/2}\sqrt{d}\exp(2\pi i\sigma/8) = \sum_{x \in L/aL} \exp(2\pi i x \cdot x/a),$$

где $a = 8d^3$. Из этого вытекает, что значение $\sigma \pmod 8$ определяется a^n числами $x \cdot x \pmod a$.) Обсудим близкую формулу, недавно полученную Милгрэмом (сравните с обсуждением в § 5 гл. 2).

Как и во второй главе, скажем, что пространство L имеет *тип* II, если для любого $x \in L$ выполняется сравненне

(1) $\quad x \cdot x \equiv 0 \pmod 2.$

Пусть $L^{\#}$ обозначает двойственную решетку, состоящую из всех элементов $u \in \mathbf{Q} \otimes L$, для которых $u \cdot L \subset \mathbf{Z}$. Тогда факторгруппа $L^{\#}/L$ является конечной абелевой группой порядка d. Если решетка L имеет тип II, то, полагая

$$\varphi(u) = \frac{1}{2}\, u \cdot u \pmod{\mathbf{Z}},$$

получаем хорошо известную квадратичную функцию $\varphi: L^{\#}/L \to \mathbf{Q}/\mathbf{Z}$.

Т е о р е м а (Милгрэм). *Если решетка L имеет тип* II, *то гауссова сумма*

$$\sum_{u \in L^{\#}/L} \exp(2\pi i\varphi(u))$$

определена и равна $\sqrt{d}\exp(2\pi i\sigma/8)$.

Исходное доказательство этой формулы содержало довольно тонкие рассуждения, использующие формулу суммирования Пуассона. Приводимое ниже доказательство, предложенное Кнебушем, несколько проще.

В фиксированном рациональном пространстве с внутренним произведением рассмотрим решетки L типа II. Обозначим d-кратную сумму $\sum_{L^{\#}/L} \exp(2\pi i\varphi(u)) = \sum_{L^{\#}/L} \exp(\pi i u \cdot u)$ кратко символом $G(L)$.

Лемма 1. *Если $L_1 \subset L$ – подрешетка индекса k, то* $G(L_1) = kG(L)$.

Доказательство. Очевидно, что $L_1 \subset L \subset L^{\#} \subset L_1^{\#}$, где индекс каждой решетки в следующей за ней равен k, $d(L)$ или k соответственно. Пусть $x_1, \ldots, x_{kd(L)}$ – полное множество представителей смежных классов решетки $L_1^{\#}$ по подрешетке L. Тогда гауссова сумма $G(L_1)$ может быть записана в виде

$$G(L_1) = \sum_{x_j} \sum_{u \in L/L_1} \exp(2\pi i\varphi(x_j + u)).$$

Если подставим

$$\varphi(x_j + u) \equiv \varphi(x_j) + x_j \cdot u \pmod{\mathbf{Z}},$$

то получим, что

$$G(L_1) = \sum_{x_j} \exp(2\pi i\varphi(x_j)) \sum_{u \in L/L_1} \exp(2\pi i(x_j \cdot u)).$$

Но для каждого фиксированного элемента x_j k-кратная сумма

$$(2) \qquad \sum_{u \in L/L_1} \exp(2\pi i(x_j \cdot u))$$

может быть вычислена следующим образом. Если $x_j \in L^{\#}$, то эта сумма, очевидно, равна $1 + \ldots + 1 = k$. Если же $x_j \notin L^{\#}$, то соответствие

$$u \mapsto \exp(2\pi i(x_j \cdot u))$$

определяет нетривиальный гомоморфизм из L/L_1 в $\mathbf{C}^*$, так что стандартными рассуждениями [44, с. 82] можно показать, что сумма (2) равна нулю. Следовательно, сумма $G(L_1)$ равна

$$\sum_{x_j \in L^{\#}/L} \exp(2\pi i\varphi(x_k))k = kG(L),$$

как и утверждалось в формулировке леммы. □

Очевидно, что $d(L_1) = k^2 d(L)$. Поэтому из леммы 1 следует, что $G(L)/\sqrt{d(L)} = G(L_1)/\sqrt{d(L_1)}$.

В действительности число $G(L)/\sqrt{d(L)}$ совершенно не зависит от решетки L, а зависит лишь от объемлющего рационального пространства с внутренним произведением. Это очевидно, поскольку любые две решетки L и L', порождающие одно и то же рациональ-

ное пространство, должны содержать общую подрешетку $L \cap L'$, имеющую конечный индекс в каждой из них.

В связи с вычислением инварианта $G(L)/\sqrt{d(L)}$ для пространства с внутренним произведением $\mathbf{Q} \otimes L$ напомним, что любое рациональное пространство с внутренним произведеннем изоморфно ортогональной сумме одномерных пространств и, следовательно, содержит решетку типа II, расщепляемую в ортогональную сумму одномерных решеток. Отметнм, что инвариант $G(L)/\sqrt{d(L)}$ мультипликативен относительно ортогональных сумм. Легко проверяется тождество

$$G(L_1 \oplus L_2) = G(L_1)G(L_2)$$

и аналогично ему тождество

$$d(L_1 \oplus L_2) = d(L_1)d(L_2).$$

Таким образом, для вычисления инварнанта $G(L)/\sqrt{d(L)}$ для любого рационального пространства с внутренним пронзведением достаточно вычислить его для одномерного пространства с внутренним пронзведением.

Следующее элементарное наблюдение потребуется нам для вычислений в одномерном случае.

Л е м м а 2. *Для любой константы* $c > 0$ *интеграл* $\int_0^A \exp(c\pi i s^2)ds$ *стремится при* $A \to \infty$ *к корректно определенному конечному пределу.*

Для доказательства сходимости мнимой части этого интеграла проведем замену $u = cs^2$ и проинтегрируем между последовательными целыми значениями переменной u, отметив, что получается знакопеременный ряд, в котором абсолютные величины членов монотонно стремятся к нулю. Сходимость вещественной части доказывается аналогично с использованием полуцелых значений. □

Рассмотрим теперь одномерную решетку типа II, скажем $L \cong \cong \langle 2m \rangle$. Предположим для определенности, что $m > 0$. Очевидно, что факторгруппа $L^{\#}/L$ -- циклическая группа порядка $2m$ и что сумма $G(L)$ равна $2m$-кратной сумме

$$\sum_{k=0}^{2m-1} \exp(\pi i k^2/2m).$$

Для вычисления этой суммы, следуя Дирихле и Ландау, введем ассоциированную с ней периодическую функцию f: $\mathbf{R} \to \mathbf{C}$ с периодом 1, такую, что

$$f(t) = \sum_{k=0}^{2m-1} \exp(\pi i(k+t)^2/2m)$$

при $0 \leqslant t \leqslant 1$. Таким образом, значение $f(0) = f(1)$ равно гауссовой сумме $G(L)$ (сравните с [44, с. 88]).

Поскольку функция f непрерывная и кусочно гладкая, то ее разложение в ряд Фурье всюду сходится к функции f. (См., например, книгу Титчмарша [42] или первый том Куранта и Гильберта [72][1].) Запишем ряд Фурье в виде

$$f(t) = \sum_{-\infty}^{\infty} a_n \exp(-2\pi i n t),$$

где

$$a_n = \int_0^1 f(x) \exp(2\pi i n t)\, dt.$$

Отметим, в частности, что гауссова сумма $G(L) = f(0)$ равна $\sum_{-\infty}^{\infty} a_n$.

Для вычисления коэффициента a_n сначала используем определение функции $f(t)$ и получим, что

$$a_n = \sum_{k=0}^{2m-1} \int_0^1 \exp\left(2\pi i \left(\frac{(k+t)^2}{4m} + nt\right)\right) dt.$$

Далее, выделим полный квадрат так, чтобы выполнялось сравнение

$$\frac{(k+t)^2}{4m} + nt \equiv (k + t + 2mn)^2 / 4m \pmod{\mathbf{Z}},$$

а затем сделаем подстановку $s = k + t + 2mn$. Это дает

$$a_n = \sum_{k=0}^{2m-1} \int_{k+2mn}^{k+1+2mn} \exp(2\pi i s^2 / 4m)\, ds =$$

$$= \int_{2mn}^{2m(n+1)} \exp(\pi i s^2 / 2m)\, ds.$$

Теперь, суммируя по n, получаем формулу

$$G(L) = \sum a_n = \int_{-\infty}^{\infty} \exp(\pi i s^2 / 2m)\, ds,$$

---

[1]) Кроме того, этот факт содержится почти в любом университетском учебнике по математическому анализу. – *Примеч. пер.*

где несобственный интеграл корректно определен в силу леммы 2. В действительности, подставляя $u = s/\sqrt{2m}$, получаем, что сумма $G(L) = G(\langle 2m \rangle)$ равна

$$\sqrt{2m} \int_{-\infty}^{\infty} \exp(\pi i u^2) du.$$

Таким образом, частное

$$G(\langle 2m \rangle)/\sqrt{2m} = \int_{-\infty}^{\infty} \exp(\pi i u^2) du$$

не зависит от m. Для вычисления этого интеграла найдем гауссову сумму в случае $m = 1$:

$$G(\langle 2m \rangle)/\sqrt{2m} = (1+i)/\sqrt{2} = \exp(2\pi i/8).$$

Аналогичным образом, частное $G(\langle -2m \rangle)/\sqrt{2m}$ равно комплексно сопряженному значению $\exp(-2\pi i/8)$. Таким образом, показано, что для каждой одномерной решетки L инвариант $G(L)/\sqrt{d(L)}$ равен $\exp(2\pi i\sigma/8)$. Отсюда немедленно выводится соответствующая формула для ортогональных сумм одномерных решеток и, следовательно, формула для произвольной решетки. Этим завершается доказательство теоремы Милгрэма. □

Теорема Браун может быть восстановлена из формулы Милгрэма следующим образом. Пусть L – произвольная решетка в рациональном пространстве с внутренним произведением, удовлетворяющая лишь предположению о том, что $x \cdot y \in \mathbf{Z}$ при $x, y \in L$. Как и ранее, пусть $d > 0$ (здесь d – абсолютное значение определителя формы) и $n = \mathrm{rk}(L)$.

Следствие. *Если число q является кратным числа $2d$, то*

$$\sum_{x \in L/qL} \exp(\pi i x \cdot x/q) = q^{n/2}\sqrt{d}\exp(2\pi i\sigma/8).$$

Очевидно, что приведенная в начале этого приложения формула, непосредственно следует из этой формулы при $q = a/2$.

Доказательство следствия. На решетке $L^{\#}$ рассмотрим новое пространство с внутренним произведением $qx \cdot y$. Отметим, что решетка $L^{\#}$ вместе с этим новым внутренним произведением имеет тип II, а двойственная к ней решетка равна $q^{-1}L$. Применяя теорему Милгрэма, получаем, что

$$\sum_{u \in q^{-1}L/L^{\#}} \exp(\pi i q u \cdot u) = \sqrt{q^n/d}\exp(2\pi i\sigma/8).$$

Теперь подставим $u = q^{-1}x$ и домножим обе части равенства на d. Поскольку решетка $qL^{\#}$ содержит решетку qL в качестве подгруппы индекса d, левая часть примет вид

$$d \sum_{x \in L/qL^{\#}} \exp(\pi i x \cdot x/q) = \sum_{x \in L/qL} \exp(\pi i x \cdot x/q).$$

Этим завершается доказательство. □

Кнебуш отметил тесную связь формулы Милгрэма с принадлежащим Вейлю [14] вариантом квадратичного закона взаимности. Для такой же, как и выше, решетки L через $(L^{\#}/L)_p$ обозначим p-примарную компоненту конечной абелевой группы $L^{\#}/L$. Тогда группа $L^{\#}/L$ разлагается в прямую сумму различных компонент $(L^{\#}/L)_p$ и, следовательно, гауссова сумма $G(L)$ может быть соответственно представлена в виде произведения $\Pi G((L^{\#}/L)_p)$, где почти все (т.е. все, за исключением, быть может, конечного числа) сомножители равны 1. Аналогичным образом порядок d группы $L^{\#}/L$ разлагается в произведение его p-примарных компонент d_p.

Л е м м а 3. *Частное* $\gamma_p(L) = G((L^{\#}/L)_p)/\sqrt{d_p}$ *зависит лишь от* p*-адического пополнения* $\mathbf{Q}_p \otimes L$ *пространства с внутренним произведением* $\mathbf{Q} \otimes L$. *Соответствие* $\mathbf{Q}_p \otimes L \mapsto \gamma_p(L)$ *задает гомоморфизм из конечной аддитивной группы* $W(\mathbf{Q}_p)$ *в мультипликативную группу корней из единицы в* $\mathbf{C}^*$.

Будем говорить, что γ_p является *характером* группы Витта $W(\mathbf{Q}_p)$.

Доказательство первого утверждения полностью аналогично доказательству леммы 1. Просто вместо кольца $\mathbf{Z}$ и поля $\mathbf{Q}$ используются кольцо целых p-адических чисел $\mathbf{Z}_p$ и поле p-адических чисел $\mathbf{Q}_p$. Для доказательства второго утверждения предположим, что пополнение $\mathbf{Q}_p \otimes L$ является расщепляемым пространством с внутренним произведением. Тогда это пополнение имеет в подходящем базисе матрицу внутреннего произведения $\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$ и этот базис порождает самодвойственную $\mathbf{Z}_p$-решетку. Но из существования самодвойственной решетки следует, что $\gamma_p(L) = 1$. Поскольку функция γ_p, очевидно, мультипликативна относительно ортогональных сумм, то это завершает доказательство леммы. □

Определим $\gamma_\infty(L)$ как корень из единицы $\exp(-2\pi i\sigma/8)$. Очевидно, он зависит только от вещественного пополнения $\mathbf{R} \otimes L$ пространства с внутренним произведением $\mathbf{Q} \otimes L$.

Теорема взаимности Вейля. *Для любой решетки* L *произведение* $\prod_{p \leqslant \infty} \gamma_p(\mathbf{Q} \otimes L)$ *равно* 1.

Доказательство непосредственно следует из теоремы Милгрэма. □

Посмотрим, что означает эта формула взаимности в случае ранга 1. Предположим, что решетка L порождена одним вектором l_1 и, для определенности, что $l_1 \cdot l_1 = 4m$, где m – нечетное число. Запишем это кратко: $L = \langle 4m \rangle$.

Лемма 4. *Характер* $\gamma_2\langle 4m\rangle$ *равен* $\exp(2\pi i m/8)$.

Действительно, $L^{\#}/L$ – циклическая группа порядка $|4m|$, порожденная элементом $l_1/4m$. Следовательно, 2-примарная компонента $(L^{\#}/L)_2$ – циклическая группа порядка 4, порожденная элементом $l_1/4$, где $\varphi(l_1/4) \equiv m/8 \pmod{\mathbf{Z}}$. Отсюда легко выводится, что

$$\gamma_2\langle 4m\rangle = \sum_{j=1}^{4} \exp(2\pi i j^2 m/8)/\sqrt{4} =$$

$$= \exp(2\pi i m/8). \quad \square$$

Предположим теперь, что m – нечетное простое число p.

Лемма 5. *Характер* $\gamma_p\langle 4p\rangle$ *равен* $\exp(2\pi i(1-p)/8)$.

Доказательство получается из леммы 4 решением уравнения взаимности

$$\gamma_2\langle 4p\rangle\gamma_p\langle 4p\rangle\gamma_\infty\langle 4p\rangle = 1. \quad \square$$

В более общем случае предположим, что $m = pu$, где u взаимно просто с p.

Лемма 6. *Характер* $\gamma_p\langle 4pu\rangle$ *равен* $(u/p)\gamma_p\langle 4p\rangle$.

Приведенный здесь символ Лежандра (u/p) равен либо +1, либо −1 в зависимости от того, является ли число u квадратичным вычетом по модулю p или нет.

Доказательство леммы 6. Действуя как и выше, получаем, что p-примарная компонента $(L^{\#}/L)_p$ порождена вектором l_1/p, для которого $\varphi(l_1/p) \equiv 2u/p \pmod{\mathbf{Z}}$. Следовательно,

$$\gamma_p\langle 4pu\rangle = \sum_{j=1}^{p} \exp(2\pi i(2uj^2/p)).$$

Если $(u/p) = +1$, то очевидно, что выражение uj^2 пробегает все квадратичные вычеты по модулю p, принимая дважды каждое ненулевое значение и принимая значение нуль по модулю p один раз. С другой стороны, если $(u/p) = -1$, то выражение uj^2 прини-

мает дважды значение каждого невычета, опять же принимая нулевое значение один раз. Поскольку сумма $\exp(2\pi i(2k/p))$ *по всем* классам вычетов k по модулю p равна 0, то из этого легко выводится требуемое заключение. (Сравните с [44, с. 85].) □

Пусть теперь p и q – различные нечетные простые числа. Применяя формулу взаимности

$$\gamma_2(L)\gamma_p(L)\gamma_q(L)\gamma_\infty(L) = 1$$

к решетке $L = \langle 4pq \rangle$, получаем равенство

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\exp(2\pi i(p-1)(q-1)/8) = 1.$$

Это и есть классический квадратичный закон взаимности.

Заключительное замечание. Над произвольным числовым полем имеется аналог формулы взаимности Вейля, который может быть выведен из рациональной формулы взаимности (см. [84], [34]). Он имеет вид

$$\prod_v \gamma_v(X) = 1,$$

где X является пространством с внутренним произведением над числовым полем F, а v пробегает все нормирования поля F. Функция γ_v определяется следующим образом.

Случай 1. Если v – комплексное архимедово нормирование, то $\gamma_v(X) = 1$.

Случай 2. Если v – вещественное архимедово нормирование, то

$$\gamma_v(X) = \exp(-2\pi i\sigma_v(X)/8),$$

где $\sigma_v(X)$ – ассоциированная с ним сигнатура.

Случай 3. Если $v = \mathfrak{p}$-адическое нормирование, то $\mathfrak{p}$ является простым идеалом в кольце целых чисел D и тогда $\gamma_v(X)$ определяется как отношение

$$G((L^\#/L)_\mathfrak{p})/\sqrt{|(L^\#/L)_\mathfrak{p}|}.$$

Здесь L может быть любой D-решеткой в пространстве X, удовлетворяющей условию $\frac{1}{2}l \cdot l \in D$ при $l \in L$, а через $L^\#$ обозначена двойственная решетка относительно Q-значного внутреннего произведения

$$x, y \longmapsto \operatorname{trace}_{F/Q} x \cdot y.$$

Гауссова сумма $G((L^{\#}/L)_{\mathfrak{p}})$ определяется как сумма выражений $\exp(\pi i \operatorname{trace}(u \cdot u))$ по всем $u \in (L^{\#}/L)_{\mathfrak{p}}$.

Теперь закон взаимности $\prod_{v} \gamma_v(X) = 1$ легко выводится из формулы Милгрзма, примененной к внутреннему произведению $\operatorname{trace}(x \cdot y)$ на пространстве L.

Один частный случай этого закона взаимности представляет особый интерес. Предположим, что пространство

$$X = (\langle \alpha \rangle \oplus \langle -1 \rangle) \otimes (\langle \beta \rangle \oplus \langle -1 \rangle)$$

представляет элемент из идеала $I^2(F)$ в кольце Витта. Тогда легко проверяется, что $\gamma_v(X) = \pm 1$. В случае $F_v \ncong \mathbf{C}$ Вейль и Шарлау показали, что $\gamma_v(X) = -1$ для выбранных подходящим образом α и β. Соответствие

$$\alpha, \beta \longmapsto \gamma_v((\langle \alpha \rangle - \langle 1 \rangle)(\langle \beta \rangle - \langle 1 \rangle)) = \pm 1$$

в действительности является "символом Гильберта", связанным с нормированием v. Равенство $\prod_{v} \gamma_v((\langle \alpha \rangle - \langle 1 \rangle)(\langle \beta \rangle - \langle 1 \rangle)) = 1$ является формой Гильберта квадратичного закона взаимности. (Сравните как с [61], так и с пп. 5.4–5.9 гл. 3 и с п. 4.4 гл. 4.)

Приложение 5

РЕШЕТКА ЛИЧА И ДРУГИЕ РЕШЕТКИ В РАЗМЕРНОСТИ 24

Построим теперь самодвойственную унимодулярную решетку $L \subset \mathbf{R}^{24}$, для которой $x \cdot x \geqslant 4$ при любом ненулевом $x \in L$ (сравните с § 6, 7 гл. 2).

Построение начинается со следующего комбинаторного утверждения. Пусть через $\mathbf{F}_2^{24}$ обозначено векторное пространство строк длиной 24 над полем вычетов по модулю 2.

Л е м м а. *Существует двенадцатимерное подпространство $S \subset \mathbf{F}_{24}$ со следующим свойством. Для каждого ненулевого вектора $s = (s_1, \ldots, s_{24}) \in S$ число равных единице компонент не меньше 8 и делится на 4. Кроме того, подпространство S содержит вектор $(1, \ldots, 1)$, состоящий из 24 единиц.*

Д о к а з а т е л ь с т в о. Следуя Личу, зададим пространство S как пространство строк явно указанной матрицы размера 12×24. Через A обозначим симметрическую матрицу размером 11×11 над полем $\mathbf{F}_2$, первая строка которой равна

1 1 1 0 1 1 0 1 0 0 0,

а остальные строки получаются циклической перестановкой элементов влево. Таким образом, каждая строка матрицы A содержит шесть единиц. Аккуратная проверка показывает, что:

(1) *каждая пара различных строк матрицы A имеет ровно три общих единицы* (т.е. в одних и тех же столбцах).

Через B обозначим симметрическую матрицу

$$B = \left(\begin{array}{c|ccc} 0 & 1 & 1 & \ldots\ 1 \\ \hline 1 & & & \\ 1 & & & \\ \vdots & & A & \\ 1 & & & \end{array}\right)$$

размером 12×12, получающуюся из матрицы A добавлением первой строки 0 1 1 1 1 1 1 1 1 1 1 1 и соответствующе-

го первого столбца. Используя (1), легко проверяем следующее утверждение.

(2) *Матрица B удовлетворяет равенству $B^2 = BB^t = I$. Следовательно, матрица B невырожденная и любые два ее столбца ортогональны относительно внутреннего произведения $r \cdot r' = \Sigma r_i r_i'$.*

Блочная матрица

$$C = \boxed{I}\boxed{B}$$

является теперь требуемой 12×24-матрицей ранга 12. Очевидно, что сумма всех строк матрицы C равна строке $(1, 1, \ldots, 1)$.

Отметим, что:

(3) *число единиц в каждой строке равно либо 8, либо 12. Кроме того, любые две различные строки матрицы C ортогональны.*

Для числа единиц в строке $s = (s_1, \ldots, s_{24})$ будет удобно использовать обозначение $\|s\|$. Как следствие (3) получаем следующее утверждение.

(4) *Если строка s является линейной комбинацией строк матрицы C, то $\|s\| \equiv 0 \pmod 4$.*

Это доказывается индукцией по числу входящих строк. Если строка s' получается из строки s добавлением строки r, то очевидно, что

$$\|s'\| = \|s\| + \|r\| - 2n,$$

где через n обозначено число общих единиц в строках s и r. Но, в силу (3), строки s и r ортогональны и, таким образом, число n четно. Предполагая по индукции, что число $\|s\|$ делится на 4, получаем, что число $\|s'\|$ также делится на 4.

(5) *Если строка s является ненулевой линейной комбинацией строк матрицы C, то $\|s\| \geqslant 8$.*

Доказательство. В силу (4) достаточно доказать, что $\|s\| \geqslant 5$. Предположим, что строка s является суммой k различных строк матрицы C. Случай $k = 1$ уже рассмотрен в (3). Если $k = 2$, то из (1) легко выводится, что $\|s\| = 8$. Если $k = 3$ и s является суммой первой строки матрицы C и двух других строк, то опять из (1) выводится, что $\|s\| = 8$. Если строка s является суммой трех строк матрицы C, не включающей первой строки, то очевидно, что первые тринадцать элементов строки s содержат ровно четыре единицы. Если бы все одиннадцать оставшихся элементов были нулями, то это означало бы, что сумма трех соответствующих строк матрицы A равна нулю. Следовательно, сумма остальных восьми строк матрицы также равнялась бы нулю. Тогда и сумма соответствующих восьми строк матрицы B равнялась бы нулю, что противоречит (2). Следовательно, $\|s\| \geqslant 5$.

Наконец, если $k \geqslant 4$, то первые двенадцать элементов строки s содержат не менее четырех единиц, а оставшиеся элементы содержат, в силу (2), не менее одной единицы. Поэтому опять получаем, что $\|s\| \geqslant 5$. Это доказывает утверждение (5) и завершает доказательство леммы. □

Замечание 1. Матрица C была построена весьма специальным способом. Следующее описание пространства строк S представляется немного более мотивированным. Рассмотрим поле $\mathbf{F}_{2048}$ из 2^{11} элементов. Утверждаем, что пространство S может быть отождествлено с совокупностью всех "соотношений" между корнями 23-й степени из единицы в поле $\mathbf{F}_{2048}$. Через ω обозначим корень 23-й степени из единицы, удовлетворяющий неприводимому уравнению

$$1 + \omega + \omega^5 + \omega^6 + \omega^7 + \omega^9 + \omega^{11} = 0$$

над полем $\mathbf{F}_2$, а через φ обозначим автоморфизм Фробениуса $\alpha \mapsto \alpha^2$. Тогда список

$$\varphi^{11}(\omega^{-1}), \varphi^{10}(\omega^{-1}), \ldots, \varphi^1(\omega^{-1}), 1, \varphi^1(\omega), \varphi^2(\omega), \ldots, \varphi^{11}(\omega)$$

содержит ровно один раз каждый корень 23-й степени из 1. Тогда гространство S является множеством всех строк $(s_1, \ldots, s_{24})$ с элементами из $\mathbf{F}_2$, имеющих нулевую сумму и удовлетворяющих линейному соотношению

$$s_2\varphi^{11}(\omega^{-1}) + s_3\varphi^{10}(\omega^{-1}) + \ldots + s_{12}\varphi^1(\omega^{-1}) + \\ + s_{13} + s_{14}\varphi^1(\omega) + \ldots + s_{24}\varphi^{11}(\omega) = 0.$$

Подробности опускаются.

Замечание 2. Имеется интересная простая группа, связанная с матрицей C. Группа Матье M_{24} может быть определена как группа всех перестановок столбцов матрицы C, которые преобразуют каждую строку матрицы C в линейную комбинацию ее строк. Эта группа действует 5-транзитивно и имеет порядок $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. Хотя она была описана Матье в 1861 г., ее существование было впервые достоверно установлено Виттом в 1938 г.

Теперь мы готовы построить решетку Лича. Через L_0 обозначим решетку в пространстве $\mathbf{R}^{24}$ с ортогональным базисом $b_1, \ldots, b_{24}$, для которого $b_i \cdot b_i = \frac{1}{8}$, а через L обозначим подрешетку решетки L_0, состоящую из всех линейных комбинаций $t_1 b_1 + \ldots + t_{24} b_{24}$ с целыми коэффициентами, для которых: либо

(6) *все числа* $t_1, \ldots, t_{24}$ *четные,* $t_1 + \ldots + t_{24} \equiv 0 \pmod 8$, *а строка* $\frac{1}{2}(t_1, \ldots, t_{24})$, *взятая по модулю* 2, *принадлежит векторному пространству* S *из леммы*; либо

(7) *все числа* $t_1, \ldots, t_{24}$ *нечетные,* $t_1 + \ldots + t_{24} \equiv 4 \pmod 8$, *а строка* $\frac{1}{2}(t_1, \ldots, t_{24})$, *взятая по модулю* 2, *принадлежит пространству* S.

Простые рассуждения показывают, что множество L замкнуто относительно сложения и образует подрешетку индекса 2^{36} в решетке L_0. Следовательно,

$$\det L = 4^{36} \det L_0 = 1.$$

Покажем, что норма $\frac{1}{8}(t_1^2 + \ldots + t_{24}^2)$ *элемента решетки* L *всегда является четным целым числом.* Другими словами,

$$t_1^2 + \ldots + t_{24}^2 \equiv 0 \pmod{16}.$$

Если коэффициент t_i четный, то число t_i^2 сравнимо с 0 или с 4 по модулю 16 в зависимости от того, сравним ли коэффициент t_i с 0 или с 2 по модулю 4. Но из леммы следует, что число коэффициентов t_i, сравнимых с 2 по модулю 4, делится на 4. Если коэффициент t_i нечетный, то число t_i^2 сравнимо с 1 или с 9 по модулю 16 в зависимости от того, сравним ли коэффициент t_i с ± 1 или с ± 3 по модулю 8. Таким образом,

$$\Sigma t_i^2 \equiv \alpha_1 + 9\alpha_3 + 9\alpha_5 + \alpha_7 \pmod{16},$$

где через α_j обозначено число коэффициентов t_i, сравнимых по модулю 8 с числом j. Отметим, что

$$\begin{aligned} \alpha_1 + \alpha_3 + \alpha_5 + \alpha_7 &= 24 \equiv 0 \pmod 8, \\ \alpha_1 + 3\alpha_3 + 5\alpha_5 + 7\alpha_7 &\equiv 4 \pmod 8, \\ \alpha_1 + \alpha_5 &\equiv 0 \pmod 4, \end{aligned}$$

где последние два сравнения следуют из (7) и из леммы. Складывая первые два сравнения и добавляя удвоенное третье, получаем, что

$$4\alpha_3 + 4\alpha_5 \equiv 4 \pmod 8.$$

Таким образом, число $\alpha_3 + \alpha_5$ нечетное и, следовательно, $\Sigma t_i^2 \equiv 24 + 8(\alpha_3 + \alpha_5) \equiv 0 \pmod{16}$.

Поэтому для любых $x, y \in L$

$$x \cdot y = \frac{1}{2}((x+y)\cdot(x+y) - x\cdot x - y\cdot y) \in \mathbf{Z}.$$

Итак, решетка L самодвойственная.

Отметим, что ни один из элемеитов $x \in L$ не может удовлетворять условию $x \cdot x = 2$. Действительно, если $t_1^2 + \ldots + t_{24}^2 = 16$, то, конечно, козффициенты t_i не могут быть одновременно нечетными. Но единственными представлениями числа 16 в виде суммы четных квадратов являются

$$16 = 4^2 = 2^2 + 2^2 + 2^2 + 2^2,$$

и обе зти возможности исключаются (6) и леммой. Следовательно, $x \cdot x \geqslant 4$ для каждого $x \neq 0$.

Дальнейшую информацию о решетке Лича читатель может найти в [39].

З а к л ю ч и т е л ь н о е з а м е ч а н и е. Полная классификация решеток типа II в пространстве $\mathbf{R}^{24}$ была дана в [60]. Там было показано, что существует ровно 24 таких решетки L с точностью до изоморфизма. Полным инвариантом решетки L является конечное подмножество $R(L)$, состоящее из всех векторов $x \in L$, норма $x \cdot x$ которых равна 2. Очевидно, что для любого $x_0 \in R(L)$ отражение

$$y \longmapsto y - (x_0 \cdot y)x_0$$

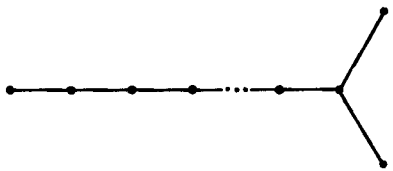
относительно гиперплоскости, перпендикулярной вектору x_0, отображает решетку L в себя, а значит, отображает и множество $R(L)$ в себя. Следовательно, множество $R(L)$ является "системой корней" (см. [12]) в некотором евклидовом пространстве. Отметим, что угол между двумя векторами из множества $R(L)$ может быть равен $0°, 60°, 90°, 120°$ или $180°$.

Используя теорему о классификации систем корней, видим, что множество $R(L)$ является дизъюнктным объединением взаимно перпендикулярных систем корней, каждая из которых может быть описана "диаграммой Дынкина" одного из следующих трех типов. В каждом случае, любая вершина диаграммы представляет базисный вектор с нормой $x \cdot x = 2$ в m-мерной решетке, а внутреннее произведение таких двух векторов равно либо -1, либо 0 в зависимости от того, соединены зти вершины отрезком или нет. Ассоциированная система корней состоит из *всех* векторов с нормой 2 из решетки L, порожденной зтими базисными векторами.

Т и п A_m $(m \geqslant 1)$. В этом случае диаграмма состоит из m вершин, соединеных $m-1$ отрезком следующим образом:

В терминах вспомогательных ортонормированных векторов $e_1, \ldots, e_{m+1}$ i-я вершина этой диаграммы может быть отождествлена с вектором разности $e_i - e_{i+1}$. Таким образом, решетка $\bar{L}$ может быть отождествлена с решеткой, состоящей из всех строк целых чисел длины $m+1$, имеющих нулевую сумму. Определитель решетки $\bar{L}$ равен $m+1$.

Т и п D_m $(m \geqslant 4)$. В этом случае m вершин соединены следующим образом:



В терминах ортогональных векторов эти вершины можно отождествить с векторами $e_i - e_{i+1}$ и $e_{m-1} + e_m$. Решетка $\bar{L}$ может быть отождествлена с решеткой, состоящей из всех строк целых чисел длины m, имеющих четную сумму. Ее определитель равен 4.

Т и п E_m $(m = 6, 7, 8)$. В этих трех исключительных случаях m вершин соединены следующим образом:

Определитель решетки $\bar{L}$ равен $9 - m$. (Сравните с обсуждением в § 7 гл. 2.)

Нимейер дал явный список 24 различных систем корней, получающихся из унимодулярных решеток типа II в пространстве $\mathbf{R}^{24}$. В общем случае система корней $R(L)$ порождает подрешетку $\bar{L}$ конечного индекса в решетке L. Единственным исключением из этого правила является решетка Лича, для которой $\bar{L} = 0$. В общем случае определитель решетки $\bar{L}$ больше 1 и, следовательно, она является собственной подрешеткой решетки L. Опять же имеется ровно одно исключение, а именно решетка $L = \bar{L} = \Gamma_8 \oplus \Gamma_8 \oplus \Gamma_8$ с системой корней $R(L)$, равной $E_8 \cup E_8 \cup E_8$. Отметим, что подрешетка $\bar{L}$ может быть (и, как правило, является) разложимой даже тогда, когда унимодулярная решетка L неразложима.

ХРОНОЛОГИЧЕСКАЯ ТАБЛИЦА

Адриен Мари Лежандр	1752 – 1833
Карл Фридрих Гаусс	1777 – 1855
Джеймс Джозеф Сильвестр	1814 – 1897
Шарль Эрмит	1822 – 1901
Фердинанд Готхольд Макс Эйзенштейн	1823 – 1852
Леопольд Кронекер	1823 – 1891
Генри Джон Стефан Смит	1826 – 1883
Александр Николаевич Коркин	1837 – 1908
Арнольд Мейер	1844 – 1896
Егор Иванович Золотарев	1847 – 1878
Герман Минковский	1864 – 1909
Карл Людвиг Зигель	1896 – 1981
Хельмут Хассе	родился в 1898 г.
Эрнст Витт	родился в 1911 г.
Альбрехт Пфистер	родился в 1934 г.

СПИСОК ЛИТЕРАТУРЫ

1. Алгебраическая теория чисел/Под ред. Дж. Касселса, А. Фрелиха. – М.: Мир, 1969.
2. *Арасон, Пфистер* (Arason J.K., Pfister A.)
Beweis des Krullschen Durchschnittsatzes für den Wittring. – Invent. Math., 1971, v. 12, p. 173–176.
3. *Артин* (Artin E.)
Algebraic numbers and algebraic functions. – Princeton University, New York University, 1950–1951.
4. *Артин* (Artin E.)
Геометрическая алгебра. – М.: Наука, 1969.
5. *Арф* (Arf C.)
Untersuchungen über quadratische Formen in Körpern der Characteristic 2. – J. reine angew. Math., 1941, Bd 183, S. 148–167; см. также: 1954, Bd 193, S. 121–125.
6. *Басс* (Bass H.)
Lectures on topics in algebraic K-theory. – Bombay: Tata Institute, 1967.
7. *Биркгоф, Маклейн* (Birkhoff G., MacLane S.)
A survey of modern algebra. – New York: MacMillan, 1941.
8. *ван дер Блий* (Blij F. van der)
An invariant of quadratic forms mod 8. – Indag. Math., 1959, v. 21, p. 291–293.
9. *Боревич З.И., Шафаревич И.Р.*
Теория чисел. – М.: Наука, 1972.
10. *Браун* (Braun H.)
Geschlechter quadratischer Formen. – J. reine angew. Math., 1940, Bd 182, S. 32–49.
11. *Бурбаки* (Bourbaki N.)
Алгебра (модули, кольца, формы). – М.: Наука, 1966.
12. *Бурбаки* (Bourbaki N.)
Группы и алгебры Ли (Группы Кокстера и системы Титса. Группы, порожденные отражениями. Системы корней). – М.: Мир, 1972.
13. *ван дер Варден* (Waerden B.L. van der)
Die Reduktionstheorie der positiven quadratischen Formen. – Acta Math., 1956, v. 96, p. 265–309.
14. *Вейль* (Weil A.)
Sur certains groupes d'operateurs unitaires. – Acta Math. 1964, v. 111, p. 143–211.
15. *Вейль* (Weil A.)
Sur la formule de Siegel dans la théorie des groupes classiques. – Acta Math., 1965, v. 113, p. 1–87.

16. *Витт* (Witt E.)
Theorie der quadratischen Formen in beliebigen Körpern. – J. reine angew. Math., 1937, Bd 176, S. 31–44.
17. *Витт* (Witt E.)
Eine Identität zwischen Modulformen zweiten Grades. – Abh. Math. Sem. Univ. Hamburg, 1941, Bd 14, S. 323–337.
18. *Гельфанд И.М., Мищенко А.С.*
Квадратичные формы над коммутативными групповыми кольцами и *K*-теория. – Функ. анализ и его прилож., 1969, т. 3, вып. 4, с. 28–33.
19. *Гильберт, Кон-Фоссен* (Hilbert D., Cohn-Vossen S.)
Наглядная геометрия. – М.: Наука, 1981.
20. *Дайсон* (Dyson F.J.)
Quaternion determinants. – Helv. Phys. Acta, 1972, v. 45, p. 289–302.
21. *Джейер, Гардер, Кнебуш, Шарлау* (Geyer W.-D., Harder G., Knebusch M., Scharlau W.)
Ein Residuensatz für symmetrische Bilinearformen. – Invent. Math., 1970, v. 11, p. 319–328.
22. *Джекобсон* (Jacobson N.)
A note on hermitian forms. – Bull. Amer. Math. Soc., 1940, v. 46, p. 264–268.
23. *Диксон* (Dickson L.E.)
History of the theory of numbers, 2 and 3. – New York: G.E. Stechart and Co., 1934.
24. *Зарисский, Самюэль* (Zariski O., Samuel P.)
Коммутативная алгебра, Т. I. – М.: ИЛ, 1963.
25. *Зигель* (Siegel C.L.)
Gesammelte Abhandlungen, I. –Berlin; Heidelberg: Springer-Verlag, 1966, S. 326–405.
26. *Картан, Эйленберг* (Cartan H., Eilenberg S.)
Гомологическая алгебра. – М.: ИЛ, 1960. – 510 с.
27. *Кнебуш* (Knebusch M.)
Grothendieck und Wittringe von nichtausgearteten symmetrichen Bilinearformen. – Sitzungsber. Heidelb. Akad. Wiss. Math.-naturw. Kl., 1969/70,3 Abh.
28. *Кнебуш* (Knebusch M.)
Runde Formen über semilokalen Ringen. – Math. Ann., 1971, Bd 193, S. 21–34.
29. *Кнебуш* (Knebusch M.)
Ein Satz über die Werte von quadratische Formen über Körpen. – Invent. Math., 1971, v. 12, p. 300–303.
30. *Кнебуш, Розенберг, Уэр* (Knebusch M., Rosenberg A., Ware R.)
Structure of Witt rings, quotients of abelian group rings, and oderings of fields. – Bull. Amer. Math. Soc., 1971, v. 77, p. 205–209.
31. *Кнебуш, Розенберг, Уэр* (Knebusch M., Rosenberg A., Ware R.)
Structure of Witt rings and quotients of Abelian group rings. – Amer. J. Math., 1972, v. 44, p. 119–155.
32. *Кнебуш, Розенберг, Уэр* (Knebusch M., Rosenberg A., Ware R.)
Grothendieck and Witt rings of hermitian forms over Dedekind rings. – Pacific J. Math., 1972, v. 43, № 3, p. 657–673.
33. *Кнебуш, Розенберг, Уэр* (Knebusch M., Rosenberg A., Ware R.)
Signatures on semilocal rings. – Bull. Amer. Math. Soc., 1972, v. 78, p. 62–64.
34. *Кнебуш, Шарлау* (Knebusch M., Scharlau W.)
Über das Verhalten der Witt-Gruppe bei Körpererweiterungen. – Math. Ann., 1971, Bd 193, S. 189–196.

35. *Кнебуш, Шарлау* (Knebusch M., Scharlau W.)
Quadratische Formen und quadratische Reziprozitätsgesetze über algebraischen Zahlkörpern. – Math. Zs., 1971, Bd 121, S. 346–368.
36. *Кнезер* (Kneser M.)
Zur Theorie der Kristallgitter. – Math. Ann., 1954, Bd 127, S. 105–106.
37. *Кнезер* (Kneser M.)
Klassenzahlen definiter quadratischer Formen. – Arch. Math., 1957, Bd 8, S. 241–250.
38. *Конвей* (Conway J.H.)
A group of order 8, 315, 553, 613, 086, 720, 000. – Bull. London Math. Soc., 1969, v. 1, p. 79–88.
39. *Конвей* (Conway J.H.)
A characterization of Leech's lattice. – Invent. Math., 1969, v. 7, p. 137–142.
40. *Конвей* (Conway J.H.)
Groups, lattices, and quadratic forms. – Computers in Algebra and Number Theory, AMS, SIAM–AMS Proceedings, 1971, v. 4, p. 13–139.
41. *Коркин А.Н., Золотарев Е.И.*
Sur les formes quadratiques positives. – Math. Ann., 1877, Bd 11, S. 242–292.
42. *Курант, Гильберт* (Courant R., Hilbert D.)
Методы математической физики. Т. I. – М.: Гостехиздат, 1951.
43. *Ландгер* (Landherr W.)
Äquivalenz Hermitescher Formen über einen beliebigen algebraischen Zahlkörper. – Abh. Math. Sem. Univ. Hamburg, 1935, Bd 11, S. 245–248.
44. *Ленг* (Lang S.)
Algebraic number theory. – Addison-Wesley, 1970.
45. *Ленг* (Lang S.)
Алгебра. – М.: Мир, 1968.
46. *Лич* (Leech J.)
Notes on sphere packings. – Can. J. Math., 1967, v. 19, p. 251–267.
47. *Лич, Слоун* (Leech J., Sloane N.J.A.)
New sphere packings in dimensions 9–15. – Bull. Amer. Math. Soc., 1970, v. 76, p. 1006–1010.
48. *Лоренц* (Lorenz F.)
Quadratische Formen über Körpern. – Berlin; Heidelberg; New York: Springer-Verlag, 1970. – (Lecture Notes in Mathematics, Bd 130).
49. *Лоренц, Лейхт* (Lorenz F., Leicht J.)
Die Primideale des Wittschen Ringes. – Invent. Math., 1970, v. 10, p. 82–88.
50. *Маккензи, Шейнеман* (MacKenzie R., Scheuneman J.)
A number field without a relative integral basis. – Amer. Math. Monthly, 1971, v. 78, p. 882.
51. *Маклейн* (MacLane S.)
Hamiltonian mechanics and geometry. – Amer. Math. Monthly, 1970, v. 77, p. 570–585.
52. *Марс* (Mars J.G.M.)
The Siegel formula for orthogonal groups. – A.M.S. Proc. of Symposia Pure Math., 1966, v. 9, p. 133–142.
53. *Масси, Столлингс* (Massey W., Stallings J.)
Алгебраическая топология. Введение. – М.: Мир, 1977.
54. *Мейер* (Meyer A.)
Über die Auflösung der $ax^2 + by^2 + cz^2 + du^2 + ev^2 = 0$ in ganzen Zahlen. – Vierteljahrs, Naturforsch, Gesells, Zürich, 1884, Bd 29, S. 220–222.
55. *Милнор* (Milnor J.)
On simply connected 4-manifolds. – In: Symposium Internacional Topologia Algebraica. – Mexico, 1958.

56. *Милнор* (Milnor J.)
On isometries of inner product spaces. – Invent. Math., 1969, v. 8, p. 83–97.
57. *Милнор* (Milnor J.)
Algebraic K-theory and quadratic forms. – Invent. Math., 1970, v. 9, p. 318–344. (Русский перевод: *Милнор Дж.* Алгебраическая K-теория и квадратичные формы. – Математика, 1971, т. 15, с. 3–27.)
58. *Милнор* (Milnor J.)
Symmetric inner products in characteristic 2. – In: Prospects in Mathematics. – Princeton: University Press, 1971. – (Annals Study, v. 70).
59. *Милнор* (Milnor J.)
Введение в алгебраическую K-теорию. – М.: Мир, 1974.
60. *Нимейер* (Niemeier H.-V.)
Definite quadratische Formen der Diskriminante 1 und Dimension 24. – J. Number Theory, 1973, v. 5, № 2, p. 142–178.
61. *О'Мира* (O'Meara O.T.)
Introduction to quadratic forms. – Berlin; Heidelberg; New York: Springer-Verlag, 1963.
62. *Пфистер* (Pfister A.)
Quadratishe Formen in beliebigen Körpern. – Invent. Math., 1966, v. 1, p. 116–132.
63. *Роджерс* (Rogers C.A.)
The packing of equal spheres. – Proc. London Math. Soc., 1958, v. 8, p. 609–620.
64. *Роджерс* (Rogers C.A.)
Packing and covering. – Cambridge: University Press, 1964.
65. *Сах* (Sah Chih-Han)
Simmetric bilinear forms and quadratic forms. – J. Algebra, 1972, v. 20, p. 144–160.
66. *Серр* (Serre J.-P.)
Курс арифметики. – М.: Мир, 1972.
67. *Спеньер* (Spanier E.)
Алгебраическая топология. – М.: Мир, 1971.
68. *Спрингер* (Springer T.A.)
Quadratic forms over fields with a discrete valuation 1. – Indag. Math., 1955, v. 17, p. 352–362.
69. *Стинрод* (Steenrod N.)
Топология косых произведений. – М.: ИЛ, 1953.
70. *Суон* (Swan R.)
Vector bundles and projective modules. – Trans. Amer. Math. Soc., 1962, v. 105, p. 264–277.
71. *Суон* (Swan R.)
Algebraic K-theory. – Berlin, Heidelberg, New York: Springer-Verlag, 1968. – (Lecture Notes in Mathematics, v. 76).
72. *Титчмарш* (Titchmarsh E.C.)
Теория функций. – М.: Наука, 1980.
73. *Уолл* (Wall C.T.C.)
Surgery on compact manifolds. – Academic Press, 1970.
74. *Уотсон* (Watson G.L.)
Integral quadratic forms. – Cambridge: University Press, 1960.
75. *Фрёлих* (Frölich A.)
Discriminants of algebraic number fields. – Math. Zs., 1960, Bd 74, S. 18–28. (см. также: Ideals in an extension fields ..., S. 29–38.)
76. *Фрёлих* (Frölich A.)
Hermitian and quadratic forms over rings with involution. – Quart. J. Math. Oxford, 1969, v. 20, p. 297–317.

77 *Фрёлих* (Frölich A.)
On the K-theory of unimodular forms over rings of algebraic integers. – Quart. J. Math. Oxford, 1971, v. 22, № 87, p. 401–423.
78. *Фрёлих, Мак-Ивет* (Frölich A., McEvett)
Forms over rings with involution. – J. Algebra, 1969, v. 12, p. 79–104.
79. *Хирцебрух* (Hirzebruch F.)
Топологические методы в алгебраической геометрии. – М.: Мир, 1973.
80. *Шарлау* (Scharlau W.)
Quadratic forms. – Kingston, Canada: Queen's University, 1969. – (Queen's papers on pure and applied math , v. 22).
81. *Шарлау* (Scharlau W.)
Zur Pfisterschen Theorie der quadratischen Formen. – Invent. Math., 1969, v. 6, p. 327–328.
82. *Шарлау* (Scharlau W.)
Induction theorems and structure of the Witt group. – Invent. Math. 1970, v. 11, p. 37–44.
83. *Шарлау* (Scharlau W.)
Hermitesche Formen über lokalen Körpern. – Math. Ann., 1970, Bd 186, S. 201–208.
84. *Шарлау* (Scharlau W.)
Quadratic reciprocity laws. – J. Number Theory, 1972, v. 4, p. 78–97.
85. *Шевалле* (Chevally C.)
The algebraic theory of spinors. – New York: Columbia University Press, 1954.

АЛФАВИТНЫЙ УКАЗАТЕЛЬ

СПИСОК ОБОЗНАЧЕНИЙ