§15. Симметричные билинейные и квадратичные формы

В этом параграфе мы по умолчанию считаем, что основное поле $\Bbbk$ имеет $\mathrm{char}(\Bbbk) \neq 2$.

15.1. Пространства со скалярным произведением. Будем называть *пространством со скалярным произведением* конечномерное векторное пространство V над произвольным полем $\Bbbk$ характеристики $\mathrm{char}\,\Bbbk \neq 2$ с зафиксированной на нём невырожденной[1] симметричной билинейной формой $\beta : V \times V \to \Bbbk$. В этом и следующем разделах буква V по умолчанию обозначает именно такое пространство.

15.1.1. Ортогональные прямые суммы. Из двух пространств V_1, V_2 со скалярными произведениями β_1, β_2 можно изготовить пространство $V_1 \oplus V_2$ со скалярным произведением $\beta_1 \dot{+} \beta_2$, относительно которого слагаемые ортогональны друг другу и которое ограничивается на V_1 и V_2 в β_1 и β_2. Это скалярное произведение задаётся формулой

$$\left[\beta_1 \dot{+} \beta_2\right]\left((u_1, u_2), (w_1, w_2)\right) \stackrel{\text{def}}{=} \beta_1(u_1, u_2) + \beta_2(w_1, w_2)\,.$$

Его матрица Грама в любом базисе, первые $\dim V_1$ векторов которого образуют базис в V_1 с матрицей Грама B_1, а последние $\dim V_2$ векторов — базис в V_2 с матрицей Грама B_2, имеет блочный вид

$$\begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}.$$

Пространство $V_1 \oplus V_2$ со скалярным произведением $\beta_1 \dot{+} \beta_2$ обозначается $V_1 \dot{+} V_2$ и называется *ортогональной прямой суммой* пространств V_1 и V_2.

Упражнение 15.1. Обозначим через H_{2n} гиперболическое пространство[2] размерности $2n$. Постройте изометрический изоморфизм[3] $H_{2m} \dot{+} H_{2k} \xrightarrow{\sim} H_{2(m+k)}$.

15.1.2. Изотропные и анизотропные подпространства. Ненулевой вектор $v \in V$ называется *изотропным*, если $\beta(v, v) = 0$. Подпространство $U \subset V$, целиком состоящее из изотропных векторов, изотропно в смысле n° 14.2.2 на стр. 171, т. е. $\beta(u, w) = 0$ для всех $u, w \in U$, поскольку

$$2\beta(u, w) = \beta(u + w, u + w) - \beta(u, u) - \beta(w, w) = 0\,.$$

Подпространство $U \subset V$ называется *анизотропным*, если в нём нет изотропных векторов. Скалярное произведение на V называется *анизотропным*, если анизотропно всё пространство V. Например, евклидово скалярное произведение на вещественном векторном пространстве анизотропно. Так как анизотропная форма обладает свойствами (5,6) из предл. 14.1 на стр. 169, каждая анизотропная форма невырождена. Поэтому для любого анизотропного подпространства $U \subset V$ имеет место ортогональное разложение $V = U \oplus U^{\perp}$ из предл. 14.4 на стр. 174.

Предложение 15.1

Каждое изотропное подпространство U в пространстве V со скалярным произведением β содержится в некотором гиперболическом подпространстве $W \subset V$ размерности $\dim W = 2\dim U$. При этом любой базис подпространства U дополняется до гиперболического базиса пространства W.

[1] См. предл. 14.1 на стр. 169.
[2] См. прим. 14.2 на стр. 170.
[3] См. n° 14.1.4 на стр. 169.

Доказательство. Рассмотрим произвольный базис $u_1, u_2, \dots, u_m$ в U, дополним его до базиса в V и обозначим через $u_1^\vee, u_2^\vee, \dots, u_m^\vee$ первые m векторов ортогонально двойственного базиса. Тогда

$$\beta(u_i, u_j^\vee) = \begin{cases} 1 & \text{при } i = j \\ 0 & \text{при } i \neq j\,, \end{cases} \tag{15-1}$$

и эти соотношения ортогональности не нарушаются при добавлении к любому из векторов $u_j^\vee$ произвольной линейной комбинации векторов u_i. Заменим каждый из векторов $u_j^\vee$ на вектор

$$w_j = u_j^\vee - \frac{1}{2}\sum_{\nu=1}^{m} \beta(u_j^\vee, u_\nu^\vee)\cdot u_\nu\,.$$

Векторы $w_1, w_2, \dots, w_m$ по-прежнему удовлетворяют соотношениям (15-1) и вдобавок

$$\beta(w_i, w_j) = \beta(u_i^\vee, u_j^\vee) - \frac{1}{2}\,\beta(u_i^\vee, u_j^\vee) - \frac{1}{2}\,\beta(u_j^\vee, u_i^\vee) = 0\,,$$

т. е. $2m$ векторов u_i, w_j, $1 \leqslant i, j \leqslant m$, образуют гиперболический базис в своей линейной оболочке, которую мы и возьмём в качестве W. □

Теорема 15.1

Каждое пространство V со скалярным произведением распадается в прямую ортогональную сумму $V \simeq H_{2k} \dotplus A$, первое слагаемое которой гиперболическое и может быть нулевым или совпадать со всем пространством V, а второе слагаемое $A = H_{2k}^\perp$ анизотропно.

Доказательство. Индукция по $\dim V$. Если V анизотропно (что так при $\dim V = 1$), доказывать нечего. Если существует ненулевой изотропный вектор $e \in V$, то по предл. 15.1 он лежит в некоторой гиперболической плоскости $H_2 \subset V$, и $V = H_2 \oplus H_2^\perp$ согласно предл. 14.4. По индукции, $H_2^\perp = H_{2m} \oplus A$, где $A = H_{2m}^\perp$ анизотропно. Поэтому $V = H_{2m+2} \oplus A$ и $A = H_{2m+2}^\perp$. □

Замечание 15.1. Ниже, в теор. 15.4 на стр. 182, мы увидим, что разложение из теор. 15.1 единственно в следующем смысле: если $V \simeq H_{2k} \dotplus U \simeq H_{2m} \dotplus W$, где U и W анизотропны, то $k = m$ и существует изометрический изоморфизм $U \xrightarrow{\sim} W$.

Следствие 15.1

Следующие свойства пространства V со скалярным произведением эквивалентны:

1) V изометрически изоморфно гиперболическому пространству
2) V является прямой суммой двух изотропных подпространств
3) $\dim V$ чётна, и в V имеется изотропное подпространство половинной размерности.

Доказательство. Импликация (1)⇒(2) очевидна. Пусть выполнено (2). По предл. 14.2 размерность каждого из из двух изотропных прямых слагаемых не превышает половины размерности V, что возможно только если обе эти размерности равны $\frac{1}{2}\dim V$. Тем самым, (2)⇒(3). По предл. 15.1 на стр. 178 каждое изотропное подпространство размерности $\frac{1}{2}\dim V$ содержится в гиперболическом подпространстве размерности $\dim V$, которое таким образом совпадает со всем пространством V, что даёт импликацию (3)⇒(1). □

15.2. Изометрии и отражения. Всякий анизотропный вектор $e \in V$ задаёт разложение пространства V в прямую ортогональную сумму $V = \Bbbk \cdot e \oplus e^{\perp}$. Линейный оператор $\sigma_e : V \to V$, тождественно действующий на гиперплоскости $e^{\perp}$ и переводящий вектор e в $-e$, называется *отражением* в гиперплоскости $e^{\perp}$, см. рис. 15◇1. Произвольный вектор $v = v_e + v_{e^{\perp}} \in V$, где $v_e = e\,\beta(e,v)\,/\,\beta(e,e)$ — проекция вектора v на одномерное подпространство[1] $\Bbbk \cdot e$ вдоль гиперплоскости $e^{\perp}$, а $v_{e^{\perp}} = v - v_e \in e^{\perp}$, переходит при этом в вектор

$$\sigma_e(v) = -v_e + v_{e^{\perp}} = v - 2v_e = v - 2\,\frac{\beta(e,v)}{\beta(e,e)} \cdot e\,. \tag{15-2}$$

Упражнение 15.2. Убедитесь, что $\sigma_e \in \mathrm{O}_{\beta}(V)$ и $\sigma_e^2 = \mathrm{Id}_V$, и докажите для любых изометрии $f \in \mathrm{O}(V)$ и анизотропного вектора $e \in V$ равенство $f \circ \sigma_e \circ f^{-1} = \sigma_{f(e)}$.

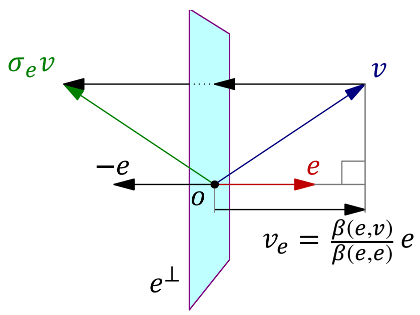

Рис. 15◇1. Отражение σ_e.

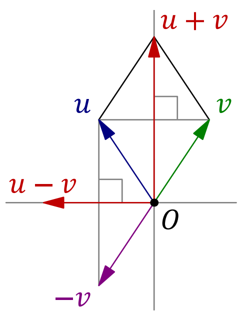

Рис. 15◇2. Отражения в ромбе.

Лемма 15.1

В любом пространстве V со скалярным произведением β для каждой пары различных анизотропных векторов u, v с равными скалярными квадратами $\beta(u,u) = \beta(v,v) \neq 0$ существует отражение, переводящее u либо в v, либо в $-v$.

Доказательство. Если u и v коллинеарны, то искомым отражением является $\sigma_v = \sigma_u$. Если u и v не коллинеарны, то хотя бы одна из двух диагоналей $u+v$, $u-v$ натянутого на них ромба (см. рис. 15◇2) анизотропна, поскольку эти диагонали ортогональны:

$$\beta(u+v, u-v) = \beta(u,u) - \beta(v,v) = 0\,,$$

и их линейная оболочка содержит анизотропные векторы u, v. Тем самым, хотя бы одно из отражений σ_{u-v}, σ_{u+v} определено. При этом $\sigma_{u-v}(u) = v$, а $\sigma_{u+v}(u) = -v$. □

Упражнение 15.3. Проверьте, последние два равенства.

Теорема 15.2

Всякая изометрия n-мерного пространства со скалярным произведением является композицией не более чем $2n$ отражений.

[1]Мы пользуемся тем, что $e^{\vee} = e\,/\,\beta(e,e)$ является двойственным к e относительно формы β базисным вектором одномерного пространства $\Bbbk e$ и по форм. (14-17) на стр. 174 ортогональная проекция произвольного вектора v на это подпространство равна $v_e = \beta(e,v)e^{\vee}$.

Доказательство. Индукция по n. Ортогональная группа одномерного пространства состоит из тождественного оператора E и отражения $-E$. Пусть $n > 1$ и $f : V \to V$ — изометрия. Выберем в V какой-нибудь анизотропный вектор v и обозначим через σ отражение, переводящее $f(v)$ в v или в $-v$. Композиция σf переводит v в $\pm v$, а значит, переводит в себя $(n-1)$-мерную гиперплоскость $v^{\perp}$. По индукции, действие σf на $v^{\perp}$ является композицией не более $2n-2$ отражений в гиперплоскостях внутри $v^{\perp}$. Продолжим их до отражений всего пространства V, добавив в зеркало каждого отражения вектор v. Композиция полученных отражений совпадает с σf на гиперплоскости $v^{\perp}$, а её действие на v либо такое же, как у σf (при $\sigma f(v) = v$), либо отличается от него знаком (при $\sigma f(v) = -v$). Поэтому σf, как оператор на всём пространстве V, есть композиция построенных $2n-2$ отражений и, возможно, ещё одного отражения в гиперплоскости $v^{\perp}$. Следовательно, $f = \sigma\sigma f$ это композиция не более $2n$ отражений. □

Упражнение 15.4. Покажите, что в анизотропном пространстве V в условиях лем. 15.1 всегда найдётся отражение, переводящее u в точности в v, и выведите отсюда, что любая изометрия n-мерного анизотропного пространства является композицией не более n отражений.

Теорема 15.3 (лемма Витта)
Пусть четыре пространства U_1, W_1, U_2, W_2 со скалярными произведениями таковы, что некоторые два из трёх пространств U_1 , $U_1 \dotplus W_1$, W_1 изометрически изоморфны соответствующей паре пространств из тройки U_2 , $U_2 \dotplus W_2$, W_2. Тогда оставшиеся третьи элементы троек тоже изометрически изоморфны.

Доказательство. Если есть изометрические изоморфизмы $f : U_1 \xrightarrow{\sim} U_2$ и $g : W_1 \xrightarrow{\sim} W_2$, то их прямая сумма $f \oplus g : U_1 \dotplus W_1 \to U_2 \dotplus W_2$, $(u, w) \mapsto (f(u), g(w))$, является требуемым изометричеким изоморфизмом. Оставшиеся два случая симметричны, и мы разберём один из них. Пусть имеются изометрические изоморфизмы

$$f : U_1 \xrightarrow{\sim} U_2 \quad \text{и} \quad h : U_1 \dotplus W_1 \xrightarrow{\sim} U_2 \dotplus W_2 \,.$$

Изометрический изоморфизм $g : W_1 \xrightarrow{\sim} W_2$ строится индукцией по $\dim U_1 = \dim U_2$. Если пространство U_1 одномерно с базисом u, то вектор u анизотропен. Поэтому векторы $f(u)$ и $h(u, 0)$ тоже анизотропны и имеют одинаковые скалярные квадраты. Обозначим через σ отражение пространства $U_2 \dotplus W_2$, переводящее $h(u, 0)$ в $\big(\pm f(u), 0\big)$. Композиция

$$\sigma h : U_1 \dotplus W_1 \xrightarrow{\sim} U_2 \dotplus W_2$$

изометрично отображает одномерное подпространство U_1 первой суммы на одномерное подпространство U_2 второй, а значит, изометрично отображает ортогональное дополнение к U_1 в первой сумме на ортогональное дополнение к U_2 во второй, что и даёт требуемый изоморфизм $\sigma h|_{W_1} : W_1 \xrightarrow{\sim} W_2$. Пусть теперь $\dim U_1 > 1$. Выберем в U_1 любой анизотропный вектор u и рассмотрим ортогональные разложения

$$U_1 \dotplus W_1 = \Bbbk \cdot u \dotplus u^{\perp} \dotplus W_1 \quad \text{и} \quad U_2 \dotplus W_2 = \Bbbk \cdot f(u) \dotplus f(u)^{\perp} \dotplus W_2 \,,$$

в которых $u^{\perp} \subset U_1$ и $f(u)^{\perp} \subset U_2$ означают ортогональные дополнения к анизотропным векторам u и $f(u)$ внутри U_1 и U_2 соответственно. Так как пространства $\Bbbk \cdot u$ и $\Bbbk \cdot f(u)$ изометрически изоморфны, по уже доказанному существуют изометрии

$$f' : u^{\perp} \xrightarrow{\sim} f(u)^{\perp} \quad \text{и} \quad h' : u^{\perp} \dotplus W_1 \xrightarrow{\sim} f(u)^{\perp} \dotplus W_2 \,,$$

к которым применимо индуктивное предположение. □

Теорема 15.4
Построенное в теор. 15.1 разложение пространства V со скалярным произведением в прямую ортогональную сумму гиперболического и анизотропного подпространств единственно в том смысле, что для любых двух таких разложений $V = H_{2k} \dotplus U = H_{2m} \dotplus W$ имеет место равенство $k = m$ и существует изометрический изоморфизм $U \simeq W$.

Доказательство. Пусть $m \geqslant k$, так что $H_{2m} = H_{2k} \dotplus H_{2(m-k)}$. Тождественное отображение $\mathrm{Id} : V \to V$ задаёт изометрический изоморфизм $H_{2k} \dotplus U \xrightarrow{\sim} H_{2k} \dotplus H_{2(m-k)} \dotplus W$. По лемме Витта существует изометрический изоморфизм $U \xrightarrow{\sim} H_{2(m-k)} \dotplus W$. Так как U анизотропно, $H_{2(m-k)} = 0$ (иначе в U будет ненулевой изотропный вектор), откуда $k = m$ и $U \simeq W$. □

Теорема 15.5
Если скалярное произведение на пространстве V невырожденно ограничивается на подпространства $U, W \subset V$ и существует изометрический изоморфизм $\varphi : U \xrightarrow{\sim} W$, то он продолжается (неоднозначно) до такого изометрического автоморфизма $f : V \xrightarrow{\sim} V$, что $f|_U = \varphi$.

Доказательство. Если есть хоть какой-нибудь изометрический изоморфизм $\psi : U^\perp \xrightarrow{\sim} W^\perp$, то изометрия $f = \varphi \oplus \psi : U \oplus U^\perp \xrightarrow{\sim} W \oplus W^\perp$, $(u, u') \mapsto \big(\varphi(h'), \psi(u')\big)$ является требуемым автоморфизмом пространства V. В силу сделанных предположений имеются изометрические изоморфизмы $\eta : U \dotplus U^\perp \xrightarrow{\sim} V$, $(u, u') \mapsto u + u'$, и $\zeta : U \dotplus W^\perp \xrightarrow{\sim} V$, $(u, w') \mapsto \varphi(u) + w'$. Композиция $\zeta^{-1}\eta : U \dotplus U^\perp \xrightarrow{\sim} U \dotplus W^\perp$ тоже изометрический изоморфизм. Так что по лемме Витта[1] ортогоналы $U^\perp$ и $W^\perp$ изометрически изоморфны. □

Следствие 15.2
Для каждого натурального числа k в диапазоне $1 \leqslant k \leqslant \dim V/2$ группа изометрий $\mathrm{O}(V)$ транзитивно действует на k-мерных изотропных и $2k$-мерных гиперболических подпространствах в V.

Доказательство. Утверждение про гиперболические подпространства вытекает непосредственно из теор. 15.5, а про изотропные — получается из него применением предл. 15.1. □

15.3. Квадратичные формы. Функция $q : V \to \Bbbk$ на n-мерном векторном пространстве V над полем $\Bbbk$ называется *квадратичной формой*, если она является однородным многочленом второй степени от координат в некотором базисе, т. е. существуют такие базис $\boldsymbol{e} = (e_1, \dots, e_n)$ в V и однородный многочлен второй степени $q_{\boldsymbol{e}} \in \Bbbk[x_1, x_2, \dots, x_n]$, что

$$q(\lambda_1 e_1 + \lambda_2 e_2 + \dots + \lambda_n e_n) = q_{\boldsymbol{e}}(\lambda_1, \lambda_2, \dots, \lambda_n)$$

для всех $(\lambda_1, \lambda_2, \dots, \lambda_n) \in \Bbbk^n$. Если $\mathrm{char}(\Bbbk) \neq 2$, то многочлен $q_{\boldsymbol{e}}$ можно записать в виде

$$q_{\boldsymbol{e}}(x_1, x_2, \dots, x_n) = \sum_{i,j=1}^{n} q_{ij} x_i x_j \,, \tag{15-3}$$

где суммирование происходит по всем парам индексов $1 \leqslant i, j \leqslant n$, а коэффициенты q_{ij} симметричны по i и j, т. е. при $i \neq j$ число $q_{ji} = q_{ij}$ равно *половине*[2] фактического коэффициента

[1] См. теор. 15.3 на стр. 181.
[2] Обратите внимание, что над полем характеристики 2 многочлен $x_1 x_2$ не записывается в виде (15-3).

при $x_i x_j$ в многочлене $q_{\boldsymbol{e}}$, получающегося после приведения подобных слагаемых в (15-3). Если организовать числа q_{ij} в симметричную матрицу $Q_{\boldsymbol{e}} = \left(q_{ij}\right)$, которую мы будем называть *матрицей Грама* многочлена $q_{\boldsymbol{e}}$, и обозначить через x и $x^t = (x_1, x_2, \dots, x_n)$ столбец и строку, составленные из переменных, то (15-3) можно переписать в виде

$$q(x_1, x_2, \dots, x_n) = \sum_{i,j=1}^{n} x_i q_{ij} x_j = x^t\, Q_{\boldsymbol{e}}\, x\,. \tag{15-4}$$

Сравнивая это с форм. (14-3) на стр. 167, мы заключаем, что $q(v) = \widetilde{q}(v, v)$, где $\widetilde{q} : V \times V \to \Bbbk$ — симметричная билинейная форма с матрицей Грама $Q_{\boldsymbol{e}}$ в базисе $\boldsymbol{e}$. Поскольку

$$q(u + w) - q(u) - q(w) = \widetilde{q}(u + w, u + w) - \widetilde{q}(u, u) - \widetilde{q}(w, w) = 2\widetilde{q}(u, w)\,,$$

симметричная билинейная форма $\widetilde{q}$ со свойством $\widetilde{q}(v, v) = q(v)$ однозначно определяется квадратичной формой q, если $\operatorname{char} \Bbbk \neq 2$. Симметричная билинейная форма $\widetilde{q}$ называется *поляризацией* квадратичной формы q. Обратите внимание, что взаимно однозначное соответствие между квадратичными и симметричными билинейными формами

$$\begin{gathered} \widetilde{q}(u, w) \mapsto q(v) = \widetilde{q}(v, v) \\ q(v) \mapsto \widetilde{q}(u, w) = \frac{1}{2}\big(q(u + w) - q(u) - q(w)\big) \end{gathered} \tag{15-5}$$

не зависят от базиса $\boldsymbol{e}$ в V. В частности, для любого базиса $\boldsymbol{f} = \boldsymbol{e}\, C_{\boldsymbol{ef}}$ в V значение $q(v)$ является однородным многочленом второй степени $q_{\boldsymbol{f}}$ от координат вектора v в базисе $\boldsymbol{f}$, причём матрица Грама этого многочлена, равная матрице Грама билинейной формы $\widetilde{q}$ в базисе $\boldsymbol{f}$, будет равна[1] $Q_{\boldsymbol{f}} = C_{\boldsymbol{ef}}^t Q_{\boldsymbol{e}}\, C_{\boldsymbol{ef}}$.

Поскольку при переходе от базиса к базису определитель Грама умножается на квадрат определителя матрицы перехода, класс числа $\det Q_{\boldsymbol{e}} \in \Bbbk$ по модулю умножения на ненулевые квадраты из поля $\Bbbk$ не зависит от выбора базиса $\boldsymbol{e}$. Мы будем обозначать этот класс $\det q \in \Bbbk/\Bbbk^{*2}$ и называть его *определителем Грама* квадратичной формы q. Квадратичная форма q называется *вырожденной*, если $\det q = 0$. Формы с $\det q \neq 0$ называются *невырожденными*. Таким образом, невырожденность квадратичной формы q означает в точности то же, что невырожденность её поляризации[2] $\widetilde{q}$. Под *рангом* квадратичной формы q мы понимаем ранг её поляризации $\widetilde{q}$, равный рангу матрицы Грама $Q_{\boldsymbol{e}}$ в любом базисе $\boldsymbol{e}$. Также, как и для симметричных билинейных форм, мы будем называть ненулевой вектор $v \in V$ *изотропным* для квадратичной формы q, если $q(v) = 0$. Квадратичная форма называется *анизотропной*, если $q(v) \neq 0$ при $v \neq 0$.

Из доказанных выше результатов про симметричные билинейные формы немедленно получаются аналогичные результаты про квадратичные формы.

Следствие 15.3 (из теор. 15.1 на стр. 179)
Всякая квадратичная форма q над произвольным полем $\Bbbk$ характеристики $\operatorname{char} \Bbbk \neq 2$ в подходящих координатах записывается в виде $x_1 x_{i+1} + x_2 x_{i+2} + \dots + x_i x_{2i} + \alpha(x_{2i+1}, x_{2i+2}\, \dots, x_r)$, где $r = \operatorname{rk}(q)$ и $\alpha(x) \neq 0$ при $x \neq 0$. □

Следствие 15.4 (из теор. 14.2 на стр. 176)
Всякая квадратичная форма над произвольным полем $\Bbbk$ характеристики $\operatorname{char} \Bbbk \neq 2$ линейной обратимой заменой переменных приводится к виду $\sum a_i x_i^2$. □

[1] См. формулу (14-2) на стр. 167.

[2] См. предл. 14.1 на стр. 169.

Следствие 15.5 (из сл. 14.1 на стр. 177)
Два однородных многочлена второй степени $f,g \in \Bbbk[x_1,x_2,\dots,x_n]$ над алгебраически замкнутым полем $\Bbbk$ характеристики $\operatorname{char}(\Bbbk) \neq 2$ тогда и только тогда переводятся друг в друга линейными обратимыми заменами переменных, когда задаваемые им квадратичные формы $f,g : \Bbbk^n \to \Bbbk$ имеют одинаковый ранг. □

Пример 15.1 (квадратичные формы от двух переменных)
Согласно сл. 15.4, ненулевая квадратичная форма от двух переменных

$$q(x) = a\,x_1^2 + 2\,b\,x_1x_2 + c\,x_2^2 = (x_1,x_2)\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \tag{15-6}$$

подходящей линейной заменой координат приводятся либо к виду αt^2 с $\alpha \neq 0$, либо к виду

$$\alpha t_1^2 + \beta\, t_2^2\,, \quad \text{где} \quad \alpha\beta \neq 0\,.$$

Условимся писать $\xi \sim \eta$ для чисел $\xi,\eta \in \Bbbk$, если $\xi = \lambda^2\eta$ для какого-нибудь ненулевого $\lambda \in \Bbbk$. Тогда в первом случае $ac - b^2 \sim \det q \sim \alpha \cdot 0 = 0$, т. е. форма q вырождена, а во втором случае $ac - b^2 \sim \det q \sim \alpha\beta \neq 0$ и форма q невырождена. Тем самым, вырожденность ненулевой квадратичной формы (15-6) означает, что с точностью до постоянного множителя она является полным квадратом линейной формы $t \in V^*$. Такая форма q зануляется вдоль одномерного подпространства $\operatorname{Ann}(t) \subset V$ и отлична от нуля на всех остальных векторах.

Если форма (15-6) невырождена, и у неё есть ненулевой изотропный вектор $v = (\vartheta_1,\vartheta_2)$, то из равенства $\alpha\vartheta_1^2 + \beta\vartheta_2^2 = 0$ вытекает, что $\vartheta_2 \neq 0$ и $-\det q \sim -\alpha\beta \sim -\beta/\alpha = (\vartheta_1/\vartheta_2)^2$ является квадратом в поле $\Bbbk$. В этом случае многочлен

$$\alpha t_1^2 + \beta\, t_2^2 = \alpha\left(t_1 + \frac{\vartheta_1}{\vartheta_2}t_2\right)\left(t_1 - \frac{\vartheta_1}{\vartheta_2}t_2\right)$$

раскладывается над полем $\Bbbk$ в произведение двух непропорциональных линейных форм. Поэтому квадратичная форма q, у которой $-\det q$ является ненулевым квадратом, тождественно зануляется на двух одномерных подпространствах и отлична от нуля на всех прочих векторах. Мы будем называть такие формы *гиперболическими*[1]. Если же $-\det q$ не квадрат, то форма q анизотропна. Число $-\det(q) = b^2 - ac$ часто обозначают через $D/4$ и называют D *дискриминантом* квадратичной формы (15-6).

15.4. Квадратичные формы над конечными полями. Из курса алгебры известно[2], что для каждого простого $p \in \mathbb{N}$ любого $m \in \mathbb{N}$ существует единственное с точностью до изоморфизма поле $\mathbb{F}_q$ из $q = p^m$ элементов, и каждое конечное поле изоморфно одному и только одному из полей $\mathbb{F}_q$. Следуя принятому в начале этой лекции соглашению, всюду далее мы считаем, что $p = \operatorname{char}\mathbb{F}_q > 2$. Зафиксируем какой-нибудь элемент $\varepsilon \in \mathbb{F}_q$, не являющийся квадратом.

Упражнение 15.5. Убедитесь, что ненулевые квадраты образуют в мультипликативной группе $\mathbb{F}_q^*$ поля $\mathbb{F}_q$ подгруппу индекса 2. В частности, нужный нам элемент ε существует, и любой ненулевой элемент поля $\mathbb{F}_q$ умножением на подходящий ненулевой квадрат можно сделать равным либо 1, либо ε.

[1]Поскольку поляризация такой формы является гиперболическим скалярным произведением.
[2]См. раздел 3.5 на стр. 45 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/1314/lec-03.pdf.

Лемма 15.2

При любых $a_1, a_2 \in \mathbb{F}_q^*$ квадратичная форма $a_1x_1^2 + a_2x_2^2$ на двумерном координатном пространстве $\mathbb{F}_q^2$ принимает все значения из поля $\mathbb{F}_q$.

Доказательство. В силу упр. 15.5 при любых фиксированных $a_1, a_2 \in \mathbb{F}_q^*$ и $b \in \mathbb{F}_q$ чисел вида $a_1x_1^2$ и чисел вида $b - a_2x_2^2$, где x_1, x_2 независимо пробегают $\mathbb{F}_q$, имеется ровно по

$$1 + \frac{q-1}{2} = \frac{q+1}{2}$$

штук. Следовательно эти два множества чисел имеют общий элемент $a_1x_1^2 = b - a_2x_2^2$. Тем самым, $f(x_1, x_2) = b$. □

Предложение 15.2

Каждая квадратичная форма q ранга r над полем $\mathbb{F}_q$ в подходящих координатах записывается как $x_1^2 + \dots + x_{r-1}^2 + x_r^2$ или как $x_1^2 + \dots + x_{r-1}^2 + \varepsilon x_r^2$, и эти две формы изометрически не изоморфны.

Доказательство. По теор. 14.2 форма q в подходящих координатах записывается в виде

$$a_1x_1^2 + \dots + a_rx_r^2 , \quad \text{где все } a_i \neq 0.$$

Согласно упр. 15.5, умножая базисные векторы на подходящие ненулевые константы, мы можем считать, что каждое a_i равно либо 1, либо ε. Если $a_i = a_j = \varepsilon$ при каких-то $i \neq j$, то в линейной оболочке U базисных векторов e_i, e_j по лем. 15.2 найдётся вектор v_i с $q(v_i) = 1$. Ортогональное дополнение к v_i в плоскости U одномерно, и форма q ограничивается на него невырожденно. Поэтому там найдётся вектор v_j с $q(v_2)$, равным 1 или ε. Заменяя e_i, e_j на v_i, v_j, мы сохраняем вид формы, но получаем $a_i = 1$, строго уменьшая тем самым число коэффициентов, равных ε. Эту процедуру можно повторять, пока таких коэффициентов останется не более одного. Формы $q = x_1^2 + \dots + x_{r-1}^2 + x_r^2$ и $q' = x_1^2 + \dots + x_{r-1}^2 + \varepsilon x_r^2$ изометрически не изоморфны, поскольку индуцированные ими невырожденные квадратичные формы q_{red} и q'_{red} на факторах $V/\ker \widetilde{q}$ и $V/\ker \widetilde{q}'$ исходного пространства V, где были заданы формы, по ядрам этих форм[1], имеют разные определи Грама: $\det q_{\text{red}} = 1$ является квадратом, а $\det q'_{\text{red}} = \varepsilon$ — нет. □

Предложение 15.3

Всякая квадратичная форма на пространстве размерности $\geqslant 3$ над полем $\mathbb{F}_q$ имеет ненулевой изотропный вектор.

Доказательство. По теор. 14.2 форма записывается в подходящем базисе как

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + \cdots .$$

Если $a_1 = 0$ или $a_2 = 0$, то вектор $(1, 0, 0, \dots)$ или вектор $(0, 1, 0, \dots)$ изотропен. Если $a_1a_2 \neq 0$, то по лем. 15.2 найдутся такие $\lambda, \mu \in \mathbb{F}_q$, что $a_1\lambda^2 + a_2\mu^2 = -a_3$. Тогда вектор $(\lambda, \mu, 1, 0, \dots)$ изотропен. □

[1] См. предл. 14.6 на стр. 176.

Предложение 15.4 (перечисление анизотропных форм)
Анизотропные формы над полем $\mathbb{F}_q$, где $q = p^m$ и $p > 2$, имеются только в размерностях 1 и 2. В размерности 2 квадратичная форма $x_1^2 + x_2^2$ анизотропна если и только если $q \equiv -1 \pmod 4$, а форма $x_1^2 + \varepsilon x_2^2$ анизотропна если и только если $q \equiv 1 \pmod 4$.

Доказательство. Из прим. 15.1 на стр. 184 вытекает, что форма $x_1^2 + x_2^2$ имеет изотропный вектор если и только если её $D/4 = -1$ является квадратом в $\mathbb{F}_q$. В этом случае вторая форма $x_1^2+\varepsilon x_2^2$ имеет $D/4 = -\varepsilon$, не являющееся квадратом, и тем самым анизотропна. Наоборот, если -1 не квадрат, то $-\varepsilon$ квадрат, и форма $x_1^2+\varepsilon x_2^2$ имеет изотропный вектор. Остаётся убедиться, что -1 является квадратом в $\mathbb{F}_q$ если и только если $q \equiv 1 \pmod 4$. Для этого рассмотрим гомоморфизм мультипликативных групп $\gamma : \mathbb{F}_q^* \to \mathbb{F}_q^*$, $x \mapsto x^{\frac{q-1}{2}}$. Поскольку порядок $|\mathbb{F}_q^*| = q - 1$, для каждого $x \in \mathbb{F}_q^*$ выполняется равенство $x^{q-1} = 1$, из которого вытекает, что все ненулевые квадраты лежат в $\ker \gamma$, а все $x \in \operatorname{im} \gamma$ имеют $x^2 = 1$, откуда $\operatorname{im} \gamma \subset \{\pm 1\}$. Так как у уравнения $x^{\frac{q-1}{2}} = 1$ не более $(q-1)/2$ корней в поле $\mathbb{F}_q$, образ γ имеет порядок 2, а $\ker \gamma \subset \mathbb{F}_q^*$ имеет индекс 2 и совпадает с группой квадратов, т. е. $x \in \mathbb{F}_q^*$ является квадратом тогда и только тогда, когда $x^{\frac{q-1}{2}} = 1$. В частности, -1 квадрат если и только если $(q-1)/2$ чётно. □

15.5. Вещественные квадратичные формы. Из сл. 15.4 вытекает, что любая квадратичная форма на вещественном вектором пространстве V в подходящем базисе записывается в виде

$$q(x) = x_1^2 + x_2^2 + \dots + x_p^2 - x_{p+1}^2 - x_{p+2}^2 - \dots - x_{p+m}^2 \,. \tag{15-7}$$

Для этого надо перейти к базису с диагональной матрицей Грама и поделить каждый базисный вектор e_i с $q(e_i) \neq 0$ на $\sqrt{|q(e_i)|}$. Числа p и m в представлении (15-7) называются *положительным* и *отрицательным индексами инерции*, упорядоченная пара (p, m) — *сигнатурой*, а разность $p - m$ — просто *индексом* вещественной квадратичной формы q.

Теорема 15.6
Числа p и m в представлении (15-7) не зависят от выбора базиса, в котором квадратичная форма имеет вид (15-7).

Доказательство. Будем считать, что $p \geqslant m$, поскольку противоположный случай сводится к этому заменой q на $-q$. Сумма $p + m = \operatorname{rk} q$ равна рангу билинейной формы $\widetilde{q}$ и не зависит от выбора базиса. Линейная оболочка базисных векторов e_k с номерами $k > p+m$ является ядром билинейной формы $\widetilde{q}$. Классы $[e_i]$ остальных базисных векторов по модулю $\ker \widetilde{q}$ образуют базис фактор пространства $W = V/\ker \widetilde{q}$. По предл. 14.6 на стр. 176 форма $\widetilde{q}$ корректно задаёт на W невырожденную симметричную билинейную форму $\widetilde{q}_{\mathrm{red}}([u],[w]) = \widetilde{q}(u, w)$, которая в базисе из классов $[e_i]$ с $1 \leqslant i \leqslant p+m$ записывается той же самой формулой (15-7). Каждая пара базисных векторов $[e_i]$, $[e_{p+i}]$ порождает гиперболическую плоскость с гиперболическим базисом из векторов $\big([e_i] \pm [e_{p+i}]\big)/\sqrt{2}$. Поэтому форма $\widetilde{q}_{\mathrm{red}}$ является прямой ортогональной суммой гиперболического пространства H_{2m}, натянутого на классы $[e_i]$, $[e_{p+i}]$ с $1 \leqslant i \leqslant m$, и анизотропного пространства размерности $p - m$, натянутого на оставшиеся классы $[e_j]$ с $m < j \leqslant p$. По теор. 15.4 на стр. 182 размерности гиперболического и анизотропного слагаемых не зависят от выбора разложения пространства со скалярным произведением в ортогональную сумму гиперболического и анизотропного. Поэтому индекс $p-m$ и отрицательный индекс инерции m не зависят от выбора базиса, в котором форма q имеет вид (15-7). □

Следствие 15.6 (из доказательства теор. 15.6)
Для каждого n на пространстве $\mathbb{R}^n$ с точностью до изометрического изоморфизма имеются ровно два анизотропных скалярных произведения — евклидово и *антиевклидово*, получающееся из евклидова сменой знака. Вещественные квадратичные формы положительного индекса имеют ненулевое евклидово анизотропное слагаемое, а формы отрицательного индекса — ненулевое антиевклидово анизотропное слагаемое, размерности которых равны абсолютной величине индекса. Гиперболичность невырожденной вещественной квадратичной формы равносильна тому, что её индекс равен нулю. □

Следствие 15.7
Два однородных многочлена второй степени $f, g \in \mathbb{R}[x_1, x_2, \dots, x_n]$ тогда и только тогда переводятся друг в друга линейными обратимыми заменами переменных, когда задаваемые ими квадратичные формы $f, g : \mathbb{R}^n \to \mathbb{R}$ имеют одинаковый ранг и индекс. □

15.5.1. Квадратичные формы на евклидовом пространстве. Если на вещественном векторном пространстве V имеется евклидова структура, то поляризацию $\widetilde{q}$ любой квадратичной формы q на V можно единственным образом представить в виде $\widetilde{q}(u, w) = (u, F_q w)$, где скобки в правой части означают евклидово скалярное произведение на V, а через $F_q : V \to V$ обозначен линейный оператор, отвечающий симметричной билинейной форме $\widetilde{q}$ при изоморфизме между формами и операторами[1], который задаётся евклидовым скалярным произведением. В любом евклидово ортонормальном базисе пространства V матрица оператора F_q совпадает с матрицей Грама формы $\widetilde{q}$ в этом базисе. В частности, она симметрична, а значит, оператор F_q евклидово самосопряжён. Согласно теор. 15.7 на стр. 187 в пространстве V найдётся евклидово ортонормальный базис, в котором матрица оператора F_q диагональна и имеет на диагонали в точности все собственные числа оператора F_q учётом их кратностей. Мы получаем следующие полезные результаты.

Теорема 15.7 (теорема о нормальном базисе)
Для любой квадратичной формы q на евклидовом пространстве V существует евклидово ортонормальный базис, в котором матрица Грама формы q диагональна. Диагональные элементы такой матрицы с точностью до перестановки не зависят от выбора указанного базиса и равны собственным числам того единственного линейного оператора $f : V \to V$, для которого

$$q(v) = (v, fv) \quad \text{при всех } v \in V.$$

Если все $\dim V$ собственных чисел различны, то ортонормальный базис, в котором матрица Грама формы q диагональна, единственен с точностью до перестановки базисных векторов и замены их направлений на противоположные. □

Следствие 15.8
Два однородных многочлена второй степени $f, g \in \mathbb{R}[x_1, x_2, \dots, x_n]$ тогда и только тогда переводятся друг в друга ортогональными[2] заменами переменных, когда их матрицы Грама в ортонормальном базисе имеют одинаковые наборы собственных чисел (с учётом кратностей). □

---

[1] См. n° 14.2.4 на стр. 173.
[2] Т. е. сохраняющими стандартное евклидово скалярное произведение на $\mathbb{R}^n$

15.5.2. Вычисление сигнатуры квадратичной формы на $\mathbb{R}^n$ можно осуществить несколькими способами.

Пример 15.2 (использование евклидовой структуры)
Согласно теор. 15.7 и предваряющему её рассуждению, положительный и отрицательный индексы инерции квадратичной формы на $\mathbb{R}^n$ равны количествам положительных и отрицательных собственных чисел (с учётом кратностей) матрицы Грама этой формы в любом ортонормальном для стандартной евклидовой структуры базисе пространства $\mathbb{R}^n$.

Пример 15.3 (метод Якоби – Сильвестра)
Обозначим через $V_k \subset \mathbb{R}^n$ линейную оболочку первых k базисных векторов $e_1, \dots, e_k$, а через $\varDelta_k$ их определитель Грама, т. е. рассматриваемый с точностью до умножения на ненулевые положительные числа[1] главный угловой $k \times k$ минор матрицы Грама формы, сосредоточенный в первых k строках и столбцах. Если ограничение формы на подпространство V_k неособо, то $\varDelta_k = (-1)^{m_k}$, где показатель m_k равен отрицательному индексу инерции ограничения формы на V_k. Таким образом, когда все $\varDelta_i \neq 0$, соседние миноры $\varDelta_k$, $\varDelta_{k+1}$ различаются знаком если и только если отрицательный индекс инерции $m_{k+1} = m_k + 1$. Поэтому полный отрицательный индекс инерции $m = m_n$ в этом случае равен числу перемен знака в последовательности $1, \varDelta_1, \varDelta_2, \dots, \varDelta_n$.

Если некоторый $\varDelta_k = 0$, но при этом $\varDelta_{k-1}$ и $\varDelta_{k+1}$ оба ненулевые, то ограничения формы на подпространства V_{k+1} и V_{k-1}, а также на двумерное ортогональное дополнение W к подпространству V_{k-1} внутри V_{k+1} невырождены, и в W имеется изотропный вектор, порождающий ядро ограничения формы на подпространство V_k, где она вырождена. Тем самым, $W \simeq H_2$ является гиперболической плоскостью с сигнатурой $(1,1)$, и из ортогонального разложения $V_{k+1} = V_{k-1} \dotplus W$ вытекает равенство $(p_{k+1}, m_{k+1}) = (p_{k-1}+1, m_{k-1}+1)$. Обратите внимание, что в этом случае $\varDelta_{k-1}$ и $\varDelta_{k+1}$ имеют противоположные знаки, т. е. при $\varDelta_k = 0$ неравенство $\varDelta_{k-1}\varDelta_{k+1} > 0$ невозможно.

Если $\varDelta_k = \varDelta_{k+1} = 0$, но при этом $\varDelta_{k-1}$ и $\varDelta_{k+2}$ оба ненулевые, то $V_{k+2} = V_{k-1} \dotplus W$, где W — трёхмерное ортогональное дополнение к V_{k-1} внутри V_{k+2}. Как и выше, ограничение формы на W невырождено, и в W есть изотропный вектор. Поэтому W имеет сигнатуру $(2,1)$ или $(1,2)$, откуда $(p_{k+2}, m_{k+2}) = (p_{k-1}+2, m_{k-1}+1)$, если $\varDelta_{k-1}\varDelta_{k+2} < 0$, и $(p_{k+2}, m_{k+2}) = (p_{k-1}+1, m_{k-1}+2)$, если $\varDelta_{k-1}\varDelta_{k+2} > 0$.

Итак, когда в последовательности $1, \varDelta_1, \varDelta_2, \dots, \varDelta_n$ не встречается более двух нулей подряд, прочтение её слева направо позволяет проследить за изменением сигнатуры (p_i, m_i) ограничения формы на пространства V_i с ненулевыми $\varDelta_i$ и найти индекс.

Скажем, пусть $\varDelta_1 < 0$, $\varDelta_2 = 0$, $\varDelta_3 > 0$, $\varDelta_4 = 0$, $\varDelta_5 = 0$, $\varDelta_6 < 0$. Тогда

$$(p_1, m_1) = (0,1), \quad (p_3, m_3) = (2,1), \quad (p_6, m_6) = (3,3).$$

Примером такой формы является форма с матрицей Грама

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

[1] Т. е. на ненулевые квадраты поля $\mathbb{R}$.

Пример 15.4 (метод Гаусса)
Над любым полем $\Bbbk$ перейти от произвольного базиса $e_1, \dots, e_n$ к ортогональному базису заданной симметричной билинейной формы $\widetilde{q}$ можно при помощи гауссовых элементарных преобразований базисных векторов[1]: перестановок каких-нибудь двух векторов e_i, e_j местами и замен одного из базисных векторов e_i на вектор $e_i' = e_i + \lambda e_j$, где $j \neq i$, а $\lambda \in \Bbbk$ произвольно, или на вектор $e_i' = \lambda e_i$, где $\lambda \in \Bbbk^*$ отлично от нуля. При перестановке местами векторов e_i, e_j в матрице Грама формы $\widetilde{q}$ одновременно переставляются друг с другом i-я и j-я строки, а также i-й и j-й столбцы. Обратите внимание, что диагональные элементы $\widetilde{q}(e_i, e_i)$ и $\widetilde{q}(e_j, e_j)$ при этом переставятся друг с другом, а элементы $\widetilde{q}(e_i, e_j) = \widetilde{q}(e_j, e_i)$ останутся без изменения. Например, перестановка первого и третьего базисного вектора действует на симметричную 3×3 матрицу так:

$$\begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \mapsto \begin{pmatrix} f & e & c \\ e & d & b \\ c & b & a \end{pmatrix}.$$

При замене вектора e_i вектором λe_i i-я строка и i-й столбец матрицы Грама одновременно умножаются на λ. Обратите внимание, что диагональный элемент $\widetilde{q}(e_i, e_i)$ при этом умножится на λ^2. Например, замена e_2 на $2e_2$ подействует на предыдущую матрицу так:

$$\begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \mapsto \begin{pmatrix} a & 2b & c \\ 2b & 4d & 2e \\ c & 2e & f \end{pmatrix}.$$

Наконец, замена e_i на $e_i' = e_i + \lambda e_j$ преобразует стоящие в i-й строке и i-м столбце недиагональные элементы $q_{ik} = \widetilde{q}(e_i, e_k)$ и $q_{ki} = \widetilde{q}(e_k, e_i)$ с $k \neq i$ в элементы $q_{ik}' = q_{ik} + \lambda q_{jk}$ и $q_{ki}' = q_{ki} + \lambda q_{kj}$ соответственно, а диагональный элемент $q_{ii} = \widetilde{q}(e_i, e_i)$ — в

$$q_{ii}' = q_{ii} + \lambda q_{ij} + \lambda q_{ji} + \lambda^2 q_{jj}.$$

Иными словами, в матрице Грама к i-й строке прибавится j-я, умноженная на λ, и одновременно к i-у столбцу прибавится j-й, умноженный на λ, после чего к диагональному элементу в позиции[2] (i, i) добавится ещё диагональный элемент из позиции (j, j), умноженный на λ^2. Например, замена e_3 на $e_3 + 3e_2$ подействует на предыдущую матрицу так:

$$\begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \mapsto \begin{pmatrix} a & b & c + 3b \\ b & d & e + 3d \\ c + 3b & e + 3d & f + 6e + 9d \end{pmatrix}.$$

Метод Гаусса заключается в том, чтобы при помощи описанных трёх типов преобразований матрицы Грама превратить заданную симметричную матрицу в диагональную. Для вещественной формы количества положительных и отрицательных чисел на диагонали итоговой матрицы — это в точности положительный и отрицательный индексы инерции.

Для иллюстрации вычислим методом Гаусса сигнатуру вещественной квадратичной формы с матрицей Грама

$$\begin{pmatrix} -1 & 2 & 0 & -3 \\ 2 & 2 & -1 & 0 \\ 0 & -1 & 0 & -2 \\ -3 & 0 & -2 & 0 \end{pmatrix}.$$

[1] См. n° 6.1 на стр. 74.
[2] Обратите внимание, что в текущий момент этот элемент уже увеличился на $\lambda q_{ij} + \lambda q_{ji} = 2\lambda q_{ij}$.

Сначала обнулим 1-ю строку и 1-й столбец вне диагонали, добавляя к векторам e_2, e_4 соответственно векторы $2e_1$ и $-3e_1$:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 6 & -1 & -6 \\ 0 & -1 & 0 & -2 \\ 0 & -6 & -2 & 9 \end{pmatrix}.$$

Теперь обнулим вне диагонали 2-ю строку и 2-й столбец, добавляя к текущим векторам e_3, e_4 соответственно текущие векторы $e_1/6$ и e_1:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & -\frac{1}{6} & -3 \\ 0 & 0 & -3 & 3 \end{pmatrix}.$$

Наконец, обнулим вне диагонали 3-ю строку и 3-й столбец, добавляя к текущему вектору e_4 текущий вектор $-18e_3$:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & -\frac{1}{6} & 0 \\ 0 & 0 & 0 & 57 \end{pmatrix}.$$

Таким образом, форма имеет сигнатуру $(2,2)$.

15.6. Самосопряжённые операторы. Пусть на векторном пространстве V над произвольным полем $\Bbbk$ задана невырожденная симметричная билинейная форма

$$(\,*\,,\,*\,)\colon V\times V\to\Bbbk\,,\quad u,w\mapsto(u,w)\,. \tag{15-8}$$

Как и в евклидовом пространстве[1], будем называть линейный оператор $f: V\to V$ *самосопряжённым* относительно скалярного произведения (15-8), если $(fu,w)=(u,fw)$ при всех $u,w\in V$. Самосопряжённость оператора f равносильна тому, что при биекции между формами и операторами, которая задаётся скалярным произведением[2] (15-8), отвечающая оператору f билинейная форма $\beta_f(u,w)=(u,fw)$ является симметричной.

Упражнение 15.6. Убедитесь в этом.

На матричном языке самосопряжённость оператора f означает, что его матрица F в любом базисе пространства V связана с матрицей Грама G скалярного произведения (15-8) в том же базисе соотношением $F^tG=GF$. Дословно теми же рассуждениями, что и для евклидовых пространств[3] устанавливаются два ключевых свойства самосопряжённых операторов:

Упражнение 15.7. Пусть линейный оператор $f: V\to V$ самосопряжён. Покажите, что
- а) для любого f-инвариантного подпространства $U\subset V$ ортогонал $U^\perp$ тоже f-инвариантен
- б) собственные векторы оператора f с разными собственными значениями ортогональны.

[1] Ср. с n° 12.3 на стр. 148.
[2] См. n° 14.2.4 на стр. 173.
[3] См. лем. 12.2 и лем. 12.3 на стр. 149.

Предложение 15.5

Если характеристический многочлен самосопряжённого линейного оператора $f : V \to V$ полностью раскладывается в поле $\Bbbk$ на линейные множители и все ненулевые собственные векторы оператора f анизотропны, то в пространстве V имеется ортогональный базис из собственных векторов оператора f.

Доказательство. Индукция по $\dim V$. Если оператор f является умножением на скаляр (что имеет место при $\dim V = 1$), то подойдёт любой ортогональный базис пространства V. Допустим, что $\dim V > 1$ и оператор f не скалярен. Поскольку характеристический многочлен $\det(tE - F)$ имеет корни в поле $\Bbbk$, у оператора F есть ненулевое собственное подпространство

$$V_\lambda = \{v \in V \mid fv = \lambda v\} \subsetneq V\,.$$

По условию леммы, оно анизотропно, и значит, скалярное произведение ограничивается на него невырождено. Поэтому $V = V_\lambda \oplus V_\lambda^\perp$, и ограничение скалярного произведения на $V_\lambda^\perp$ тоже невырождено. По упр. 15.7 оператор f переводит подпространство $V_\lambda^\perp$ в себя. Тем самым, характеристический многочлен оператора f является произведением характеристических многочленов ограничений $f|_{V_\lambda}$ и $f|_{V_\lambda^\perp}$. В силу единственности разложения на множители в кольце $\Bbbk[t]$ и предположения леммы, каждый из этих двух характеристических многочленов полностью раскладываются на линейные множители в поле $\Bbbk$. По индуктивному предположению, в подпространстве $V_\lambda^\perp$ есть ортогональный базис из собственных векторов оператора f. Добавляя к нему любой ортогональный базис собственного пространства V_λ, получаем нужный базис в V. $\square$

Упр. 15.5. Ненулевые квадраты составляют образ гомоморфизма мультипликативных групп

$$\mathbb{F}_q^* \to \mathbb{F}_q^*, \quad x \mapsto x^2 .$$

Так как уравнение $x^2 = 1$ имеет в поле $\mathbb{F}_q$ ровно два корня $x = \pm 1$, ядро этого гомоморфизма состоит из двух элементов, а значит, образ является подгруппой порядка $(q-1)/2$.

Упр. 15.6. Если оператор f самосопряжён, то $\beta_f(u,w) = (u,fw) = (fu,w) = (w,fu) = \beta_f(w,u)$. Если билинейная форма β_f симметрична, то $(fu,w) = (w,fu) = \beta_f(w,u) = \beta_f(u,w) = (u,fw)$

Упр. 15.7. Пусть $w \in U^\perp$, т. е. $(u,w) = 0$ для всех $u \in U$. Тогда $(u,fw) = (fu,w) = 0$ для всех $u \in U$, ибо $fu \in U$. Тем самым, $fw \in U^\perp$. Если $fu = \lambda u$ и $fw = \mu w$, то из равенства $(fu,w) = (u,fw)$ вытекает равенство $(\lambda - \mu) \cdot (u,w) = 0$.