Алгебра

Антон Ермилов, Александр Киракосян
При поддержке Наташи Мурашкиной и Анны Никифоровской
По лекциям Афанасьевой Софьи

11 января 2018 г.

Содержание

1. Формы над линейными пространствами

1.1. Билинейные и полуторалинейные формы

***Определение* 1.1.**
V — векторное пространство над K.

Отображение $\alpha : V \times V \to K$ называется билинейной формой если α удовлетворяет следующим условиям:

1. $\alpha(x_1 + x_2, y) = \alpha(x_1, y) + \alpha(x_2, y)$
2. $\alpha(\lambda x, y) = \lambda\alpha(x, y)$
3. $\alpha(x, y_1 + y_2) = \alpha(x, y_1) + \alpha(x, y_2)$
4. $\alpha(x, \lambda y) = \lambda\alpha(x, y)$

Пример.

1) $V = \mathbb{R}^n$, $\alpha(x, y) = \langle x, y\rangle$.
2) $V = C[a, b]$, $\alpha(f, g) = \int\limits_a^b f(x)g(x)\,dx$
3) $V = K^2$, $\alpha(x, y) = \det\big((x, y)\big)$
4) $V = K^{n\times n}$, $\alpha(X, Y) = \mathrm{tr}(X \cdot Y)$

Обозначение.
K — поле.

Рассмотрим автоморфизм $i : K \to K$, такое что, $i^2 = \mathrm{id}$. Тогда над таким полем можно ввести операцию сопряжения, а именно $\overline{\lambda} = i(\lambda)$.

Замечание.
Сопряжение сохраняет 1 и 0 поля K.

***Определение* 1.2.**
Отображение $\alpha : V \times V \to K$ называется полуторалинейной формой, если α удовлетворяет следующим свойствам:

1. $\alpha(x_1 + x_2, y) = \alpha(x_1, y) + \alpha(x_2, y)$
2. $\alpha(\lambda x, y) = \overline{\lambda}\alpha(x, y)$
3. $\alpha(x, y_1 + y_2) = \alpha(x, y_1) + \alpha(x, y_2)$
4. $\alpha(x, \lambda y) = \lambda\alpha(x, y)$

***Определение* 1.3.**

Пусть V — конечномерное векторное пространство над полем K с выбранным базисом e_1, e_2 … e_n, а α — билинейная или полуторалинейная форма.

Матрицу A имеющую вид:

$$A = \begin{pmatrix} \alpha(e_1,e_1) & \alpha(e_1,e_2) & \cdots & \alpha(e_1,e_n) \\ \alpha(e_2,e_1) & \alpha(e_2,e_2) & \cdots & \alpha(e_2,e_n) \\ \vdots & \vdots & \ddots & \vdots \\ \alpha(e_n,e_1) & \alpha(e_n,e_2) & \cdots & \alpha(e_n,e_n) \end{pmatrix}$$

будем называть матрицей формы α в базисе e.

Утверждение 1.1.

Пусть V — конечномерное пространство над K, α билинейная форма, а A — ее матрица в базисе e_1, e_2 … e_n.

Пусть $x = \sum x_i e_i$, $y = \sum y_i e_i$ — вектора из пространства V. Тогда $\alpha(x,y) = x^T A y$.

Доказательство.

$\alpha(x,y) = \alpha(\sum x_i e_i, \sum y_i e_i) = \sum\limits_{i,j} x_i y_j \alpha(e_i,e_j) = x^T A y$ □

Замечание.

Для полуторалинейной формы $\alpha(x,y) = \overline{x}^T A y$.

Утверждение 1.2.

Пусть V — конечномерное векторное пространство над K, C — матрица перехода от базиса e к базису f.

Тогда, если A_e — матрица формы α в базисе e, а A_f — матрица формы α в базисе f, то $A_f = \overline{C}^T A_e C$.

Доказательство.

Пусть $e = (e_1, e_2, \ldots, e_n)$, $f = (f_1, f_2, \ldots, f_n)$

Рассмотрим любые x, $y \in V$. Т.к. C — матрица перехода, то $x_e = C x_f$, $y_e = C y_f$.

$\alpha(x,y) = \overline{x}_e^T A_e y_e = (\overline{C}\,\overline{x}_f)^T A_e (C y_f) = \overline{x}_f^T \overline{C}^T A_e C y_f$

С другой стороны, если расписывать форму через матрицу в базисе f:

$\alpha(x,y) = \overline{x}_f^T A_f y_f = \overline{x}_f^T \overline{C}^T A_e C y_f \implies A_f = \overline{C}^T A_e C$

Последний переход верен. т.к. равенство было получено для любых $x, y \in V$. □

Замечание. Утверждение для случая, когда α билинейна получается удалением всех операций сопряжения, т.е. $A_f = C^T A_e C$.

1.2. Ядро билинейной формы и ортогональное дополнение

***Определение* 1.4.**

V — векторное пространство над полем K, а α — билинейная или полуторалинейная форма.

Множество $\{y \in V : \alpha(x,y) = 0 \ \ \forall\, x \in V\}$ называется ядром формы α и обозначается $\operatorname{Ker}\alpha$.

Форма α называется невырожденной, если $\operatorname{Ker}\alpha = \{0\}$

***Определение* 1.5.**

V — векторное пространство над полем K, $\operatorname{Char} K \neq 2$. α — билинейная форма.

α называется симметричной билинейной формой, если $\forall x, y \in V:\ \alpha(x,y) = \alpha(y,x)$

α называется антисимметричной билинейной формой, если $\forall x, y \in V:\ \alpha(x,y) = -\alpha(y,x)$

***Определение* 1.6.**

α — билинейная (анти-)симметричная форма

Вектора $x, y \in V,\ x, y$ называются ортогональными ($x \perp y$), если $\alpha(x,y) = 0$

***Определение* 1.7.**

U — подпространство V

Множество $U^\perp = \{v \in V : v \perp u\ \ \forall u \in U\}$ называется ортогональным дополнением подпространства U.

Свойства.

1. $U^\perp$ — подпространство V
2. $V^\perp = \operatorname{Ker} \alpha$
3. Если e_1, e_2, …, e_m — базис U, то $v \in U^\perp \iff v \underset{i=1..m}{\perp} e_i$

Доказательство.

1. $0 \in U^\perp$

   $u, v \in U^\perp \implies u + \lambda v \in U^\perp$, т.к. $\alpha(u + \lambda v, x) = \alpha(u,x) + \lambda\alpha(v,x) = 0$
2. Ровно по определению ядра пространства.
3. Стрелка вправо очевидна (т.к. если $v \in U^\perp$, то, в частности, $x \perp e_i$).

   Стрелка влево. Если $x = \sum \beta_i e_i \in U$, то $\alpha(v,x) = \alpha(v, \sum \beta_i e_i) = \sum \beta_i \alpha(v, e_i) = 0$

□

Замечание.

$\operatorname{Ker} \alpha$ — подпространство V (т.к. $\operatorname{Ker} \alpha = V^\perp$ — подпространство V).

***Определение* 1.8.**

α — симметричная билинейная форма.

$\operatorname{rank} \alpha = \operatorname{rank} A$, где A — матрица формы α в базисе e_1, …, e_n.

Утверждение 1.3.

$\dim \operatorname{Ker} \alpha = \dim V - \operatorname{rank} A$, где A — матрица формы α в каком-то базисе.

Доказательство.

Пусть A была записана в базисе $e_1, \ldots, e_n$.

$v \in \operatorname{Ker} \alpha \iff v \in V^\perp \iff v \underset{i=1..m}{\perp} e_i$, т.е. $\alpha(e_i, v) = 0$ для всех i.

Распишем $\alpha(e_i, v)$.

$$0 = \alpha(e_i, v) = \overline{e_i}^T A v = \big(0, \dots, 1, \dots, 0\big) \begin{pmatrix} \alpha(e_1, e_1) & \cdots & \alpha(e_1, e_n) \\ \alpha(e_2, e_1) & \cdots & \alpha(e_2, e_n) \\ \vdots & \ddots & \vdots \\ \alpha(e_n, e_1) & \cdots & \alpha(e_n, e_n) \end{pmatrix} v = \big(\alpha(e_i, e_1), \dots, \alpha(e_i, e_n)\big)\, v$$

Значит, мы получили, что любая строчка матрицы A, домноженная на v равна 0. Это означает, что $Av = 0 \iff v \in \operatorname{Ker} A$.

Т.е. $V^\perp = \operatorname{Ker} A$. При этом мы знаем, что $\dim \operatorname{Ker} A = \dim V - \operatorname{rank} A$, т.е. получили требуемое. □

Следствие.

1. Ранг матрицы формы α не зависит от выбора базиса, в частности, определение $\operatorname{rank} \alpha$ корректно.
2. α — невырождена $\iff$ строки A линейно независимы.

Доказательство.

1. $\operatorname{rank} A = \dim V - \dim \operatorname{Ker} \alpha$ — не зависит от базиса.
2. $\operatorname{rank} A = \dim V - \dim \operatorname{Ker} \alpha = \dim V$, а значит строки A линейно независимы.

□

Замечание.

Получаем утверждение $\dim \operatorname{Ker} \alpha = \dim V - \operatorname{rank} \alpha$.

Лемма.

V — конечномерное векторное пространство над полем K, U — подпространство V, а α — симметричная или антисимметричная билинейная форма.

Тогда если α — невырождена, то $\dim U^\perp = \dim V - \dim U$ и $U^{\perp\perp} = U$.

Доказательство.

Пусть $e_1, \dots, e_m$ — базис U.

Дополним его до базиса пространства V: $e_1, \dots, e_m, e_{m+1}, \dots, e_n$.

Пусть матрица A — матрица формы α. Введем матрицу B состоящую из первых m строк матрицы A. Размер матрицы B будет $m \times n$. Докажем, что $U^\perp = \operatorname{Ker} B$.

$v \in U^\perp \iff \forall i \in [1..m] :\ \alpha(e_i, v) = 0$.

Рассмотрим $\alpha(e_i, v)$.

$$0 = \alpha(e_i, v) = \overline{e_i}^T A v = \big(0, \dots, 1, \dots, 0\big) \begin{pmatrix} \alpha(e_1, e_1) & \cdots & \alpha(e_1, e_n) \\ \alpha(e_2, e_1) & \cdots & \alpha(e_2, e_n) \\ \vdots & \ddots & \vdots \\ \alpha(e_n, e_1) & \cdots & \alpha(e_n, e_n) \end{pmatrix} v = \big(\alpha(e_i, e_1), \dots, \alpha(e_i, e_n)\big)\, v$$

(Эта строка аналогична строке из доказательства утверждения 1.3)

Таким образом, мы получили, что первые m строк матрицы A после домножения на v дают 0. Это означает, что $Bv = 0 \iff v \in \operatorname{Ker} B$, что мы и хотели.

Далее, т.к. $U^\perp = \operatorname{Ker} B$, то $\dim U^\perp = \dim \operatorname{Ker} B = n - \operatorname{rank} B$.

Осталось доказать, что $\operatorname{rank} B = m$, т.е. все строки B линейно независимы. Это очевидно следует из того, что все строки A линейно независимы (т.к. α невырожденная).

Теперь докажем, что $U^{\perp\perp} = U$.

$\dim U^{\perp\perp} = n - \dim U^{\perp} = n - (n - m) = m = \dim U$

Осталось заметить, что $U \subseteq U^{\perp\perp}$.

Действительно, пусть $x \in U$, тогда нам нужно проверить, что $\forall y \in U^{\perp} :\ \alpha(x, y) = 0$, т.е., что x ортогонален всем векторам из $U^{\perp}$.

$\alpha(x, y) = 0$ т.к. $x \in U,\ y \in U^{\perp}$. □

Замечание.

Конечномерность существенна.

Пример.

Рассмотрим $V = C([a, b]),\ \ \alpha(f, g) = \int\limits_a^b fg,\ \ U = \{f : f(a) = 0\} \leqslant V$.

Проверим, что $U^{\perp\perp} \neq U$.

$U^{\perp} = \{g : \int\limits_a^b fg = 0\ \ \forall f : f(a) = 0\} = \{0\}$ (строго доказано не было)

Тогда, $U^{\perp\perp} = V \neq U$.

1.3. Ортогонализация Грама-Шмидта

Лемма.

Пусть V — конечномерное векторное пространство над полем K

α — билинейная форма, $U \leqslant V$.

Тогда $V = U \oplus U^{\perp}$ если и только если $\alpha\Big|_U$ — невырожденная.

Доказательство.

Заметим, что $U \cap U^{\perp} = \{v \in U : \alpha(u, v) = 0\ \ \forall u \in U\} = \operatorname{Ker} \alpha\Big|_U$

Значит, $U \cap U^{\perp} = \{0\} \iff \alpha\Big|_U$ — невырождена.

Тогда мы получили стрелку вправо. А именно, если сумма прямая, то пересечение состоит только из нуля, а тогда суженная форма невырожденная.

В другую сторону, мы получили, что пересечение имеет размерность 0. Изучим сумму размерностей $\dim U + \dim U^{\perp}$.

Пусть базис U это $e_1, \dots e_m$. Дополним до базиса V: $e_1, \dots, e_m, e_{m+1}, \dots e_n$.

Рассмотрим матрицу B состоящую из первых m строк матрицы формы α. Заметим, что в силу невырожденности формы эти строки будут линейно независимы.

Пусть $v \in U^{\perp}$.

Тогда $\alpha(e_i, v) = 0\ \ \forall i \in [1..m] \iff Bv = 0 \iff v \in \operatorname{Ker} B$.

А значит, $\dim U^{\perp} = \dim V - \operatorname{rank} B = \dim V - m = \dim V - \dim U$.

Получили, что $\dim U^{\perp} + \dim U = \dim V$.

А так как $U \cap U^{\perp} = \{0\}$, то сумма будет прямой, что и требовалось. □

Утверждение 1.4.

Пусть $e_1, \ldots, e_n$ — базис пространства V, α — билинейная форма, а ее матрица в базисе e это A.

Тогда α — симметричная $\iff A = A^T$

Доказательство.

Очевидно из определений матрицы формы и симметричной формы. □

Утверждение 1.5.

Билинейная симметричная форма однозначно определяется своими значениями при совпадающих векторах, т.е. значениями вида $\alpha(v, v)$.

Доказательство.

$\alpha(x + y, x + y) = \alpha(x, x) + 2\alpha(x, y) + \alpha(y, y)$

$\alpha(x, y) = \frac{1}{2}(\alpha(x + y, x + y) - \alpha(x, x) - \alpha(y, y))$. □

Следствие.

Если $\alpha(x, x) = 0\ \forall x$, то $\alpha = 0$.

Замечание.

Теперь мы можем определять лишь форму $q(x) = \alpha(x, x)$. По ней однозначно восстанавливается вся билинейная форма α.

***Определение* 1.9.**

Базис $e_1, \ldots, e_n$ назовём ортогональным (для формы α), если $e_i \perp e_j\ \ \forall\, i \neq j$

Базис $e_1, \ldots, e_n$ назовём ортонормированным (для формы α), если $\alpha(e_i, e_j) = \delta_{i,j} = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$

Замечание.

Форма α имеет диагональный вид в ортогональном базисе и единично-диагональный в ортонормированном.

Утверждение 1.6.

Для любой симметричной билинейной формы существует ортогональный базис.

Доказательство.

Индукция по $\dim V = n$. База при $n = 1$ очевидна.

Переход $n \to n + 1$:

1) $\alpha = 0 \implies$ нам подойдёт любой базис.

2) $\alpha \neq 0$

Т.к. $\alpha \neq 0$, то $\exists\, v \in V : \alpha(v, v) \neq 0$

Рассмотрим пространство образованное вектором v — $\langle v \rangle$.

$\alpha\Big|_{\langle v \rangle}$ — невырождена $\implies V = \langle v \rangle \oplus \langle v \rangle^\perp$

Строим ортогональный базис $\langle v \rangle^\perp$ — $e_1, \ldots e_n$.

Тогда нам подойдет базис $v, e_1, e_2, \ldots, e_n$ ($v \perp e_i$ из-за ортогональности подпространств) □

Теорема 1.7 (Ортогонализация Грама-Шмидта)**.**

$e_1, \ldots, e_n$ — базис V, α — билинейная симметричная форма.

$V_0 = \{0\},\ V_k = \langle e_1, \ldots, e_k \rangle$

A — матрица α в базисе $e_1, \dots, e_n$, A_k — матрица $\alpha\Big|_{V_k}$ в базисе $e_1, \dots, e_k$.

$\delta_0 = 1,\ \delta_k = \det A_k$

Тогда, если все $\delta_1, \delta_2, ...\delta_k \neq 0$, то существует единственный ортогональный базис $f_1, \dots f_n$ пространства V, такой что $f_k \in e_k + V_{k-1}$ ($f_k = e_k + u$, где $u \in V_{k-1}$) при всех $k \in [1..n]$.

При этом дополнительно будет верно, что $\alpha(f_k, f_k) = \frac{\delta_k}{\delta_{k-1}}$.

Доказательство.

Рассмотрим индукцию по n.

База при $n = 1$.

$f_1 = e_1$ (можно выбрать единственным образом), при этом $\alpha(f_1, f_1) = \alpha(e_1, e_1) = \det A_1 = \delta_1$

Переход $n \to n + 1$.

В V_n уже построен единственный возможный ортогональный базис $f_1, \dots, f_n$. Найдем последний вектор f_{n+1}.

Хотим получить $f_{n+1} = e_{n+1} + \sum\limits_{i=1}^{n} \lambda_i f_i$ для каких-то λ_i.

Из ортогональности имеем $0 = \alpha(f_{n+1}, f_i) = \alpha(e_{n+1}, f_i) + \lambda_i \alpha(f_i, f_i) \implies \lambda_i = -\frac{\alpha(e_{n+1}, f_i)}{\alpha(f_i, f_i)}$.

А значит, все λ_i строго определены.

Заметим, что $f_{n+1} \notin V_n$, а значит мы действительно получили ортогональный базис.

Проверим, что $\alpha(f_{n+1}, f_{n+1}) = \frac{\delta_{n+1}}{\delta_n}$.

Пусть A_f – матрица формы α в базисе f.

Тогда $A_f = C^T A C$ для какой-то матрицы перехода C. Изучим ее.

Пусть $f_k = e_k + \sum\limits_{i=1}^{k-1} \lambda_{ki} e_i$, тогда

$$C = \begin{pmatrix} 1 & \lambda_{2,1} & \lambda_{3,1} & \cdots & \lambda_{n+1,1} \\ 0 & 1 & \lambda_{3,2} & \cdots & \lambda_{n+1,2} \\ 0 & 0 & 1 & \cdots & \lambda_{n+1,3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \implies \det C = 1$$

Тогда $\det A_f = \det C^T \cdot \det A \cdot \det C = \det A$.

При этом по предположению

$$A_f = \begin{pmatrix} \delta_1 & 0 & \cdots & 0 & 0 \\ 0 & \frac{\delta_2}{\delta_1} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \frac{\delta_n}{\delta_{n-1}} & 0 \\ 0 & 0 & \cdots & 0 & \alpha(f_{n+1}, f_{n+1}) \end{pmatrix}$$

Тогда $\delta_{n+1} = \det A = \det A_f = \delta_1 \cdot \frac{\delta_2}{\delta_1} \cdot \dots \frac{\delta_n}{\delta_{n-1}} \cdot \alpha(f_{n+1}, f_{n+1}) = \delta_n \cdot \alpha(f_{n+1}, f_{n+1})$.

Таким образом, получаем $\alpha(f_{n+1}, f_{n+1}) = \frac{\delta_{n+1}}{\delta_n}$. □

1.4. Квадратичная форма

***Определение* 1.10.**

α — симметричная билинейная форма над K и $\operatorname{Char} K \neq 2$.

Функция $q : V \to K$, такая что $q(x) = \alpha(x, x)$, называется квадратичной формой, ассоциированной с α.

Замечание.

$v \in V$, $\lambda \in K$

$q(\lambda v) = \lambda^2 q(v)$

Замечание.

Любая квадратичная форма имеет вид $q(x_1, \ldots, x_n) = \sum\limits_{i,j} a_{i,j} x_i x_j = x^T A x$

Пример.

Скалярное произведение в $\mathbb{R}^n$.

$q(x_1, \ \ldots, \ x_m) = x_1^2 + \ldots + x_n^2$

Лемма.

1) Если $K = \mathbb{C}$, α — билинейная форма, q — ассоциированная с ней квадратичная форма, то существует базис, в котором форма q принимает следующий вид:

$q(x) = x_1^2 + \ldots + x_r^2$

Причём $r = \operatorname{rank} \alpha$.

2) Если $K = \mathbb{R}$, α — билинейная форма, q — ассоциированная с ней квадратичная форма, то существует базис, в котором форма q принимает следующий вид:

$q(x) = x_1^2 + \ldots + x_k^2 - x_{k+1}^2 - \ldots - x_{k+l}^2$

Причём $k + l = \operatorname{rank} \alpha$.

Доказательство.

Мы уже знаем, что для любой симметричной билинейной формы существует ортогональный базис, матрица в котором диагональна. В частности, эти вектора можно нормировать и получить требуемое. □

***Определение* 1.11.**

Вид $q(x) = \sum x_1^2 + \ldots + x_n^2$ положительно определенной квадратичной называется нормальным.

Пример.

Пусть в $\mathbb{R}^3$ $q(x, y, z) = xy + yz + xz$.

Найдем базис, в котором форма имеет вид $q(x', y', z') = x'^2 + y'^2 + z'^2$.

$$A = \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix}$$

$$\begin{pmatrix} x & y & z \end{pmatrix} A \begin{pmatrix} x \\ y \\ z \end{pmatrix} = q(x, y, z)$$

$$\begin{cases} x = x_1 + y_1 \\ y = x_1 - y_1 \end{cases} \implies q(x_1, y_1, z) = x_1^2 - y_1^2 + 2x_1 z = (x_1 + z)^2 - y_1^2 - z^2$$

Получили, что в базисе $e_1 = \frac{x+y}{2} + z$, $e_2 = \frac{x-y}{2}$, $e_3 = z$ квадратичная форма будет иметь нужный нам вид.

***Определение* 1.12.**

Вещественная квадратичная форма q над полем $\mathbb{R}$ положительно определена, если $\forall x \neq 0 :\ q(x) > 0$, и отрицательно определена, если $\forall x \neq 0 :\ q(x) < 0$

Пример.

1) x^2

2) Скалярное произведение

Теорема 1.8.

Если q — вещественная квадратичная форма, то существует базис, в котором она принимает следующий вид:

$q(x) = x_1^2 + \ldots + x_k^2 - x_{k+1}^2 - \ldots - x_{k+l}^2$

Причём:

k — максимальная размерность подпространства, на котором форма q положительно определена.

l — максимальная размерность подпространства, на котором форма q отрицательно определена.

Доказательство.

Первое уже было доказано.

Пусть $m := \max\{\dim U : U \leqslant V,\ q\Big|_U$ положительно определена$\}$.

Тогда $k \leqslant m$, т.к. в базисе $e_1, ...e_n$ квадратичная форма q имеет вид $q(x) = \sum\limits_{i=1}^{k} x_i^2 - \sum\limits_{i=k+1}^{k+l} x_i^2$.

То есть, на пространстве $\langle e_1, \ldots, e_k\rangle$ наша форма q положительно определена.

Осталось заметить, что для любого подпространства $U \leqslant V$, на котором наша квадратичная форма положительно определена, верно, что $U \cap \langle e_{k+1}, \ldots, e_n\rangle = \{0\}$.

Это так, поскольку $\forall x \in \langle e_{k+1}, \ldots, e_n\rangle : q(x) \leqslant 0$.

А значит, $\forall U : \dim U \leqslant k \implies k = m$.

Для параметра l доказательство аналогично (можно заменить q на $-q$). □

***Определение* 1.13.**

Пара чисел (k, l) называется сигнатурой квадратичной формы.

Следствие (закон инерции).

Сигнатура не зависит от базиса.

Теорема 1.9 (Якоби).

A — матрица формы q.

$\delta_1, \ldots, \delta_n$ — угловые миноры.

Если все $\delta_i \neq 0$, то l равно числу перемен знака в последовательности $1, \delta_1, \ldots, \delta_n$.

Доказательство.

Рассмотрим матрицу нашей квадратичной формы и посчитаем её угловые миноры.

Поскольку все они не равны нулю, то, применив ортогонализацию Грама-Шмидта, мы можем привести матрицу к диагональному виду. При этом все диагональные элементы будут выражаться через значения угловых миноров:

$\alpha(f_i, f_i) = q(f_i) = \frac{\delta_i}{\delta_{i-1}}$

В новом ортогональном базисе сигнатура не изменится. И, в частности, значению l в нём будет соответствовать количество отрицательных чисел.

А это — в точности количество перемен знака в нашей последовательности. □

Следствие (Критерий Сильвестра).

q — положительно определена $\iff \delta_i > 0 \ \ \forall i \in [1..n]$.

1.5. Кривые и поверхности второго порядка

***Определение* 1.14.**

V — векторное пространство над полем K, $\dim V = n$

Тогда рассмотрим следующее уравнение поверхности:

$S(x) = \sum\limits_{i,j} a_{i,j}x_ix_j + 2\sum\limits_{i=1}^{n} b_ix_i + c = x^TAx + 2Bx + c = 0, \ a_{i,j} = a_{j,i}$

Будем также рассматривать следующие её преобразования:

1) Замена базиса $x \mapsto Cx$, где C — невырожденная матрица перехода

2) Параллельный перенос $x \mapsto x + u, \ u \in V$

Лемма.

При помощи преобразований (1) и (2) уравнение поверхности можно привести к виду

$\sum\limits_{i\in I} \alpha_i x_i^2 + \sum\limits_{i\notin I} \beta_i x_i + c = 0$, где $I \subset [1..n]$.

Замечание.

Для доказательства этой леммы нам потребуется ввести следующие обозначения:

Обозначение.

Будем называть x^TAx из уравнения поверхности малой квадратичной формой $\kappa(x)$.

Введём также понятие большой квадратичной формы $\Omega(x,t) = \kappa(x) + 2tBx + ct^2$ над пространством $W = V \oplus K$. Мы даже можем выписать её матрицу:

$$\begin{pmatrix} A & B^T \\ B & c \end{pmatrix}$$

Замечание.

Заметим, что у нас существует естественное вложение $i : V \hookrightarrow V \oplus K$, такое что $x \mapsto (x, 1)$.

В частности, если мы научимся делать замену координат и сдвиг в новом пространстве, то научимся получать его и в исходном.

Факт.

Рассмотрим замену координат и параллельный перенос в новом пространстве W.

Если в V замене координат соответствовала матрица C, то в новом пространстве ей будет соответствовать следующая матрица:

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

Аналогично, сдвигу на вектор u в V можно сопоставить отображение вида $\begin{pmatrix} x & t \end{pmatrix} \to \begin{pmatrix} x + tu & t \end{pmatrix}$.

Отсюда получаем, что этому преобразованию можно сопоставить следующую матрицу:

$$\begin{pmatrix} E & u \\ 0 & 1 \end{pmatrix}$$

Заметим, что обе эти матрицы — обратимы (первая обратима потому, что C — обратима). А значит, они являются матрицами замены координат в новом пространстве.

Нас интересует композиция этих преобразований, в результате которых мы хотим привести нашу матрицу к некоторому "удобному" виду.

Композиция же в общем случае для некоторых произвольных C и u может быть представлена так:

$$\begin{pmatrix} C & u \\ 0 & 1 \end{pmatrix}$$

Лемма.

Ранг и сигнатура малой и большой квадратичных форм не меняется при преобразованиях (1) и (2).

Доказательство.

Для большой квадратичной формы это очевидно, так как эти преобразования представляют собой замену координат, при которой ранг и сигнатура не меняются (уже было доказано).

В случае малой квадратичной формы это также верно. Достаточно заметить, что при параллельном переносе у нас и вовсе не меняется квадратичная форма. А про замену координат, опять же, у нас уже было доказано. □

Лемма.

Ω можно привести к виду $\sum\limits_{i\in I} x_i^2 + \sum\limits_{i\notin I} a_i x_i t + ct^2$, где $I \subset [1..n]$.

Доказательство.

Рассмотрим интересующую нас матрицу перехода $D := \begin{pmatrix} C & u \\ 0 & 1 \end{pmatrix}$

Тогда $D^T \begin{pmatrix} A & B^T \\ B & c \end{pmatrix} D = \begin{pmatrix} C^TAC & C^TAu + C^TB^T \\ u^TAC + BC & u^TAu + Bu + c \end{pmatrix}$

В общем случае, надо подобрать такую C, чтобы C^TAC была диагональна.

Тогда мы получим, что квадратичная форма имеет вид $\sum\limits_{i=1}^{n} a_i x_i^2 + \sum\limits_{i=1}^{n} b_i x_i + c = 0 \implies$ можем выделить полные квадраты, тем самым подобрав нужный вектор u. □

Замечание.

На самом деле, если матрица малой квадратичной формы обратима, то форму приведется к виду $\sum\limits_{i=1}^{n} a_i x_i^2 + c = 0$.

1.6. Антисимметричные билинейные формы

***Определение* 1.15.**

Билинейная форма над полем K, таким что $\operatorname{Char} K \neq 2$, называется антисимметричной (кососимметрической) если $\alpha(x, y) = -\alpha(y, x)$.

Замечание. $\alpha(x, x) = 0$

***Определение* 1.16.**

Базис $e_1, ..., e_n$ называется симплектическим, если для некоторого $m < \lfloor \frac{n}{2} \rfloor$ выполняется $\alpha(e_{2k-1}, e_{2k}) = 1 \ \ \forall k \in [1..m]$ и $\alpha(e_i, e_j) = 0$ для всех остальных пар.

Замечание.

Матрица антисимметричной формы в симплектическом базисе имеет вид:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ -1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & -1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

Теорема 1.10.

Для любой антисимметричной билинейной формы существует симплектический базис.

Доказательство.

Индукция по n — размерности пространства.

База для $n = 1$, тогда подойдет любой базис.

Переход.

1) Если форма α тождественно равна 0, то можем выбрать любой базис.

2) Пусть существуют $e_1, e_2 : \alpha(e_1, e_2) = c \neq 0$.

Тогда мы можем заменить e_1 на $\frac{e_1}{c}$, и получить пару векторов, такую что $\alpha(e_1, e_2) = 1$.

Тогда пространство $V = \langle e_1, e_2 \rangle \oplus \langle e_1, e_2 \rangle^{\perp}$.

Во втором подпространстве по предположению существуют симплектический базис $e_3, ...e_n$, тогда $e_1, \ldots, e_n$ — симплектический. □

Замечание.

Ранг антисимметричной билинейной формы четен.

2. Евклидовы и эрмитовы пространства

2.1. Введение

***Определение* 2.1.**
Конечномерное векторное пространство V над $\mathbb{R}$ с симметричной билинейной формой α называется евклидовым, если ассоциированная с ней квадратичная форма положительно определена.

Форму α в таком случае будем называть скалярным произведением и обозначать $\langle x, y\rangle$.

***Определение* 2.2.**
V — векторное пространство над $\mathbb{C}$.

Полуторалинейная форма α называется эрмитовой, если $\alpha(x,y) = \overline{\alpha(y,x)}$

Свойства.

1. α — эрмитова $\iff \overline{A}^T = A$ (A — матрица α, $\overline{A}$ — матрица из сопряжённых элементов.)
2. $\alpha(x,x) \in \mathbb{R}$.

Доказательство.

1. $\overline{\alpha(e_i,e_j)} = \alpha(e_j,e_i)$
2. $\alpha(x,x) = \overline{\alpha(x,x)} \implies \alpha(x,x) \in \mathbb{R}$

□

***Определение* 2.3.**
Конечномерное векторное пространство V над $\mathbb{C}$ с эрмитовой формой α называется эрмитовым, если для любого ненулевого вектора $\alpha(x,x) > 0$.

Форма же α называется эрмитовым скалярным произведением.

***Определение* 2.4.**
$f : U \to V$ называется гомоморфизмом евклидовых (эрмитовых) пространств, если f — гомоморфизм векторных пространств, такой что $\langle f(x),\, f(y)\rangle = \langle x,\, y\rangle \;\; \forall\, x,\, y \in U$.

Т.е., если f сохраняет скалярное произведение.

Пример.
1) $\mathbb{R}^2$ со стандартным скалярным произведением.

2) $C([a,b])$ со скалярным произведением $\int\limits_a^b f(x)g(x)\,dx$.

***Определение* 2.5.**
$\langle\cdot,\cdot\rangle$ — скалярное произведение (евклидово, эрмитово), $v_1,\, \ldots,\, v_k \in V$.

$G(v_1,\, \ldots,\, v_k) = \begin{pmatrix} \langle v_1,v_1\rangle & \cdots & \langle v_1,v_k\rangle \\ \vdots & \ddots & \vdots \\ \langle v_k,v_1\rangle & \cdots & \langle v_k,v_k\rangle \end{pmatrix}$ — матрица Грама системы векторов $v_1,\, \ldots,\, v_k$

Замечание.

Если вектора $v_1, \ldots, v_n$ образуют базис, то матрица Грама совпадает с матрицей билинейной формы скалярного произведения в базисе $v_1, \ldots, v_n$.

2.2. Евклидовы пространства

Лемма.

V — евклидово пространство.

$v_1, \ldots, v_k \in V$

Тогда $\det G(v_1, \ldots, v_k) \geqslant 0$, причём равенство достигается тогда и только тогда, когда $v_1, \ldots, v_k$ — линейно зависимы.

Доказательство.

1) $v_1, \ldots, v_k$ — линейно независимы, а значит являются базисом пространства $\langle v_1, \ldots, v_k \rangle$.

Тогда G является матрицей квадратичной формой, которая в этом базисе положительно определена (т.к. скалярное произведение).

Следовательно, по критерию Сильвестра $\det G > 0$.

2) $v_1, \ldots, v_k$ — линейно зависимы $\implies \exists \lambda_j : \sum\limits_{j=1}^{k} \lambda_j v_j = 0$

Докажем, что столбцы матрицы Грама, домноженные на λ_j дают в сумме 0.

Рассмотрим строку i.

$\sum\limits_{j=1}^{k} \lambda_j \langle v_i, v_j \rangle = \langle v_i, \sum\limits_{j=1}^{k} \lambda_j v_j \rangle = \langle v_i, 0 \rangle = 0.$

А значит, столбцы линейно зависимы, а тогда определитель 0. □

***Определение* 2.6.**

Длина вектора $\|v\| = \sqrt{\langle v, v \rangle}$.

Лемма (Неравенство Коши-Буняковского-Шварца).

$\langle x, y \rangle^2 \leqslant \|x\|^2 \cdot \|y\|^2$

Доказательство.

$$G(x, y) = \begin{pmatrix} \langle x, x \rangle & \langle x, y \rangle) \\ \langle y, x \rangle & \langle y, y \rangle \end{pmatrix}$$

Мы знаем, что $\det G \geqslant 0$, а значит $\langle x, x \rangle \cdot \langle y, y \rangle \geqslant \langle x, y \rangle \cdot \langle y, x \rangle \Rightarrow \|x\|^2 \cdot \|y\|^2 \geqslant \langle x, y \rangle^2$

□

Теорема 2.1.

Длина является нормой.

Доказательство.

1. $\sqrt{\langle v, v \rangle} \geqslant 0 \ \ \forall v$, при этом по определению скалярного произведения $\langle v, v \rangle > 0 \ \ \forall v \neq 0$.
2. $\|\lambda v\| = |\lambda| \cdot \|v\|$

3. $\|x+y\| \leqslant \|x\| + \|y\|$

Возводим в квадрат.

$\langle x+y, x+y\rangle \leqslant \|x\|^2 + \|y\|^2 + 2\|x\| \cdot \|y\|$

$\|x\|^2 + \|y\|^2 + 2\langle x, y\rangle \leqslant \|x\|^2 + \|y\|^2 + 2\|x\| \cdot \|y\|$

$\langle x, y\rangle \leqslant \|x\| \cdot \|y\|$

А это неравенство Коши-Буняковского-Шварца.

□

Следствие.

1) $\rho(x, y) = \|x - y\|$

2) $-1 \leqslant \frac{\langle x, y\rangle}{\|x\|\|y\|} \leqslant 1 \ \ \forall\, x,\, y \in V \setminus \{0\}$

Тогда можем определить угол:

$\cos\varphi = \frac{\langle x, y\rangle}{\|x\|\|y\|} \implies 0 \leqslant \varphi \leqslant \pi$

***Определение* 2.7.**

Базис $e_1, \ldots, e_n$ называется ортогональным, если $\langle e_i,\, e_j\rangle = 0$ для всех $i \neq j$

Утверждение 2.2.

Ненулевые, попарно ортогональные вектора линейно независимы.

Доказательство.

От противного. Пусть $\alpha_1 e_1 + \ldots + \alpha_k e_k = 0$

При этом $\forall i:\ 0 = \langle 0, e_i\rangle = \langle \alpha_1 e_1 + \ldots + \alpha_k e_k,\, e_i\rangle = \sum\limits_{j=0}^{k} \alpha_j \langle e_j, e_i\rangle = \alpha_i \langle e_i, e_i\rangle$

$\alpha_i \langle e_i,\, e_i\rangle = 0,\ \langle e_i,\, e_i\rangle > 0 \implies \alpha_i = 0$ □

Алгоритм (ортогонализации).

Рассмотрим набор векторов $e_1, \ldots, e_n \in V,\ e_1 \neq 0$.

Построим $f_1, \ldots, f_n$ по таким правилам:

1) $f_1 = e_1$.

2) $f_{k+1} = e_{k+1} - \sum\limits_{i=1}^{k} \frac{\langle e_{k+1}, f_i\rangle}{\langle f_i, f_i\rangle} f_i$

Теорема 2.3.

$e_1, \ldots, e_n$ — набор векторов, $f_1, \ldots, f_n$ — построенный по ним набор.

$i,\, j,\, k \in \{1, \ldots, n\},\ \ i \neq j$

Тогда:

1) $\langle f_i,\, f_j\rangle = 0$

2) $\langle e_1, \ldots, e_n\rangle = \langle f_1, \ldots, f_n\rangle$

3) Если $e_1, \ldots, e_n$ — линейно независимы, то $f_1, \ldots, f_n$ — линейно независимы. В частности, $f_i \neq 0$.

4) Если $e_k \in \langle e_1, \ldots, e_{k-1}\rangle$, то $f_k = 0$

5) Если $e_1, \ldots, e_n$ — система образующих, то ненулевые $f_1, \ldots, f_n$ образуют базис.

6) Если $e_1, \ldots, e_n$ — базис V, то $f_1, \ldots, f_n$ — ортогональный базис.

Доказательство.

Модифицируем алгоритм ортогонализации Грама-Шмидта. А именно, при построении очередного f_i будем рассматривать только такие f_j для $j < i$, что $f_j \neq 0$. И покажем, что f_i будет ортогонален всем предыдущим.

Доказательство этого, аналогично доказательству корректности ортогонализации Грама-Шмидта, будет осуществляться по индукции.

Пусть мы на очередном шаге имеем $f_i = e_i - \sum\limits_{j<i} \frac{\langle e_i, f_j\rangle}{\langle f_j, f_j\rangle} f_j$, причём векторы $f_1, \ldots, f_{i-1}$ — ортогональны.

Тогда получаем, что $\langle f_i, f_j\rangle = \langle e_i, f_j\rangle - \frac{\langle e_i, f_j\rangle}{\langle f_j, f_j\rangle} \cdot \langle f_j, f_j\rangle = 0$.

А значит, очередной f_i или равен нулю (если $e_i \in \langle e_1, \ldots, e_{i-1}\rangle$), или отличен от нуля и, соответственно, ортогонален всем предыдущим векторам (если $e_i \in \langle e_1, \ldots, e_{i-1}\rangle^\perp$).

Отсюда очевидным образом следуют все 6 пунктов данной теоремы. □

2.3. Ортогональные матрицы

***Определение* 2.8.**

Заметим, что в евклидовом пространстве очень просто перейти от ортогонального базиса к ортонормированному.

Пусть $e_1, \ldots, e_n$ — ортонормированный базис.

Тогда $f_1, \ldots, f_n$ является ортонормированным базисом тогда и только тогда, когда $C^T E C = C^T C = E$.

Матрицы C, обладающие таким свойством, называются ортогональными.

Замечание.

Если C — ортогональная, то $\det C = \pm 1$.

Доказательство.

$\det E = \det\left(C^T C\right) = \det^2 C \iff \det C = \pm 1$ □

2.4. Ортогональная проекция

Утверждение 2.4.

Пусть $U \leqslant V$. Тогда $\langle \cdot, \cdot \rangle\Big|_U$ — положительно определена.

В частности, $V = U \oplus U^\perp$.

Доказательство.

Очевидно, т.к. любые мы просто рассмотрели сужение на подпространство. Положительность от этого не теряется.

Тогда, в частности, $U \cap U^\perp = \{0\}$, а значит, $V = U \oplus U^\perp$ □

***Определение* 2.9.**

$V = U \oplus U^\perp$, $v \in V$.

$v = u_1 + u_2$, т.ч. $u_1 \in U$, $u_2 \in U^\perp$.

Вектор u_1 называется ортогональной проекцией v на U.

Обозначение.

$\mathrm{pr}_U v := u_1$

$\mathrm{ort}_U v := u_2$

Замечание.

Пусть $e_1, \dots, e_k$ — ортонормированный базис U.

Тогда $\mathrm{pr}_U x = \sum\limits_{i=1}^{k} \langle x, e_i \rangle e_i$

***Определение* 2.10.**

Пусть X и Y — подмножества метрического пространства V.

Расстоянием между множествами X и Y называется $\rho(X, Y) := \inf\limits_{x \in X,\, y \in Y} \rho(x, y)$.

Утверждение 2.5.

Если $U \leqslant V$, то $\rho(x, U) = \|\mathrm{ort}_U x\|$

Доказательство.

Пусть $x = u_1 + u_2$, $\mathrm{pr}_U x = u_1$, $\mathrm{ort}_U x = u_2$

$\forall u \in U : \|x - u\| = \|u_2 + (u_1 - u)\| = \sqrt{\|u_2\|^2 + \|u_1 - u\|^2} \geqslant \|u_2\|$

А так как $\rho(x, U) = \inf\limits_{u \in U} \|x - u\|$, то $\rho(x, U) \geqslant \|\mathrm{ort}_U x\|$.

При этом, при $u = u_1$ достигается равенство, значит $\rho(x, U) = \|\mathrm{ort}_U x\|$. □

Следствие.

Пусть $e_1, \dots, e_k$ — ортонормированный базис U.

Тогда $\rho(v, U)^2 = \frac{\det G(e_1, \dots, e_k, v)}{\det G(e_1, \dots, e_k)}$

Доказательство.

1) Если $v \in U$, т.е. $(\mathrm{ort}_U v = 0)$, то $e_1, \dots, e_k, v$ — линейно зависимы.

А значит, $\det G(e_1, \dots, e_k, v) = 0$, что и требовалось.

2) Если $v \notin U$, то все наши вектора линейно независимы и образуют базис $W = \langle e_1, \dots, e_k, v \rangle$.

В частности, мы можем воспользоваться ортогонализацией Грама-Шмидта (а также её полезным свойством, связанным с угловыми минорами матрицы квадратичной формы).

Тогда получим, что $\rho(v, U)^2 = \|\mathrm{ort}_U v\|^2 = \langle \mathrm{ort}_U v, \mathrm{ort}_U v \rangle = \frac{\det G(e_1, \dots, e_k, v)}{\det G(e_1, \dots, e_k)}$. □

***Определение* 2.11.**

Пусть V — евклидово пространство, $\dim V = n$, $a_1, \dots, a_n \in V$.

$P(a_1, \dots, a_n) = \{\sum\limits_{i=1}^{n} x_i a_i \mid x \in [0, 1]\}$ назовем параллелепипедом, натянутым на вектора $a_1, \dots, a_n$.

***Определение* 2.12.**

Высотой параллелепипеда $P(a_1, \dots, a_n)$ назовем $\mathrm{ort}_{\langle a_1, \dots, a_{n-1} \rangle} a_n$ (зависит от порядка a_n).

***Определение* 2.13.**

Определим объём параллелепипеда индуктивно, как произведение высоты на основание (где основание — $(n-1)$-мерный параллелепипед):

$\mathrm{Vol}\, P(a) = \|a\|$

$\mathrm{Vol}\, P(a_1, \dots, a_n) = \left\|\mathrm{ort}_{\langle a_1, \dots, a_{n-1} \rangle} a_n\right\| \cdot \mathrm{Vol}\, P(a_1, \dots, a_{n-1})$.

Утверждение 2.6.

1) $\operatorname{Vol} P(a_1, \ldots, a_n) = \sqrt{\det G(a_1, \ldots, a_n)}$

2) $e_1, \ldots, e_n$ — ортонормированный базис V.

Тогда если $(a_1, \ldots, a_n) = (e_1, \ldots, e_n)A$, то $\operatorname{Vol} P(a_1, \ldots, a_n) = |\det A|$.

Доказательство.

1) Индукция по n.

$n = 1 \implies \operatorname{Vol} P(a) = \|a\| = \sqrt{\langle a, a\rangle} = \sqrt{\det G(a)}$

Переход: $n \to n + 1$:

$(\operatorname{Vol} P(a_1, \ldots, a_{n+1}))^2 = \left\|\operatorname{ort}_{\langle a_1, \ldots, a_n\rangle} a_{n+1}\right\|^2 \cdot \det G(a_1, \ldots, a_n)$

Если $\det G(a_1, \ldots, a_n) = 0$, то $\det G(a_1, \ldots a_{n+1}) = 0$, что и требовалось.

Если же $\det G(a_1, \ldots, a_n) > 0$, то мы снова можем воспользоваться ортогонализацией Грама-Шмидта:

$\left\|\operatorname{ort}_{\langle a_1, \ldots, a_n\rangle} a_{n+1}\right\|^2 \cdot \det G(a_1, \ldots, a_n) = \frac{\det G(a_1, \ldots, a_n, a_{n+1})}{\det G(a_1, \ldots, a_n)} \cdot \det G(a_1, \ldots, a_n) = \det G(a_1, \ldots, a_n, a_{n+1})$

2) $G(a_1, \ldots, a_n) = A^T E A = A^T A$

$\det G(a_1, \ldots, a_n) = (\det A)^2 \implies \operatorname{Vol} P(a_1, \ldots, a_n) = |\det A|$. □

Теорема 2.7.

Евклидово пространство размерности n изоморфно $\mathbb{R}^n$.

Доказательство.

Пусть V – евклидово пространство, $\dim V = n$.

Выберем в нём ортонормированный базис $e_1, \ldots, e_n$ и построим изоморфизм из V в $\mathbb{R}^n$:

$f : V \to \mathbb{R}^n$, $e_i \to (0, \ldots, 1, \ldots, 0)$, единица на i-том месте. □

2.5. Эрмитовы пространства (Унитарные)

Замечание.

V — конечномерное векторное пространство над $\mathbb{C}$

$\langle \cdot, \cdot \rangle$ — положительно определённая полуторалинейная эрмитова форма, т.е. $\langle x, y\rangle = \overline{\langle y, x\rangle}$.

Замечание.

Многие утверждения, разобранные нами выше для евклидовых пространств, верны также и для эрмитовых:

1) Полуторалинейная форма в координатах: $\alpha(x, y) = \sum a_{ij}\overline{x_i}y_j = \overline{x}^T A y$

2) При переходе в новый базис eC матрица формы преобразуется по формуле $\overline{C}^T A C$

3) Полуторалинейная форма эрмитова $\iff \overline{A}^T = A$.

4) Эрмитова квадратичная форма $q(x)$ вещественная и $q(x) = \langle x, x\rangle$

5) Поляризация: $\langle u, v\rangle = \frac{q(x+y)+q(ix+y)}{2} - q(x) - q(y)$

6) Для любой полуторалинейной эрмитовой формы существует ортогональный базис.

7) Зададим норму $\|v\| := \sqrt{\langle v, v\rangle}$. ($\langle v, v\rangle \geqslant 0$, а неравенство треугольника следует из неравенства Коши-Буняковского-Шварца).

8) V — эрмитово пространство, $\dim V = n$

Тогда $V \cong \mathbb{C}^n$ и $\langle x, y\rangle = \sum\limits_{i=1}^{n} \overline{x_i} y_i$.

Лемма.

$v_1, \ldots, v_m \in V$

Тогда $\det G(v_1, \ldots, v_m) \in \mathbb{R}$ и неотрицателен.

При этом $\det G = 0 \iff v_1, \ldots, v_m$ — линейно зависимы.

Доказательство.

Пусть $e_1, \ldots, e_n$ — ортонормированный базис V.

Положим $(v_1, \ldots, v_m) = (e_1, \ldots, e_n)C$ для некоторой матрицы C.

Тогда $G(v_1, \ldots, v_m) = \overline{C}^T E C = \overline{C}^T C$.

$\det G_v = \det\left(\overline{C}^T C\right) = \det \overline{C} \det C = \overline{\det C} \det C = |\det C|^2$

Если $n < m$, то $\operatorname{rank} G(v_1, \ldots, v_m) = n < m \implies \det G(v_1, \ldots, v_m) = 0$.

Если же $n = m$, то $\operatorname{rank} C = m \implies \det C \neq 0 \implies \det G_v > 0$. □

Следствие.

Неравенство Коши-Буняковского: $|\langle x, y\rangle|^2 = \langle x, y\rangle \cdot \overline{\langle x, y\rangle} \leqslant \|x\|^2 \cdot \|y\|^2$.

Замечание.

Аналогично получаем, что можно определить угол: $0 \leqslant \frac{|\langle x,y\rangle|}{||x||||y||} \leqslant 1$

***Определение* 2.14.**

Матрицы перехода между ортонормированными базисами эрмитова пространства называются унитарными.

C — унитарна $\iff \overline{C}^T C = E$

2.6. Овеществление и комплексификация

***Определение* 2.15.**

V — векторное пространство над $\mathbb{C}$, $\dim_{\mathbb{C}} V = n$

$V_{\mathbb{R}}$ — пространство V над $\mathbb{R}$

$V_{\mathbb{R}}$ — овеществление V.

Утверждение 2.8.

$\dim V_{\mathbb{R}} = 2 \dim V$

Доказательство.

Пусть $v_1, \ldots, v_n$ — базис V над $\mathbb{C}$.

Докажем, что $v_1, \ldots, v_n, iv_1, \ldots, iv_n$ — базис $V_{\mathbb{R}}$ над $\mathbb{R}$.

Они линейно независимы, т.к. если $\lambda_1 v_1 + \ldots + \lambda_n v_n + \mu_1 i v_1 + \ldots + \mu_n i v_n = 0$, то отдельно комплексная и мнимая части равны 0, а значит, т.к. $v_1, \ldots v_n$ — базис над $\mathbb{C}$, то все $\lambda_i,\ \mu_i = 0$.

Покажем, что система образующих.

$\forall\, v \in V : v = \sum\limits_{j=1}^{n} z_j v_j = \sum\limits_{j=1}^{n} (a_j + i b_j) v_j = \sum\limits_{j=1}^{n} a_j v_j + \sum\limits_{j=1}^{n} b_j i v_j$

Значит базис, значит $\dim V_{\mathbb{R}} = 2 \dim V$. □

Лемма.

U, V — пространства над $\mathbb{C}$

$e_1, \ldots, e_n$ — базис U, $f_1, \ldots, f_m$ — базис V, $a \in \mathrm{Hom}(U, V)$

$A = B + iC$, где $B, C \in \mathbb{R}^{m \times n}$

Тогда матрица $a_{\mathbb{R}}$ в базисе $e_1, \ldots, e_n, ie_1, \ldots, ie_n$ для $U_{\mathbb{R}}$ и в базисе $f_1, \ldots, f_m, if_1, \ldots, if_m$ для $V_{\mathbb{R}}$ имеет вид:

$$\begin{pmatrix} B & -C \\ C & B \end{pmatrix}$$

Доказательство.

Рассмотрим вектор $v \in U_{\mathbb{R}}$. $v = \sum \alpha_j e_j + \alpha'_j i e_j$.

Пусть $a(v) = \sum \beta_j f_j + \beta'_j i f_j$

Считаем матрицу $a(v) = a(\sum \alpha_j e_j) + ia(\sum \alpha'_j e_j) = (B + iC)(\sum \alpha_j e_j) + i(B + iC)(\sum \alpha'_j e_j)$.

Т.е. $B(\sum \alpha_j e_j) - C(\sum \alpha'_j e_j) = \sum \beta_j f_j$ и $iC(\sum \alpha_j e_j) + iB(\sum \alpha'_j e_j) = \sum \beta'_j i f_j$

Осталось заметить, что матрица из условия действует на v точно так же. □

Замечание.

U, V — эрмитовы пространства над $\mathbb{C}$, $a \in \mathrm{Hom}(U, V) \rightsquigarrow a_{\mathbb{R}} \in \mathrm{Hom}(U_{\mathbb{R}}, V_{\mathbb{R}})$

***Определение* 2.16.**

Пусть V — конечномерное векторное пространство над полем $\mathbb{R}$.

Введем над пространством $V \oplus V$ умножение на комплексный аргумент по следующему правилу: $(\alpha + \beta i)(u, v) = (\alpha u - \beta v, \alpha v + \beta u)$.

Полученное пространство обозначается $V^{\mathbb{C}}$ и называется комплексификацией пространства V.

Вектора из пространства $V^{\mathbb{C}}$ будем обозначать как $(u, v) = u + iv$.

Свойства.

1) $v \mapsto (v, 0)$ — вложение $V \hookrightarrow V^{\mathbb{C}}$.

2) Если a — гомоморфизм пространств V и U, то $a^{\mathbb{C}}(v_1 + iv_2) := a(v_1) + ia(v_2)$ — гомоморфизм пространств $U^{\mathbb{C}}$ и $V^{\mathbb{C}}$

Доказательство.

1) Обозначим вложение f.

$\alpha f(v) + f(u) = \alpha(v, 0) + (u, 0) = (\alpha v + u, 0) = f(\alpha v + u)$.

2) $a^{\mathbb{C}}(\alpha(v_1 + iv_2) + (v'_1 + iv'_2)) = a^{\mathbb{C}}((\alpha v_1 + v'_1) + i(\alpha v_2 + v'_2)) = a(\alpha v_1 + v'_1) + ia(\alpha v_2 + v'_2) = \alpha(a(v_1) + ia(v_2)) + (a(v'_1) + ia(v'_2)) = \alpha a^{\mathbb{C}}(v_1 + iv_2) + a^{\mathbb{C}}(v'_1 + v'_2)$ □

Замечание.

1) $\dim V^{\mathbb{C}} = \dim V$

2) Матрица $a^{\mathbb{C}}$ из базиса $U^{\mathbb{C}}$ в базис $V^{\mathbb{C}}$ совпадает с матрицей a из базиса U в базис V.

Доказательство.

1) Вспомним, что у нас существует естественное вложение $v \mapsto (v, 0)$.

Тогда покажем, что если $e_1, \ldots, e_n$ — базис V, то $(e_1, 0), \ldots, (e_n, 0)$ — базис $V^{\mathbb{C}}$.

Линейная независимость:

$$\sum_{j=1}^{n}(a_j + ib_j)(e_j, 0) = (0,0) \implies \left(\sum_{j=1}^{n} a_j e_j, \sum_{j=1}^{n} b_j e_j\right) = (0,0) \implies a_j, b_j = 0$$

Система образующих:

$$(v,u) = \left(\sum_{j=1}^{n} a_j e_j, \sum_{j=1}^{n} b_j e_j\right) = \sum_{j=1}^{n} a_j(e_j, 0) + \sum_{j=1}^{n} ib_j(e_j, 0)$$

2) В силу первого замечания. □

3. Операторы в евклидовых и эрмитовых пространствах

3.1. Унитарные и ортогональные операторы

На протяжении всего параграфа V – евклидово или эрмитово пространство.

***Определение* 3.1.**

Множество автоморфизмов V: $\{a \in \mathrm{Aut}(V) \mid \langle a(u), a(v)\rangle = \langle u, v\rangle \ \forall u, v \in V\}$ называется группой изометрий V.

Замечание.

Любая изометрия переводит базис в базис, т.к. является автоморфизмом.

Утверждение 3.1.

Если V — евклидово или эрмитово пространство, то следующие условия эквивалентны:

1. a — изометрия
2. $\forall v \in V$: $\|a(v)\| = \|v\|$
3. Для всякого базиса $e_1, \ldots, e_n$ пространства V выполняется $\overline{A}^T G A = G$, где A — матрица автоморфизма a в базисе e, G — матрица Грама.
4. a переводит некоторый ортонормированный базис в ортонормированный.

Доказательство.

$1 \Rightarrow 2$ $\|v\|^2 = \langle v, v\rangle$

$2 \Rightarrow 1$ Евклидово:

$\langle u, v\rangle = \frac{1}{2}(\|u+v\|^2 - \|u\|^2 - \|v\|^2) = \frac{1}{2}(\|a(u+v)\|^2 - \|a(u)\|^2 - \|a(v)\|^2) = \langle a(u), a(v)\rangle$

Эрмитово:

$\langle u, v\rangle = \mathrm{Re}\langle u, v\rangle + i\,\mathrm{Re}\langle iu, v\rangle$

$\mathrm{Re}\langle u, v\rangle = \frac{1}{2}(\|u+v\|^2 - \|u\|^2 - \|v\|^2)$

$1 \Rightarrow 3$ $\langle u, v\rangle = \langle a(u), a(v)\rangle$.

Тогда, т.к. в матрице Грама записаны скалярные произведения, то матрицы Грама в базисах $e_1, \ldots, e_n$ и $a(e_1), \ \ldots, \ a(e_n)$ совпадают.

А значит получаем, что $\overline{A}^T G A = G$.

Пояснение: такое домножение является заменой базиса матрицы Грама, а, как мы поняли, в базисах $e_1, \ldots e_n$ и $a(e_1), \ldots a(e_n)$ они совпадают)

$3 \Rightarrow 4$ Базис ортонормирован тогда и только тогда, когда матрица Грама в нем единичная.

Мы знаем, что матрица Грама не поменялась, а значит и базис остался ортонормированным.

$4 \Rightarrow 1$ Пусть наш базис это $e_1, \ldots, e_n$.

Очевидно, что на базисных векторах скалярное произведение сохранилось (т.к. базисы ортонормированные), а тогда оно сохранилось и для любой пары по линейности скалярного произведения и оператора a.

□

Замечание.

Мы заодно доказали, что любой ортонормированный базис переходит в ортонормированный.

***Определение* 3.2.**

Пусть $a \in \mathrm{Aut}(V)$, $\|a(v)\| = \|v\| \ \ \forall v \in V$. Тогда:

1) Если V эрмитово, то оператор a называется унитарным.

2) Если V евклидово, то оператор a называется ортогональным.

Замечание.

Исходя из предыдущего утверждения мы просто переопределили понятия изометрии для эрмитовых и евклидовых пространств.

Утверждение 3.2.

V — конечномерное векторное пространство над $\mathbb{R}$, $\dim V > 1$, $a \in \mathrm{End}(V)$

Тогда в V существует одномерное или двумерное подпространство U инвариантное относительно a.

Доказательство.

Рассмотрим характеристический многочлен χ_a.

1. Если χ_a имеет вещественный корень λ, т.е. $\chi_a(\lambda) = 0$.

   Тогда рассмотрим $U = \langle v \rangle$, где v — собственный вектора для λ. U будет одномерным и инвариантным.

2. Если же χ_a не имеет вещественных корней то рассмотрим комплексификацию $a^{\mathbb{C}} \in \mathrm{End}(V^{\mathbb{C}})$ Тогда

   $\chi_a = \chi_{a^{\mathbb{C}}} \in \mathbb{R}[x]$. Рассмотрим корень $z = \alpha + i\beta$ и соответствующий z собственный вектор $u + iv$.

   Тогда $a(u) + ia(v) = a^{\mathbb{C}}(u + iv) = (\alpha + i\beta)(u + iv) = \alpha u - \beta v + i(\beta u + \alpha v)$

   Из полученного равенства следуют равенства вещественной и мнимой части. Т.е.

   $$\begin{cases} a(u) = \alpha u - \beta v \\ a(v) = \beta u + \alpha v \end{cases}$$

   Тогда $U = \langle u, v \rangle$ — двумерное инвариантное подпространство V.

□

Обозначение. $O(V)$ - группа ортогональных операторов.

Утверждение 3.3.

Если V — одномерное пространство над $\mathbb{R}$, то группа ортогональных операторов состоит их двух элементов: $id, -id$.

Доказательство.

$V = \langle v \rangle$;

$a(v) = \lambda v$

$\|\lambda v\| = \|a(v)\| = \|v\| \implies |\lambda| = 1$

А это значит, что $a = \pm id$. □

Утверждение 3.4.

Если V — двумерное пространство над $\mathbb{R}$, то любой ортогональный оператор имеет вид

$$A = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

Доказательство.

Рассмотрим ортонормированный базис.

Тогда т.к. $A^T A = E$, то $\det A = \pm 1$.

Рассмотрим подгруппу $SO(2) \leqslant O(2)$ образованную матрицами, у которых определитель равен 1.

$[O(2) : SO(2)] = 2$, т.к. существует два класса, а именно те матрицы, у которых определитель равен 1 и те, у которых определитель -1.

Пусть $A \in SO(2) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Тогда у нас есть два условия:

$$\begin{cases} AA^T = E \\ \det A = 1 \end{cases} \iff \begin{cases} a^2 + b^2 = 1 \\ c^2 + d^2 = 1 \\ ac + bd = 0 \\ ad - bc = 1 \end{cases} \implies A = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

Подробнее про последний переход. Т.к. $a^2 + b^2 = 1$, то можно считать, что $a = \sin\varphi$; $b = \cos\varphi$. Аналогично для c и d.

Полученная матрица является матрицей поворота на угол φ, а значит группа $SO(2)$ это группа поворотов.

Осталось рассмотреть второй класс смежности группы $O(2)$.

$B \in O(2)$

Тогда, если поменять местами строки B, то получится матрица $A \in SO(2)$, т.е. $B = A \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, где $A \in OS(2)$.

Такие матрицы сводятся к матрицам из $SO(2)$ заменой порядка базисных векторов. □

Теорема 3.5.

1. V - эрмитово, $a \in \mathrm{End}(V)$. Тогда следующие условия равносильны:

   1) a — унитарный.
   2) $\mathrm{Spec}(a) \subset \{z \in \mathbb{C} \ : \ |z| = 1\}$, и существует ортонормированный базис в котором матрица a диагональна.

2. V — евклидово, $a \in \mathrm{End}(V)$. Тогда следующие условия равносильны:

1) a — ортогональный.

2) существует ортонормированный базис в котором матрица a имеет вид

$$\begin{pmatrix} A(\varphi_1) & 0 & \cdots & 0 \\ 0 & A(\varphi_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A(\varphi_n) \end{pmatrix}$$

(A — матрицы из рассуждений выше)

3. Собственные векторы оператора a, соответствующие различным собственным числам, ортогональны.

Доказательство.

1. "1 $\Longleftarrow$ 2"

   Существует базис в котором матрица имеет вид

   $$A = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix}$$

   При этом, т.к. все $\lambda_i \in \mathrm{Spec}(a)$, то $|\lambda_i| = 1$. Тогда $A^T A = E$, что и требовалось.

   "1 $\Longrightarrow$ 2"

   Т.к. a — унитарный, то $a \in \mathrm{Aut}(V)$.

   Пусть v — собственный вектор для числа λ. Тогда $\|v\| = \|a(v)\| = |\lambda|\|v\| \implies |\lambda| = 1$.

   Теперь индукция по размерности V. Если $\dim V = 1$, то матрица оператора уже диагональна.

   Теперь пусть $\dim V > 1$, а λ — собственное число.

   Тогда $V = \langle v \rangle \oplus \langle v \rangle^\perp$.

   Осталось доказать, что $\langle v \rangle^\perp$ инвариантен относительно a.

   $\forall u \in \langle v \rangle : \langle a(v), u \rangle = \langle a(v), a(\frac{1}{\lambda}u) \rangle = \langle v, \frac{1}{\lambda}u \rangle = \frac{1}{\lambda}\langle v, u \rangle = 0$

2. "1 $\Longleftarrow$ 2"

   В каком-то базисе матрица имеет вид:

   $$\begin{pmatrix} A(\varphi_1) & 0 & \cdots & 0 \\ 0 & A(\varphi_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A(\varphi_n) \end{pmatrix}$$

   Тогда в нем $A^T A = E$, т.к. для каждой клеточки так.

   "1 $\Longrightarrow$ 2"

   Сразу заметим, что раз a — ортогональный, то $a \in \mathrm{Aut}(V)$.

   Доказываем индукцией по n.

   Базу для $n = 1, 2$ мы уже проверили, когда изучали группу ортонормированных операторов.

Сделаем переход. Мы доказали, что у любого пространства есть инвариантное подпространство размерности 2 или 1. Найдем его и назовем U.

Тогда $V = U \oplus U^{\perp}$.

Чтобы воспользоваться предположением нужно показать, что $U^{\perp}$ инвариантно относительно нашего оператора.

Если $\dim U = 1$, то $U = \langle v \rangle$, а такой случай мы уже проверяли в первом пункте теоремы.

Если же $\dim U = 2$, то рассмотрим $v \in U^{\perp}$ и $u \in U$.

$\langle a(v), u \rangle = \langle a(v), a(a^{-1}u) \rangle = \langle v, a^{-1}(u) \rangle = 0$ (т.к. $a^{-1}(u) \in U$).

3. Пусть $au = \lambda u;\ av = \mu v;\ \lambda \neq \mu$.

   $\langle u, v \rangle = \langle a(u), a(v) \rangle = \langle \lambda u, \mu v \rangle = \overline{\lambda}\mu \langle u, v \rangle$

   Из полученного равенства следует, что либо $\langle u, v \rangle = 0$, либо $\overline{\lambda}\mu = 1$.

   Но при этом мы знаем, что λ лежит на единичной окружности, т.е. $\overline{\lambda}\lambda = 1$, а тогда т.к. $\mu \neq \lambda$, то второй случай отпадает. Значит, действительно, любые два вектора соответствующие различным собственным числам ортогональны.

□

3.2. Сопряжённые операторы

***Определение* 3.3.**

Линейные операторы a и a^* над евклидовым или эрмитовым пространство V называются сопряжёнными, если

$\forall v, w \in V : \langle a^*(v), w \rangle = \langle v, a(w) \rangle$

Свойство.

Если A — матрица a, то $A^* = G^{-1}\overline{A^T}G$, где A^* — матрица сопряженного a оператора a^* в том же самом базисе.

Доказательство.

Из определения: $\overline{A^*}^T G = GA \implies \overline{A^*} = (GAG^{-1})^T \implies A^* = G^{-1}\overline{A^T}G$

В последним переходе пользуемся свойствами матрицы Грама. □

Замечание.

В частности, получили, что сопряженный оператор всегда существует и единственный.

Факт.

Рассмотрим отображение $r : V \to V^*$, такой что $v \mapsto \langle v, \cdot \rangle$.

Тогда r — изоморфизм.

Доказательство.

Покажем, что r — инъекция. Т.е, что $\operatorname{Ker} r = \{0\}$.

$\operatorname{Ker} r = \{v \in V : \forall u \in V\ \ \langle v, u \rangle = 0\}$, в частности, $\langle v, v \rangle = 0 \implies v = 0$. □

Замечание.

1. Введем скалярное произведение в двойственном пространстве:

   $\langle \langle v, \cdot \rangle, \langle u, \cdot \rangle \rangle = \langle v, u \rangle$

2. Пусть $e_1, \dots, e_n$ — ортонормированный базис V.

   Тогда $r(e_1), \dots, r(e_n)$ — двойственный базис в пространстве V^*, а точнее $r(e_j)(e_i) = \delta_{i,j}$

3. Если V — эрмитово, а $z \in \mathbb{C}$, то $r(zv) = \overline{z}r(v)$.

   Отображение, обладающие таким свойством называется антилинейным.

4. Рассмотрим оператор a.

   $a^* : V \to V$, $a' : V^* \to V^*$ (сопряженный оператор из прошлого года)

   Заметим, что $r(a^*(x)) = \langle a^*(x), \cdot \rangle = \langle x, a(\cdot) \rangle = a'(\langle x, \cdot \rangle) = a'(r(x)) \ \ \forall x \in V$

   А значит, $a^* = r^{-1}a'r$.

3.3. Самосопряженные операторы

***Определение* 3.4.**

Пусть V — евклидово или эрмитово, $a \in \mathrm{End}(V)$.

Оператор a называется самосопряженным, если $a = a^*$.

Замечание.

В терминах матриц получаем равенство $A = G^{-1}\overline{A}^T G$, а в ортонормированном базисе получаем $A = \overline{A}^T$

Теорема 3.6.

Пусть V — евклидово или эрмитово, а $a \in \mathrm{End}(V)$. Тогда:

1. a — самосопряжен $\iff$ $\begin{cases} \mathrm{Spec}(a) \subset \mathbb{R} \\ \exists e_1, \dots, e_n \text{ — ортонормированный базис, т.ч. } a_e \text{ — диагональная} \end{cases}$

2. Собственные вектора, соответствующие различным собственным числам, ортогональны.

Доказательство.

1. “ $\Longleftarrow$ ”

   Рассмотрим базис, в котором A диагональна.

   Тогда $\overline{A} = A$, и $A^T = A \implies A = \overline{A}^T$, тогда, т.к. базис ортонормированный, то A — самосопряжен.

   “ $\Longrightarrow$ ”

   Покажем, что все собственные числа вещественны.

   $\forall \lambda \in \mathrm{Spec}(V) : \ av = \lambda v$

   Пусть V — эрмитово. Тогда:

   $\lambda\langle v, v\rangle = \langle v, \lambda v\rangle = \langle v, av\rangle = \langle av, v\rangle = \langle \lambda v, v\rangle = \overline{\lambda}(v, v)$

   А так как $\langle v, v\rangle \neq 0$, то $\lambda = \overline{\lambda} \implies \lambda \in \mathbb{R}$

   Если же V — евклидово, то рассмотрим $V^{\mathbb{C}}$ со скалярным произведением:

   $\langle u_1 + iv_1, u_2 + iv_2\rangle := \langle u_1, u_2\rangle + i\langle u_1, v_2\rangle - i\langle v_1, u_2\rangle + \langle v_1, v_2\rangle$

   Таким образом, получили эрмитово пространство $V^{\mathbb{C}}$. Покажем, что $a^{\mathbb{C}}$ — самосопряженный.

$\langle a^{\mathbb{C}}(u_1+iv_1), u_2+iv_1\rangle = \langle a(u_1)+ia(v_1), u_2+iv_2\rangle = \langle a(u_1),u_2\rangle + i\langle a(u_1),v_2\rangle - i\langle a(v_1),u_2\rangle + \langle a(v_1),v_2\rangle = \langle u_1, a(u_2)\rangle + i\langle u_1,a(v_2)\rangle - i\langle v_1,a(u_2)\rangle + \langle v_1,a(v_2)\rangle = \langle u_1+iv_1, a(u_2)+ia(v_2)\rangle = \langle u_1+iv_1, a^{\mathbb{C}}(u_2+iv_1)\rangle$

Но для самосопряжённых операторов над эрмитовым пространством мы знаем, что их собственные числа — вещественные.

А поскольку $\chi_a^{\mathbb{C}} = \chi_a$, то получаем, что собственные числа оператора a также будут вещественными.

Теперь предъявим ортонормированный базис, в котором матрица диагональна.

Индукция по размерности n.

База при $n=1$ — подойдет любой базис.

Переход:

Рассмотрим $\lambda \in \mathrm{Spec}(a)$, и v — соответствующий собственный вектор.

Тогда $V = \langle v\rangle \oplus \langle v\rangle^{\perp}$ (мы уже доказывали, что все такие суммы прямые).

Нужно показать, что $\langle v\rangle$ и $\langle v\rangle^{\perp}$ — инвариантны относительно a.

Инвариантность $\langle v\rangle$ очевидна. Покажем инвариантность $\langle v\rangle^{\perp}$.

Рассмотрим $v \in \langle v\rangle^{\perp}$. Хотим проверить, что $\langle u, av\rangle = 0\ \forall u \in \langle v\rangle$

$\langle u, av\rangle = \langle au, v\rangle = \langle \lambda u, v\rangle = \lambda\langle u,v\rangle = 0$

2. $au = \lambda u,\ \ av = \mu v$

   $\overline{\lambda}\langle u,v\rangle = \langle \lambda u, v\rangle = \langle au, v\rangle = \langle u, av\rangle = \langle u, \mu v\rangle = \mu\langle u,v\rangle \implies \langle u,v\rangle = 0$, т.к. $\lambda \neq \mu$

□

Следствие.

Пусть $A \in \mathbb{R}^{n\times n}$ или $A \in \mathbb{C}^{n\times n}$, при этом $\overline{A}^T = A$ (т.е. это матрица самосопряженного оператора в ортонормированном базисе). Тогда:

1. Все корни χ_A — вещественные
2. Существует ортогональная (или унитарная) матрица C, такая что $C^{-1}AC = \overline{C}^T AC$ — диагональная.

Доказательство.

Рассмотрим пространство в котором задана наша матрица ($\mathbb{R}^{n\times n}$ или $\mathbb{C}^{n\times n}$).

Тогда наша матрица задает самосопряженный оператор, а значит все собственные числа вещественны, т.е. характеристический многочлен имеет n вещественных корней.

При этом, существует ортонормированный базис, в котором матрица будет диагональна, а значит C — соответствующая матрица перехода. □

Лемма.

$\Omega = \sum a_{i,j}x_ix_j + \sum b_ix_i + c = 0$

1) Если $\sum a_{i,j}x_ix_j$ — невырождена, то Ω можно привести к диагональному виду.

2) Иначе Ω представима в виде $\sum\limits_{i\in I} x_i^2 + \sum\limits_{i\notin I} d_ix_i + s = 0$.

3.4. Нормальные операторы

***Определение* 3.5.**

V — евклидово или эрмитово пространство, $a \in \mathrm{End}(V)$.

a — нормальный, если $a \circ a^* = a^* \circ a$

Свойства.

1) $(a+b)^* = a^* + b^*$

2) $(a^{-1})^* = (a^*)^{-1}$

3) $a^{**} = a$

4) $(ab)^* = b^* a^*$

5) $\overline{A}^T \longleftrightarrow a^*$

Пример.

1) Самосопряжённые операторы $a = a^*$

2) Антисамосопряжённые (кососимметрические) опреаторы $a = -a^*$

3) Унитарные операторы $a^* = a^{-1}$

Теорема 3.7.

V — эрмитово пространство, $a \in \mathrm{End}(V)$.

1) a — нормальный оператор $\iff \exists$ ортонормированный базис, в котором матрица a диагональна. При этом диагональные элементы определены однозначно.

2) Оператор самосопряжённый $\iff$ оператор диагонализуем и элементы диагонали — $\mathrm{Spec} \subset \mathbb{R}$.

3) Оператор кососимметрический $\iff$ оператор диагонализуем и элементы диагонали — $\mathrm{Spec} \subset \mathbb{R}i$

4) Оператор унитарный $\iff$ оператор диагонализуем и элементы диагонали — $\mathrm{Spec} \subset \{z : |z| = 1\}$

Доказательство.

2 и 4 уже доказали ранее, 3 доказывать не будем. Докажем 1.

“ $\Longleftarrow$ ”

Пусть e — базис в котором матрица диагональна.

Запишем $A^* = \overline{A}^T$. При этом, т.к. A — диагональна, то $A^T = A \implies A^* = \overline{A}$.

Нужно проверить, что $AA^* = A^*A \iff A\overline{A} = \overline{A}A$.

Последнее равенство очевидно, т.к. A — диагональна.

“ $\Longrightarrow$ ”

Индукция по размерности $\dim V = n$.

$\dim V = 1$ — подойдет любой базис.

$\dim V > 1$

Рассмотрим $\lambda \in \mathrm{Spec}(a)$, V_λ — соответствующее корневое подпространство.

Если $V = V_\lambda$, то каждый вектор — собственный, а значит можем выбрать ортонормированный базис, матрица в нём диагональна.

Иначе $V = V_\lambda \oplus V_\lambda^\perp$

Для перехода нужно показать, что V и $V_\lambda^\perp$ инвариантны относительно a и a^*.

V_λ — a-инвариантно (очевидно).

V_λ — a^*-инвариантно, т.к. $\forall v \in V_\lambda : a(a^*v) = a^*av = a^*\lambda v = \lambda(a^*v)$.

$V_\lambda^\perp$ — a-инвариантно, т.к. $\forall v \in V_\lambda^\perp \ \ \forall u \in V_\lambda : \langle av, u\rangle = \langle v, a^*u\rangle = 0$, поскольку $a^*u \in V_\lambda$.

$V_\lambda^\perp$ — a^*-инвариантно, т.к. $\langle a^*v, u\rangle = \langle v, au\rangle = 0$, поскольку $au \in V_\lambda$.

Значит, можно сделать переход индукции. □

3.5. Полярное разложение

Лемма.

Пусть V — эрмитово, $a \in \mathrm{End}(V)$.

Тогда a^*a — самосопряжённый и $\mathrm{Spec}(a^*a) \in \mathbb{R}_{\geqslant 0}$

Доказательство.

$(a^*a)^* = a^*(a^*)^* = a^*a$, т.е. оператор действительно самосопряжен, в частности $\mathrm{Spec}(a^*a) \in \mathbb{R}$.

Рассмотрим собственное число λ оператора a^*a, и докажем, что $\lambda \geqslant 0$.

Пусть v — соответствующий λ собственный вектор.

$\lambda\|v\|^2 = \lambda\langle v, v\rangle = \langle \lambda v, v\rangle = \langle a^*av, v\rangle = \langle av, av\rangle = \|av\|^2 \implies \lambda = \frac{\|av\|^2}{\|v\|^2} \geqslant 0$ □

Замечание. При подстановке в условие леммы вместо оператора a сопряженного ему оператора a^* получаем аналогичное утверждение для оператора aa^*.

Следствие. Для любого оператора a существуют базисы e и f, такие что операторы a^*a_e и aa^*_f диагональны, причем все, диагональные элементы лежат в $\mathbb{R}_{\geqslant 0}$.

Доказательство. Т.к. операторы a^*a и aa^* самосопряженные, то существуют базисы, в которых они диагональны. При этом все элементы на диагонали будут положительны, т.к. они являются собственными числами операторов, которые положительны по доказанной выше лемме. □

Обозначение.

Пусть $A = \begin{pmatrix} a_1 & 0 & \cdot & 0 \\ 0 & a_2 & \cdot & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdot & a_n \end{pmatrix}$, тогда обозначим $\sqrt{A} = \begin{pmatrix} \sqrt{a}_1 & 0 & \cdot & 0 \\ 0 & \sqrt{a}_2 & \cdot & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdot & \sqrt{a}_n \end{pmatrix}$

Свойства.

1) $\sqrt{A}$ — диагональна.

2) Если $A \in \mathrm{Aut}(V)$, то $\sqrt{A} \in \mathrm{Aut}(V)$.

3) Если $A = aa^*$(или a^*a) для какого-то оператора a, то $\sqrt{A}$ самосопряженный оператор.

Доказательство.

2) Свойство диагональной матрицы быть автоморфизмом равносильно отсутствию нулевых элементов на диагонали. Операция взятия корня сохраняет данное свойство.

3) $A = aa^* \implies \mathrm{Spec}(A) \in \mathbb{R}_{\geqslant 0}$, а значит все $a_i \geqslant 0$, тогда все $\sqrt{a_i} \in \mathbb{R}$, а значит $\sqrt{A}$ - самосопряженный. □

Лемма.

Пусть V — векторное пространство над $\mathbb{C}$; a, $b \in \mathrm{End}(V)$; $ab = ba$.

Тогда у a и b есть общий собственный вектор.

Доказательство.

$\dim V = 1$ — то любой вектор является собственным.

$\dim V > 1$

Т.к. мы находимся над полем комплексных чисел, то $\exists \lambda \in \mathrm{Spec}(a)$.

Рассмотрим пространство $V_\lambda^{(a)}$. Докажем, что оно инвариантно относительно b.

Нам нужно показать, что если $av = \lambda v$, то и $abv = \lambda bv$. Проверим это

$$abv = bav = b\lambda v = \lambda bv$$

Теперь выберем в $V_\lambda^{(a)}$ собственный вектор оператора b (опять пользуемся тем, что мы над $\mathbb{C}$). Он будет собственным и для оператора a, т.е. мы нашли искомый вектор. □

Следствие.

Если V — векторное пространство над $\mathbb{C}$; a, $b \in \mathrm{End}(V)$ — нормальные и $ab = ba$, то
$\exists$ базис e, в котором a_e, b_e — диагональны.

Доказательство.

Доказываем индукцией по $\dim V = n$.

Если размерность V равна 1, то операторы диагональны в любом базисе.

Переход $n \to n + 1$.

По лемме существует общий собственный вектор v для операторов a и b. При этом можно разложить $V = \langle v \rangle \oplus \langle v \rangle^\perp$, далее, т.к. $\langle v \rangle^\perp$ инвариантно относительно a и b (т.к. нормальные), то мы можем воспользоваться предположением индукции. □

Теорема 3.8.

Пусть V — эрмитово, $a \in \mathrm{Aut}(V)$.

Тогда существует и единственное представление $a = u_1 s_1 = s_2 u_2$, такое, что s_1, s_2 — самосопряженный, а u_1, u_2 — унитарные.

Замечание.

Такая формулировка не совсем корректна. От операторов s_1 и s_2 еще требуется положительность (спектр положителен).

Доказательство.

Докажем существование.

Рассмотрим aa^* и a^*a — самосопряжённые.

По доказанной лемме существуют базисы e, f такие что $(a^*a)_e = B_1$ - диагональная, $(aa^*)_f = B_2$ - диагональная.

Тогда положим $(s_1)_e = \sqrt{B_1}$ - диагональная $(s_2)_f = \sqrt{B_2}$ - диагональная. Заметим, что мы сразу получили самосопряженность операторов s_1 и s_2.

Также мы знаем, что $a^*a = s_1^2$, $aa^* = s_2^2 \in \mathrm{Aut}(V)$, а значит s_1, $s_2 \in \mathrm{Aut}(V)$, а значит, существуют обратные операторы.

Тогда положим $u_1 = as_1^{-1}, u_2 = s_2^{-1}a$.

Заметим, что построенные операторы удовлетворяют требуемым равенствам $a = u_1 s_1 = s_2 u_2$.

Осталось показать, что u_1 и u_2 унитарные. Рассмотрим $x, y \in V$.

Тогда $\langle u_1 x, u_1 y\rangle = \langle a s_1^{-1} x, a s_1^{-1} y\rangle = \langle x, (a s_1^{-1})^* a s_1^{-1} y\rangle = \langle x, s_1^{-1} a^* a s_1^{-1} y\rangle = \langle x, s_1^{-1} s_1^2 s_1^{-1} y\rangle = \langle x, y\rangle$

$\langle u_2 x, u_2 y\rangle = \langle s_2^{-1} a x, s_2^{-1} a y\rangle = \langle x, (s_2^{-1} a)^* s_2^{-1} a y\rangle = \langle x, a^* (s_2^2)^{-1} a y\rangle = \langle x, a^* (a a^*)^{-1} a y\rangle = \langle x, y\rangle$

Перейдем к единственности.

Пусть $a = s_2 u_2 = s_2' u_2'$.

$a a^* = s_2 u_2 (s_2 u_2)^* = s_2 u_2 u_2^* s_2 = s_2^2 \implies s_2^2 = a a^*$

Это означает, что $s_2 (a a^*) = s_2^3 = (a a^*) s_2$, а тогда существует общий ортонормированный базис e, в котором матрицы операторов $a a^*$ и s_2 диагональны.

При этом, матрица s_2^2 совпадает с матрицей $a a^*$ в любом базисе, а значит, является диагональной и однозначно определенной.

Тогда мы получили, что оператор s_2 однозначно определен, а каждый элемент на диагонали равен корню из соответствующего диагонального элемента s_2^2.

Т.е. получили, что $s_2 = s_2'$

Теперь можно восстановить операторы u_2 и u_2' единственным образом как $u_2 = u_2' = s_2^{-1} a$ $\square$

4. Ад (или тензоры)

4.1. Полилинейная алгебра

В данном параграфе $V_1, \ldots, V_n, U$ — векторные пространства над полем K.

***Определение* 4.1.**
Линейное пространство всех полилинейных функций $f : V_1 \times \ldots \times V_n \to U$ будем называть полилинейным пространством.

Обозначается $\mathrm{Hom}(V_1, \ldots, V_n, U)$.

Обозначение.
Пусть $v_1 \in V_1, \ldots, v_n \in V_n$.

Функцию $f : V_1 \times \ldots \times V_n \to K$, такую, что f принимает значение 1 в точке $v_1, \ldots, v_n$ и значение 0 во всех остальных точках, обозначим $(v_1, \ldots, v_n)$.

Замечание.
Любая функция, принимающая ненулевое значение в конечном числе точек является конечной суммой функций $(v_1, \ldots, v_n)$ с коэффициентами из поля K.

***Определение* 4.2.**
Введем множество M, как множество всех финитных функций (функций, описанных в замечании выше)

Тогда $M := \{\sum\limits_{\substack{\text{конечная}\\ \text{сумма}}} a_{v_1,\ldots,v_n}(v_1, \ldots, v_n) : a_{v_1,\ldots,v_n} \in K\}$.

Замечание.
Множество M с покоординатным сложением и умножением на скаляр является векторным пространством над полем K.

Базисом будет являться множество всех функций $(v_1, \ldots, v_n)$.

***Определение* 4.3.**
Рассмотрим подпространство $M_0 \subseteq M$.

$M_0 = \langle (v_1, \ldots, v'_k + v''_k, \ldots, v_n) - (v_1, \ldots, v'_k, \ldots, v_n) - (v_1, \ldots, v''_k, \ldots, v_n),$
$(v_1, \ldots, \alpha v_k, \ldots, v_n) - \alpha(v_1, \ldots, v_k, \ldots, v_n) : \forall k \in [1..n],\ v_i \in V_i,\ v_k, v'_k, v''_k \in V_k \rangle$

***Определение* 4.4.**
Определим тензорное произведение пространств $V_1, V_2, \ldots, V_n$ как M/M_0.

Обозначается $V_1 \otimes \ldots \otimes V_n$.

Замечание.
Важно заметить, что при определении тензорного произведения мы нигде не опирались на базисы изначальных пространств.

***Определение* 4.5.**
Класс эквивалентности функции $(v_1, \ldots, v_n)$ называется разложимым тензором.

Обозначается $v_1 \otimes \ldots \otimes v_n$.

$v_1 \otimes \ldots \otimes v_n = (v_1, \ldots, v_n) + M_0$

Замечание.

При этом из-за выбора множества M_0 мы сразу получаем различные равенства на разложимые тензоры. К примеру, $v_1 \otimes \ldots \otimes \alpha v_i \otimes \ldots \otimes v_n = \alpha(v_1 \otimes \ldots \otimes v_n)$ (прямо внутри выбора M_0 прописано, что классы эквивалентности $\alpha(v_1, \ldots, v_n)$ и $(v_1, \ldots, \alpha v_i, \ldots, v_n)$ совпадают).

Лемма.

Разложимые тензоры порождают $V_1 \otimes \ldots \otimes V_n$.

Доказательство.

Действительно, функции $(v_1, \ldots, v_n)$ порождают все пространство M, а тогда их классы эквивалентности, т.е. разложимые тензоры, порождают все пространство $V_1 \otimes \ldots \otimes V_n$. □

Следствие.

Если одно из векторных пространств V_i тривиально, то и всё тензорное произведение тривиально.

Доказательство.

Из доказанной леммы нам достаточно показать, что все разложимые тензоры нулевые.

Действительно, $v_1 \otimes \cdots \otimes 0 \otimes \cdots \otimes v_n = 0 \cdot v_1 \otimes \cdots \otimes 0 \otimes \cdots \otimes v_n = 0$

Иначе говоря, класс эквивалентности $(v_1, \ldots, 0, \ldots, v_n)$ совпадает с классом эквивалентности нуля, т.к. $(v_1, \ldots, 0, \ldots, v_n) - 0 \cdot (v_1, \ldots, 0, \ldots, v_n) \in M_0$, а $0 \cdot (v_1, \ldots, 0, \ldots, v_n) = 0$. □

Обозначение.

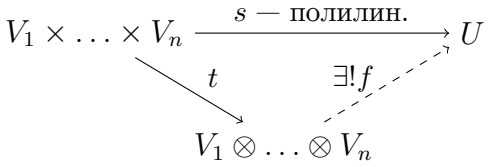
Введем отображение $t : V_1 \times \ldots \times V_n \to V_1 \otimes \ldots \otimes V_n$:

$(v_1, \ldots, v_n) \mapsto v_1 \otimes \ldots \otimes v_n$

Теорема 4.1.

1) t — полилинейно

2) t — универсально, т.е. $\forall s \in \mathrm{Hom}(V_1, \ldots, V_n, U)\ \ \exists! f \in \mathrm{Hom}(V_1 \otimes \ldots \otimes V_n, U)$, т.ч. $s = f \circ t$



Доказательство.

Проверим полилинейность t.

$\alpha t((v_1, \ldots, v_n)) = \alpha(v_1 \otimes \ldots \otimes v_n) = (v_1 \otimes \ldots \otimes \alpha v_i \otimes \ldots v_n) = t((v_1, \ldots, \alpha v_i, \ldots v_n))$

Аналогично проверяется аддитивность.

Перейдем к универсальности.

Единственность:

Пусть $f_1 \circ t = s = f_2 \circ t$

Тогда $f_1 \circ t(v_1, \ldots, v_n) = f_2 \circ t(v_1, \ldots, v_n) \implies f_1(v_1 \otimes \ldots \otimes v_n) = f_2(v_1 \otimes \ldots \otimes v_n)$, а значит, раз $v_1 \otimes \ldots \otimes v_n$ образуют все пространство, то $f_1 = f_2$.

Существование:

Определим линейное отображение $g : M \to U$ на функциях $(v_1, \ldots, v_n)$.

$g(v_1, \ldots, v_n) = s(v_1, \ldots, v_n)$.

Тогда по линейности, g единственным образом продолжается на все суммы.

$g\Big(\sum a_{v_1,\ldots,v_n}(v_1,\ldots,v_n)\Big) = \sum a_{v_1,\ldots,v_n} s(v_1,\ldots,v_n)$

Тогда можем определить $f : M/M_0 \to U$, а именно $X \mapsto g(x)$, где $x \in X$ — элемент из соответствующего класса эквивалентности.

Для обоснования корректности нужно показать, что $g(x) = g(y)$, если x и y лежат в одном классе эквивалентности.

Т.е. нужно проверить, что $g(x - y) = 0$. Мы знаем, что $x - y \in M_0$, а значит достаточно показать, что $M_0 \subseteq \operatorname{Ker} g$.

Это очевидно т.к. g обнуляется на каждом образующем векторе M_0 по линейности.

Таким образом, получили искомое отображение f. □

Замечание.

Благодаря этой теореме мы теперь можем определять гомоморфизм лишь на разложимых тензорах.

Т.е. если мы хотим задать гомоморфизм $\sigma : V_1 \otimes \ldots \otimes V_n \to U$, то мы можем задать лишь полилинейное отображение $V_1 \times \ldots \times V_n \to U$ (эквивалентно определению σ на разложимых векторах), по которому из теоремы единственным образом определяется σ.

Следствие.

1. Существует **канонический** изоморфизм векторных пространств:
   $\operatorname{Hom}(V_1,\ldots,V_n,U) \cong \operatorname{Hom}(V_1 \otimes \ldots \otimes V_n, U)$
2. $\operatorname{Hom}(V_1,\ldots,V_n,K) \cong (V_1 \otimes \ldots \otimes V_n)^*$
3. $\dim(V_1 \otimes \ldots \otimes V_n) = \dim V_1 \cdot \ldots \cdot \dim V_n$
4. Пусть $e_1^{(i)}, e_2^{(i)}, \ldots, e_{k_i}^{(i)}$ — базис V_i.
   Тогда $e_{j_1}^{(1)} \otimes e_{j_2}^{(2)} \otimes \ldots \otimes e_{j_n}^{(n)}$ — базис $V_1 \otimes \ldots \otimes V_n$, $1 \leqslant j_l \leqslant k_l$

Доказательство.

1. Рассмотрим отображение φ, сопоставляющее элементу $s \in \operatorname{Hom}(V_1,\ldots,V_n,U)$ элемент $f \in \operatorname{Hom}(V_1 \otimes \ldots \otimes V_n, U)$, такой, что $s = f \circ t$. Проверим, что φ изоморфизмом.

   Гомоморфизм:

   $\varphi(s_1 + s_2) = \varphi(f_1 \circ t + f_2 \circ t) = \varphi((f_1 + f_2) \circ t) = f_1 + f_2 = \varphi(s_1) + \varphi(s_2)$.

   $\varphi(\alpha s) = \varphi(\alpha(f \circ t)) = \varphi(\alpha f \circ t) = \alpha f = \alpha\varphi(s)$

   Сюръективность: Пусть $f \in \operatorname{Hom}(V_1 \otimes \ldots \otimes V_n, U)$. Тогда $\varphi(f \circ t) = f$. Осталось заметить, что $f \circ t \in \operatorname{Hom}(V_1,\ldots,V_n,U)$, т.к. f — гомоморфизм, а t — полилинейна.

   Инъективность: $f = \varphi(s) = 0 \implies s = f \circ t \implies s = 0$

2. Следует из первого пункта, если подставить $U = K$

   ($\operatorname{Hom}(V, K) = V^*$, если V — векторное пространство над K).

3. $\dim(V_1 \otimes \ldots \otimes V_n) = \dim(V_1 \otimes \ldots \otimes V_n)^* = \dim\Big(\operatorname{Hom}(V_1,\ldots,V_n,K)\Big) = \dim V_1 \cdot \ldots \cdot \dim V_n$

4. Уже показали, что размерность $V_1 \otimes \ldots \otimes V_n$ совпадает с количеством элементов в предъявленном базисе, значит, осталось показать, что он является системой образующих.

   Покажем, что каждый разложимый вектор $V_1 \otimes \ldots \otimes V_n$ представим в выбранном базисе. Из этого последует, что любой элемент $V_1 \otimes \ldots \otimes V_n$ представим, т.к. разложимые вектора являются системой образующих.

   Рассмотрим разложимый вектор $v_1 \otimes \ldots \otimes v_n$. Разложим каждое из v_i по базису пространства V_i, а затем по полилинейности получим представление в описанном базисе (раскроем скобки), что и требовалось.

Пример. (Комплексификация) □

Начнем с известного нам примера комплексификации.

Пусть V — векторное пространство над $\mathbb{R}$ с базисом $e_1, \ldots, e_n$.

Рассмотрим пространство $\mathbb{C} \otimes V$ как векторное пространство над $\mathbb{C}$. Для этого нужно определить домножение на комплексный аргумент. Определим его как $\alpha(z \otimes v) = \alpha z \otimes v$.

Базисом $\mathbb{C} \otimes V$ будет множество $1 \otimes e_j$, т.к. остальные базисные вектора (как пространства над $\mathbb{R}$) выражаются через домножение на i.

Покажем, что есть изоморфизм векторных пространств $\mathbb{C} \otimes V$ и $V^{\mathbb{C}}$.

Зададим отображение $1 \otimes e_j \mapsto (e_j, 0)$. Оно переводит базис в базис.

Замечание.

При определении умножения над полем $\mathbb{C}$ мы определяем умножение лишь на разложимых тензорах.

Мы имеем на это право согласно теореме про универсальность отображения $V_1 \times \ldots \times V_n \to V_1 \otimes \ldots \otimes V_n$ (см. замечание).

Пример. (Расширение скаляров)

Попробуем теперь обобщить пример выше.

Пусть L, K — поля, $K \subseteq L$ (к примеру, ситуация с $\mathbb{R}$ и $\mathbb{C}$).

V — векторное пространство над K.

Заметим, что L и V — векторные пространства над полем K, а значит мы можем рассмотреть $L \otimes V$ как векторное пространство над K.

Теперь мы хотим ввести структуру линейного пространства $L \otimes V$ над полем L. Нужно определить домножние на скаляр разложимых векторов $L \otimes V$.

Определим как $\alpha(\beta \otimes v) = (\alpha\beta) \otimes v$, где α, β — элементы поля L, v — вектор V.

Получили корректную структуру (далее все определяется по линейности).

Замечание.

Аналогичное комплексификации.

Лемма.

1) Существует **канонический** изоморфизм $V_1 \otimes V_2 \cong V_2 \otimes V_1$.

2) Существует **канонический** изоморфизм $(V_1 \otimes V_2) \otimes V_3 \cong V_1 \otimes (V_2 \otimes V_3)$.

3) Существует **канонический** изоморфизм $V_1^* \otimes \ldots \otimes V_n^* \cong (V_1 \otimes \ldots \otimes V_n)^*$.

4) Существует **канонический** изоморфизм $U^* \otimes V \cong Hom(U, V)$.

Доказательство.

Нам всегда достаточно определять отображение лишь на разложимых векторах.

1) $v_1 \otimes v_2 \mapsto v_2 \otimes v_1$

Такое отображение, очевидно является изоморфизмом, т.к. для любого выбранного базиса пространства $V_1 \otimes V_2$ он перейдет в базис $V_2 \otimes V_1$.

2) Покажем, что существует канонический изоморфизм $V_1 \otimes V_2 \otimes V_3 \cong V_1 \otimes (V_2 \otimes V_3)$.

$(v_1 \otimes v_2 \otimes v_3) \mapsto v_1 \otimes (v_2 \otimes v_3)$ — является требуемым изоморфизмом, т.к. любой базис перейдет в базис.

3) Мы знаем, что существует канонический изоморфизм $\mathrm{Hom}(V_1, \ldots, V_n, K) \cong (V_1 \otimes \ldots \otimes V_n)^*$.

Осталось найти канонический изоморфизм $V_1^* \otimes \ldots \otimes V_n^* \cong \mathrm{Hom}(V_1, \ldots, V_n, K)$.

$f_1 \otimes \ldots \otimes f_n \mapsto ((v_1, \ldots, v_n) \mapsto f_1(v_1) \ldots f_n(v_n))$.

Проверим инъективность. Пусть результирующее отображение нулевое. Тогда одно из $f_i = 0$, а тогда и $f_1 \otimes \ldots \otimes f_n = 0$, что и требовалось.

Осталось заметить, что размерности пространств совпадают.

4) Рассмотрим отображение $f \otimes v \mapsto (u \mapsto f(u)v)$.

Покажем, что оно изоморфизм.

$e_1, \ldots, e_n$ — базис U

$e^1, \ldots, e^n$ — двойственный базис U^*

$f_1, \ldots, f_m$ — базис V

Нужно проверить, что базис переходит в базис:

$e^i \otimes f_j \mapsto (u \mapsto u^i f_j)$

Рассмотрим, как действует отображение $u \mapsto u^i f_j$ на базисные вектора: $e_k \mapsto \delta^i_k f_j$, где δ^i_k — символ Кронекера. Это и есть базисный элемент $Hom(U, V)$.

□

4.2. Тензорная алгебра

Во всем параграфе V — конечномерное векторное пространство над K.

Обозначение.
$T^q_p(V) = \underbrace{V^* \otimes \ldots \otimes V^*}_{p} \otimes \underbrace{V \otimes \ldots \otimes V}_{q}$

Обозначение.
$V^{\otimes p} := \underbrace{V \otimes \ldots \otimes V}_{p}$

***Определение* 4.6.**
Элементы пространства $T^q_p(V)$ — тензоры типа (p, q)

$p + q$ — валентность

Пример.

1. $T^0_0(V) = K$
2. $T^0_1(V) = V^*$
3. $T^1_0(V) = V$
4. $T^1_1(V) = V^* \otimes V \cong \mathrm{Hom}(V, V)$

5. $T_2^0 = V^* \otimes V^* \cong (V \otimes V)^* \cong \mathrm{Hom}(V, V, K)$

***Определение* 4.7.**

$\otimes : T_p^q(V) \times T_{p'}^{q'}(V) \to T_{p+p'}^{q+q'}(V)$ — произведение тензоров.

Первый способ определения умножения тензоров:

$f \in T_p^q(V) \cong (V^{\otimes p} \otimes V^{*\otimes q})^* \cong \mathrm{Hom}(\underbrace{V, \ldots, V}_{p}, \underbrace{V^*, \ldots, V^*}_{q}, K)$

$g \in T_{p'}^{q'}(V) \cong (V^{\otimes p'} \otimes V^{*\otimes q'})^* \cong \mathrm{Hom}(\underbrace{V, \ldots, V}_{p'}, \underbrace{V^*, \ldots, V^*}_{q'}, K)$

Тогда определим $(f \otimes g)(v_1, \ldots, v_p, v'_1, \ldots, v'_{p'}, f_1, \ldots, f_q, f'_1, \ldots, f'_{q'}) =$
$= f(v_1, \ldots, v_p, f_1, \ldots, f_q) \cdot g(v'_1, \ldots, v'_{p'}, f'_1, \ldots, f'_{q'})$

Замечание.

Мы определили умножение как функцию, определив ее в каждой точке. Нужно проверить, что то, что мы определили корректно.

***Определение* 4.8.**

Второй способ определения умножения тензоров:

$T_1 = f_1 \otimes \ldots \otimes f_p \otimes v_1 \otimes \ldots \otimes v_q$

$T_2 = g'_1 \otimes \ldots \otimes g_{p'} \otimes u_1 \otimes \ldots \otimes u_{q'}$

Тогда $T_1 \otimes T_2 = f_1 \otimes \ldots \otimes f_p \otimes g'_1 \otimes \ldots \otimes g_{p'} \otimes v_1 \otimes \ldots \otimes v_q \otimes u_1 \otimes \ldots \otimes u_{q'}$

Далее по линейности.

Свойства.

$a, b \in K, \;\; f_1, f_2 \in T_p^q(V), \;\; g \in T_{p'}^{q'}(V)$

1) $(af_1 + bf_2) \otimes g = af_1 \otimes g + bf_2 \otimes g$

2) $f \otimes (ag_1 + bg_2) = af \otimes g_1 + bf \otimes g_2$

3) $(f \otimes g) \otimes h = f \otimes (g \otimes h)$

Замечание.

Коммутативности произведения в общем случае нет, т.е. $f \otimes g \neq g \otimes f$

***Определение* 4.9.**

$T(V) = \bigoplus\limits_{p,q \geqslant 0} T_p^q(V)$ — тензорная алгебра.

Введем умножение $T_p^q \otimes T_{p'}^{q'} = T_{p+p'}^{q+q'}$, а далее продолжаем по линейности (т.е. просто раскрываем скобки).

Замечание.

Аналогичная конструкция: $\{f(x) : f(x) = ax^n\} \implies K[x] = \bigoplus\{ax^n\}$

Замечание.

$e_1, \ldots, e_n$ — базис V, $e^1, \ldots, e^n$ — двойственный базис V^*, $e^i(e_j) = \delta_j^i$

$\{e^{i_1} \otimes \ldots \otimes e^{i_p} \otimes e_{j_1} \otimes \ldots \otimes e_{j_q} : 1 \leqslant i_k, j_l \leqslant n\}$ — базис $T_p^q(V)$

Любой элемент $T \in T_p^q(V)$ раскладывается по базису:

$T = \sum T_{i_1,\ldots,i_p}^{j_1,\ldots,j_q} e^{i_1} \otimes \ldots \otimes e^{i_p} \otimes e_{j_1} \otimes \ldots \otimes e_{j_q}$

Пример.

Рассмотрим, что дает нам формула для $T_2^0(V) \cong \mathrm{Hom}(V, V, K)$, т.е. для билинейных форм.

Наш базис это множество $e^i \otimes e^j$, мы знаем, во что переходят его элементы:

$e^i \otimes e^j \mapsto \big((v_1, v_2) \mapsto v_1^i \cdot v_2^j\big)$

$\sum g_{i,j} e^i \otimes e^j \mapsto ((v_1, v_2) \mapsto \sum g_{i,j} v^i v^j)$

Таким образом, коэффициенты $T_{i,j}$ образуют матрицу нашей билинейной формы $G = (g_{i,j})$.

Алгоритм (Изменение координат при замене базиса)**.**

1. e, f — базисы V, $e = fA$,
2. e^*, f^* — двойственные базисы V^*, $e^* = f^*B$, $B = (A^T)^{-1}$ (видимо, было в прошлом семестре)
3. $T = \sum T^{j_1,\ldots,j_q}_{i_1,\ldots,i_p} e^{i_1} \otimes \ldots \otimes e^{i_p} \otimes e_{j_1} \otimes \ldots \otimes e_{j_q} = \sum T'^{j_1,\ldots,j_q}_{i_1,\ldots,i_p} f^{i_1} \otimes \ldots \otimes f^{i_p} \otimes f_{j_1} \otimes \ldots \otimes f_{j_q}$

   $T'^{j_1,\ldots,j_q}_{i_1,\ldots,i_p} = \sum\limits_{\substack{1 \leqslant l_s \leqslant n \\ 1 \leqslant k_m \leqslant n}} a^{l_1}_{i_1} \cdot \ldots \cdot a^{l_p}_{i_p} \cdot b^{j_1}_{k_1} \cdot \ldots \cdot b^{j_q}_{k_q} \cdot T^{k_1,\ldots,k_q}_{l_1,\ldots,l_p}$

Пояснение.

Последний пункт — это просто раскрытие скобок (подставляем вместо всех e_i, e^i выражения через f_i или f^i, соответственно, а затем раскрываем все скобки по полилинейности)

4.3. Симметричные тензоры

В параграфе V — конечномерное векторное пространство над полем K нулевой характеристики.

Обозначение.

Группа перестановок S_q действует на $T^q_0(V)$, а именно:

Если $\sigma \in S_q$, тогда отображение f_σ действует как $f_\sigma(v_1 \otimes \ldots \otimes v_q) = v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(q)}$.

***Определение* 4.10.**

Пространство симметричных тензоров:

$S^q(V) = \{T \in T^q_0(V) \,|\, f_\sigma T = T \quad \forall \sigma \in S_q\}$, т.е. пространство тензоров, не меняющихся под действием всех элементов группы S_q.

Замечание.

Это подпространство в $T^q_0(V)$.

***Определение* 4.11.**

$S := \frac{1}{q!} \sum\limits_{\sigma \in S_q} f_\sigma$ — оператор симметризации.

Замечание.

Если $T \in T^q_0(V)$, то $S(T) \in S^q(V)$, т.к. определение симметрично относительно всех перестановок составляющих тензора.

Утверждение 4.2.

$T_1 = f_\sigma T_2 \implies S(T_1) = S(T_2)$.

Доказательство.

$S(T_1) = \frac{1}{q!} \sum\limits_{\tau \in S_q} f_\tau T_1 = \frac{1}{q!} \sum\limits_{\tau \in S_q} f_\tau f_\sigma T_2 = \frac{1}{q!} \sum\limits_{\tau \in S_q} f_{\tau\sigma} T_2 = S(T_2)$ □

Утверждение 4.3.

$S^2 = S$

Доказательство.

$$S(S(T)) = \frac{1}{q!}\sum_{\sigma\in S_q} f_\sigma S(T) = \frac{1}{q!}\sum_{\sigma\in S_q} f_\sigma\left(\frac{1}{q!}\sum_{\tau\in S_q} f_\tau T\right) =$$

$$= \frac{1}{q!}\sum_{\sigma\in S_q}\left(\frac{1}{q!}\sum_{\tau\in S_q} f_{\sigma\tau} T\right) = \frac{1}{q!}\sum_{\sigma\in S_q} S(T) = S(T) \qquad \square$$

Утверждение 4.4.
$\operatorname{Im} S = S^q(V)$

Доказательство.
$\operatorname{Im} S \subset S^q(V)$ (из определения S).

Докажем, что для любого $T \in S^q(V)$: $S(T) = T$.

$S(T) = \frac{1}{q!}\sum_{\sigma\in S_q} f_\sigma(T) = T$.

Значит, любой элемент из $S^q(V)$ лежит в $\operatorname{Im} S$, что и требовалось. $\square$

Утверждение 4.5.
Положим $e_1, \ldots, e_n$ — базис V. Тогда

1. Обозначим $S(e_{i_1}\otimes\ldots\otimes e_{i_q})$ как $e_{i_1}\ldots e_{i_q}$.
   Тогда $\{e_{i_1}\ldots e_{i_q}\}$ — базис $S^q(V)$.
2. $S^q(V) \cong \{f \in K[x_1,\ldots,x_n] \mid$ все мономы f имеют степень $q\}$
3. $\dim S^q(V) = \binom{n+q-1}{q}$

Доказательство.

1. Заметим, что $\{e_{i_1}\ldots e_{i_q}\}$ порождают $S^q(V)$, т.к. являются образами базисов при эпиморфизме $S : T_0^q(V) \to S^q(V)$.

   Заметим, что значение $e_{i_1}\ldots e_{i_q}$ не зависит от порядка e_{i_k} ($e_{i_1}\ldots e_{i_q} = e_{\sigma(i_1)}\ldots e_{\sigma(i_q)}$ для любой перестановки σ).

   Будем записывать в более краткой форме: $e_1^{k_1}e_2^{k_2}\ldots e_n^{k_n}$, где $k_1+\ldots k_n = q$ и $k_i \geqslant 0$.

   Покажем, что они линейно независимы.

   $$\sum_{k_1+\ldots+k_n=q} a_{k_1,\ldots,k_n} e_1^{k_1}\ldots e_n^{k_n} = 0.$$

   $$S(\textstyle\sum a_{k_1,\ldots,k_n} e_1^{\otimes k_1}\otimes\ldots\otimes e_n^{\otimes k_n}) = 0$$

   $$\frac{1}{q!}\sum_{\sigma\in S_q}\left(\sum_{k_1+\ldots+k_n=q} a_{k_1,\ldots,k_n} f_\sigma(e_1^{\otimes k_1}\otimes\ldots\otimes e_n^{\otimes k_n})\right) = 0$$

   $$\frac{1}{q!}\sum_{k_1+\ldots+k_n=q} a_{k_1,\ldots,k_n}\left(\sum_{\sigma\in S_q} f_\sigma(e_1^{\otimes k_1}\otimes\ldots\otimes e_n^{\otimes k_n})\right) = 0$$

   Но при ненулевых коэффициентах такая сумма не может занулиться, т.к. внутри скобок находятся **различные** базисные вектора $T_0^q(V)$. А значит, выражение равно нулю только тогда, когда все $a_{k_1,\ldots,k_n}$ равны нулю.

2. $T \in S^q(V)$
   $T = \sum a_{k_1\ldots k_n} e_1^{k_1}\ldots e_n^{k_n} \mapsto \sum a_{k_1\ldots k_n} x_1^{k_1}\ldots x_n^{k_n}$

3. Следует из первого утверждения, совпадает с количеством способов представить q в виде суммы $k_1, \ldots, k_n$.

□

***Определение* 4.12.**
$S(V) = \bigoplus_{q=0}^{\infty} S^q(V)$ — симметричная алгебра.

Введем умножение.

Пусть $T_1 \in S^q(V)$, $T_2 \in S^p(V)$. Тогда $T_1 T_2 = S(T_1 \otimes T_2)$.

Утверждение 4.6.

1. $S(V)$ — коммутативная ассоциативная алгебра.
2. $\left(e_1^{k_1} \ldots e_n^{k_n}\right)\left(e_1^{l_1} \ldots e_n^{l_n}\right) = e_1^{k_1+l_1} \ldots e_n^{k_n+l_n}$

Доказательство.

1. Докажем, что $S(S(T_1) \otimes T_2) = S(T_1 \otimes S(T_2)) = S(T_1 \otimes T_2)$.
   $S(T_1) \otimes T_2 = \frac{1}{p!} \sum\limits_{\sigma \in S_p} f_\sigma(T_1) \otimes T_2$

   $S\Big(S(T_1) \otimes T_2\Big) = S\left(\frac{1}{p!} \sum\limits_{\sigma \in S_p} f_\sigma(T_1) T_2\right) = \frac{1}{p!} \sum\limits_{\sigma \in S_p} S\Big(f_\sigma(T_1) \otimes T_2\Big) = \frac{1}{p!} \sum\limits_{\sigma \in S_p} S(T_1 \otimes T_2) = S(T_1 \otimes T_2).$

   Аналогично — для $S(T_1 \otimes S(T_2))$

   Осталось показать ассоциативность и коммутативность.

   Ассоциативность.

   $(T_1 T_2) T_3 = S(S(T_1 \otimes T_2) \otimes T_3) = S(T_1 \otimes T_2 \otimes T_3) = S(T_1 \otimes S(T_2 \otimes T_3)) = T_1(T_2 T_3)$.

   Коммутативность.

   Достаточно показать для разложимых тензоров.

   В таком случае равенство $S(T_1 \otimes T_2) = S(T_2 \otimes T_1)$ очевидно, а значит по линейности оно выполняется для всех тензоров.
2. $\left(e_1^{k_1} \ldots e_n^{k_n}\right)\left(e_1^{l_1} \ldots e_n^{l_n}\right) = S(S(e_1^{\otimes k_1} \otimes \ldots \otimes e_n^{\otimes k_n}) \otimes S(e_1^{\otimes l_1} \otimes \ldots \otimes e_n^{\otimes l_n})) = e^{k_1+l_1} \ldots e_n^{k_n+l_n}$

□

4.4. Внешняя алгебра или алгебра Грассмана

Замечание.
В этом параграфе по-прежнему считаем, что $\operatorname{Char} K = 0$.

***Определение* 4.13.**
$\Lambda^q(V) = \{T \in T_0^q(V) \,|\, f_\sigma(T) = \operatorname{sign}(\sigma) T \quad \forall \sigma \in S_q\}$ — пространство антисимметричных тензоров.

***Определение* 4.14.**
$A = \frac{1}{q!} \sum\limits_{\sigma \in S_q} \operatorname{sign}(\sigma) f_\sigma$ — оператор альтернирования.

Утверждение 4.7.
$T_1 = f_\sigma T_2 \implies A(T_1) = \operatorname{sign}(\sigma) A(T_2)$

Доказательство.
$A(T_1) = \frac{1}{q!} \sum\limits_{\tau \in S_q} \operatorname{sign}(\tau) f_\tau(T_1) = \frac{1}{q!} \sum\limits_{\tau \in S_q} \operatorname{sign}(\tau) f_{\tau\sigma}(T_2) = \operatorname{sign}(\sigma) \cdot \frac{1}{q!} \sum\limits_{\tau \in S_q} sign(\tau\sigma) f_{\tau\sigma}(T_2) = \operatorname{sign}(\sigma) A(T_2)$
□

Следствие.
$T = f_\sigma T$, $\operatorname{sign}(\sigma) = -1 \implies AT = -AT \implies AT = 0$

Утверждение 4.8.
$A^2 = A$

Доказательство.
$A^2 = \frac{1}{(q!)^2} \sum\limits_{\sigma \in S_q} \sum\limits_{\tau \in S_q} \operatorname{sign}(\sigma) \operatorname{sign}(\tau) (f_\sigma \circ f_\tau) = \frac{1}{(q!)^2} \sum\limits_{\sigma \in S_q} \sum\limits_{\tau \in S_q} \operatorname{sign}(\sigma\tau) f_{\sigma\tau} = \frac{1}{q!} \sum\limits_{\omega \in S_q} \operatorname{sign}(\omega) f_\omega = A.$ □

Утверждение 4.9.
$\operatorname{Im} A = \Lambda^q(V)$

Доказательство.
Проверим, что $\Lambda^q(V) \in \operatorname{Im} A$

$$f_\sigma(A(T)) = f_\sigma \left(\frac{1}{q!} \sum_{\tau \in S_q} \operatorname{sign}(\tau) f_\tau(T) \right) = \operatorname{sign}(\sigma) \left(\frac{1}{q!} \sum_{\tau \in S_q} \operatorname{sign}(\sigma\tau) f_{\sigma\tau}(T) \right) = \operatorname{sign}(\sigma) A(T)$$

С другой стороны, проверим, что $\forall T \in \Lambda^q(V) : A(T) = T$, т.е. что $T \in \operatorname{Im} A$.

$\forall \sigma \in S_q : f_\sigma(T) = \operatorname{sign}(\sigma) T \implies A(T) = \frac{1}{q!} \sum\limits_{\sigma \in S_q} \operatorname{sign}(\sigma) f_\sigma(T) = \frac{1}{q!} \sum\limits_{\sigma \in S_q} \operatorname{sign}^2(\sigma) T = T$

Показали включение в обе стороны, значит, $\operatorname{Im} A = \Lambda^q(V)$. □

Утверждение 4.10.
Пусть $e_1, \ldots, e_n$ — базис V.

Тогда $e_{i_1} \wedge \ldots \wedge e_{i_q} := A(e_{i_1} \otimes \ldots \otimes e_{i_q})$ порождают $\Lambda^q(V)$.

Доказательство.
Следует из того, что $e_{i_1} \wedge \ldots \wedge e_{i_q}$ — образы базисных элементов. □

Утверждение 4.11.
$e_{i_1} \wedge \ldots \wedge e_{i_q} = 0$, если $i_l = i_s$ для некоторых $i_l = i_s$.

Доказательство.
Нужно лишь заметить, что $f_\sigma(e_{i_1} \wedge \ldots \wedge e_{i_q}) = \operatorname{sign}(\sigma)(e_{i_1} \wedge \ldots \wedge e_{i_q})$. А значит, при транспозиции значение не изменяется только тогда, когда $e_{i_1} \wedge \ldots \wedge e_{i_q} = 0$. □

Утверждение 4.12.

1. $q \leqslant n \implies e_{i_1} \wedge \ldots \wedge e_{i_q}$ — базис $\Lambda^q(V)$, $1 \leqslant i_1 < \ldots < i_q \leqslant n$
2. $q > n \implies \Lambda^q(V) = 0$
3. $\dim \Lambda^q(V) = \binom{n}{q}$

Доказательство.

1. Заметим, что если $i_l > i_s$ при $l < s$, то можем поменять эти два элемента в тензоре местами.

   Уже знаем, что система образующих.

   Покажем, что тензоры $e_{i_1} \wedge \ldots \wedge e_{i_q}$ — линейно независимы.

   Пусть $\sum\limits_{i_1<\ldots<i_q} a_{i_1,\ldots,i_q} e_{i_1} \wedge \ldots \wedge e_{i_q} = 0$.

   Но тогда $A(a_{i_1,\ldots,i_q} e_{i_1} \otimes \ldots \otimes e_{i_q}) = 0$, а это возможно только если $a_{i_1,\ldots,i_q} = 0$ (аналогично утверждению про симметричные тензоры).

2. Следует из того, что $e_{i_1} \wedge \ldots \wedge e_{i_q} = 0$, если $i_l = i_s$ при некоторых l, s.

3. Следует из первого пункта, равно количеству способов выбрать q элементов из n.

□

Следствие.

$\dim \bigoplus\limits_{q=0}^{n} \Lambda^q(V) = 2^n$

Доказательство.

Следует из 3 пункта предыдущего утверждения. □

***Определение* 4.15.**

$T_1 \wedge T_2 := A(T_1 \otimes T_2)$ — внешнее произведение, где $T_1 \in \Lambda^p(V)$, $T_2 \in \Lambda^q(V)$.

***Определение* 4.16.**

При определенном внешнем произведении для элементов

$\Lambda(V) = \bigoplus_{q=0}^{n} \Lambda^q(V)$ — внешняя алгебра пространства V.

Утверждение 4.13.

$\Lambda(V)$ — косокоммутативная (т.е. $T_1 \wedge T_2 = (-1)^{pq} T_2 \wedge T_1$) ассоциативная алгебра над K.

Доказательство.

Покажем ассоциативность.

Покажем, что для всяких тензоров $T_1 \in T_0^p(V)$, $T_2 \in T_0^q(V)$:

$A(A(T_1) \otimes T_2) = A(T_1 \otimes A(T_2)) = A(T_1 \otimes T_2)$

Действительно:

$$A(T_1) \otimes T_2 = \left(\tfrac{1}{p!} \sum_{\sigma \in S_p} \operatorname{sign}(\sigma) f_\sigma(T_1) \right) \otimes T_2 = \tfrac{1}{p!} \sum_{\sigma \in S_p} \operatorname{sign}(\sigma)\ f_\sigma(T_1) \otimes T_2$$

$$A(A(T_1) \otimes T_2) = A\left(\tfrac{1}{p!} \sum_{\sigma \in S_p} \operatorname{sign}(\sigma)\ f_\sigma(T_1) \otimes T_2 \right) = \tfrac{1}{p!} \sum_{\sigma \in S_p} \operatorname{sign}(\sigma) A(f_\sigma(T_1) \otimes T_2)) =$$

$$= \tfrac{1}{p!} \sum_{\sigma \in S_p} \operatorname{sign}(\sigma)^2 A(T_1 \otimes T_2) = A(T_1 \otimes T_2)$$

Аналогично для $A(T_1 \otimes A(T_2))$.

Отсюда следует ассоциативность:

$(T_1 \wedge T_2) \wedge T_3 = A(A(T_1 \otimes T_2) \otimes T_3) = A(T_1 \otimes T_2 \otimes T_3) = A(T_1 \otimes A(T_2 \otimes T_3)) = T_1 \wedge (T_2 \wedge T_3)$

Теперь покажем косокоммутативность:

Пусть $T_1 = V_1 \otimes \ldots \otimes V_p$, $T_2 = W_1 \otimes \ldots \otimes W_q$.

Тогда $T_1 \wedge T_2 = A(T_1 \otimes T_2) = (-1)^{pq} A(T_2 \otimes T_1) = (-1)^{pq} T_2 \wedge T_1$. □

из доказанного ранее

5. Чистилище (или кватернионы)

5.1. Вещественная структура

***Определение* 5.1.**

Пусть V — векторное пространство над $\mathbb{C}$.

Оператор $\sigma : V \to V$ называется комплексно антилинейным если $\sigma(zv) = \overline{z}\sigma(v) \ \ \forall z \in \mathbb{C}$

Утверждение 5.1.

Пусть $\sigma : V_{\mathbb{R}} \to V_{\mathbb{R}}$ — комплексно антилинейный оператор, такой что $\sigma^2 = \mathrm{id}$.

Тогда $V = \mathbb{C} \otimes_{\mathbb{R}} W$, где $W = \mathrm{Ker}(\sigma - id)$.

Доказательство.

$V_{\mathbb{R}} = \mathrm{Ker}(\sigma^2 - \mathrm{id}) = \mathrm{Ker}(\sigma - \mathrm{id}) \oplus \mathrm{Ker}(\sigma + \mathrm{id})$ ($(\sigma^2 - \mathrm{id})$ — нулевой оператор)

Заметим, что умножение на i — изоморфизм пространств $\mathrm{Ker}(\sigma - \mathrm{id})$ и $\mathrm{Ker}(\sigma + \mathrm{id})$.

Действительно, проверим, что $a \in \mathrm{Ker}(\sigma - \mathrm{id}) \iff ia \in \mathrm{Ker}(\sigma + \mathrm{id})$.

$0 = (\sigma + \mathrm{id})(ia) = \sigma(ia) + ia = -i\sigma(a) + ia = -i(\sigma - \mathrm{id})(a) = 0$.

Положим тогда $W := \mathrm{Ker}(\sigma - \mathrm{id}) \implies V_{\mathbb{R}} = W \oplus iW$.

Хотим показать изоморфизм между $W \oplus iW$ и $W^{\mathbb{C}}$.

Он очевиден, т.к. в обеих частях элементы имеют вид (a, b) с покоординатным сложением.

Осталось проверить умножение на константу из $\mathbb{C}$:

$\forall v, w \in W : (a + ib)(v + iw) = av - bw + i(bv + aw)$, что и требовалось.

А значит, $V = \mathbb{C} \otimes_{\mathbb{R}} W$ □

5.2. Тело кватернионов

Замечание.

Большая часть утверждений доказывается элементарно и непосредственно, а потому их доказательства опущены.

***Определение* 5.2.**

Рассмотрим четырёхмерное пространство $V = \mathbb{C}^{2\times 2}$.

И рассмотрим комплексно антилинейный оператор σ на таком пространстве:

$\sigma : \mathbb{C}^{2\times 2} \to \mathbb{C}^{2\times 2}, A \mapsto \overline{\mathrm{Adj}(A)}^T$

То есть, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{d} & -\overline{c} \\ -\overline{b} & \overline{a} \end{pmatrix}$

Утверждение 5.2.

1. $\sigma(AB) = \sigma(A)\sigma(B) \ \ \forall A, B \in \mathbb{C}^{2\times 2}$
2. $\sigma(zA) = \overline{z}\sigma(A) \ \ \forall z \in \mathbb{C}$
3. $\sigma^2 = id$

Доказательство.
В случае матриц 2×2 делается элементарно по определению. □

Утверждение 5.3.
$V_{\mathbb{R}} = \operatorname{Ker}(\sigma - \mathrm{id}) \oplus \operatorname{Ker}(\sigma + \mathrm{id})$

$$\operatorname{Ker}(\sigma - \mathrm{id}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{array}{c} a = \overline{d} \\ b = -\overline{c} \end{array} \right\} = \left\{ \begin{pmatrix} x + iy & z + it \\ -z + it & x - iy \end{pmatrix} \;\middle|\; x, y, z, t \in \mathbb{R} \right\}$$

Тогда базис этого пространства представим следующим образом:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

***Определение* 5.3.**
Определим $\mathbb{H} = \operatorname{Ker}(\sigma - id)$ как тело кватернионов.

Замечание.
$\forall h \in \mathbb{H} : h = a + bi + cj + dk,\ a, b, c, d \in \mathbb{R}$.

Свойства.

1. $i^2 = j^2 = k^2 = ijk = -1$
2. $ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j$

Утверждение 5.4.

1. $\mathbb{R} \hookrightarrow \mathbb{H}$
   $a \mapsto a = a + 0i + 0j + 0k$
2. $\mathbb{I} = \{xi + yj + zk \,|\, x, y, z \in \mathbb{R}\}$ — подпространство чисто мнимых кватернионов.
   $\mathbb{I} = \{A \in \mathbb{C}^{2\times 2} \,|\, \overline{A}^T = -A,\ \operatorname{tr} A = 0\}$

***Определение* 5.4.**
$\overline{a + bi + cj + dk} = a - bi - cj - dk$ — сопряжение.
$\operatorname{Re}(a + ib + jc + kd) = a$
$\operatorname{Im}(a + ib + jc + kd) = ib + jc + kd$

***Определение* 5.5.**
Можно ввести скалярное произведение $\langle u, v \rangle = \operatorname{Re}(u \cdot \overline{v})$.
И норму: $\|u\|^2 = \operatorname{Re}(u \cdot \overline{u})$.

Лемма.

1. $\forall\, 0 \neq u \in \mathbb{H}$ существует обратный элемент $u^{-1} = \frac{\overline{u}}{\|u\|^2}$
2. Если $u, v \in \mathbb{I}$, то $\operatorname{Im}(uv) = u \times v$. Здесь $\times$ — векторное произведение.

Доказательство.

1. $u \cdot \overline{u} = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \cdot \begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix} = \begin{pmatrix} \|a\|^2 + \|b\|^2 & 0 \\ 0 & \|a\|^2 + \|b\|^2 \end{pmatrix} = \|u\|^2 \cdot 1 \implies u^{-1} = \frac{\overline{u}}{\|u\|^2}$
   Аналогично проверяется, что $\overline{u} \cdot u = \|u\|^2 \cdot 1$.

2. Знаем, что векторное произведение $\overrightarrow{a} = (a_x, a_y, a_z)$ и $\overrightarrow{b} = (b_x, b_y, b_z)$ имеет вид

$$\overrightarrow{a} \times \overrightarrow{b} = (a_y b_z - a_z b_y, a_z b_x - a_x b_z, a_x b_y - a_y b_x)$$

Пусть $u = b_1 i + c_1 j + d_1 k \in \mathbb{I}, v = b_2 i + c_2 j + d_2 k \in I$. Тогда:

$$\mathrm{Im}(uv) = \mathrm{Im}(-b_1 b_2 + b_1 c_2 k - b_1 d_2 j - c_1 b_2 k - c_1 c_2 + c_1 d_2 i + d_1 b_2 j - d_1 c_2 i - d_1 d_2) =$$
$$= (c_1 d_2 - d_1 c_2) i + (d_1 b_2 - b_1 d_2) j + (b_1 c_2 - c_1 b_2) k$$

□

6. Рай (или теория Галуа)

6.1. Расширения полей

***Определение* 6.1.**
Пусть L, K — поля.

Поле L называется расширением поля K, если $K \subseteq L$.

Обозначение.
Обозначается L/K или $K \subseteq L$.

Замечание.
Если L — расширение K, то L является векторным пространством над K.

***Определение* 6.2.**
Степенью расширения L/K назовем размерность L как векторного пространства над K.

Обозначается $[L : K]$

***Определение* 6.3.**
Пусть поле L — расширение поля K.

Элемент $\alpha \in L$ называется алгебраическим над K, если существует ненулевой многочлен $f \in K[x]$, такой что $f(\alpha) = 0$.

***Определение* 6.4.**
Любой элемент $\alpha \in L$ не являющийся алгебраическим над полем K называется трансцендентным над полем K.

***Определение* 6.5.**
Расширение L/K называется алгебраическим, если все элементы L алгебраические над K.

Пример.
1) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ — алгебраическое расширение.

2) $\mathbb{Q}(x)/\mathbb{Q}$ — не алгебраическое расширение.

Лемма.

1. Любое конечное расширение является алгебраическим.
2. Если $M \subseteq K \subseteq L$, тогда $[L : M] = [L : K] \cdot [K : M]$.

Доказательство.

1. Пусть наше расширение это L/K. Обозначим размерность расширения: $[L : K] = n$.

   Рассмотрим $\alpha \in L$ и докажем, что α алгебраическое.

   Заметим, что элементы $1, \alpha, \alpha^2, \ldots, \alpha^n$ — линейно зависимы над K (т.к. $[L : K] = n$), а значит существуют $a_0, a_1, \ldots, a_n \in K$, такие что $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$.

   Тогда для $f = a_0 + a_1x + \cdots + a_nx^n$ получаем, что $f(\alpha) = 0$, что и требовалось.

2. Пусть $[K : M] = n$, а $[L : K] = m$.

   Пусть $u_1, \dots u_n$ — базис K над M, а $v_1, \dots v_m$ — базис L над K,

   Тогда докажем, что $u_i v_j$ — образуют базис L над M.

   Покажем, что система образующих.

   Пусть $\alpha \in L$. Тогда, из того, что v_i образуют базис L над K: $\alpha = \sum\limits_{j=1}^{m} \delta_j v_j$, где $\delta_j \in K$.

   Каждое $\delta_j \in K$, а значит, из того, что u_i образуют базис K над M следует, что существует линейное представление δ_j: $\delta_j = \sum\limits_{i=1}^{n} \gamma_{ij} u_i$, где $\gamma_{ij} \in M$

   Получили, что $\alpha = \sum\limits_{j=1}^{m} \sum\limits_{i=1}^{n} \gamma_{ij} u_i v_j$, что и требовалось.

   Покажем линейную независимость.

   Рассмотрим линейное представление нуля $\sum\limits_{i,j} \gamma_{ij} u_i v_j$.

   Тогда $\sum\limits_{i,j} \gamma_{ij} u_i v_j = \sum\limits_{j} \left(\sum\limits_{i} \gamma_{ij} u_i \right) v_j = 0$.

   Получили линейное представление 0 из векторов v_j, а значит, т.к. v_j образуют базис, то все коэффициенты равны 0.

   Т.е. все $\sum\limits_{i} \gamma_{ij} u_i = 0$, а значит, т.к. u_i линейно независимы, то и все $\gamma_{ij} = 0$.

   Значит, изначальное представление нуля было тривиальным. Что и требовалось.

□

Замечание.

При доказательстве второго утверждения мы пользовались конечностью расширений, тем не менее, утверждение все еще остается верным, а именно, если одно из расширений $M \subseteq K$ и $K \subseteq L$ бесконечно, то и расширение $M \subseteq L$ бесконечно.

Следствие.

Если $M \subseteq K \subseteq L$ — конечные расширения, то $[K : M] \mid [L : M]$ и $[L : K] \mid [L : M]$.

***Определение* 6.6.**

Пусть L расширение K, а $\alpha \in L$ — алгебраический.

Рассмотрим множество I_α всех многочленов $p(x) \in K[x]$, таких, что $p(\alpha) = 0$.

Тогда $f(x)$ со старшим коэффициентом равным одному, такой что $I_\alpha = f(x)K[x]$ называется минимальным многочленом элемента α.

Обозначается f_α.

Утверждение 6.1.

Минимальный многочлен существует для любого алгебраического элемента α.

Доказательство.

Выбранное множество I_α является идеалом кольца $K[x]$. При этом, т.к. $K[x]$ — кольцо главных идеалов, то любой идеал в нем имеет вид $I = g(x)K[x]$, в частности, для идеала I_α существует многочлен f его образующий.

Старший коэффициент равный одному достигается посредством домножения на константу поля K. □

Замечание.

Из того, что α алгебраический, следует, что идеал не пуст (иначе старший коэффициент равный одному недостижим).

Свойства.

1. Минимальный многочлен f_α неприводим.
2. Идеал I_α является максимальным идеалом.

Доказательство.

Докажем, что идеал I_α — простой.

Пусть $f(x) = g(x)h(x) \in I_\alpha$. Тогда $f(\alpha) = 0$, а значит, либо $g(\alpha) = 0$, либо $h(\alpha) = 0$, что и требовалось.

1. Если f_α приводим, т.е. $f_\alpha(x) = g(x)h(x)$, то либо $g(x) = 0$, либо $h(x) = 0$, а тогда f_α не мог образовывать весь идеал.
2. Теперь вспомним, находимся в кольце главных идеалов, а значит любой простой идеал максимален. В частности, I_α окажется максимальным.

□

Обозначение.

Пусть $K \subseteq L$, $\alpha \in L$.

Обозначим $K(\alpha)$ как поле, являющиеся пересечением всех таких полей M, что $K \subseteq M \subseteq L$ и $\alpha \in M$.

Замечание.

Определение корректно, т.к. в пересечении участвует хотя бы один элемент (а именно L).

Замечание.

$K(\alpha)$ является расширеним поля K и в различной литературе называется простым расширением (у нас такого определения не было).

Обозначение.

Пусть L — расширение поля K, α — элемент поля L.

Тогда как $K[\alpha]$ обозначим множество значений всех многочленов с коэффициентами из K в точке α.

Замечание.

Множество $K[\alpha]$ является кольцом.

Замечание.

$K[\alpha] \subseteq K(\alpha)$, т.к. любое поле, содержащие α, содержит и значения всех многочленов в этой точке.

Утверждение 6.2.

Пусть $K \subseteq L$, $\alpha \in L$. Тогда:

1. Если α — алгебраическое, то $K(\alpha) = K[\alpha] \cong K[x]/(f_\alpha)$.
2. Если α — трансцендентное, то $K(\alpha) \cong K(x) = \operatorname{Quot} K[x]$.

Доказательство.

Рассмотрим гомоморфизм колец

$$\theta : K[x] \to K[\alpha]$$
$$g(x) \mapsto g(\alpha)$$

Из определения $\operatorname{Ker}\theta = I_\alpha$, а $\operatorname{Im}\theta = K[\alpha]$, а тогда по теореме о гомоморфизме $K[\alpha] \cong K[x]/I_\alpha$.

Рассмотрим два случая.

1. Если тогда α — алгебраический, то $I_\alpha \neq 0$ и существует минимальный многочлен.

   I_α максимальный, а значит $K[\alpha] \cong K[x]/I_\alpha$ — поле.

   А тогда $K(\alpha) \subseteq K[\alpha]$ из определения $K(\alpha)$.

   При этом включение в другую сторону уже известно, а значит $K(\alpha) = K[\alpha]$.

2. Если α — трансцендентный, то $I_\alpha = 0$, а тогда θ — изоморфизм.

   Значит, $K[x]$ и $K[\alpha]$ изоморфны, а тогда изоморфны и их поля частных $\operatorname{Quot} K[x] \cong \operatorname{Quot} K[\alpha]$.

   Осталось показать, что $\operatorname{Quot} K[\alpha] = K(\alpha)$.

   $\operatorname{Quot} K[\alpha] \subseteq K(\alpha)$ (т.к. $K(\alpha)$ содержит α), и $K(\alpha) \subseteq \operatorname{Quot} K[\alpha]$ (т.к. $\operatorname{Quot} K[\alpha]$ является полем содержащим α), а значит, они равны.

□

***Определение* 6.7.**

Два расширения $K \subseteq M$ и $K \subseteq L$ называются эквивалентными, если существует изоморфизм $\sigma : M \to L$ такой, что σ тождественен на K.

Утверждение 6.3.

Если K — поле, $f(x) \in K[x]$ — неприводим, тогда существует и единственное с точностью до эквивалентности расширение вида $K(\alpha)$ такое, что $f(\alpha) = 0$.

Доказательство.

Если f — линейный, то f имеет единственный корень, а значит нас интересует лишь расширение этим корнем, которое совпадает с K (так как корень уже лежит в поле K).

Если же f не линейный.

Рассмотрим идеал $I = f(x)K[x]$.

Тогда I — максимальный идеал в $K[x]$ (т.к. простой, а мы в кольце главных идеалов), а значит кольцо $M = K[x]/I$ — поле.

Рассмотрим вложение

$$K \hookrightarrow M$$
$$a \mapsto a + (f)$$

Значит M является расширением K.

Возьмем в качестве α класс эквивалентности многочлена x. Проверим, что $f(\overline{x}) = 0$. Действительно, $f(\overline{x}) = \overline{f(x)} = 0$.

Единственность следует из того, что элемент α в выбранном поле будет алгебраическим, а значит расширение $K(\alpha)$ будет изоморфно $K[x]/(f)$, т.к. f как раз будет минимальным многочленом (f неприводим). □

Замечание.

Базисом полученного расширения будет множество $1, \overline{x}, \ldots, \overline{x^{\deg f - 1}}$, соответственно расширение конечно его размерность равна $\deg f$.

Обозначение.

Пусть $K \subseteq L$, $\alpha_1, \ldots, \alpha_n \in L$.

Введем $K(\alpha_1, \ldots, \alpha_n)$ как минимальное поле, содержащие K и все элементы $\alpha_1, \ldots, \alpha_n$.

Более формально можно ввести аналогично определению $K(\alpha)$.

А именно $K(\alpha_1, \ldots, \alpha_n)$ это пересечение всех полей M, таких что $K \subseteq M \subseteq L$ и $\alpha_1, \ldots, \alpha_n \in M$.

Замечание.

Поле $K(\alpha_1, \ldots, \alpha_n)$ — поле, полученное присоединением элементов $\alpha_1, \ldots, \alpha_n$ к полю K.

Утверждение 6.4.

1. Поле $K(\alpha_1, \ldots, \alpha_n)$ единственно с точностью до эквивалентности.
2. $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1)(\alpha_2)\ldots(\alpha_n)$

   Вроде бы, второго утверждения явно не было, но тем не менее мы им неявно пользовались.

Доказательство.

1. Без доказательства. (Кажется, что это следует из второго пункта)
2. Индукция по n. База для $n = 1$ очевидна.

   Переход $n \to n + 1$.

   Покажем, что $K(\alpha, \ldots, \alpha_n, \alpha_{n+1}) = K(\alpha_1, \ldots, \alpha_n)(\alpha_{n+1})$.

   Последние равенство очевидно из определений $K(\alpha)$ и $K(\alpha_1, \ldots, \alpha_n)$, а точнее очевидны оба включения.

   Осталось применить предположение индукции и получить требуемое.

□

Следствие.

Не имеет значение в каком порядке присоединять элементы к полю (изначальное определение $K(\alpha_1, \ldots, \alpha_n)$ от этого не зависит).

Лемма.

1. Конечные расширения и только они получаются присоединением конечного числа алгебраических элементов.
2. Пусть α, β — алгебраические элементы над полем K.

   Тогда $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ — алгебраические над K.
3. Если $M \subseteq K \subseteq L$ — алгебраические расширения, то и $M \subseteq L$ — алгебраическое расширение.

Доказательство.

1. Рассмотрим расширение $K(\alpha_1, \ldots, \alpha_n)$.

   Оно равно $K(\alpha_1)\ldots(\alpha_n)$. Каждое из n расширений в цепочке конечно (как уже знаем, если α — алгебраическое, то $K(\alpha) \cong K[x]/(f_\alpha) \implies [K(\alpha) : K] \leqslant \deg f_\alpha < +\infty$), а значит и результирующее расширение конечно.

   В другую сторону. Пусть расширение $K \subseteq L$ конечно.

   Индукция по степени расширения. Если она равна 1, то поля уже совпадают. Иначе, существует $\alpha \in L$ не лежащие в K.

   Т.к. расширение $K \subseteq L$ конечное, то α — алгебраический, а значит мы можем рассмотреть поле $K(\alpha)$.

   При этом $K(\alpha) \neq K \implies [K(\alpha) : K] > 1$, а значит $[L : K(\alpha)] < [L : K]$.

   Тогда по предположению индукции расширение $L/K(\alpha)$ получается присоединением конечного числа алгебраических элементов, а тогда и для изначального расширения это верно. Что и требовалось.

2. α и β алгебраические, а значит оба промежуточных расширения $K \subseteq K(\alpha) \subseteq K(\alpha, \beta)$ конечны, а тогда и результирующее расширение конечно.

   При этом, $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in K(\alpha, \beta)$, а значит из конечности расширения они являются алгебраическими.

3. Рассмотри $\alpha \in L$ и покажем, что α — алгебраический над M.

   α — алгебраический над $K \implies a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$, $a_i \in K$

   Рассмотрим следующую башню расширений:

   $M \subseteq M(a_0, \ldots, a_n) \subseteq M(a_0, \ldots, a_n, \alpha) \subseteq L$

   a_i — алгебраические над $M \implies [M(a_0, \ldots, a_n) : M] < \infty$

   А значит, $M \subseteq M(a_0, \ldots, a_n)$ — конечное.

   $M(a_0, \ldots, a_n) \subseteq M(a_0, \ldots, a_n, \alpha)$ — конечное, т.к. α алгебраический над $M(a_0, \ldots, a_n)$.

   Тогда и $[M(a_0, \ldots, a_n, \alpha) : M]$ — конечное, а значит α — алгебраический элемент над M.

□

Замечание.

Важно заметить, что для третьего пункта не важна конечность расширений.

***Определение* 6.8.**

Поле, полученное присоединением всех корней многочлена f, называется полем разложения многочлена f.

***Определение* 6.9.**

Поле K называется алгебраически замкнутым, если любой многочлен над полем K имеет корень.

Теорема 6.5.

Для всякого поля K существует алгебраическое расширение $K \subseteq \overline{K}$, такое что $\overline{K}$ — алгебраически замкнуто.

Доказательство.

Шаг первый: построим расширение L_1, $K \subseteq L_1$, в котором любой неконстантый многочлен $f(x) \in K[x]$ имеет корень в L_1.

Введем бесконечный набор переменных x_f, где $f \in K[x]$ (т.е. каждому многочлену над K сопоставили переменную).

Рассмотрим кольцо многочленов от нашего набора переменных: $R = K[x_f]$.

Теперь введем идеал I, порожденный многочленами вида $f(x_f)$ (т.е. в каждый многочлен подставили свою переменную).

Докажем, что $I \neq R$

Пусть равенство есть, тогда, в частности, $1 \in I$.

Значит она имеет представление: $q_1 f_1(x_{f_1}) + q_2 f_2(x_{f_2}) + \ldots + q_n f_n(x_{f_n}) = 1,\ q_i \in R$.

Рассмотрим расширение $K \subseteq F$, полученное присоединением всех корней многочленов $f_1, \ldots, f_n$.

Расширение будет конечным, т.к. оно получено добавлением конечного числа алгебраических элементов.

Над полем F сохранилось равенство $q_1 f_1(x_{f_1}) + q_2 f_2(x_{f_2}) + \ldots + q_n f_n(x_{f_n}) = 1$ как равенство многочленов, а значит для оно останется выполнено после любой подстановки.

Подставим в качестве каждого x_{f_i} корень f_i.

Получим равенство $0 = 1$. Противоречие, значит $I \neq R$.

Перейдем к построению L_1.

Рассмотрим максимальный идеал M, содержащий I. Известно, что $M \neq R$.

Положим $L_1 = R/M$ — поле.

Хотим показать, что существует вложение $\sigma : K \hookrightarrow L_1$.

Очевидным образом существует $\theta : K \hookrightarrow R$.

Кроме того, существует проекция $\pi : R \to L_1$, т.ч. $a \mapsto \overline{a}$.

Значит, надо показать, что композиция этих двух отображений не переводит никакие два элемента из K в один и тот же класс эквивалентности.

Пусть это не так. Тогда $\exists\, a, b \in K : a - b \in M \implies a - b = f$ для некоторого $f \in M$.

Но т.к. $M \neq R$, то $\deg f \geqslant 1$, поскольку иначе в M лежала бы единица. Противоречие.

Осталось проверить, что любой неконстантный многочлен над K имеет корень в L_1.

Рассмотрим $f \in K[x]$. т.ч. $\deg f > 1$.

Заметим, что $f(\overline{x_f}) = \overline{f(x_f)} = 0$, а значит у f есть корень $\overline{x_f}$ в L_1, что и требовалось.

Похожее рассуждение уже проводилось ранее.

Шаг второй: Построим алгебраически замкнутое расширение K.

Рассмотрим цепочку расширений, описанным выше образом: $K \subseteq L_1 \subseteq L_2 \subseteq L_3 \subseteq \ldots$

Выберем $L = \bigcup_{i=1}^{\infty} L_i$ — поле, т.к. для любых двух элементов из L существует их общее подполе L_n.

При этом L — алгебраически замкнутое, т.к. $\forall f \in L[x]\ \ \exists n : f \in L_n[x]$, а тогда в $L_{n+1}[x]$ будет нужный нам корень.

Шаг третий: Построим требуемое расширение $\overline{K}$.

Определим $\overline{K}$ как объединение всех таких полей M, что $K \subseteq M \subseteq L$ и расширение $K \subseteq M$ — алгебраическое.

Очевидно, что это объединение не пусто, т.к. K в нем лежит.

Полученное расширение $K \subseteq \overline{K}$ является алгебраическим (т.к. каждый элемент алгебраический).

Осталось показать, что $\overline{K}$ алгебраически замкнуто.

Рассмотрим $f \in \overline{K}[x]$. Он имеет корень в L (т.к. L алгебраически замкнуто). Назовем этот корень α.

Тогда α — алгебраический над $\overline{K}$, а значит, $\overline{K}(\alpha)$ лежит в нашем объединении (т.к. расширение алгебраическое над K). Но тогда $\overline{K} \supseteq \overline{K}(\alpha)$, а значит $\overline{K} \ni \alpha$, что и требовалось. □

***Определение* 6.10.**
Пусть K — поле.

Алгебраическое расширение $\overline{K} \supseteq K$, такое что $\overline{K}$ — алгебраически замкнуто, называется алгебраическим замыканием поля K.

6.2. Продолжение гомоморфизмов

Обозначение.
$\sigma : K \to L$ — гомоморфизм полей
$f(x) = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$
$f^\sigma(x) = \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_n)x^n \in L[x]$

Лемма.
Если $f(\alpha) = 0$, то $f^\sigma(\sigma(\alpha)) = 0$

Доказательство.
Т.к. $f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$
$f^\sigma(\sigma(\alpha)) = \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \ldots + \sigma(a_n)\sigma(\alpha)^n = \sigma(f(\alpha)) = 0$ □

***Определение* 6.11.**
Пусть $K \subseteq L$, $K' \subseteq L'$ — расширения, а $\varphi : K \to K'$ – гомоморфизм полей.

Тогда продолжением гомоморфизма φ называется гомоморфизм $\varphi' : L \to L'$, т.ч. $\varphi'\Big|_K = \varphi$.

Утверждение 6.6.
$K \subseteq L,\ K' \subseteq L'$ — расширения полей.
$f \in K[x],\ \ f$ — неприводим.
$\varphi : K \to K'$ — изоморфизм
$\alpha \in L,\ f(\alpha) = 0$
$\alpha' \in L',\ f^\varphi(\alpha') = 0$

1. Тогда φ продолжается до изоморфизма $\varphi' : K'(\alpha) \to K(\alpha')$, причём $\varphi'(\alpha) = \alpha'$.
2. Тогда φ продолжается до изоморфизма полей разложения многочленов f и f^φ.

Доказательство.

1. Построим изоморфизм $K(\alpha) \to K'(\alpha')$ явно.

   Любой элемент $K(\alpha)$ имеет вид: $\sum\limits_{i=0}^{\deg f - 1} a_i \alpha^i$, т.к. поле изоморфно $K[x]/(f)$.

   Тогда переведем $\sum\limits_{i=0}^{\deg f - 1} a_i \alpha^i \mapsto \sum\limits_{i=0}^{\deg f - 1} \varphi(a_i) \alpha'^i$

Очевидно, что на поле K (т.е. константах в факторе кольца многочленов) φ' совпадает с φ, т.е. φ' действительно продолжение φ.

2. Будем продолжать последовательно. Рассмотрим корень $f - \alpha$. Тогда $\varphi(\alpha)$ — корень f^φ.

   Сделаем расширение $K(\alpha)$. Поля $K(\alpha)$ и $K'(\varphi(\alpha))$ будут изоморфны (см. первый пункт), а значит, многочлены f и f^φ в них раскладываются одинаково. Сопоставим их множители разложения друг-другу и продолжим процесс.

   Т.к. мы получаем изоморфизм полей на каждом шаге, то многочлены разложатся на линейные множители одновременно.

□

Замечание.

Полученное в первом случае отображение единственно, т.к. если определено $\varphi(\alpha)$, то определены и все элементы поля $K(\alpha)$.

Обозначение.

Пусть L — расширение K.

Группу автоморфизмов L, тождественных на K обозначим $\mathrm{Aut}_K L$.

***Определение* 6.12.**

Пусть $\overline{K}$ — алгебраическое замыкание K.

Элементы $\alpha, \beta \in \overline{K}$ называются сопряженными, если $\alpha = \sigma\beta$ для какой-то $\sigma \in \mathrm{Aut}_K \overline{K}$.

Свойства.

1) Если α и β сопряжены, то $f(\alpha) = 0 \iff f(\beta) = 0$.

2) Любые два корня неприводимого многочлена сопряжены.

Доказательство.

1) Пусть α и β сопряжены, т.е. $\alpha = \sigma\beta$. И пусть β является корнем какого-то многочлена f.

Тогда $f(\alpha) = f^\sigma(\alpha) = f^\sigma(\sigma\beta) = 0$, что и требовалось.

Первый переход следует из того, что σ — автоморфизм, который тождественно действует на K. Последний переход следует из первой леммы.

2) Пусть наш многочлен f, а α и β два его корня. Из доказанного утверждения следует, что существует продолжение тождественного автоморфизма, такое что $\alpha = \sigma\beta$, значит, они сопряжены. □

Следствие.

Множество сопряженных с α элементов совпадает с множеством корней f_α.

***Определение* 6.13.**

Алгебраическое расширение $K \subseteq L$ называется нормальным, если всякий неприводимый многочлен над K, имеющий корень в L раскладывается в L на линейные множители.

6.3. Кратные корни

Замечание.

Пусть f — многочлен над полем K. Рассматриваем корни f в алгебраическом замыкании $\overline{K}$. Тогда:

1. f имеет кратные корни $\iff$ f и f' имеют общий корень.

   Вторая часть — то же, что и $\Big(f, f'\Big) = f(x)K[x] + f'(x)K[x] \neq K[x]$.

2. f — неприводим, $\deg f > 1$, то f имеет кратные корни тогда и только тогда, когда $f' = 0$.

Лемма.

f — неприводим, $\deg f > 1$. Тогда

1. Если $\operatorname{Char} K = 0$, то f — не имеет кратных корней.
2. Если $\operatorname{Char} K = p > 0$, то f имеет кратные корни тогда и только тогда, когда $f(x) = g(x^p)$, $g \in K[x]$.

Доказательство.

1. Если f имеет кратные корни, то $f' = 0$, но если характеристика поля равна нулю, то из этого следует, что f был константой. Противоречие.
2. “$\Longleftarrow$”

   $f(x) = g(x^p) \implies f'(x) = g'(x^p) \cdot 0 = 0$

   “$\Longrightarrow$”

   $f(x) = a_0 + a_1 x + \ldots + a_n x^n$

   $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1} = 0$

   $k a_k = 0 \implies a_k = 0$ или $k \vdots p \implies f(x) = g(x^p)$, что и требовалось.

□

***Определение* 6.14.**

Пусть $\operatorname{Char} K = p > 0$.

$f(x) = g(x^{p^e})$ и g не имеет кратных корней.

Тогда назовём $\deg g$ редуцированной степенью f.

Утверждение 6.7.

$K \subseteq L$ — расширение полей, $\alpha \in L$

$f = f_\alpha$ раскладывается на линейные множители в поле L. s $\sigma : K \hookrightarrow L$ — вложение.

Тогда существует ровно m продолжений σ до вложения $\tilde{\sigma} : K(\alpha) \hookrightarrow L$, где m совпадает с редуцированной степенью f, если $\operatorname{Char} K = p > 0$ или со степенью f, если $\operatorname{Char} K = 0$.

Доказательство.

Каждое продолжение гомоморфизма $\tilde{\sigma}$ переводит α в сопряжённый с ним элемент $\tilde{\sigma}(\alpha)$, чем полностью и определяется, а значит, количество продолжений $\tilde{\sigma}$ совпадает с количеством различных корней f.

Таким образом, если $\operatorname{Char} K = 0$, то у f нет кратных корней, а значит $m = \deg f$.

Если же $\operatorname{Char} K = p > 0$, то пусть $f(x) = g(x^{p^e})$ где $g \in K[x]$ и не имеет кратных корней.

f – неприводим в $K[x] \implies g$ неприводим в $K[x]$

В $L[t]$ многочлен g представим как $g(t) = \prod\limits_{i=1}^{m}(t - \beta_i)$, где все β_i — различны.

А тогда $f(x) = g(x^{p^e}) = \prod\limits_{i=1}^{m}(x^{p^e} - \beta_i)$.

Пусть α_i — корень f, обнуляющий скобку с номером i, т.е. $\alpha_i^{p^e} = \beta_i$.

Заметим, что тогда $x^{p^e} - \beta_i = x^{p^e} - \alpha_i^{p^e} = (x - \alpha_i)^{p^e}$

Вспомним, что $f(x) = \prod_{i=1}^{m}(x^{p^e} - \beta_i) = \prod_{i=1}^{m}(x - \alpha_i)^{p^e} \implies f$ имеет ровно m различных корней. □

***Определение* 6.15.**

Пусть $K \subseteq L$ — конечное расширение

$\sigma : K \hookrightarrow M$ — вложение, M алгебраически замкнуто.

Количество продолжений σ до вложения $L \hookrightarrow M$ назовем сепарабельной степенью.

Обозначается $[L : K]_s$.

Замечание.

$[L : K]_s$ – не зависит от M и σ.

Было приведено без доказательства.

Утверждение 6.8.

Пусть $K \subseteq L \subseteq M$. Тогда

1. $[M : K]_s = [M : L]_s \cdot [L : K]_s$
2. $[L : K]_s \leqslant [L : K]$

Доказательство.

1. Пусть $\sigma : K \hookrightarrow N$, где N — алгебраически замкнуто.

   $\{\sigma_i\}$ — продолжения σ на $L \hookrightarrow N$, $|\{\sigma_i\}| = [L : K]_s$

   $\{\tau_{i,j}\}$ — продолжение σ_i до $M \hookrightarrow N$, $|\{\tau_{i,j}\}| = [M : L]_s$ (при фиксированном i)

   А значит, $[M : K]_s = |\{\tau_{i,j}\}_{\forall i,j}| = [M : L]_s[L : K]_s$

2. $[L : K] < \infty$

   Рассмотрим следующую цепочку расширений:

   $K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots \subset K(\alpha_1, \ldots, \alpha_n) = L$

   По уже доказанному:

   $[L : K]_s = [K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)]_s \cdot \ldots \cdot [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})]_s$

   Остаётся доказать, что $[M(\alpha) : M]_s \leqslant [M(\alpha) : M]$

   Но знаем, что:

   $[M(\alpha) : M]_s =$ редуцированная степень f_α

   $[M(\alpha) : M] = \deg f_\alpha$

   А редуцированная степень $f_\alpha \leqslant \deg f_\alpha$

   Что и требовалось.

□

Следствие.

L/K — конечное расширение. Тогда $|\mathrm{Aut}_K L| \leqslant [L : K]$

Доказательство.

В $[L : K]_s$ посчитаны все продолжения, а в $\mathrm{Aut}_K L$ лишь те, которые сохраняют K. □

6.4. Конечные поля

Утверждение 6.9.
F — конечное поле. Тогда:

1. $|F| = p^k$, где p — простое, $p = \operatorname{Char} F$
2. Если $|F| = q$, то $a^{q-1} = 1 \ \ \forall a \in F^*$

Доказательство.
Утверждения из второго семестра... □

Везде далее мы рассматриваем f как многочлен над полем $\mathbb{F}_p$.

Лемма.
Корни многочлена $f(x) = x^{p^n} - x$ в его поле разложения образуют поле.

Доказательство.
Рассмотрим поле разложения $f(x) = x^{p^n} - x$.

Проверим, что корни $x^{p^n} - x$ образуют поле.

Для этого нужно проверить, что сумма, произведение и обратные элементы все еще лежат в поле.

Если α, β — корни, то $\alpha^{p^n} = \alpha$ и $\beta^{p^n} = \beta$,

А значит, $(\alpha\beta)^{p^n} = \alpha\beta$ и $\alpha^{p^n} + \beta^{p^n} = (\alpha + \beta)^{p^n} = \alpha + \beta$

$(-\alpha)^{p^n} = -\alpha$ (в случае $\operatorname{Char} K = 2$ тоже нет проблем, т.к. там $-\alpha = \alpha$).

a^{p^n-2} — обратный элемент ($a \cdot a^{p^n-2} = a^{p^n-1} = 1$).

$\left(a^{p^n-2}\right)^{p^n} = a^{p^{2n}-2p^n} = a^{((p^n-1)^2)} \cdot a^{-1} = (a^{(p^n-1)})^{p^n-1} \cdot a^{-1} = a^{-1}$ □

Лемма.
Конечные поля одинакового порядка изоморфны.

Доказательство.
Пусть поле K содержит q элементов и его характеристика $\operatorname{Char} K = p$, тогда $q = p^n$.

Рассмотрим подполе размера p. Оно изоморфно $\mathbb{F}_p$.

Докажем, что поле разложения многочлена $f(x) = x^{p^n} - x$ (над $\mathbb{F}_p$) изоморфно полю K.

Заметим, что любой элемент поля K удовлетворяет соотношению $x^{p^n} - x$, при этом у многочлена f не более чем p^n корней, а значит множество корней f совпадает с множеством элементов поля K.

Покажем, что все элементы поля разложения f являются корнями f.

Поле разложения f имеет вид $F_p(\alpha_1, \ldots, \alpha_k)$, где α_i — различные корни.

Уже известно, что все элементы изначального поля F_p являются корнями f.

При каждом из расширений $F_p \subseteq F_p(\alpha_1) \subseteq \ldots \subseteq F_p(\alpha_1, \ldots, \alpha_k)$ к полю добавляются только корни многочлена f (это следует из вида расширения и из того, что если α и β — корни, то и $\alpha + \beta$ и $\alpha \cdot \beta$ тоже корни), а значит и в итоговом поле все элементы будут являться корнями.

Таким образом, множество элементов поля разложения f совпадает с множеством корней f, которое, в свою очередь совпадает с полем K, а значит K изоморфно полю разложения f.

Осталось заметить, что все поля разложения над одним полем изоморфны. □

Утверждение 6.10.

1. $\forall p \in \mathbb{P}$ и $\forall n \in \mathbb{N}$ $\exists$ поле из p^n элементов.
2. $\forall m$ существует одно (с точностью до эквивалентности) расширение поля $\mathbb{F}_q$ степени m.

Доказательство.

1. Рассмотрим все корни многочлена $f(x) = x^{p^n} - x$ в его поле разложения.

   Эти корни образуют поле.

   Осталось заметить, что все они различны, т.к. по доказанной ранее лемме, если у многочлена имеются кратные корни, то он имеет вид $g(x^p)$.

   Таким образом, мы получили поле размера p^n.

2. $[K : \mathbb{F}_q] = m \implies |K| = q^m$, а конечные поля одинакового порядка изоморфны.

□

6.5. Автоморфизмы поля $\mathbb{F}_q$

Предисловие.

Здесь и далее — $q = p^n$.

$\sigma \in \operatorname{Aut} \mathbb{F}_q$, $\sigma\Big|_{\mathbb{F}_p} = \mathrm{id}$, поскольку $\operatorname{Aut} \mathbb{F}_p = \{\mathrm{id}\}$.

***Определение* 6.16.**

Автоморфизм $\varphi : \mathbb{F}_q \to \mathbb{F}_q$, т.ч. $x \mapsto x^p$, называется эндоморфизмом Фробениуса.

Замечание.

Почему автоморфизм станет ясно из следующего утверждения.

Утверждение 6.11.

1. φ — автоморфизм $\mathbb{F}_q$.
2. $\operatorname{Aut} \mathbb{F}_q = \langle \varphi \rangle$ и $|\operatorname{Aut} \mathbb{F}_q| = n$.

   Т.е. $\operatorname{Aut} \mathbb{F}_q$ — циклическая.

Доказательство.

1. $\left|\operatorname{Aut}_{\mathbb{F}_p} \mathbb{F}_q\right| \leqslant [\mathbb{F}_q : \mathbb{F}_p] = n$, $|\mathbb{F}_q| < \infty$

   φ — инъективно, т.к. $\operatorname{Ker} \varphi = \{0\}$ (иначе в поле был бы нильпотентный элемент)

   При этом поля конечны, а значит, φ — автоморфизм.

2. $\operatorname{ord} \varphi \mid n$, т.к. $\varphi^n(x) = x^{p^n} = x \implies \varphi^n = \mathrm{id}$

   Пусть $\operatorname{ord} \varphi = d$.

   $\forall t \in \mathbb{F}_q : t = \varphi^d(t) = t^{p^d}$, т.е. t — корень $x^{p^d} - x$.

   Но у этого многочлена не более p^d корней, а в нашем поле p^n элементов.

   Т.е. равенство возможно только если $d \geqslant n$. Но раз он делит n, то $d = n$.

□