Алгебра, II семестр

Весна 2015, лектор: Всемирнов Максим Александрович

Авторы: Глеб Валин, Михаил Никонов, Ольга Черникова, Игорь Лабутин, Дима Розплохас, Даниил Лиференко, Саша Малышева, Егор Суворов, Дмитрий Лапшин, Саша Маркелов, Стас Беляев

Собрано: 6 сентября 2015 г. 04:52

Оглавление

Глава 1

Теория делимости в кольцах

1.1. Делимость

R — кольцо.

Def 1.1.1. a делит b слева, если

$$\exists c \in R \colon b = ac$$

a — левый делитель b.

Def 1.1.2. a делит b справа, если

$$\exists d \in R \colon b = da$$

a — правый делитель b.

Если R коммутативно, то говорят просто о делителе:

$$a \mid b \Leftrightarrow b \vdots a$$

Если R не коммутативно: $a \mid_R b$ — a делит b слева, $a \ {}_R\!\mid b$ — a делит b справа.
Свойства:

1. $a \mid b \wedge b \mid c \Rightarrow a \mid c$
2. $a \mid_R b \wedge b \mid_R c \Rightarrow a \mid_R c$
3. $a \ {}_R\!\mid b \wedge b \ {}_R\!\mid c \Rightarrow a \ {}_R\!\mid c$

   ▶

   $$b = da$$
   $$c = fb = (fd)a$$

   Для делимости слева аналогично, для двусторонней — показать обе выкладки ◀

4. Если R — кольцо с единицей, то $a \mid a$, $a \mid_R a$, $a \ {}_R\!\mid a$.

   ▶

   $$a = a \cdot 1 = 1 \cdot a$$

   ◀

Def 1.1.3.

$$ab = 0, a \neq 0, b \neq 0$$

a — левый нетривиальный делитель нуля, b — правый нетривиальный делитель нуля.

Def 1.1.4. Коммутативное кольцо с единицей — область целостности, если в нём нет делителей нуля.

$$\forall a, b \in R \colon ab = 0 \Rightarrow a = 0 \vee b = 0$$

Def 1.1.5. R — кольцо с единицей. R^* — мультипликативная группа кольца R

$$R^* = \{a \in R \mid \exists b \in R \colon ab = ba = 1\}$$

1.2. Ассоциированность

Def 1.2.1. R — кольцо с единицей. Введём $\sim$ — отношение ассоциированности:

$$a \sim b \Leftrightarrow \exists c \in R^* \colon a = bc$$

R^* — группа, док-во было в 1 семестре.

Замечание 1.2.1. Ассоциированность — отношение эквивалентности.

▶ 1.

$$a \sim a \Leftarrow a = a \cdot 1 \Leftarrow 1 \in R^*$$

2.

$$a \sim b \Rightarrow b \sim a$$
$$a = bc, c \in R^*$$
$$\exists d \colon cd = 1$$
$$ad = bcd = b \Rightarrow b \sim a$$

3.

$$a \sim b, b \sim c \Rightarrow a \sim c$$
$$\exists u \in R^* \colon a = bu$$
$$\exists v \in R^* \colon b = cv$$
$$a = c(uv) \Rightarrow a \sim c, uv \in R^* \text{ (так как } R \text{ — группа)}$$

◀

Свойства:

1. Если $a \sim b$, то $a \mid b \wedge b \mid a$.
2. Если R — область целостности и $a \mid b$ и $b \mid a$, то $a \sim b$.

▶ 1.

$$a = bc, c \in R^* \Rightarrow b \mid a$$
$$a \sim b \Rightarrow b \sim a \Rightarrow a \mid b$$

2.

$$a|b \Rightarrow \exists u \colon b = au$$
$$b|a \Rightarrow \exists v \colon a = bv$$

- $$a = 0 \Rightarrow b = 0, 0 = 0 \cdot 1 \Rightarrow a \sim b$$
- $$a \neq 0, a = auv$$
$$a(1 - uv) = 0 \xrightarrow{R \text{ — область целостности}} 1 - uv = 0$$
$$\Rightarrow u \in R^*, v \in R^* \Rightarrow a \sim b$$

◀

1.3. Идеалы в кольце

R — произвольное кольцо

Def 1.3.1. $\emptyset \neq I \subseteq R$ — левый идеал в R, если:

1. $\forall a, b \in I : a \pm b \in I$
2. $\forall a \in I, \forall r \in R : ra \in I$

Замечание 1.3.1. $I + I \subseteq I$, $RI \subseteq I$, I — подкольцо $I \cdot I \subseteq I$

Def 1.3.2. I — правый идеал, если:

1. $\forall a, b \in I : a \pm b \in I$
2. $\forall a \in I \forall r \in R : ar \in I, (IR \subseteq I))$

Def 1.3.3. Двусторонний идеал, если I — левый ($IR \subseteq I$) и правый ($RI \subseteq I$)

Замечание 1.3.2. в первом условии достаточно требовать: $\forall a, b \in I : a - b \in I$

▶ 1. $\exists a \in I \Rightarrow 0 = a - a \in I, 0 \in I$
2. $a + I \Rightarrow 0 - a \in I \Rightarrow -a \in I$
3. $a, b, -b \in I$. $a + b = a - (-b) \in I$

◀

Замечание 1.3.3. R — кольцо. $I = \{0\}$, $I = R$ — двусторонние идеалы.

Пример 1.3.1. Рассмотрим кольцо $\mathbb{Z}$.

$$I = m\mathbb{Z} = \{a \mid m \text{ делит } a\}$$

$R = M(n, K)$, где M — кольцо матриц размера n над полем K.
$S \subseteq \{1, \dots, n\}$
${}_S I$ — множество матриц, у которых: $\forall j \in S$, j-ый столбец заполнен нулями
I_S — множество матриц, у которых: $\forall j \in S$, j-ая строка заполнена нулями
${}_S I$ — левые идеалы не являются правыми
I_S — правые идеалы не являются левыми

Замечание 1.3.4. Далее «идеал» — двусторонний идеал.

1.3.1. Операции над идеалами

1. $I_\alpha (\alpha \in A)$ — идеал в кольце R (левый, правый, двусторонний). $I = \bigcap_{\alpha \in A} I_\alpha$ — идеал (левый, правый, двусторонний).
2. I_1, I_2 — идеалы в R (левые, правые, двусторонние). $I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\}$ — идеал (левый, правый, двусторонний).
3. I_1, I_2 — идеалы в R. $I_1 \cdot I_2 = \left\{\sum_{i=1}^{k} a_i b_i \mid a_i \in I_1, b_i \in I_2, k \in \mathbb{N}\right\}$ Если I_1, I_2 — левые, правые, двусторонние, то $I_1 \cdot I_2$ — левый, правый, двусторонний. Если I_1 — левый, а I_2 — правый, то $I_1 \cdot I_2$ — двусторонний.

▶ Все док-ва для левых, для правых аналогично, для двусторонних — обе выкладки.

1.

$$I = \cap_{\alpha\in A} I_\alpha, \forall a, b \in I$$
$$\forall \alpha \in A \colon a, b \in I_\alpha \wedge \forall \alpha \in A \colon a \pm b \in I_\alpha \Rightarrow a \pm b \in \cap_{\alpha\in A} I_\alpha$$
$$\forall r \in R, a \in I \colon \forall \alpha \in A \colon a \in I_\alpha, ra \in I_\alpha \Rightarrow ra \in \cap_{\alpha\in A} I_\alpha$$

2.

$$I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\}$$
$$a, c \in I_1 \wedge b, d \in I_2$$
$$a + b = I_1 + I_2 \wedge c + d \in I_1 + I_2$$
$$(a + b) \pm (c + d) = (a \pm c) + (b \pm d) \in I_1 + I_2$$
$$r \in R, a + b \in I_1 + I_2, a \in I_1, b \in I_2$$
$$r(a + b) = ra + rb \in I_1 + I_2$$

3. •

$$\sum_{i=1}^{k} a_i b_i, a_i \in I_1, b_i \in I_2$$
$$\sum_{i=1}^{s} c_i d_i, c_i \in I_1, d_i \in I_2$$
$$a_1 b_1 + \cdots + a_k b_k + (\pm c_1) d_1 + \cdots + (\pm c_s) d_s = a_1 b_1 + \dots a_k b_k + (\pm \dots \pm c_s d_s) \in I_1 I_2$$

•

$$r \in R$$
$$r\left(\sum^{k} a_i b_i\right) = \sum^{k} (r a_i) b_i \in I_1 \cdot I_2$$
$$\left(\sum^{k} a_i b_i\right) r = \sum^{k} a_i (b_i r) = I_1 \cdot I_2$$

I_1 — левый, I_2 — правый, $I_1 \cdot I_2$ — двусторонний

◀

1.3.2. Идеалы, порождённые семейством

Def 1.3.4. R — кольцо, $\{a_\alpha\}_{\alpha\in A}, a_\alpha \in R$. Идеал (левый, правый, двусторонний), порождённый $\{a_\alpha\}_{\alpha\in A}$ — наименьший по включению идеал (левый, правый, двусторонний), содержащий в себе это семейство.

$$J = \bigcap_{\beta\in B} I_\beta$$
$$\forall \beta \in B, I_\beta \supset A \wedge B \text{ — идеал (левый, правый, двухсторонний)}$$

Def 1.3.5. Альтернативное определение

$$J' = \left\{r_1 a_{\alpha_1} + \cdots + r_k a_{\alpha_k} + n_1 a_{\beta_1} + \cdots + n_s a_{\beta_s}\right\}$$
$$k, s \in \mathbb{N} \cup \{0\}; r_i \in R; \alpha_i, \beta_i \in A; n_i \in \mathbb{Z}$$

▶

$$J' \text{ — идеал}, a_\alpha \in J' \Rightarrow J \subseteq J'$$
$$a_\alpha \in J \Rightarrow J' \subseteq J$$
$$r(r_1 a_{\alpha_1} + \cdots + r_k a_{\alpha_k} + n_1 a_{\beta_1} + \cdots + n_s a_{\beta_s}) = rr_1 a_{\alpha_1} + \cdots + rr_k a_{\alpha_k} + rn_1 a_{\beta_1} + \cdots + rn_s a_{\beta_s}$$
$$\sum_{i=1}^{k} r_i a_{\alpha_i} \in J$$
$$\sum_{i=1}^{s} n_i a_{\beta_i} \in J$$

Замечание 1.3.5. Если $1 \in R$, то слагаемые $n_i a_{\beta_i}$ можно опустить

$$n_i > 0, n_i a_{\beta_i} = \underbrace{a_{\beta_i} + \cdots + a_{\beta_i}}_{n \text{ раз}} = \underbrace{(1 + \cdots + 1)}_{\in R} a_{\beta_i}$$

◀

Пример 1.3.2. $R = 2\mathbb{Z}$ — идеал, порождённый 2.

$$\forall r \in 2\mathbb{Z}, r \cdot 2 \in 4\mathbb{Z}$$

Обозначения:

- ${}_R\{(a_\alpha \mid \alpha \in A)\}$ — левый идеал, порождённый $\{a_\alpha\}_{\alpha \in A}$.
- $\{(a_\alpha \mid \alpha \in A)\}_R$ — правый идеал, порождённый $\{a_\alpha\}_{\alpha \in A}$.
- $\{(a_\alpha \mid \alpha \in A)\}$ — двусторонний идеал, порождённый $\{a_\alpha\}_{\alpha \in A}$.

Def 1.3.6. Главный идеал — идеал, порождённый одним элементом.

$$Ra, R(a), (a)R, aR, (a)$$
$${}_R(a_1, \ldots, a_n) = Ra_1 + \cdots + Ra_n$$
$$(a_1, \ldots, a_n)q_R = a_1 R + \cdots + a_n R$$

Пример 1.3.3. R — кольцо с единицей.

1. - $a \mid_R b \Leftrightarrow (a)_R \supseteq (b)_R$
   - $a \mid_R b \Leftrightarrow {}_R(a) \supseteq {}_R(b)$
2. R — область целостности.
   $(a) = (b) \Leftrightarrow a \sim b$

▶ 1. $\Rightarrow$

$$a \mid_R b \Rightarrow \exists c \colon b = ac$$
$$(b)_R = \{br \mid r \in R\} = \{acr \mid r \in R\} \subseteq (a)_R$$

$\Leftarrow$

$$(b)_R \subseteq (a)_R \Rightarrow b \in (a)_R$$
$$\exists c \colon b = ac$$
$$c \in R \Rightarrow a \mid_R b$$

2.

$$\begin{cases} (a) \subseteq (b) \Leftrightarrow b \mid a \\ (a) \supseteq (b) \Leftrightarrow a \mid b \end{cases} \Leftrightarrow a \sim b$$

◀

Def 1.3.7. R — коммутативное кольцо с единицей. Всякий идеал порожденный одним элементом — главный.

Def 1.3.8. R — область целостности. R — область главных идеалов (ОГИ), если каждый идеал в нем главный.

Пример 1.3.4. $R = K[x, y]$. Тогда R — не ОГИ.

▶

$$I = \{f \in K[x, y] \mid f(0, 0) = 0\}$$

$$I = (d) \Rightarrow \begin{cases} x \in d \\ y \in d \end{cases} \Rightarrow \begin{cases} d \mid x \\ d \mid y \end{cases} \Rightarrow d = const \neq 0$$

но $d \notin I$ — противоречие. Поэтому I — не главный идеал. ◀

1.4. Наибольший общий делитель

Def 1.4.1. R — коммутативное кольцо, $a_1, \ldots, a_n \in R$, $d \in R$. d называется наибольшим общим делителем, если

1. $d \mid a_1, \ldots, d \mid a_n$
2. Если $\delta \mid a_1, \ldots, \delta \mid a_n$, то $\delta \mid d$

$$d = \gcd(a_1, \ldots, a_n) = НОД(a_1, \ldots, a_n)$$

Замечание 1.4.1. Если R — область целостности, то gcd определен с точностью до ассоциированности.

▶

$$\begin{cases} \delta \mid d \\ d \mid \delta \end{cases} \Rightarrow d \sim \delta$$

◀

Def 1.4.2. $a_1, \ldots, a_n \in R$, $1 \in R$. $(a_1, \ldots, a_n)$ — взаимно просты, если

$$\gcd(a_1, \ldots, a_n) = 1$$

Следствие 1.4.0.1. $\gcd(a, b) = \gcd(a - bq, b), q \in R$

Следствие 1.4.0.2. $\gcd(a, 0) = a$

Следствие 1.4.0.3. $d = \gcd(a_1, \ldots, a_n)$, $1 \in R$, $a_1 = db_1, \ldots, a_n = db_n$. Тогда $b_1, \ldots, b_n$ — взаимно просты.

▶ 1.

$$d = \gcd(a, b)$$

$$\begin{cases} d \mid a \\ d \mid b \end{cases} \Rightarrow d \mid a - bq \Rightarrow d \text{ — общий делитель } a - bq \text{ и } b$$

Пусть $\exists \delta \colon \delta \mid a - bq \wedge \delta \mid b$. Тогда

$$a = a - bq + bq \Rightarrow \delta \text{ — общий делитель } a \text{ и } b \Rightarrow$$
$$\Rightarrow \delta \mid d \Rightarrow d = \gcd(a - bq, b)$$

2.

$$\begin{cases} a \mid a \\ a \mid 0 \end{cases} \Rightarrow a \text{ — общий делитель}$$

$$\begin{cases} \delta \mid a \\ \delta \mid 0 \end{cases} \Rightarrow \delta \mid a \Rightarrow a = \gcd(a, 0)$$

3.

$$d = \gcd(a_1, \dots, a_n), a_i = db_i, a_i \neq 0$$
$$1 \mid b_1, \dots, b_n$$
$$\delta \mid b_1, \dots, b_n$$
$$d\delta \mid a_1, \dots, a_n$$
$$d\delta \mid d \Rightarrow \exists u \colon d\delta u = d, d \neq 0 \Rightarrow \delta u = 1 \Rightarrow \delta \mid 1$$

◀

Теорема 1.4.1. R — коммутативное кольцо с единицей. $a_1, \dots, a_n \in R$.

1. Если $(a_1, \dots, a_n) = (d)$, то $d = \gcd(a_1, \dots, a_n)$ и
$$\exists x_1, \dots, x_n \in R \colon d = a_1 x_1 + \dots + a_n x_n$$
2. Если R — ОГИ, то $\forall a_1, \dots, a_n \exists \gcd(a_1, \dots, a_n)$ и допускается линейное представление.
3. R — ОГИ, $d = \gcd(a_1, \dots, a_n)$. Тогда
$$(d) = (a_1, \dots, a_n)$$

Замечание 1.4.2. Наибольший общий делитель, если и существует, то не всегда допускает линейное представление:

$$K[X, Y]; \gcd(x, y) = 1$$
$$1 = xf(x, y) + yg(x, y)$$

Подставим $x = y = 0$ — противоречие.

▶ 1.

$$(a_1, \dots, a_n) = (d)$$
$$a_1, \dots, a_n \in (d)$$
$$a_i = db_i \Rightarrow d \mid a_i \Rightarrow d \text{ — общий делитель}$$

С другой стороны $d \in (a_1, \dots, a_n)$

$$\exists x_1, \dots, x_n \in R \colon d = a_1x_1 + \dots + a_nx_n = S$$
$$\delta \text{ — общй делитель } a_1, \dots, a_n \Rightarrow \delta \mid S \Rightarrow \delta \mid d$$

2. Так как d — ОГИ, то $\exists d \colon (d) = (a_1, \dots, a_n)$. Значит по предыдущему пункту: $d = \gcd$ и существует линейное представление.
3.

$$d = \gcd(a_1, \dots, a_n)$$
$$(a_1, \dots, a_n) = (\delta) \text{ так как ОГИ}$$
$$\text{Значит } \delta = \gcd(a_1, \dots, a_n) \Rightarrow d \sim \delta \Rightarrow (d) = (a_1, \dots, a_n)$$

◀

Замечание 1.4.3. Существуют кольца, в которых наибольший общий делитель не всегда определен.

Теорема 1.4.2. R — ОГИ, a и b — взаимно просты и $a \mid bc$, тогда $a \mid c$.

▶

$$\gcd(a, b) = 1$$
$$\exists u, v \colon au + bv = 1 \mid c \Rightarrow auc + bcv = c$$
$$a \mid bc \Rightarrow a \mid c$$

◀

1.5. Евклидовы кольца

Def 1.5.1. R — область целостности, $\lambda \colon R \setminus \{0\} \to \mathbb{N}$ λ — Евклидова функция (евклидова норма), елси $\forall a, \forall b \neq 0, \exists q, r \in R \colon a = bq + r$ и ($r = 0$ или $\lambda(r) < \lambda(b)$)

Def 1.5.2. R — область целостности, R — евклидово кольцо, если на нем можно задать евклидову функцию.

Пример 1.5.1.
1. $R = \mathbb{Z}, \lambda(r) = |x|$
2. $R = K[x], \lambda = deg(g), K$ — поле
3. $\mathbb{Z}[i]$
4. $\mathbb{Z}[\omega]$

▶

$$\mathbb{Z}[i] = \{u + vi \mid u, v \in \mathbb{Z}\}$$
$$\lambda(u + vi) = |u + vi|^2 = u^2 + v^2, \lambda \text{ — евклидова функция, что и будем доказывать.}$$
$$\text{Пусть } a = u + vi, b = s + ti,\ u, v, s, t \in \mathbb{Z}, (s, t) \neq (0, 0)$$
$$\frac{a}{b} = \frac{u + vi}{s + ti} = \frac{(u + vi)(s - ti)}{s^2 + t^2} = \gamma + \delta i, \gamma, \delta \in \mathbb{Q}$$
$$\langle j \rangle \text{ — ближайшее целое, } |j - \langle j \rangle| \leq \frac{1}{2}$$
$$q = \langle \gamma \rangle + \langle \delta \rangle i, a = bq + r$$
$$r = a - bq = u + vi - (s + ti)(\langle \gamma \rangle + \langle \delta \rangle i) \Rightarrow r \in \mathbb{Z}[i]$$
$$\frac{\lambda(r)}{\lambda(b)} = \frac{|r|^2}{|b|^2} = \left|\frac{a - bq}{b}\right|^2 = \left|\frac{a}{b} - q\right|^2 = |\gamma + \delta i - \langle \gamma \rangle - \langle \delta \rangle i|^2 = |\gamma - \langle \gamma \rangle|^2 + |\delta - \langle \delta \rangle|^2 \leq \frac{1}{4} + \frac{1}{4} < 1$$
$$\lambda(r) < \lambda(b)$$

◀

Теорема 1.5.1. Если R евклидово, то R — ОГИ.

▶

$$I \text{ — идеал в } R$$
$$I = \{0\} = (0) \text{ — главный. Пусть } I \neq \{0\}$$
$$\mathbb{N} \cup \{0\} \supseteq \Lambda = \{\lambda(a) \mid a \in I \setminus \{0\}\} \neq \emptyset \Rightarrow \exists m \text{ — наименьший элемент в } \Lambda$$
$$\text{значит } \exists b \neq 0, b \in I : \lambda(b) = m$$
$$\text{Докажем, что } I = (b)$$
$$I \supseteq (b) \text{ очевидно}$$
$$a \in I, a = bq + r, r = 0 \text{ или } \lambda(r) < \lambda(b) = m$$
$$r = a - bq \in I, \text{ если } r \neq 0 \text{ то получаем противоречие с минимальностью } m \Rightarrow r = 0$$
$$a = bq \in (b)$$
$$I \in (b)$$
$$I = (b)$$

◀

Следствие 1.5.1.1. $\mathbb{Z}, K[x], \mathbb{Z}[i]$ — ОГИ (K — поле)

В частности, любой идел в $\mathbb{Z}$ имеет вид $m\mathbb{Z}$.

Алгоритм Евклида поиска НОД в Евклидовых кольцах

R — евклидово кольцо. $a, b \in R$
$b = 0 : gcd(a, 0) = a = a \cdot 1 + 0 \cdot 0$
$b \neq 0 :$

$$r_i, x_i, y_i$$
$$r_i = ax_i + by_i$$
$$r_0 = a, x_0 = 1, y_0 = 0$$
$$r_1 = b, x_1 = 0, y_1 = 1$$

$$r_{i-1} = r_i q_i + r_{i+1}$$
$$r_{i+1} = 0 \vee \lambda(r_{i+1}) < \lambda(r_i)$$

Продолжаем до тех пор, пока не получим нулевой остаток.

$$\lambda(r_1) > \lambda(r_2) > \cdots > \lambda(r_i) > \cdots$$

$$\exists n \colon r_{n+1} = 0$$
$$r_{i+1} = r_{i-1} - r_i q_i =$$
$$= (ax_{i-1} + by_{i-1}) - (ax_i + by_i)q_i =$$
$$= a(x_{i-1} - x_i q_i) + b(y_{i-1} - y_i q_i)$$
$$x_{i+1} = x_{i-1} - x_i q_i$$
$$y_{i+1} = y_{i-1} - y_i q_i$$
$$r_{n+1} = 0, r_n \neq 0$$
$$gcd(a,b) = r_n = ax_n + by_n$$
$$gcd(r_{i+1}, r_i) = gcd(r_i q_i + r_{i+1}, r_i) = gcd(r_{i-1}, r_i) = gcd(r_i, r_{i+1})$$
$$gcd(a,b) = gcd(r_0, r_1) = gcd(r_1, r_2) = \cdots = gcd(r_n, r_{n+1}) = gcd(r_n, 0) = r_n$$

1.6. Неприводимый, состовные и простые элементы

R — область целостности

Def 1.6.1. $a \in R \setminus (\{0\} \cup R^*)$, a — **составной**, если $a = bc;\ b, c \notin R^*$

Def 1.6.2. $a \in R \setminus (\{0\} \cup R^*)$, a — **неприводимый**, если из $a = bc$ следует, что $b \in R^*$ или $c \in R^*$

Def 1.6.3. $a \in R \setminus (\{0\} \cup R^*)$, a — **простой**, если $\forall b, c \in R\,(a \mid bc \Rightarrow a \mid b$ или $a \mid c)$

$$p|ab \Rightarrow p|a \vee p|b$$

R — область целостности
$\{0\} \cup R^* \cup \{$ неприводимые $\} \cup \{$ составные $\}$

Теорема 1.6.1. 1. R — область целостности

Всякий простой элемент неприводим.

2. R — ОГИ, всякий неприводимый простой.

▶ 1. $p \in R, p$ — простой.

$$p = ab \Rightarrow a|p, b|p$$
$$p|ab \xRightarrow[\text{p — простой}]{} p|a \cup p|b$$

$$\begin{matrix} p|a \wedge a|p \Rightarrow a \sim p, b \in R^* \\ p|b \wedge b|p \Rightarrow b \sim p, b \in R^* \end{matrix} \Rightarrow p\text{— неприводим}$$

2. R — ОГИ
   p — неприводимый.

$$p|ab$$

   $p|a(ok)$
   $p \nmid a$:

$$(p,a)=(d)$$

$$p=dv$$

$$d \nsim p(\text{Если } d\sim p, \text{ то } p|d|a!\,?)$$

$$\begin{matrix} p=dv \\ p \nsim d \\ p \text{ — неприводим} \end{matrix} \Rightarrow d\in R^*$$

$$(p,a)=(d)=(1)$$

   p, a — взаимно просты.

$$\begin{matrix} p|ab \\ p \text{ взаимно прост с } a \end{matrix} \Rightarrow p|b$$

$$\Rightarrow p\text{— простой}$$

◀

prume — простой.
irreducible — неприводимый
composite — составной

1.7. Факториальные кольца

Def 1.7.1. В кольце R выполнена теорема об однозначном разложение на множители.

1.

$$a\in R^*\setminus\{0\}$$

$$a=\varepsilon\prod_{i=1}^{n}p_i$$

$$\varepsilon\in R^*, n\geqslant 0, p_i\text{— неприводимы}$$

   Или эквивалентное условие

$$a\in R, a\notin\{0\}\cup R^*$$

$$a=\prod_{i=1}^{n}p_i, n\geqslant 1$$

2.

$$0\neq a=\varepsilon,\prod_{i=1}^{n}p_i=\eta\prod_{j=1}^{n}q_j$$

$$\varepsilon,\eta\in R^*, p_i, q_i\text{ — неприводимы}\Rightarrow n=m$$

$$\text{и } \exists\sigma\in S_n\colon \forall i=1\ldots n\colon p_i\sim q_{\sigma(i)}$$

Такое кольцо называется факториальным (unique factorization domain UFD)

Пример не факториального кольца

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

Упражнение

$$6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$$

▶ $2, 3, 1 + \sqrt{5}i, 1 - \sqrt{5}i$ — неприводимые, попарно не ассоциированные.

$$N \colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{N} \cup \{0\}$$

$$N(a + b\sqrt{5}i) = |a + b\sqrt{5}i|^2 = a^2 + 5b^2$$

$$N(z_1 z_2) = N(z_1)N(z_2)$$

$$z_1 \in R^*$$

$$z_1 z_2 = 1$$

$$N(z_1)N(z_2) = N(1) = 1$$

$$x_1 = a + b\sqrt{5}i$$

$$a^2 + 5b^2 \in \mathbb{Z}$$

$$a^2 + 5b^2 = 1, b = 0, a = \pm 1$$

$2, 3, 1 \pm \sqrt{5}i$ — неприводимые, попарно не ассоциированы.

$$\mathbb{Z}[\sqrt{5}]^* = \{\pm 1\} \Rightarrow 2, 3, 1 \pm \sqrt{-5} \text{ — попарно не ассоциированы}$$

$$z_1 z_2 = 1$$

$$N(z_1) = 1, z_1 = \pm 1$$

$$N(z_2) = 1, z_2 = \pm 1$$

$$2 = z_1 z_2$$

$$4 = N(2) = N(z_1)N(z_2)$$

$$N(z_1) = N(z_2) = 2 \text{— невозможно}$$

$$z_1 = a + b\sqrt{-5}$$

$$a^2 + 5b^2 = 2 \text{ нет решений в } \mathbb{Z}$$

$$N(1 + \sqrt{5}i) = 6$$

$$1 \pm \sqrt{5}i = z_1 z_2$$

6 1
1 6
2 3
3 2

Нет элементов нормы 2 $\Rightarrow$ нет решений.

$$9 = N(3) = N(z_1)N(z_2)$$

9 1

1 9

3 3

$a^2 + 5b^2 = 3$ — нет решений в целых $\Rightarrow$ нет элементов нормы 3.

◀

Замечание: В этом же кольце не для всех пар определен gcd.
Докажем: ОГИ — факториальны.
$K[x_1, \cdots, x_n]$ — факториально(но не ОГИ $n \geqslant 2$)
$\mathbb{Z}[x_1, \cdots, x_n]$ — факториально(но не ОГИ, если $n \geqslant 1$)
R — факториальная о.ц. $\Rightarrow R[x]$ — факториальна.

1.8. Нётеровы кольца и условия обрыва возрастающих цепей идеалов

R — коммутативное кольцо
Выполнено условие обрыва возрастающей цепей идеалов, если $I_1 \subset I_2 \cdots (I_j)$ — идеалы.
$\exists n \colon I_n = I_{n+1} = \cdots$
(нет бесконечных строго возрастающих цепочек)
$I_1 \subsetneq I_2 \subsetneq I_3 \cdots$ — такие цепочки невозможны.

Def 1.8.1. Кольцо, в котором выполняется условие обрыва возрастающей цепочки идеалов, называется Нётеровым.

Пример 1.8.1. $\mathbb{Z}$ — нётерово.
(m)

$$(m_1) \subset (m_2) \subset \cdots$$

$$m_1 \vdots m_2 \vdots m_3 \cdots m_i$$

Теорема 1.8.1. Следующие условия равносильны

1. R — нётерово.
2. Всякий идеал в R конечно порожден.

Следствие 1.8.1.1. R — ОГИ $\Rightarrow$ R нётерово $\Rightarrow$ в R выполнено условие обрыва возрастающих цепей идеалов.

▶ 1) $\Rightarrow$ 2) :
I — идеал в R

$$a_1 \in I$$

$$I = (a_1) \colon ok$$
$$I \neq (a_1) \Rightarrow \exists a_2 \in I \setminus (a_1)$$
$$(a_1, a_2)$$

$$I = (a_1, a_2) : ok$$
$$I \neq (a_1, a_2) \Rightarrow \exists a_3 \in I \setminus (a_1, a_2)$$
$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \cdots$$

так как R Нётерово, то цепочка обрывается.

$$\exists n : I = (a_1, \cdots a_n)$$

$2) \Rightarrow 1)$:

$$I_1 \subset I_2 \subset \cdots \subset I_k \subset \cdots$$
$$I = \cup_{j=1}^{\infty} I_j — \text{идеал в} R$$
$$a, b \in I$$
$$\exists i, j a \in I_i, b \in I_j$$
$$m = max(i, j)$$
$$I_j, I_i \subset I_m \Rightarrow a, b \in I_m$$
$$a \pm b \in I_m \Rightarrow a \pm b \in \cup I_j = I$$
$$a \in I, r \in R$$
$$\exists j : a \in I_j, r \in R, ra \in I_j \Rightarrow ra \in \cup_j I_j = I$$

I — идеал.
I — конечно порожден $\exists a_1, \cdots, a_n$

$$I = (a_1, \cdots, a_n)$$

$$a_1 \cdots a_n \in \cup_j I_j$$
$$\exists j_k : a_k \in I_{j_k} k = 1 \cdots n$$
$$m = max(j_1, \cdots, j_k)$$
$$I_{j_k} \subset I_m$$
$$a_1, \cdots, a_k \subset I_m$$
$$(a_1, \cdots, a_k) \subset I_m \subset I_{m+1} \subset \cdots$$
$$\subset \cup_j I_j = I = (a_1, \cdots, a_n)$$
$$\Rightarrow I_m = I_{m+1} = \cdots$$

◀

1.9. Факториальность ОГИ

Теорема 1.9.1. R — ОГИ $\Rightarrow R$ факториально.

1. Всякий ненулевой необратимый элемент делится хотя бы на один неприводимый.
2. Всякий ненулевой необратимый элемент раскладывается в произведение неприводимых.
3. Единственность.

▶ 1.

$$R\text{— ОГИ}, a \in R, a \notin \{0\} \cup R^*$$

$$a = a_0$$

$$a_0\text{— неприводимо: } ok$$

$$a_0\text{— составное} \Rightarrow a_0 = a_1 b_1, a_1 b_1 \notin R^*$$

$$a_1\text{— неприводимо: } ok$$

$$a_1\text{— составное} \Rightarrow a_1 = a_2 b_2, a_2 b_2 \notin R^*$$

$$a_0 \vdots a_1 \vdots a_2 \vdots \cdots$$

$$(a_0) \subset (a_1) \subset (a_2) \subset \cdots$$

$$\text{По теореме об обрыве цепей, } \exists n : (a_n) = (a_{n+1}) = \cdots$$

$$a_n \sim a_{n+1}$$

$$a_n = a_{n+1} b_{n+1}; a_{n+1} b_{n+1} \notin R^* \Rightarrow a_{n+1} \nsim a_n$$

Либо на каком-то шаге a_i неприводим $\Rightarrow a_i \mid a$, либо процесс никогда не обрывается (противоречие с теоремой об обрыве цепей).

2.

$$R\text{— ОГИ}, a \in R, a \notin \{0\} \cup R^*$$

По пункту 1, $\exists p_1$ — неприводимый

$$a = p_1 b_1$$

$$b_1 \in R^* \Rightarrow \varepsilon = b_1$$

$$b_1 \notin R^* \Rightarrow \exists p_2 = p_1 b_2$$

$$a \vdots b_1 \vdots b_2 \vdots \cdots$$

$$\text{т.к. } p_i \notin R^*,$$

$$(a) \subsetneq (b_1) \subsetneq (b_2) \subsetneq \cdots$$

$$\text{По теореме об обрыве цепей, } \exists n : b_n \in R^*, \varepsilon = b_n$$

$$a = \varepsilon p_1 p_2 \ldots p_n$$

Следствие 1.9.1.1. В ОГИ теорема об однозначности разложения на множители справедлива в части существования.

3.

$$R\text{— ОГИ}, a = \varepsilon \prod_{i=1}^{n} p_i = \eta \prod_{j=1}^{m} q_j$$

$$\varepsilon, \eta \in R^*, p_i, q_j\text{— неприводимы.}$$

$$n \leqslant m$$

Индукция по n.

База:

$$n = 0$$

$$\varepsilon = \eta \prod_{j=1}^{m} q_j$$

Если бы $m \geqslant 1$, то справа — необратимо $\Rightarrow m = 0$

Переход:

$$n \geqslant 1$$

$$\varepsilon \prod_{i=1}^{n} p_i = \eta \prod_{j=1}^{m} q_j$$

$$p_n \mid \eta \prod_{j=1}^{m} q_j$$

p_n — неприводим, R — ОГИ $\Rightarrow p_n$ — простой

$$p_n \nmid \eta \Rightarrow \exists j \colon p_n \mid q_j$$

Не умоляя общности, $p_n \mid q_m$

$q_m = p_n \beta, q_m$ — неприводим, β — обратимый

$$\varepsilon(\prod_{i=1}^{n-1} p_i)p_n = \eta\beta(\prod_{j=1}^{m-1} q_j)p_n$$

$$\varepsilon \prod_{i=1}^{n-1} p_i = \eta\beta \prod_{j=1}^{m-1} q_j$$

По предположению, $n - 1 = m - 1 \Rightarrow n = m$ и $\exists \sigma \in S_{n-1} \colon \forall i = 1..n-1, p_i \sim q_{\sigma(i)}$

$$p_n \sim q_m = q_n$$

◀

1.10. Разложение на неприводимые множители в C[x] и R[x]

$K[x], K$ — поле.

$x - c$ всегда неприводим

$$x - c = fg \Rightarrow \deg f = 0, \text{ либо } \deg q = 0$$

$$f \in K^* = K[x]^* \text{ или } g \in K^* = K[x]^*$$

Если K — алгебраически замкнутое поле, то других неприводимых в $K[x]$ нет (всякий многочлен степени $\geqslant 1$ делится на линейный).

Теорема 1.10.1. C — алгебраически замкнуто

$$f \in C[x] \Rightarrow f = a \prod_{i=1}^{m} (x - c_i)^{a_i}, a_i \geqslant 1, a \in C$$

(без доказательства)

Вообще говоря, отсутствие корней не влечет неприводимости многочлена, но, если $\deg f = 2$ или $\deg f = 3$, то f — неприводим $\Leftrightarrow$ f не имеет корней.

$$f = gh \text{ и } g, h \notin K^*$$

$$\deg f = 2 \Leftrightarrow \deg g = \deg h = 1$$

$$\deg f = 3 \Leftrightarrow \deg g = 1, \deg h = 2 \text{ или } \deg g = 2, \deg h = 1$$

Теорема 1.10.2.

$$f \in R[x], f \neq 0$$

$$f = a\prod_{i=1}^{n}(x - c_i)^{a_i}\prod_{j=1}^{m}(x^2 + b_j x + c_j)^{d_j}, b_j^2 - 4c_j < 0$$

▶

$$f \in R[x], z \in C \setminus R, z\text{— корень } f$$

Докажем, что $\bar{z}$ — тоже корень f, причем той же кратности, что и z.

$$f \in R[x]$$

$$f(x) = a_n x^n + \cdots + a_0$$

$$0 = f(z) = a_n z^n + \cdots + a_0$$

$$0 = \bar{0} = \bar{a_n}(\bar{z})^n + \cdots + \bar{a_0} = a_n(\bar{z})^n + \cdots + a_0 = f(\bar{z})$$

Если z — корень f кратности k, то

$$f(z) = f'(z) = \cdots = f^{(k-1)}(z) = 0, f^{(k)}(z) \neq 0$$

$$f(\bar{z}) = f'(\bar{z}) = \cdots = f^{(k-1)}(\bar{z}) = 0, f^{(k)}(\bar{z}) \neq 0$$

Значит $\bar{z}$ — корень той же кратности.

$$f \in R[x] \subset C[x]$$

$$f = q\prod_{i=1}^{n}(x - z_i)^{\alpha_i}, z_i \in C$$

отдельно вещественные корни, отдельно комплексные $z_i \in C \setminus R$

$$(x - z)^{\alpha_i}(x - \bar{z})^{\alpha_i} = ((x - z)(x - \bar{z}))^{\alpha_i}$$

$$(x - z_i)(x - \bar{z_i}) = x^2 - 2\operatorname{Re}(z_i)x + |z_i|^2$$

$$D = 4\operatorname{Re}(z_i)^2 - 4|z_i|^2 = -4\operatorname{Im}(z_i)^2 < 0$$

◀

1.11. Гомоморфизм колец и двусторонние идеалы

R — произвольное кольцо, не обязательно коммутативное.

$$f : R \to R'$$

Def 1.11.1. f - гомоморфизм колец, если

$$\forall a, b \in R$$

$$f(a \pm b) = f(a) \pm f(b), f(ab) = f(a)f(b), f(0_R) = 0_{R'}$$

Def 1.11.2.

$$f^{-1}(0_{R'}) — \text{ядро гомоморфизма}, \ker f(kernel)$$

Теорема 1.11.1. $\ker f$ — двусторонний идеал в R.

▶

$$\ker f \neq 0, 0_R \in \ker f$$
$$a, b \in \ker f$$
$$f(a \pm b) = f(a) \pm f(b) = 0 + 0 = 0$$
$$a \pm b \in \ker f$$
$$a \in \ker f$$
$$r \in R$$
$$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0$$
$$ra \in \ker f$$
$$f(ar) = f(a)f(r) = 0 \cdot f(r) = 0$$
$$ar \in \ker f$$

◀

Двусторонние идеалы — в точности ядра гомоморфизмов.

1.12. Сравнение по модулю двустороннего идеала

R - кольцо, I - двусторонний идеал.

$$a \equiv b(modI), \text{если } a - b \in I$$

Пример

$$Z, a \equiv b(modm)$$
$$a - b \vdots m$$
$$a - b \in mZ = (m)$$

Теорема 1.12.1. Сравнимость — отношение эквивалентности.

▶ 1. Рефлексивность.

$$a \equiv a(modI) \Leftrightarrow a - a = 0 \in I$$

2. Симметричность.

$$a \equiv b(mod I) \Rightarrow a - b \in I \Rightarrow -(a-b) \in I \Rightarrow b - a \in I \Rightarrow b \equiv a(mod I)$$

3. Транзитивность.

$$a \equiv b(mod I), b \equiv c(mod I) \Rightarrow a - b \in I, b - c \in I \Rightarrow a - c \in I \Rightarrow a \equiv c(mod I)$$

◀

Def 1.12.1. $a \in R$, $[a]$ — класс эквивалентности R

$$[a] = \{b \in R \colon a \equiv b(I)\}$$

$R/\equiv$ или R/I — множество классов эквивалентости

Свойства сравнения
Пусть $a \equiv b(I)$, $c \equiv d(I)$. Тогда

1. $a \pm c \equiv b \pm d$
2. $ac \equiv bd$

▶

$$a - b \in I$$
$$c - d \in I$$

1. $(a-b) \pm (c-d) \in I \Rightarrow (a \pm c) - (b \pm d) \in I \Rightarrow a \pm c \equiv b \pm d$
2. $(a-b)c \in I$, $b(c-d) \in I$

$$(a-b)c + b(c-d) = ac - bd \in I \Rightarrow ac \equiv bd(I)$$

◀

Следствие 1.12.1.1. $a \equiv b(I)$, тогда $ac \equiv bc(I)$, $ca \equiv cb(I)$. Так как $c \equiv c(I)$.

1.13. Факторкольцо

R — кольцо, I — двусторонний идеал R.
R/I хотим превратить в кольцо.
Определим операции:

1. $[a] + [b] = [a + b]$
2. $[a] \cdot [b] = [a \cdot b]$

$$+, \cdot \colon R/I \times R/I \to R/I$$

Проблема: результат может зависеть от выбора представителей класса

$$[a] = [a']$$
$$[b] = [b']$$
$$[a+b] \stackrel{?}{=} [a'+b']$$
$$[ab] \stackrel{?}{=} [a'b']$$

Проверка корректности операций

$$a \equiv a'(I)$$
$$b \equiv b'(I)$$
$$a + b \equiv a' + b'(I) \Rightarrow [a + b] = [a' + b']$$
$$ab \equiv a'b'(I) \Rightarrow [ab] = [a'b']$$

Теорема 1.13.1. $(R/I, +, \times)$ — кольцо. Если R — коммутативное, то R/I — коммутативное. Если R содержит 1, то и R/I содержит 1.

▶
1. $([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c])$
2. $[a] + [b] = [a + b] = [b + a] = [b] + [a]$
3. $0_{R/I} = [0]$

$$[0] + [a] = [0 + a] = [a]$$
$$[a] + [0] = [a + 0] = [a]$$
$$b \in [0] \Leftrightarrow b - 0 \in I \Leftrightarrow b \in I$$
$$[0] = I$$

4. $-[a] = [-a]$

$$[a] + [-a] = [a + (-a)] = [0]$$
$$[-a] + [a] = [(-a) + a] = [0]$$

5. $([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c] = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \cdot [b \cdot c] = [a] \cdot ([b] \cdot [c])$
6. $[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a \cdot (b + c)] = [(a \cdot b + a \cdot c)] = [a \cdot b] + [a \cdot c] = [a] \cdot [c] + [a] \cdot [b]$
   $([b] + [c]) \cdot [a] = [b + c] \cdot [a] = [(b + c) \cdot a] = [(b \cdot a + c \cdot a)] = [b \cdot a] + [c \cdot a] = [b] \cdot [a] + [c] \cdot [a]$
7. Если R — коммутативное

$$[a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b] \cdot [a]$$

8. Если R содержит 1

$$1_{R/I} = [1_R]$$
$$[a] \cdot [1_R] = [a \cdot 1_R] = [a]$$
$$[1_R] \cdot [a] = [1_R \cdot a] = [a]$$

◀

Def 1.13.1. $(R, +, \cdot)$ — факторкольцо кольца R по двустороннему идеалу I (факторкольцо R по I)

Пример 1.13.1.

$$R = \mathbb{Z}$$
$$I = m\mathbb{Z}, m > 1$$
$$\mathbb{Z}/m\mathbb{Z} \stackrel{\text{def}}{=} R/I$$
$$x \in \mathbb{Z}/m\mathbb{Z}$$
$$x = [a] = b \in \mathbb{Z} \colon b = a(m)$$

В один класс попадают числа, дающие один остаток при делении на m.

$$\varphi\colon R \to R/I$$
$$a \mapsto [a]$$
$$\varphi(a+b) = [a+b] = [a] + [b] = \varphi(a) + \varphi(b)$$
$$\varphi(a \cdot b) = [a \cdot b] = [a] \cdot [b] = \varphi(a) \cdot \varphi(b)$$
$$\varphi \text{ — гомоморфизм}$$
$$\ker \varphi = \varphi^{-1}(0_{R/I}) = \varphi^{-1}([0]) = I$$

Значит каждый идеал — ядро некоторого гомоморфизма. Вместе с доказанным ранее, ядра гомоморфизмов — в точности двусторонние идеалы.

Теорема 1.13.2. (о гомоморфизме) $f\colon R \to R'$ — гомоморфизм. Тогда $f(R)$ изоморфно $R/\ker f$.

▶ Построим $\varphi\colon f(R) \to R/\ker f$, следующим образом:

$$\forall x \in f(R), \exists a\colon f(a) = x$$
$$\varphi(x) = [a]$$

Докажем, что это изоморфизм.

Проверка корректности

$$\text{Доказать: } f(a) = f(a') \Rightarrow [a] = [a']$$
$$f(a - a') = f(a) - f(a') = x - x = 0$$
$$(a - a') \in \ker f$$
$$a \equiv a' (\ker f)$$
$$[a] = [a']$$

φ — гомоморфизм

$$x, y \in f(R)$$
$$a \in f^{-1}(x)$$
$$b \in f^{-1}(y)$$
$$f(a+b) = f(a) + f(b) = x + y$$
$$(a+b) \in f^{-1}(\{x+y\})$$
$$\varphi(x+y) = [a+b] = [a] + [b] = \varphi(x) + \varphi(y)$$
$$f(ab) = f(a)f(b) = xy$$
$$(ab) \in f^{-1}(\{xy\})$$
$$\varphi(xy) = [ab] = [a] \cdot [b] = \varphi(x) \cdot \varphi(y)$$

φ — **биекция**

$$\text{Пусть } [a] \in R/\ker f$$
$$a \in R$$
$$f(a) \in f(R)$$
$$a \in f^{-1}(\{f(a)\})$$
$$\varphi(f(a)) = [a] \Rightarrow \varphi \text{ — сюрьекция}$$
$$x, y \in f(R)$$
$$a \in f^{-1}(\{x\})$$
$$b \in f^{-1}(\{y\})$$
$$\text{Пусть } \varphi(x) = \varphi(y)$$
$$[a] = [b]$$
$$a \equiv b(\ker f)$$
$$(b-a) \in \ker f$$
$$x = f(a) = f(a) + 0 = f(a) + f(b-a) = f(a+b-a) = f(b) = y$$
$$\text{Значит } \varphi \text{ — инъекция.}$$

◀

1.14. Максимальные идеалы

Def 1.14.1. R — кольцо. Двусторонний идеал I называется максимальным, если

1. $R \neq I$
2. Если $I \subseteq J \subseteq R$, где J — двусторонний идеал, то

$$J = I \text{ или } J = R$$

Иначе говоря, возьмем множество всех идеалов R, кроме самого R и упорядочим их по включению. Максимальный идеал — максимальный элемент множества.

Теорема 1.14.1. R — коммутативное кольцо с 1. I — идеал R.

$$R/I \text{ — поле } \Leftrightarrow I \text{ — максимальный идеал}$$

▶ **Влево**

$$I \text{ — максимальный идеал}$$
$$1_R \notin I$$
$$(1) = R \supsetneq I$$
$$[1] \neq [0]$$
$$x \in R/I \colon x \neq 0_{R/I}$$
$$x = [a], a \notin I$$
$$I \subsetneq I + (a) \subset R$$
$$I + (a) = R$$
$$I + (a) = \{b + a \cdot c \mid b \in I, c \in R\}$$
$$\exists b \in I, c \in R \colon 1 = b + a \cdot c$$
$$[1] = [b + ac] = [b] + [a] \cdot [c] = x \cdot [c] = [c] \cdot x$$
$$c \text{ — обратный к } x$$

Вправо

$$R/I \text{ — поле}$$
$$\text{Пусть } I \subset J \subset R$$
$$\text{Пусть } I \neq J$$
$$\text{Докажем, что } J = R$$
$$J \neq I \Rightarrow \exists a \in J \colon a \notin I$$
$$[a]_I \neq [0]_I$$
$$R/I \text{ — поле } \Rightarrow \exists [b]_I \colon [b]_I \cdot [a]_I = [1]_I$$
$$1 = ba(I)$$
$$1 = ba + c, c \in J$$
$$ba \in J, c \in J \Rightarrow 1 \in J \Rightarrow r = r\dot{1} \in J \forall r \in R \Rightarrow J = R$$

◀

Утверждение 1.14.1. Пусть R — ОГИ. $a \nsim 1$

$$(a) \text{ — максимальный} \Leftrightarrow a \text{ — неприводим}$$

▶ Пусть $a = \varepsilon p_1 p_2 \dots p_k$, p_i — неприводим

$$(a) \subsetneq (p_i) \subsetneq R$$

◀

Следствие 1.14.1.1. $R = \mathbb{Z}$

$$\mathbb{Z}/m\mathbb{Z} \text{ — поле} \Leftrightarrow m \text{ — простое}$$

Следствие 1.14.1.2. $R = K[x]$, K — поле.

$$K[x]/f \text{ — поле } \Leftrightarrow f \text{ — неприводим над } K$$

1.15. Расширение полей и присоеденение корней

Def 1.15.1. F — подполе K, если F, K — поля, $F \subseteq K$.

Def 1.15.2. K — расширение F, если F, K — поля, $F \subseteq K$.

Теорема 1.15.1. F — поле, $f \in F[x]$, f — неприводимый многочлен, $K = F[x]_{/(f)}$. Тогда:

$$K \text{ — поле}, f \text{ имеет корень в} K$$

▶

$$f \text{ — неприводимый} \Rightarrow (f) \text{ — максимальный идеал} \Rightarrow$$
$$F[x]_{/(f)} \text{ — поле}$$

Введем гомоморфизм $\varphi\colon F[x] \to F[x]_{/(f)}$, редукция по модулю идеала. По теореме о делении с остатком, каждый класс вычитов в $F[x]_{/(f)}$ содержит единственный многочлен степени $\leq n-1$, где $n = \deg f \Rightarrow$ сужение $\varphi|_F$ на множество констант — инъективно.

$$F_K \cong \varphi(F) \subseteq K \text{ отождевствляем } F \text{ и } \varphi(F),\ [const] = const$$

$$x \xrightarrow{\varphi} [x] = \alpha$$
$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, a_n \neq 0$$
$$[f(x)] = 0_K, 0_K \text{ — класс нулевого многочлена в } K$$
$$0_K = [a_0] + [a_1][x] + \cdots + [a_n][x]^n = f(\alpha) \Rightarrow$$
$$x \text{ — корень } f \text{ в поле } K$$

◀

Замечание 1.15.1. В этом доказательстве сужение φ на множество многочленов степени $\leq n-1$ инъективно $\Rightarrow$ всякий элемент поля K единственным образом представляется в виде

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = [c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}]$$

Def 1.15.3. K — поле, полученное присоединением корня f.

Пример 1.15.1. $\mathbb{R}, f = x^2 + 1$.

$$\mathbb{R}[x]_{/(x^2+1)} = \{a + b[x] \mid a, b \in \mathbb{R}\}$$
$$(a + b[x])(c + d[x]) =$$
$$= ac + (ad + bx)[x] + bd[x^2] =$$
$$= ac + (ad + bc)[x] + bd[-1] =$$
$$= ac - bd + (ad + bc)[x] \text{ — напоминает умножение в } \mathbb{C}$$
$$\mathbb{R}[x]_{/(x^2+1)} \to \mathbb{C}$$
$$a + b[x] \to a + bi$$

Def 1.15.4. F — поле, $f \in F[x], \deg f \geq 1$. Поле $K \supseteq F$ называется полем разложения f, если f раскладывается в K на линейные множители, но не разложим в любом подполе K.

Теорема 1.15.2. $\exists K$ — поле разложения f.

▶ 1. $\exists L$, в котором f раскладывается на линейные множетели. Докажем по индукции по суммарной степени нелинейных множителей f:

База: Суммарной степени нелинейных множителей ноль. Значит, f разложим на линейные множители.

Переход:

$$\exists f_1 | f, \deg f_1 \geq 2, f_1 \text{ — неприводим}$$

$$F[x]_{/(f_1)} = L_1, \text{ в } L_1, f_1 \text{имеет корень}$$

$$F[x] \subseteq L_1[x]$$

$$f_1 = (x - \alpha)g \text{ в } L_1[x]$$

По индукционному предположению, $\exists L$ — расширение L_1, в котором f раскладывается на линейные множители.

$$F \subseteq L_1 \subseteq L$$

2. $K = \bigcap M$, $M \subset L$, M — подполе L, f — раскладывается на линейный члены.

◀

1.16. Поле частных областей целостности

R — область целостности. Задача: построить "наименьшее возможное"поле F, содержащие R:

Def 1.16.1.

$$X = \{(a, b) \mid a, b \in R, b \neq 0\} \text{ — множество дробей}$$

Введем отношение эквивалентности на X: $\sim$: $(a, b) \sim (a_1, b_1) \Leftrightarrow ab_1 = a_1 b$ Тогда, полем частных кольца R называется фактор-множество X: $X_{/\sim}$

Def 1.16.2. $\frac{a}{b} = [(a, b)]$ — дробь.

Зададим на $X_{/\sim}$ сложение и умножение:

Def 1.16.3.

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Def 1.16.4.

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ad + bc}{bd}$$

Утверждение 1.16.1. $+, \cdot$ — операции на $X_{/\sim}$.

1. $b \neq 0, d \neq 0 \Rightarrow bd \neq 0$
2. Корректность: $\forall$ представиль класса эквивалентности подходит.

Утверждение 1.16.2. $\{\frac{a}{1} \mid a \in R\}$ — подкольцо K, изоморфное R.

Теорема 1.16.1. $K = (X_{/\sim}, +, \cdot)$ — поле.

▶ Очевидны все свойства, кроме дистрибутивности.

$$\left(\frac{a}{b} + \frac{c}{d}\right)\frac{e}{f} = \frac{ad + bc}{bd}\frac{e}{f} = \frac{ade + bce}{bdf}$$

$$\frac{a}{b} \cdot \frac{e}{f} + \frac{c}{d} \cdot \frac{e}{f} = \frac{ae}{bf} + \frac{ce}{df} = \frac{aedf + cbef}{bdf^2}$$

$$\frac{ade+bce}{bdf} \sim \frac{aedf+cbef}{bdf^2}$$

Нулевой и единичный элементы:

$$0_K = \frac{0}{1}$$

$$1_K = \frac{1}{1}$$

Всякий ненулевой элемент обратим:

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1} = 1_K$$

◀

1.17. Поле рациональных функций. Разложение на простые дроби

Def 1.17.1. Поле частных кольца $F[x]$ (F-поле) называется полем рациональных функций и обозначается $F(x)$.

Def 1.17.2. Всякая дробь в $f(x)$ может быть единственным образом записан в виде $\frac{f}{g}$, $gcd(f,g)=1$ старший коэффицент g равен еденице.

Def 1.17.3. $\frac{f}{g} \in F(x)$ $\frac{f}{g}$ - правильная дробь, если $\deg f < \deg g$

Def 1.17.4. $\frac{f}{g} \in F(x)$ $\frac{f}{g}$ - примарная дробь, если $g = q^k$, где q - неприводима, а $\deg f < \deg g$

Def 1.17.5. $\frac{f}{g} \in F(x)$ $\frac{f}{g}$ - простейшая дробь, если $g = q^k$, где q - неприводима, а $\deg f < \deg q$

Теорема 1.17.1. $\frac{f}{g} \in F(x)$ может быть представлена в виде многочлена и суммы простейших дробей, причем такое разложение единственно. $\frac{f}{g} = h (h \in F(x)) +$ сумма простейших

▶ План

1. Существует разложение $\frac{f}{g} = h + \frac{f'}{g}$ $\frac{f'}{g}$ - правильная дробь.
2. Всякая правильная дробь есть сумма примарных.
3. Всякая примарная дробь - есть сумма простейших.

Замечание 1.17.1. По теореме о деление с остатком $f = h \cdot g + f'$, $\deg f' < \deg g$; $\frac{f}{g} = h + \frac{f'}{g}$. При этом $h, f' \in F(x)$ $\frac{f}{g}$ - правильная дробь.

Лемма 1.17.1. Пусть есть правильная дробь $\frac{f}{g_1 g_2} \Rightarrow$ существуют f_1, f_2 такие, что $\frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2}$. При это $\frac{f_1}{g_1}$, $\frac{f_2}{g_2}$ - правильные (g_1, g_2 - взаимно простые.)

▶ $g_1, g_2 \in F(x)$, $gcd(g_1, g_2) = 1 \Rightarrow (g_1, g_2) = 1$ (Идеал порожденный g_1 и g_2 совподает с идеалом порожденным еденицей), так как F(x) - ОГИ $\Rightarrow$ числитель можем представить через g_1 и g_2

$$\exists h_1, h_2 \in F(x) : f = g_1 h_2 + g_2 h_1$$

Так как $f \in F(x)$, но h_1, h_2 в этом разложении определены не однозначно. Рассмотрим деление с остатком h_1 на $g_1 \Rightarrow$

$$h_1 = g_1 u_1 + f_1, \deg f_1 < \deg g_1 \Rightarrow$$
$$f = g_1 h_2 + g_2(g_1 u_1 + f_1) = g_1(h_2 + g_2 u_1) + g_2 f_1 = g_1 f_2 + g_2 f_1$$
$$\deg f_1 < \deg g_1, g_1 f_2 = f - g_2 f_1$$

Степени:

$$\deg g_1 + \deg f_2 \leqslant \max(\deg f, \deg g_2 + \deg f_1)$$
$$\deg g_1 + \deg f_2 \leqslant \deg f_1 + \deg g_2 \Rightarrow$$
$$\deg f_2 \leqslant \deg g_2 + (\deg f_1 - \deg g_1) \Rightarrow$$
$$\deg f_2 < \deg g_2 \Rightarrow \frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2}$$

и каждое из слогаемых - правильная дробь. ◀

Лемма 1.17.2. Любая правильна дробь является суммой примарных дробей, то есть таких, у котрых старший коэффициент равен еденице, $g = q_1^{a_1} \cdot \ldots \cdot q_k^{a_k}$, где каждая q — неприводимая, попарно не ассоциируемые, со старшем коэффициентом равным еденице. $\frac{f}{g} = \frac{f_1}{q_1^{a_1}} + \cdots + \frac{f_k}{q_k^{a_k}}$ Все слогаемые примарные.

▶ Докажем по индукции:

База: Для $k = 1$ $\frac{f}{g} = \frac{f_1}{q_1^{a_1}}$ и $\deg f < \deg g$ так как дробь правильная

Переход: Пусть для $k >= 2$ и для $k-1$ утверждение доказано, тогда

$\frac{f}{g} = \frac{f}{q_1^{a_1} \cdot \ldots \cdot q_k^{a_k}}$, обозначим первые $k-1$ множетели как g_1

и соответственно $g_2 = g_k^{a_k}$. Тогда докажем, что g_1 и g_2 взаимнопросты:

Так как g не ассоциирумое $\Rightarrow \gcd(g_1, g_2) = 1 \Rightarrow$

$$\frac{f}{g} = \frac{f_{k-1}}{q_1^{a_1} \cdot \ldots \cdot q_{k-1}^{a_{k-1}}} + \frac{f_k}{q_k^{a_k}}$$

обе дроби правильные $\frac{f_k}{q_k^{a_k}}$ — примарная и по инукционному предположению $\frac{f_{(k-1)}}{q_1^{a_1} \cdot \ldots \cdot q_{(k-1)}^{a_{(k-1)}}}$

можем разложить в сумму примарных дробей

◀

Лемма 1.17.3. Любая примарная дробь есть сумма простейших

$$g = q^a, \frac{f}{g} : \deg f < \deg g \Rightarrow$$

$$\frac{f}{g} = \frac{f_1}{q^1} + \cdots + \frac{f_k}{q^a}$$

и для всех f_i верно: $\deg f_i < \deg q$

▶ Докажем по индукции, по степени a:

База: Для $a = 1 \Rightarrow \frac{f}{g} = \frac{f_1}{q^1}$ $\deg f < \deg g = \deg q \Rightarrow \frac{f}{g}$ - простая.

Переход: Пусть для $a >= 2$ и для $a-1$ утверждение верно, тогда $\frac{f}{g} = \frac{f_k}{q^a} \Rightarrow$

По теореме о делении с остатком (f на q):

$$f = uq + f_a, \deg f_a < \deg q \Rightarrow$$

$$\frac{f}{g} = \frac{uq + f_a}{q^a} = \frac{u}{q^{a-1}} + \frac{f_a}{q^a}$$

$\Rightarrow \frac{f_a}{q^a}$ - простейшая

Осталось проверить, что $\frac{u}{q^{(a-1)}}$ - правильная дробь

Опять применим "трюк"сравнение степеней:

$$uq = f - f_a \Rightarrow \deg u + \deg q \leqslant max(\deg f, \deg f_a)$$

так как $\deg f < \deg q^a$ и $\deg f_a < \deg q \Rightarrow$

$$\deg u + \deg q < \deg(q^a) \Rightarrow \deg u < \deg q^{a-1}$$

$\Rightarrow \frac{u}{q^{a-1}}$ - правильная дробь $\Rightarrow$ Индукционный переход совершон.

◀

◀

Замечание 1.17.2. $f = f_1 g^{a-1} + f_2 g^{a_2} + \cdots + f_{k-1} g + f_k$, $\deg f_i < \deg g$, разложение единственным оброзом.

Алгоритм нахождения:

Пусть f_k остаток при деление f на g и так дале. $(f = ug + f_k = (u_1 g + f_{k-1})$

Теорема 1.17.2. Единственность представления.

▶ Пусть существует два разложения:

$$\frac{f}{g} = h + \sum_{i=1}^{k} \sum_{j=1}^{a_k} \frac{f_{ij}}{q_i^j} = \bar{h} + \sum_{i=1}^{k} \sum_{j=1}^{a_k} \frac{\bar{f_{ij}}}{q_i^j}$$

При этом $\deg f_{ij} < \deg q_i$

Хотим доказать, что $h = \bar{h}, f_{ij} = \bar{f_{ij}}$

$n = a_1 + \cdots + a_k$

Индукция по n Докажем по индукции:

База: Для $n = 0$ $h = \bar{h}$ очевидно

Переход: Пусть для $n \geqslant 1$ и для $n - 1$ уже доказанно

$\Rightarrow$ Существует такое $a_i > 0$ (НУО $a_k > 0$)

$\Rightarrow$ Домножим $h + \sum_{i=1}^{k} \sum_{j=1}^{a_k} \frac{f_{ij}}{q_i^j}$ на $q_1^{a_1} \cdot \ldots \cdot q_k^{a_k}$ и рассмотрим разность:

$$0 = h - \bar{h} + \sum_{i=1}^{k} \sum_{j=1}^{a_k} \frac{f_{ij} - \bar{f_{ij}}}{q_i^j}$$

Домножем на общий знаменатель $\Rightarrow$

$$0 = q_k(\ldots) + (f_{ka_k} - \bar{f_{ka_k}})(q_1^{a_1} \cdot \ldots \cdot q_{k-1}^{a_{k-1}})$$

$\Rightarrow$ последние слогаемое делится на q_k, но $q_1^{a_1} \cdot \ldots \cdot q_{k-1}^{a_{k-1}}$ взаимно прост с $q_k \Rightarrow f_{ij} - \bar{f_{ij}}$ делится на q_k, но

$$\deg(f_{ka_k} - \bar{f_{ka_k}}) \leqslant max(\deg(f_{ka_k}), \deg(\bar{f_{ka_k}})) < \deg(q_k)$$
$$\Rightarrow f_{ka_k} - \bar{f_{ka_k}} = 0 \Rightarrow f_{ka_k} = \bar{f_{ka_k}}$$

◀

Глава 2

Линейная алгебра

2.1. Системы линейных уравнений

Def 2.1.1. n уравнений с m неизвестными. K - поле.

$$\begin{cases} \sum_{j=1}^{m} a_{ij}x_j = b_i, \quad i = 1 \dots n \\ \dots \end{cases}$$

$$a_{ij}, b_i \in K$$

Замечание 2.1.1. Более общая концепция есть в коммутативном кольце с 1

Def 2.1.2. Система — однородная , если все $b_i = 0$.

Def 2.1.3. Если у системы есть решения, то она — совместна, иначе — несовместна

Def 2.1.4. Матричный вид

$A = a_{ij}(i = 1 \dots n, j = 1 \dots m)$ матрица коэффициентов

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$$

$$B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

$AX = B$

$(A|B)$ расширенная матрица системы

Def 2.1.5. Элементарные преобразования

1. i уравнение $+=$ j уравнение $\cdot\, c(\in K)$
2. i уравнение $=$ i уравнение $\cdot\, c \neq 0(\in K)$
3. Поменять местами i уравнение и j уравнение

Замечание 2.1.2. Во 2 пункте в общем случае $c \in R^*$

Замечание 2.1.3. Преобразование 3 типа может быть выражено через первые два

1. $i \mathrel{+}= j$

2. $j \mathrel{+}= (-i)$
3. $i \mathrel{+}= j$
4. $j = -j$

Замечание 2.1.4. Система не менеят множества решений, так как новая система — следствие старой и есть обратное преобразование

Def 2.1.6. Обратное преобразование

1. i уравнение $\mathrel{+}=$ j уравнение $\cdot (-c)(\in K)$
2. i уравнение $=$ i уравнение $\cdot c^{-1}(\in K)$
3. Поменять местами i уравнение и j уравнение

Def 2.1.7. Элементарные преобразования в матричной форме

1. умножить слева на
$$\begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & c_{ij} & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$
2. умножить слева на
$$\begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & c_{ii} & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$
3. умножить слева на
$$\begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0_{ii} & \cdots & 1_{ij} & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1_{ji} & \cdots & 0_{jj} & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

Def 2.1.8. Ступенчатый вид матрицы

1. все ненулевые строки (имеющие по крайней мере один ненулевой элемент) располагаются над всеми чисто нулевыми строками;
2. ведущий элемент (первый ненулевой элемент строки при отсчёте слева направо) каждой ненулевой строки располагается строго правее ведущего элемента в строке, расположенной выше данной.

Def 2.1.9. Приведенный ступенчатый вид матрицы — такой ступенчатый вид, корый удовлетворяет дополнительному условию, что каждый ведущий элемент ненулевой строки - это единица, и он является единственным ненулевым элементом в своём столбце.

Def 2.1.10. Приведение матрицы к ступенчатому виду методом Гаусса

1. Прямой ход
   (a) Идём по столбцам слева направо.
   (b) Находим в текущем столбце ненулевой коэффициент(пусть он находится в строчке i), если такого не находится, то переходим к следующему столбцу и итерации
   (c) Меняем местами i строчку и 1 строчку
   (d) Пусть мы находимся сейчас на j столбце, тогда из каждой k строки вычитаем первую строку с коэффициентом $\frac{a_{kj}}{a_{1j}}$.
   (e) В точке $(1; j)$ получили начало новой ступеньки
   (f) Мысленно отбрасываем первую строку и столбец, переходим к подматрице и следующей итерации
2. Проверка на совместность системы : пусть после i строчки ступеньки заканчиваются. Тогда в строчках $j > i$ имеем уравнения вида $0 = b_j$, если хотя бы одно b_j не равно 0, то система несовместна.
3. Обратный ход: для каждой $(i; j)$ позиции начала ступеньки из каждой $k < i$ строки вычитаем i строку с коэффициентом $\frac{a_{kj}}{a_{ij}}$
4. Получение приведенного вида : для каждой $(i; j)$ позиции начала ступеньки делим строку i на коэффициент в $(i; j)$ позиции в матрице.
5. Получение решений: пусть после i строчки ступеньки заканчиваются. Тогда имеем i уравнений вида $x_j = b_k$ (для зависимых переменных) и $m - i$ свободных переменных - им мы имеем право придавать любое значение.

Замечание 2.1.5. Если работаем над эвклидовым кольцом, то при выборе ненулевого коэффициента в очередном столбце выбираем такой с наименьшим значением эвклидовой функции среди подходящих.

2.2. Векторные пространства

Def 2.2.1. K — поле, $V \neq 0$

$$+ \colon V \times V \to V$$
$$\cdot \colon K \times V \to V$$

V — векторное пространство над полем K, если:

1. $\forall v_1, v_2, v_3 \in V \colon (v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$
2. $\exists 0 \in V \ \forall v \in V \colon 0 + v = v + 0 = v$
3. $\forall v \in V \ \exists - v \in V \colon v + (-v) = (-v) + v = 0$
4. $\forall v_1, v_2 \in V \colon v_1 + v_2 = v_2 + v_1$
5. $\forall v \in V \colon 1_K \cdot v = v$
6. $\forall a, b \in K \ \forall v \in V \colon (ab)v = a(bv)$
7. $\forall a \in K \ \forall v_1, v_2 \in V \colon a(v_1 + v_2) = av_1 + av_2$

8. $\forall a, b \in K\ \forall v \in V \colon (a+b)v = av + bv$

Пример 2.2.1. 1. $V = K$, внешнее умножение — умножение в поле K

2. K^n — пространство векторов столбцов

$$K^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mid a_i \in K \right\}$$

3. ${}^nK$ — пространство векторов строк

$${}^nK = \{(a_1 \dots a_n) \mid a_i \in K\}$$

4. $K \subseteq L$, K — поле, L — тело

$$\cdot \colon K \times L \to L \text{ (сужение умножения в } L)$$

$\mathbb{C}$ — векторное пространство над $\mathbb{R}$

5. $\mathbb{H}$ — векторное пространство над $\mathbb{R}$

6. $\mathbb{H}$ — векторное пространство над $\mathbb{C}$

7. $Q(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ — векторное пространство над $\mathbb{Q}$
$\mathbb{R}$ — векторное пространство над $\mathbb{Q}$

8. $M(n, m, k)$ — векторное пространство над K

9. $$\cdot \colon K \times K[x] \to K[x] \text{ (сужение обычного умножения)}$$
$K[x]$ — векторное пространство над K

10. $C([a, b] \to \mathbb{R})$ — векторное пространство над $\mathbb{R}$

Свойства векторного пространства

1. 0_v — единственный
▶ $v + 0_1 = v = v + 0_2$ ◀

2. $\forall a \in K \colon a \cdot 0_v = 0_v$
▶ $a \cdot 0_v = a \cdot (0_v + 0_v) = a \cdot 0_v + a \cdot 0_v$
$0_v = a \cdot 0_v$ ◀

3. $\forall v \in V \colon 0_k \cdot v = 0_v$
▶ $0_k \cdot v = (0_k + 0_k) \cdot v = 0_k \cdot v + 0_k \cdot v$ ◀

4. $\forall a \in K\ \forall v \in V \colon (-a) \cdot v = a \cdot (-v) = -(a \cdot v)$
▶ $av + (-a)v = (a + (-a))v = 0_k \cdot v = 0_v$
$-(av) = (-a)v$
2-е равенство аналогично ◀

2.3. Подпространства, линейные комбинации

Def 2.3.1. $v_1, \dots, v_n \in V, a_1, \dots, a_n \in K$

$$a_1v_1 + \dots + a_nv_n \text{— линейная комбинация } v_i \text{ с коэфициентами } a_i$$

Def 2.3.2. $i \in I, v_i \in V, a_i \in K$, почти все (= все, кроме конечного числа) a_i равны 0

$$\sum_{i\in I} a_iv_i \text{— линейная комбинация (сумма конечна, так как почти все } a_i = 0)$$

Def 2.3.3. V — векторное пространтсво над K, $0 \neq U \subseteq V$

U называют подпространством в V, если U— векторное пространство над K относительно $+|_{U\times U}, \cdot|_{K}$

Пример 2.3.1. 1. $\mathbb{C} \subseteq \mathbb{H}$, векторное пространство над $\mathbb{R}$

2. $K[x^2] \subseteq K[x]$

3. $\mathbb{R}[x]$ — можно рассматривать, как подпространство в $C([a,b] \to \mathbb{R})$

Утверждение 2.3.1. V — векторное пространство над K, $0 \neq U \subseteq V$

$$U\text{— подпространство } V \Leftrightarrow \begin{cases} U \text{ замкнуто относительно сложения} \\ U \text{ замкнуто относительно умножения на скаляр} \end{cases}$$

▶ Посмотрим на пункты из определения векторного пространства. $1, 4, 5, 6, 7, 8$ — очевидны. Рассмотрим остальные:

2. $\exists 0 \in K\ \forall u \in U : 0_k \cdot u \in U$
   $0_v = 0_k \cdot u = 0_u$
3. $\forall u \in U : (-1_k) \cdot u \in U$
   $(-1_k) \cdot u = -u \in V$, а значит обратный в U

◀

Лемма 2.3.1. (Упражнение) Пересечение подпространств - подпространство.

Утверждение 2.3.2. $\{v_i\}_{i\in I} \subseteq V$, какое наименьшее подпространство, содержащее это семейство векторов? Ответ:

$$\bigcap_{\substack{U\text{— подпространство. } V \\ \{v_i\}_{i\in I} \subseteq U}} U = \left\{ \sum_{i\in I} a_iv_i \mid \text{почти все} a_i = 0 \right\} \text{— мн-во всех конечных линеных комбинаций векторов из } \{v_i\}_{i\in I}$$

Def 2.3.4. $\{v_i\}_{i\in I}$ — семейство образующих

Def 2.3.5. $\langle v_i \mid i \in I\rangle$ — подпространство, порожденное семейством $\{v_i\}_{i\in I}$ (линейная оболочка векторов v_i)

Def 2.3.6. Если $V = \langle v_i \mid i \in I\rangle$, то говорят, что семейство образующих порождает пространство V

Пример 2.3.2. 1. $\mathbb{C}$ — векторное пространство над $\mathbb{R}, \mathbb{C} = \langle 1, i\rangle$

2. $K[x] = \langle 1, x, x^2, \dots\rangle$

2.4. Линейная зависимость и линейная независимость

Def 2.4.1. $\{v_i\}_{i\in I}$ — линейно зависимые, если $\exists a_i$ — почти все (но не все) $a_i = 0$, такие что:

$$\sum_{i\in I} a_i v_i = 0$$

Def 2.4.2. Если $\{v_i\}_{i\in I}$ не являются линейно зависимыми, то они называются линейно независимыми.

Эквивалентные определения

1. $\forall a_i$ почти все (но не все) $a_i = 0$: $\sum\limits_{i\in I} a_i v_i \neq 0$
2. $\forall a_i$ почти все $a_i = 0$: $\sum\limits_{i\in I} a_i v_i = 0 \Rightarrow$ все $a_i = 0$

Пример 2.4.1. $\mathbb{C}$ — в.п. над $\mathbb{R}$

1. $\{1, i\}$ — линейно независимые
2. $\{1, 1+i, i\}$ — линейно зависимые
   $1 \cdot 1 + (-1)\cdot(1+i) + 1 \cdot i = 0$
3. $\{1, x, x^2, \dots\}$ — линейно независимые ($K[x]$)

Свойства линейной зависимости и линейной независимости

1. Любая подсистема линейно независимой системы — лининейно независима
2. Любая надсистема линейно зависимой системы — линейно зависима
3. Семейство, содержащее 0 — линейно зависима
4. Семейство, содержащее 2 одинаковых вектора — линейно зависима
5. Семейство линейно независимо $\Leftrightarrow$ всякое его конечное подсемейство — линейно независимо

Лемма 2.4.1. $\{v_i\}_{i\in I}$ линейно зависимые $\Rightarrow$ один из v_i есть линейная комбинация остальных

▶ $\sum\limits_{i\in I} a_i v_i = 0$, почти все (но не все) $a_i = 0, j$: $a_j \neq 0$
$a_j v_j + \sum\limits_{\substack{i\in I\\ i\neq j}} a_i v_i = 0 \Rightarrow v_j = \sum\limits_{\substack{i\in I\\ i\neq j}} (\frac{-a_i}{a_j}) v_i$ ◀

Теорема 2.4.1. (О линейной зависимости линейных комбинаций)
V — векторное пространство над K, $v_1, \dots, v_n \in V$, $u_1, \dots, u_m \in \langle v_1, \dots, v_n\rangle$

Если $m > n$, то $u_1, \dots, u_m$ линейно зависимые

▶ $u_i = \sum\limits_{j=1}^{n} a_{ij} v_j$, $a_{ij} \in K$
$x_1, \dots, x_m = ?$
$0 = x_1 \cdot u_1 + \dots + x_m \cdot u_m = \sum\limits_{i=1}^{m} x_i u_i = \sum\limits_{i=1}^{m} x_i \sum\limits_{j=1}^{n} a_{ij} v_j = \sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n} (x_i a_{ij}) v_j = \sum\limits_{j=1}^{n}\sum\limits_{i=1}^{m} (x_i a_{ij}) v_j$
Потребуем, чтобы для $j = 1, \dots, n$: $\sum\limits_{i=1}^{m} x_i a_{ij} = 0$
Это система n линейных уравнений с m неизвестными, $m > n \Rightarrow \exists x_i$ (не все 0), являющиеся решением этой системы
$\sum\limits_{i=1}^{m} x_i u_i = \sum\limits_{j=1}^{n} 0 \cdot v_j = 0$
Так как не все $x_i = 0$, то $\{u_i\}_{i=1}^{m}$ - линейно зависимые ◀

2.5. Базис векторного пространства

Def 2.5.1. Базис векторного пространства — линейно независимая система образующих.

Теорема 2.5.1. V — векторное пространство над полем K, $\{v_\alpha\}_{\alpha\in I} \subset V$. Следующие условия равносильны:

1. $\{v_\alpha\}$ — базис V.
2. $\{v_\alpha\}$ — максимальное по включению линейно независимое семейство.
3. $\{v_\alpha\}$ — минимальное по включению семейство образующих
4. Всякий вектор $v \in V$ единственным образом представляется в виде конечной линейной комбинации векторов из $\{v_\alpha\}$
5. Всякий $v \in V$ раскладывается в виде конечной линейной комбинации векторов из $\{v_\alpha\}$ и нулевой вектор раскладывается единственным образом (то есть с нулевыми коэффициентами).

▶ **1 ⇒ 2:** Так как $\{v_\alpha\}_{\alpha\in I}$ — базис, то это линейно независимое семейство. Рассмотрим $v \in V$ и $\{v_\alpha\}_{\alpha\in I} \cup \{v\}$. Надо проверить, что это семейство линейно зависимо $\forall v$.

$$v = \sum_{\alpha\in I} a_\alpha v_\alpha$$

и почти все коэффициенты $a_\alpha = 0$ (так как $\{v_\alpha\}_{\alpha\in I}$ — базис).

$$0 = -v + \sum_{\alpha\in I} a_\alpha v_\alpha$$

Нетривиальная линейная комбинация и почти все коэффициенты равны нулю, поэтому вектора $\{v\} \cup \{v_\alpha\}_{\alpha\in I}$ — линейно зависимы.

2 ⇒ 1: $\{v_\alpha\}$ — максимальное линейно независимое семейство.
Необходимо проверить, что $\{v_\alpha\}$ — семейство образующих. $v \in V$, $\{v\} \cup \{v_\alpha\}$ — линейно зависимы, поэтому существует линейная комбинация, равная нулю, и v входит в нее с ненулевым коэффициентом.

$$av + \sum_{\alpha\in I} a_\alpha v_\alpha = 0$$

и почти все $a_\alpha = 0$, $a \neq 0$.

$$v = \sum_{\alpha\in I} (-a^{-1}a_\alpha) v_\alpha$$

В силу произвольности v $\{v_\alpha\}$ — семейство образующих, следовательно, базис.

1 ⇒ 3: v_α — базис, следовательно, семейство образующих. Необходимо проверить, что оно минимальное по включению.
$v \in \{v_\alpha\}, v = v_{\alpha_0}, \alpha_0 \in I$. Пусть

$$\{v_\alpha\}_{\alpha\in I\setminus\{\alpha_0\}}$$

— семейство образующих. Тогда

$$v_{\alpha_0} = \sum_{\alpha\neq\alpha_0} a_\alpha v_\alpha$$

Получили

$$0 = -v_{\alpha_0} + \sum_{\alpha\neq\alpha_0} a_\alpha v_\alpha$$

и почти все $a_\alpha = 0$. Это противоречие с линейной независимостью $v_{\alpha_{\alpha\in I}}$. Тогда $\{v_\alpha\}$ — минимальное по включению.

3 ⇒ 1: $\{v_\alpha\}$ — минимальное по включению семейство образующих. Хотим проверить, что $\{v_\alpha\}$ — линейно независимые.

Пусть линейно зависимые. Тогда $\sum_{\alpha\in I} a_\alpha v_\alpha = 0$, почти все, но не все $a_\alpha = 0$. $\exists\alpha_0 : a_\alpha \neq 0$. Тогда v_{α_0} — (конечная) линейная комбинация остальных векторов, поэтому

$$\{v_\alpha\}_{\alpha\in I\setminus\alpha_0}$$

— тоже семейство образующих.

$$v_{\alpha_0} = \sum_{\alpha\in I\neq\alpha_0} a_\alpha v_\alpha$$

почти все $a_\alpha = 0$. $u \in V$,

$$u = \sum_{\alpha\in I} b_\alpha v_\alpha$$

почти все $b_\alpha = 0$.

$$\begin{aligned} u &= \sum_{\alpha\neq\alpha_0} b_\alpha v_\alpha + b_{\alpha_0} v_{\alpha_0} = \\ &= \sum_{\alpha\neq\alpha_0} b_\alpha v_\alpha + \sum_{\alpha\neq\alpha_0} b_{\alpha_0} a_\alpha v_\alpha = \\ &= \sum_{\alpha\neq\alpha_0} (b_{\alpha+b_{\alpha_0}a_\alpha}) v_\alpha \end{aligned}$$

Почти все коэффициенты равны 0, противоречие с минимальностью. Значит $\{v_\alpha\}$ — линейно независимы, значит базис.

5 — переформулировка пункта 1. Рассмотрим $\{v_\alpha\}$. Утверждение, что всякий $v \in V$ — (конечная) линейная комбинация $\{v_\alpha\}_{\alpha\in I}$, равносильно утверждению, что $\{v_\alpha\}$ — семейство образующих.

Утверждение, что 0_v представим только в виде тривиальной линейной комбинации $\{v_\alpha\}$ равносильно тому, что $\{v_\alpha\}$ — линейно независимы.

4 ⇒ 5: 4 — более сильное условие.

5 ⇒ 4: $v \in V$ Пусть

$$v = \sum_{\alpha\in I} a_\alpha v_\alpha = \sum_{\alpha\in I} b_\alpha v_\alpha$$

почти все a_α, b_α равны 0. Тогда:

$$\sum_{\alpha\in I} (a_\alpha - b_\alpha) v_\alpha = 0$$

почти все $a_\alpha - b_\alpha = 0$. Тогда $\forall\alpha, a_\alpha = b_\alpha$.

◀

Пример 2.5.1. **Базис в K^n:**

$$e_i = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}$$

Единичный вектор — на i-й строчке стоит 1, все остальные 0.

$$\sum_{i=1}^{n} a_i e_i = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

$e_1, e_2, \dots, e_n$ — стандартный базис.

Базис в K^3:

$$\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}$$

Так же базис в K^3.

$M(n \times m, K)$**:** Стандартные матричные единицы.

$$e_{ij} = \begin{pmatrix}0 & \cdots & 0 & \cdots & 0\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ 0 & \cdots & 1_{ij} & \cdots & 0\\ \vdots & \ddots & \vdots & \ddots & \vdots\\ 0 & \cdots & 0 & \cdots & 0\end{pmatrix}$$

В $K[x]$**:** $\{1, x, x^2, \cdots\}$ — базис.

Упражнение:

$$P_i(x) \in K[x]; i = 0, 1, \dots; \deg P_i = i$$

Докажите, что $\{P_i\}$ — базис $K[x]$ над K.

Теорема 2.5.2. V — векторное пространство над K. Тогда в V есть базис.

Def 2.5.2. V — конечнопорожденное(конечномерное) если в нем есть конечная система образующих.

▶ Докажем теорему для конечнопорожденных пространств.

Лемма 2.5.1. V — конечнопорожденное векторное пространство. Всякое линейно независимое семейство может быть дополнено до базиса.

▶ Пусть $V = \langle u_1, u_2, \dots, u_m\rangle$, V порожден данными векторами, то есть это система образующих. $\{v_\alpha\}$ — линейно независимо. Попробуем дополнить $\{v_\alpha\}$ до базиса.

Пусть существует $v \in V \setminus \langle v_\alpha \mid \alpha \in I\rangle$, то есть существует вектор, который нельзя получить с помощью нашего множества. Добавим его в множество и оно останется линейно независимым. $\{v\} \cup \{v_\alpha\}_{\alpha\in I}$.

Число векторов в линейно независимом семействе не более m. Все v являются линейными комбинациями $u_1, \dots, u_m$. Если число векторов больше m, то они линейно зависимы (теорема о линейной зависимости линейной комбинации). Таким образом процесс оборвется за конечное число шагов. ◀

Первое доказательство. Возьмем любое линейно независимое множество и дополним его до базиса. ◀

▶

Лемма 2.5.2. V — конечнопорожденное векторное пространство. Из всякой конечной системы образующих можно выбрать базис.

▶ $u_1, \dots, u_m$ — семейство образующих.

Если они линейно независимые, то базис найден. Если линейно зависимы, то один из них есть линейная комбинация остальных. Значит $\{u_1, \dots, u_m\} \setminus \{u_j\}$ — тоже семейство образующих. Так как исходное семейство конечно, то процесс оборвется. Значит найдем базис. ◀

Второе доказательство. Есть семейство образующих, применим лемму. ◀

Пример 2.5.2. $\mathbb{R}$ — векторное пространство над $\mathbb{Q}$. Базис $\mathbb{R}$ над $\mathbb{Q}$ есть, но уже несчетный.

Теорема 2.5.3. Любые два базиса конечнопорожденного векторного пространства содержат одно и то же число элементов.

▶ Из теоремы о линейной зависимости линейных комбинаций следует, что всякий базис конечен.
V — векторное пространство. $u_1, \dots, u_m$ и $v_1, \dots, v_n$ — базисы V.
$u_1, \dots, u_m$ — образующие V, $v_1, \dots, v_n$ — линейно независимые и линейные комбинации векторов $u_1, \dots, u_m$. По теореме о линейной зависимости линейных комбинаций $n \leqslant m$, аналогично $m \leqslant n$. Значит $n = m$. ◀

Def 2.5.3. Если V — конечнопорожденное векторное пространство, то число векторов в базисе называется размерностью V над K.

$$\dim \quad \dim_K V$$

Если векторное пространство не является конечнопорожденным, то $\dim V = \infty$.

Пример 2.5.3.
1. $\dim_K K^n = n$
2. $\dim_K M(n \times m, K) = nm$
3. $\dim_K K[x] = \infty$
4. $\dim_K \{g \in K[x] \mid \deg g \leqslant n \in \mathbb{N}_0\} = n + 1$
5. $\dim_{\mathbb{R}} \mathbb{C} = 2$ $(1, i)$
6. $\dim_{\mathbb{R}} \mathbb{H} = 4$ $(1, \mathbb{i}, \mathbb{j}, \mathbb{k})$
7. $\dim_{\mathbb{C}} \mathbb{H} = 2$ $(1, \mathbb{j})$

$AX = 0$, множество решений — векторное пространство. Размерность пространства решений равно числу свободных переменных.

2.6. Координаты вектора. Матрица перехода. Замена координат.

Def 2.6.1. K — поле, V — вектороное пространство над K.
$\{v_\alpha\}_{\alpha \in I}$ — базис V.

$$v \in V \Rightarrow v = \sum_{\alpha \in I} a_\alpha v_\alpha$$

почти все $a_\alpha = 0$ и такое разложение единственно. $\{a_\alpha\}_{\alpha \in I}$ — набор координат вектора v в базисе $\{v_\alpha\}$.

Def 2.6.2. $\dim V = n < +\infty$, $v_1, \dots, v_n$ — базис V. $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ — столбец координат v в базисе $v_1, \dots, v_n$.

Пример 2.6.1. $\mathbb{C}$ над $\mathbb{R}$. Базис — $\{1, i\}$

$$z \mapsto \begin{pmatrix} \operatorname{Re} z \\ \operatorname{Im} z \end{pmatrix}$$

Def 2.6.3. $\{v_1, \dots, v_n\}$, $\{v'_1, \dots, v'_n\}$ — базисы V.

$$v'_j = \sum_{i=1}^{n} a_{ij} v_i, a_{ij} \in K$$

$$A = (a_{ij})_{i,j=1,\dots n}$$

j-й столбец A — столбец координат v'_j в базисе v_i.

A — матрица перехода от $v_1, \dots, v_n$ к базису $v'_1, \dots, v'_n$

$$A = [A]_{\{v_i\} \to \{v'_i\}}$$

Пример 2.6.2. $\mathbb{R}^2$, рассмотрим стандартный базис и базис повернутый на угол φ.

$$v'_1 \to \begin{pmatrix} \cos\varphi \\ \sin\varphi \end{pmatrix}$$
$$v'_2 \to \begin{pmatrix} -\sin\varphi \\ \cos\varphi \end{pmatrix}$$
$$A = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

Теорема 2.6.1. V — векторное пространство над K, $\dim V = n$,
$\{v_1, \dots, v_n\}$, $\{v'_1, \dots, v'_n\}$, $\{v''_1, \dots, v''_n\}$ — базисы V. A — матрица перехода $\{v_i\} \to \{v'_i\}$, B — матрица перехода $\{v'_i\} \to \{v''_i\}$, C — матрица перехода от $\{v_i\} \to \{v''_i\}$. Тогда $C = A \cdot B$.

▶

$$v''_j = \sum_{i=1}^{n} c_{ij} v_i$$
$$v''_j = \sum_{r=1}^{n} b_{rj} v'_r \qquad = \sum_{r=1}^{n} b_{rj} \left(\sum_{i=1}^{n} a_{ir} v_i \right) =$$
$$= \sum_{r=1}^{n} \sum_{i=1}^{n} (b_{rj} a_{ir}) v_i \qquad = \sum_{r=1}^{n} \sum_{i=1}^{n} a_{ir} b_{rj} v_i =$$
$$= \sum_{i=1}^{n} \underbrace{\left(\sum_{r=1}^{n} a_{ir} b_{rj} \right)}_{c_{ij}} v_i \qquad \Rightarrow c_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj}$$
$$C = AB$$

◀

Следствие 2.6.1.1. Матрица перехода от базиса к базису является обратимой и обратная к ней — это матрица перехода от $\{v'_i\}$ к $\{v_i\}$.

▶

$$\{v_i\} \underbrace{\rightrightarrows}_{A} \{v'_i\} \underbrace{\rightrightarrows}_{B} \{v_i\}$$

$A \cdot B$ — матрица перехода от $\{v_i\}$ к $\{v_i\}$.

$$v_i = 0 \cdot v_1 + \dots + 1 \cdot v_i + \dots + 0 \cdot v_n$$

т.е. единичная матрица. $AB = E \wedge BA = E \Rightarrow B = A^{-1}$ ◀

Пример 2.6.3. $\mathbb{R}^2$, стандартный базис и базис повернутый на φ. Матрица перехода от $\{v'_1, v'_2\}$ к $\{v_1, v_2\}$:

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}^{-1} = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix}$$

Получили поворот на $-\varphi$.

Теорема 2.6.2. V — векторное пространства над K. $v_1, \dots, v_n$, $v'_1, \dots, v'_n$ — базисы V. $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ — координаты v в базисе $\{v_1, \cdots, v_n\}$, $\begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix}$ — координаты v в базисе $\{v'_1, \cdots, v'_n\}$. Тогда

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = A \cdot \begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix}$$

▶

$$v = \sum_{i=1}^{n} b_i v_i$$

$$v = \sum_{j=1}^{n} b'_j v'_j = \sum_{j=1}^{n} b'_j \left(\sum_{i=1}^{n} a_{ij} v_i \right) = \sum_{i=1}^{n} \underbrace{\left(\sum_{j=1}^{n} a_{ij} b'_j \right)}_{b_i} v_i$$

$$b_i = \sum_{j=1}^{n} a_{ij} b'_j$$

◀

2.7. Сумма и пересечение подпространств

Теорема 2.7.1. V — векторное пространство над K, $U, W < V$. Тогда

1. $U \cap W < V$ (упражнение).
2. $$U + W = \{u + w \mid u \in U, w \in W\}$$ $$U + W < V$$

Объединение подпространством быть не обязано.

▶ Достаточно проверить замкнутость относительно операций.

$$(\underbrace{u}_{\in U} + \underbrace{w}_{\in W}) + (\underbrace{u'}_{\in U} + \underbrace{w'}_{\in W}) = (\underbrace{u + u'}_{\in U}) + (\underbrace{w + w'}_{\in W}) \in U + W$$

$$c(\underbrace{u}_{\in U} + \underbrace{w}_{\in W}) = \underbrace{cu}_{\in U} + \underbrace{cw}_{\in W} \in U + W$$

$$U + W \neq \emptyset$$

$$0_v = 0_u + 0_w \in U + W$$

◀

Теорема 2.7.2. Пусть в обозначениях выше $\dim U = n < \infty$, $\dim W = m < \infty$ Тогда $U+W$ и $U \cap W$ конечномерны и

$$\dim(U + W) + \dim(U \cap W) = \dim U + \dim W$$

▶

$$U \cap W < U \quad U \cap W < W$$

Так как $\dim U < \infty$, то и $\dim(U \cap W) < \infty$.
$v_1, \dots, v_r$ — базис $U \cap W$. $\{v_1, \dots, v_r\} < U$, дополним до базиса U:

$$\{v_1, \dots, v_r, u_{r+1}, \dots, u_n\} \quad n = \dim U$$

Аналогично дополним до базиса W:

$$\{v_1, \dots, v_r, w_{r+1}, \dots, w_m\} \quad m = \dim W$$

Утверждаем, что

$$v_1, \dots, v_r, u_{r+1}, \dots, u_n, w_{r+1}, \dots, w_m$$

— базис $U + W$.

$$v \in U + W$$
$$v = u + w, u \in U, w \in W$$
$$u = \sum_{i=1}^{r} a_i v_i + \sum_{i=r+1}^{n} b_i u_i$$
$$w = \sum_{i=1}^{r} c_i v_i + \sum_{i=r+1}^{m} d_i w_i$$
$$v = \sum_{i=1}^{r} (a_i + c_i) v_i + \sum_{i=r+1}^{n} b_i u_i + \sum_{i=r+1}^{m} d_i w_i$$

Таким образом, это — система образующих $U + W$. Проверим линейную независимость.

$$\sum_{i=1}^{r} a_i v_i + \sum_{i=r+1}^{n} b_i u_i + \sum_{i=r+1}^{m} c_i w_i = 0$$
$$v = \underbrace{\sum_{i=1}^{r} a_i v_i + \sum_{i=r+1}^{n} b_i u_i}_{\in U} = \underbrace{- \sum_{i=r+1}^{m} c_i w_i}_{\in W}$$
$$v = U \cap W \Rightarrow v = \sum_{i=1}^{r} d_i v_i = \sum_{i=1}^{r} d_i v_i + \sum_{i=r+1}^{n} 0 u_i$$

$\{v_i, u_i\}$ — базис U, следовательно разложение должно быть единственным, значит $b_i = 0$.

$$\sum_{i=1}^{n} a_i v_i + \sum_{i=r+1}^{m} c_i w_i = 0$$

$\{v_i, w_i\}$ — базис W, значит $a_i = 0$ и $c_i = 0$.
Таким образом, $v_1, \dots, v_r, u_{r+1}, \dots, u_n, w_{r+1}, \dots, w_m$ — линейно независимы, а значит они — базис $U + W$.

$$\dim(U + W) + \dim(U \cap W) = r + (n - r) + (m - r) + r = n + m = \dim(U) + \dim(W)$$

◀

2.8. Линейные отображения

Def 2.8.1. U, V — векторные пространства над K. $f\colon U \to V$ называется линейным отображением, если

$$\forall u_1, u_2 \in U, c_1, c_2 \in K, f(c_1u_1 + c_2u_2) = c_1f(u_1) + c_2f(u_2)$$

— линейность.

Замечание 2.8.1.
- $\forall u_1, u_2 \in U, f(u_1 + u_2) = f(u_1) + f(u_2)$ — адитивность.
- $\forall c \in K, \forall u \in U, f(cu) = cf(u)$ — однородность степени 1.

Def 2.8.2. $f\colon U \to V$ — линейное отображение. $f(U) = \mathrm{Im}(F)$ — образ f.

$$f^{-1}(0_v) = \{u \in U \mid f(u) = 0_v\} = \ker f$$

— ядро f.

Упражнение:

$$\mathrm{Im}\, f < V \quad \ker f < U$$

Следствие 2.8.0.1. Свойства линейного отображения

1. $f(0_u) = 0_v$
2. $f(0_k u) = 0_k f(u) = 0_v$: ядро не пусто (всегда содержит ноль).

Лемма 2.8.1. $f\colon u \to v$ — линейное отображение.

$$f \text{ — инъективно} \Leftrightarrow \ker f = \{0_u\}$$

▶ **⇒:** f — инъективно.

$$\forall x \in V\, |f^{-1}(V)| \leqslant 1 \Rightarrow |f^{-1}(0)| \leqslant 1$$

но $0 \subset f^{-1}(0) \Rightarrow \ker f = \{0\}$

⇐:

$$u_1, u_2 \in U : f(u_1) = f(u_2)$$
$$f(u_1 - u_2) = f(u_1) - f(u_2) = 0$$
$$u_1 - u_2 \in \ker f = \{0\} \Rightarrow u_1 = u_2$$

В силу произвольности u_1 и u_2, f инъективно.

◀

Def 2.8.3. U, V — векторные пространства над K. $f\colon U \to V$ — изоморфизм, если

1. f — линейное отображение.
2. f — биекция.

Говорим, что U и V изоморфны: $U \cong V$.

Замечание 2.8.2. Линейное отображение $f\colon U \to V$ — изоморфизм, если

1. $\ker f = \{0\}$
2. $\mathrm{Im}\, f = f(U) = V$

Def 2.8.4. U, V — векторное пространство. $Hom(U,V)$, $\mathcal{L}(U,V)$ — пространство линейных отображений из U в V.

Теорема 2.8.1. $\mathcal{L}(U,V)$ — векторное пространство над K:
$f, g \in \mathcal{L}(U,V)$

$$\forall u \in U, (f+g)(u) = f(u) + g(u)$$
$$(\alpha f)(u) = \alpha f(u)$$

$f+g, \alpha f$ — линейные отображения.

▶

$$\begin{aligned}(f+g)(\beta_1 u_1 + \beta_2 u_2) &= f(\beta_1 u_1 + \beta_2 u_2) + g(\beta_1 u_1 + \beta_2 u_2) = \\ &= \beta_1 f(u_1) + \beta_2 f(u_2) + \beta_1 g(u_1) + \beta_2 g(u_2) = \\ &= \beta_1 (f(u_1) + g(u_1)) + \beta_2 (f(u_2) + g(u_2)) = \\ &= \beta_1 (f+g)(u_1) + \beta_2 (f+g)(u_2) \Rightarrow f+g \in \mathcal{L}(U,V)\end{aligned}$$

◀

Когда два конечномерных векторных пространства изоморфны?

Лемма 2.8.2. $U \cong V, f : U \to V$ — изоморфизм, $\dim U < \infty$, $u_1, \cdots, u_n$ — базис U.
Тогда $f(u_1), \dots, f(u_n)$ — базис V.

▶

$$\alpha_1 f(u_1) + \cdots + \alpha_n f(u_n) = 0$$
$$f(\underbrace{\alpha_1 u_1 + \cdots + \alpha_n u_n}_{\in \ker f = \{0\}}) = 0$$

$\alpha_1 u_1 + \cdots + \alpha_n u_n = 0$ и $u_1, \dots, u_n$ — базис U, поэтому

$$\alpha_1 = \cdots = \alpha_n = 0$$

откуда $f(u_1), \dots, f(u_n)$ — линейно независимы.
Рассмотрим $v \in V$: так как f — сюръекция, то $\exists u \in U, f(u) = v$. Говорим, что U и V изоморфны $U \cong V$.

$$\exists \alpha_1, \dots, \alpha_n \in K, u = \alpha_1 u_1 + \cdots + \alpha_n u_n$$
$$v = f(u) = \alpha_1 f(u_1) + \cdots + \alpha_n f(u_n)$$

Верно, что $\forall v \in V, f(u_1), \dots, f(u_n)$ — семейство порождающих. Значит, $f(u_1), \dots, f(u_n)$ — базис V. ◀

Следствие 2.8.1.1. U, V — векторное пространство над K, конечномерное.

$$U \cong V \Leftrightarrow \dim U = \dim V$$

▶ **⇒:** Переводим базис в базис, получаем $\dim U = \dim V$.
⇐: $\dim U = \dim V$. Рассмотрим функцию $f : U \to V$: $u_1, \dots, u_n$ — базис U, $v_1, \dots, v_n$ — базис V.

$$u = \alpha_1 u_1 + \cdots + \alpha_n u_n$$
$$f(u) = \alpha_1 v_1 + \cdots + \alpha_n v_n$$

f — линейно (упражнение).
Покажем, что f сюръективно:

$$\exists \alpha_1, \dots, \alpha_n \colon v = \alpha_1 v_1 + \dots + \alpha_n v_n$$
$$v = f(\alpha_1 u_1 + \dots + \alpha_n u_n)$$

f — сюръективно.
Покажем, что f инъективно:

$$u \in \ker f = \alpha_1 u_1 + \dots + \alpha_n u_n, f(u) = 0, \alpha v_1 + \dots + \alpha_n v_n = 0$$

$v_1, \dots, v_n$ — базис V, значит $\alpha_1 = \dots = \alpha_n = 0$, откуда $\ker f = \{0\}$, и f — инъективно.

◀

Следствие 2.8.1.2. $\dim U = n \Rightarrow U \cong K^n$

▶ Фиксируем базис в U: $u_1, \dots, u_n$:

$$u = \alpha_1 u_1 + \dots + \alpha_n u_n \to \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Зависит от выбора базиса. ◀

Замечание 2.8.3. В общем случае, если два векторных пространства изоморфны, то мощность их базисов совпадает.

Замечание 2.8.4. U, V, $\{u_i\}_{i \in I}$ — базис U, $f \in \mathcal{L}(U, V)$. Тогда f полностью определяется своими значениями на базисных векторах:

$$u = \sum_{i \in I} \alpha_i u_i \quad \text{почти все } \alpha_i = 0$$
$$f(u) = \sum_{i \in I} \alpha_i f(u_i)$$

Пример 2.8.1. $U = K^n$, $V = K^m$, $A \in M(n, m, K)$. $f \colon U \to V; u \mapsto Au$. f — линейное отображение:

$$A(\alpha_1 u_1 + \alpha_2 u_2) = \alpha_1 A u_1 + \alpha_2 A u_2$$

Общая ситуация $\dim U = m$, $\dim V = n$. Фиксируем $u_1, \dots, u_m$ — базисы U, $v_1, \dots, v_n$ — базисы V

Замечание 2.8.5. Если $U = V$, то базисы могут быть различными.

$$f \in \mathcal{L}(U, V)$$

Def 2.8.5. Матрицей f в базисах $\{u_1 \dots, u_m\}$, $\{v_1, \dots, v_n\}$ называется следующая матрица $A \in M(n, m, K)$:

$$f(u_j) = \sum \alpha_{ij} v_i$$
$$A = (\alpha_{ij})_{i=1..n, j=1..m}$$

Пример 2.8.2. $\mathbb{R}^2$. Поворот на угол φ вокруг начала координат — линейное отображение.

$$u_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad u_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$f(u_1) = \begin{pmatrix} \cos\varphi \\ \sin\varphi \end{pmatrix} \quad f(u_2) = \begin{pmatrix} -\sin\varphi \\ \cos\varphi \end{pmatrix}$$

Матрица поворота на φ в этих базисах

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

Пример 2.8.3. $U = \{f \in \mathbb{R}[x] \mid \deg f \leqslant n\}$, $\dim_{\mathbb{R}} U = n+1$.

$$\frac{\mathrm{d}}{\mathrm{d}x} \colon U \to V = \{f \in \mathbb{R}[x] \mid \deg f \leqslant n-1\}$$

$$u_0 = 1, \dots, u_n = x^n$$

$$v_0 = 1, \dots, v_{n-1} = x^{n-1}$$

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & n \end{pmatrix}$$

$$A = [f]_{\{u_1,\cdots,u_m\},\{v_1,\cdots,v_n\}}$$

Замечание 2.8.6.

$$u \in U, u \to \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix}, u = \sum_{j=1}^{m} \beta_j u_j$$

$$f(u) = \sum_{i=1}^{n} \gamma_i v_i, f(u) \to \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}$$

$$\begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = A \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix}$$

$$f(u) = f\left(\sum_{j=1}^{m} \beta_j u_i\right) = \sum_{j=1}^{n} \beta_j f(u_j) = \sum_{j=1}^{m} \beta_j \sum_{i=1}^{n} \alpha_{ij} v_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \alpha_{ij}\beta_j\right) v_i$$

$$\gamma_i = \sum_{j=1}^{m} \alpha_{ij}\beta_j$$

U, V, $\dim U = m < \infty$, $\dim V = n < \infty$. Фиксируем базис. Хотим рассмотреть переход $\mathcal{L}(U,V) \to M(n,m,K)$. $f \to [f]_{\{u_j\},\{v_i\}}$ — линейное отображение.

$$[f_1 + f_2] = [f_1] + [f_2]$$

$$[\alpha f] = \alpha [f]$$

j-ый столбец $[f_1 + f_2]$ — координаты разложения $(f_1 + f_2)(u_j)$ в базисе $v_1, \dots, v_n$.

$$f_1(u_j) + f_2(u_j)$$

$$A = (\alpha_{ij})$$

$$f(u_j) = \sum_{i=1}^{n} \alpha_{ij} v_i$$

Получили отображение $f \to A$. Нулевой матрице соответствует нулевое отображение $f \colon U \to V \colon u \mapsto 0_v$.

Следствие 2.8.1.3.

$$\mathcal{L}(U,V) \cong M(n,m,K)$$

2.8.1. Матрица композиции линейных отображений

Теорема 2.8.2. $U \overset{g}{\to} V \overset{f}{\to} W$, g, f — линейные отображения, U, V, W — конечномерные. $\{u_i\}_{i=1..m}$, $\{v_i\}_{i=1..n}$, $\{w_i\}_{i=1..k}$ — базисы U, V, W.

$$[f \circ g]_{\{u_i\},\{w_i\}} = [f]_{\{v_i\},\{w_i\}}[g]_{\{u_i\},\{v_i\}}$$

▶

$$A = (a_{ij}) = [f], B = (b_{js}) = [g]$$
$$C = (c_{is}) = [f \circ g]$$
$$C = m \times k$$
$$(f \circ g)(u_s) = f(g(u_s)) = f\left(\sum_{j=1}^{n} b_{js} v_j\right) = \sum_{j=1}^{n} b_{js} f(v_j) =$$
$$= \sum_{j=1}^{n} b_{js} \sum_{i=1}^{k} a_{ij} w_i = \sum_{i=1}^{k} \left(\sum_{j=1}^{n} b_{js} a_{ij}\right) w_i = \sum_{i=1}^{k} \underbrace{\left(\sum_{j=1}^{n} a_{ij} b_{js}\right)}_{c_{is}} w_i$$
$$\Rightarrow c_{is} = \sum_{j=1}^{n} a_{ij} b_{js} \Rightarrow C = AB$$

◀

2.8.2. Преобразование матрицы линейного отображения при замене базисов

Теорема 2.8.3. U, V — конечномерные векторные пространства, $f\colon U \to V$ — линейное отображение. $\{u_1, \dots, u_m\}$, $\{u'_1, \dots, u'_m\}$ — базисы U, $\{v_1, \dots, v_n\}$, $\{v'_1, \dots, v'_n\}$ — базисы V. C — матрица перехода от $\{u_j\}$ к $\{u'_j\}$, D — матрица перехода от $\{v_i\}$ к $\{v'_i\}$, A — матрица f в базисах $\{u_j\}$, $\{v_i\}$, A' — матрица f в базисах $\{u'_j\}$, $\{v'_i\}$. Тогда

$$A' = D^{-1}AC$$

Замечание 2.8.7. $\dim U = m$, $\dim V = n$. $A, A' \in M(n, m, K)$, $C \in M(m, m, K)$, $D \in M(n, n, K)$.

▶ $A = (a_{ij})$, $A' = (a'_{ij})$, $C = (c_{js})$. D^{-1} — матрица перехода от $\{v'_r\}$ к $\{v_r\}$, $D^{-1} = (\check{d}_{ri})$.

$$f(u'_s) = \sum_r a'_{rs} v'_r$$
$$f(u'_s) = f(\sum_{j=1}^{m} c_{js} u_j) = \sum_{j=1}^{m} c_{js} f(u_j) = \sum_{j=1}^{m} c_{js} \sum_{i=1}^{n} a_{ij} v_i = \sum_{j=1}^{m} c_{js} \sum_{i=1}^{n} a_{ij} \sum_{r=1}^{n} \check{d}_{ri} v'_r =$$
$$= \sum_{r=1}^{n} \left(\sum_{j=1}^{m} \sum_{i=1}^{n} c_{js} a_{ij} \check{d}_{ri}\right) v'_r = \sum_{r=1}^{n} \left(\sum_{j=1}^{m} \sum_{i=1}^{n} \check{d}_{ri} a_{ij} c_{js}\right) v'_r$$
$$\sum_{j=1}^{m} \sum_{i=1}^{n} \check{d}_{ri} a_{ij} c_{js} = a'_{rs}$$
$$(A')_{rs} = a'_{rs} = \left(\sum_{j=1}^{m} \sum_{i=1}^{n} (\check{d}_{ri} a_{ij}) c_{js}\right) = \sum_{j=1}^{m} (D^{-1}A)_{rj} c_{js} = (D^{-1}AC)_{rs} \Rightarrow A' = D^{-1}AC$$

◀

Теорема 2.8.4. U, V — конечномерные векторные пространства над K, $\dim U = m$, $\dim V = n$, $f\colon U \to V$ — линейное отображение. Тогда существуют базисы U и V, что

$$[f] = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

E_r — единичная матрица размера r.

▶ Пусть $\dim \ker f = m - r$ для некоторого $0 \leqslant r \leqslant m$. $u_{r+1}, \dots, u_m$ — базис $\ker f$. Дополним до базиса U:

$$u_1, \dots, u_r, \underbrace{u_{r+1}, \dots, u_m}_{\text{базис } \ker f}$$

Для $i = 1..r$ возьмём $v_i = f(u_i)$. Утверждаем, что v_i — линейно независимые.

$$0 = \sum_{i=1}^{r} \alpha_i v_i = \sum_{i=1}^{r} \alpha_i f(u_i) = f\left(\sum_{i=1}^{r} \alpha_i u_i\right)$$

$$\sum_{i=1}^{r} \alpha_i u_i \in \ker f \Rightarrow \sum_{i=1}^{r} \alpha_i u_i = \sum_{i=r+1}^{m} \beta_i u_i$$

$$\sum_{i=1}^{r} \alpha_i u_i - \sum_{i=r+1}^{m} \beta_i u_i = 0$$

$u_1, \dots, u_m$ — базис U, значит α_i и β_i равны 0 и $f(u_i)$ линейно независимы. Значит $v_1, \dots, v_r$ линейно независимы.

Дополним до базиса V:

$$v_1, \dots, v_r, v_{r+1}, \dots, v_n$$
$$\forall j = 1..r, f(u_j) = v_j$$

Покажем, что для $j = 1..r$ j-ый столбец $[f]$ есть $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, а для прочих j — нулевой столбец:

$$v_j = 0v_1 + \dots + 0v_{j-1} + 1v_j + 0v_{j+1} + \dots$$
$$\forall j\colon r < j \leqslant m, f(u_j) = 0 = 0v_1 + \dots + 0v_n$$

Откуда

$$[f] = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

◀

Следствие 2.8.4.1. 1. $A \in M(n, m, K)$. Тогда существуют обратимые матрицы $C \in M(m, m, K)$ и $D \in M(n, n, K)$, что

$$D^{-1}AC = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$
$$U = K^m, V = K^n$$
$$f\colon U \to V\colon x \mapsto Ax$$

2. U, V — векторные конечномерные пространства над K. $f\colon U \to V$ — линейное отображение.

$$\dim \operatorname{Im} f + \dim \ker f = \dim U$$

▶ В обозначениях из доказательства теоремы $\dim \ker f = m - r$.

$$\operatorname{Im} f = \{f(u) \mid u \in U\} = \left\{ f\left(\sum_{j=1}^{m} \alpha_i u_j\right) \mid \alpha_i \in K \right\} =$$

$$= \left\{ \sum_{j=1}^{m} \alpha_i f(u_j) \mid \alpha_j \in K \right\} = \left\{ \sum_{j=1}^{r} \alpha_j f(u_j) \mid \alpha_j \in K \right\}$$

$$\Rightarrow \operatorname{Im} f = \langle f(u_1), \dots, f(u_r) \rangle = \langle v_1, \dots, v_r \rangle$$

Доказываем линейную независимость $v_1, \dots, v_r$: $v_1, \dots, v_r$ — базис $\operatorname{Im} f$, $\dim \operatorname{Im} f = r$.

$$\dim \operatorname{Im} f + \dim \ker f = r + m - r = m = \dim U$$

◀

2.9. Ранг матрицы

Def 2.9.1. $A \in M(n, m, K)$. Наибольшее r такое, что в A есть ненулевой минор размера r, называется рангом матрицы.

$$\operatorname{rang} A$$

Def 2.9.2. Строковый ранг A — это размерность пространства, порожденного строками A.

Def 2.9.3. Столбцовый ранг — это размерность пространства, порожденного столбцами A.

Теорема 2.9.1. Ранг матрицы, ее строковой ранг и столбцовый ранг совпадают.

Замечание 2.9.1. 1. Ранг — число ненулевых строк после приведения к ступенчатому виду.

2. Если существуют обратимые C, D, такие что

$$D^{-1}AC = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

то r — ранг.

3. Критерий разрешимости: после приведения к ступенчатому виду число ступенек равно числу ступенек расширенной матрицы (это утвержденние равносильно теореме Кронера-Каппели).

▶ Докажем, что строковый ранг и обычный совпадают. План такой:

1. Не меняется при элементарном преобразование над строками.
2. Сравним оба ранга для ступенчатых. Столбцовый ранг A равен строковому рангу A^T. У обычного ранга $A \sim A^T$.

Докажем:

1. Ранг по строкам не меняется при элементарных преобразованиях.

$$A = \begin{pmatrix} A_1 \\ A_2 \\ \dots \\ A_n \end{pmatrix}$$

$A_1, \cdots, A_n$ — строки.

$$\dim \langle A_1, \dots, A_n \rangle$$

Пространство $\langle A_1, \dots, A_n \rangle$ не меняется при элементарных преобразованиях:

(a) $A_i \leftrightarrow A_j$ (Поменять две строки местами).
(b) $A_i \to cA_i$ (Домножить строчку на константу).
(c) $A_1 \to A_i + \lambda A_j$ (Прибвить к строке другую строчку).

▶

$$v = \sum_{k=1}^{n} c_k A_k = \sum_{k\neq i,j} c_k A_k + c_i A_i + c_j A_j = \sum_{k\neq i,j} c_k A_k + c_i(A_i + \lambda A_j) + (c_j - c_i\lambda)A_j$$

◀

2. Ранг не меняестя при элементарных преобразованиях. Подробно было доказано в книге Боревича «Определители и Матрицы», страница 67.
3. Строковый ранг и обычный совпадают. Любую матрицу можно привести к степенчитаму виду.

$$A \to \begin{pmatrix} 1 & 0 & x & x & 0 & x & 0 & \cdots & x \\ 0 & 1 & x & x & 0 & x & 0 & \cdots & x \\ 0 & 0 & 0 & 0 & 1 & x & 0 & \cdots & x \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix} = B$$

Достаточно показать, что ранг и строковый ранг B совпадают. В B есть r ненулевых строк, поэтому строковый ранг не больше r:

$$0 = \lambda_1 B_1 + \cdots + \lambda_r B_r = (x, \lambda_1, x, x, \lambda_2, \dots, \lambda_r) \Rightarrow \lambda_1 = \cdots = \lambda_r = 0$$
$$\Rightarrow \dim\langle B_1, \dots, B_r, 0, \dots, 0\rangle = \dim\langle B_1, \dots, B_r\rangle = r$$

Значит, строковый ранг есть ровно r.
$\operatorname{rang} B \geqslant r$: выбираем строки $1..r$, и соответствующие им столбцы.

$$\begin{vmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{vmatrix} = 1 \neq 0$$

Если $\min\{\text{число строк } B, \text{число столбцов } B\} = r$, тогда ранг, очевидно, равен r. Иначе любая квадратная подматрица B размера $r+1$ содержит нулевую строку, значит все миноры размера $r+1$ равны 0. Тогда $\operatorname{rang} B = r$, значит строковой и обычный ранги совпадают.
4. Столбцовый ранг A равен строковому рангу A^T равен рангу A^T равен рангу A равен строковому рангу A.

◀

Следствие 2.9.1.1. Строковой ранг не меняется при элементарных преобразованиях столбцов.

Замечание 2.9.2. Из доказательства следует, что $\operatorname{rang} A$ — число ненулевых строк после приведения к ступенчатому виду.

Замечание 2.9.3. $A \in M(n, m, k)$, $f\colon K^m \to K^n\colon x \mapsto Ax$. Тогда $\operatorname{rang} A = \dim \operatorname{Im} f$, $A = (A_1, \dots, A_m)$, A_i — столбцы.

$$\operatorname{Im} f = \{Ax \mid x \in K^m\} = \left\{ A \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \mid x_i \in K \right\} =$$
$$= \{A_1 x_1 + \cdots + A_m x_m \mid x_i \in K\} =$$
$$= \{x_1 A_1 + \cdots + x_m A_m \mid x_i \in K\} = \langle A_1, \dots, A_m\rangle$$

Получили, что $\dim \operatorname{Im} f =$ столбцовый ранг $A = \operatorname{rang} A$.

Def 2.9.4. U, V — конечномерные векторные пространства над K, $f\colon U \to V$ — линейное преобразование.

$$\operatorname{rang} f = \dim \operatorname{Im} f$$
$$\operatorname{rang} f = \operatorname{rang}[f]_{\{u_1,\cdots,u_m\},\{v_1,\cdots,v_n\}}$$

Следствие 2.9.1.2.

$$\operatorname{rang}\begin{pmatrix} 1 & * \\ 0 & C \end{pmatrix} = 1 + \operatorname{rang} C$$
$$\operatorname{rang}\begin{pmatrix} 1 & 0 \\ * & C \end{pmatrix} = 1 + \operatorname{rang} C$$

2.10. Ранг произведения матриц

Теорема 2.10.1. $A \in M(n,m,K)$, $B \in M(m,l,k)$.

$$\operatorname{rang} A + \operatorname{rang} B - m \leqslant \operatorname{rang} AB \leqslant \min\{\operatorname{rang} A, \operatorname{rang} B\}$$

▶ 1.

$$A \cdot B = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \cdot \begin{pmatrix} B_1 \\ \vdots \\ B_m \end{pmatrix} = \begin{pmatrix} a_{11}B_1 + \cdots + a_{1m}B_m \\ a_{21}B_1 + \cdots + a_{2m}B_m \\ \vdots \\ a_{n1}B_1 + \cdots + a_{nm}B_m \end{pmatrix}$$

Строки произведения — это линейные комбинации строк B. Следовательно, пространство, порожденное AB, не больше пространства, порожденного строками B, и $\operatorname{rang} AB \leqslant \operatorname{rang} B$. Столбцы AB — линейная комбинация столбцов A, откуда $\operatorname{rang} AB \leqslant \operatorname{rang} A$ и

$$\operatorname{rang} AB \leqslant \min\{\operatorname{rang} A, \operatorname{rang} B\}$$

2. $f\colon K^l \to K^m\colon x \mapsto Bx$, $g\colon K^m \to K^n\colon y \mapsto Ay$.

$$[g \circ f] = A \cdot B$$
$$U = \operatorname{Im} f, h = g\big|_{\operatorname{Im} f}$$

$h\colon U \to V$ — линейное преобразование.

$$\dim \operatorname{Im} h + \dim \ker h = \dim U$$
$$\operatorname{rang} AB = \dim \operatorname{Im}(g \circ f) = \dim \operatorname{Im}\left(g\big|_{Im(f)}\right) = \dim \operatorname{Im} f - \dim \ker\left(g\big|_{\operatorname{Im} f}\right) \geqslant$$
$$\geqslant \dim \operatorname{Im} f - \dim \ker g = \dim \operatorname{Im} f - (m - \dim \operatorname{Im} g) =$$
$$= \dim \operatorname{Im} f + \dim \operatorname{Im} g - m = \operatorname{rang} A + \operatorname{rang} B - m$$

◀

2.11. Ещё раз об элементарных преобразованиях и элементарных матрицах

Элементарные матрицы:

1. Элементарная диагональная — диагональная, один элемент диагонали заменили на $c \neq 0$:

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

2. Элементарная трансвекция $E + \lambda e_{ij}$, $i \neq j$:

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

3. Элементарная транспозиция строк: берём единичную матрицу и меняем две строки местами:

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

Элементарное преобразование над строками матриц — умножение слева на элементарную матрицу нужного размера. Элементарное преобразование над столбцами матриц — умножение справа на элементарную матрицу.

Теорема 2.11.1. $A \in M(n, n, K)$, $\det A \neq 0$. Тогда A есть призведение элементарных диагональных матриц и элементарных трансвекций.

▶ Привели к ступенчатому виду (верхней треугольной матрице):

$$A \to \begin{pmatrix} 1 & 0 & * & \cdots & 0 \\ 0 & 1 & * & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} = B$$

$\det A \neq 0 \Rightarrow \det B \neq 0$, значит на диагонале B ненулевые элементы, и $B = E$.
Существует последовательность элементарных матриц $C_1, \ldots, C_k$, что

$$C_k C_{k-1} \ldots C_1 A = E$$
$$A = (C_k \ldots C_1)^{-1} = C_1^{-1} \ldots C_k^{-1}$$

Обратные к элементарным матрицам — элементарные.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & c^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$(E + \lambda e_{ij})^{-1} = E - \lambda e_{ij}$$

◀

Напоминание: $A \in M(n,m,K)$, $C \in M(m,m,K)$, $D \in M(n,n,K)$ — невырожденные матрицы.

$$D^{-1}AC = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

D, C — обратимые матрицы.

C, D^{-1} можно представить в виде произведения элементарных метриц.

Следствие 2.11.1.1. $\exists C_1, \dots, C_k, D_1, \dots, D_l$ — элементарные матрицы, что

$$D_l \dots D_1 A C_1 \dots C_k = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

Следствие 2.11.1.2. $A \in M(n,m,K)$ элементарными преобразованиями над строками и столбцами может быть приведена к виду $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$, где $r = \operatorname{rang} A$.

Что изменится, если рассмотреть $A \in M(n,m,R)$, R — евклидово кольцо?

В диагональных элементарных матрицах требуем, чтобы $c \in R^\times$, то есть можно домножать строки (столбцы) только на обратимые элементы $c \in R^\times$.

Теорема 2.11.2. $A \in M(n,m,R)$. Тогда существуют $d_1, \dots, d_r \in R \setminus \{0\}$, что $d_i \mid d_{i+1}$ и матрица A может быть приведина элементарными преобразованиями над строками и столбцами к

$$\begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \cdots & 0 \\ 0 & 0 & d_r & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

причем d_i определены однозначно с точность до ассоциативности.

Без доказательства.

2.11.1. Системы линейных уравнений над евклидовыми кольцами

Уравнение $ax + by = c$ разрешимо тогда и только тогда, когда $\gcd(a,b) \mid c$.

$A \in M(n,m,R)$, R — евклидово кольцо. B — столбец высоты n над R. Когда система $AX = B$ разрешима над R?

Def 2.11.1. $\delta_i(A)$ — НОД всех миноров порядка i матрицы системы. $\delta_i(A \mid B)$ — НОД всех миноров порядка i расширенной матрицы.

Теорема 2.11.3. В введеных обозначениях $AX = B$ разрешимо в R тогда и только тогда, когда

1. $\operatorname{rang} A = \operatorname{rang}(A \mid B)$
2. $\forall i, \delta_i(A) = \delta_i(A \mid B)$

Замечание 2.11.1. Рассмотрим линейный случай.

$$A = (a,b), \delta_1(A) = \gcd(a,b)$$
$$(A \mid B) = (a,b,c), \delta_1(A \mid B) = \gcd(a,b,c)$$
$$\gcd(a,b) = \gcd(a,b,c) \overset{a,b \neq 0}{\Longleftrightarrow} \gcd(a,b) \mid c$$

Без доказательства. Указание: δ_i не меняется при элементарных преобразованиях. Пусть привели A к почти единичному виду. $d_1 \mid ... \mid d_r$

$$\delta_1 = d_1$$
$$\delta_2 = d_1 d_2$$
$$\vdots$$
$$\delta_r = d_1 d_2 ... d_r \Rightarrow d_i = \frac{\delta_i}{\delta_{i-1}}$$

2.12. Прямая сумма векторных подпространств

Def 2.12.1. V — векторное пространство над K, $U, W \subset V$. Сумма $U + W$ называется прямой суммой, если $U \cap W = \{0\}$

$$U \oplus W$$

Теорема 2.12.1. Если пространство конечномерно, то $U+W$ — прямая сумма тогда и только тогда, когда $\dim(U + W) = \dim(U) + \dim(W)$.

Сумма $U + W$ прямая тогда и только тогда, когда всякий $v \in U + W$ единственным образом представляется в виде $v = u + w$.

▶ **⇒:** $v \in U + W$, $v = u + w = u' + w'$ $(u, u' \in U,\ w, w' \in W)$.

$$u - u' = w - w'$$
$$\begin{cases} u - u' \in U \\ w - w' \in W \end{cases} \Rightarrow \begin{cases} (u - u') \in (U \cap W) \\ (w - w') \in (U \cap W) \end{cases} \Rightarrow \begin{cases} u = u' \\ w = w' \end{cases}$$

⇐: $v \in U \cap W$.

$$v = (v \in U) + (0 \in W) = (0 \in U) + (v \in W)$$

В силу единственности $v = 0$, значит пересечение тривиально.

◀

2.13. Двойственное пространство

Def 2.13.1. V — векторное пространство над K. Двойственное пространство

$$V^* = \{\Phi \mid \Phi \colon V \to K \text{ — линейное отображение}\}$$

— множество линейных отображений из V в K (пространство над K).

Def 2.13.2. Линейное отображение $f \colon V \to K = K^1$ называется линейным функционалом. V^* — пространство линейных функционалов на V.

Замечание 2.13.1. Всякий линейный функционал полностью определяется своими значениями на базисных элементах V. Пусть $\{v_i\}_{i \in I}$ — базис V, $\Phi \in V^*$:

$$v \in V, v = \sum_{i \in I} \alpha_i v_i \quad \text{почти все } \alpha_i = 0$$
$$\Phi(v) = \Phi\left(\sum_{i \in I} \alpha_i v_i\right) = \sum_{i \in I} \alpha_i \Phi_i(v_i)$$

Пусть $\dim V = n < \infty$. Зафиксируем базис $v_1, ..., v_n$

$v_i^* \in V^*$

$$v = \sum_{i=1}^{n} \alpha_i v_i$$

$$v_i^*(v) \leftrightharpoons \alpha_i$$

$$v_i^*(v_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

Теорема 2.13.1. $\dim V = n < \infty$. В указанных выше обозначениях $v_1^*, \dots, v_n^*$ — базис V^*.

▶ $\Phi \in V^*$: $V \to K$ — линейное отображение, $\beta_i = \Phi(v_i)$. Нужно проверить, что $\Phi = \sum_{i=1}^{n} \beta_i v_i^*$:

$$\forall v \in V, \Phi(v) = \left(\sum_{i=1}^{n} \beta_i v_i^* \right)(v)$$

Достаточно проверить это равенство для $v = v_1, \dots, v_n$. $\Phi(v_j) = \beta_j$:

$$\left(\sum_{i=1}^{n} \beta_i v_i^* \right)(v_j) = \sum_{i=1}^{n} \beta_i v_i^*(v_j) = \beta_j$$

$$\forall j = 1..n, \Phi(v_j) = \left(\sum_{i=1}^{n} \beta_i v_i^* \right)(v_j) \Rightarrow$$

$$\Rightarrow \Phi = \sum_{i=1}^{n} \beta_i v_i^*$$

Получили, что $v_1^*, \cdots, v_n^*$ — семейство образующих. Необходимо проверить линейную независимость.

$$\sum_{i=1}^{n} \beta_i v_i^* = 0 \in V^*$$

$$\forall j, \left(\sum_{i=1}^{n} \beta_i v_i^* \right)(v_j) = 0$$

$$\sum_{i=1}^{n} \beta_i v_i^*(v_j) = \beta_j$$

Откуда $\forall j, \beta_j = 0$ и $v_1^* \cdots v_n^*$ — линейно независимые. ◀

Следствие 2.13.1.1.

$$\dim V < \infty \Rightarrow V \simeq V^*$$

Изоморфизм может быть построен следующим образом: $\Psi \colon V \to V^*$. $v_1, \dots, c_n$ — базис V. Отображение

$$\alpha_1 v_1 + \cdots + \alpha_n v_n \mapsto \alpha_1 v_1^* + \cdots \alpha_n v_n^*$$

является изоморфизмом.

▶ $\dim(V^*) = n = \dim V \Rightarrow V^* \cong V$. Ψ — линейно.

$\Phi \in V^*$, Φ — линейная комбинация $v_1^*, \dots, v_n^*$. Значит, Ψ сюръективно.

$$\Psi(\alpha_1 v_1 + \cdots + \alpha_n v_n) = 0 \iff \alpha_1 v_1^* + \cdots + \alpha_n v_n^* = 0 \Leftrightarrow \alpha_1 = \cdots = \alpha_n = 0$$

$\ker(\Psi) = \{0\} \Rightarrow \Psi$ инъективно. Таким образом, Ψ — биекция. ◀

Замечание 2.13.2. Построенный изоморфизм зависит от выбора базиса в V.

Замечание 2.13.3. $V = K^n$, тогда всякий $\varphi \in V^*$ может быть представлен в виде $\varphi(v) = uv$, где u — фиксированная строка $u = (u_1, \cdots, u_n)$.

$$\Phi \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = u_1 v_1 + \cdots + u_n v_n$$

Базис V $= \{e_1, \cdots, e_n\}$ — стандартный базис.
$\varphi = \sum_{i=1}^{n} u_i e_i^*, u = (u_1, \cdots, u_n)$.

2.13.1. Второе двойственное пространство

V, V^*, V^{**}

$$V \to V^{**}, u \to \varphi_u (\varphi_u \in V^{**})$$

Определим φ_u на произвольном элементе $\varphi_u(f) = f(u), (f \in V^*)$

1. φ_u — линейный функционал на V^*.

$$\varphi_u(\alpha_1 f_1 + \alpha_2 f_2) = (\alpha_1 f_1 + \alpha_2 f_2)(u) =$$
$$= \alpha_1 f_1(u) + \alpha_2 f_2(u) = \alpha_1 \varphi_u(f_1) + \alpha_2 \varphi_u(f_2)$$

2. $u \to \varphi_u$ линейное отображение

$$\beta_1 u_1 + \beta_2 u_2 \to \varphi_{\beta_1 u_1 + \beta_2 u_2}$$

$$\varphi_{\beta_1 u_1 + \beta_2 u_2}(f) = f(\beta_1 u_1 + \beta_2 u_2) =$$
$$= \beta_1 f(u_1) + \beta_2 f(u_2) = \beta_1 \varphi_{u_1}(f) + \beta_2 \varphi_{u_2}(f)$$

Построили гомоморфизм из V в V^{**}, $u \to \varphi_u$

3. Инъективность. Достаточно проверить, что ядро тривиально.

Для каких u $\varphi_u = 0 \in V^{**}$?

$$\forall f \in V^* \varphi_u(f) = 0 \Rightarrow f(u) = 0$$

Если $u \neq 0$, то можно дополнить $\{u\}$ до базиса V.

Рассмотрим f: $f(u) = 1$, $f(u_j) = 0$ для остальных векторов из этого базиса и доопределим на всем V по линейности.

$\varphi_u(f) = f(u) = 1 \neq 0$

Если $u \neq 0$, то и $\varphi_u \neq 0$.

Значит, ядро отображения $u \to \varphi_u$ состоит только из 0, то есть имеется инъективный гомоморфизм из V в V^{**}.

4. Пусть $\dim(V) = n < \infty$

$\dim(V^*) = n, \dim(V^{**}) = n$

$V \to V^{**} (u \to \varphi_u)$ — инъективный гомоморфизм.

$\Rightarrow$ dim образа есть n, то есть это отображение на все V^{**}, значит это сюръекция, то есть это изоморфизм.

Пример 2.13.1. V — пространство финитных(начиная с какого-то места только 0) над полем K.

$$V = \{(a_1, a_2, \cdots) : \text{почти все } a_i = 0\}$$

$B = (b_1, b_2, \cdots)$ — бесконечная последовательность.

$$f_B : V \to K$$

$$(a_1, a_2, a_3, \cdots) \to f_B(a_1, a_2, \cdot) = \sum_{i=1}^{\infty} a_i b_i \in K$$

f_B корректно определено на множестве финитных последовательностей(так как любая сумма превращается в конечную).

f_B линейно:

$$f_B(\alpha(a_1, a_2, \cdots) + \alpha'(a_1', a_2', \cdots)) = \alpha f_B(a_1, a_2, \cdots) + \alpha' f_B(a_1', a_2', \cdots)$$

$f_B \in V^*$ — линейное отображение со значением в поле K.

Если $B \neq B'$, то $f_B \neq f_{B'}$

Зафиксируем координату, по которой они отличаются. Пусть $b_i \neq b_i'$

$$f_B(0, \cdots, 1, \cdots) = b_i \neq b_i' = f_B'(0, \cdots, 1, \cdots)$$

Рассмотрим случай, когда K — конечное или счетное

V^* гораздо больше V.

K — K конечно или счетно, то V — счетно. (Представим V в виде счетного объединения конечной степини K).

Мощность V^* не меньше, чем мощность всех бесконечных последовательностей из 0 и 1(из K) $\Rightarrow$ не меньше, чем мощность множества подмножеств в $\mathbb{N} \Rightarrow$ не меньше мощности континуума.

То есть V^* не счетно(даже нет счетного базиса).

Итог: в случае K — конечное или счтное

V — счетное.

V^* — не счетное(даже нет счетного базиса).

Линейные функционалы могут иметь достаточно хитрую природу об этом следующи примеры.

Пример 2.13.2. $V = C([a, b] \to \mathbb{R})$

1. Интегральные функционалы: $f \to \int_a^b f(x)dx (f \in V)$
2. Весовая функция ρ $f \to \int_a^b f(x)\rho(x)dx$

   Мера определения весовой функции.
3. $f \to \int_a^b f(x)d\mu$

   μ — мера на отрезке $[a, b]$.
4. Мера сконцентрирована в 1 точке.

   $\mu(c) = 1, \mu(x) = 0$ — во всех остальных точках.

   $f \to f(c) = \delta_c(f)$

   $v = C'(\mathbb{R} \to \mathbb{R})$
5. $f \to f(a) + f'(b)$

2.14. Линейные операторы, собственные числа, собственные векторы и характерестический многочлен

V — векторное пространство над K.

$End(V)$ — пространство линейных отображений из V в V, то есть пространство линейных операторов на V.

(endomorphisms)

Цель: найти наиболее простой вид матрицы линейного оператора.

Найти один базис в V, в котором матрица линейного оператора имеет наиболее простой вид.

$\dim(V) = n < \infty$ $f \in End(V)$

$v_1, \cdots, v_n$, $f \to [f]_{\{v_1,\cdots,v_n\},\{v_1,\cdots,v_n\}}$

Если C — матрица перехода к другому базису.

$C^{-1}[f]_{\{v\}}C = [f]_{\{v'\}}$

Def 2.14.1. (работает и при бесконечномерном случае)

$f \in End(v)$

λ — собственное число оператора f, если $\exists v \neq 0, f(v) = \lambda v, \lambda \in K$.

Def 2.14.2. Если λ — собственное число f, то всякий v, такой что $f(v) = \lambda v$, называется собственным вектором.

Замечание 2.14.1. v_1, v_2 — собственные векторы f, отвечающие λ, тогда $\alpha_1 v_1 + \alpha_2 v_2$ — собственный вектор f, отвечающий λ (их линейная комбинация).

$$f(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1 f(v_1) + \alpha_2 f(v_2) =$$
$$= \alpha_1 \lambda v_1 + \alpha_2 \lambda v_2 = \lambda(\alpha_1 v_1 + \alpha_2 v_2)$$

$[f]_{v_i}$

Множество собственных векторов f, отвечающих λ — подпространство в V.

$$U_1(\lambda) = \{\delta : f(\delta) = \lambda\delta\}$$
$$U_1(\lambda) \leqslant V$$

λ — собственное число $\Leftrightarrow \dim(U_1(\lambda)) > 0$

В этом случае говорим, что $U_1(\lambda)$ — пространство собственных векторов, отвечающих λ.

$V = K^n$

$End(V) \cong M(n, n, K)$

$A \in M(n, n, K)$

λ — собственное число A, если $\exists v \neq 0, Av = \lambda v$

Если λ — собственное число A, то v: $Av = \lambda v$ называется собственным вектором матрицы A.

Пусть $dim V = n < \infty$ зафиксируем базис $v_1, \cdots, v_n$

$$f \in End(v)$$
$$f(v) = \lambda v$$
$$A = [f]_{\{v_i\}}$$
$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$
$$v = x_1 v_1 + \cdots + x_n v_n$$

$$[f]_{v_i} \cdot [\vec{V}]_{\{v_i\}} = \lambda [\vec{V}]_{\{v_i\}}$$
$$AX = \lambda X$$

Def 2.14.3. Теперь перейдем к характеристическому многочлену:
$A \in M(n, n, K)$ $\chi_A(t) = det(A - tE) \in K[t]$ — характеристический многочлен матрицы A.
$\dim V = n < \infty$
$f \in end(v)$
$\chi_f(t)$ — характеристический многочлен матрицы f в некотором базисе.

Замечание 2.14.2. χ_f не зависит от выбора базиса в пространстве V.

▶ A — матрица f в каком-то базисе.
В другом базисе: $C^{-1}AC$, где C — матрица перехода от базиса к базису.

$$\chi_{C^{-1}AC}(t) = \det(C^{-1}AC - tE) = \det(C^{-1}AC - C^{-1}(tE)C) =$$
$$= \det(C^{-1}(A - tE)C) = \det(C^{-1}) \det(A - tE) \det(C) = \det(A - tE) \cdot \det(C^{-1}) \det C =$$
$$= \det(A - tE) \det(C^{-1}C) = \det(A - tE) = \chi_A(t)$$

◀

$$\chi_A(t) = \det(A - tE) = \det\left(\begin{pmatrix} a_{11} - t & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - t \end{pmatrix}\right) =$$
$$= (-1)^n t^n + (-1)^{n-1}(a_{11} + a_{nn})t^{n-1} + \cdots + \det(A)$$

$a_{11} + a_{22} + \cdots + a_{nn}$ — след A (trace)
Tr(A).

Теорема 2.14.1. $\dim V = n < \infty, f \in End(V)$
Тогда собственные числа f — это, в точности, корни $\chi_f(t)$

▶ Пусть A — матрица f в некотором базисе.
Собсвенные числа f совпадают с собственными числами A.
$\exists x \neq 0, AX = \lambda X$

$$AX = \lambda EX$$
$$(A - \lambda E)X = 0$$

λ — собственное число $\Leftrightarrow (A - \lambda E)X = 0$ имеет нетривиальное решение $\Leftrightarrow \det(A - \lambda E) = 0 \Leftrightarrow$ $\chi_A(\lambda) = 0 \Leftrightarrow \lambda$ — корень $\chi_A = \chi_f$. ◀

Наиболее простое описание следует ожидать, когда K — алгебраически замкнутое поле (тогда χ_A полностью раскладывается на множетели)
Далее предполагаем, что K — алгебраически замкнуто.

$$\chi_f(t) = \chi_A(t) = (-1)^n \prod (t - \lambda_i)^{a_i}$$
$$\sum a_i = n$$

λ_i — попарно различны.
a_i — алгебраическая кратность собственного числа λ_i
$\dim U_1(\lambda_i) = b_i$ — геометрическая кратность собственного числа λ_i.

Пример 2.14.1.

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

$$\chi_A(t) = (2-t)(-t) - 1(-1) = t^2 - 2t + 1 = (t-1)^2$$

алгебраическая кратность $= 2$

$$A - E = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$$

$$(A-E)X = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} X = 0$$

$$X = \begin{pmatrix} C \\ C \end{pmatrix}$$

$$U_1(1) = \{ \begin{pmatrix} C \\ C \end{pmatrix}, c \in K \}$$

$$b = 1 = \dim(U_1(1))$$

Позднее увидем, что геометрическая кратность всегда не больше арифметической.

2.15. Формулировка теоремы о каноническом виде матрицы линейного оператора

Def 2.15.1. $\mathcal{J}_k(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}$

$\mathcal{J}_k(\lambda)$ — Жорданова клетка, размера k, отвечает λ.

$\mathcal{J}_1(\lambda) = (\lambda)$

Теорема 2.15.1. K — алгебраически замкнутое поле, V — векторное пространство над K, $f \in End(V)$.

Тогда существует базис V, в котором матрица f имеет блочно диагональный вид.

Причем, диагональные блоки — это какие-то клетки Жордана, отвечающие собственным числам f.

Причем такое представление единственное с точностью до перестановки блоков. Кроме того, число клеток, отвечающих одному и тому же λ, равно геометрической кратности λ, а суммарный размер клеток, отвечающих λ, равен алгебраической кратности λ.

Def 2.15.2. Матрица из предыдущей теоремы называется канонической жордановой формой матрицы линейного оператора, а соответствующий базис — жорданов базис.

Следствие 2.15.1.1. Геометрическая кратность $\leqslant$ алгебраической кратности.

Следствие 2.15.1.2. $A \in M(n, n, K)$, K — алгебраически замкнуто.

$\exists C \det C \neq 0$

$C^{-1}AC$ — жорданова форма.

$V = K^n$

$f(v) = Av$, C — матрица перехода от стандартного базиса к жорданову базису.

Пример 2.15.1. Пусть λ — единственное собственное число f $\chi_f(t) = (-1)^n(t-\lambda)^n$

1. $n = 1$, клетка размера 1, алгебраическая кратность = геометрической кратности.
2. $n = 2$,
   (a) $1 + 1$, алгебраическая кратность = геометрической кратности = 2
   (b) 2, алгебраическая кратность = 2, геометрическая кратность = 1.

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda \\ 0 \end{pmatrix}$$

   Если v_1, v_2 — жорданов базис, то v_1 — собственный вектор.
   $Av_2 \to v_1 + \lambda v_2$

$$(f - \lambda E) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} X = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

3. $n = 3$
   (a) $1 + 1 + 1$, геометрическая кратность = 3
   (b) $2 + 1$, геометрическая кратность = 2
   (c) 3, геометрическая кратность = 1
4. $n = 7$ $3 + 2 + 2$
   $3 + 3 + 1$
   Геометрическая кратность совпадает, максимальная размерность совпадает.

2.16. Применение жордановой формы

1. Вычисление A^m
   $C^{-1}AC = B$ — жорданова форма.

$$A = CBC^{-1}$$

$$A^m = (CBC^{-1})^m = CB^mC^{-1}$$

   Достаточно возвести жордановы клетки в степень m.

$$\mathcal{J}_k(\lambda)^m = (\lambda E + \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}) = (\lambda E + \mathcal{J})^m =$$

$$= \sum_{r=0}^{m} C_m^r \lambda^{m-r} \mathcal{J}^r$$

$$\mathcal{J}^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{J}^k = 0$$

$$(\mathcal{J}_k(\lambda))^m = \sum_{r=0}^{k-1} C_m^r \lambda^{m-r} \mathcal{J}^r$$

$$\begin{pmatrix} \lambda^m & C_m^1\lambda^{m-1} & \dots & C_m^{k-1}\lambda^{m-k+1} \\ 0 & \ddots & \ddots & \ddots \\ 0 & \ddots & \ddots & C_m^2\lambda^{m-2} \\ 0 & \ddots & \ddots & C_m^1\lambda^{m-1} \\ 0 & \ddots & \ddots & \lambda^m \end{pmatrix}$$

2. $A^m, g(A), g \in K[t]$ $C^{-1}AC = B$ — жорданова форма. $g(A) = Cg(B)C^{-1}$

3. Вычисление некоторых специальных функций

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

$$v_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

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

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}^m = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & m+1 \\ 1 & m \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} m+1 & -m \\ m & -m+1 \end{pmatrix}$$

$$exp(t) = \sum_{k=0}^{\infty} \frac{t^k}{k!}$$

$$A \in M(n, n, \mathbb{C})$$

$$exp(A) = \sum_{k=0}^{\infty} \frac{A^k}{k!}$$

$$A = a_{ij}$$

$$M = max|a_{ij}|$$

$$|(A^k)_{ij}| \leqslant n^{k-1}M^k \leqslant (nM)^k$$

$$(\sum_{k=0}^{N} \frac{(A^k)_{ij}}{k!}) \leqslant \sum_{k=0}^{N} \frac{(nM)^k}{k!} \leqslant \sum_{k=0}^{\infty} \frac{(nM)^k}{k!} < e^{nM}$$

$$C^{-1}AC = B(\text{— жорданова форма})$$

$$\exp(A) = C\exp(B)C^{-1}$$

2.17. Инвариантные подпространства

Def 2.17.1. V — векторное пространства над K, $\dim V = n < \infty$,
$U < V$ инвариантно относительно f, если $\forall u \in U : f(u) \in U$

Пример 2.17.1. 1. λ — собственное число f, $U_1(\lambda)$ — f-инвариант

2. $\{0\}, V$ — также f-инвариантны.

Теорема 2.17.1. Пусть $V = U \oplus W$ и U — f-инвариантное, тогда $\exists$ базис $u_1, \cdots, u_k \in U$,
$w_1, \cdots, w_{n-k} \in W$, в котором матрица f имеет вид $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ (Первый квадрат $k \times k$).

Если же оба U и W инвариантны, то матрица f в этом базисе имеет вид: $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$ Более того, это верно для любого базиса V, где первая часть векторов из U, а вторая — из W.

▶ 1.

$$[f]_{u_1,\cdots,u_k,w_1,\cdots w_{n-k}}$$

$$f(u_i) \in U$$

$$f(u_i) = \sum_{j=1}^{k} \alpha_{ji} u_j + 0w_1 + \cdots + 0w_{n-k}$$

2. Если и W инвариантно

$$f(w_i) = 0u_1 + \cdots + 0u_n + \sum_{j=1}^{n-k} B_{ji} w_j$$

◀

Следствие 2.17.1.1. Если пространство V раскладывается в прямую сумму подпространств
f— инвариант подпространств, то выбрав в каждом из подпространств по базису, получаем, что матрица f в этом базисе блочно-диагональная.

▶ индукция по число инвариантных подпространств.(упражнение) ◀

$$f \in End(V)$$

$$f^k = f \circ f \circ \cdots \circ f$$

$$H \in K[t], H = a_0 + a_1 t + \cdots + a_k t^k$$

$$H(f) = a_0 id + a_1 f + \cdots + a_k f^k \in End(v)$$

Теорема 2.17.2. V — конечномерное векторное пространство над K, $f \in \mathrm{End}(V)$, $H \in K[t]$. Тогда $\ker H(f)$ и $\mathrm{Im}\, H(f)$ есть f — инвариантные подпространства V.

▶

$$H(t) = a_0 + a_1 t + \cdots + d_n t^n$$
$$H(f) = a_0 id + a_1 f + \cdots + d_n f^n$$
$$f^k = \underbrace{f \circ f \circ \ldots \circ f}_{k}$$

Лемма 2.17.1. $H_1, H_2 \in K[x]$

$$H_1(f) H_2(f) = H_2(f) H_1(f)$$

▶ 1.

$$f^k \circ f^e = f^e \circ f^k = f^{k+e}$$

2.

$$H(f) \circ f^l = \left(\sum_{i=0}^{n} a_k f^k \right) f^l = \sum_{i=0}^{n} a_k f^k f^l =$$
$$= \sum_{i=0}^{n} a_k f^l f^k = f^l \sum_{i=0}^{n} a_k f^k = f^l \circ H(f)$$

3.

$$H_1(f)H_2(f) = H_1(f) \left(\sum_{i=0}^{m} b_k f^k \right) = \sum_{i=0}^{m} b_k H_1(f) f^k =$$
$$= \sum_{i=0}^{m} b_k f^k H_1(f) = H_2(f)H_1(f)$$

◀

$$U = \operatorname{Im} H(f) = \{v \in V \mid \exists w \in V : H(f)w = v\}$$
$$f(U) \overset{?}{\subset} U$$

$u \in U$, $w, \in V$, $H(f)w = u$

$$f(u) = f(H(f)(w)) = (f \circ H(f))(w) = (H(f) \circ f)(w) = H(f)(f(w)) \in \operatorname{Im} H(f) = U$$

Про U доказали.

$f \in \operatorname{End}(V)$, $H(f) \in \operatorname{End}(V)$, $V \overset{H(f)}{\longrightarrow} V$.

$$U = \ker H(f) = \{v \in V \mid H(f)(v) = 0\}$$

$u \in U$

$$H(f)(f(u)) = (H(f) \circ f)(u) = (f \circ H(f))(u) = f(\underbrace{H(f)(u)}_{u \in U = \ker H(f)}) = f(0) = 0$$

◀

Замечание 2.17.1. f — обратим, $\operatorname{Im} f = V$, $\ker f = \{0\}$.

Если $H(f)$ — обратимый оператор, то $\operatorname{Im} H(f) = V$, $\ker H(f) = \{0\}$.

2.18. Теорема Гамильтона— Кэли

Вопрос: найти H такое, чтобы $\ker H(f)$ было «как можно больше».

$$\ker H(f) = V \Leftrightarrow H(f) = 0$$

Теорема 2.18.1 (Гамильтона— Кэли)**.** $\dim V = n < \infty$, $f \in \operatorname{End}(V)$. Тогда

$$\chi_f(f) = 0_{\text{в кольце операторов}}$$

▶ Зафиксируем базис V. $A = [f]$ — матрица f в этом базисе.

$$H[f] = H(A)$$

$$\chi_f = \chi_A$$

Нулевому оператору отвечает нулевая матрица.

Перешли к равносильному утверждению в матрицах:

$$\chi_A(A) = 0$$

Докажем его:

$$\chi_A = \det(A - tE)$$
$$A - tE \in M(n, n, K[t])$$
$$B = (A - tE)^{\text{взаимная}} \in M(n, n, K[t])$$
$$(A - tE)B = B(A - tE) = (\det(A - tE))E$$

При вычислении алгебраического дополниния считаем определитель размера $n-1$ и каждый элемент — многочлен от t степени не более 1. Таким образом, каждое алгебраическое дополение есть многочлен от t степени не более $n-1$. Разложим B как многочлен по степеням t:

$$B(t) \equiv B_0 + tB_1 + \cdots + t^{n-1}B_{n-1}$$
$$B_i \in M(n, n, K)$$
$$(A - tE)(B_0 + tB_1 + \cdots + t^{n-1}B_{n-1}) = \det(A - tE)E = (a_0 + a_1 t + \cdots + a_n t^n)E$$
$$\begin{aligned} AB_0 &= a_0 E \\ AB_1 - B_0 &= a_1 E \\ &\vdots \\ AB_k - B_{k-1} &= a_k E \\ &\vdots \\ -B_{n-1} &= a_n E \end{aligned}$$

Сложив эти строки с коэффицентами $E, A^1, \ldots, A^n$, получим

$$AB_0 + (A^2B_1 - AB_0) + (A^3B_2 - A^2B_1) + \cdots + (A^{k+1}B_k - A^kB_{k-1}) + \cdots + (0 - A^nB_{n-1}) =$$
$$= a_0E + a_1A + \cdots + a_nA^n = \chi_A(A)$$
$$0 = \chi_A(A)$$

◀

Замечание 2.18.1. $f \in \mathrm{End}(V)$. Аннулятор:

$$\mathrm{Ann}(f) = \{H \in K[t] \mid H(f) = 0\}$$

Это множество замкнуто по сумме, разности и умножение на произвольный многочлен, то есть идеал в кольце $K[t]$. $K[t]$ — область главных идеалов. Тогда

$$\mathrm{Ann}(f) = \big(\mu_f(t)\big)$$

μ_f — минимальный аннулятор.

Как мы знаем, $\chi_f \in \mathrm{Ann}(f)$, тогда $\mu_f \mid \chi_f$.

Пример 2.18.1. $f = \lambda id$. Тогда

$$\chi_f = (\lambda - t)^n$$
$$\mu_f = t - \lambda$$

2.19. Разложение в прямую сумму корневых

Теорема 2.19.1. $H_1, H_2 \in K[t]$, $f \in \mathrm{End}(V)$, H_1 и H_2 взаимно просты. Тогда

$$\ker((H_1H_2)(f)) = \ker H_1(f) \oplus \ker H_2(f)$$

▶ 1. $v \in \ker H_i(f)$, $H_i(f)(v) = 0$.

$$(H_1H_2(f))(v) = (H_1(f) \circ H_2(f))(v) = (H_2(f) \circ H_1(f))(v)$$

Если $H_i(f)(v) = 0$, то и $(H_1H_2(f))(v) = 0$. Получили, что $\ker H_i(f) \subset \ker(H_1H_2)(f)$

2. $v \in \ker H_1(f) \cap \ker H_2(f)$.

$$1 = G_1H_1 + G_2H_2$$
$$id = G_1(f) \circ H_1(f) + G_2(f) \circ H_2(f)$$
$$v = id(v) = G_1(f) \circ H_1(f)(v) + G_2(f) \circ H_2(f)(v) = G_1(f)(0) + G_2(f)(0) = 0$$

Таким образом, $\ker H_1(f) \cap \ker H_2(f) = \{0\}$ и сумма — прямая.

3. $v \in \ker(H_1H_2)(f)$.

$$1 = H_1G_1 + H_2G_2$$
$$id = H_1(f) \circ G_1(f) + H_2(f) \circ G_2(f)$$
$$v = id(v) = \underbrace{(G_1(f) \circ H_1(f))(v)}_{v_2} + \underbrace{(G_2(f) \circ H_2(f))(v)}_{v_1}$$
$$v = v_2 + v_1$$

Проверим, что $v_1 \in \ker H_1(f)$

$$H_1(f)(v_1) = (H_1H_2G_2)(f)(v) = (G_2(f) \circ (H_1H_2)(f))(v) = G_2(f)(\underbrace{(H_1H_2)(f)(v)}_{=0}) = 0$$

Аналогично $v_2 \in \ker H_2(f)$.

◀

Следствие 2.19.1.1. $H(t) = H_i(t) \circ ... \circ H_k(t)$, H_i попарно взаимно просты. Тогда

$$\ker H(f) = \bigoplus_{i=1}^{k} \ker H_1(f)$$

$\dim V = n < \infty$, K алгебраически замкнуто. Тогда

$$V = \ker \mathbb{0} = \ker \chi_f(f)$$
$$\chi_f(f) = \prod_{i=1}^{k} (t - \lambda_i)^{a_i} \quad \lambda_i \neq \lambda_j$$
$$V = \bigoplus_{i=1}^{k} \ker(f - \lambda id)^{a_i}$$

Def 2.19.1. k-корневое пространство, отвечающее λ

$$U_k(\lambda) = \ker(f - \lambda id)^k$$

Соотвественно, $U_1(\lambda)$ есть собственные вектора f.

Как можно заметить,

$$U_1(\lambda) \subset U_2(\lambda) \subset ...$$

Причём оно стабилизируется, потому что размерность ограничена сверху размерностью пространства V, а при каждом включении, меняющем пространство, размерность тоже увеличивается.

Def 2.19.2. Корневое пространство, отвечающее λ

$$U(\lambda) = \bigcup_{k=1}^{\infty} \ker(f - \lambda id)^k$$

Def 2.19.3. Корневой вектор — вектор корневого пространства. Если он при этом лежит в $U_k(\lambda)$, но не лежит в $U_{k-1}(\lambda)$, его называют корневым вектором высоты k.

2.20. Жорданова форма оператора с единственным собственным числом

Теорема 2.20.1. Мы уже умеем представлять V в виде:

$$V = \bigoplus_{i=1}^{n} \ker(f - \lambda_i id)^{a_i}$$

Сузим оператор f:

$$f\Big|_{U_{a_i}(\lambda_i)}$$

В такой ситуации λ — единственное собственное число суженного оператора f.

▶ Возьмём некоторое собственное число $\gamma \neq \lambda$ и посмотрим на оператор

$$f - \gamma id = f - \lambda id + (\lambda - \gamma)id$$

Покажем, что он обратим (тогда ядро тривиально, тогда γ не может быть собственным числом).

Обратимость не зависит от домножения на ненулевой скаляр. Домножим оператор на $\frac{1}{\lambda-\gamma}$:

$$(f - \gamma id) \cdot \frac{1}{\lambda - \gamma} = \frac{f - \lambda id + (\lambda - \gamma)id}{\lambda - \gamma} = \frac{f - \lambda id}{\lambda - \gamma} + id = id - \underbrace{\frac{f - \lambda id}{\gamma - \lambda}}_{g}$$

Т.к. $(f - \lambda id)^{a_i} = 0$ (так как мы живём в соответствующем корневом пространстве), то $g^{a_i} = 0$, то есть g — нильпотентный. А тождественное минус нильпотентный всегда обратимо, можно явно предъявить:

$$(id - g)(id + g + \cdots + g^{a-1}) = id - g^a = id$$

◀

Пусть V — векторное пространство и есть подпространство $U < V$.

Def 2.20.1. Набор векторов $v_1, ..., v_k$ называется относительно линейно независимым относительно подпространства U, если следующее равенство выполняется только при $\alpha_i = 0$:

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k + u = 0$$
$$\alpha_i \in K, u \in U$$

Замечание 2.20.1. Обычная линейная независимость — это относительная относительно подпространства из нуля.

Def 2.20.2. Относительное семейство образующих, если любой $v \in V$ можно представить в виде

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k + u = v$$
$$a_i \in K, u \in U$$

Def 2.20.3. Относительный базис — если относительно линейно независимо и заодно является относительным семейством образующих (всё относительно одного фиксированного U).

Замечание 2.20.2. Такая конструкция уже возникала: когда мы брали базис U (u_i) и дополняли его до базиса V (v_i), мы дополняли его именно относительным базисом, то есть эти вот v_i — относительный базис V относительно U. Так что почти ничего нового.

Рассмотрим цепочку корневых пространств:

$$0 \subset U_1(\lambda) \subset U_2(\lambda) \subset \dots \subset U_a(\lambda) = V$$

(на U_a закончили, так как $f - \lambda id$ занулилось и ядром стало всё пространство).

Теперь найдём место стабилизации, то есть такое наибольшее m, что $U_{m-1}(\lambda) \subsetneq U_m(\lambda)$. То есть у нас есть корневые вектора высоты m, но больше высоты — уже нет. В частности, отсюда следует, что $U_m(\lambda) = V$.

Найдём относительный базис $U_m(\lambda)$ относительно $U_{m-1}(\lambda)$: $v_1^{(m)}, \dots, v_j^{(m)}$.

Лемма 2.20.1. При $r \geqslant 2$: Пусть $u_1, \dots, u_s \in U_r(\lambda)$ и относительно линейно независимы относительно $U_{r-1}(\lambda)$. Тогда на эти вектора можно подействовать оператором $f - \lambda id$ и получим:

$$(f - \lambda id)u_1, \dots, (f - \lambda id)u_s \in U_{r-1}(\lambda)$$

Также они относительно линейно независимы относительно $U_{r-2}(\lambda)$.

▶
- Чтобы показать, что они лежат в $(r-1)$-м корневом пространстве, надо применить оператор $(f - \lambda id)$ $(r-1)$ раз:

  $$(f - \lambda id)^{r-1}((f - \lambda id)u_i) = (f - \lambda id)^r u_i = 0$$

  Так как u_i лежало в r-м корневом пространстве, то последний переход верен.
- От противного: предположим линейную зависимость. Имеем:

  $$\alpha_1(f - \lambda id)u_1 + \dots + \alpha_s(f - \lambda id)u_s + \underbrace{w}_{\in U_{r-2}(\lambda)} = 0$$

  Подействуем на это дело $(r-2)$ степенью оператора, тогда w занулится:

  $$\alpha_1(f - \lambda id)^{r-1}u_1 + \dots + \alpha_s(f - \lambda id)^{r-1}u_s + 0 = 0$$
  $$(f - \lambda id)^{r-1}\underbrace{(\alpha_1 u_1 + \dots + \alpha_s u_s)}_{\widetilde{w}} = 0$$
  $$\widetilde{w} \in \ker(f - \lambda id)^{r-1} = U_{r-1}(\lambda)$$

  Так как u_i относительно линейно независимы относительно $U_{r-1}(\lambda)$, то $\alpha_i = 0$, что и требовалось доказать.

◀

А теперь алгоритм действий построения башни векторов (мы сейчас хотим нарисовать какую-нибудь осмысленную красивую картинку из корневых пространств):

- Взяли относительный базис $V = U_m(\lambda)$ относительно $U_{m-1}(\lambda)$ из векторов $v_1^{(m)}, v_2^{(m)}, \dots, v_{j_m}^{(m)}$.
- Применили оператор $f - \lambda id$, спустили эти вектора на уровень ниже, они остались линейно независимыми. Но, возможно, они перестали быть относительным базисом (уже относительно $U_{m-2}(\lambda)$, иногда надо дополнить, получим набор $v_1^{(m-1)}, v_2^{(m-1)}, \dots, v_{j_{m-1}}^{(m-1)}$ (очевидно, что $j_m \leqslant j_{m-1}$, так как старые включены).
- Продолжили спускаться до уровня 1. В конце получили $v_1^{(1)}, v_2^{(1)}, \dots, v_{j_2}^{(1)}, v_{j_2+1}^{(1)}, \dots, v_{j_1}^{(1)}$. (то, что после j_2-го элемента — дополнили до базиса $U_1(\lambda)$)

$$
\begin{array}{r|ccccccccccccc}
V = U_m(\lambda) & v_1^{(m)} & v_2^{(m)} & \dots & v_{j_m}^{(m)} & & & & & & & & & \\
(f-\lambda id)(\dots) & \downarrow & \downarrow & \ddots & \downarrow & & & & & & & & & \\
U_{m-1}(\lambda) & v_1^{(m-1)} & v_2^{(m-1)} & \dots & v_{j_m}^{(m-1)} & v_{j_m+1}^{(m-1)} & \dots & v_{j_{m-1}}^{(m-1)} & & & & & & \\
 & \downarrow & \downarrow & \ddots & \downarrow & \downarrow & \ddots & \downarrow & & & & & & \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & & & & & & \\
 & \downarrow & \downarrow & \ddots & \downarrow & \downarrow & \ddots & \downarrow & & & & & & \\
U_1(\lambda) & v_1^{(1)} & v_2^{(1)} & \dots & v_{j_m}^{(1)} & v_{j_m+1}^{(1)} & \dots & v_{j_{m-1}}^{(m-1)} & \dots & v_{j_2}^{(1)} & v_{j_2+1}^{(1)} & \dots & v_{j_1}^{(1)}
\end{array}
$$

Посмотрим на эту схему. Каждая строчка из $v_i^{(k)}$ дополняет базис $(k-1)$-го корневого пространства до полного базиса k-го корневого пространства (не относительного). Если взять все вектора из строчек с k-й и вниз, получим базис (не относительный) $U_k(\lambda)$. Таким образом, если взять вообще все вектора, то это будет базис пространства V.

Теперь давайте прочитаем табличку не по строкам, а по столбцам: сначала первый столбец сверху вниз, потом второй, и так далее. Посмотрим на пространства, порождённые столбцами. Пространство V является прямой суммой этих пространств (они не пересекаются, потому что порождены непересекающимися подмножествами базиса V). Возьмём какое-нибудь пространство с базисом-столбцом $v_i^{(r)}, v_i^{(r-1)}, \dots, v_i^{(1)}$ (с высоты r появляется столбец и растёт вниз). Хотим выписать для него матрицу (так как матрица всего f будет состоять из таких блоков, потому что f — прямая сумма): По лемме 2.20.1 знаем, что для любого $2 \leqslant s \leqslant r$:

$$
\begin{aligned}
(f - \lambda id)v_i^{(s)} &= v_i^{(s-1)} \\
fv_i^{(s)} - \lambda v_i^{(s)} &= v_i^{(s-1)} \\
fv_i^{(s)} &= \lambda v_i^{(s)} + v_i^{(s-1)}
\end{aligned}
$$

А для $s = 1$ имеем $fv_i^{(1)} = \lambda v_i(1)$ (потому что собственный вектор). То есть матрица преобразования f имеет вид (это мы смотрим, куда f переводит каждый вектор из базиса):

$$
\begin{vmatrix}
 & v_i^{(1)} & v_i^{(2)} & v_i^{(3)} & \dots & v_i^{(r-1)} & v_i^{(r)} \\
v_i^{(1)} & \lambda & 1 & 0 & \dots & 0 & 0 \\
v_i^{(2)} & 0 & \lambda & 1 & \dots & 0 & 0 \\
v_i^{(2)} & 0 & 0 & \lambda & \dots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
v_i^{(r-1)} & 0 & 0 & 0 & \dots & \lambda & 1 \\
v_i^{(r)} & 0 & 0 & 0 & \dots & 0 & \lambda
\end{vmatrix}
$$

Это в точности Жорданова клетка. То есть матрица для f есть несколько Жордановых клеток — Жорданова форма.

- Параметр m отвечает максимальному размеру клетки.
- Количество клеток есть в точности геометрическая кратность собственного числа λ (число векторов на последнем уровне).
- Количество клеток размера k и выше — число векторов на k-м снизу уровне нашей диаграммы. Перефразируя: число векторов в относительном базисе $U_k(\lambda)$ относительно $U_{k-1}(\lambda)$, то есть $\dim U_k(\lambda) - \dim U_{k-1}(\lambda)$.
- Количество клеток размера в точности k:

$$(\dim U_k(\lambda) - \dim U_{k-1}(\lambda)) - (\dim U_{k+1}(\lambda) - \dim U_k(\lambda)) = 2\dim U_k(\lambda) - \dim U_{k-1}(\lambda) - U_{k+1}(\lambda)$$

Следствие 2.20.1.1. Мы выразили количество клеток размера в точности k через размерности корневых пространств, которые от базиса не зависят. Значит, количество клеток однозначно определяется оператором.

Следствие 2.20.1.2. Так как количество клеток неотрицательно, можно написать:

$$2\dim U_k(\lambda) \geqslant \dim U_{k-1}(\lambda) + \dim(U_{k+1}(\lambda))$$

То есть последовательность размерностей корневых пространств вогнута.

Лемма 2.20.2. Пусть A матрица в Жордановой форме. λ — собственное число. Алгебраическая кратность λ = суммарному размеру всех клеток, отвечающих данному собственному числу.

▶ $\chi_f(t)$. Кратность λ как кратность корня $\chi_f(t)$.
$\chi_f(t)$ не зависит от выбора базиса.
Характеристический многочлен матрицы в Жордановой форме: $\prod_{\lambda_i}(\lambda_i - t)^{a_i}$.
a_i — количество λ_i на диагонали Жордановой формы. То есть суммарный размер всех клеток, отвечающих данном собственному числу. ◀

2.21. Диагонализуемый оператор

Def 2.21.1. $f \in End(v), \dim(V) < \infty$
f — диагонализуем, если существует базис V, в котором матрица f имеет диагональный вид.

Теорема 2.21.1. f — диагонализуем $\Leftrightarrow$ существует базис V, состоящий из собственных векторов f.

▶ $\Rightarrow$
f — диагонализуем.
Существует базис $v_1, \cdots, v_n$: $[f]_{v_1,\cdots,v_n} = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$
(λ не обязательно различные).
$f(v_i) = 0 \cdot v_1 + \cdots + 0 \cdot v_{n-1} + \lambda_i v_i + 0 \cdots v_{i+1} + \cdots + 0 v_n = \lambda_i v_i \Rightarrow v_i$ собственный вектор отвечающий $\lambda_i \Rightarrow$ базис $v_1, \cdots, v_n$ состоит из собственных векторов.
$\Leftarrow$
$\exists v_1, \cdots, v_n$: $f(v_i) = \lambda_i v_i$
$[f]_{v_1,\cdots,v_n} = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$
То есть в базисе $v_1, \cdots, v_n$ матрица $[f]$ диагоналная, то есть f — диагонализуемая. ◀

Замечание 2.21.1. Не всякий оператор диагонализуем.

Если у f лишь одно собственное число(K — алгебраически замкнуто), то геометрическая кратность меньше алгебраической кратности

$$\dim U_1(\lambda) < \dim V$$

$$U_1 \lneqq V$$

$\Rightarrow f$ не диагонализуем.

$$End(V)$$

$$\dim_{\mathbb{C}}(V) = n < \infty$$

$$M(n, n, \mathbb{C})$$

$$\dim_{\mathbb{C}}(M(n, n, \mathbb{C})) = n^2$$

$$\dim_{\mathbb{R}}(M(n, n, \mathbb{C})) = 2n^2$$

Множество недиагонализуемых операторов есть множество меры 0.

Глава 3

Пространства со скалярным произведением

3.1. Билинейные и полуторалинейные формы

Def 3.1.1. V — векторное пространство над K.
$B\colon V\times V\to K, B$ — билинейная форма, если B линейно по каждому аргументу.

$$B(\alpha_1 x_1+\alpha_2 x_2, y)=\alpha_1 B(x_1,y)+\alpha_2 B(x_2,y)$$
$$B(x,\alpha_1 y_1+\alpha_2 y_2)=\alpha_1 B(x,y_1)+\alpha_2(x,y_2)$$

Def 3.1.2. B — билинейная форма.

1. B — симметрическая, если $\forall x,y\in V, B(x,y)=B(y,x)$.
2. B — кососимметрическая, если
   (a) $\forall x,y\in VB(x,y)=-B(y,x)$
   (b) $\forall x\in V, B(x,x)=0$

Замечание 3.1.1. Если $charK\neq 2$, то $a\Rightarrow b$.

$$B(x,x)=-B(x,x)\Rightarrow 2B(x,x)=0\Rightarrow B(x,x)=0$$

Замечание 3.1.2. Для произвольного поля $b\to a$.

$$0=B(x+y,x+y)=B(x+y,x)+B(x+y,y)=B(x,x)+B(y,x)+B(x,y)+B(y,y)$$
$$B(y,x)+B(x,y)=0$$
$$B(x,y)=-B(y,x)$$

$$B(0,y)=B(0+0,y)=B(0,y)+B(0,y)$$
$$\forall y\in V\colon 0=B(0,y)$$
$$\forall x\in V\colon 0=B(x,0)$$

Def 3.1.3. B — невырожденная, если

$$\forall x\neq 0\exists y\colon B(x,y)\neq 0$$
$$\forall y\neq 0\exists x\colon B(x,y)\neq 0$$

Def 3.1.4. Пусть $K = \mathbb{R}, V$ — векторное пространство над $\mathbb{R}$.
$B\colon V \times V \to \mathbb{R}, B$ — билинейная форма.
B — положительно определенна, если $\forall x\colon B(x,x) \geqslant 0$ и $B(x,x) = 0 \Leftrightarrow x = 0$

Def 3.1.5. B — неотрицательно определена, если $\forall x\colon B(x,x) \geqslant 0$

Замечание 3.1.3. Положительная определнность $\Rightarrow$ невырожденность.

Пример 3.1.1. 1. $\mathbb{R}^n$

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

$$B(x,y) = x^T y = \sum_{i=1}^{n} x_i y_i$$

B — симметричный положительный оператор.

2. $a_1, \cdots, a_n \in R$ $B(x,y) = \sum_{i=1}^{n} a_i x_i y_i$ B — симметричная
B — положительно определенная $\Leftrightarrow$ все $a_i > 0$

3. K — произвольное

$$A \in M(n,n,K), V = K^n$$
$$B\colon V \times V \to K$$
$$B(x,y) = x^T A y$$

Если $A = A^T$, то B — симметричная.

$$B(x,y) = x^T A y = (x^t A y)^T = y^T A^T (x^T)^T = y^T A^T x = y^T A x = B(y,x)$$

Верно и обратное. Если $A \neq A^T$ $\exists i, j a_{ij} \neq a_{ji}$

$$x = \begin{pmatrix} 0 \\ 0 \\ 1(-i) \\ 0 \end{pmatrix}$$

$$y = \begin{pmatrix} 0 \\ 0 \\ 1(-j) \\ 0 \end{pmatrix}$$

$x^T A y = a_{ij}, y^T A x = a_{ji} \Rightarrow B$ не симметричная.
B — кососимметричная $\Leftrightarrow$

(a) $A = -A^T$
(b) на диагонали A нули.

4.

$$V = C([a,b], \mathbb{R})$$
$$B(f,g) = \int_a^b f(t) g(t) dt$$

B — симметричная

$$\int_a^b f^2(t)dt \geqslant 0$$

$$\int_a^b f^2(t)dt = 0 \Leftrightarrow f = 0$$

Положительно определен.

5. $V = C([a,b], \mathbb{R})$ ρ — непрерывная функция на $[a,b]$. $B(f,g) = \int_a^b \rho(t)f(t)g(t)dt$
   B — симметрична.
   Если $\rho > 0$, на $[a,b]$, то B — положительно определено.
   (Упражнение. Когда B — невыраждена?)

6. $V = \mathbb{R}[t]$

$$B(f,g) = \int_0^\infty e^{-t} f(t)g(t)dt$$

$$B(f,g) = \int_{-\infty}^\infty e^{-t^2} f(t)g(t)dt$$

Def 3.1.6. V — векторное пространство над $R, \dim_{\mathbb{R}} V < \infty$
$B \colon V \times V \to \mathbb{R}$, B — симмитрична, положительно определенная.
Тогда (V, B) называется евклидовым пространством.

Def 3.1.7. K — поле.
$- \colon K \to K$ — изоморфизм поля K.
$- \neq id$
$-^2 = id$
$\forall a \in K \colon \overline{\overline{a}} = a$ — инвлюция на поле K.

Пример 3.1.2. $\mathbb{C}$ и комплексное сопряжение.

Def 3.1.8. V — векторное пространство над K.
$B \colon V \times V \to K$ B — полуторолиненая форма если:

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

Def 3.1.9. B — называется эрмитово симметричная если $B(x,y) = \overline{B(y,x)}$

Def 3.1.10. Если B — эрмитова симмитричная. $B(x,x) \in \mathbb{R}$
и если $\forall x \in V, B(x,x) \geqslant 0, B(x,x) = 0 \Leftrightarrow x = 0$, то B — положительно определенная.

Def 3.1.11. B — невырожденная, если

$$\forall x \neq 0 \exists y B(x,y) \neq 0$$

$$\forall y \neq 0 \exists x B(x,y) \neq 0$$

Положительно определенная $\Rightarrow$ невырожденная.

Def 3.1.12. $K = \mathbb{C}, \dim_{\mathbb{C}} V = n < \infty$

$B\colon V \times V \to K, B$ — эрмитово симмитрично, положительно определенное, тогда (V, B) — называется унитарным пространством.

Пример 3.1.3.

C^n

$$B(x, y) = \sum_{i=1}^{n} x_i \overline{y_i}$$

$$B(x, \lambda y) = \overline{\lambda} B(x, y)$$

эрмитово симмитрично, положительно определено.

$B(x, y) = x^T A \overline{y}$ (Упражнение B — эрмитово симмитрично $\Leftrightarrow A = \overline{A}^T$)

$V = C([a, b] \to \mathbb{C})$

$$B(f, g) = \int_a^b f(t)\overline{g(t)}dt$$

$$B(f, f) = \int_a^b |f|^2 dt$$

B — положительно определенный.

$B(u, v)$ — полуторолинейно эрмитово симметрично.

K — поле с инволюцией.

Если $K = \mathbb{C}$

$$B(u, v) = \overline{B(u, v)} \Rightarrow B(u, v) \in \mathbb{R}$$

Выше было: $-$ — инволюция на K(то есть, в частности, - $\neq id$)

$$B(u_1 + u_2, v) = B(u_1, v) + B(u_2, v)$$

$$B(u, v_1 + v_2) = B(u, v_1) + B(u, v_2)$$

$$B(\lambda u, v) = \lambda B(u, v)$$

$$B(u, \lambda v) = \overline{\lambda} B(u, v)$$

Далее - — либо инволюция на K, либо id.

B, соответственно, полуторолинейная или билинейная форма.

3.2. Матрица Грама

Def 3.2.1. $\dim_k V < \infty$

$B\colon V \times V \to K$ (полуторолинейная(билинейная форма)) $v_1, \cdots, v_n$ — базис V.

$\Gamma = (B(v_i, v_j))_{i,j=1,n}$ — матрица Грама формы B, отвечающая базису $v_1, \cdots, v_n$.

Почему нам достаточно Γ, чтобы востановить значение билинейной формы на всем пространстве.

$$x, y \in V$$

$$x = \sum_{i=1}^{n} x_i v_i$$

$$y = \sum_{i=1}^{n} y_i v_i$$

$$B(x,y) = B(\sum_{i=1}^{n} x_i v_i, \sum_{j=1}^{n} y_j v_j) =$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n} x_i \overline{y_j} B(v_i, v_j) =$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n} x_i B(v_i, v_j)\overline{y_j} =$$

$$= (x_1, \cdots, x_n) B(v_i, v_j) \begin{pmatrix} \overline{y_1} \\ \vdots \\ \overline{y_n} \end{pmatrix}$$

Замечание 3.2.1. Замечание о бесконечно мерном случае. $x = \sum x_i v_i$, где почти все $x_i = 0$ $y = \sum y_i v_j$, где почти все $y_i = 0$

$B(x,y) = \sum_i \sum_j x_i B(v_i, v_j)\overline{y_j}$, почти все $x_i, y_j = 0$

Лемма 3.2.1. Матрица Грама эрмитово симметрична $\Leftrightarrow$ форма эрмитово симметрична.

▶ Эрмитово симметрична $B(x,y) = \overline{B(y,x)}$

$$\Gamma = B(v_i, v_j)$$

$\Gamma^T = \overline{\Gamma}$ — эрмитовски симметричная матрица.

Верно и обратное.

$$x \to \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$y \to \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

$$B(x,y) = x^T \Gamma \overline{y}$$

$$\overline{B(x,y)} = \overline{(x^T \Gamma \overline{y})} = (\overline{x^T \Gamma \overline{y}})^T =$$

$$(x^{-T}\overline{\Gamma} y)^T = y^T \overline{\Gamma}^T (\overline{x}^T)^T = y^T \Gamma \overline{x} = B(y,x)$$

$$B(x,y) = \overline{B(y,x)}$$

◀

Лемма 3.2.2.

1. B — эрмитово симметрична полуторолинейная $\Leftrightarrow$ ее матрица Грама эрмитово симметрична.
2. B — симметрична билинейная форма $\Leftrightarrow$ ее матрица Грама (в любом базисе) симметричная матрица.
3. B — кососимметричная билинейная форма $\Leftrightarrow$ ее матрица Грама — кососимметричная матрица с нулевой диагональю.

▶ 1,2 смотрите выше. 3

$$\forall x, yB(x,y) = -B(y,x)$$

$$\forall xB(x,x) = 0$$

$$\Gamma^T = -\Gamma \Rightarrow B(x,y) = -B(y,x) \forall (x,y)$$

$$B(x,y) = x^T \Gamma y = (x^T \Gamma y)^T = y^T \Gamma^T x = -y^T \Gamma x = -B(y,x)$$

В обратную сторону, если верно для $\forall x, y$, то, в частности, верно и для базисных векторов. Если $B(x,x) = 0 \forall x\ B(v_i, v_j) = 0 \Rightarrow$ диагональ Γ — нулевая.
$\Gamma^T = -\Gamma +$ нулевая диагональ.

$$B(x,x) = x^T \Gamma x = \sum_{i,j} x_i \Gamma_{ij} x_j = \sum_i \Gamma_{ii} x_i^2 + \sum_{i<j} (\Gamma_{ij} + \Gamma_{ji}) x_i x_j = 0$$

◀

Лемма 3.2.3. B — невырожденная $\Leftrightarrow$ Γ невырожденная.

▶

$$\forall x \neq 0 \exists y B(x,y) \neq 0$$

$$\forall x \neq 0 \exists \overline{y} x^T \Gamma \overline{y} \neq 0$$

$\Leftrightarrow$ для строки $x^T \Gamma$ найдется столбец $\overline{y}$, такой что $x^T \Gamma \overline{y} \neq 0$

$$(c_1, \cdots, c_n)$$

$$\exists y c_1 \overline{y_1} + \cdots + c_n \overline{y_n} \neq 0 \Leftrightarrow \forall x (c_1, \cdots, c_n) \neq (0, \cdots, 0) \Leftrightarrow \forall x \neq 0 x^T \Gamma \neq 0$$

Отображение из пространства строк в пространство строк.

$$x^T \to x^T \Gamma$$

Невырожденно $\Leftrightarrow$ ядро отображения тривиально $\Leftrightarrow \det \Gamma \neq 0$

$$x \to \Gamma^T x$$

Невырожденно $\Leftrightarrow \det(\Gamma^T) \neq 0 \Leftrightarrow \det(P \neq 0)$
Аналогично, $\forall \overline{y} \exists x B(x,y) \neq 0 \Leftrightarrow \det(\Gamma) \neq 0$ ◀

Def 3.2.2. $K = \mathbb{R}, B$ — симмитричная положительно определенная. $\forall x \neq 0, x^T \Gamma x > 0$ Матрица Γ с таким свойством называется положительно определенной матрицей.

Def 3.2.3. $K = \mathbb{C} B$ — полуторалинейная эрмитово симметричная положительно определенная

$$\forall x \neq 0, x^T \Gamma \overline{x} > 0$$

$$\Gamma^T = \overline{\Gamma}$$

Лемма 3.2.4. $v_1, \cdots, v_n; v_1', \cdots, v_n'$ — базисы V
B — полуторолинейная(билинейная) форма на V.
Γ, Γ' — матрица Грама в соответствующих базисах.
C — матрица переходв от $v_1, \cdots, v_n$ к $v_1', \cdots, v_n'$, тогда

$$\Gamma' = C^T \Gamma \overline{C}$$

▶ x, y — столбцы координат в старом базисе.
x', y' — столбцы координат в новом базисе.

$$u = \sum x_i v_i = \sum x'_i v'_i$$

$$v = \sum y_i v_i = \sum y'_i v'_i$$

$$x = Cx', y = Cy'$$

$$x'^T C^T \Gamma \overline{C} \overline{y} = x^T \Gamma \overline{y} = B(u, v) = x^T \Gamma' \overline{y'}$$

$\forall$ столбцов x', y'

$$x'^T \Gamma' \overline{y'} = x'^T C^T \Gamma \overline{C} \overline{y'}$$

$$\Gamma' = C^T \Gamma \overline{C}$$

$$\forall i, j (\Gamma')_{ij} = (C^T \Gamma \overline{C})_{ij} \Rightarrow \Gamma = C^T \Gamma \overline{C}$$

◀

3.3. Процесс ортогонализации

Def 3.3.1. B — полуторалинейная(билинейная) форма на V.
$v_1, \cdots, v_n$ пространства V называется ортогональным базисом, если $B(v_i, v_j) = 0$ для всех $i \neq j$.
Базис ортонормирован, если он ортогонален и $B(v_i, v_i) = 1$ для всех i.

Def 3.3.2.

$$x \perp y$$

$x, y \in V$ ортогональны, если $B(x, y) = 0$

Замечание 3.3.1. B — эрмитово симметрична(симметрична, кососимметрична).

$$x \perp y \Rightarrow y \perp x$$

Замечание 3.3.2. Не для всякой билинейной формы(даже невырожденной) существует ортогональный базис.

Пример 3.3.1. B — кососимметрична, невырожденная.
$v_1, \cdots, v_n$ — ортогональный базис?

$$v_1 \perp v_2, \cdots v_1 \perp v_n$$

Но и $v_1 \perp v_1 \Rightarrow v_2$ ортогонален $\forall$ вектору из V $\forall i B(v_1, v_i) = 0$
$\forall y \in V, B(v_1, y) = 0$ противоречие с невырожденностью.

Теорема 3.3.1. $K = \mathbb{C}$(или $\mathbb{R}$) $V, \dim V < \infty$. B — эрмитова симметричная положительно определенная.
Тогда существует ортогональный базис.

▶ **Шаг 1** Строим ортогоналный базис.
Пусть $v_1, \cdots, v_n$ — базис V.
Найдем новый базис $u_1, \cdots, u_n$
1. $< u_1, \cdots, u_i >=< v_1, \cdots, v_i >, i = 1, \cdots, n$

2. $u_i \perp u_j, i \neq j$
   $u_1 = v_1$
   Предположим, что построили $u_1, \cdots, u_i < u_1, \cdots, u_i >=< v_1, \vdots, v_i >$ и добавляем u_{i+1} в виде линейной комбинации v_{i+1} и $u_1, \cdots, u_i$

$$u_{i+1} = v_{i+1} + \sum_{j=1}^{i} \alpha_j u_j$$

$$< u_1, \cdots, u_{i+1} >=< v_1, \cdots, v_{i+1}) >$$

   Условие ортогональности: $u_{i+1} \perp u_1 \cdots u_i$

$$0 = B(u_{i+1}, \cdots, u_k) = B(v_{i+1}, u_k) + \sum_{j=1} \alpha_j B(u_j, u_k) =$$

$$= B(v_{i+1}, u_k) + \alpha_k B(u_k, u_k)$$

   $B(u_k, u_k) > 0$ в силу положительной определенности $u_k \neq 0$(так как $u_1, \cdots u_k$ — линейно независимые).
   Нашли u_{i+1}

Шаг 2 Нормируем $u_1, \cdots, u_n$ — ортогональный базис.

$$w_i = \lambda_i u_i$$

$$1 = B(w_i, w_i) = \lambda_i \overline{\lambda_i} B(u_i, u_i)$$

$|\lambda_i|^2 = \frac{1}{B(u_i, u_i)} > 0$ В силу положительной определенности.

$$\lambda_i = \frac{1}{\sqrt{B(u_i, u_i)}}$$

Процесс ортогонализации Грама-Шмидта.

◀