АлГем

Сергей Григорян

13 января 2025 г.

Содержание

1 Лекция 14

1.1 Алгебраические структуры

Определение 1.1. Группой наз-ся мн-во G с опред. на нём бинарной алг. операцией. (Обозначим как $*\colon G \times G \to G$ - отображение)
Кроме того, * удовл. след. св-вам:

I) Ассоциативность: $(a * b) * c = a * (b * c)$

II) $\exists$ нейтрального эл-та e отн-но $*$:

$$a * e = e * a = a$$

III) $\exists$ обратный эл-т a^{-1}:

$$a * a^{-1} = a^{-1} * a = e$$

Пример. *1)* $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ - 0 *нейтр. эл-т,* $\forall a \to -a$ *- противоположный (обратный) эл-т.*

2) $(\mathbb{R} \setminus \{0\}, *), (\mathbb{Q} \setminus \{0\}, *)$

3) $(\mathbb{R}, *)$ *- не группа, нарушается III для 0*

4) Пусть X *- произв. мн-во,* $S(X)$ *- мн-во всех вз. однозн. отобр.* $X \to X$*:*

$$\phi, \psi \text{ - вз. одн. отобр.}$$

$$(\phi \cdot \psi)(x) = \phi(\psi(x))$$

Тогда:

$$(S(X), \circ) \text{ - группа}$$

$$e(x) = x$$

5) Пусть $X = \{1, 2, \ldots n\}$

$$\phi\colon \{1, 2, \ldots n\} \to \{1, 2, \ldots n\} \text{ - подстановка}$$

$$S(\{1, 2, \ldots n\}) = S_n \text{ - симметрич. группа степени } n.$$

Утверждение 1.1. *Во всякой группе G нейтральный эл-т единственный.*

Доказательство.
$$e = e * e' = e'$$
$\square$

Определение 1.2. Пусть G группа. Эл-т b наз-ся **левым обратным** к a, если $b * a = e$

Эл-т c наз-ся правым обратным к a, если $c * a = e$

Утверждение 1.2. *$\forall a \in G$ левый обратный к нему совпад. с правым обратным к нему и совпад. с a^{-1}*

Доказательство.
$$b * a = e, a * c = e$$
$$c = e * c = (b * a) * c = b * (a * c) = b * e = b$$
$$\Rightarrow b * a = a * b = e \Rightarrow b = a^{-1}$$
В част-ти, для каждого эл-та a обратный эл-т единственный. $\square$

Определение 1.3. Мн-во R с опред. на нём бинарной алг. операциями "$+$" и "$*$" наз-ся **кольцом**, если эти операции удовл. св-вам:

a) $(R, +)$ - абелева группа (т. е. группа с комутативностью).

b) Ассоц. $*$

c) Левая и правая дистрибутивность $*$ отн-но $+$:
$$(a + b) * c = a * c + b * c$$
$$a * (b + c) = a * b + a * c$$

Пример. *1)* $(\mathbb{Z}, +, *), (\mathbb{Q}, +, *), (\mathbb{R}, +, *)$ *- 0 - нейтр. эл-т +*

2) $(M_n(\mathbb{R}), +, *)$

Определение 1.4. Если в R $\exists 1 \in R$, т. ч.:
$$1 * a = a * 1 = a, \forall \in R$$
то 1 наз-ся единицей кольца.

1.2 Сравнения и вычеты

Определение 1.5. Назовём $a, b \in Z$ сравнимыми по модулю n ($n \in \mathbb{N}, n > 1$), если a и b имеют равные остатки при делении на n.

Обозначение.

$$a \equiv b \pmod{n} \iff a - b = qn, q \in \mathbb{Z}$$

$$2 \equiv 17 \pmod{5}$$

$$3 \equiv 0 \pmod{3}$$

Замечание. *Сравнения по одному и другому* $\mod$ *можно складывать и умножать:*

$$\begin{cases} a_1 \equiv b_1 \pmod{n} \\ a_2 \equiv b_2 \pmod{n} \end{cases} \Rightarrow \begin{cases} a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{n} \\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n} \end{cases}$$

Доказательство.

$$(a_1 \pm a_2) - (b_1 \pm b_2) = (a_1 - b_1) \pm (a_2 - b_2) = q_1 n \pm q_2 n = n(q_1 \pm q_2) \vdots n$$

$$a_1 a_2 = (b_1 + q_1 n)(b_2 + q_2 n) = (b_1 b_2 + (q_2 b_1 + q_1 b_2 + q_1 q_2 n)n) \vdots n$$

$$\Rightarrow a_1 a_2 - b_1 b_2 \vdots n$$

□

Обозначение.

$$a \in \mathbb{Z}$$

$$\{\, a + n \cdot q \,\} \Rightarrow \overline{a} \text{ - класс вычетов } a \text{ по модулю } n$$

Классы вычетов по модулю $n \to \mathbb{Z}_n$*:*

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$$

Замечание.

$$\overline{a} + \overline{b} = \overline{a + b}$$

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

Проверка коректности:

$$\begin{cases} a \equiv a_1 \pmod n \\ b \equiv b_1 \pmod n \end{cases} \Rightarrow \overline{a} + \overline{b} \stackrel{?}{=} \overline{a_1} + \overline{b_1}$$

$$a + b \equiv a_1 + b_1$$
$$\overline{a} + \overline{b} \equiv \overline{a + b} \equiv \overline{a_1 + b_1} \equiv \overline{a_1} + \overline{b_1}$$

Утверждение 1.3. *Мн-во Z_n классов вычетов по мод. n явл-ся кольцом с операциями* "$+$" "$*$"

Доказательство. Опер-ция опр-на и кореектна:

$$(\mathbb{Z}_n, +) \text{ - абелева группа}$$

$$\overline{0} \text{ - нейтральный эл-т}$$

$\square$

Определение 1.6. Пусть R - кольцо с 1.
Эл-т $a \in R$ - обратимый $\iff \exists b \in R \colon a * b = b * a = 1$

Определение 1.7. R^* - мн-во всех обратимых эл-ов кольца R с 1.

Утверждение 1.4. R^* *- группа с операцией умножения.*

Доказательство. Покажем, что если a обратим, то обратный к нему эл-т b тоже обратим:

$$a * b = b * a = 1 \Rightarrow \text{ по опр-ю это верно}$$

$$\Rightarrow a \in R^* \Rightarrow b \in R^*$$

Покажем теперь, что если $a, b \in R^* \Rightarrow a * b \in R^*$:

$$a, b \in R^* \Rightarrow a^{-1}, b^{-1} \in R^*$$

$$(ab)^{-1} = b^{-1}a^{-1}$$
$$abb^{-1}a^{-1} = a * 1 * a^{-1} = 1$$
$$\Rightarrow a \cdot b \in R^*$$

$\square$

Задача 1.1. Z_n^* - мн-во всех классов вычетов, взаимно простых с n.

Утверждение 1.5. *В любом кольце R:*

$$0 * a = a * 0 = 0, \forall a \in R$$

Доказательство.

$$0 * a + 0 * a = (0 + 0) * a = 0 * a$$

$$0 * a = 0$$

$\square$

Следствие 1.1. *Если R - ненулевое кольцо с 1. То $0 \neq 1$:*

Доказательство. От прот. пусть $0 = 1$:
$\forall a \in R$: $a = a * 1 = a * 0 = 0 \Rightarrow R$ - нулевое. Противоречие!!! $\square$

Следствие 1.2. *Если R ненулевое кольцо с 1, то $0 \notin R^*$*

Определение 1.8. Мн-во F с опред. на нём бинарными алг. операциями $+, *$ наз-ся **полем**, если:

1) $(F, +)$ - абелева группа с нейтр. эл-ом 0.

2) $(F \setminus \{ 0 \}, *)$ - абелева группа с нейтр. эл-ом 1.

3) $(a + b)c = ac + bc$ - дистрибутивность.

Замечание. *В любом поле содерж. 0 и 1.* $\Rightarrow |F| \geq 2$

Замечание.

$$F^* = F \setminus \{ 0 \} \text{ - мультипликативная группа поля}$$

Определение 1.9. Поле - это коммутативное колько с 1, у кот. каждый ненулевой эл-т обратим.

Пример. *1)* $(\mathbb{Q}, +, *)$ *- поле рац. чисел.*

2) $(\mathbb{R}, +, *)$ *- поле действ. чисел.*

3) $(\mathbb{C}, +, *)$ *- поле комплексных чисел.*

4) $(Boolean)$

Утверждение 1.6. *В поле нет делителей нуля.*

Доказательство. Пусть $a \cdot b = 0, a \neq 0, b \neq 0$:

$$a \cdot b = 0 \Rightarrow a = 0 \cdot b^{-1} = 0!!!$$

□

Теорема 1.1. *Кольцо классов вычетов $\mathbb{Z}_n$ явл-ся полем $\iff$ n - простое.*

Доказательство. a) Необходимость. Пусть n - сост. $\Rightarrow \exists p, q > 1 \colon n = pq$

$\overline{p} \cdot \overline{q} = \overline{p \cdot q} = \overline{n} = \overline{0} \Rightarrow \overline{p}, \overline{q}$ - делители 0 - противоречие с тем, что $\mathbb{Z}_n$ - поле!!!

b) Дост. Пусть n - простое, покажем, что $(\mathbb{Z}_n \setminus \{ 0 \}, \cdot)$ - абелева группа. Нетривиальная часть: покажем, что $\forall \overline{a} \neq \overline{0}, \exists$ обратимый. Для этого покажем, что:

$$\overline{0} \cdot \overline{a}, \overline{1} \cdot \overline{a}, \dots, \overline{(n-1)}\overline{a} \text{ - попарно различны.}$$

Пусть $\overline{k}\overline{a} = \overline{l}\overline{a}$, б. о. о. $0 \leq k < l \leq n-1$.

$$\overline{(l-k)a} = \overline{o} \iff n|(l-k)a$$

Однако $n \nmid a, \Rightarrow n|(l-k) \Rightarrow l = k!!! \Rightarrow \exists b \colon \overline{b}\overline{a} = \overline{a}\overline{b} = \overline{1}$ и $\overline{b} \neq \overline{0}$

□

2 Лекция 15

2.1 Характеристика поля

F - поле.

$$\exists 0, 1 \in F, 0 \neq 1$$

$$\underbrace{1 + 1 + 1 + \ldots + 1}_{n} = n_F$$

Положим:

$$0_F = 0$$

$$(-n_F) = -(n_F), n \in \mathbb{N}$$

Лемма 2.1.

$$(n+m)_F = n_F + m_F$$

$$(nm)_F = n_F \cdot m_F$$

Доказательство. $n > 0, m > 0$:

$$(1 + 1 \underset{n}{+} \ldots + 1)(1 + 1 \underset{m}{+} \ldots + 1) = 1 + 1 \underset{n \cdot m}{+} \ldots + 1$$

$\square$

Определение 2.1. Хар-кой поля F наз-ся наим. натур. число $n \in \mathbb{N}$, т. ч.:

$$n_F = 0$$

Если $\forall n \in \mathbb{N}, n_F \neq 0$, то говорят, что хар-ка равна 0.

Пример. $\mathbb{Z}_p$: $\overline{1} + \overline{1} \underset{p}{+} \ldots + \overline{1} = \overline{0} = \overline{p}$
Поля: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *имеют хар-ку 0.*

Обозначение. $char(F)$ *- хар-ка поля* F

Утверждение 2.1. *Если поле* F *имеет ненулевую хар-ку* ($char(F) \neq 0$), *то* $char(F) = p$, *где* p *- простое число.*

Доказательство. От прот., пусть $char(F) = n$, n - составное:

$$n = p \cdot q, 1 < p, q < n$$

$$n_F = p_F \cdot q_F = 0!!! \text{(Прот-е, т. к. в поле нет делителей нуля.)}$$

$$\Rightarrow char(F) \text{ - простое.}$$

$\square$

Определение 2.2. Пусть G - группа/кольцо/поле. Непустое подмн-во $H \subset G$ наз-ся **подгруппой/подкольцом/подполем**, если оно само является группой/кольцом/полем, отн-но операции, опр-ой на G.

Утверждение 2.2. *Если* H *- подгруппа в группе* G, *то* $e_G = e_H$.

Доказательство.

$$e_H \cdot e_H = e_H$$

В G для e_H есть обратный e_H^{-1}:

$$e_H = e_H \cdot e_G = e_G$$

$\square$

Следствие 2.1. *У подкольца* 0 *совпадает с* 0 *кольца, а у всякого подполя 0 и 1 совпадают с 0 и 1 поля.*

$$(F, +) \text{ - аб. гр. с нейтр. эл-ом } 0$$

$$(F, *) \text{ - аб. гр. с нейтр. эл-ом } 1$$

Утверждение 2.3 (Критерий подгруппы)**.** *Непустое подмн-во H в группе G явл. подгруппой в ней* $\iff$

a) H замкнуто отн-но групповой оп-ции в G (*)

$$\forall a, b \in H (a * b \in H)$$

b) H замкнуто отн-но взятия обратного эл-та, т. е.:

$$\forall a \in H (a^{-1} \in H)$$

Доказательство. 1) **Необх.** Пусть H - подгруппа в G $[H \leq G]$ - очев., по опр-ю подгруппы.

2) **Дост.** $H \neq \emptyset$ и выполн-ся усл-я $a), b)$

$$a) \iff \text{"*"опр-на в } H$$

- Ассоц-ть вып-ся в H, т. к. вып-ся в G
- $\forall a \in H, \exists a^{-1} \in H$
- $\forall a \in H \Rightarrow \exists a^{-1} \in H \Rightarrow a * a^{-1} = e \in H$

$\square$

Утверждение 2.4. *Пусть G - группа/кольцо/поле. Пусть G_i - подгруппа/подкольцо/подполе G. Тогда:*

$$\bigcap_i G_i \text{ - подгруппа/подкольцо/подполе}$$

Доказательство. Докажем для поля F:

$$\forall i, F_i \leq F$$

$$(F_i, +) \text{ - аб. группа} \Rightarrow$$

$$\forall i\colon \begin{cases} \forall a, b \in F_i \Rightarrow a + b \in F_i \\ \forall a \in F_i \Rightarrow -a \in F_i \end{cases} \to \bigcup_i (F_i, +) \text{ - аб. группа.}$$

$\forall i\colon (F_i^*, *)$ - аб. группа $\Rightarrow \forall a, b \in F_i^* \Rightarrow a{*}b \in F_i, a^{-1} \in F_i \Rightarrow (\bigcap\limits_i F_i^*)$ - аб. группа.

□

2.2 Гомоморфизим и изоморфизм групп.

Пусть $(G_1, *)$, $(G_2, *)$ - группы.

Определение 2.3. Отображение $\phi : G_1 \to G_2$ наз-ся гомоморфизмом, если ϕ сохраняет в этих группах операции.

$$\forall a, b \in G_i \hookrightarrow \phi(a \circ b) = \phi(a) * \phi(b)$$

Определение 2.4. Отобр. $\phi : X \to Y$ наз-ся инъективным, если:

$$\forall a, b \in X\colon a \neq b \hookrightarrow \phi(a) \neq \phi(b)$$

Определение 2.5. Отобр. $\phi : X \to Y$ наз-ся сюрьективным, если:

$$\phi(X) = Y, (\forall y \in Y, \exists x \in X\colon \phi(x) = y)$$

Определение 2.6. Отобр. $\phi\colon X \to Y$ наз-ся биективным, если оно С + И.

Определение 2.7. **Изоморфизм** - биективный гомоморфизм.

Замечание. *Всё перечисленное для групп переносится на кольца и поля.*

Утверждение 2.5. *При гомоморфизме групп $f : G_1 \to G_2$:*

a) Нейтральный эл-т переходит в нейтральный:

$$f(e_{G_1}) = e_{G_2}$$

b) ϕ - коммутирует со взятием обратно эл-та:

$$\phi(a^{-1}) = \phi^{-1}(a)$$

Доказательство. a) $*$ - умножение:

$$e_1 * e_1 = e_1 \Rightarrow \phi(e_1) \cdot \phi(e_1) = \phi(e_1) = \phi^{-1}(e_1)$$

$$\phi(e_1) = \phi(e_1) \cdot e_2 = e_2$$

b)

$$a \cdot a^{-1} = a^{-1} \cdot a = e_1$$

$$\phi(a)\phi(a^{-1}) = \phi(a^{-1})\phi(a) = e_2$$

$$\phi(a^{-1}) = \phi^{-1}(a)$$

□

Следствие 2.2. *При гомоморфизме полей 0 и 1 первого поля переходят в 0 и 1 второго.*

2.3 Простое подполе

Определение 2.8. Поле F наз-ся **простым**, если оно не имеет подполей, отличных от него самого.

Пример. *Поле $\mathbb{Q}$ и $\mathbb{Z}_p$ - простые поля.*

Доказательство. Пусть $M \subset \mathbb{Q}$ - простое.

$$0, 1 \in M$$

$$1+1\underset{n}{+}\ldots+1=n\in M\Rightarrow\frac{1}{n}\in M\Rightarrow\frac{m}{n}\in M\Rightarrow\mathbb{Q}\subset M$$
$$\Rightarrow M=\mathbb{Q}$$

Аналогично, пусть $N\subset\mathbb{Z}_p$:

$$\overline{0},\overline{1}\in N\Rightarrow k*\overline{1}=\overline{1}+\overline{1}\underset{k}{+}\ldots+\overline{1}\in N\Rightarrow\mathbb{Z}_p\subset N\Rightarrow\mathbb{Z}_p=N$$

□

Теорема 2.2. *Всякое поле содержит пустое подполе, и притом только 1.*

Доказательство. F содержит подполя F_i ($F_i\subset F$). Положим:

$$D=\bigcap_{F_i\leq F}F_i\Rightarrow D\leq F,\text{ причём } D \text{ в любом другом подполе поля } F$$

Почему D простое подполе?
От прот., пусть $M\leq D\leq F\Rightarrow M\leq F\wedge D\not\subset M$!!, т. е. есть подполе F, в кот. нет D - противоречие.
Почему оно единственно?
От прот., пусть D и D' - 2 простых подполя $\Rightarrow D\cap D'$ - подполе поля F.

$$D\cap D'\subset D,D'\Rightarrow D\cap D'=D,D'\Rightarrow D=D'$$

□

Теорема 2.3 (Об описании простых подполей). *a) Если $char(F)=0$, то его простое подполе D изоморфно $\mathbb{Q}$*

b) Если $char(F)=p,p$ - простое, то его простое подполе D изоморфно $\mathbb{Z}_p$

Доказательство. a) $0,1\in D$. Если $n_F=0\Rightarrow n=0$

$$\Rightarrow 1+1\underset{n}{+}\ldots+1=n_F\in D\Rightarrow\exists\text{ вложение }\mathbb{Z}\text{ в }F\colon n\vdash n_F$$

Это гомоморфизм, т. к.:

$$(n+m)=n_F+m_F$$

$$(n \cdot m)_F = n_F \cdot m_F$$

Пусть $n_F = m_F \Rightarrow (n \cdot m)_F = 0 \Rightarrow n - m = 0 \Rightarrow n = m$
Покажем, что и поле $\mathbb{Q}$ может быть изоморфно вложено в $F \Rightarrow$
Нужно построить инъективный гомоморфизм:
Определеим соотв.: $\mathbb{Q} \to \frac{m}{n}, m \in \mathbb{Z}, n \in \mathbb{N} \mapsto$ решение ур-я $n_F \cdot x = m_F$, т. е. $x = m_F \cdot n_F^{-1}$
Проверим:

1) Сохранение сложения:

$$\frac{m}{n_1}, \frac{m_2}{n_2} \Rightarrow \frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2} \mapsto (n_{1_F} n_{2_F})y = m_{1_F} n_{2_F} + m_{2_F} n_{1_F}$$

$$\frac{m_1}{n_1} \mapsto n_{1_F} x_1 = m_{1_F}$$

$$\frac{m_2}{n_2} \mapsto n_{2_F} x_2 = m_{2_F}$$

$$x_1 + x_2 \stackrel{?}{=} y$$

Домножим ур-ия с x_1 и x_2 на n_2 и n_1 соотв. и сложим их:

$$n_{1_F} n_{2_F} (x_1 + x_2) = m_{1_F} n_{2_F} + m_{2_F} n_{1_F}$$

Т. к. решение единственно, то $y = x_1 + x_2$

2) Сохрание умножения:

$$\frac{m_1}{n_1} \cdot \frac{m_2}{n_2} \mapsto n_1 n_2 y = m_1 m_2$$

$$y \stackrel{?}{=} x_1 x_2$$

Перемножим ур-ия с x-ми:

$$n_{1_F} n_{2_F} x_1 x_2 = m_{1_F} m_{2_F} \Rightarrow y = x_1 x_2, \text{ т. к. решение единственно}$$

3) Инъективность

$$\frac{m_1}{n_1} \mapsto \text{ решение } n_{1_F} x = m_{1_F} \Rightarrow x = n_{1_F}^{-1} m_{1_F}$$

$$\frac{m_2}{n_2} \mapsto x \colon n_{2_F} x = m_{2_F} \Rightarrow x = n_{2_F}^{-1} m_{2_F}$$

$$\Rightarrow n_1 m_2 = n_2 m_1 \Rightarrow (n_1 m_2 - n_2 m_1) = 0$$
$$char(F) = 0 \Rightarrow n_2 m_1 = n_1 m_2 \Rightarrow \frac{n_2}{m_2} = \frac{n_1}{m_1}$$
$\Rightarrow \exists$ в F подполе $D_F \cong \mathbb{Q}$

b)
$$char(F) = p \text{ и } 0, 1 \in F \Rightarrow n_F \in F, \forall n$$
$$\Rightarrow \{ 0_F, \ldots, (p-1)_F \} \cong \mathbb{Z}_p$$

Тогда в D_F есть простое подполе, изом. $\mathbb{Z}_p \Rightarrow D_F \cong \mathbb{Z}_p$

$\square$

3 Лекция 16

3.1 Линейные пр-ва

Пусть F - поле.

Определение 3.1. ЛП (линейным пр-вом) над полем F наз-ся мн-во V, на кот. опр-ны оп-ции:

a) Сложение эл-ов из
$$V : \forall a, b \in V \hookrightarrow a + b \in V$$

b) Умножение эл-ов V на число из F:
$$\forall \lambda \in F, a \in V, \lambda a \in V$$

c) $(V_1, +)$ - абелева группа.

d) Унитарность:
$$1 * a = a, \forall a \in V$$

e) Ассоциативность отн-но скалярного множителя:
$$(\lambda \cdot \mu) a = \lambda \cdot (\mu a), \forall \lambda, \mu \in F, a \in V$$

f) Дистрибутивность:

$$(\lambda + \mu)a = \lambda a + \mu a$$

g)

$$\lambda(a+b) = \lambda a + \lambda b$$

Эл-ты ЛП принято называть **векторами**. $\overline{0}$ - нулевой вектор.

Пример. *0) Нулевое пр-во* $\{\,\overline{0}\,\}$*:*

$$\overline{0} + \overline{0} = \overline{0}$$

$$\lambda\overline{0} = \overline{0}$$

1) $M_{m\times n}(F)$ *- лин. пр-во отн-но естественных операций.*

$$M_{m\times 1}(F) = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix} \right\} = F^m \text{ - арифметическое пр-во над } F \text{ раз-ти } m$$

2) $V_i, i = 1, 2, 3.$ $F = \mathbb{R}$

3) $F[x]$ *- пр-во мн-нов с коэфф-ми из поля* F

$$F_n[x] = \{\, f(x) \in F[x] \mid deg(f) \leq n \,\}$$

3.1.1 Подпр-во ЛП

Пусть V - ЛП на поле F.

Определение 3.2. Непустое подмн-во $W \subset V$, наз-ся **подпр-вом** в V, если оно само явл-ся ЛП отн-но операций, опред. в V.

Обозначение. $W \leq V$ *-* W *подпр-во* V

Утверждение 3.1. *Если* $W \leq V$*, то* $0_W = 0_V$*, и если для* $w \in W, -w$ *- ему прот. вектор в* W*, то он же явл-ся прот. вектором в* V*.*

Доказательство. Было доказано в терминах подгрупп. □

Утверждение 3.2 (Критерий подпр-ва). *Непустое подмн-во $W \subset V$ над F - подпр-во в $V \iff$*

a) W замкнуто от-но сложения, т. е.:

$$\forall a, b \in W \hookrightarrow a + b \in W$$

b) W замкнуто от-но умножения на скаляр, т. е.:

$$\forall \lambda \in F, \forall a \in W \hookrightarrow \lambda a \in W$$

Доказательство. $\Rightarrow$) Очевидно.

$\Leftarrow$) Пусть усл-ия a и b вып-ся. Верно ли:

$$W \overset{?}{\leq} V$$

$$a \in W : (-1)a \in W. \text{ Покажем, что } (-1)a = -a$$

$$(-1)a + a = (-1)a + 1 \cdot a = (-1 + 1)a = 0a = \overline{0}$$

$$a + (-a) = \overline{0} \Rightarrow \overline{0} \in W$$

Из этих следствий следует верность критерия подпр-ва.

□

Следствие 3.1. *Пересечение любого числа подпр-в ЛП V само явл-ся подпр-вом.*

Доказательство. $W_i \leq V \Rightarrow \bigcap_i W_i \leq V$ □

3.1.2 Подполе лин. объектов системы векторов

Пусть S - произв. сист. векторов из V (возм. бесконечное)

Определение 3.3. Линейная оболочка системы S наз-ся наименьшая по включению подпр-во в V, содерж. S

Обозначение.

$$< S >= \bigcap_{W \leq V, S \leq W} W$$

Утверждение 3.3. $< S >= \{ \sum_{i=1}^{n} \alpha_i s_i \mid s_i \in S, \alpha_i \in F, n \in \mathbb{Z}_+ \}$

Замечание. *Если $n = 0$, то рассм.* $\overline{0}$

Доказательство.

$$L = \left\{ \sum_{i=1}^{n} \alpha_i s_i \;\middle|\; s_i \in S, \alpha_i \in F, n \in \mathbb{Z}_+ \right\}$$

$$s_i \in S \Rightarrow 1 \cdot s_i \in L \Rightarrow \forall s \in S, s \in L$$

Покажем, что $L \leq V \wedge S \subset L$:

$$\sum_i \alpha_i s_i \in L, \sum_i \beta_i s_i \in L \Rightarrow \sum_i (\alpha_i + \beta_i) s_i \in L$$

$$\lambda(\sum \alpha_i s_i) = \sum_i (\lambda \alpha_i) s_i \Rightarrow L \leq V$$

По опред. $\Rightarrow < S > \subset L$. Теперь покажем $L \subset < S >$:

$$s_i \in S, \forall i \Rightarrow s_i \in < S >$$

Т. к. $< S >$ - подпр-во V

$$\Rightarrow \alpha \cdot s_i \in < S >, \forall \alpha \in F \Rightarrow \sum_i \alpha_i s_i \in < S > \Rightarrow L \subset < S >$$

□

Определение 3.4. Если $< S >= V$, то говорят, что V порождено S.

Определение 3.5. ЛП V наз-ся **конечно-порождённым**, если оно имеет конечное порождающее мн-во

3.1.3 Базис

Определение 3.6. Пусть V - ЛП над F. Базисом в V наз-ся уп. система векторов $G = \begin{pmatrix} e_1 & e_2 & e_3 & \dots & e_n \end{pmatrix}$, если вып-ны усл-ия:

a) G - ЛНЗ над F (т. е. $\sum_i \alpha_i e_i = \overline{0} \iff \alpha_i = 0 \in F, \forall i$).

b) Каждый вектор пр-ва V представим в виде ЛК векторов G. Это усл-ие равносильно следующему:

$$< \{ e_1, \dots, e_n \} >= V$$

Пример. *1) F^n базис:*

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots e_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \sum_{i=1}^{n} \alpha_i e_i$$

2) $F_n[x]$ базис:

$$1, x, x^2, \dots, x^n$$

Утверждение 3.4. *Всякое конечнопорождённое ЛП V имеет базис.*

Доказательство. Среди все конечных мн-во, порождающих V, выберем наименьшее по мощности. (мощность конечного мн-ва - это число его эл-ов). $\Rightarrow S_0$. Явл-ся ли S_0 базисом?

Если S_0 ЛЗ, то $\exists s_0 \in S_0$, представимый как ЛК остальных эл-ов мн-ва $\Rightarrow S_0 \subset < S_0 \setminus \{ s_0 \} > \Rightarrow < S_0 \setminus \{ s_0 \} >= V$. Но это противоречие с тем, что S_0 - наименьшее по мощности. $\Rightarrow S_0$ - ЛНЗ. □

Утверждение 3.5 (Основная лемма теории ЛП)**.** *V - ЛП над F. $V = \begin{pmatrix} u_1 & \dots & u_n \end{pmatrix}$ и $W = \begin{pmatrix} w_1 & \dots & w_m \end{pmatrix}$. Известно, что $\forall w_i \in W$ - представим как ЛК векторв V. Тогда, если $m > n$, то сист. W - ЛЗ*

Доказательство. Индукция по n:

- База: n = 1

$$V = \begin{pmatrix} u \end{pmatrix}$$

По усл-ию:

$$w_1 = \lambda_1 u, w_2 = \lambda_2 u, \dots w_m = \lambda_m u$$

Если $\exists \lambda_i = 0$, то W - ЛЗ. Иначе возьмём ЛК:

$$\lambda_2 w_1 - \lambda_1 w_2 + 0w_3 + 0w_4 + \dots + 0w_m = 0 \Rightarrow W \text{ - ЛЗ}$$

- Переход: пусть утв. справедливо, для V, т. ч. $|V| = n-1$. Докажем, для $|V| = n$:

$$w_1 = \sum_{i=1}^{n} \lambda_{1i} u_i$$

$$\vdots$$

$$w_j = \sum_{i=1}^{n} \lambda_{ji} u_i$$

Для каждого $i = 2, m$, отнимем от w_i $w_1 \cdot \frac{\lambda_{1i}}{\lambda_{11}}$. Таким образом перейдем к системам:

$$\overline{V} = \begin{pmatrix} u_2 & \dots & u_n \end{pmatrix}, \overline{W} = \begin{pmatrix} w_2 - w_1 \cdot \frac{\lambda_{1i}}{\lambda_{11}} & \dots \end{pmatrix}$$

По предположению индукции: $\overline{W}$ - ЛЗ $\Rightarrow W$ - ЛЗ.

□

4 Лекция 17

4.1 Конечномерные ЛП

Определение 4.1. Линейное пр-во V над F наз-ся n-мерным (или размерности n), если в V сущ-ет ЛНЗ система, сост. из n векторов, а всякая система, векторов, сост. из $n+1$ вектора - ЛЗ.

Если же $\forall n \in \mathbb{N}$ в пр-ве V $\exists$ ЛНЗ система из n векторов, то V наз-ся бесконечномерным.

Обозначение.

$$dim_F V = n \ \textit{или} \ dim_F V = \infty$$

Теорема 4.1. *Пусть V - конечномерное ЛП над F. Тогда любые два базиса в V обязательно имеют одинаковое число векторов. (или равномощны)*
Причём их кол-во равно $dim_F V$.

Доказательство. a) Если G и Q - базисы, имеющие разное число эл-ов, то базис, с большим числом веткоров - ЛЗ, по основой лемме.

b) Покажем, что число векторов в базисе $G = dim_F V$.

$$G = \begin{pmatrix} e_1 & e_2 & \dots & e_n \end{pmatrix}, \text{ - ЛНЗ}$$

Покажем, что любая сист. из $W\colon\ |W| = n+1$ - ЛНЗ $\Rightarrow dim_F V = n$ $\square$

Замечание. *Иногда размерность определяют как число базисных векторов.*

Замечание. *В пр-ве $\left\{ \overline{0} \right\}$ - пустой базис. $|\emptyset| = 0 \Rightarrow dim_F \left\{ \overline{0} \right\} = 0$*

Пример. *1) $V_i, i = 1,2,3$, $dimV_i = i$*

2)

$$F^n = \left\{ \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \right\}, dimF^n = n$$

Базис:

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

3)

$$M_{m\times n}(F), dimM_{m\times n} = m \cdot n$$

4)

$F_n[x]$ *- мн-ны с коэффициентами из поля* $F, dimF_n[x] = n + 1$

Базис: $1, x, x^2, \dots, x^n$

5) *$\mathbb{C}$ - над $\mathbb{C}$: $dim_{\mathbb{C}}\mathbb{C} = 1$. Базис: 1*
$\mathbb{C}$ - над $\mathbb{R}$: $dim_{\mathbb{R}}\mathbb{C} = 2$. Базис: 1, i

$$z = a \cdot 1 + b \cdot i, a, b \in \mathbb{R}$$

6) *$\mathbb{R}$ над $\mathbb{Q}$ - бесконечномерное ЛП. Докажем бесконечномерность от противного:*

Доказательство. Пусть $dim_{\mathbb{Q}}\mathbb{R} = n$. Выберем произвольное число $r \in \mathbb{R}, r \underset{G}{\longleftrightarrow} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \dots \\ \alpha_n \end{pmatrix}, \alpha_i \in \mathbb{Q}$. Т. е. $\mathbb{R} \cong \mathbb{Q}^n$ - счётно, что противоречит континуальности $\mathbb{R}$. □

Теорема 4.2. *Пусть S - произв. система (конеч. или бесконечная) система векторов в конечномерном ЛП V над F. Тогда макс. ЛНЗ подсистема S_0 в S образует базис в $< S >$.*
(P. S. Максимальная, т. е. если добавить ещё один вектор, то она станет ЛЗ).

Доказательство. По т. из прошлой лекции, каждый вектор из $< S >$ представим в виде ЛК веткоров из S. Покажем, что $\forall s \in S$ представим в виде ЛК вект. из S_0.

- $s \in S_0$ - очев
- $s \in S \backslash S_0$. Рассм. (S_0, s). Она ЛЗ по соглашению максимальности. Тогда вектор s представим в виде ЛК векторов из S_0.

□

Следствие 4.1. *ЛП V над F конечномерное $\iff$ V - конечнопорождённое.*

Доказательство. a) Необх. Пусть $dim_F V < \infty$. Тогда конечный базис - это порождающая система.

b) Дост. Пусть V - конечнопорождённое $\overset{Th}{\Rightarrow}$ $\exists$ конечный базис $\Rightarrow$ его мощность $= dim_F V$

□

Теорема 4.3. *Любую ЛНЗ систему векторов конечномерного ЛП V можно дополнить до базиса в V.*

Доказательство. Пусть S состоит из всех векторов V. Тогда $< S >= V$. Пусть S_0 - ЛНЗ подсистема в S. Пусть $|S_0| = k$, т. е. S_0 сост. из k векторов. Если S_0 - макс. ЛНЗ подсистема в S, то, по предыдущей теореме, это базис. Иначе $\exists S_{k+1} \in S$, т. ч. $S_1 = (S_0, S_{k+1})$ - ЛНЗ. Если S_1 - макс. ЛНЗ подсист., то S - базис в $< S >$. Т. к. V - конечномерное, то этот процесс оборвётся за конечное число шагов, т. к. не сущ-ет ЛНЗ подсистемы из больше чем $dim_F V$ векторов. □

V - конечном. ЛП над F, $G = \begin{pmatrix} e_1 & e_2 & \dots & e_n \end{pmatrix}$ - базис в V.

$$a \in V, a = \sum_{i=1}^{n} \alpha_i e_i = E \cdot \alpha, \alpha = \begin{pmatrix} \alpha_1 \\ \dots \\ \alpha_n \end{pmatrix} \in F^n$$

Утверждение 4.1. *a) Для каждого вектора $a \in V$, его коорд. столбец отн-но базиса G определён одно-но.*

b) При сложении векторов, их коорд. столбцы складываются, а при умножении вектора на $\lambda \in F$, коорд. столбец умнож. на λ.

Доказательство.

$$a = G\alpha, b = G\beta$$
$$a + b = G\alpha + G\beta = G(\alpha + \beta)$$
$$\lambda a = \lambda G\alpha = G(\lambda\alpha)$$

□

4.1.1 Изоморфизм ЛП

Определение 4.2. Пусть V и W - ЛП над F. Тогда $\phi : V \to W$. Наз-ся изоморфизмом, если:

a) ϕ - биективно

b) ϕ - сохр. определённые в V и W оп-ции:

$$\phi(a + b) = \phi(a) + \phi(b)$$
$$\forall \lambda \in F, \phi(\lambda a) = \lambda\phi(a)$$

Замечание. $\phi(\overline{0_v}) = \overline{0_w}$

Теорема 4.4. *Пусть V - конечном. ЛП над F и $dim_F V = n$. Тогда $V \cong F^n$ (изоморфно).*

Доказательство. Фикс. $G = \begin{pmatrix} e_1 & e_2 & \dots & e_n \end{pmatrix}$ - базис в V_0.

$$V \ni a \xleftrightarrow{\phi} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \text{ т. ч. } a = G\alpha$$

$$\phi : V \to F^n \text{ по пред. утв. сохр.} + \text{ и } \cdot\lambda$$

Проверим биективность:

- ϕ - инъективно?

$$\phi(a) = \phi = \beta = \phi(b) \Rightarrow \phi(a - b) = \phi(a) - \phi(b) = \alpha - \beta = 0 \Rightarrow$$

$$a - b = G \cdot 0 = \overline{0} \Rightarrow a = b$$

- ϕ - Сюрьективно?

$$\forall \alpha \in F^n \colon \exists a = G\alpha \Rightarrow \phi(a) = \alpha$$

Ч. Т. Д.

□

Следствие 4.2 (Теорема об изоморфизме лин. пр-в)**.** *Два конечном. ЛП V_1 и V_2 над F изоморфны $\iff$ $dim_F V_1 = dim_F V_2$*

Доказательство. a) Необх. Пусть $dim_F V_1 = n \Rightarrow G = \begin{pmatrix} e_1 & \dots & e_n \end{pmatrix}$ - базис в V_1.

$\exists$ изоморф. $\phi : V_1 \to V_2$. $\phi(G) = \begin{pmatrix} \phi(e_1) & \dots & \phi(e_n) \end{pmatrix}$ - базис ли в V_2?

$$\forall b \in V_2 \colon b = \phi(a) = \phi(G \cdot \alpha) = \phi(G) \cdot \alpha$$

$$\phi(G) \text{ - ЛНЗ } \left(\phi\left(\sum_i \alpha_i e_i \right) = \sum_i \alpha_i \phi(e_i) \right)$$

Т. к. при изоморф. ЛНЗ $\mapsto$ ЛНЗ.

$$\Rightarrow dim_F V_2 = n$$

b) По предыдущей теореме, $V_1 \underset{\phi}{\cong} F^n \underset{\psi}{\cong} V_2$. Тогда $V_1 \underset{\phi \circ \psi^{-1}}{\cong} V_2$ ($\phi \circ \psi^{-1}$ - композиция изоморфизмов).

$\square$

<u>Следствие</u> 4.3. *Если пр-ва рассм. над одним и тем же полем, то единственной существенной хар-ой этих пр-в является размерность.*

<u>Теорема</u> 4.5. *Пусть F - конечное поле, т. ч. $char(F) = p$ - простое. Тогда $\exists n \in \mathbb{N}$, т. ч. $|F| = p^n$*

Доказательство. Было док-но, что в $F, \exists D_F \cong \mathbb{Z}_p, |\mathbb{Z}_p| = p$. Рассм. поле F как ЛП над полем D_F.

$$dim_{D_F} F = n, G \text{ - базис } F \text{ над } D_F$$

$$\forall a \in F, a = G \begin{pmatrix} \alpha_1 \\ \dots \\ \alpha_n \end{pmatrix}, \alpha \in D_F^n, |F| = \left| \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \right\}, \alpha_i \in D_F \right| = p \times p \dots p \times p = p^n$$

$\square$

<u>Замечание</u>. *Пусть V - ЛП размерности m над конечным полем F: $|F| = p^n$. Тогда $|V| = p^{nm}$*

Доказательство.

$$G = \begin{pmatrix} e_1 & \dots & e_n \end{pmatrix}$$

$$V \ni v = G \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

$$|V| = p^n \times \dots \times p^n = (p^n)^m = p^{nm}$$

$\square$

Вывод: конечномерное ЛП над конечным полем, содержит конечное число элементов.

5 Лекция 18

F - поле

Определение 5.1. Система линейных ур-ий (СЛУ) - система ур-ий, сост. из ур-ий первой степени:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases} \tag{1}$$

Причём, $a_{ij}, b_i \in F$

Обозначение.

$$A \in M_{m \times n}(F)$$

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in F^n$$

$$B \in F^m$$

Тогда система записывается в формате:

$$AX = B$$

Расширенной матрицей A наз-ся:

$$\widetilde{A} = (A|B) \in M_{m \times (n+1)}(F)$$

Определение 5.2. СЛУ наз-ся **совместной**, если она имеет хотя одно решение. Если она не имеет решений, то она **несовместна**.

Определение 5.3. Совместная СЛУ наз-ся **определённой**, если она имеет **единтсвенное решение**, и **неопределённой** — иначе.

Утверждение 5.1. *Всякое решение X системы (1) - это набор коэф., с кот. столбец B свобоных членов, представляется в виде ЛК столбцов матрицы A.*

Доказательство. Стобцы матрицы AX - это ЛК столбцов A с коэф. из X $\square$

Следствие 5.1. *Если столбцы A - ЛНЗ, то система (1) имеет не более чем одно решение.*

Доказательство. Если A - несовместна, то следствие верно. Иначе: Пусть $X_1 \neq X_2$ — два решения.

$$AX_1 = b$$

$$AX_2 = b$$

$$\Rightarrow AX_1 - AX_2 = A(X_1 - X_2) = 0, \text{ причём } X_1 - X_2 \neq 0$$

Получили, что есть нетрив. ЛК столбоцов матрицы A, дающая 0, что противоречит ЛНЗ столбцов A. $\square$

Определение 5.4. Системе:

$$AX = B$$

Соотв. **однородная** система:

$$AX = 0$$

Утверждение 5.2. *Мн-во V_0 решений однородной СЛУ явл-ся подпр-ом в F^n ($V_0 \leq F^n$)*

Доказательство.

$$X_1, X_2 \in V_0$$
$$AX_1 + AX_2 = A(X_1 + X_2) = 0 \Rightarrow (X_1 + X_2) \in V_0$$
$$AX_1 = 0 \Rightarrow \lambda AX_1 = 0, \lambda \in F$$
$$X = 0 \in V_0$$
$$\Rightarrow V_0 \leq F^n$$

$\square$

Утверждение 5.3. *Пусть даны: неоднородн система $AX = B$ и V_b — её мн-во решений. Пусть также X_0 — частное решение этой СЛУ. Пусть $AX = 0$ соотв. однородн. СЛУ и V_0 - её решения. Тогда:*

$$V_b = X_0 + V_0$$

Доказательство. $\supseteq$)

$$X_0 + V_0 = \{\, X_0 + u \mid u \in V_0 \,\}$$

$$A(X_0 + u) = AX_0 + Au = AX_0 = B \Rightarrow X_0 + u \in V_b$$

$\subseteq$)

$$\forall X \in V_b$$

$$AX = B = AX_0 \Rightarrow A(X - X_0) = B \Rightarrow X - X_0 \in V_0 \Rightarrow X \in V_0 + X_0$$

$\square$

5.1 Элементарные преобразования строк матрицы

Определение 5.5. Элементарные преобразования (ЭП) строк матрицы $M_{m\times n}(F)$ — это преобразования 3-ех типов:

I тип: $(i \neq j)$: К i-ой строке M прибавляем j-ую строку, умноженную на $\lambda \in F$:

$$\overline{a_i} \mapsto \overline{a_i} + \lambda \overline{a_j}$$

II тип: $(i \neq j)$: перемена местами i-ой и j-ой строки:

$$\overline{a_i} \leftrightarrow \overline{a_j}$$

III тип: i-ая строка умножается на $\lambda \neq 0$.

Утверждение 5.4. *ЭП строк M $\iff$ умножению M слева на одну из элементарных матриц.*

$$E_{ij} \text{ - матрица с 1 в } (i;j) \text{ и 0 в других местах}$$

I тип:

$$D_{ij} = E + \lambda E_{ij}$$

II тип:

$$P_{ij} = E - E_{ii} - E_{jj} + E_{ij} + E_{ji}$$

III тип:

$$Z_i = E + E_{ii} \cdot \lambda$$

Утверждение 5.5. *Все матрицы ЭП обратимы.*

Доказательство.
$$D_{ij}^{-1}(\lambda) = D_{ij}(-\lambda)$$
$$P_{ij}^{-1} = P_{ij}$$
$$Z_i^{-1}(\lambda) = Z_i(\lambda^{-1})$$
□

Задача 5.1. Показать, что если совершать умножение матрицы M на матрицы ЭП нужно размера **справа**, то получатся ЭП столбцов.

Определение 5.6. Для строки $\begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix}$, первый ненулевой её эл-т наз-ся **лидером**. (или ведущим элементом)

Пример.
$$\begin{pmatrix} 0 & 0 & 0 & \underline{7} & 4 & 0 & 0 \end{pmatrix}$$

Определение 5.7. Матрица $A_{m\times n}$ наз-ся **ступенчатой**, если выполняются два условия:

a) Если a_{ij} и $a_{i+1,k}$ — лидеры 2-х соседний строк, то $j < k$

b) Ниже нулевой строки A могут расп-ся только нулвые строки A.

Теорема 5.1. *Всякую матрицу можно привести к ступенчатому виду с помощью конечного числа ЭП строк.*

Док-во: ***Прямой ход метода Гаусса.*** $A_{m\times n}$. Доказывать будем индукцией по m (числу строк).

База: $m = 1$ - очев., т. к. одна строка — это уже ступеначатая матрица.

Предп. инд.: Пусть дана матрица размер $(m-1)\times n$ - утв. справедливо. Д-ем для матр. $m \times n$.

Найдём в матрице A лидера строки с наименьшим номером столбца. При необходимости, передвинем его на 1-ую строку A. Пусть теперь a_{1k} - лидер первой строки. Используя ЭП I типа, обнулим k-ые члены строк ниже. Мысленно уберём 1-ую строку и применим предп. инд-ции к оставшейся матрице. Получили матрицу ступ. вида.

□

Определение 5.8. Ступенчатая матрица A наз-ся упрощённой, если вып-ся два усл-ия:

a) Лидеры всех строк равны 1.

b) Столбцы, содерж. лидеров строк, содержат только нулевые эл-ты, за искл. лидера, кот. равен 1

Теорема 5.2. *Всякую ненулевую матрицу, можно привести к упрощ. виду, с помощью конечного числа ЭП строк.*

Док-во: ***Обратный ход метода Гаусса.*** Приведём A к ступенч. виду. Пусть $a_{1k_1}, a_{2k_2}, \ldots, a_{rk_r}$ — лидеры строк ступ. матрицы A'.
Для каждого $i = \overline{1, r}$ умножим i-ую строку на $\frac{1}{a_{ik_i}}$. Тогда лидеры станут равны 1.
Затем, будем идти от r-ой строки к 1-ой. Для i-ой строки, обнулим эл-ты a_{jk_i} над ней ЭП I-ого типа. Получили нужный вид. □

Теорема 5.3. *Если от СЛУ $(A|B)$ перейти к СЛУ $(A'|B')$ с помощью конечного числа ЭП строк, то эти системы эквив-ны.*

Доказательство. Дост-но док-ть для одно ЭП:

$$\exists \text{ ЭМ } Q\colon (A'|B') = (QA|QB)$$

V - мн-во решений СЛУ $(A|B)$. V' - мн-во решений СЛУ $(A'|B')$.

$$X_0 \in V \Rightarrow AX_0 = B \Rightarrow QAX_0 = QB \Rightarrow A'X_0 = B' \Rightarrow X_0 \in V'$$
$$X_0' \in V' \Rightarrow A'X_0' = B' \Rightarrow Q^{-1}A'X_0' = Q^{-1}B' \Rightarrow AX_0' = B \Rightarrow X_0' \in V$$

□

5.2 Метод Гаусса

$$AX = B$$
$$\widetilde{A} = (A|B) \text{ - расширенная матрицы}$$

I шаг: Приведём $\widetilde{A}$ к ступ. виду $\widetilde{A}_{\text{ступ.}}$

I случай: В $\widetilde{A}_{\text{ступ.}}$ есть лидер в столбце своб. членов $\Rightarrow$ СЛУ несовм.

II случай: В $\widetilde{A}_{\text{ступ.}}$ такого лидера нет. Покажем, что СЛУ совместна.
Пусть лидеры в $\widetilde{A}_{\text{ступ.}}$: $a_{1k_1}, a_{2k_2}, \dots a_{rk_r}$

Определение 5.9. Назовём $x_{k_1}, x_{k_2}, \dots, x_{k_r}$ — **главными** (базисными), а остальные — **свободными** (параметрические).

$$1 \leq k_1 < \dots < k_r \leq n$$

II, а) Все неизв. — главные (свободных нет). Тогда $r = n$:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases}$$

Тогда $x_i = b_i$

6 Лекция 19 (СКИП)

7 Лекция 20

7.1 Применения рангов матрицы

Определение 7.1. Минор M_{ij} наз-ся **невырожденным** если $\operatorname{rk} M_{ij} =$ k

Определение 7.2. Рангом матрицы по минору наз-ся максимальный порядок среди порядков всех невырожденных миноров.

$$\operatorname{rk}_M A$$

Теорема 7.1 (Фробениуса)**.** *Для $\forall$ матрицы A:*

$$\operatorname{rk}_r A = \operatorname{rk}_c A = \operatorname{rk}_M A$$

Утверждение 7.1. *Минор явл-ся невырожденным $\iff$ его* $\det \neq 0$

Рассм. однородн систему:

$$AX = 0$$

$$V = X_0 + V_0$$

X_0 - частн. реш, V_0 - общ. реш. однородн. матрицы.

Определение 7.3. Матрица F наз-ся фунд. матрицей системы $AX = 0$, если по столбцам этой матрицы располагаются коор-т столбцы базиса пр-ва $V_0 \iff$

a) $AF = 0$

b) Столбцы F - ЛНЗ.

c) Каждое решение X_0 однор. системы $AX = 0$ — ЛК стобцов F.

Замечание. *Если система $AX = 0$ имеет только тривиальное решение, то говорят, что* ***фунд. матрицы не сущ-ет.***

Если $\operatorname{rk} A = r$, то имеем r — главных неизвестных, $n - r = d$ — свободных неизвестных.

Теорема 7.2. *Для упрощ. системы $(E_r|D)X = 0$, фунд. матрица $\Phi = \begin{pmatrix} -D \\ E_d \end{pmatrix}$*

Доказательство. a)

$$AF = \begin{pmatrix} E_r & D \end{pmatrix} \begin{pmatrix} -D \\ E_d \end{pmatrix} = E_r \cdot (-D) + D \cdot E_d = -D + D = 0$$

b)

$$\Phi \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_d \end{pmatrix} = \begin{pmatrix} -D \\ E_d \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_d \end{pmatrix} = \begin{pmatrix} * \\ \vdots \\ * \\ \lambda_1 \\ \vdots \\ \lambda_d \end{pmatrix} = 0 \Rightarrow \lambda_i = 0, \forall i$$

c)

$$X_0 \in V_0 \Rightarrow X_0 = \begin{pmatrix} * \\ \vdots \\ * \\ x_1 \\ \vdots \\ x_d \end{pmatrix}$$

$$V_0 \ni Y_0 = \Phi \begin{pmatrix} x_1 \\ \dots \\ x_d \end{pmatrix} = \begin{pmatrix} -D \\ E_d \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} = \begin{pmatrix} * \\ \vdots \\ * \\ x_1 \\ \vdots \\ x_d \end{pmatrix} \Rightarrow Y_0 = X_0$$

□

Следствие 7.1.

$$\dim V_0 = d = n - \operatorname{rk} A$$

Теорема 7.3 (Кронекера-Капелли)**.** *СЛУ* $AX = B$ *— совместна* $\iff$ $\operatorname{rk} A = \operatorname{rk} \begin{pmatrix} A & B \end{pmatrix}$

Доказательство. Приведём $\begin{pmatrix} A & B \end{pmatrix}$ к ступенч. виду. СЛУ явл. совм. (Гаусс) $\iff$ нет лидера в столбце своюю. членов. □

Теорема 7.4 (Критерий определённости совм. СЛУ)**.** *Совместная СЛУ определенна, если её ранг равен числу неизвестных.*

Теорема 7.5. *Пусть* $C = AB$*, тогда* $\operatorname{rk} C \leq min(\operatorname{rk} A, \operatorname{rk} B)$

Доказательство. i-ая строка C явл-ся ЛК строк $B \Rightarrow \dim rows(C) \leq \dim rows(B) \iff \operatorname{rk} C \leq \operatorname{rk} B$ Аналогично, $\operatorname{rk} C \leq \operatorname{rk} A \Rightarrow \operatorname{rk} C \leq min(\operatorname{rk} A, \operatorname{rk} B)$

□

7.1.1 Применнеие рангов к исследованию квадр. матрицы на обратимость

Определение 7.4. $A \in M_n(\mathbb{F})$ наз-ся обратимой $\iff \exists A^{-1} \in M_n(\mathbb{F})$:

$$A^{-1}A = AA^{-1} = E_n$$

Определение 7.5. Матрица A наз-ся обратимой слева, если $\exists B \in M_n(\mathbb{F})\colon BA = E$, справа — $\exists C \in M_n(\mathbb{F})\colon AC = E$

Теорема 7.6 (Об обратной матрице)**.** *Следующие условия на квадратную матрицу $A_{n\times n}$ эквив-ны:*

1) *A - обратима*

2) *A - обратима слева или справа.*

3) *A - невырожд.*

4) *A приводится к E_n с помощью ЭП **только строк или только столбцов**.*

5) *A представима в виде произведения элементарных матриц.*

Доказательство.

$1 \Rightarrow 2)$ Очев.

$2 \Rightarrow 3)$ Пусть $B\cdot A = E$. При этом ранг $E = n \le min(\operatorname{rk} A, \operatorname{rk} B) \le \operatorname{rk} A \le n$. Получаем $\operatorname{rk} A = n \Rightarrow A$ - невырожд.

$3 \Rightarrow 4)$ Приведём невырожд. матрицу к упрощ. виду. Получим $A_{\text{упрощ.}} = E_n$. Чтобы получить преобразования через строки, вместо столбцов (или наоборот):

$$Q_k \cdot \ldots \cdot$$

$4 \Rightarrow 5)$ Из п. 4, получаем:

$$\exists Q_1, \ldots, Q_k\colon Q_k \cdot \ldots \cdot Q_1 A = E$$

$$\Rightarrow A = Q_1^{-1} \cdot \ldots \cdot Q_k^{-1} E$$

$5 \Rightarrow 1)$

$$A = T_1 \cdot \ldots \cdot T_k \Rightarrow A^{-1} = T_k^{-1} \cdot \ldots \cdot T_1^{-1}$$
$$AA^{-1} = A^{-1}A = E$$

□

Следствие 7.2. *Вырожденные матрицы необратимы*

Следствие 7.3. *Произведение двух невырож. матриц невырожд.*

Следствие 7.4. *Мн-во всех невырож. матриц образует группу отн-но операции "$\cdot$"*

Доказательство. Операция определена по предыдущему следствию. Ассоцитавность выполняется. Нейтральный элемент — E. Обратные матрицы также невырождены. □

Обозначение. $GL_n(\mathbb{F})$ — *General Linear Group.*

7.2 Операции над подпространствами

V - конечномерн. пр-во

$$U \leq V, W \leq V$$

Определение 7.6. Пересечением подпр-в U и W наз-ся мн-во:

$$U \cap W = \{\, x \in V \mid x \in U \land x \in W \,\}$$

Утверждение 7.2.

$$U \cap W \leq V$$

Доказать сам-но.

Замечание. *Объединение двух подпр-вом не явл-ся подпр-вом в общем случае.*

Определение 7.7. Алг. сумма подпр-в U, W:

$$U + W = \{\, x_1 + x_2 \mid x_1 \in U, x_2 \in W \,\}$$

Утверждение 7.3.

$$U + W \leq V$$

Доказательство. a)

$$x, y \in U + W \Rightarrow x = x_1 + x_2, y = y_1 + y_2$$

Где $x_1, y_1 \in U, x_2, y_2 \in W$

$$x + y = x_1 + x_2 + y_1 + y_2 = (x_1 + y_1) + (x_2 + y_2) \Rightarrow x + y \in U + W$$

b) Остальное док-ть сам-но.

□

Определение 7.8. $U_i \leq V, \forall i = \overline{1, n}$

$$\sum_{i=1}^{n} U_i = \left\{ \sum_{i=1}^{n} x_i \;\middle|\; x_i \in U_i \right\}$$

Утверждение 7.4. *Пусть* $U_i =< S_i >, i = \overline{1, n}$. *Тогда*

$$\sum_{i=1}^{n} U_i =< S_1 \cup S_2 \ldots \cup S_n >$$

Определение 7.9. Объединение упор. систем векторов подразумевается конкатенация этих систем (приписывание).

Утверждение 7.5. *Пусть* $L =< \bigcup_{i=1}^{n} S_i >$.

$$U_i =< S_i > \subseteq L \Rightarrow U_1 + \ldots U_n \leq L$$

В обратную сторону:

$$L =< \bigcup_{i=1}^{n} S_i > \subset < \bigcup_{i=1}^{n} U_i > = U_1 + \ldots + U_n$$

$$\Rightarrow \sum_{i=1}^{n} U_i =< \bigcup_{i=1}^{n} S_n >$$

Следствие 7.5.

$$\dim(\sum_{i=1}^{n} U_i) \leq \sum_{i=1}^{n} \dim U_i$$

Доказательство. Пусть S_i — базис в U_i. $\dim(\sum_{i=1}^n U_i)$ равна мощности макс. ЛНЗ подсистеме $\bigcup_{i=1}^n S_i \leq$ мощности $\bigcup_{i=1}^n S_i \leq$

$$\leq \left|\bigcup_{i=1}^n S_i\right| \leq \sum_{i=1}^n |S_i| = \sum_{i=1}^n \dim U_i$$

$\square$

Следствие 7.6. $\dim(\sum_{i=1}^n U_i) = \sum_{i=1}^n \dim U_i \iff$ *когда объединение базисов в U_i дает базис в $\sum_{i=1}^n U_i$*

Определение 7.10. Пусть $U_i \leq V$. $\sum_{i=1}^n U_i$ наз-ся **прямой суммой подпр-в**, если $\forall x \in \sum_{i=1}^n U_i$:

$$\exists!(x_1, x_2, \ldots, x_k), x_i \in U_i \colon x = \sum_{i=1}^n x_i$$

Обозначение.

$$\bigoplus_{i=1}^n U_i \text{ - \textit{прямая сумма}}$$

Определение 7.11 (ЛНЗ для подпр-в)**.** Подпр-ва $U_1, \ldots U_n$ наз-ся ЛНЗ, если:

$$\sum_{i=1}^n x_i = \overline{0}, x_i \in U_i \iff \forall i \colon x_i = \overline{0}$$

Теорема 7.7 (О характризации прямой суммы подпр-в)**.** *Пусть $U_i \leq V_i, i = \overline{1,k}$. Тогда следующие условия эквив-ны:*

1)
$$\sum_{i=1}^n U_i = \bigoplus_{i=1}^n U_i$$

2)
$$\forall i = \{\, 1, \ldots, n \,\} : U_i \cap (\sum_{j=1, j\neq i}^n U_j) = \{\, \overline{0} \,\}$$

3)
$$U_1, \ldots, U_n \text{ — \textit{ЛНЗ}}$$

4) *Объединение базисов U_i даёт базис в сумме U_i*

5) $\sum_{i=1}^n \dim U_i = \dim(\sum_{i=1}^n U_i)$

8 Лекция 21 (СКИП))

9 Лекция 22

9.1 Сопряжённое пр-во

V - ЛП над F

$$f : V \to F$$

Определение 9.1. f — **линейный функционал** (ЛФ), если соблюдаются:

1) Аддитивность:

$$\forall x, y \in V : f(x+y) = f(x) + f(y)$$

2) Однородность:

$$\forall \lambda \in F, \forall x \in V : f(\lambda x) = \lambda f(x)$$

Определение 9.2. V^* —

10 Лекция 24(вроде)

Утверждение 10.1. *ЛО $\phi : U \to V$ — инъективно* $\iff \ker \phi = \{\,\overline{0}\,\}$

Доказательство.

- Необх.: пусть ϕ - инъективно $\Rightarrow \forall x \neq \overline{0} \hookrightarrow$

$$\phi(x) \neq \phi(\overline{0}) = \overline{0} \Rightarrow \ker \phi = \{\,\overline{0}\,\}$$

- Дост.: пусть $\ker \phi = \{\,\overline{0}\,\}$. Покажем, что ϕ - инъективно. Пусть $\exists x_1, x_2 \in V : \phi(x_1) = \phi(x_2)$

$$\hookrightarrow \phi(x_1) - \phi(x_2) = \phi(x_1 - x_2) = \overline{0} \Rightarrow x_1 = x_2$$

$\square$

Следствие 10.1. *Пусть ϕ: $V \to W$ — ЛО, кот. удовл. одному из двух условий экв-ных условий утв-я* (10.1). *Тогда ϕ переводит ЛНЗ в ЛНЗ.*

Доказательство. Пусть система $x_1, \ldots, x_n$ — ЛНЗ. От прот., пусть:

$$\phi(x_1), \ldots, \phi(x_n) \text{ — ЛЗ}$$

Тогда $\exists$ нетрив. ЛК:

$$\lambda_1\phi(x_1) + \lambda_2\phi(x_2) + \ldots + \lambda_n\phi(x_n) = \overline{0}$$

$$\phi(\lambda_1 x_1 + \ldots + \lambda_n x_n) = \overline{0} \Rightarrow \sum_{i=1}^{n} \lambda_i x_i = \overline{0} \in \ker\phi, \exists i\colon \lambda_i \neq 0$$

Прот. с тем, что $x_1, \ldots, x_n$ — ЛНЗ. □

Теорема 10.1 (Теорема о гомоморфизмах ЛП)**.** *Пусть $\phi\colon V \to W$ - ЛО. Пусть $V = \ker\phi \oplus U$. Тогда $\exists$ канонический изоморфизм пр-в U на $\operatorname{Im}\phi$. Более того, если:*

$$\phi|_U\colon U \to \operatorname{Im}\phi \text{ — изоморфизм}$$

Доказательство. $\phi(U) \subseteq \operatorname{Im}\phi$. ...??? □

Теорема 10.2 (О ядре и образе ЛО)**.** $\phi\colon V \to W$ *— ЛО. Тогда справ-во:*

$$\dim\ker\phi + \dim\operatorname{Im}\phi = \dim V$$

Доказательство. Пусть, как в теореме (10.1), $V = \ker\phi \oplus U$:

$$\phi|_U\colon U \to \operatorname{Im}\phi \Rightarrow \dim V = \dim\operatorname{Im}\phi$$

По т. (10.1):

$$\dim V = \dim\ker V + \dim V = \dim\ker\phi + \dim\operatorname{Im}\phi$$

□

Замечание. *Верно ли, что если $\phi\colon V \to V$, то $\hookrightarrow V = \ker\phi \oplus \operatorname{Im}\phi$. Нет, это не так.*

Определение 10.1 (Матрицы ЛО)**.** $\phi\colon V \to W$. Пусть

$$G = \begin{pmatrix} e_1 & \ldots & e_n \end{pmatrix} \text{ — базис } V$$

$$G' = \begin{pmatrix} f_1 & \ldots & f_m \end{pmatrix} \text{ — базис } W$$

$$W \ni \phi(e_1) = a_{11}f_1 + \dots a_{m1}f_m$$

$$\vdots$$

$$\phi(e_n) = a_{n1}f_1 + \dots + a_{nm}f_m$$

$$A_\phi = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \in M_{m\times n}(F)$$

Можно записать иначе:

$$\begin{pmatrix} \phi(e_1) \\ \vdots \\ \phi(e_n) \end{pmatrix} = A_\phi^T \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$$

$$\begin{pmatrix} \phi(e_1) & \dots & \phi(e_n) \end{pmatrix} = \begin{pmatrix} f_1 & \dots & f_n \end{pmatrix} A_\phi$$

$$\phi(G) = f \cdot A_\phi$$

Определение 10.2. Построенная матрица A_ϕ наз-ся матрицей ЛО ϕ отн-но базисов G и G'

$$\phi \underset{(G,G')}{\longleftrightarrow} A_\phi$$

Утверждение 10.2.

$$\phi \colon V \to W$$

Пусть G — базис в V, f — базис в W

$$\phi \underset{(G,G')}{\longleftrightarrow} A_\phi, V \ni x \underset{G}{\longleftrightarrow} \alpha, \phi(x) \underset{f}{\longleftrightarrow} \beta$$

Тогда $\beta = A_\phi \alpha$

Доказательство.

$$x = G\alpha, \phi(x) = f\beta$$

$$\phi(x) = \phi(G\alpha) = \phi(G)\cdot\alpha = f \cdot A_\phi \cdot \alpha \Rightarrow \beta = A_\phi\alpha$$

$\square$

10.1 Операции над ЛО

Пусть $\mathcal{L}(V, W)$ — мн-во всех ЛО из V в W. (или $\hom(V, W)$)

$$\phi, \psi \in \mathcal{L}(V, W)$$

$$\Rightarrow (\phi + \psi)(x) = \phi(x) + \psi(x)$$
$$(\lambda\phi)(x) = \lambda\phi(x)$$

Покажем аддитивность:

$$(\phi + \psi)(x + y) = \phi(x + y) + \psi(x + y) = \phi(x) + \phi(y) + \psi(x) + \psi(y) =$$

$$= (\phi + \psi)(x) + (\phi + \psi)(y)$$

Замечание. *Легко проверить выполнение аксиом ЛП для $\mathcal{V}, \mathcal{W}$, причём в кач-ве нулевого вектора выступет нулевое отображение.*

Утверждение 10.3. *Соответствие:*

$$\phi \underset{(G,G')}{\longleftrightarrow} A_\phi$$

явл-ся изоморфизмом пр-ва $\mathcal{L}(V, W)$ на пр-во $M_{m\times n}(F)$

Доказательство. a) Сохранение " + "?

$$(\phi + \psi)(G) = \big((\phi + \psi)(e_1) \quad \dots \quad (\phi + \psi)(e_n))\big) =$$

$$= \big(\phi(e_1) + \psi(e_1) \quad \dots \quad \phi(e_n) + \psi(e_n)\big)$$
$$= \big(\phi(e_1) \quad \dots \quad \phi(e_n)\big) + \big(\psi(e_1) \quad \dots \quad \psi(e_n)\big) = f \cdot A_\phi + f \cdot A_\psi =$$
$$= f(A_\phi + A_\psi)$$

b) Биективность? Инъективность возникает из того, что только 0 имеет нулевую матрицу.
Сюрьективность? $\forall A \in M_{m\times n}(F)\exists!$ ЛО, со столбцами вида $\phi(e_1), \dots, \phi(e_n)$

$\square$

Следствие 10.2.

$$\dim \mathcal{L}(V, W) = \dim M_{m\times n} = m \cdot n = \dim W \cdot \dim V$$

10.2 Ранг лин. отображения

Определение 10.3. $\phi\colon V \to W$ — ЛО. Ранг $\phi(\operatorname{rk}\phi)$ наз-ся размерностью пр-во $\operatorname{Im}\phi$

Теорема 10.3 (О ранге лин. отображения)**.** *$\phi : V \to W$ — ЛО. Тогда $\operatorname{rk}\phi$ равен $\operatorname{rk} A_\phi$ не зависимо от выбора базисов в V и W.*

Доказательство. Вспомним рав-во:

$$\operatorname{Im}\phi =< \phi(e_1), \dots, \phi(e_n) >, \text{ где } E \text{ — базис } V$$

$$\forall i\colon \phi(e_i) \in \operatorname{Im}\phi \Rightarrow \supseteq$$

$\subseteq$? Пусть $y \in \operatorname{Im}\phi$. Тогда $\exists x \in V : y = \phi(x) = \phi(\sum_{i=1}^n x_i e_i) =$

$$= \sum_{i=1}^n x_i \phi(e_i) \in < \phi(e_1), \dots, \phi(e_n) >$$

$$\operatorname{rk}\phi = \dim\operatorname{Im}\phi = \dim < \phi(e_1), \dots, \phi(e_n) > = \operatorname{rk} A_\phi$$

□

10.3 Изменение матр. ЛО при замене базисов

Теорема 10.4. *Пусть $\phi : V \to W$ — ЛО. Пусть G, G' — базисы V, $G' = GS$, (т. е. $S = S_{G\to G'}$)*
Пусть F, F' - базисы W, $F' = FT$
Пусть $\phi \underset{(G,F)}{\longleftrightarrow} A_\phi$ и $\phi \underset{(G',F')}{\longleftrightarrow} A'_\phi$
Тогда:

$$A'_\phi = T^{-1} \cdot A_\phi \cdot S$$

Доказательство.

$$\phi(G) = F \cdot A_\phi \text{ и } \phi(G') = F' \cdot A'_\phi$$

$$F = F' \cdot T^{-1}$$

Имеем:

$$\phi(G') = \phi(GS) = \phi(G) \cdot S = F \cdot A_\phi \cdot S = F' \cdot T^{-1} \cdot A_\phi \cdot S$$

$$\Rightarrow A'_\phi = T^{-1} \cdot A_\phi \cdot S$$

□

Следствие 10.3. *Пусть T и S невырожденные матрицы, т. ч.:*

$$T^{-1} \cdot A \cdot S \text{ — имеет смысл}$$

Тогда:

$$\operatorname{rk}(T^{-1} \cdot A \cdot S) = \operatorname{rk} A$$

Доказательство.

$$A = A_\phi, \phi\colon V \to W$$

$$\operatorname{rk}(A_\phi) = \operatorname{rk}(T^{-1} \cdot A_\phi \cdot S)$$

Т. к. ранг не зависит от выбранных базисов. □

К какому наиболее простому виду можно привести матрицу отображения подоходящей заменой базиса? Ответ: к единичному диагональному виду.

Теорема 10.5. *Пусть $\phi\colon V \to W$ — ЛО. Тогда в V и W $\exists G, F$ — базисы, т. ч.:*

$$\phi \underset{(G,F)}{\longleftrightarrow} \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}, r = \operatorname{rk} \phi$$

Доказательство. Пусть $V = U \oplus \ker \phi$, U — прямое дополнение к $\ker \phi$

$$\phi|_U\colon U \to \operatorname{Im} \phi$$

Выберем в пр-ве V базис, согласованный с разл. в $\oplus$, т. е.:

$$e_1, \dots e_r \text{ — базис в } U, e_{r+1}, \dots, e_n \text{ — базис в } \ker \phi$$

$$f_1 = \phi(e_1), \dots, f_r = \phi(e_r) \text{ — базис в } \operatorname{Im} \phi$$

И дополним его до базиса в W

$$f_{r+1}, \dots, f_n$$

Покажем, что пара базисов (E, F) — искомая пара базисов.

$$\phi(e_1) = f_1 = 1 \cdot f_1 + 0 \cdot f_2 + \ldots + \cdot 0 \cdot f_n$$

$$\phi(e_2) = f_2 = 0 \cdot f_1 + 1 \cdot f_2 + 0 \cdot f_3 + \ldots + 0 \cdot f_n$$

$$\vdots$$

$$\phi(e_r) = 0 \cdot f_1 + 0 \cdot f_2 + \ldots + 0 \cdot f_{r-1} + 1 \cdot f_r + 0 \cdot f_{r+1} + \ldots + 0 \cdot f_n$$

$$\phi(e_{r+i}) = \overline{0}, \forall i > 0$$

□

11 Лекция 26

11.1 Определители произовльного порядка

$$\sigma \colon M \to M \text{ — подстановка}$$

Утверждение 11.1. *Следующие три определения эквив-ны: подстановка наз-ся* ***чётной****, если:*

1) *Чётности верхней и нижней строк совпадают*

2) $n_1 + n_2$ *— чётно, где* n_i *- число инверсий в* i*-ой строке* ($i = 1, 2$)

3) *Она раскладывается в произведение чётного числа транспозиций*

Доказательство.

$1 \iff 2)$ $n_1 + n_2 \in 2\mathbb{Z} \iff \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{pmatrix} \text{ч} \\ \text{ч} \end{pmatrix} \vee \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{pmatrix} \text{нч} \\ \text{нч} \end{pmatrix} \iff$ чётность строк совпадет

$1 \iff 3)$ Т. к. каждая транспозиция меняет чётность кол-ва инверсий, то число множителей в произведении чётно.

□

Обозначение. *Знак подстановки*:

$$\varepsilon \colon S_h \to \{\pm 1\}$$

$$\varepsilon(\sigma) = \begin{cases} 1, & \text{если } \sigma \text{ — чётно} \\ -1, & \text{если } \sigma \text{ — нечётно} \end{cases} = (-1)^{\mathrm{inv}(\sigma)} = (-1)^{\tau(\sigma)}$$

$\mathrm{inv}(\sigma)$ *— суммарное число инверсий* ($n_1 + n_2$)

$\tau(\sigma)$ *— размер минимального по кол-ву транспозиций разложения* σ

Утверждение 11.2. *Знак перестановки явл-ся гомоморфизмом мультипликативных групп:*

$$\varepsilon(\sigma \cdot p) = \varepsilon(\sigma) \cdot \varepsilon(p)$$

Доказательство.

$$\sigma = \tau_1 \dots \tau_k$$
$$p = \tau'_1 \dots \tau'_s$$
$$\Rightarrow \sigma \cdot p = \tau_1 \dots \tau_k \cdot \tau'_1 \dots \tau'_s$$
$$\varepsilon(\sigma \cdot p) = (-1)^{k+s} = (-1)^k (-1)^s = \varepsilon(\sigma) \cdot \varepsilon(p)$$

□

Вспомним определитель 3-его порядка:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{21}a_{32}a_{13} -$$
$$-a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{21}a_{12}a_{33}$$

Сделаем сопоставление:

$$a_{i_1 j_1} a_{i_2 j_2} a_{i_3 j_3} \mapsto \begin{pmatrix} i_1 & i_2 & i_3 \\ j_1 & j_2 & j_3 \end{pmatrix}$$

Слагаемое	Подстановка σ	$\varepsilon(\sigma)$
$a_{11}a_{22}a_{33}$	id	$+1$
$a_{12}a_{23}a_{31}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$+1$
$a_{13}a_{21}a_{32}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$+1$
$\vdots$	$\vdots$	$\vdots$

На основании этой таблицы строиться формула общего вида (и соотв. определение):

$$\det A = |A| = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)}$$

Утверждение 11.3. *При транспонировании матрицы A её определитель не меняется. Пусть* $a_{1\sigma(1)} \dots a_{n\sigma(n)}$ *входит в состав* $\det A$ *(и соотв. в состав* $\det(A^T)$*)*

$$\det A \to \varepsilon \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$
$$\det A^T \to \varepsilon \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

11.2 Полилинейные кососимметрические ф-ции

Определение 11.1. $f\colon V^n \to F$ наз-ся **полилинейной**, если она линейна по каждому из своих арг-ов:

$$V^n = \{\, (a_1, \ldots, a_n), a_i \in V \,\}$$
$$f(a_1, \ldots, a_n) \in F$$

Линейность подразумевает:

1) Аддитивность:

$$f(\ldots, a_i + a_i', \ldots) = f(\ldots, a_i, \ldots) + f(\ldots, a_i', \ldots)$$

2) Однородность:

$$\forall \lambda \in F\colon f(\ldots \lambda a_i \ldots) = \lambda f(\ldots a_i \ldots)$$

Пусть $\operatorname{char} F \neq 2$

Определение 11.2. Полилин. ф-ция $f\colon V^n \to F$ наз-ся кососимметрическим, если:

a) $f(\ldots a_i \ldots a_j \ldots) = -f(\ldots a_j \ldots a_i \ldots), i \neq j$

b) $f(\ldots a \ldots a \ldots) = 0$

Доказательство.

a) $\Rightarrow$ b)

$$f(\ldots a \ldots a \ldots) = -f(\ldots a \ldots a \ldots)$$

Если $\operatorname{char} F = 2$, то опр-е не пол-ся. Иначе всё ок.

b) $\Leftarrow$ a)

$$0 = f(\ldots a_i + a_j \ldots a_i + a_j) = f(\ldots a_i \ldots a_j \ldots) + f(\ldots a_i \ldots a_i \ldots) +$$
$$+ f(\ldots a_j \ldots a_j \ldots) + f(\ldots a_j \ldots a_i \ldots) =$$
$$= f(\ldots a_i \ldots a_j \ldots) + f(\ldots a_j \ldots a_i \ldots)$$

$\square$

Замечание. *В случае* $\operatorname{char} F = 2$, *п.* $b)$ *выбирается в кач-ве опр-я.*

Утверждение 11.4. *Пусть* $f\colon V^n \to F$ *— полилин. кососим., тогда* $\forall \sigma \in S_n$

$$f(a_{\sigma(1)} \dots a_{\sigma(n)}) = \varepsilon(\sigma) f(a_1 \dots a_n)$$

Доказательство. Индукция по $\tau(\sigma)$:

База: $\tau(\sigma) = 1 \Rightarrow \sigma$ — очев.

Переход: Пусть для σ, т. ч. $\tau(\sigma) < k$, утв-е вып-ся. Тогда для $\tau(\sigma) = k$, утв-е верно, (делаем ещё один *swap*, чётность мен-ся, и утв-е верно)

$\square$

Теорема 11.1 (О характеризации определителя его св-вам)**.**

$$A \in M_n(F)$$

Тогда:

a) $\det A$ *— полилин., кососим. ф-ция от строк (или столбцов) матрицы* A

b) Пусть $f\colon M_n(F) \to F$ *— полилин. кососим. ф-ция от строк (или столбцов) матрицы. Тогда:*

$$f(A) = f(E) \cdot \det A, \text{ где } E \text{ — единич. матрица}$$

Доказательство. a) Зафикс. все элем-ты, матрицы $A : a_{ij}, i > 1$:

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) \cdot a_{1\sigma(1)} \dots a_{n\sigma(n)} = \sum_j \alpha_j a_{1j}$$

— лин. форма коорд. I строки.

1) $\operatorname{char} F \neq 2$. Проверим, что $\det A$ — кососим ф-ция от строк A:

$$\det(\overline{a_1} \dots \overline{a_i} \dots \overline{a_j} \dots \overline{a_n}) \stackrel{?}{=} -\det(\overline{a_1} \dots \overline{a_j} \dots \overline{a_i} \dots \overline{a_n})$$

I. $a_{1\sigma(1)}\dots a_{i\sigma(i)}\dots a_{j\sigma(j)}\dots a_{n\sigma(n)} \mapsto \det A$

II. $a_{1\sigma(1)}\dots a_{j\sigma(j)}\dots a_{i\sigma(i)}\dots a_{n\sigma(n)} \mapsto \det A'$

$\Rightarrow \varepsilon(I) = -\varepsilon(II) \Rightarrow \det A' = -\det A$

2) $\operatorname{char} F = 2$

$$\det(\overline{a_1}\dots\overline{a_i}\dots\overline{a_j}\dots\overline{a_n}) \stackrel{?}{=} 0, (\overline{a_i} = \overline{a_j})$$

b)

$$e_1 = \begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix}$$
$$e_2 = \begin{pmatrix} 0 & 1 & \dots & 0 \end{pmatrix}$$
$$\vdots$$
$$e_n = \begin{pmatrix} 0 & 0 & \dots & 1 \end{pmatrix}$$

$$f(a_1,\dots,a_n) = f\left(\sum_{j_1} a_{1j_1}e_{j_1}, \sum_{j_2} a_{2,j_2}e_{j_2}\dots\sum_{j_n} a_{nj_n}e_{j_n}\right) =$$

$$= \sum_{j_1}\sum_{j_2}\dots\sum_{j_n}\varepsilon(j)a_1j_1\dots a_{nj_n}f(e_1,\dots,e_n) = \det A f(E)$$

□

Утверждение 11.5. *a) Если над матрицей A совершить ЭП строк I типа ($a_i \mapsto a_i + \lambda a_j$), то опр-тель не меняется.*

b) При преобразованиях второго типа ($a_i \leftrightarrow a_j$) опр-тель изменит свой знак.

c) При преобразованиях третьего типа ($a_i \mapsto \lambda a_i$) опр-тель умножается на λ

Доказательство. a)

$$\det(\overline{a_1}\dots\overline{a_i} + \lambda\overline{a_j}\dots\overline{a_n}) =$$

$$= \det(\overline{a_1}\dots\overline{a_i}\dots\overline{a_n}) + \lambda\det(\overline{a_1}\dots\overline{a_j}\dots\overline{a_j}\dots\overline{a_n}) =$$
$$= \det(\overline{a_1}\dots\overline{a_i}\dots\overline{a_n})$$

b) Из кососим.

c) Следсвие однородности.

$\square$

Определение 11.3. Матрица $A \in M_n(F)$ наз-ся верхнетреугольной (нижнетреугольной), если $a_{ij} = 0, i > j (i < j)$

Утверждение 11.6. *Определитель верхнетреугольной (нижнетреугольной) матрицы равен произведению эл-ов на главной диагонали.*

Доказательство.

$$\varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)} \to \det A$$

Если $\sigma \neq e$, то $\exists i$, т. ч. $\sigma(i) < i \Rightarrow a_{i\sigma(i)} = 0$ (Легко док-ть от прот.) $\Rightarrow$ единственное ненулевое произведение — произведение эл-ов главной диагонали. $\square$

Определение 11.4. Минором k-ого порядка матрицы A наз-ся $\det M^{i_1 i_2 \ldots i_k}_{j_1 j_2 \ldots j_k}$

Определение 11.5. Ранг матрицы по минорам наз-ся порядок её наибольшего ненулевого минора. ($\det M \neq 0$)

$$\mathrm{rk}_M A$$

Теорема 11.2 (Фробениус, 1873-75 гг.)**.** *Все 3 понятия ранга матрицы эквив-ны, т. е.:*

$$\mathrm{rk}_r A = \mathrm{rk}_c A = \mathrm{rk}_M A$$