

Алгебраическая теория квадратичных форм*

Александр Лузгарев

Содержание

1	Квадратичные формы: начало	2
1.1	Основные понятия	2
1.2	Теорема Витта о сокращении	7
1.3	Первая теорема Касселса о представимости	12
1.4	Теорема о подформе	13
1.5	Поведение квадратичных форм при конечных расширениях полей	15
2	Теория Пфистера	16
2.1	Формы Пфистера	16
2.2	Суммы квадратов и s -инвариант	19
2.3	Связанные формы Пфистера	20
2.4	Мультипликативные формы	21
3	К-теория Милнора	24
3.1	Элементарные инварианты	24
3.2	Группа Брауэра	26
3.3	Группа Брауэра–Уолла	32
3.4	Когомологии Галуа	35
3.5	Теорема Меркурьева	41
3.6	Высшие инварианты	43

*Конспект лекций спецкурса, весна 2010.

Источники:

- Albrecht Pfister, *Quadratic forms with applications to algebraic geometry and topology*, London Math. Soc. Lect. Notes 217, Cambridge University Press, 1995.
- Bruno Kahn, *Formes quadratiques sur un corps*, Societe Mathematique de France, 2009.
- конспект лекций Олега Ижболдина, 1997.
- Philippe Gille, Tamás Szamuely, *Central simple algebras and Galois cohomology*. Cambridge University Press, 2006.

Автор благодарен Алексею Степанову за исправленные неточности и доказательство следствия 1.2.4.

1 Квадратичные формы: начало

1.1 Основные понятия

1.1.1 Определение. Пусть V — n -мерное векторное пространство над полем F . Мы всегда будем предполагать, что характеристика F отлична от двух. **Симметричная билинейная форма** на V — это отображение $b: V \times V \rightarrow k$ такое, что $b(u, v) = b(v, u)$ и $b(\alpha u_1 + u_2, v) = \alpha b(u_1, v) + b(u_2, v)$. Если (e_1, \dots, e_n) — базис V , то $b(x_1 e_1 + \dots + x_n e_n, y_1 e_1 + \dots + y_n e_n) = \sum a_{ij} x_i y_j = x^t A y$, где $x = (x_1, \dots, x_n)^T \in k^n$, $y = (y_1, \dots, y_n)^T \in F^n$ — столбцы координат, $a_{ij} = b(e_i, e_j)$, $A = (a_{ij})$ — **матрица Грама**. Пусть W — подпространство V ; определим ортогонал к W :

$$W^\perp = \{u \in V : b(u, w) = 0 \text{ для всех } w \in W\}.$$

1.1.2 Лемма. $\dim W^\perp + \dim W \geq \dim V$.

Доказательство. Пусть u_1, \dots, u_m — базис W ; построим линейное отображение $\alpha: V \rightarrow k^m: v \mapsto (b(v, u_i))_{i=1}^m$. При этом $\text{Ker}(\alpha) = W^\perp$, $\dim \text{Im}(\alpha) \leq m = \dim W$, поэтому $\dim V = \dim \text{Ker}(\alpha) + \dim \text{Im}(\alpha) \leq \dim W^\perp + \dim W$. \square

Отображение $\varphi: V \rightarrow k$ называется **квадратичным отображением** или **квадратичной формой**, и пара (V, φ) называется **квадратичным пространством** над k , если φ удовлетворяет следующим условиям:

1. $\varphi(av) = a^2 \varphi(v)$ для всех $a \in k, v \in V$;
2. отображение $b_\varphi: V \times V \rightarrow k$, заданное формулой

$$b_\varphi(v, w) := \frac{1}{2}(\varphi(v + w) - \varphi(v) - \varphi(w)),$$

является k -билинейным.

При этом b_φ называется **симметричной билинейной формой**, ассоциированной с φ (из определения очевидно, что b_φ симметрична). Форма φ восстанавливается по b_φ формулой $\varphi(v) = b_\varphi(v, v)$. Пусть $B = \{e_1, \dots, e_n\}$ — базис V . Матрицей [Грама] квадратичной формы в базисе B называется матрица $A = (b_\varphi(e_i, e_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$. Легко видеть, что эта матрица симметрична. Обратно, по любой симметричной матрице из $M(n, k)$ строится квадратичная форма на k^n . Если x — столбец координат некоторого вектора $v \in V$, то значение квадратичной формы на этом векторе записывается так:

$$\varphi(v) = x^t A x.$$

Значение билинейной симметричной формы b_φ на двух векторах $v, w \in V$ с координатными столбцами x и y соответственно записывается так:

$$b_\varphi(v, w) = x^t A y = y^t A x.$$

Два n -мерных векторных квадратичных пространства (V, φ) и (V', φ') называются **изометричными**, если существует k -линейный изоморфизм $T: V \rightarrow V'$ такой, что

$$\varphi(v) = \varphi'(Tv) \text{ для всех } v \in V.$$

Обозначение: $(V, \varphi) \cong (V', \varphi')$. В большинстве случаев мы забываем про пространства, на которых определены формы, и пишем $\varphi \cong \varphi'$. Очевидно, что изометричность является отношением эквивалентности. Если в каждом из пространств V, V' выбраны базисы, их можно отождествить с k^n , и изоморфизм T превращается в автоморфизм k^n , то есть, записывается матрицей из $GL(n, k)$. При этом если A — матрица φ , A' — матрица φ' , то $x^t A y = (Tx)^t A' (Ty)$ для всех $x, y \in k^n$, откуда $A = T^t A' T$.

Определителем φ называется определитель матрицы Грама φ . Заметим, что при замене базиса определитель матрицы Грама умножается на квадрат определителя матрицы замены базиса; поэтому $\det(\varphi) \in k^*/(k^*)^2 \cup \{0\}$ — определен только с точностью до домножения на квадраты в поле k .

Пусть $(V_1, \varphi_1), (V_2, \varphi_2)$ — два квадратичных пространства над k размерностей n_1 и n_2 соответственно. По ним можно построить квадратичное пространство (V, φ) размерности $n = n_1 + n_2$:

$$\begin{aligned} V &= V_1 \oplus V_2, \\ \varphi(v) &= \varphi_1(v_1) + \varphi_2(v_2) \end{aligned}$$

для $v_1 \in V_1, v_2 \in V_2, v = v_1 + v_2 \in V$. Это пространство (V, φ) называется **прямой суммой** (V_1, φ_1) и (V_2, φ_2) . Обозначается это так: $(V, \varphi) = (V_1, \varphi_1) \oplus (V_2, \varphi_2)$ или $(V_1, \varphi_1) \perp (V_2, \varphi_2)$. Мы будем также писать $\varphi = \varphi_1 \oplus \varphi_2 = \varphi_1 \perp \varphi_2$. Если A_1 — матрица φ_1 , A_2 — матрица φ_2 в некоторых базисах B_1, B_2 пространств V_1, V_2 , то $B = B_1 \sqcup B_2$ — базис V , в котором φ имеет матрицу

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

Аналогично можно определить сумму любого натурального количества квадратичных пространств. Класс изометричности суммы зависит только от слагаемых, но не от их порядка. Обратно, пусть (V, φ) — квадратичное пространство и $\{V_i\}_{1 \leq i \leq r}$ — набор подпространств V таких, что $V = V_1 \oplus \dots \oplus V_r$ и $b_\varphi(v_i, v_j) = 0$ для всех $v_i \in V_i, v_j \in V_j, i \neq j$. Тогда $\varphi = \varphi_1 \oplus \dots \oplus \varphi_r$ для $\varphi_i = \varphi|_{V_i}$.

1.1.3 Теорема. Любое квадратичное пространство (V, φ) над k изометрично прямой сумме одномерных подпространств. Другими словами, каждая n -арная квадратичная форма φ над k эквивалентна диагональной форме ψ вида $\psi(x) = \sum_{i=1}^n a_i x_i^2$, $a_i \in k$.

Доказательство. Индукция по $n = \dim V$. Если $\varphi(v) = 0$ для всех $v \in V$, то $b_\varphi = 0$, и любой базис V является ортогональным. Если $\varphi(v_1) = a_1 \neq 0$ для некоторого $v_1 \in V$, рассмотрим подпространство

$$U = (kv_1)^\perp = \{u \in V : b_\varphi(u, v_1) = 0\}$$

всех векторов, ортогональных к v_1 (относительно b_φ). При этом по лемме 1.1.2 размерность U не меньше, чем $n - 1$, но $v_1 \notin U$, поэтому $\dim U = n - 1$, откуда $V = kv_1 \oplus U$ и $\varphi = \varphi_1 \oplus \varphi_2$ для $\varphi_1 = \varphi|_{kv_1}$, $\varphi_2 = \varphi|_{U}$. \square

Заметим, что в качестве a_1 можно взять любой элемент из k^* вида $\varphi(v_1)$ для $v_1 \in V$.

Второе доказательство. Приведем явный алгоритм. Будем действовать индукцией по n ; база $n = 1$ очевидна. Пусть теперь $n > 1$. Запишем нашу форму в координатах с помощью какого-нибудь базиса V : $\varphi(x_1, \dots, x_n) = \sum_{i,j=1}^n a_{ij} x_i x_j$. Предположим сначала, что найдется диагональный коэффициент $a_{ii} \neq 0$. После перестановки базисных векторов можно считать, что $a_{11} \neq 0$. Посмотрим на слагаемые, содержащие x_1 : $\varphi(x_1, \dots, x_n) = a_{11} x_1^2 + 2a_{12} x_1 x_2 + \dots + 2a_{1n} x_1 x_n + \varphi'(x_2, \dots, x_n)$. Выделим полный квадрат: $\varphi(x_1, \dots, x_n) = a_{11} (x_1 + \frac{a_{12}}{a_{11}} x_2 + \dots + \frac{a_{1n}}{a_{11}} x_n)^2 + \varphi''(x_2, \dots, x_n)$, и по предположению индукции форма φ'' от меньшего количества переменных приводится к диагональному виду.

Теперь предположим, что все диагональные коэффициенты равны 0, но найдется недиагональный коэффициент $a_{ij} \neq 0, i \neq j$. После перестановки базисных векторов можно считать, что $a_{12} \neq 0$ (а все a_{ii} равны 0). Сделаем замену: $x'_1 = x_1 + x_2, x'_2 = x_1 - x_2$. При этом $\varphi(x_1, \dots, x_n) = 2a_{12} x_1 x_2 + \varphi'(x_1, \dots, x_n) = \frac{1}{2} a_{12} x_1'^2 - \frac{1}{2} a_{12} x_2'^2 + \varphi''(x'_1, x'_2, x_3, \dots, x_n)$. При этом $\varphi''(x'_1, x'_2, x_3, \dots, x_n)$ не содержит мономов вида $x_1'^2$, поскольку $\varphi'(x_1, \dots, x_n)$ не содержит мономов вида $x_1 x_2, x_1^2$ и x_2^2 . Значит, в новом базисе у нашей формы появился ненулевой диагональный коэффициент, и можно выделить полный квадрат, как и выше.

Наконец, если все коэффициенты φ равны нулю, то форма нулевая и она уже записана в диагональном виде. \square

Диагональную форму $\varphi(x) = \sum_{i=1}^n a_i x_i^2$ мы будем обозначать

$$\varphi = \langle a_1, \dots, a_n \rangle = \langle a_1 \rangle \perp \dots \perp \langle a_n \rangle.$$

Пусть (V, φ) — квадратичное пространство, A — матрица формы φ . Подпространство $\text{rad } V = V^\perp = \{u \in V : b_\varphi(u, v) = 0 \text{ для всех } v \in V\}$ называется **радикалом** (V, φ) . Пространство (V, φ) называется **регулярным** или **невырожденным**, если $\text{rad } V = 0$. Как всегда, мы часто говорим о регулярности (невырожденности) *формы*, опуская упоминание о пространстве.

Нетрудно видеть, что $\text{rad } V = \{u \in V : u^t A v = 0 \text{ для всех } v \in V\} = \{u \in V : u^t A = 0\}$; поэтому $\text{rad } V = 0 \iff \det A \neq 0$; радикал и регулярность инвариантны относительно изометрии; если φ не регулярно, то $\varphi \cong \langle a_1, \dots, a_{n-1}, 0 \rangle$, то есть φ эквивалентна форме, зависящей лишь от $n - 1$ переменных. Поэтому можно предполагать, что все формы регулярны. Более точно:

1.1.4 Теорема (о выделении регулярной части). *Пусть (V, φ) — квадратичная форма. Существует разложение $(V, \varphi) = (W_0, \varphi_0) \perp (W_1, \varphi_1)$, где $\varphi_0(W_0) = 0$ для всех $w_0 \in W_0$, а (W_1, φ_1) — невырожденная форма. Более того, это разложение единственно с точностью до изометрии.*

Доказательство. Существование такого разложения следует из теоремы 1.1.3. Заметим, что в любом подобном разложении $W_0 \perp W_0$ и $W_0 \perp W_1$, откуда $W_0 \perp V$, то есть $W_0 \subset \text{rad}(V)$. Если при этом $W_0 \neq \text{rad}(V)$, то $\text{rad}(V) \cap W_1 \neq 0$, то есть в W_1 найдется вектор, ортогональный V , чего не может быть по невырожденности W_1 . Значит, $W_0 = \text{rad}(V)$. Возьмем теперь два таких разложения: $V = W_0 \oplus W_1 = W'_0 \oplus W'_1$, при этом $W_0 = W'_0 = \text{rad}(V)$. Определим отображение $T: W_1 \rightarrow W'_1$ как композицию вложения $W_1 \subset V$ и проекции V на W'_1 . По построению T линейно, при этом для $w \in W_1$ разность $Tw - w$ лежит в $W_0 = \text{rad}(V)$. Поэтому $\varphi(Tw) = \varphi(w + (Tw - w)) = \varphi(w) + 2b_\varphi(w, Tw - w) + \varphi(Tw - w)$ и два последних слагаемых равны 0. Значит, T — изометрия. Заметим также, что T можно продолжить до изометрии всего пространства, если дополнить ее тождественным отображением на W_0 . \square

Пусть φ — квадратичная форма над k , $L \supset k$ — расширение полей. Тогда φ можно рассматривать как квадратичную форму над L , которую мы будем обозначать φ_L или $\varphi \otimes L$. При этом

$$\varphi = \varphi_k \text{ регулярна} \iff \varphi_L \text{ регулярна.}$$

Пусть (V, φ) — n -мерное квадратичное пространство над k

1. Для $a \in k$ будем говорить, что φ **представляет a над k** , если существует ненулевой вектор $v \in V$ такой, что $\varphi(v) = a$.
2. $\widetilde{D}_k(\varphi) = \{\varphi(v) : 0 \neq v \in V\}$ — множество элементов k , представимых формой φ .
3. $D_k(\varphi) = \widetilde{D}_k(\varphi) \setminus \{0\} \subseteq k^*$.

4. φ называется универсальной (над k), если $D_k(\varphi) = k^*$.

5. φ называется изотропной (над k), если $0 \in \widetilde{D}_k(\varphi)$, иначе φ называется анизотропной (над k).

1.1.5 Пример. $x_1^2 + x_2^2$ не универсальна, анизотропна над \mathbb{R} , но универсальная, изотропна над \mathbb{C} .

Очевидно, что одномерное регулярное пространство не может быть изотропным. Посмотрим на двумерные.

1.1.6 Утверждение. *Есть только одна (с точностью до изометрии) регулярная изотропная квадратичная форма φ размерности 2, а именно, $\varphi(x) = 2x_1x_2$. Кроме того, $\varphi \cong \langle a, -a \rangle$ для любого $a \in k^*$. В частности, φ универсальна.*

Доказательство. Пусть φ — двумерная регулярная изотропная форма на пространстве V и $v_1 \in V$, $\varphi(v_1) = 0$. Поскольку φ регулярна, найдется $w \in V$ такой, что $b_\varphi(v_1, w) \neq 0$. Домножая w на подходящий элемент k^* , можно считать, что $b_\varphi(v_1, w) = 1$. Для любого $\lambda \in k$ векторы v_1 и $v_2 = w + \lambda v_1$ образуют базис пространства V , в котором $\varphi(v_1) = 0$ и $b_\varphi(v_1, v_2) = b_\varphi(v_1, w + \lambda v_1) = b_\varphi(v_1, w) + \lambda b_\varphi(v_1, v_1) = 1$. Наконец, $\varphi(v_2) = \varphi(w + \lambda v_1) = \varphi(w) + 2\lambda b_\varphi(w, v_1) + \lambda^2 \varphi(v_1) = \varphi(w) + 2\lambda$. Значит, если положить $\lambda = -\varphi(w)/2$, получим $\varphi(v_2) = 0$. \square

Класс изометричности этой формы обозначается $\mathbb{H} \cong \langle 1, -1 \rangle$ и называется гиперболической плоскостью. Заметим, что $\det(\langle 1, -1 \rangle) = -1$. Обратно, если (V, φ) — двумерное квадратичное пространство и $\det(\varphi) = -1$, то (V, φ) — гиперболическая плоскость.

1.1.7 Утверждение. *Пусть (V, φ) — регулярное изотропное квадратичное пространство над k , $\dim V = n \geq 2$. Тогда $V = U \oplus W$ и $U \cong \mathbb{H}$, $\dim W = n - 2$, $\varphi \cong \langle 1, -1 \rangle \oplus \psi$, где $\psi = \varphi|_W$.*

Доказательство. Как и в предыдущем предложении, можно найти $v_1, v_2 \in V$ такие, что двумерное подпространство $U = kv_1 + kv_2 \subseteq V$ вместе с квадратичной формой $\varphi|_U$ изоморфно гиперболической плоскости \mathbb{H} . Положим $W = U^\perp$, тогда $\dim W \geq n - 2$ и $U \cap U^\perp = \text{rad } U = 0$, поскольку U регулярно. Значит, $\dim W = n - 2$ и $V = U \oplus W$. \square

1.1.8 Теорема. *Для невырожденной формы φ и $a \in k^*$ равносильны:*

1. $a \in D_k(\varphi)$;
2. $\varphi \perp \langle -a \rangle$ изотропна;
3. $\varphi = \langle a \rangle \perp \varphi_1$.

Доказательство. (1) \Rightarrow (3) из замечания после доказательства теоремы 1.1.3, (3) \Rightarrow (2) из предложения 1.1.6, (2) \Rightarrow (1): если V — пространство формы φ , то изотропность $\varphi \perp \langle -a \rangle$ на пространстве $V \perp kv_1$ означает, что для некоторых $v \in V$, $\lambda \in k$, не равных одновременно 0, выполняется $\varphi(v) - a\lambda^2 = 0$. Если форма φ изотропна, то (как следует из двух предыдущих утверждений) она принимает вообще все значения, и a в том числе. Если же φ не изотропна, то $\varphi(v)$ не может равняться 0, откуда $\lambda \neq 0$. Поэтому $\varphi(v/\lambda) = a\lambda^2/\lambda^2 = a$, что и требовалось. \square

1.1.9 Лемма. Если форма $\langle a, b \rangle$ представляет элемент $c \in k^*$, то $\langle a, b \rangle \cong \langle c, abc \rangle$.

Доказательство. Из замечания после доказательства теоремы 1.1.3 ясно, что $\langle a, b \rangle \cong \langle c, d \rangle$ для некоторого $d \in k$. Из сравнения определителей видно, что $ab = cd$, поэтому $abc = c^2d$ и заменой второго базисного вектора формы $\langle c, d \rangle$ на пропорциональный можно заменить d на abc . \square

1.2 Теорема Витта о сокращении

Пусть (V, φ) — квадратичная форма; v — анизотропный вектор. Определим отражение s_v относительно вектора v формулой

$$s_v(u) = u - 2 \frac{\varphi(u, v)}{\varphi(v, v)} v.$$

Простое вычисление показывает, что отражение является изометрией.

1.2.1 Лемма. Пусть $v_1, v_2 \in V$ и $\varphi(v_1) = \varphi(v_2) \neq 0$. Тогда существует композиция отражений, переводящая v_1 в v_2 .

Доказательство. Если $\varphi(v_1 - v_2) \neq 0$, то подойдет отражение относительно $v_1 - v_2$: $s_{v_1 - v_2}(v_1) = v_2$. Если $\varphi(v_1 + v_2) \neq 0$, то подойдет композиция отражения относительно $v_1 + v_2$ ($s_{v_1 + v_2}(v_1) = -v_2$) и отражения относительно v_2 . Если же $\varphi(v_1 - v_2) = \varphi(v_1 + v_2) = 0$, то $\varphi(v_1) = \frac{1}{4}\varphi((v_1 + v_2) + (v_1 - v_2)) = \frac{1}{2}\varphi(v_1 + v_2, v_1 - v_2)$ и $\varphi(v_2) = \frac{1}{4}\varphi((v_1 + v_2) - (v_1 - v_2)) = -\frac{1}{2}\varphi(v_1 + v_2, v_1 - v_2)$, откуда $\varphi(v_1) = \varphi(v_2) = 0$, что невозможно. \square

1.2.2 Следствие. Любая изометрия невырожденного пространства есть композиция отражений.

Доказательство. Пусть $T: V \rightarrow V$ — изометрия невырожденного квадратичного пространства (V, φ) . Доказываем индукцией по $n = \dim V$; база $n = 1$ очевидна. Пусть $n > 1$. Возьмем $v \in V$ такой, что $\varphi(Tv) = \varphi(v) \neq 0$. По лемме найдется композиция отражений $S: V \rightarrow V$ такая, что $Sv = Tv$. Отображение $S^{-1}T$, таким образом, является изометрией и оставляет v на месте; значит, $S^{-1}T$ оставляет на месте и $W = (kv)^\perp$ — подпространство размерности $n - 1$. По предположению индукции изометрия $S^{-1}T|_W$ является композицией отражений (относительно векторов из W). Заметим, что любое

отражение относительно вектора из W оставляет на месте v , поскольку $v \perp W$. Значит, изометрия $S^{-1}T$ является композицией тех же самых отражений, рассматриваемых уже как преобразований всего пространства V . Перенос S в другую часть, получаем, что и T является композицией отражений. \square

1.2.3 Теорема (Витта о сокращении). *Если $q \perp \varphi_1 \cong q \perp \varphi_2$, то $\varphi_1 \cong \varphi_2$.*

Доказательство. Можно считать, что формы невырождены; $q = \langle a_1, \dots, a_n \rangle$. Докажем, что из $\langle a \rangle \perp \varphi_1 \cong \langle a \rangle \perp \varphi_2$ следует, что $\varphi_1 \cong \varphi_2$. Пусть форма $\psi_1 = \langle a \rangle \perp \varphi_1$ задана на пространстве $kv_1 \oplus W_1$, а $\psi_2 = \langle a \rangle \perp \varphi_2$ — на пространстве $kv_2 \oplus W_2$. Изометричность этих форм означает, что существует линейное отображение $T: kv_1 \oplus W_1 \rightarrow kv_2 \oplus W_2$, для которого $\psi_2(Tv) = \psi_1(v)$. Запишем $Tv_1 = xv_2 + w_2$. Тогда $\psi_2(v_2) = a$ и $\psi_2(Tv_1) = a$. По лемме найдется изометрия $S: kv_2 \oplus W_2 \rightarrow kv_2 \oplus W_2$ такая, что $Sw_2 = Tv_1$. Рассмотрим отображение $S^{-1}T: kv_1 \oplus W_1 \rightarrow kv_2 \oplus W_2$. Нетрудно видеть, что $S^{-1}T$ является изометрией между ψ_1 и ψ_2 ; кроме того, $S^{-1}Tv_1 = v_2$, поэтому $S^{-1}T$ переводит $W_1 = (kv_1)^\perp$ в $W_2 = (kv_2)^\perp$. Это означает, что ограничение $S^{-1}T$ на W_1 и дает нужную изометрию между φ_1 и φ_2 . \square

1.2.4 Следствие (Теорема о продолжении изометрии). *Пусть (V, φ) — квадратичное пространство, W_1, W_2 — подпространства в V , и пусть $\alpha: W_1 \rightarrow W_2$ — изометрия между ними такая, что $\alpha(W_1 \cap \text{rad } V) = W_2 \cap \text{rad } V$. Тогда существует изометрия $\beta: V \rightarrow V$ такая, что $\beta|_{W_1} = \alpha$.*

Доказательство. Сначала докажем теорему для случая $\text{rad } V = 0$ (то есть, форма φ невырождена на V).

В случае, когда W_1 невырождено, утверждение следует из теоремы Витта о сокращении. Действительно, в этом случае V раскладывается в прямую сумму W_i и его ортогонального дополнения ($i = 1, 2$). По теореме о сокращении существует изометрия $\gamma: W_1^\perp \rightarrow W_2^\perp$. Тогда $\beta = (\alpha, \gamma)$ — изометрия $V \rightarrow V$.

Если же W_1 — вырожденное подпространство в невырожденном пространстве V , то можно выбрать базис $u_1, \dots, u_{2m}, v_1, \dots, v_k$ пространства V , содержащий базис $u_1, u_3, \dots, u_{2s-1}, v_1, \dots, v_r$ пространства W_1 такой, что матрица формы φ в этом базисе будет иметь вид

$$\text{diag} \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \alpha_1, \dots, \alpha_k \right).$$

В этом случае нетрудно распространить изометрию на невырожденное подпространство, порожденное $u_1, \dots, u_{2s}, v_1, \dots, v_r$, а затем использовать теорему о сокращении.

Перейдем к общему случаю. Выберем подпространство \widetilde{W}_1 такое, что $W_1 = (W_1 \cap \text{rad } V) \oplus \widetilde{W}_1$, и расширим его до подпространства \widetilde{V} такого, что $V = \text{rad } V \oplus \widetilde{V}$. Тогда

$$W_2 = \alpha(W_1) = \alpha(W_1 \cap \text{rad } V) \oplus \alpha(\widetilde{W}_1) = (W_2 \cap \text{rad } V) \oplus \alpha(\widetilde{W}_1).$$

Расширим $\alpha(\widetilde{W}_1)$ до подпространства \widetilde{V}' так, что $V = \text{rad } V \oplus \widetilde{V}'$. Заметим, что теперь у нас есть два ортогональных дополнения до $\text{rad } V$: \widetilde{V} и \widetilde{V}' . По теореме о выделении

регулярной части, невырожденные подпространства \tilde{V} и \tilde{V}' изометричны. К их подпространствам $\tilde{W}_1 \leq \tilde{V}$ и $\alpha(\tilde{W}_1) \leq \tilde{V}'$ можно применить только что доказанный случай невырожденной формы и получить изометрию $\tilde{V} \rightarrow \tilde{V}'$, продолжающую $\alpha_{\tilde{W}_1}$. Далее, изометрию $\alpha|_{W_1 \cap \text{rad } V}$ между $W_1 \cap \text{rad } V$ и $\alpha(W_1 \cap \text{rad } V)$ можно продолжить до изометрии $\text{rad } V \rightarrow \text{rad } V$ произвольным линейным отображением, поскольку форма на этих подпространствах нулевая. Ортогональная прямая сумма этих двух изометрий дает нужную изометрию на V . \square

1.2.5 Следствие. Любая невырожденная форма φ представляется в виде

$$\varphi \cong \underbrace{\mathbb{H} \perp \cdots \perp \mathbb{H}}_{r \text{ раз}} \perp \varphi_{\text{ан}},$$

где анизотропная часть $\varphi_{\text{ан}}$ определена однозначно с точностью до изометрии, и индекс Витта $i(\varphi) := r$ определен однозначно.

Доказательство. По предложению 1.1.7 если форма изотропна, из нее можно выделить \mathbb{H} . Продолжая этот процесс, дойдем до какой-то анизотропной формы (потому что размерность все время убывает). Осталось проверить единственность. Предположим, что $\varphi \cong \perp \varphi_{\text{ан}}$, $\varphi \cong \underbrace{\mathbb{H} \perp \cdots \perp \mathbb{H}}_{r \text{ раз}} \perp \psi \cong \underbrace{\mathbb{H} \perp \cdots \perp \mathbb{H}}_{r' \text{ раз}} \perp \psi'$, где ψ, ψ' анизотропны. Не умаляя общности, $r \geq r'$. Если $r > r'$, то сокращая (по теореме Витта) слева и справа r' раз на \mathbb{H} , получаем, что $\underbrace{\mathbb{H} \perp \cdots \perp \mathbb{H}}_{r-r' \text{ раз}} \perp \psi \cong \psi'$, но слева стоит изотропная форма, а справа — анизотропная. Поэтому $r = r'$ и после сокращения получаем $\psi \cong \psi'$. \square

Пока что считаем все квадратичные формы невырожденными и диагональными. Обозначим $G(k) = k^*/(k^*)^2$ — **square class group**. Пусть $\varphi \cong \langle a_1, \dots, a_m \rangle$, $a_i \in k^*$; $\det \varphi = (\prod a_i)(k^*)^2 \in G(k)$ — **определитель (детерминант)** φ , $d(\varphi) = (-1)^{m(m-1)/2} \det \varphi \in G(k)$ — **дискриминант** φ . Если $\varphi \cong \langle a_1, \dots, a_m \rangle$, $\psi \cong \langle b_1, \dots, b_n \rangle$ — две формы, то $\varphi \perp \psi \cong \langle a_1, \dots, a_m, b_1, \dots, b_n \rangle$ — **(ортогональная) сумма** φ и ψ , $\varphi \otimes \psi \cong \langle \dots, a_i b_j, \dots \rangle_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ — **(тензорное) произведение** φ и ψ . Если $\varphi \cong \langle a_1, \dots, a_m \rangle$ и $a \in k^*$, то $a\varphi \cong \langle aa_1, \dots, aa_m \rangle$ — **произведение** φ на a . Если $r \in \mathbb{N}$, то $r \times \varphi \cong \underbrace{\varphi \perp \cdots \perp \varphi}_{r \text{ раз}}$ — r -кратная сумма φ с собой, $0 \times \varphi = 0$ — пустая форма размерности 0.

Рассмотрим абелев моноид невырожденных квадратичных форм относительно ортогональной суммы; по теореме Витта он является моноид с сокращением, поэтому он вкладывается в свою группу Гротендика. На этой абелевой группе определено умножение, индуцированной тензорным произведением. В результате получаем **кольцо** (коммутативное, ассоциативное, с 1) **Витта–Гротендика** $\widetilde{W}(k)$.

1.2.6 Определение. Квадратичная форма φ называется **гиперболической**, если она изоморфна прямой сумме гиперболических плоскостей: $\varphi = r \times \mathbb{H}$ для некоторого $r \geq 0$.

1.2.7 Утверждение. Гиперболические формы (и противоположные к ним) образуют идеал в кольце $\widetilde{W}(k)$.

Доказательство. Очевидно, что сумма гиперболических форм гиперболична; поскольку одномерные формы аддитивно порождают $\widetilde{W}(k)$, достаточно доказать, что $\mathbb{H} \otimes \langle a \rangle$ гиперболична, но $\mathbb{H} \otimes \langle a \rangle \cong \langle a, -a \rangle \cong \mathbb{H}$. \square

1.2.8 Определение. Фактор-кольцо кольца Витта–Гротендика $\widetilde{W}(k)$ по идеалу гиперболических форм называется **кольцом Витта** и обозначается $W(k)$.

Вот другое определение кольца Витта: две невырожденные формы φ, ψ над k называются **подобными**, если $\varphi_{ap} \cong \psi_{ap}$. Обозначение: $\varphi \sim \psi$. Множество классов эквивалентности регулярных форм над k обозначается $W(k)$.

1.2.9 Теорема (Витт, 1937). Множество $W(k)$ является коммутативным ассоциативным кольцом с 1 относительно операций, индуцированных \oplus и \otimes и называется **кольцом Витта**. Относительно операции \oplus множество $W(k)$ является абелевой группой и называется **группой Витта**.

Доказательство. Очевидно. \square

Заметим, что в качестве представителя элемента $W(k)$ можно взять квадратичную форму (а не формальную разность двух квадратичных форм, как в $\widetilde{W}(k)$), и для ненулевого класса эту форму можно выбрать анизотропной.

1.2.10 Примеры. 1. Если поле k алгебраически замкнуто, то $W(k) = \mathbb{Z}/2\mathbb{Z}$.

2. $W(\mathbb{R}) = \mathbb{Z}$.

3. $W(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ для $p \equiv 1 \pmod{4}$ и $W(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/4\mathbb{Z}$ для $p \equiv 3 \pmod{4}$.

Дадим еще одну характеристику индекса Витта.

1.2.11 Определение. Пусть (V, q) — квадратичная форма. Подпространство $W \leq V$ называется **вполне изотропным**, если $q|_W = 0$. Это условие равносильно тому, что всякий вектор $v \in W$ изотропен.

1.2.12 Утверждение. Пусть (V, q) — квадратичная форма. Все максимальные вполне изотропные подпространства V имеют одинаковую размерность, равную индексу Витта $i(q)$ формы q .

Доказательство. Очевидно, что если $q = (m \times \mathbb{H}) \perp \varphi$, то в V есть вполне изотропное подпространство размерности m . Обратно, пусть в V есть такое подпространство. Докажем индукцией по m , что тогда в V вкладывается сумма m гиперболических плоскостей. При $m = 0$ доказывать нечего. Если $m > 0$, выберем изотропный вектор $v \in V$. Рассуждение из доказательства предложения 1.1.7 показывает, что найдется вектор $v' \in V$

такой, что $kv \oplus kv' \cong \mathbb{H}$; стало быть, $q \cong \mathbb{H} \perp q'$. Пусть $W = v^\perp$. Тогда $kv \subset W$ и на факторе W/kv возникает корректно определенная форма \tilde{q} , задаваемая равенством $\tilde{q}(w + kv) := q(w)$. Легко видеть, что $\tilde{q} \cong q'$. Но по построению \tilde{q} имеет вполне изотропное подпространство размерности $m - 1$, поэтому такое подпространство есть и в q' . По предположению индукции, в q' есть сумма $m - 1$ гиперболических плоскостей, поэтому в q есть сумма m гиперболических плоскостей. \square

1.2.13 Лемма. Пусть q, q' — две анизотропные формы. Предположим, что $i(q \perp -q') \geq n$. Тогда существуют квадратичные формы φ, q_1, q'_1 такие, что $\dim \varphi = n$ и $q \cong \varphi \perp q_1$ и $q' \cong \varphi \perp q'_1$.

Доказательство. Индукция по n . Пусть $n = 1$: $q \perp -q'$ изотропна, поэтому найдутся $x \in V, x' \in V'$ такие, что $q(x) = q'(x') \neq 0$ (здесь V, V' — подлежащие пространства форм q и q' соответственно), и утверждение очевидно. Если $n > 1$, действуя так же, получаем, что $q \cong \langle a \rangle \perp q_2, q' \cong \langle a \rangle \perp q'_2$ для некоторых a, q_2, q'_2 . Тогда $i(q_2 \perp q'_2) \geq n - 1$ и можно применить индукционное предположение. \square

1.2.14 Лемма. Пусть $a, b \in k^*$. Тогда $\langle a, b \rangle \cong \langle a + b, ab(a + b) \rangle$.

Доказательство. Немедленно следует из леммы 1.1.9. \square

1.2.15 Теорема. 1. Аддитивная группа кольца $\widetilde{W}(k)$ порождается (как абелева группа) образующими $\langle a \rangle, a \in k^*$, удовлетворяющими соотношениям $\langle ab^2 \rangle = \langle a \rangle$ и $\langle a, b \rangle = \langle a + b, ab(a + b) \rangle$.

2. Аддитивная группа кольца $W(k)$ порождается (как абелева группа) образующими $\langle a \rangle, a \in k^*$, удовлетворяющими соотношениям $\langle ab^2 \rangle = \langle a \rangle, \langle a, b \rangle = \langle a + b, ab(a + b) \rangle$ и дополнительным соотношениям $\langle -a \rangle = -\langle a \rangle$.

Доказательство. Пусть $V(k)$ — группа, порожденная соотношениями из первого пункта формулировки теоремы. Обозначим через $[a]$ образующую, соответствующую скаляру $a \in k^*$. Предыдущие результаты показывают, что существует сюръективный гомоморфизм $V(k) \rightarrow \widetilde{W}(k)$, переводящий $[a]$ в $\langle a \rangle$. Для доказательства первого пункта остается показать, что если $a_1, \dots, a_n, b_1, \dots, b_n \in k^*$ таковы, что $\langle a_1, \dots, a_n \rangle \cong \langle b_1, \dots, b_n \rangle$, то $[a_1] + \dots + [a_n] = [b_1] + \dots + [b_n]$.

Будем действовать индукцией по n с тривиальной базой $n = 1$. Пусть $n = 2$. Поскольку $\langle a_1, a_2 \rangle \cong \langle b_1, b_2 \rangle$, то найдутся $x_1, x_2 \in k$ такие, что $b_1 = a_1 x_1^2 + a_2 x_2^2$. Если $x_2 = 0$, то $\langle b_1 \rangle = \langle a_1 \rangle$, откуда $\langle b_2 \rangle = \langle a_2 \rangle$ и доказывать нечего. Если $x_1 = 0$, все аналогично. Если же $x_1 x_2 \neq 0$, заменяя a_i на $a_i x_i^2$, можно считать, что $x_1 = x_2 = 1$. По лемме 1.2.14 имеем $\langle b_2 \rangle \cong \langle a_1 a_2 (a_1 + a_2) \rangle$ и доказательство окончено.

Наконец, предположим, что $n \geq 3$. Обозначим $q = \langle a_1, \dots, a_{n-1} \rangle, q' = \langle b_1, \dots, b_{n-1} \rangle$. Тогда $q \perp -q' \sim \langle b_n, -a_n \rangle$, откуда, по лемме 1.2.13 существуют $c_1, \dots, c_{n-2}, e, f \in k^*$ такие, что $q \cong \langle c_1, \dots, c_{n-2}, e \rangle$ и $q' \cong \langle c_1, \dots, c_{n-1}, f \rangle$ и по теореме Витта $\langle e, a_n \rangle \cong \langle f, b_n \rangle$. Применяя индукционное предположение, получаем $[a_1] + \dots + [a_{n-1}] = [c_1] + \dots + [c_{n-2}] +$

$[e], [b_1] + \dots + [b_{n-1}] = [c_1] + \dots + [c_{n-2}] + [f]$ и $[e] + [a_n] = [f] + [b_n]$, и отсюда все следует. Второй пункт теоремы доказывается совершенно аналогично. \square

1.3 Первая теорема Касселса о представимости

Пусть φ — квадратичная форма над k , $k(t)$ — поле рациональных функций над k от одной переменной t .

1.3.1 Лемма. Если φ анизотропна над k , то $\varphi_{k(t)}$ анизотропна над $k(t)$.

Доказательство. Пусть $\varphi(f) = 0$, где $f = (f_1, \dots, f_n)$, $f_i \in k(t)$. Пусть g_0 — общий знаменатель функций f_i : $f_i = g_i/g_0$, где $g_0, g_1, \dots, g_n \in k[t]$. Тогда $\varphi(g) = g_0^2(f) = 0$ для $0 \neq g = (g_1, \dots, g_n)$. Теперь пусть $d = \gcd(g_1, \dots, g_n) \in k[t]$; $g_i = dh_i$, $h_i \in k[t]$ — взаимно просты. Пусть $h = (h_1, \dots, h_n)$, тогда $\varphi(g) = d^2\varphi(h) = 0$ — тождество. Поскольку $k[t]$ — область целостности, имеем $\varphi(h) = 0$. Положим $c_i = h_i(0) \in k$, $c = (c_1, \dots, c_n)$ — ненулевой вектор (иначе все h_i делились бы на t). Поэтому $c \in k^n$ и $\varphi(c) = 0$, противоречие. \square

1.3.2 Теорема. Пусть $\varphi(x) = \varphi(x_1, \dots, x_n) = \sum_{i,j=1}^n a_{ij}x_i x_j$ — n -арная квадратичная форма над k . Пусть $0 \neq p(t) \in k[t]$. Предположим, что φ представляет p над полем $k(t)$. Тогда φ представляет p над кольцом $k[t]$, то есть найдутся $f_i \in k[t]$ такие, что $\varphi(f_1, \dots, f_n) = p$.

Доказательство. Если φ не регулярна, можно заменить φ на $(n-1)$ -форму и действовать по индукции. Если $n = 1$, $\varphi(x) = a_{11}x_1^2$, $a_{11}f_1^2 = p$ для $f_1 \in k(t)$, откуда $f_1 \in k[t]$. Предположим теперь, что φ регулярна, но изотропна. Тогда $\varphi \cong H \perp \psi$ над k , то есть можно считать, что $\varphi(x) = 2x_1x_2 + \psi(x_3, \dots, x_n)$. Положим $x_1 = p(t)$, $x_2 = 1/2$, $x_3 = \dots = x_n = 0$. Наконец, φ регулярна и анизотропна. По предположению

$$\varphi\left(\frac{f_1}{f_0}, \dots, \frac{f_n}{f_0}\right) = p$$

для некоторых многочленов $f_0, \dots, f_n \in k[t]$; не умаляя общности, имеем $\gcd(f_0, \dots, f_n) = 1$. Более того, можно считать, что из всех представлений в таком виде выбрано то, у которого $d = \deg f_0$ минимальна. Предположим, что $d > 0$ и получим противоречие. Рассмотрим новую форму $\psi = \langle -p(t) \rangle \oplus \varphi_{k(t)}$ над $k(t)$: $\psi(x_0, \dots, x_n) = -p(t)x_0^2 + \varphi(x_1, \dots, x_n)$. Очевидно, что $\psi(f_0, \dots, f_n) = 0$. Поделим с остатком f_i на f_0 : $f_i = f_0g_i + r_i$, $\deg r_i < d$. В частности, $g_0 = 1$, $r_0 = 0$, $\deg r_0 = -\infty$. $\psi(g) \neq 0$ по минимальности $d = \deg f_0$. В частности, f и g линейно независимы над $k(t)$. Определим $h = \lambda f - \mu g \in (k(t))^{n+1}$, $\lambda = \psi(g)$, $\mu = 2b_\psi(f, g)$. $h = (h_0, \dots, h_n)$, $\lambda \neq 0$, значит, $h \neq 0$. Но

$$\psi(h) = \lambda^2\psi(f) - 2\lambda\mu b_\psi(f, g) + \mu^2\psi(g) = 0.$$

На самом деле $h_0 \neq 0$, иначе ψ была бы изотропна над $k(t)$ и, по лемме, над k . Осталось оценить $\deg h_0$:

$$\begin{aligned} h_0 &= \lambda f_0 - \mu = \psi(g)f_0 - b_\psi(f, g) = \frac{1}{f_0} \psi(f_0 g - f) \\ &= \frac{1}{f_0} \sum_{i,j=1}^n a_{ij} (f_0 g_i - f_i) (f_0 g_j - f_j). \end{aligned}$$

Поэтому $\deg \psi(f_0 g - f) \leq 2 \max_{i=1, \dots, n} \deg(f_0 g_i - f_i) = 2 \max_{i=1, \dots, n} \deg r_i \leq 2(d-1)$, откуда $\deg h_0 = -d + \deg \psi(f_0 g - f) \leq d-2$, противоречие. \square

1.3.3 Теорема (обобщение). Пусть $\varphi(x) = \sum_{i,j=1}^n a_{ij} x_i x_j$ — квадратичная форма над $k(t)$ такая, что $a_{ij} \in k[t]$ и $\deg a_{ij} \leq 1$ для всех (i, j) . Предположим, что φ анизотропна над $k(t)$. Пусть φ представляет над $k(t)$ многочлен $0 \neq p(t) \in k[t]$. Тогда φ представляет $p(t)$ над $k[t]$.

Доказательство. Доказательство повторяется, но в этот раз $\deg \psi(f_0 g - f) \leq 1 + 2 \max \deg r_i \leq 2d-1$, откуда $\deg h_0 \leq d-1 < d$. \square

1.3.4 Замечание. Доказательство перестает быть верным, если φ изотропна! Пусть $\varphi = \langle t, -t \rangle$, $p(t) = 1$; тогда φ представляет p над $k(t)$, но не над $k[t]$.

1.4 Теорема о подформе

1.4.1 Теорема (Принцип подстановки). Пусть φ — n -арная квадратичная форма над k , $0 \neq p = p(t_1, \dots, t_m) \in k[t_1, \dots, t_m]$ и $c_1, \dots, c_m \in k$. Если φ представляет p над полем рациональных функций $k(t_1, \dots, t_m)$, то φ представляет элемент $p(c_1, \dots, c_m)$ над k .

Доказательство. Индукция по m . \square

1.4.2 Лемма. Пусть $d, a_1, \dots, a_n \in k^*$; предположим, что $\varphi = \langle a_1, \dots, a_n \rangle$ представляет многочлен $d + a_1 t^2$ над $k(t)$. Тогда или φ изотропна над k или $\varphi' = \langle a_2, \dots, a_n \rangle$ представляет d над k .

Доказательство. Предположим, что φ анизотропна. Из теоремы Касселса получаем, что $\sum_{i=1}^n a_i f_i^2 = d + a_1 t^2$ для некоторых $f_i \in k[t]$. Легко видеть, что $\deg f_i = 1$, пусть $f_i = b_i + c_i t$; уравнение $b_1 + c_1 t = \pm t$ имеет некоторое решение $t = c$. Подставляя c , видим, что φ' представляет d . \square

1.4.3 Теорема (Теорема о подформе). Пусть $\varphi \cong \langle a_1, \dots, a_n \rangle$, $\psi \cong \langle b_1, \dots, b_m \rangle$ — регулярные квадратичные формы над k . Предположим, что φ анизотропна. Следующие утверждения эквивалентны:

1. ψ изоморфна подформе φ , то есть $\varphi \cong \psi \perp \xi$ для некоторой квадратичной формы ξ над k (возможно, $\xi = 0$).

2. $D_L(\psi) \subseteq D_L(\varphi)$ для любого поля $L \supseteq k$.

3. φ представляет «общее значение» ψ , то есть φ представляет $\psi(t_1, \dots, t_m) = b_1 t_1^2 + \dots + b_m t_m^2$ над полем рациональных функций $k(t_1, \dots, t_m)$.

В частности, из любого из этих утверждений следует, что $m \leq n$.

Доказательство. (1) \Rightarrow (2) \Rightarrow (3) — очевидно. Докажем (3) \Rightarrow (1) индукцией по m , база тривиальна. Пусть теперь $m > 0$. По принципу подстановки φ представляет $b_1 \neq 0$ над k . Значит, мы можем записать $\varphi \cong \langle b_1 \rangle \perp \varphi'$, где φ' автоматически анизотропна. Поскольку φ представляет $b_1 t_1^2 + (b_2 t_2^2 + \dots + b_m t_m^2)$ над $k(t_2, \dots, t_m)(t_1)$, по лемме φ' представляет $d = \psi'(t_2, \dots, t_m) = b_2 t_2^2 + \dots + b_m t_m^2$. Теперь можно применить предположение индукции к паре (φ', ψ') и получить, что $\varphi' \cong \psi' \perp \xi$ и $\varphi \cong \langle b_1 \rangle \perp \varphi' \cong \langle b_1 \rangle \perp \psi' \perp \xi \cong \psi \perp \xi$. \square

1.4.4 Определение. В ситуации пункта 1 теоремы 1.4.3 будем говорить, что ψ — **подформа** φ и писать $\psi \leq \varphi$.

1.4.5 Определение. Пусть φ — квадратичная форма. Напомним, что $D(\varphi) = \{a \in k^* \mid \exists x, \varphi(x) = a\}$ — множество ненулевых элементов, представляемых формой φ . Положим $G(\varphi) = \{a \in k^* \mid a\varphi \cong \varphi\}$ — множество коэффициентов подобия φ .

1.4.6 Лемма. 1. Если $\varphi \leq \varphi'$, то $D(\varphi) \subseteq D(\varphi')$.

2. Если φ изотропна, то $D(\varphi) = k^*$.

3. Для любого $\lambda \in k^*$ имеем $G(\lambda\varphi) = G(\varphi)$.

4. $G(\varphi)$ зависит лишь от класса φ в кольце Витта $W(k)$.

5. $G(\varphi)$ — подгруппа k^* , содержащая $(k^*)^2$. Если $a \in G(\varphi)$, $b \in D(\varphi)$, то $ab \in D(\varphi)$.

6. Если $1 \in D(\varphi)$, то $G(\varphi) \subseteq D(\varphi)$.

Доказательство. Пункты 1–3 очевидны, для доказательства 4 достаточно проверить, что $G(\varphi) = G(\varphi \perp \mathbb{H})$. Заметим, что $a\mathbb{H} \cong \langle a, -a \rangle \cong \mathbb{H}$ для любого $a \in k^*$. Если $a \in G(\varphi)$, то $\varphi \cong a\varphi$, поэтому

$$\varphi \perp \mathbb{H} \cong a\varphi \perp \mathbb{H} \cong a\varphi \perp a\mathbb{H} \cong a(\varphi \perp \mathbb{H}).$$

Обратно, если $\varphi \perp \mathbb{H} \cong a(\varphi \perp \mathbb{H}) \cong a\varphi \perp a\mathbb{H} \cong a\varphi \perp \mathbb{H}$, то по теореме Витта о сокращении получаем, что $\varphi \cong a\varphi$. Далее, 5 очевидно и 6 следует из 5. \square

1.4.7 Лемма. Пусть φ — квадратичная форма над k и $\varphi' \leq \varphi$. Если $\dim \varphi' > \dim \varphi - i(\varphi)$, то φ' изотропна.

Первое доказательство. Пусть V — пространство формы φ , W — подпространство, соответствующее φ' , $H \leq V$ — максимальное вполне изотропное подпространство размерности $i(\varphi)$ (см. предложение 1.2.12). При этом $\dim(W) + \dim(H) > \dim(V)$, откуда пересечение $W \cap H$ непусто. \square

Второе доказательство. Запишем $\varphi' \perp \varphi'' \cong \varphi \cong \varphi_{\text{ан}} \perp i(q) \times \mathbb{H}$ для некоторой формы φ'' . Тогда $\varphi' \perp \varphi'' \perp -\varphi'' \cong \varphi_{\text{ан}} \perp -\varphi'' \perp i(q) \times \mathbb{H}$. Заметим, что $\varphi'' \perp -\varphi'' \cong \dim(\varphi'') \times \mathbb{H}$, поэтому $\varphi' \cong \varphi_{\text{ан}} \perp -\varphi'' \perp (i(q) - \dim(\varphi'')) \times \mathbb{H}$ и φ' изотропна. \square

1.5 Поведение квадратичных форм при конечных расширениях полей

Посмотрим на самый простой нетривиальный случай — квадратичное расширение.

1.5.1 Лемма. Пусть $L = k(\sqrt{a})$, φ — анизотропная форма над k . Тогда равносильны:

1. φ_L изотропна;
2. $\varphi = b\langle 1, -a \rangle \perp \psi$ для некоторых $b \in k^*$ и формы ψ .

Доказательство. Очевидно, что из второго пункта следует первый. Пусть теперь φ_L изотропна. Это означает, что в $V \otimes L$ есть изотропный вектор, то есть, $\varphi(v + w\sqrt{a}) = 0$ для некоторых $v, w \in V$, не равных одновременно нулю. Значит, $\varphi(v) + a\varphi(w) + 2\sqrt{a}b_\varphi(v, w) = 0$, откуда $\varphi(v) = -a\varphi(w)$ и $b_\varphi(v, w) = 0$. Разложим V в прямую сумму пространства $W = kv + kw$ и ортогонального дополнения W^\perp . Относительно этого разбиения и получим необходимое разложение формы φ . \square

1.5.2 Теорема. Пусть $L = k(\sqrt{a})$, φ — анизотропная форма над k . Тогда равносильны:

1. $i(\varphi_L) \geq i$;
2. $\varphi = \langle 1, -a \rangle \otimes \varphi' \perp \psi$, где $\text{rk } \varphi' = i$.

Доказательство. Индукция по i ; используется, что $i(\varphi \perp \mathbb{H}) = i(\varphi) + 1$. \square

1.5.3 Следствие. В условиях теоремы если φ_L гиперболична, то $\varphi = \langle 1, -a \rangle \otimes \psi$.

Таким образом, ядро отображения $W(k) \rightarrow W(k(\sqrt{a}))$ порождается формами вида $\langle 1, -a \rangle$.

1.5.4 Теорема (Спрингер). Пусть k — подполе L и степень $[L : k]$ нечетна. Тогда $i(\varphi_L) = i(\varphi)$.

Доказательство. Достаточно проверить, что из анизотропности φ следует анизотропность φ_L и проверить при этом лишь случай расширения, порожденного одним элементом: $L = k(\alpha)$. Будем доказывать индукцией по $n = [L : k]$ с тривиальной базой $n = 1$. Предположим противное: пусть P — минимальный многочлен α , $d = \dim(\varphi)$ и $(x_1, \dots, x_d) \in L^d \setminus \{0\}$ таковы, что $\varphi(x_1, \dots, x_d) = 0$. Можно записать $x_i = g_i(\alpha)$, где $g \in k[t]$, $m := \max(\deg g_i) < n$ и g_i не все равны 0. Разделив на наибольший общий делитель, можно считать, что они взаимно просты в совокупности. Получаем равенство в $k[t]$:

$$\varphi(g_1, \dots, g_d) = P \cdot h$$

для некоторого $h \in k[t]$. При этом $\deg(h) = 2m - n \leq n - 2$: действительно, из анизотропности φ следует, что $\deg(\varphi(g_1, \dots, g_d)) = 2m$. В частности, $\deg(h)$ нечетна. Пусть h' — неприводимый множитель h нечетной степени; очевидно, что $\deg(h') \leq n - 2$. Обозначим $F = k[t]/(h')$; это расширение k нечетной степени, меньшей n . Пусть β — образ t в F . Тогда $\varphi_F(g_1(\beta), \dots, g_d(\beta)) = 0$. По предположению индукции φ_F анизотропна, поэтому $g_1(\beta) = \dots = g_d(\beta) = 0$, откуда h' является общим делителем g_1, \dots, g_d , что противоречит предположению. \square

1.5.5 Следствие. Если степень L над k нечетна, то отображение $W(k) \rightarrow W(L)$ инъективно.

2 Теория Пфистера

2.1 Формы Пфистера

2.1.1 Определение. Рассмотрим отображение $\overline{\dim}: W(k) \rightarrow \mathbb{Z}/2\mathbb{Z}$, индуцированное размерностью. Ядро этого отображения называется **фундаментальным идеалом** кольца $W(k)$ и обозначается через IF .

2.1.2 Лемма. 1. Идеал IF аддитивно порождается формами вида $\langle 1, -a \rangle$, $a \in k^*$.

2. n -ая степень этого идеала $I^n F := (IF)^n$ аддитивно порождается тензорными произведениями n бинарных форм:

$$\langle 1, -a_1 \rangle \otimes \dots \otimes \langle 1, -a_n \rangle =: \langle\langle a_1, \dots, a_n \rangle\rangle.$$

Доказательство. Очевидно, что IF порождается формами вида $\langle a, b \rangle$, $a, b \in k^*$. При этом $\langle a, b \rangle \sim \langle 1, a \rangle \perp -\langle 1, -b \rangle$. Второе утверждение немедленно следует из первого. \square

2.1.3 Определение. 1. Форма вида $\langle\langle a_1, \dots, a_n \rangle\rangle$ для $a_1, \dots, a_n \in k^*$ называется **n -формой Пфистера** и имеет размерность 2^n . Форма называется **формой Пфистера**, если она является n -формой Пфистера для некоторого n .

2. Если φ — форма Пфистера, то φ представляет 1, поэтому $\varphi \cong \langle 1 \rangle \perp -\varphi'$ для некоторой формы φ' . Такая форма φ' называется **чистой формой**, ассоциированной с φ .

3. Обозначим через $P_n(k)$ множество классов изометрий n -форм Пфистера; $P(k) = \bigcup_n P_n(k)$; $GP_n(k) = \{[q] \in W(F) \mid \exists a \in k^*, aq \in P_n(k)\}$; $GP(k) = \bigcup_n GP_n(k)$.

2.1.4 Лемма. Пусть $a_1, \dots, a_n, b_n \in F^*$. Тогда

$$\langle\langle a_1, \dots, a_{n-1}, a_n b_n \rangle\rangle \perp \langle\langle a_1, \dots, a_{n-1}, a_n, b_n \rangle\rangle \sim \langle\langle a_1, \dots, a_n \rangle\rangle \perp \langle\langle a_1, \dots, a_{n-1}, b_n \rangle\rangle.$$

Доказательство. Докажем сначала это для $n = 1$:

$$\begin{aligned} \langle\langle a_1 b_1 \rangle\rangle \perp \langle\langle a_1, b_1 \rangle\rangle &\cong \langle 1, -a_1 b_1, 1, -a_1, -b_1, a_1 b_1 \rangle \\ &\sim \langle 1, 1, -a_1, -b_1 \rangle \\ &\cong \langle\langle a_1 \rangle\rangle \perp \langle\langle b_1 \rangle\rangle. \end{aligned}$$

Остается домножить обе части этого соотношения на $\langle\langle a_1, \dots, a_{n-1} \rangle\rangle$. \square

Пусть $\tilde{I}F$ — ядро отображения $\dim: \tilde{W}(k) \rightarrow \mathbb{Z}$ и $\tilde{I}^n F = (\tilde{I}F)^n$. Отображение $\tilde{W}(k) \rightarrow W(k)$ индуцирует гомоморфизмы $\tilde{I}^n F \rightarrow I^n F$.

2.1.5 Лемма. Эти гомоморфизмы биективны для всех $n \geq 1$.

Доказательство. Достаточно рассмотреть случай $n = 1$. Для доказательства сюръективности заметим, что $\langle 1 \rangle - \langle a \rangle$ переходит в $\langle 1, -a \rangle$. Инъективность: пусть q, q' — формы одной размерности такие, что $q - q'$ переходит в 0 в кольце $W(k)$. Тогда $q \perp -q' \sim 0$, откуда $q \cong q'$. \square

Если $n = 1$, форма $\varphi = \langle 1, -a \rangle$ является нормой квадратичного расширения $A = k(\sqrt{a})$ поля k . Если $n = 2$, $\varphi = \langle\langle a, b \rangle\rangle$ есть приведенная норма алгебры кватернионов $A = \begin{pmatrix} a & b \\ k & \end{pmatrix}$. Если $n = 3$, $\varphi = \langle\langle a, b, c \rangle\rangle$ есть норма неассоциативной алгебры октонионов A , определяемой a, b, c . В каждом из этих случаев выполняется тождество $\varphi(x \cdot y) = \varphi(x)\varphi(y)$ для всех $x, y \in A$. В частности, если $\varphi(x) \neq 0$, то $\varphi \cong \varphi(x)\varphi$. Иными словами, $D(\varphi) = G(\varphi)$. Если $n \geq 4$, $\varphi = \langle\langle a_1, \dots, a_n \rangle\rangle$ соответствует алгебре Кэли–Диксона A , определяемой a_1, \dots, a_n , но не обязательно $\varphi(x \cdot y) = \varphi(x)\varphi(y)$.

2.1.6 Теорема (Пфистер). Если φ — форма Пфистера, $\varphi(x) \neq 0$, то $\varphi \cong \varphi(x)\varphi$. Иными словами, $D(\varphi) = G(\varphi)$.

2.1.7 Лемма. Если $a, b, t \in k^*$, то $\langle\langle a, b \rangle\rangle \cong \langle\langle -ab, a + b \rangle\rangle$, $\langle\langle a, b \rangle\rangle \cong \langle\langle a, (t^2 - a)b \rangle\rangle$.

Доказательство. Заметим, что $\langle -a, -b \rangle \cong \langle -a - b, ab(-a - b) \rangle$, откуда

$$\langle\langle a, b \rangle\rangle = \langle 1, -a, -b, ab \rangle \cong \langle 1, ab, -a - b, ab(-a - b) \rangle = \langle\langle -ab, a + b \rangle\rangle.$$

С другой стороны, для 1-форм Пфистера теорема 2.1.6 уже доказана, так что $\langle 1, -a \rangle \cong (t^2 - a)\langle 1, -a \rangle$, откуда $\langle -b, ab \rangle \cong \langle -(t^2 - a)b, (t^2 - a)ab \rangle$ и $\langle\langle a, b \rangle\rangle = \langle 1, -a, -b, ab \rangle \cong \langle 1, -a, -(t^2 - a)b, (t^2 - a)ab \rangle = \langle\langle a, (t^2 - a)b \rangle\rangle$. \square

2.1.8 Утверждение. Пусть $\varphi = \langle\langle a_1, \dots, a_n \rangle\rangle$ — n -форма Пфистера и $b \in D(\varphi')$, где φ' — чистая форма, ассоциированная с φ . Тогда найдутся $b_2, \dots, b_n \in k^*$ такие, что $\varphi \cong \langle\langle b, b_2, \dots, b_n \rangle\rangle$.

Доказательство. Доказываем индукцией по n . Если $n = 1$, то $b = a_1 c^2$ для некоторого $c \in k^*$, и все очевидно. Предположим, что $n > 1$ и обозначим $\tau = \langle\langle a_1, \dots, a_{n-1} \rangle\rangle \cong \langle 1 \rangle \perp -\tau'$, тогда $\varphi' = \tau' \perp a_n \tau$. Запишем $b = x + a_n y$ для $x \in D(\tau') \cup \{0\}$, $y \in D(\tau) \cup \{0\}$. Рассмотрим несколько случаев:

1. Если $y = 0$, то $x \neq 0$ и $b \in D(\tau')$, откуда по предположению индукции $\tau \cong \langle\langle b, b_2, \dots, b_{n-1} \rangle\rangle$, поэтому $\varphi \cong \langle\langle b, b_2, \dots, b_{n-1}, a_n \rangle\rangle$.
2. Если $y \neq 0$, мы покажем, что $\varphi \cong \langle\langle a_1, \dots, a_{n-1}, a_n y \rangle\rangle$. Запишем $y = t^2 - y_0$ для $y_0 \in D(\tau') \cup \{0\}$.

(а) Если $y_0 = 0$, $y = t^2$ и все очевидно.

(б) Если $y_0 \in D(\tau')$, то по предположению индукции имеем $\tau \cong \langle\langle y_0, c_1, \dots, c_{n-1} \rangle\rangle$, поэтому

$$\begin{aligned} \varphi &\cong \langle\langle y_0, c_2, \dots, c_{n-1}, a_n \rangle\rangle \\ &\cong \langle\langle y_0, c_2, \dots, c_{n-1}, (t^2 - y_0) a_n \rangle\rangle \\ &= \langle\langle y_0, c_2, \dots, c_{n-1}, a_n y \rangle\rangle \\ &\cong \langle\langle a_1, \dots, a_{n-1}, a_n y \rangle\rangle, \end{aligned}$$

что и требовалось.

Теперь если $x = 0$, то $a_n y = b$ и все в порядке. Если же $x \in D(\tau')$, то $\tau = \langle\langle x, d_2, \dots, d_{n-1} \rangle\rangle$, откуда

$$\varphi \cong \langle\langle x, d_2, \dots, d_{n-1}, a_n y \rangle\rangle \cong \langle\langle x + a_n y, d_2, \dots, d_{n-1}, -x a_n y \rangle\rangle \cong \langle\langle b, \dots \rangle\rangle.$$

□

2.1.9 Следствие. Изотропная форма Пфистера гиперболична.

Доказательство. Если φ изотропна, то $1 \in D(\varphi')$

□

Доказательство теоремы 2.1.6. Запишем $\varphi(x) = t^2 - a$ для $a \in D(\varphi') \cup \{0\}$. Если $a = 0$, утверждение очевидно. Если $a \in D(\varphi')$, то $\varphi \cong \langle\langle a \rangle\rangle \otimes \tau$ для некоторой формы Пфистера τ . Тогда $\varphi(x) \varphi = (t^2 - a) \langle\langle a \rangle\rangle \tau \cong \langle\langle a \rangle\rangle \tau \cong \varphi$, поскольку $\langle\langle a \rangle\rangle$ мультипликативна.

□

2.1.10 Следствие. Две пропорциональные формы Пфистера изометричны.

Доказательство. Действительно, если φ, φ' — две формы Пфистера, $a \in k^*$ и $a\varphi \cong \varphi'$, то из $1 \in D(\varphi)$ следует $a \in D(\varphi')$, откуда $\varphi' \cong a\varphi'$ по теореме 2.1.6.

□

2.1.11 Следствие. Пусть $\varphi \in P(k)$. Тогда, для всякого $a \in D(\varphi)$ и $b \in k^*$ имеем $\varphi \otimes \langle\langle a \rangle\rangle \sim 0$ и $\varphi \otimes \langle\langle ab \rangle\rangle \cong \varphi \otimes \langle\langle b \rangle\rangle$.

Доказательство. Первая часть немедленно следует из теоремы 2.1.6; вторая — из первой и леммы 2.1.4. \square

2.1.12 Следствие. Пусть q — квадратичная форма размерности > 1 над k и $\varphi \in P_n(k)$. Предположим, что $q \otimes \varphi$ изотропна. Тогда

1. Найдется изотропная форма q' такая, что $q \otimes \varphi \cong q' \otimes \varphi$.
2. Анизотропная часть $q \otimes \varphi$ имеет вид $\rho \otimes \varphi$ для некоторой формы ρ .
3. Индекс Витта формы $q \otimes \varphi$ делится на 2^n .

Доказательство. 1. Если форма φ изотропна, то она гиперболична и все очевидно.

Пусть φ анизотропна. Запишем $q \cong \langle a_1, \dots, a_n \rangle$. По предположению существуют $b_1, \dots, b_n \in D(\varphi) \cup \{0\}$ такие, что $a_1 b_1 + \dots + a_n b_n = 0$ и не все b_i равны нулю. Не умаляя общности, можно считать, что $b_1, \dots, b_r \in D(\varphi)$ и $b_{r+1} = \dots = b_n = 0$. Положим $q' = \langle a_1 b_1, \dots, a_r b_r, a_{r+1}, \dots, a_n \rangle$. Тогда q' изотропна и $q' \otimes \varphi \cong a_1 b_1 \varphi \perp \dots \perp a_r b_r \varphi \perp a_{r+1} \varphi \perp \dots \perp a_n \varphi \cong a_1 \varphi \perp \dots \perp a_r \varphi \perp a_{r+1} \varphi \perp \dots \perp a_n \varphi \cong q \otimes \varphi$.

2. Если q' такая, как в предыдущем абзаце и $m = i(q')$ максимален, то $q \otimes \varphi \cong (m \times \mathbb{H} \perp \rho) \otimes \varphi \sim \rho \otimes \varphi$ и $\rho \otimes \varphi$ анизотропна по предыдущему пункту.
3. следует из предыдущего.

\square

2.2 Суммы квадратов и s -инвариант

2.2.1 Определение. Пусть k — поле; s -инвариантом k называется наименьшее целое $s(k)$ такое, что -1 является суммой $s(k)$ квадратов в k . Если такого не существует, полагаем $s(k) = +\infty$.

2.2.2 Теорема (Артин–Шрайер). $s(k) = +\infty$ тогда и только тогда, когда k можно снабдить структурой упорядоченного поля. В этом случае говорят, что k — формально вещественное поле.

2.2.3 Теорема. Если $s(k) < +\infty$, то это степень двойки.

Доказательство. Положим $s = s(k)$, пусть n — целое число такое, что $2^n \leq s < 2^{n+1}$. Положим $\varphi = \langle\langle -1 \rangle\rangle^{\otimes n}$. Из определения s следует, что найдутся x, y такие, что $y \neq 0$ и $\varphi(x) = -\varphi(y)$. При этом $\varphi(y) \neq 0$ (иначе $s < 2^n$). Значит, $-1 = \varphi(x)/\varphi(y) \in D(\varphi)$ по теореме 2.1.6, откуда $s \leq 2^n$. \square

2.2.4 Определение. Если A — абелева группа, экспонентой A называется наименьшее целое число $m > 0$ такое, что $mA = 0$ (или $+\infty$, если такого не существует).

2.2.5 Утверждение. 1. Экспонента $W(k)$ равна $2s(k)$.

2. Если $s(k) < +\infty$, то всякий элемент IF является нильпотентом. В частности, $W(k)$ — локальное кольцо с максимальным идеалом IF .

Доказательство. 1. Экспонента аддитивной группы кольца равна порядку единицы. Обозначим $s = s(k)$. Это степень двойки, поэтому достаточно показать, что $s \times \langle 1 \rangle \not\sim 0$ и $2s \times \langle 1 \rangle \sim 0$. Первое следует из определения s ; для доказательства второго заметим, что $(s+1) \times \langle 1 \rangle$ является изотропной подформой формы Пфистера $2s \times \langle 1 \rangle$, которая гиперболична.

2. Для всякой формы $q = \langle a_1, \dots, a_n \rangle$ размерности n имеем $q \otimes q \cong n \times \langle 1 \rangle \perp \perp_{i \neq j} \langle a_i a_j \rangle \cong n \times \langle 1 \rangle \perp \varphi \perp \varphi$, где $\varphi = \perp_{i < j} \langle a_i a_j \rangle$. Если $q \in IF$, то $q^2 \in 2W(k)$, поэтому $q^{2^r} \in 2^r W(k)$ для всех $r > 1$.

□

2.3 Связанные формы Пфистера

2.3.1 Определение. Пусть φ_1, φ_2 — две формы Пфистера. Будем говорить, что φ_1 и φ_2 являются r -связанными, если существует r -форма Пфистера τ и формы Пфистера ψ_1 и ψ_2 такие, что $\varphi_1 \cong \tau \otimes \psi_1$ и $\varphi_2 \cong \tau \otimes \psi_2$. Формы φ_1 и φ_2 называются связанными, если они являются $(n-1)$ -связанными n -формами Пфистера.

2.3.2 Теорема. Пусть φ_1, φ_2 — две анизотропные формы Пфистера и $a_1, a_2 \in k^*$. Тогда $i(a_1 \varphi_1 \perp a_2 \varphi_2) = 0$ или 2^r , где r — наибольшее целое число, для которого φ_1 и φ_2 являются r -связанными.

Для доказательства теоремы нам потребуется некоторое усиление предложения 2.1.8.

2.3.3 Утверждение. Пусть $\varphi \in P_r(k)$, $\psi \in P_s(k)$ — две формы Пфистера, ψ' — чистая форма, ассоциированная с ψ . Если $a \in D(\psi' \otimes \varphi)$, то существует $\tau \in P(k)$ такая, что $\psi \otimes \varphi \cong \langle\langle a \rangle\rangle \otimes \tau \otimes \varphi$.

Доказательство. Индукция по s . Если $s = 1$, то $\psi \cong \langle\langle b \rangle\rangle$ и $a \in D(b\varphi)$, откуда $ab \in D(\varphi)$. По следствию 2.1.11 имеем $\langle\langle a \rangle\rangle \otimes \varphi \cong \langle\langle b \rangle\rangle \otimes \varphi$. Пусть теперь $s > 1$, $\psi \cong \langle\langle b \rangle\rangle \otimes \psi_1$, ψ'_1 — чистая форма, ассоциированная с ψ_1 . Тогда $\psi' \otimes \varphi \cong b\psi_1 \otimes \varphi \perp \psi'_1 \otimes \varphi$. Запишем $a = bx + y$, где $x \in D(\psi_1 \otimes \varphi) \cup \{0\}$, $y \in D(\psi'_1 \otimes \varphi) \cup \{0\}$. Предположим сначала, что $x, y \neq 0$. Тогда $\psi \otimes \varphi \cong \langle\langle b \rangle\rangle \otimes \psi_1 \otimes \varphi \cong \langle\langle bx \rangle\rangle \otimes \psi_1 \otimes \varphi$ по следствию 2.1.11. Кроме того, по предположению индукции, существует форма Пфистера $\tau_1 \in P_{s-1}(k)$ такая, что $\psi_1 \otimes \varphi \cong \langle\langle y \rangle\rangle \otimes \tau_1 \otimes \varphi$. Теперь по лемме 2.1.7 имеем $\psi \otimes \varphi \cong \langle\langle bx, y \rangle\rangle \otimes \tau \otimes \varphi \cong \langle\langle a, -bxy \rangle\rangle \otimes \tau_1 \otimes \varphi$. Если же $y = 0$ или $x = 0$, достаточно только половины из этих рассуждений. □

Доказательство теоремы. Пусть $\tau \in P_r(k)$, $\psi_1, \psi_2 \in P(k)$ таковы, что $\varphi_1 \cong \tau \otimes \psi_1$, $\varphi_2 \cong \tau \otimes \psi_2$ и r максимально. Если форма $a_1\varphi_1 \perp a_2\varphi_2$ анизотропна, доказывать нечего. Если же она изотропна, то найдется $b \in D(a_1\varphi_1) \cap D(-a_2\varphi_2)$, откуда $a_1b \in D(\varphi_1)$ и $-a_2b \in D(\varphi_2)$. Тогда $a_1\varphi_1 \cong b\varphi_1$ и $a_2\varphi_2 \cong -b\varphi_2$. Теперь не умаляя общности можно считать, что $a_1 = 1$, $a_2 = -1$. Имеем $\varphi_1 \perp -\varphi_2 \sim \tau \otimes (\psi'_2 \perp -\psi'_1)$, где ψ'_1 и ψ'_2 — чистые формы, ассоциированные с ψ_1 и ψ_2 . При этом $\dim(\varphi_1 \perp -\varphi_2) - \dim(\tau \otimes (\psi'_2 \perp -\psi'_1)) = 2^{r+1}$. Осталось показать, что форма $\tau \otimes (\psi'_2 \perp -\psi'_1)$ анизотропна. Предположим противное. Тогда $a \in D(\tau \otimes \psi'_1) \cap D(\tau \otimes \psi'_2)$. Но тогда из предложения 2.3.3 следует, что φ_1 и φ_2 на самом деле $(r+1)$ -связанные, что противоречит выбору r . \square

2.4 Мультипликативные формы

2.4.1 Определение. Пусть V — конечномерное векторное пространство над k . Мы будем обозначать через $k(V)$ поле частных кольца $\bigoplus_{n \geq 0} S^n(V)$, где $S^n(V)$ — n -ая симметрическая степень V . После выбора базиса (e_1, \dots, e_n) в V поле $k(V)$ отождествляется с полем рациональных функций от переменных (e_1, \dots, e_n) . С точки зрения алгебраической геометрии $k(V)$ является полем функций аффинного многообразия \mathbb{V} такого, что $\mathbb{V}(k) = V^*$ — пространство, двойственное к V . В частности, если (V, q) — квадратичное пространство, то q можно считать элементом $S^2(V^*)$, то есть, элементом $k(V^*)$. Если (T_1, \dots, T_n) — базис, двойственный к (e_1, \dots, e_n) , то $k(V^*) \cong k(T_1, \dots, T_n)$. Очевидно, что $q = q(T_1, \dots, T_n) \in D(q_{k(V^*)})$.

2.4.2 Определение. Квадратичная форма φ на пространстве V называется **мультипликативной**, если для $a = (\varphi, 0) \in K^*$ и $b = (0, \varphi) \in K^*$ имеем $ab \in D(\varphi_K)$, где $K = k(V^* \times V^*)$. Пусть (T_1, \dots, T_N) — базис V^* и $K = k(U_1, \dots, U_n, V_1, \dots, V_n)$, где $U_i = (T_i, 0)$ и $V_i = (0, T_i)$. Тогда условие мультипликативности можно переформулировать так: найдутся $f_1, \dots, f_n \in K$ такие, что $\varphi(U_1, \dots, U_n)\varphi(V_1, \dots, V_n) = \varphi(f_1, \dots, f_n)$.

2.4.3 Теорема (Классификация анизотропных мультипликативных форм). Пусть φ — анизотропная квадратичная форма над k . Следующие условия эквивалентны:

1. φ мультипликативна.
2. Для всякого расширения K/k множество $D(\varphi_K)$ является подгруппой в K^* .
3. Для всякого чисто трансцендентного расширения K/k множество $D(\varphi_K)$ является подгруппой в K^* .
4. φ является формой Pfистера.

Доказательство. (4) \Rightarrow (2) — из теоремы 2.1.6, (2) \Rightarrow (1) и (2) \Rightarrow (3) — очевидно, (1) \Rightarrow (2) — из принципа подстановки (применительно к K ; заметим, что если q мультипликативна, то она остается мультипликативной после любого расширения k). Остается

доказать (3) \Rightarrow (4). Пусть $n = \dim(q)$ и m — наибольшее целое, для которого q содержит некоторую подформу, изометричную m -форме Пфистера. Покажем, что $n = 2^m$. Предположим противное: $n > 2^m$, $\varphi \leq q$ и $\varphi \in P_m(k)$. Запишем $q \cong \varphi \perp q'$. Пусть $K = k(V^* \times V^*)$, где V — пространство, на котором задана форма φ . По (3) \Rightarrow (1), примененному к φ , есть тождество $\varphi(U)\varphi(V) = \varphi(f)$, где $f \in K \otimes_k V$. Пусть $a \in D(q')$. Над K имеет место

$$0 \neq \varphi(U) + a\varphi(V) = \frac{\varphi(f)}{\varphi(V)} + a\varphi(V) = \varphi(V) \left(\varphi \left(\frac{f}{\varphi(V)} \right) + a \right).$$

Оба множителя справа лежат в $D(q_K)$. Из мультипликативности q следует, что $\varphi(U) + a\varphi(V) \in D(q_K)$. Отсюда по теореме о подформе $q \geq \varphi \perp a\varphi \in P_{m+1}(k)$, что противоречит максимальнойности m . \square

Таким образом, если n — степень двойки, то имеется тождество

$$(x_1^2 + \dots + x_n^2)(y_1^2 + \dots + y_n^2) = z_1^2 + \dots + z_n^2,$$

где z_1, \dots, z_n — рациональные функции от $x_1, \dots, x_n, y_1, \dots, y_n$. На самом деле, можно доказать, что существуют такие функции z_i , линейные по y , то есть $z_i = \sum_j t_{ij}(x_1, \dots, x_n)y_j$, где $t_{ij} \in k(x_1, \dots, x_n)$.

2.4.4 Определение. Квадратичная форма φ называется **round-формой**, если $D_k(\varphi) = G_k(\varphi)$.

2.4.5 Определение. Обозначим через $W_t(k)$ подгруппу кручения группы $W(k)$: $W_t(k) = \{w \in W(k) \mid l \times w = 0 \text{ для некоторого } l \in \mathbb{N}\}$. Для $w \in W_t(k)$ наименьшее l такое, что $l \times w = 0$, называется **порядком** w .

2.4.6 Теорема. $W_t(k)$ является 2-группой, то есть порядок любого элемента $w \in W_t(k)$ является степенью двойки.

Доказательство. Пусть $w' \in W_t(k)$ имеет порядок $l = 2^r s$, где s нечетно и $s > 1$. Тогда $w = 2^r w'$ имеет порядок s . Выберем анизотропную квадратичную форму $\varphi = \langle a_1, \dots, a_m \rangle$, представителем которой является w . Тогда s — наименьшее положительное число, для которого $s \times \varphi \sim 0$.

Возьмем теперь любую степень двойки n , большую m , и рассмотрим форму $\psi = \langle 1, -\sum_1^n x_i^2 \rangle$ над $k(x) = k(x_1, \dots, x_n)$, где x_i — набор переменных над k . Нетрудно видеть, что $n \times \psi$ — изотропная форма Пфистера, поэтому $n \times \psi \sim 0$ над $k(x)$. Из $s \times \varphi \sim 0$ и $n \times \psi \sim 0$ получаем, что $s \times (\varphi \otimes \psi) \sim 0$ и $n \times (\varphi \otimes \psi) \sim 0$, откуда $\varphi \otimes \psi \sim 0$, поскольку s и n взаимно просты. Это означает, что $\varphi \cong (\sum_1^n x_i^2) \varphi$ над $k(x)$. В частности, φ представляет элемент $a_1 \sum_1^n x_i^2$ над $k(x)$. Но $a_1 \sum_1^n x_i^2$ — это общий элемент квадратичной формы $n \times \langle a_1 \rangle$. Поскольку φ анизотропна над k , из теоремы 1.4.3 о подформе теперь следует, что φ содержит $n \times \langle a_1 \rangle$, поэтому $m = \dim \varphi \geq n$ — противоречие. \square

2.4.7 Замечание. С помощью такого же типа рассуждений (со ссылкой на теорему о подформе) нетрудно доказать (упражнение!), что, скажем, выражение $x^2 + y^2 + z^2 + t^2$ не может быть представлено в виде суммы *трех* квадратов рациональных функций от переменных x, y, z, t .

2.4.8 Теорема. Пусть $\varphi \leq \psi$ — две формы Пфистера. Тогда существует форма Пфистера τ такая, что $\psi = \varphi \otimes \tau$.

Доказательство. Доказывается аналогично; индукция по $\dim \psi - \dim \varphi$. Пусть $\psi = \varphi \perp q$ и $a \in D(q)$; нетрудно показать, что $\varphi \otimes \langle 1, a \rangle \leq \psi$. \square

2.4.9 Определение. Пусть (V, q) — квадратичное пространство размерности n и Q — матрица формы q в некотором базисе. **Дискриминантом** формы q называется элемент $d(q) = (-1)^{\frac{n(n-1)}{2}} \det Q \in k^*/(k^*)^2$. Он не зависит от выбора базиса в V .

2.4.10 Утверждение. Отображение $e_0: W(k) \rightarrow \mathbb{Z}/2$, $e_0(\varphi) = \dim(\varphi) \bmod 2$, является сюръективным гомоморфизмом колец. Ядро этого гомоморфизма — фундаментальный идеал IF , поэтому $W(k)/IF \cong \mathbb{Z}/2$.

Доказательство. См. определение 2.1.1. \square

Множитель $(-1)^{\frac{n(n-1)}{2}}$ позволяет дискриминанту быть корректно определенным на кольце Витта — дискриминант не меняется при замене формы на эквивалентную. Заметим, что при этом дискриминант не является гомоморфизмом: вообще говоря, неверно, что $d(q_1 \perp q_2) = d(q_1)d(q_2)$. Но если ограничиться рассмотрением форм четной размерности (то есть представителей элементов из IF), то оказывается, что дискриминант является гомоморфизмом, поскольку для формы φ четной размерности $d(\varphi) = (-1)^{\frac{\dim(\varphi)}{2}} \det(\varphi)$. Чуть позднее (теорема 3.1.2) мы докажем, что дискриминант отождествляет IF/I^2F с $k^*/(k^*)^2$.

2.4.11 Определение. Степени фундаментального идеала определяют фильтрацию кольца Витта. Пусть $\overline{I^n F} = I^n F / I^{n+1} F$ (при этом $I^0 F = W(k)$). Построим абелеву группу $gr(W) = \overline{I^0 F} \oplus \overline{I^1 F} \oplus \overline{I^2 F} \oplus \dots$ и введем на этой группе операцию умножения, индуцированную умножением в кольце Витта $W(k)$: для $\bar{x} \in \overline{I^m F}$, $\bar{y} \in \overline{I^n F}$ элемент $\bar{x} \cdot \bar{y} = \overline{x \cdot y} \in \overline{I^{m+n} F}$ корректно определен. Полученное кольцо называется **градуированным кольцом Витта** поля k .

Оказывается, что $\overline{I^2 F}$ отождествляется с 2-кручением группы Брауэра — классического объекта. В ближайшее время мы построим по форме q центральную простую алгебру (Клиффорда), и сопоставление форме класса этой алгебры в группе Брауэра поля k окажется гомоморфизмом $e_2: I^2 F \rightarrow Br(k)$, который превратится в изоморфизм $\bar{e}_2: \overline{I^2 F} \rightarrow {}_2 Br(k)$.

3 К-теория Милнора

3.1 Элементарные инварианты

3.1.1 Утверждение. 1. Если $q = \langle a_1, \dots, a_n \rangle$, то $d_q = (-1)^{\frac{n(n-1)}{2}} a_1 \dots a_n$.

2. $d(q \perp q') = d_q d_{q'} (-1)^{nn'}$, где $n' = \dim q'$.

3. $d(q \perp \mathbb{H}) = d_q$.

4. $d(q \otimes q') = (d_q)^{n'} (d_{q'})^n$.

Доказательство. Легко. □

3.1.2 Теорема. Инвариант d индуцирует изоморфизм $IF/I^2F \rightarrow k^*/(k^*)^2$.

Доказательство. Из предыдущего предложения следует, что d является гомоморфизмом и $d|_{I^2F} = 1$. Значит, d индуцирует гомоморфизм $\bar{d}: IF/I^2F \rightarrow k^*/(k^*)^2$. Он сюръективен, поскольку $d(\langle 1, -a \rangle) = a$ для $a \in k^*/(k^*)^2$. Для доказательства инъективности предположим, что $q \in IF$ и $d(q) = 1$. Введем индукцию по $2n = \dim q$. Если $n = 1$, то $q = \langle a_1, a_2 \rangle$ и $a_2 = -a_1$ по модулю $(k^*)^2$, откуда $\varphi \cong a_1 \langle 1, -1 \rangle$ и $\tilde{\varphi} = 0$ в $W(k)$. Если $n > 1$, то $\varphi = \langle a_1, a_2, a_3 \rangle \perp \langle a_4, \dots, a_{2n} \rangle \sim \langle a_1, a_2, a_3, a_1 a_2 a_3 \rangle \perp \langle -a_1 a_2 a_3, a_4, \dots, a_{2n} \rangle$. Заметим, что $\langle a_1, a_2, a_3, a_1 a_2 a_3 \rangle \cong \langle a_1, a_2 \rangle \otimes \langle 1, a_1 a_3 \rangle \in I^2F$, размерность формы $\langle -a_1 a_2 a_3, a_4, \dots, a_{2n} \rangle$ равна $2(n-1)$, а дискриминант равен 1. Значит, она лежит в I^2F по предположению индукции, откуда $\varphi \in I^2F$. □

3.1.3 Следствие. 1. Если размерность формы q нечетна, то $q \equiv \langle d(q) \rangle \pmod{I^2F}$.

2. Если размерность формы q четна, то $q \equiv \langle 1, -d(q) \rangle \pmod{I^2F}$.

Доказательство. Очевидно. □

Можно явно описать расширение $\mathbb{Z}/2$ с помощью $k^*/(k^*)^2$, определенное $W(k)/I^2F$. Обозначим через $Q(k)$ множество $\mathbb{Z}/2 \otimes k^*/(k^*)^2$, снабженное следующей операцией:

$$(a, u) + (b, v) = (a + b, (-1)^{ab} uv).$$

3.1.4 Утверждение. Отображение $q \mapsto (\overline{\dim}(q), d(q))$ индуцирует изоморфизм

$$W(k)/I^2F \rightarrow Q(k).$$

Доказательство. Достаточно проверить, что это гомоморфизм; это напрямую следует из предложения 3.1.1. □

3.1.5 Определение. Пусть (V, q) — квадратичное пространство над k . Алгеброй Клиффорда $C(q)$ формы q называется фактор-алгебра тензорной алгебры $T(V)$ пространства V по двустороннему идеалу, порожденному элементами вида $v \otimes v - q(v)1$, $v \in V$.

Если $q = \langle a_1, \dots, a_n \rangle$ в ортогональном базисе (e_1, \dots, e_n) пространства V , то $C(q)$ можно описать как алгебру, порожденную элементами e_i с соотношениями $e_i^2 = a_i$ и $e_i e_j + e_j e_i = 0$ для $i \neq j$.

3.1.6 Утверждение (универсальное свойство $C(q)$). Если A — k -алгебра, $f: V \rightarrow A$ — гомоморфизм векторных пространств над k такой, что $f(v)^2 = q(v)$ для всех $v \in V$, то f единственным образом продолжается до гомоморфизма k -алгебр $\tilde{f}: C(V) \rightarrow A$.

Поскольку $T(V)$ является градуированной алгеброй и соотношения в $C(q)$ однородны по модулю 2, то алгебра $C(q)$ обладает естественной $\mathbb{Z}/2$ -градуировкой. Будем обозначать через $C_0(q)$ (соответственно $C_1(q)$) ее четную (соответственно нечетную) часть. Алгебру с $\mathbb{Z}/2$ -градуировкой еще называют **супералгеброй**.

3.1.7 Определение. Пусть A, B — две супералгебры над k . Градуированным тензорным произведением A и B называется супералгебра $A \hat{\otimes}_k B$ такая, что

- $A \hat{\otimes}_k B$ совпадает с $A \otimes_k B$ как векторное пространство;
- если $(a, a', b, b') \in A^2 \times B^2$ — однородны, то

$$(a \hat{\otimes} b)(a' \hat{\otimes} b') = (-1)^{|a'| |b|} a a' \hat{\otimes} b b';$$

- если $a \in A, b \in B$ однородны степеней i, j , то ab однороден степени $i + j$.

3.1.8 Утверждение. Если $\dim q = n$, то $\dim_k C(q) = 2^n$.

Если $(V_1, q_1), (V_2, q_2)$ — два квадратичных пространства над k , включения $V_i \hookrightarrow V_1 \otimes V_2 \hookrightarrow C(q_1 \perp q_2)$ вместе с универсальным свойством алгебры Клиффорда индуцируют гомоморфизмы алгебр $C(q_i) \rightarrow C(q_1 \perp q_2)$, которые являются и гомоморфизмами супералгебр. В $C(q_1 \perp q_2)$ выполнено $v_1 v_2 = -v_2 v_1$ для $(v_1, v_2) \in V_1 \times V_2$; эти гомоморфизмы продолжаются до гомоморфизма супералгебр $C(q_1) \hat{\otimes}_k C(q_2) \rightarrow C(q_1 \perp q_2)$.

3.1.9 Теорема. Этот гомоморфизм является изоморфизмом супералгебр.

Доказательство. Сюръективность очевидна; инъективность следует из предыдущего предложения и соображений размерности. \square

3.1.10 Следствие. Пусть q — квадратичная форма, $a \in k^*$ и $q' = \langle -a \rangle \perp q$. Тогда $C(q')$ изоморфна (как алгебра) $C_0(q')$.

Доказательство. $C(q') \cong C(\langle -a \rangle) \hat{\otimes}_k C(q)$, откуда

$$C(q') \cong C_0(\langle -a \rangle) \hat{\otimes}_k C(q) \oplus C_1(\langle -a \rangle) \hat{\otimes}_k C(q) = C(q) \oplus zC(q)$$

(изоморфизмы векторных пространств), где z — каноническая образующая $C_q(\langle -a \rangle)$, $z^2 = -a$. Отсюда $C_0(q') \cong C_0(q) \oplus zC_1(q)$. Остается отождествить последнее слагаемое с $C(q)$. Но z коммутирует с $C_0(q)$ и антикоммутирует с $C_1(q)$; в частности, $(zv)^2 =$

$zvzv = -z^2v^2 = \alpha q(v)$ для всех $v \in V$. Из универсального свойства алгебры Клиффорда теперь следует, что линейное отображение $V \rightarrow C_0(q) \oplus zC_1(q)$, $v \mapsto zv$ продолжается до гомоморфизма алгебр $C(\alpha q) \rightarrow C_0(q) \oplus zC_1(q)$. Очевидно, что этот гомоморфизм сюръективен, и биективен по соображениям размерности. \square

3.1.11 Следствие. $\dim C_0(q) = \dim C_1(q) = 2^{n-1}$.

3.2 Группа Брауэра

3.2.1 Определение. Пусть A — кольцо. A -модуль M называется **простым**, если у него нет подмодулей, кроме M и 0 . M называется **полупростым**, если он удовлетворяет следующим эквивалентным условиям:

1. M — сумма своих простых подмодулей;
2. M — прямая сумма простых модулей;
3. всякий подмодуль M выделяется прямым слагаемым.

3.2.2 Определение. Кольцо A называется **полупростым**, если оно удовлетворяет следующим эквивалентным условиям:

1. всякий левый A -модуль прост;
2. A прост как левый A -модуль;
3. всякий идеал A выделяется прямым слагаемым.

Полупростое кольцо A называется **простым**, если в нем нет двусторонних идеалов, отличных от 0 и A .

3.2.3 Теорема. *Всякое полупростое кольцо является прямым произведением конечного числа простых колец. Оно является простым тогда и только тогда, когда всякий простой модуль над ним изоморфен ему. Всякое простое кольцо изоморфно алгебре матриц над телом.*

3.2.4 Определение. Алгебру над полем F будем называть **простой F -алгеброй**, если она конечномерна над F и является простым кольцом. F -алгебра называется **центральной**, если ее центр совпадает с F .

3.2.5 Определение. Пусть A — F -алгебра, B — подалгебра A . **Централизатор B в A** — это $B' = \{a \in A \mid ab = ba \ \forall b \in B\}$. B' является подалгеброй в A .

3.2.6 Теорема. 1. Пусть K/F — расширение полей. F -алгебра A является **центральной простой** тогда и только тогда, когда K -алгебра $A_K := K \otimes_F A$ является **центральной простой**.

2. Пусть A — центральная простая F -алгебра.

(a) Размерность A над F является точным квадратом.

(b) Пусть B — простая F -подалгебра A , B' — ее централизатор в A . Тогда

i. B' проста.

ii. $[B : F][B' : F] = [A : F]$.

iii. централизатор B' в A совпадает с B .

iv. если B центральна, то B' центральна и гомоморфизм $B \otimes_F B' \rightarrow A$ является изоморфизмом.

(c) Пусть B — центральная простая F -алгебра. Тогда алгебра $A \otimes_F B$ является центральной простой.

(d) Пусть A^0 — алгебра, противоположная к A . Тогда существует канонический изоморфизм $A \otimes_F A^0 \cong \text{End}_F(A)$.

3.2.7 Определение. Пусть F — поле. Две конечномерные центральные простые F -алгебры A, B называются **подобными**, если выполняются следующие эквивалентные условия:

1. Для некоторого тела D с центром F и целых a, b выполняется $A \cong M_a(D)$ и $B \cong M_b(D)$.
2. Найдутся целые a, b такие, что $M_b(A) \cong M_a(B)$.
3. Категории левых A -модулей и левых B -модулей эквивалентны.

Будем говорить, что A **нейтральна**, если A подобна F .

Из третьего условия видно, что это подобие является отношением эквивалентности.

3.2.8 Теорема. 1. Совокупность классов подобия центральных простых F -алгебр образует множество $\text{Br}(F)$.

2. Тензорное произведение снабжает $\text{Br}(F)$ структурой группы; нейтральным элементом является класс нейтральных алгебр; обратный к классу алгебры A — это класс противоположной алгебры A^0 ; эта группа коммутативна.

3. Если K/F — расширение полей, то расширение скаляров индуцирует гомоморфизм $\text{Br}(F) \rightarrow \text{Br}(K)$.

Доказательство. Очевидно. □

3.2.9 Замечание. Группа $\text{Br}(F)$ называется **группой Брауэра** поля F .

3.2.10 Примеры. 1. Если поле F алгебраически замкнуто, то $\text{Br}(F) = 0$.

2. $\text{Br}(\mathbb{R}) \cong \mathbb{Z}/2$; эту группу порождает класс кватернионов Гамильтона $\begin{pmatrix} -1 & -1 \\ & \mathbb{R} \end{pmatrix}$

$$3. \operatorname{Br}(\mathbb{F}_q) = 0.$$

Заметим, что $\langle\langle a \rangle\rangle \perp \langle\langle b \rangle\rangle \equiv \langle\langle ab \rangle\rangle \pmod{I^2 F}$ (см. лемму 2.1.4). Кроме того, $\langle\langle x, 1 - x \rangle\rangle \cong \langle\langle 1, \dots \rangle\rangle \sim 0$. Рассмотрим абелеву группу, порожденную символами $\{a_1, \dots, a_n\}$, где $a_i \in k^*$, с соотношениями

$$1. \{ \dots, a, \dots \} + \{ \dots, b, \dots \} = \{ \dots, ab, \dots \};$$

$$2. \{ \dots, x, \dots, 1 - x, \dots \} = 0.$$

Введем на этой группе умножение так:

$$\{a_1, \dots, a_n\} \cdot \{b_1, \dots, b_m\} = \{a_1, \dots, a_n, b_1, \dots, b_m\}.$$

Получится градуированное кольцо, которое обозначается через $K_*^M(k)$ и называется К-теорией Милнора поля k . Эквивалентно,

$$K_*^M(k) \cong T(k^*)/\chi \otimes (1 - \chi)$$

— фактор-алгебра тензорной алгебры (над \mathbb{Z}) мультипликативной группы поля k .

3.2.11 Определение. Пусть A — центральная простая F -алгебра. Расширение K/F называется **нейтрализующим полем**, если A_K нейтральна.

3.2.12 Теорема. Пусть A — центральная простая F -алгебра; E/F — конечное расширение. E является нейтрализующим полем для A тогда и только тогда, когда существует центральная простая F -алгебра B , подобная A , такая, что E является максимальной коммутативной подалгеброй в B . Более того, следующие утверждения эквивалентны:

1. E — максимальная коммутативная подалгебра в B .

2. E совпадает со своим централизатором.

$$3. [B : F] = [E : F]^2.$$

3.2.13 Теорема (Сколем–Нетер). Пусть A — центральная простая F -алгебра, B, C — две простые подалгебры A и $f: B \rightarrow C$ — изоморфизм F -алгебр. Тогда существует обратимый $a \in A$ такой, что $f(x) = axa^{-1}$ для всех $x \in B$. В частности, любой автоморфизм алгебры A является внутренним.

3.2.14 Определение. Пусть A — центральная простая F -алгебра. Запишем $A = M_n(D)$ для некоторого тела D .

1. **Степень A** — это целое число $\sqrt{[A : F]}$.

2. **Индекс A** — это целое число $\sqrt{[D : F]}$.

3. Экспонента A — это порядок класса алгебры A в $\text{Br}(F)$.

3.2.15 Утверждение. Для всякой центральной простой F -алгебры A

1. экспонента A делит ее индекс, а индекс делит ее степень;
2. индекс и экспонента A состоят из одинаковых простых делителей.

3.2.16 Утверждение. Пусть A — центральная простая F -алгебра; K/F — расширение полей.

1. $\text{ind}(A)$ делится на $\text{ind}(A_K)$.
2. Если $[K : F] = n < +\infty$, то $\text{ind}(A)/\text{ind}(A_K)$ является делителем n .
3. Если K/F — чисто трансцендентное расширение, то $\text{ind}(A_K) = \text{ind}(A)$.

3.2.17 Лемма (Альберт). Пусть F — поле характеристики не 2, D — конечномерное центральное тело над F и $a \in F^* \setminus (F^*)^2$. Пусть $E = F(\sqrt{a})$. Тогда D_E не является телом тогда и только тогда, когда D содержит подполе, изоморфное E .

Доказательство. D содержит подполе, изоморфное E тогда и только тогда, когда a является квадратом в D . Тогда

$$(1 \otimes x - \sqrt{a} \otimes 1)(1 \otimes x + \sqrt{a} \otimes 1) = 0,$$

поэтому D_E содержит делители нуля и не может быть телом. Обратно, если D_E — не тело, то найдутся $s, t, u, v \in D$, не все равные нулю, такие, что $(1 \otimes s + \sqrt{a} \otimes t)(1 \otimes u + \sqrt{a} \otimes v) = 0$. Тогда $s, u \neq 0$ и, после домножения слева на s^{-1} и справа на u^{-1} , можно считать, что $s = u = 1$. Тогда $0 = (1 + t\sqrt{a})(1 + v\sqrt{a}) = 1 + tvd + (t + v)\sqrt{a}$. Отсюда $v = -t$ и $1 - dt^2 = 0$; теперь видно, что $(t^{-1})^2 = a$. \square

3.2.18 Утверждение. Пусть A — центральная простая алгебра над F , K — подполе в A и $B = K'$. Тогда A_K подобна B .

3.2.19 Определение. Пусть $a, b \in F^*$. Алгеброй кватернионов, построенной по паре (a, b) , называется F -алгебра $\left(\begin{smallmatrix} a & b \\ F & \end{smallmatrix}\right)$ с базисом $(1, i, j, k)$ такая, что $i^2 = a, j^2 = b, ij = -ji = k$.

3.2.20 Замечание. Алгебра $\left(\begin{smallmatrix} a & b \\ F & \end{smallmatrix}\right)$ совпадает с алгеброй $C(\langle a, b \rangle)$ (если забыть про структуру супералгебры на этой алгебре Клиффорда).

3.2.21 Теорема. Пусть $a, b \in F^*$. Следующие условия эквивалентны:

1. Квадратичная форма $\langle 1, -a, -b \rangle$ изотропна.
2. Квадратичная форма $\langle\langle a, b \rangle\rangle$ изотропна.
3. Алгебра $Q = \left(\begin{smallmatrix} a & b \\ F & \end{smallmatrix}\right)$ не является телом.

4. Алгебра Q изоморфна $M_2(F)$.

В частности, Q — центральная простая алгебра над F степени 2.

Доказательство. (1) \iff (2) — нетрудно. (2) \iff (3): заметим, что если $x, y, z, t \in F$, то $(x + yi + zj + tk)(x - yi - zj - tk) = x^2 - ay^2 - bz^2 + abt^2 = q(x, y, z, t)$, где $q = \langle\langle a, b \rangle\rangle$. Значит, если q изотропна, то в Q есть делители нуля, а если q анизотропна, то всякий элемент $x + yi + zj + tk \in Q \setminus \{0\}$ обратим; обратный к нему равен $(x - yi - zj - tk)/q(x, y, z, t)$.

Очевидно, что (4) \Rightarrow (3). Покажем что (3) \Rightarrow (4). Предположим, что $a = 1$, $b = -1$ и построим изоморфизм $\begin{pmatrix} a & b \\ F & F \end{pmatrix} \cong M_2(F)$. Пусть $(E_{ij})_{i,j \in \{0,1\}}$ — канонический базис $\text{End}_F(F \hat{\otimes} F)$. Тогда нужный изоморфизм устанавливается так:

$$1 \mapsto E_{00} + E_{11}$$

$$i \mapsto E_{01} + E_{10}$$

$$j \mapsto E_{01} - E_{10}$$

$$k \mapsto E_{11} - E_{00}$$

Заметим, что $\begin{pmatrix} a & b \\ F & F \end{pmatrix} \cong \begin{pmatrix} as^2 & bt^2 \\ F & F \end{pmatrix}$ для $s, t \in F^*$. Значит, для произвольных a, b существует расширение E/F такое, что $Q_E \cong \begin{pmatrix} 1 & -1 \\ E & E \end{pmatrix}$. Значит, и Q является центральной простой и, очевидно, степени 2. Если Q не является телом, то она обязана быть изоморфна $M_2(F)$. \square

Верно и обратное:

3.2.22 Теорема. *Всякая центральная простая F -алгебра A степени 2 является алгеброй кватернионов.*

Доказательство. Можно считать, что A — тело. Пусть $E \subset A$ — максимальное коммутативное подтело A . Тогда $E = F(\sqrt{a})$ для подходящего $a \in F^*$. Возьмем $i \in E$ такое, что $i^2 = a$. Рассмотрим внутренний автоморфизм σ алгебры A , определенный i : видно, что $\sigma^2 = 1$. Если i не централен, то $\sigma \neq 1$; поэтому у σ есть собственное число, равное -1 , то есть, найдется $j \in A$ такой, что $\sigma(j) = -j$. Стало быть, $ij = -ji$. Легко видеть, что j не централен, поэтому j порождает максимальное коммутативное подтело K в A . Автоморфизм σ переводит K в себя и его ограничение на F тривиально; поэтому множество неподвижных точек $\sigma|_K$ совпадает с F . В частности, $j^2 = b \in F$. Наконец, положим $k = ij$. Если $x + yi + zj + tk = 0$ — какая-то нетривиальная линейная комбинация, то после сопряжения при помощи i, j и k получим соотношения

$$x + yi - zj - tk = 0$$

$$x - yi + zj - tk = 0$$

$$x - yi - zj + tk = 0$$

откуда $x = y = z = t = 0$. \square

3.2.23 Лемма. Для $a, b \in F^*$ обозначим через (a, b) класс алгебры $\left(\begin{smallmatrix} a & b \\ & F \end{smallmatrix}\right)$ в $\text{Br}(F)$. Тогда

$$\begin{aligned}(a, b) &= (b, a) \\ (a^2, b) &= 0 \\ (a, 1-a) &= 0 \quad (a \neq 1) \\ (a, -a) &= 0 \\ (a, bb') &= (a, b) + (a, b')\end{aligned}$$

Доказательство. Первое свойство очевидно. Следующие три получаются из теоремы 3.2.21. Для доказательства последнего построим изоморфизм

$$\varphi: \left(\begin{smallmatrix} a & b \\ & F \end{smallmatrix}\right) \times_F \left(\begin{smallmatrix} a & b' \\ & F \end{smallmatrix}\right) \xrightarrow{\sim} M_2 \left(\left(\begin{smallmatrix} a & bb' \\ & F \end{smallmatrix}\right) \right).$$

Пусть $(1, i, j, k)$, $(1, i', j', k')$, $(1, i'', j'', k'')$ — соответственно канонические базисы алгебр $\left(\begin{smallmatrix} a & b \\ & F \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} a & b' \\ & F \end{smallmatrix}\right)$ и $\left(\begin{smallmatrix} a & bb' \\ & F \end{smallmatrix}\right)$. Вот образы некоторых элементов при нашем изоморфизме:

$$\begin{aligned}\varphi(i \otimes 1) &= \begin{pmatrix} i'' & 0 \\ 0 & i'' \end{pmatrix} & \varphi(1 \otimes i') &= \begin{pmatrix} -i'' & 0 \\ 0 & i'' \end{pmatrix} \\ \varphi(j \otimes 1) &= \begin{pmatrix} 0 & -j'' \\ -b'^{-1}j'' & 0 \end{pmatrix} & \varphi(1 \otimes j') &= \begin{pmatrix} 0 & b' \\ 1 & 0 \end{pmatrix} \\ \varphi(k \otimes 1) &= \begin{pmatrix} 0 & -k'' \\ -b'^{-1}k'' & 0 \end{pmatrix} & \varphi(1 \otimes k') &= \begin{pmatrix} 0 & -b'i'' \\ i'' & 0 \end{pmatrix}.\end{aligned}$$

Необходимо лишь проверить, что φ является гомоморфизмом алгебр; любой гомоморфизм из одной простой алгебры в другую является инъективным, и сюръективность вытекает из соображений размерности. \square

3.2.24 Лемма (Альберт). Пусть $a, b, c, d \in F^*$ таковы, что $(a, b) = (c, d)$. Тогда существует $e \in F^*$ такой, что $(a, b) = (a, e) = (c, e) = (c, d)$.

Доказательство. Пусть $D = \left(\begin{smallmatrix} a & b \\ & F \end{smallmatrix}\right)$ и D_0 — векторное F -подпространство в D , состоящее из элементов следа 0 (ортогональных к 1 по отношению к приведенной норме); тогда $\dim D_0 = 3$. Ограничение q на D_0 совпадает с отображением $x \mapsto -x^2$. По предположению, найдутся $\alpha, \beta, \gamma, \delta \in D_0$ такие, что

$$\begin{aligned}\alpha^2 &= a, \beta^2 = b, \alpha\beta + \beta\alpha = 0 \\ \gamma^2 &= c, \delta^2 = d, \gamma\delta + \delta\gamma = 0.\end{aligned}$$

Иными словами, (α, β) и (γ, δ) — пары ортогональных векторов. Но $\dim D_0 = 3$, поэтому найдется $\varepsilon \in D_0$, ортогональный к α и γ . Тогда можно взять $e = \varepsilon^2$. \square

3.3 Группа Брауэра–Уолла

В этом разделе мы определим аналог группы Брауэра для супералгебр. Пусть A — супералгебра над F .

3.3.1 Определение. Супералгебра A называется **простой**, если она не имеет градуированных двусторонних идеалов, кроме 0 и A .

3.3.2 Определение. (Градуированным) **центром** супералгебры A называется $\hat{Z}(A) = Z_0(A) \oplus Z_1(A)$, где $Z_i(A) = \{a \in A_i \mid \forall x \in A_j, ax = (-1)^{ij}xa, j = 0, 1\}$. Супералгебра A над F называется **центральной**, если $\hat{Z}(A) = (F, 0)$.

3.3.3 Примеры. 1. Пусть A — алгебра над F . Определим супералгебру $i(A)$ так: $i(A)_0 = A$, $i(A)_1 = 0$. Если A центральная простая алгебра, то $i(A)$ — центральная простая супералгебра.

2. Пусть $V = V_0 \hat{\oplus} V_1$ — конечномерное векторное суперпространство над F . Алгебра $\text{End}_F(V)$ допускает естественную градуировку, в которой эндоморфизм u является четным, если $u(V_i) \subset V_i$ и нечетным, если $u(V_i) = V_{i+1}$ для всех $i \in \mathbb{Z}/2$. Полученная супералгебра является центральной простой.

3. Пусть $a \in F^*$. Супералгебра $C(\langle a \rangle)$ изоморфна (как алгебра без градуировки) $F[t]/(t^2 - a)$. Ее градуировка определяется однозначно из условия $|t| = 1$. Нетрудно видеть, что эта супералгебра является центральной простой.

3.3.4 Утверждение. Если A, B — центральные простые F -супералгебры, то $A \hat{\otimes}_F B$ — тоже центральная простая супералгебра.

3.3.5 Теорема. Для всякой невырожденной квадратичной формы q супералгебра $C(q)$ над F является центральной простой.

Доказательство. Приведение формы к диагональному виду с учетом теоремы 3.1.9 и предложения 3.3.4 сводит задачу к случаю $\dim q = 1$, который приведен в примере 3.3.3 (3). \square

3.3.6 Определение. Две F -супералгебры A, B называются **подобными**, если существуют два векторных суперпространства V, W над F такие, что $A \hat{\otimes} \text{End}_F(V) \cong B \hat{\otimes} \text{End}_F(W)$ (см. пример 3.3.3 (2)). Обозначение: $A \sim B$.

Пусть A — супералгебра. **Противоположная супералгебра** A^* определяется так: как векторное пространство $A^* = \{a^* \mid a \in A\}$, градуировка вводится так, что $A_i^* = \{a^* \mid |a| = i\}$, а произведение выглядит так: $a^*b^* = (-1)^{|a||b|}(ba)^*$ для однородных a, b .

3.3.7 Теорема. Отношения подобия является отношением эквивалентности на множестве центральных простых F -супералгебр, совместимым с градуированным тензорным произведением. Полугруппа классов эквивалентности является коммутативной группой и называется **группой Брауэра–Уолла** поля F и обозначается через $BW(F)$. Если A — центральная простая F -супералгебра, класса

$\langle A \rangle \in BW(F)$, то представителем класса $-\langle A \rangle$ является супералгебра A^* , противоположная к A .

Доказательство. Для проверки коммутативности $BW(F)$ заметим, что если A и B — супералгебры над F , то имеется изоморфизм F -супералгебр $A \hat{\otimes} B \xrightarrow{\sim} B \hat{\otimes} A$, задаваемый так: $a \hat{\otimes} b \mapsto (-1)^{|a||b|} b \hat{\otimes} a$ для однородных a, b . \square

3.3.8 Утверждение. 1. Имеется изоморфизм $C(\mathbb{H}) \cong \text{End}_F(F \hat{\otimes} F)$.

2. Если $a, b, c \in F^*$, то

$$(a) \ C(\langle ac, bc \rangle) \hat{\otimes} i \left(\begin{pmatrix} ac & bc \\ F & \end{pmatrix} \right) \cong C(\langle a, b \rangle) \hat{\otimes} i \left(\begin{pmatrix} a & b \\ F & \end{pmatrix} \right);$$

$$(b) \ C(\langle\langle a, b \rangle\rangle) \sim i \left(\begin{pmatrix} a & b \\ F & \end{pmatrix} \right);$$

$$(c) \ C(\langle\langle a, b, c \rangle\rangle) \sim 1.$$

Доказательство. Заметим, что все участвующие в формулировке супералгебры являются центральными простыми. Поэтому для проверки изоморфизма достаточно построить гомоморфизм и установить совпадение размерностей; тогда построенный гомоморфизм будет инъективным в силу простоты и сюръективным из соображений размерности.

1. Пусть (e_1, e_2) — канонический базис гиперболической плоскости $\mathbb{H} = \langle 1, -1 \rangle$. Тогда в $C(\mathbb{H})$ есть базис $(1, e_1, e_2, e_1 e_2)$ и $|e_1| = |e_2| = 1$, $e_1^2 = 1$, $e_2^2 = -1$, $e_1 e_2 = -e_2 e_1$. Супералгебра $\text{End}_F(F \hat{\otimes} F)$ обладает базисом $(E_{ij})_{i,j \in \{0,1\}}$ с $|E_{00}| = |E_{11}| = 0$ и $|E_{01}| = |E_{10}| = 1$. Можно проверить, что искомый изоморфизм индуцируется отображением $1 \mapsto E_{00} + E_{11}$, $e_1 \mapsto E_{01} + E_{10}$, $e_2 \mapsto E_{01} - E_{10}$.
2. Первое тождество сводится к случаю $ac = 1$. Таким образом, достаточно построить гомоморфизм супералгебр

$$C(\langle 1, ab \rangle) \hat{\otimes} i(M_2(F)) \xrightarrow{\sim} C(\langle a, b \rangle) \hat{\otimes} \left(\begin{pmatrix} a & b \\ F & \end{pmatrix} \right).$$

Запишем $M_2(F)$ как алгебру кватернионов с базисом $(1, i, j, ij)$, в котором $i^2 = a$, $j^2 = 1$, $ij = -ji$. Пусть $(1, i', j', i'j')$ — канонический базис алгебры $\begin{pmatrix} a & b \\ F & \end{pmatrix}$, в котором $i'^2 = a$, $j'^2 = b$, $i'j' = -j'i'$. Пусть, наконец, (e_1, e_2) (соответственно (e'_1, e'_2)) — канонический ортогональный базис формы $\langle 1, ab \rangle$ (соответственно $\langle a, b \rangle$). Тогда в $C(\langle 1, ab \rangle)$ (соответственно $C(\langle a, b \rangle)$) появляется базис $(1, e_1, e_2, e_1 e_2)$ с $e_1^2 = 1$, $e_2^2 = ab$, $e_1 e_2 = -e_2 e_1$ (соответственно $(1, e'_1, e'_2, e'_1 e'_2)$ с $e_1'^2 = a$, $e_2'^2 = b$, $e'_1 e'_2 = -e'_2 e'_1$). Можно проверить, что отображения

$$e_1 \hat{\otimes} 1 \mapsto e'_1 \hat{\otimes} i'^{-1}$$

$$e_2 \hat{\otimes} 1 \mapsto e'_2 \hat{\otimes} i'$$

$$1 \hat{\otimes} i \mapsto 1 \hat{\otimes} i'$$

$$1 \hat{\otimes} j \mapsto e'_1 e'_2 \hat{\otimes} (i'j')^{-1}$$

индуцируют требуемый гомоморфизм. Наконец, остальные два пункта следуют из уже доказанного. □

3.3.9 Следствие. *Отображение $q \mapsto C(q)$ индуцирует гомоморфизм*

$$C: W(F)/I^3F \rightarrow BW(F).$$

Доказательство. По теореме 3.3.5 всякая невырожденная форма q определяет элемент $\langle C(q) \rangle \in BW(F)$, и по теореме 3.1.9 имеем $\langle C(q \perp q') \rangle = \langle C(q) \rangle + \langle C(q') \rangle$. Остается применить предложение 3.3.8. □

Пусть $A = A_0 \oplus A_1$ — центральная простая F -супералгебра. Возможны два случая:

- F -алгебра A является простой (неградуированной) алгеброй. Тогда A_0 полупроста и ее центр является этальной F -алгеброй ранга 2. В этом случае говорят, что A имеет **четный тип**.
- A не центральна как F -алгебра. Тогда A полупроста и ее центр $Z(A)$ является этальной F -алгеброй ранга 2, а A_0 — центральная простая F -алгебра. Кроме того, A_0 модуль A_1 изоморфен A_0 . В этом случае говорят, что A имеет **нечетный тип**.

Определим отображение

$$\begin{aligned} \varphi: BW(F) &\rightarrow \mathbb{Z}/2 \times F^*/(F^*)^2 \times \text{Br}(F) \\ \langle A \rangle &\mapsto (\varepsilon(A), \delta(A), b(A)) \end{aligned}$$

следующим образом:

- $\varepsilon(A) = \begin{cases} 1, & \text{если } A \text{ нечетного типа;} \\ 0, & \text{если } A \text{ четного типа.} \end{cases}$
- $\delta(A) = \begin{cases} d(Z(A)), & \text{если } A \text{ нечетного типа;} \\ d(Z(A_0)), & \text{если } A \text{ четного типа,} \end{cases}$

где через $d(E)$ обозначается дискриминант этальной F -алгебры E .

- $b(A) = \begin{cases} [A_0], & \text{если } A \text{ нечетного типа;} \\ [A], & \text{если } A \text{ четного типа,} \end{cases}$

3.3.10 Теорема. 1. *Отображение φ является биекцией.*

2. *ε является гомоморфизмом.*

3. *Пусть $BW^{(1)}(F)$ — ядро ε . Ограничение δ на $BW^{(1)}(F)$ является гомоморфизмом.*

4. *Пусть $BW^{(2)}(F)$ — ядро δ . Тогда $BW^{(2)}(F) = i(B(F))$ и ограничение b на $BW^{(2)}(F)$ является обратным к i .*

5. Отображение $\langle A \rangle \mapsto (\varepsilon(A), \delta(A))$ индуцирует изоморфизм

$$BW(F)/BW^{(2)}(F) \rightarrow Q(F),$$

где $Q(F)$ — группа, определенная перед предложением 3.1.4.

6. Групповой закон, индуцированный на $\mathbb{Z}/2 \times F^*/(F^*)^2 \times B(F)$ переносом структуры посредством отображения φ , записывается так:

$$(m, a, x) + (n, b, y) = (m + n, (-1)^{mn} ab, x + y + ((-1)^{m(n+1)} a, (-1)^{(m+1)n} b)),$$

где через (u, v) обозначается класс алгебры кватернионов $\begin{pmatrix} u & v \\ & \end{pmatrix}_F$ в $\text{Br}(F)$.

3.4 Когомологии Галуа

3.4.1 Определение. Пусть G — конечная группа. (**Левым**) G -модулем называется абелева группа A , снабженная левым действием группы G , то есть гомоморфизмом $\varphi: G \rightarrow \text{Aut}(A)$. Если A записывается аддитивно, то для $(g, a) \in G \times A$ мы будем обозначать $\varphi(g)(a)$ через ga . При этом

$$g(a + b) = ga + gb,$$

$$(gh)a = g(ha).$$

3.4.2 Замечания.

Можно определить правое действие G на A как *анти-гомоморфизм* из G в $\text{Aut}(A)$; если A записывается аддитивно, то при этом $(g, a) \mapsto ag$. Задание левого и правого действия G на A эквивалентно: если φ — левое действие, то $g \mapsto \varphi(g)^{-1}$ — правое, и наоборот.

Если A записывается мультипликативно, то левое (соответственно правое) действие удобнее записывать как $(g, a) \mapsto {}^g a$ (соответственно $(g, a) \mapsto a^g$) для избежания конфликта с записью умножения в A .

Если $f: H \rightarrow G$ — гомоморфизм групп, то на G -модуле A появляется структура H -модуля с помощью определения $ha = f(h)a$.

3.4.3 Определение. Пусть G — конечная группа, A — левый G -модуль с аддитивной записью. Определим **коцепной комплекс** G со значениями в A :

$$0 \rightarrow C^0(G, A) \xrightarrow{d^0} C^1(G, A) \xrightarrow{d^1} \dots \xrightarrow{d^{n-1}} C^n(G, A) \xrightarrow{d^n} \dots$$

где $C^n(G, A)$ — множество всех отображений из G^n в A и

$$\begin{aligned} d^n f(g_1, \dots, g_{n+1}) &= g_1 f(g_2, \dots, g_{n+1}) \\ &+ \sum_{j=1}^n (-1)^j f(g_1, \dots, g_j g_{j+1}, \dots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \dots, g_n). \end{aligned}$$

Элемент $f \in C^n(G, A)$ называется n -коцепью G со значениями в A . Если $d^n f = 0$, f называется n -коциклом; подгруппа n -коциклов обозначается через $Z^n(G, A)$. Если $f \in \text{Im } d^{n-1}$, f называется n -кограницей; подгруппа n -кограниц обозначается через $B^n(G, A)$.

3.4.4 Примеры.

0-коцикл — это элемент $A^G := \{a \in A \mid ga = a \forall g \in G\}$.

1-коцикл — это отображение $f: G \rightarrow A$ такое, что $f(gh) = f(g) + gf(h)$. Такое отображение называется **скрещенным гомоморфизмом**.

2-коцикл — это отображение $f: G \times G \rightarrow A$ такое, что

$$f(g, h) + f(gh, k) = fg(h, k) + f(g, hk).$$

Такое f называется **системой факторов**.

3.4.5 Лемма. Если $n > 0$, то $d^{n+1}d^n = 0$; иными словами, $B^n(G, A) \subset Z^n(G, A)$.

Доказательство. Простое вычисление. □

3.4.6 Определение. n -ой группой когомологий G со значениями в A называется фактор-группа $H^n(G, A) = Z^n(G, A)/B^n(G, A)$.

3.4.7 Утверждение. 1. Функтор $(G, A) \mapsto H^n(G, A)$ ковариантен по A и контравариантен по G . Если $f: H \rightarrow G$ — гомоморфизм групп, обозначим через f^* индуцированный гомоморфизм групп когомологий.

2. Пусть $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$ — короткая точная последовательность G -модулей. Тогда существует длинная точная последовательность

$$\begin{aligned} 0 \rightarrow H^0(G, A') \rightarrow H^0(G, A) \rightarrow H^0(G, A'') \rightarrow H^1(G, A') \rightarrow \dots \\ \rightarrow H^n(G, A') \rightarrow H^n(G, A) \rightarrow H^n(G, A'') \rightarrow H^{n+1}(G, A) \rightarrow \dots \end{aligned}$$

3. Если действие G на A тривиально, то существует канонический изоморфизм между $H^1(G, A)$ и $\text{Hom}(G, A)$.

3.4.8 Определение. 1. Пусть $H \leq G$. Отображение $H^*(G, A) \rightarrow H^*(H, A)$, индуцированное вложением H в G , называется **морфизмом ограничения** и обозначается через Res_G^H .

2. Пусть $H \rightarrow G$ — сюръективный гомоморфизм групп. Индуцированное им отображение $H^*(G, A) \rightarrow H^*(H, A)$ называется **морфизмом инфляции** и обозначается через Inf_G^H .

3.4.9 Теорема. Пусть G — конечная группа, $H \leq G$.

1. Существует единственный набор гомоморфизмов

$$\text{Cor}_H^G: H^n(H, A) \rightarrow H^n(G, A)$$

(для любого G -модуля A и для любого $n \geq 0$), естественных по A , согласованных с длинными точными последовательностями, ассоциированными с короткими точными последовательностями G -модулей, и таких, что в степени 0

$$\text{Cor}_H^G(a) = \sum_{g \in G/H} ga$$

для всех $a \in H^0(H, A) = A^H$.

2. Если $m = (G : H)$ — индекс H в G , то $\text{Cor}_H^G \circ \text{Res}_G^H = m$.

3.4.10 Определение. Пусть A, B — G -модули. Тензорным произведением A и B называется абелева группа $A \otimes B$, снабженная диагональным действием G : $g(a \otimes b) = ga \otimes gb$.

3.4.11 Теорема. Пусть A, B — два G -модуля. Существуют билинейные гомоморфизмы

$$H^p(G, A) \times H^q(G, B) \rightarrow H^{p+q}(G, A \otimes B), \quad p, q \geq 0$$

$$(x, y) \mapsto x \cdot y,$$

естественные по A и B . Они обладают следующими свойствами:

1. **Ассоциативность:** если C — еще один G -модуль и $x \in H^p(G, A)$, $y \in H^q(G, B)$, $z \in H^r(G, C)$, то $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ с учетом изоморфизма $(A \otimes B) \otimes C \xrightarrow{\sim} A \otimes (B \otimes C)$, при котором $(a \otimes b) \otimes c \mapsto a \otimes (b \otimes c)$.
2. **Коммутативность:** если $x \in H^p(G, A)$, $y \in H^q(G, B)$, то $x \cdot y = (-1)^{pq} y \cdot x$ с учетом изоморфизма $A \otimes B \xrightarrow{\sim} B \otimes A$, при котором $a \otimes b \mapsto b \otimes a$.
3. **Контравариантность по G :** если $f: H \rightarrow G$ — гомоморфизм групп, то $f^*(x \cdot y) = f^*x \cdot f^*y$ для всех $x \in H^p(G, A)$, $y \in H^q(G, B)$.
4. **Формула проекции:** если H — подгруппа G , то $\text{Cor}_H^G(x \cdot \text{Res}_G^H y) = (\text{Cor}_H^G x) \cdot y$ для всех $x \in H^p(H, A)$, $y \in H^q(G, B)$.

Таким образом введенное произведение на когомологиях называется чашечным произведением.

Чашечное произведение можно определить как билинейное отображение на коцепях: если $f \in C^m(G, A)$, $f' \in C^n(G, B)$, то

$$(f \cdot f')(g_1, \dots, g_{m+n}) = f(g_1, \dots, g_m) \otimes g_1 \dots g_m f'(g_{m+1}, \dots, g_{m+n}).$$

3.4.12 Определение. Топологическая группа G называется **проконечной**, если она удовлетворяет одному из следующих эквивалентных условий:

1. G является проективным пределом конечных групп;
2. G отделима и всякая открытая подгруппа G имеет конечный индекс.

3.4.13 Определение. Пусть G — проконечная группа. **Топологический G -модуль** — это абелева группа A , снабженная левым действием группы G , такая, что $A = \bigcup_H A^H$, где объединение берется по всем открытым (следовательно, замкнутым и конечного индекса) подгруппам G . Если G — проконечная группа, A — топологический G -модуль, определим группы когомологий G с коэффициентами в A формулой

$$H^n(G, A) = \varinjlim H^n(G/H, A^H),$$

где H пробегает все различные открытые подгруппы в G , а морфизмы, участвующие в определении предела — морфизмы инфляции.

Можно доказать, что когомологии проконечных групп обладают теми же основными свойствами, что и когомологии конечных групп.

3.4.14 Определение. Пусть F_s — сепарабельное замыкание F . Группа F -автоморфизмов поля F_s обладает структурой проконечной группы:

$$G_F = \varprojlim \text{Gal}(E/F),$$

где E/F пробегает все конечные подрасширения Галуа в F_s . Группа G_F называется **абсолютной группой Галуа** поля F ; ее когомологии называются **когомологиями Галуа**; обычно мы пишем $H^*(F, A)$ вместо $H^*(G_F, A)$.

3.4.15 Лемма. *Автоморфизмы поля E являются линейно независимыми над E отображениями.*

Доказательство. Допустим, что $\sum a_\varphi \varphi = 0$, где φ — автоморфизмы E , $a_\varphi \in E$. Можно предположить, что множество ненулевых коэффициентов a_φ имеет минимально возможную мощность. В этом множестве хотя бы два элемента; возьмем $\varphi_1 \neq \varphi_2$ такие, что $a_{\varphi_1}, a_{\varphi_2} \neq 0$. Найдется $x \in E$ такой, что $\varphi_1(x) \neq \varphi_2(x)$. Тогда для любого $y \in E$ имеем

$$\sum a_\varphi \varphi(y) = 0,$$

откуда

$$0 = \sum a_\varphi \varphi(xy) - \varphi_1(x) \sum a_\varphi \varphi(y) = \sum a_\varphi (\varphi(x) - \varphi_1(x)) \varphi(y),$$

поэтому $\sum a_\varphi (\varphi(x) - \varphi_1(x)) \varphi = 0$ — новая линейная зависимость, в которой меньше ненулевых слагаемых, чем в исходной: противоречие. \square

3.4.16 Теорема. Гильберта 90 Пусть E/F — расширение Галуа с группой G . Тогда $H^1(G, E^*) = 0$.

Доказательство. Пусть $(a_g)_{g \in G}$ — 1-коцикл G со значениями в E^* . По лемме 3.4.15 найдется $x \in E$ такой, что $a = \sum_{g \in G} a_g g x \neq 0$. Поэтому для любого $h \in G$

$${}^h a = \sum_{g \in G} {}^h a_g {}^{hg} x = \sum_{g \in G} a_h^{-1} a_{hg} {}^{hg} x = a_h^{-1} \sum_{g \in G} a_g g x = a_h^{-1} a,$$

что и означает, что (a_g) является 1-кограницей. \square

3.4.17 Следствие. $H^1(F, F_s^*) = 0$.

3.4.18 Определение. Пусть E/F — расширение Галуа с группой G . Пусть G действует слева на E , c — 2-коцикл G со значениями в E^* . **Скращенным произведением**, соответствующим c , называется следующая F -алгебра $E \times_s G$:

- *Аддитивная структура:* $E \times_c G$ — векторное пространство над E с базисом G .
- *Мультипликативная структура:* умножение F -билинейно и если $x, y \in E$, $g, h \in G$, то

$$(x \cdot g)(y \cdot h) = x {}^g y c_{g,h} \cdot gh.$$

3.4.19 Теорема. 1. Таким образом определенная алгебра $E \times_c G$ является ассоциативной и центральной простой над F степени $n = [E : F]$; E — максимальная коммутативная подалгебра $E \times_c G$.

2. Всякая центральная простая F -алгебра A , содержащая E как максимальное коммутативное под-тело, имеет вид $E \times_c G$.

3. Пусть c, c' — коциклы G со значениями в E^* . $E \times_c G \cong E \times_{c'} G$ тогда и только тогда, когда c и c' когомологичны (то есть $c/c' \in B^2(G, E^*)$).

3.4.20 Следствие. Существует канонический изоморфизм

$$\mathfrak{u}_{E/F}: H^2(G, E^*) \xrightarrow{\sim} \text{Br}(E/F),$$

где $\text{Br}(E, F) = \text{Ker}(\text{Br}(F) \rightarrow \text{Br}(E))$.

3.4.21 Пример. $E = F(\sqrt{a})$, где $a \notin F^*/(F^*)^2$. Тогда $G = \{1, g\}$. Будем обозначать действие g через $x \mapsto \bar{x}$. 2-коцикл G с коэффициентами в E^* задается четырьмя элементами $c_{1,1}$, $c_{1,g}$, $c_{g,1}$ и $c_{g,g}$. Применяя соотношение коцикла к тройкам $(1, 1, g)$, $(g, 1, 1)$ и (g, g, g) , получаем

$$\begin{aligned} c_{1,1} &= c_{1,g} \\ c_{g,1} &= \overline{c_{1,1}} \\ c_{g,g} c_{1,g} &= \overline{c_{g,g}} c_{g,1}. \end{aligned}$$

После деления на кограницу можно считать, что $c_{1,1} = 1$ (такой 2-коцикл называют **нормализованным**). Тогда $c_{1,g} = c_{g,1} = 1$ и $c_{g,g} = b \in F^*$. Пусть $\alpha \in E^*$ и $\alpha^2 = a$; положим $\beta = \alpha \cdot g \in A$. Тогда $\alpha\beta = -\beta\alpha$ и $\beta^2 = -ab$; значит, мы получили алгебру кватернионов $\left(\begin{smallmatrix} a & -ab \\ F & F \end{smallmatrix} \right)$.

3.4.22 Теорема. *Изоморфизмы $\mathfrak{u}_{E/F}$ из следствия 3.4.20 склеиваются в изоморфизм*

$$\mathfrak{u}_F: H^2(F, F_s^*) \xrightarrow{\sim} \text{Br}(F).$$

Пусть n — натуральное число, взаимно простое с характеристикой F ; тогда возведение в степень n сюръективно на F_s^* . Рассмотрим точную последовательность Куммера G_F -модулей

$$1 \rightarrow \mu_n \rightarrow F_s^* \xrightarrow{n} F_s^* \rightarrow 1,$$

где μ_n — группа корней n -ой степени из 1 в F_s . Ей соответствует длинная точная последовательностей когомологий Галуа:

$$\begin{aligned} 1 \rightarrow H^0(F, \mu_n) \rightarrow H^0(F, F_s^*) \xrightarrow{n} H^0(F, F_s^*) \\ \xrightarrow{\delta} H^1(F, \mu_n) \rightarrow H^1(F, F_s^*) \xrightarrow{n} H^1(F, F_s^*) \\ \rightarrow H^2(F, \mu_n) \rightarrow H^2(F, F_s^*) \xrightarrow{n} H^2(F, F_s^*). \end{aligned}$$

Заметим, что $H^0(F, F_s^*) = F^*$ и $H^1(F, F_s^*) = 0$ по теореме Гильберта 90. Мы получили следующую теорему:

3.4.23 Теорема (теория Куммера). *Эта точная последовательность приводит к изоморфизмам*

$$\begin{aligned} F^*/(F^*)^n &\xrightarrow{\sim} H^1(F, \mu_n) \\ H^2(F, \mu_n) &\xrightarrow{\sim} {}_n\text{Br}(F). \end{aligned}$$

Первый изоморфизм мы будем обозначать через $a \mapsto (a)$. В случае $n = 2$ группа μ_2 является тривиальным G_F -модулем, изоморфным группе $\mathbb{Z}/2$. Получаем изоморфизмы

$$\begin{aligned} F^*/(F^*)^2 &\xrightarrow{\sim} H^1(F, \mathbb{Z}/2) \\ H^2(F, \mathbb{Z}/2) &\xrightarrow{\sim} {}_2\text{Br}(F). \end{aligned}$$

В частности, если $a, b \in F^*$, то класс (a, b) алгебры кватернионов, определенной элементами a и b является элементом $H^2(F, \mathbb{Z}/2)$.

3.4.24 Утверждение. $(a, b) = (a) \cdot (b)$.

Доказательство. По определению чашечное произведение задается формулой $(g, h) \mapsto (a)(g) \cdot (b)(h)$, и его образ в $H^2(F, F_s^*)$ представляется 2-коциклом $b_{g,h} = (-1)^{(a)(g) \cdot (b)(g)}$. В примере 3.4.21 мы видели, что класс алгебры $\left(\begin{smallmatrix} a & b \\ F & \end{smallmatrix}\right)$ в $H^2(F, F_s^*)$ представляется 2-коциклом

$$c_{g,h} = \begin{cases} 1, & \text{если } (a)(g) = 0 \text{ или } (a)(h) = 0; \\ -ab, & \text{если } (a)(g) = (a)(h) = 1. \end{cases}$$

Осталось проверить, что $b_{g,h}$ и $c_{g,h}$ кохомологичны. Возьмем $\alpha, \beta \in F_s^*$ такие, что $\alpha^2 = a, \beta^2 = b$. Легко видеть, что $b_{g,h}^{-1}c_{g,h} = f(gh)^{-1}f(g)^gf(h)$, где

$$f(g) = \begin{cases} 1, & \text{если } (a)(g) = 0; \\ \alpha\beta, & \text{если } (a)(g) = 1, (b)(g) = 0; \\ -\alpha\beta, & \text{если } (a)(g) = (b)(g) = 1. \end{cases}$$

□

3.5 Теорема Меркурьева

3.5.1 Утверждение. Пусть q — квадратичная форма над F . Тогда $\varepsilon(C(q)) = \overline{\dim q}$ и $\delta(C(q)) = d(q)$ (см. обозначения перед теоремой 3.3.10).

Доказательство. Рассмотрим гомоморфизмы $(\overline{\dim}, d)$ и $(\varepsilon, \delta) \circ C$ из $W(F)/I^3F$ в $Q(F)$. Для доказательства их совпадения достаточно проверить это на порождающих $W(F)$, скажем, на классах одномерных форм $\langle a \rangle$, $a \in F^*$, что очевидно. □

3.5.2 Лемма. Пусть $q \in I^2F$. Тогда $C_0(q) \cong A \times A$ и $C(q) \cong M_2(A)$ для некоторой центральной простой алгебры A .

Доказательство. По предложению 3.5.1 алгебра $C(q)$ имеет четный тип и $\delta(C(q)) = 1$. По теореме 3.3.10 получаем, что $C(q)$ подобна алгебре $i(A_0)$ для некоторой центральной простой алгебры A_0 . Другими словами, существует векторное суперпространство $V = V_0 \oplus V_1$ такое, что $C(q) \cong i(A_0) \hat{\otimes}_F \text{End}_F(V)$. Размерности $C_0(q)$ и $C_1(q)$ совпадают, поэтому $\dim V_0 = \dim V_1$. отождествляя V_1 с V_0 , получаем, что

$$C(q) \cong i(A_0) \hat{\otimes}_F \text{End}_F(V) \cong i(A_0 \otimes_F \text{End}_F(V_0)) \hat{\otimes}_F M_2(F),$$

и получаем нужное утверждение для $A = A_0 \otimes_F \text{End}_F(V_0)$. □

$\dim q$	$d(q)$	$Z(C(q))$	$C(q)$	$Z(C_0(q))$	$C_0(q)$	$\deg(q)$
нечетно	$\notin (F^*)^2$	$F(\sqrt{d})$	простая	F	центральная простая	0
	$\in (F^*)^2$	$F \times F$	$C_0(q) \times C_0(q)$			
четно	$\notin (F^*)^2$	F	цпа	$F(\sqrt{d})$	простая	1
	$\in (F^*)^2$		$M_2(A)$	$F \times F$	$A \times A$, A цпа	≥ 2

3.5.3 Определение. Для квадратичной формы q обозначим через $c(q)$ элемент $b(C(q)) \in \text{Br}(F)$ — инвариант Клиффорда q . Таким образом,

$$c(q) = \begin{cases} [C_0(q)], & \text{если } A \text{ нечетного типа;} \\ [C(q)], & \text{если } A \text{ четного типа.} \end{cases}$$

3.5.4 Утверждение. Пусть q, q' — две квадратичные формы. Тогда

$$c(q \perp q') = c(q) + c(q') + ((-1)^{m(n+1)}d(q), (-1)^{(m+1)n}d(q')),$$

где $m = \dim q$, $n = \dim q'$.

Доказательство. Тривиально следует из теоремы 3.3.10. □

3.5.5 Утверждение. 1. Пусть $\varphi, \psi \in IF$. Тогда $c(\varphi \otimes \psi) = (d(\varphi), d(\psi))$.

2. Пусть q — квадратичная форма, $a \in F^*$. Тогда

$$c(aq) = \begin{cases} c(q) + (a, d(q)), & \text{если } \dim q \text{ четна;} \\ [c(q)], & \text{если } \dim q \text{ нечетна.} \end{cases}$$

3.5.6 Лемма. 1. Пусть $a, b \in F^*$. Тогда $\langle\langle a, b \rangle\rangle$ гиперболична $\iff c(\langle\langle a, b \rangle\rangle) = 0$.

2. Пусть $a, b, c, d \in F^*$. Тогда $\langle\langle a, b \rangle\rangle \cong \langle\langle c, d \rangle\rangle \iff (a, b) = (c, d)$.

3. Пусть $\sigma, \tau \in GP_2(F)$. Тогда σ пропорциональна $\tau \iff c(\sigma) = c(\tau)$.

Доказательство. (1) — очевидно. Для доказательства (2) предположим сначала, что $b = d$. Тогда $(ac, b) = 0$, поэтому $\langle\langle ac, b \rangle\rangle \sim 0$ по пункту (1). Значит, $\langle\langle a, b \rangle\rangle \perp -\langle\langle c, d \rangle\rangle \sim c\langle\langle ac, b \rangle\rangle \sim 0$, что и требовалось. В общем случае применим лемму Альберта 3.2.24: найдется e такое, что $(a, b) = (a, e) = (c, e) = (c, d)$, поэтому $\langle\langle a, b \rangle\rangle \cong \langle\langle a, e \rangle\rangle \cong \langle\langle c, e \rangle\rangle \cong \langle\langle c, d \rangle\rangle$. В (3) пусть $\sigma = a\sigma_0$, $\tau = b\tau_0$, где $\sigma_0, \tau_0 \in P_2(F)$. Тогда $c(\sigma) = c(\sigma_0)$, $c(\tau) = c(\tau_0)$, и все следует из пункта (2). □

Из предложения 3.5.4 следует, что ограничение инварианта Клиффорда c на I^2F является гомоморфизмом, принимающим значения в подгруппе 2-кручения ${}_2Br(F)$ группы Брауэра $Br(F)$.

3.5.7 Теорема (Меркурьев). Гомоморфизм

$$c: I^2F/I^3F \rightarrow {}_2Br(F),$$

индуцированный инвариантом Клиффорда, является изоморфизмом.

Обозначим через $BW_2(F)$ множество элементов $x \in BW(F)$ таких, что $b(x) \in {}_2Br(F)$. Легко проверить, что $BW_2(F)$ является подгруппой в $BW(F)$, содержащей $i({}_2Br(F))$ (но она не совпадает с подгруппой 2-кручения $BW(F)$!). Из теоремы Меркурьева нетрудно вывести следующее утверждение.

3.5.8 Следствие. Гомоморфизм C (см. следствие 3.3.9) индуцирует изоморфизм

$$C: W(F)/I^3F \rightarrow BW_2(F).$$

3.6 Высшие инварианты

Мы будем обозначать через $H^n F$ группы когомологий Галуа $H^n(F, \mathbb{Z}/2)$. Мы знаем, что инварианты $\overline{\dim}$, d и c можно рассматривать как инварианты

$$e^n: W(F) \rightarrow H^n F$$

для $n = 0, 1, 2$ (см. теорему 3.4.23 и замечание после нее).

3.6.1 Теорема. Для $n \leq 2$ инвариант e^n индуцирует изоморфизм

$$\bar{e}^n: I^n F / I^{n+1} F \rightarrow H^n F,$$

причем

$$e^{p+q}(xy) = e^p(x) \cdot e^q(y)$$

для $p + q \leq 2$, $x \in I^p F / I^{p+1} F \times I^q F / I^{q+1} F$.

Доказательство. Первое утверждение является переформулировкой уже известных теорем 3.1.2 и 3.5.7. Второе нужно проверить только для $p = q = 1$, а это следует из предложений 3.5.5 и 3.4.24. \square

Напомним, что K -теорией Милнора называется градуированное кольцо $K_*^M(F)$, заданное образующими $\{a\}$, $a \in F^*$ и соотношениями $\{ab\} = \{a\} + \{b\}$ ($a, b \in F^*$), $\{a\} \cdot \{1 - a\} = 0$ ($a \in F^* \setminus \{1\}$). Иными словами, $K_*^M(F)$ является фактором тензорной алгебры \mathbb{Z} -модуля F^* по двустороннему идеалу, порожденному элементами $a \otimes (1 - a)$ для $a \neq 1$. Легко видеть, что $K_0(F) = \mathbb{Z}$, $K_1(F) = F^*$. Будем обозначать произведение $\{a_1\} \cdot \dots \cdot \{a_n\} \in K_n^M(F)$ через $\{a_1, \dots, a_n\}$.

3.6.2 Лемма. В кольце $K_*^M(F)$ выполнены соотношения $\{a, a\} = \{a, -1\}$ и $\{a, b\} = -\{b, a\}$ для всех $a, b \in F^*$.

Доказательство. Поскольку 1 является нейтральным элементом абелевой группы F^* , имеем $\{1, 1\} = \{1, -1\} = 0$. Пусть теперь $a \neq 0, 1$. Тогда $\{a, 1 - a\} = 0 = \{a^{-1}, 1 - a^{-1}\}$. Из билинейности следует, что $\{a^{-1}, 1 - a^{-1}\} = -\{a, 1 - a^{-1}\} = -\{a, \frac{1-a}{a}\} = -\{a, 1 - a\} + \{a, -a\}$, поэтому $\{a, -a\} = 0$. Но $-a = \frac{a}{-1}$, поэтому $\{a, a\} = \{a, -1\}$. Для доказательства второго соотношения заметим, что $\{ab, ab\} = \{a, a\} + \{b, b\} + \{a, b\} + \{b, a\} = \{a, -1\} + \{b, -1\} + \{a, b\} + \{b, a\} = \{ab, -1\} + \{a, b\} + \{b, a\} = \{ab, ab\} + \{a, b\} + \{b, a\}$ по уже доказанному; отсюда $\{a, b\} + \{b, a\} = 0$. \square

3.6.3 Примеры. 1. Пусть $F = \mathbb{F}_q$. Известно, что мультипликативная группа конечного поля является циклической, поэтому $K_1^M(\mathbb{F}_q) \cong \mathbb{Z}/(q-1)$. Умножение в $K_*^M(\mathbb{F}_q)$ дает нам сюръективный гомоморфизм

$$\mathbb{F}_q^* \otimes_{\mathbb{Z}} \mathbb{F}_q^* \rightarrow K_2^M(\mathbb{F}_q).$$

Пусть a — образующая группы \mathbb{F}_q^* ; тогда $K_2^M(\mathbb{F}_q)$ также является циклической с образующей $\{a, a\}$. Но по лемме 3.6.2 $\{a, a\} = \{a, -1\}$, стало быть, эта образующая имеет порядок 1 или 2. Значит, во всяком случае,

$$K_2^M(\mathbb{F}_q) \cong K_2^M(\mathbb{F}_q)/2.$$

Заметим, что уравнение $x^2 + y^2 = a$ имеет нетривиальное решение над \mathbb{F}_q . Можно считать, что $x \neq 0$, тогда $1 + y^2/x^2 = a/x^2$ и

$$\begin{aligned} \{a, -1\} &= \{a/x^2, -1\} \\ &= \{a/x^2, -1\} + \{a/x^2, 1 - a/x^2\} \\ &= \{a/x^2, a/x^2 - 1\} \\ &= \{a/x^2, y^2/x^2\} \\ &= \{a/x^2, 1\} \\ &= 0 \end{aligned}$$

в группе $K_2^M(\mathbb{F}_q)/2$, значит, и в $K_2^M(\mathbb{F}_q)$. Поэтому $K_2^M(\mathbb{F}_q) = 0$ и, следовательно, $K_n^M(\mathbb{F}_q) = 0$ для всех $n \geq 2$.

2. Пусть $F = \mathbb{R}$; тогда $\mathbb{R}^*/2 \cong \mathbb{Z}/2$ — циклическая группа порядка 2 с образующей -1 . Значит, $T_{\mathbb{Z}/2}(\mathbb{R}^*/2) = (\mathbb{Z}/2)[t]$, где $t = \{-1\}$. С другой стороны, из двух элементов $a, 1 - a$ хотя бы один является положительным, поэтому из него извлекается квадратный корень в \mathbb{R} . Это означает, что элемент $a \otimes (1 - a)$ является 2-делимым в $(\mathbb{R}^*/2)^{\otimes 2}$. Поэтому $K_*^M(\mathbb{R})/2 \cong T_{\mathbb{Z}/2}(\mathbb{R}^*/2) \cong (\mathbb{Z}/2)[t]$, где $t = \{-1\}$.

3.6.4 Утверждение. Пусть $n \geq 0$. Существуют гомоморфизмы

$$\begin{aligned} a^n: K_n^M(F)/2 &\rightarrow I^n F / I^{n+1} F, \\ b^n: K_n^M(F)/2 &\rightarrow H^n F \end{aligned}$$

такие, что

$$\begin{aligned} a^n(\{a_1, \dots, a_n\}) &= \langle\langle a_1, \dots, a_n \rangle\rangle \\ b^n(\{a, 1, \dots, a_n\}) &= (a_1) \cdots (a_n). \end{aligned}$$

Кроме того, гомоморфизм a^n является сюръективным. Произведение $(a_1) \cdots (a_n)$ в $H^n F$ мы будем обозначать через (a_1, \dots, a_n) .

Доказательство. Докажем, что a^n и b^n — корректно определенные отображения. Со-
поставление $(a_1, \dots, a_n) \mapsto \langle\langle a_1, \dots, a_n \rangle\rangle$ является полилинейным по лемме 2.1.4. Форма $2 = \langle 1, 1 \rangle$ лежит в $I^0 F$, поэтому $2I^n F / I^{n+1} F = 0$. Форма $\langle\langle a, 1 - a \rangle\rangle$ изотропна, поэтому она эквивалентна 0. Отображение $(a_1, \dots, a_n) \mapsto (a_1) \cdots (a_n)$ является полилинейным в силу определения; кроме того, очевидно, что $2H^n F = 0$. Наконец из леммы 3.2.23 и предложения 3.4.24 следует, что $(a) \cdot (1 - a) = 0$. Сюръективность a^n следует из того, что $I^n F / I^{n+1} F$ порождается классами n -форм Пфистера □

3.6.5 Утверждение (Милнор). Существует отображение

$$w: \widetilde{W}(F) \rightarrow K_*^M(F)/2$$

такое, что $w(q \perp q') = w(q)w(q')$ для $q, q' \in \widetilde{W}(F)$ и $w(\langle a \rangle) = 1 + \{a\}$. Кроме того,

$$w((\langle 1 \rangle - \langle a_1 \rangle) \otimes \cdots \otimes (\langle 1 \rangle - \langle a_1 \rangle)) = 1 + \{-1\}^{2^{n-1}-n} \{a_1, \dots, a_n\}.$$

Для $q \in \widetilde{W}(F)$ запишем $w(q) = \sum_{n \geq 0} w_n(q)$, где $w_n(q) \in K_*^M(F)/2$. Классы $w_n(q)$ называются классами Штифеля–Уитни формы q .

Доказательство. В силу предложения 1.2.15, для доказательства существования w достаточно проверить, что $w(\langle a, b \rangle) = w(\langle a+b, ab(a+b) \rangle)$ для всех $a, b \in F^*$, $a+b \neq 0$. По определению $w(\langle a, b \rangle) = (1 + \{a\})(1 + \{b\}) = 1 + \{ab\} + \{a, b\}$ и $w(\langle a+b, ab(a+b) \rangle) = (1 + \{a+b\})(1 + \{ab(a+b)\}) = 1 + \{ab\} + \{a+b, ab(a+b)\}$. Осталось заметить, что $\{a+b, ab(a+b)\} = \{a+b, -ab\} = \{a, -ab\} + \{1+b/a, -ab\} = \{a, b\} + \{a+b/a, -b/a\} = \{a, b\}$.

Положим $\langle\langle a_1, \dots, a_n \rangle\rangle := (\langle 1 \rangle - \langle a_1 \rangle) \otimes \cdots \otimes (\langle 1 \rangle - \langle a_n \rangle)$. Для доказательства последней формулы проведем индукцию по n . Очевидно, что

$$\langle\langle a_1, \dots, a_n \rangle\rangle = \langle\langle a_1, \dots, a_{n-1} \rangle\rangle - a_n \langle\langle a_1, \dots, a_{n-1} \rangle\rangle.$$

Значит,

$$w(\langle\langle a_1, \dots, a_n \rangle\rangle) = w(\langle\langle a_1, \dots, a_{n-1} \rangle\rangle) w(a_n \langle\langle a_1, \dots, a_{n-1} \rangle\rangle)^{-1}.$$

Обозначим $X_n = \{-1\}^{2^{n-1}-n} \{a_1, \dots, a_n\}$. Нетрудно видеть, что если $q \in \widetilde{W}(F)$ — произвольная форма размерности m , $a \in F^*$ и

$$w(q) = \sum_{i \geq 0} w_i(q), \quad w_i(q) \in K_*^M(F)/2.$$

то

$$w(aq) = \sum_{i \geq 0} (1 + \{a\})^{m-i} w_i(q).$$

Поэтому

$$w(a_n \langle\langle a_1, \dots, a_{n-1} \rangle\rangle) = 1 + (1 + \{a_n\})^{-2^{n-2}} X_{n-1}.$$

Значит,

$$\begin{aligned} w(\langle\langle a_1, \dots, a_n \rangle\rangle) &= (1 + X_{n-1})(1 + (1 + \{a_n\})^{-2^{n-2}} X_{n-1})^{-1} \\ &= (1 + X_{n-1})(1 + \{a_n\})^{2^{n-2}} \left((1 + \{a_n\})^{2^{n-2}} + X_{n-1} \right)^{-1} \\ &= (1 + X_{n-1} + \{a_n\}^{2^{n-2}} + X_{n-1}\{a_n\}^{2^{n-2}})(1 + \{a_n\}^{2^{n-2}} + X_{n-1})^{-1}. \end{aligned}$$

Заметим, что $\{a_n\}^{2^{n-2}} = \{-1\}^{2^{n-2}-1} \{a_n\}$ (по лемме 3.6.2), откуда $X_{n-1}\{a_n\}^{2^{n-2}} = X_n$ и

$$w(\langle\langle a_1, \dots, a_n \rangle\rangle) = 1 + X_n(1 + \{a_n\}^{2^{n-2}} + X_{n-1})^{-1}.$$

Обозначим $A := \{a_n\}^{2^{n-2}}$, $B := X_{n-1}$. Тогда

$$X_n(\{a_n\}^{2^{n-2}} + X_{n-1}) = A^2B + AB^2 = \{-1\}^{2^{n-2}} AB + \{-1\}^{2^{n-2}} AB = 0,$$

откуда $w(\langle\langle a_1, \dots, a_n \rangle\rangle) = 1 + X_n$. □