Лекция 2

Ортогональная группа

Определение 2.1 *Пусть q - невырожденная квадратичная форма над k. Ортогональной группой* $\mathrm{O}(q)$ *называется подгруппа в* $\mathrm{GL}(V_q)$, *состоящая из таких линейных автоморфизмов* φ, *что* $q(\varphi(v)) = q(v)$ *для любого* $v \in V_q$.

Пусть w - анизотропный вектор формы q. Мы можем сопоставить ему некоторый элемент $\tau_w \in \mathrm{O}(q)$ (называемый *элементарным отражением*) следующим образом: $\tau_w(v) = v - \frac{2B_q(w,v)}{q(w)} \cdot w$. Нетрудно видеть, что это преобразование действительно сохраняет форму q, что $\tau_w^2 = Id$, и $\tau_w(w) = -w$.

Лемма 2.2 *Пусть $u, v \in V_q$ - такие векторы, что $q(u) = q(v) \neq 0$. Тогда существует такой вектор $w \in V_q$, что $q(w) \neq 0$, и $\tau_w(u) = \pm v$. Более того, если $q(u-v) \neq 0$, то $\tau_{(u-v)}(u) = v$.*

Доказательство: Так как $char(k) \neq 2$, то одно из чисел $q(u-v), q(u+v)$ - ненулевое. Легко видеть, что $\tau_{(u\pm v)}(u) = u - \frac{2B_q(u\pm v,u)}{q(u\pm v)}(u \pm v) = u - \frac{4q(u)\pm 4B_q(u,v)}{2q(u)\pm 2B_q(u,v)}(u \pm v) = \mp v$. □

В качестве следствия, мы получаем, что группа $\mathrm{O}(q)$ порождена элементарными отражениями.

Теорема 2.3

(*a*) *Пусть q - это невырожденная n-мерная квадратичная форма и $\phi \in O(q)$ - ортогональное преобразование. Тогда существуют $v_1, \ldots, v_m \in V_q$, такие что $q(v_i) \neq 0$, $\phi = \tau_{v_1} \circ \cdots \circ \tau_{v_m}$ и $0 \leq m \leq 2n$.*

(*b*) *Если q - анизотропна, то можно считать $0 \leq m \leq n$.*

Доказательство: (a) Будем использовать индукцию по n. При $n = 0$ утверждение очевидно. Пусть утверждение верно для $n-1$, и q - это n-мерная невырожденная форма. Пусть $x_1 \in V_q$ - это произвольный анизотропный вектор ($q(x_1) \neq 0$). По лемме 2.2, существует $v_1 \in V_q$, такой, что $q(v_1) \neq 0$ и $\tau_{v_1}(\phi(x_1))$ равно либо x_1, либо $-x_1$. В первом случае, положим $\psi := \tau_{v_1} \circ \phi$; во втором - положим $v_2 := x_1$ и $\psi := \tau_{v_2} \circ \tau_{v_1} \circ \phi$. В любом случае, $\psi \in O(q)$ и $\psi(x_1) = x_1$. Это означает, что $\psi|_L = id$, где $L = k \cdot x_1$, откуда следует, что $\psi(L^{\perp}) = L^{\perp}$, то есть, $\psi|_{L^{\perp}} \in O(q|_{L^{\perp}})$. По предположению индукции, существуют такие $v_3, \ldots, v_m \in L^{\perp}$, что $q(v_j) \neq 0$, $\psi|_{L^{\perp}} = \tau_{v_3} \circ \cdots \circ \tau_{v_m}$ и $m \leq 2n$. Так как $v_j \in L^{\perp}$ при $j \geq 3$, то $\tau_{v_3} \circ \cdots \circ \tau_{v_m}(x_1) = x_1$. Это означает, что $\psi = \tau_{v_3} \circ \cdots \circ \tau_{v_m}$. Стало быть, ϕ равно произведению не более, чем $2n$ отражений (т.к. $\tau_z \circ \tau_z = id$).

(b) Опять используем индукцию по размерности. Рассмотрим оператор $\rho := id - \phi$. Положим $U := \ker(\rho)$. Так как q - анизотропна, то $q|_{U^{\perp}}$ - невырождена (равно как и ограничение на любое другое подпространство). Ясно, что $\phi(U^{\perp}) = U^{\perp}$, и значит, $\phi|_{U^{\perp}} \in O(q|_{U^{\perp}})$. Если $U^{\perp} \neq V_q$, то, по индукции $\phi|_{U^{\perp}} = \tau_{v_1} \circ \cdots \circ \tau_{v_m}$, где $v_i \in U^{\perp}$ и $m \leq \dim U^{\perp} < n$. А так как $\tau_{v_i}|_U = id$, то и $\phi = \tau_{v_1} \circ \tau_{v_m}$. Так что мы можем предполагать, что $U^{\perp} = V_q$ и $U = 0$. Возьмём произвольный ненулевой $x_1 \in U^{\perp}$. Тогда $v_1 := x_1 - \phi(x_1) \neq 0$, и из анизотропности q следует, что $q(x_1 - \phi(x_1)) \neq 0$. По лемме 2.2, $\tau_{v_1}(x_1) = \phi(x_1)$. Далее мы рассуждаем как в пункте (a). $\square$

Теорема Витта о сокращении

Базисным фактом при работе с квадратичными формами является следующий результат.

Теорема Витта о сокращении *Пусть q_1, q_2, p - квадратичные формы над k, такие, что $q_1 \perp p \cong q_2 \perp p$. Тогда $q_1 \cong q_2$.*

Доказательство: Так как любая квадратичная форма диагонализуема, то достаточно рассмотреть случай, когда p - одномерна. Если p - нулевая одномерная форма, то невырожденная часть q_1 изоморфна невырожденной части $q_1 \perp p \cong q_2 \perp p$, а последняя изоморфна невырожденной части q_2. Так как $\dim(q_1) = \dim(q_2)$, то эти формы изоморфны. Пусть теперь $p = \langle c \rangle$, где $c \in k^*$. Пусть $r := q_1 \perp p$. Это разложение даёт нам вложение $i_1 : p \hookrightarrow r$. Отождествляя r с $q_2 \perp p$, мы получаем второе вложение $i_2 : p \hookrightarrow r$. При этом, $i_1(p)^{\perp} \cong q_1$, и $i_2(p)^{\perp} \cong q_2$. Если $v \in V_p$ - образуящая с $q(v) = c$, то $i_1(v), i_2(v)$ - два вектора в V_r, с нормой равной $p(v)$. По лемме 2.2, существует $\varphi \in \mathrm{O}(r)$, такое, что $\varphi(i_1(v)) = \pm i_2(v)$. Ясно, что тогда φ изоморфно отображает $i_1(p)^{\perp} \cong q_1$ на $i_2(p)^{\perp} \cong q_2$. $\square$

Мы видели, что любая квадратичная форма однозначно восстанавливается по своей невырожденной части и размерности. Поэтому, достаточно изучать невырожденные квадратичные формы. Оказывается, что среди таких форм можно также выделить некоторые элементарные.

Определение 2.5 *Форма вида $\mathbb{H} := \langle 1, -1 \rangle$ называется элементарной гиперболической. Ортогональная сумма таких форм называется ги-*

перболической формой.

Замечаем, что форма $\mathbb{H}$ является изотропной, а форма $\perp_{i=1}^{m} \mathbb{H}$ содержит изотропное подпространство (то есть, подпр-во, состоящее из изотропных векторов) размерности m.

Упражнение 2.1

(1) *Показать, что для любого $a \in k^*$, $a \cdot \mathbb{H} \cong \mathbb{H}$.*

(2) *Пусть $q = \langle 1, -a \rangle$. Показать, что $\lambda \cdot q \cong q$ равносильно тому, что λ - ненулевое значение q.*

Теорема 2.6 *Пусть q - невырожденная квадратичная форма над k. Тогда максимальная размерность изотропного подпространства в V_q равна максимальному m, такому, что форма $\perp_{i=1}^{m} \mathbb{H}$ является подформой ($\Leftrightarrow$ прямым слагаемым) в q. В частности, форма q изотропна тогда и только тогда, когда она содержит гиперболическое слагаемое.*

Доказательство: Ясно, что если $\perp_{i=1}^{m} \mathbb{H}$ вкладывается в q, то в V_q имеется изотропное подпространство размерности m. Обратно, докажем индукцией по m, что если такое подпространство имеется, то $q = (\perp_{i=1}^{m} \mathbb{H}) \perp q$". При $m = 0$ доказывать нечего. Переход $(m-1) \to (m)$: пусть $U \subset V_q$ - изотропное подпространство размерности m, и $v \in U$.

Лемма 2.7 *Пусть q - невырожденная форма, и $v \in V_q$ изотропный вектор. Тогда существует вложение $i : \mathbb{H} \hookrightarrow q$, такое, что $v \in image(i)$.*

Доказательство: Так как q - невырожденная, то существует такой $w \in V_q$, что $B_q(v, w) \neq 0$. Тогда размерность линейной оболочки $L(v, w)$ равна 2, и ясно, что $q|_{L(v,w)}$ - элементарная гиперболическая форма. □

Таким образом, $q = \mathbb{H} \perp q'$, где $v \in V_{\mathbb{H}}$. Пусть $W = v^{\perp}$. Тогда $k \cdot v \subset W$, и на $W/(k \cdot v)$ возникает корректно определённая форма $\tilde{q}$, заданная равенством $\tilde{q}(w\,(mod\,kv)) := q(w)$. Легко видеть, что $\tilde{q} \cong q'$. По построению, $\tilde{q}$ имеет изотропное подпространство размерности $(m-1)$, стало быть, и q' имеет такое подпространство. По предположению индукции, $q' = (\perp_{i=1}^{m-1} \mathbb{H}) \perp q$". Значит, $q = (\perp_{i=1}^{m} \mathbb{H}) \perp q$". □

Определение 2.8 *Индексом Витта $i_W(q)$ невырожденной квадратичной формы q называется такое максимальное m, что $q = \perp_{i=1}^{m} \mathbb{H} \perp q_{an}$. Форма q_{an} называется анизотропной частью формы q.*

Заметим, что по теореме 2.7, форма q_{an} анизотропна, а по теореме Витта о сокращении, форма q_{an} единственна с точностью до изоморфизма.

Кольцо Витта квадратичных форм

Операция $+$ превращает множество классов квадратичных невырожденных форм по модулю изоморфизма в коммутативную полугруппу. При этом имеется дистрибутивность по отношению к операции $\cdot$. Это означает, что на группе Гротендика, отвечающей нашей полугруппе имеется структура (коммутативного) кольца.

Определение 2.9 *Кольцом Витта-Гротендика квадратичных форм $\widetilde{W}(k)$ поля k называется группа Гротендика моноида классов изоморфизма невырожденных квадратичных форм над k, с умножением происходящим из тензорного умножения на соответствующих билинейных формах.*

Таким образом, элементом $\widetilde{W}(k)$ является формальная разность $[q_1]-[q_2]$, где q_1, q_2 - невырожденные квадратичные формы над k.

Упражнение 2.2 *Напомним, что если M - коммутативная полугруппа, то её группой Гротендика $G(M)$ называется множество формальных разностей $[a]-[b]$, где $a, b \in M$, по модулю эквивалентности: $[a]-[b] \sim [c]-[d] \Leftrightarrow$ существует $e \in M$, такое, что $a+d+e = b+c+e$. Операция задана как: $([a]-[b])+([c]-[d]) := ([a+c]-[b+d])$, и обратный как: $-([a]-[b]) := ([b]-[a])$. Имеется естественный морфизм полугрупп $M \xrightarrow{i} G(M)$.*

Проверьте, что $G(M)$ обладает следующим универсальным свойством: для любой группы H, и любого морфизма полугрупп $\varphi : M \to H$ существует единственный морфизм групп $\tilde{\varphi} : G(M) \to H$, такой, что $\varphi = \tilde{\varphi} \circ i$. Зачем нужно e в определении выше?

Ввиду теоремы Витта о сокращении, мы получаем, что $([q_1]-[q_2])$ и $([p_1]-[p_2])$ представляют один и тот же элемент в $\widetilde{W}(k)$ тогда и только тогда, когда $q_1 \perp p_2 \cong p_1 \perp q_2$. В частности полугруппа классов изоморфизма невырожденных квадратичных форм вкладывается в свою группу Гротендика $\widetilde{W}(k)$.

Утверждение 2.10 *Подгруппа в $\widetilde{W}(k)$, порождённая элементом $([\mathbb{H}]-[0])$ является идеалом.*

Доказательство: Это следует из того, что $\langle a \rangle \cdot \mathbb{H} \cong \mathbb{H}$ - см. упражнение 2.1(1). $\square$

Определение 2.11 *Факторкольцо $\widetilde{W}(k)/(\mathbb{Z} \cdot \mathbb{H})$ называется кольцом Витта квадратичных форм $W(k)$.*

Утверждение 2.12 *Множество элементов $W(k)$ естественно ото-*

ждествляется с множеством классов изоморфизма анизотропных форм над k.

Доказательство: Естественное отображение задано вложением множества классов изоморфизма анизотропных форм в множество классов изоморфизма всех невырожденных форм. То, что полученное отображение сюрьективно следует из того, что $([q_1]-[q_2])=([q_1 \perp -q_2]-[\perp_{i=1}^{\dim(q_2)} \mathbb{H}])$ в $\widetilde{W}(k)$, и $([q]-[0])=([q_{an}]-[0])+([\sum_{i=1}^{i_W(q)} \mathbb{H}]-[0])$. Инъективность же следует из того, что если q, p - анизотропны и $([q]-[p])=([\perp_{j=1}^{m} \mathbb{H}]-[0])$, то $q \cong p$. $\square$

Пример. $W(\mathbb{R})$

Анизотропные формы над $\mathbb{R}$ бывают трёх типов: 1) 0; 2) $\perp_{i=1}^{m} \langle 1\rangle$, $m>0$; и 3) $\perp_{i=1}^{n} \langle -1\rangle$, $n>0$. Это показывает, что $W(\mathbb{R}) \cong \mathbb{Z}$.