АлГем

Сергей Григорян

1 ноября 2024 г.

Содержание

1 Лекция 15

1.1 Характеристика поля

F - поле.

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

$$1 + 1 + \underset{n}{1 +} \ldots + 1 = n_F$$

Положим:

$$0_F = 0$$

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

Лемма 1.1.

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

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

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 1.1. 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 1.1. *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:

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

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

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

□

Определение 1.2. 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 1.2. *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}:

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

□

Следствие 1.1. *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 1.3 (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
- $\forall a \in H, \exists a^{-1} \in H$
- $\forall a \in H \Rightarrow \exists a^{-1} \in H \Rightarrow a * a^{-1} = e \in H$

□

Утверждение 1.4. *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:

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

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

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

$\forall i\colon (F_i^*, *)$ - 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.

□

1.2 Гомоморфизим и изоморфизм групп.

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

Определение 1.3. Отображение $\phi : G_1 \rightarrow G_2$ 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 1.4. Отобр. $\phi : X \to Y$ наз-ся инъективным, если:

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

Определение 1.5. Отобр. $\phi : X \to Y$ наз-ся сюрьективным, если:

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

Определение 1.6. Отобр. $\phi\colon X \to Y$ наз-ся биективным, если оно С + И.

Определение 1.7. **Изоморфизм** - биективный гомоморфизм.

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

Утверждение 1.5. *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 1.2. *При гомоморфизме полей 0 и 1 первого поля переходят в 0 и 1 второго.*

1.3 Простое подполе

Определение 1.8. 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 1.2. *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 1.3 (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

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

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

$$\Rightarrow n_1m_2 = n_2m_1 \Rightarrow (n_1m_2 - n_2m_1) = 0$$

$$char(F) = 0 \Rightarrow n_2m_1 = n_1m_2 \Rightarrow \frac{n_2}{m_2} = \frac{n_1}{m_1}$$

$\Rightarrow \exists$ 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. $\mathbb{Z}_p \Rightarrow D_F \cong \mathbb{Z}_p$

$\square$

2 Лекция 16

2.1 Линейные пр-ва

Пусть F - поле.

Определение 2.1. 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
$$F_n[x] = \{\, f(x) \in F[x] \mid deg(f) \leq n \,\}$$

2.1.1 Подпр-во ЛП

Пусть V - ЛП на поле F.

Определение 2.2. 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 2.1. *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 2.2 (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:

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

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

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

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

Из этих следствий следует верность критерия подпр-ва.

□

Следствие 2.1. *Пересечение любого числа подпр-в ЛП* V *само явл-ся подпр-вом.*

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

2.1.2 Подполе лин. объектов системы векторов

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

Определение 2.3. 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 2.3. $< S >= \{ \sum_{i=1}^{n} \alpha_i s_i \mid s_i \in S, \alpha_i \in F, n \in \mathbb{Z}_+ \}$

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

Определение 2.5. ЛП V наз-ся **конечно-порождённым**, если оно имеет конечное порождающее мн-во

2.1.3 Базис

Определение 2.6. 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 2.4. *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 2.5 (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
$$V = \big(u\big)$$
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.

□

3 Лекция 17

3.1 Конечномерные ЛП

Определение 3.1. 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.

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

Теорема 3.1. *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)

$$F_n[x] \text{ - мн-ны с коэффициентами из поля } F, dim F_n[x] = n+1$$

Базис: $1, x, x^2, \ldots, x^n$

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 $r \in \mathbb{R}, r \underset{G}{\longleftrightarrow} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \ldots \\ \alpha_n \end{pmatrix}, \alpha_i \in \mathbb{Q}$. Т. е. $\mathbb{R} \cong \mathbb{Q}^n$ - счётно, что противоречит континуальности $\mathbb{R}$. □

Теорема 3.2. *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 3.1. *ЛП* V *над* F *конечномерное* $\Longleftrightarrow$ 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 $= dim_F V$

$\square$

Теорема 3.3. *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. $\square$

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 3.1. *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.

$$a = G\alpha, b = G\beta$$

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

$$\lambda a = \lambda G\alpha = G(\lambda\alpha)$$

$\square$

3.1.1 Изоморфизм ЛП

Определение 3.2. 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 3.4. *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 3.2 (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).

$\square$

Следствие 3.3. *Если пр-ва рассм. над одним и тем же полем, то единственной существенной хар-ой этих пр-в является размерность.*

Теорема 3.5. *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.

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

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

$\square$

Замечание. *Пусть V - ЛП размерности m над конечным полем $F \colon |F| = p^n$. Тогда $|V| = p^{nm}$*

Доказательство.

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

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

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

□

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

4 Лекция 18

F - поле

Определение 4.1. 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 4.2. СЛУ наз-ся **совместной**, если она имеет хотя одно решение. Если она не имеет решений, то она **несовместна**.

Определение 4.3. Совместная СЛУ наз-ся **определённой**, если она имеет **единтсвенное решение**, и **неопределённой** — иначе.

Утверждение 4.1. *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 □

Следствие 4.1. *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. □

Определение 4.4. Системе:

$$AX = B$$

Соотв. **однородная** система:

$$AX = 0$$

Утверждение 4.2. *Мн-во V_0 решений однородной СЛУ явл-ся подпр-ом в F^n ($V_0 \leq F^n$)*

Доказательство.

$$X_1, X_2 \in V_0$$

$$AX_1 + AX_2 = A(X_1 + X_2) = 0 \Rightarrow (X_1 + X_2) \in V_0$$

$$AX_1 = 0 \Rightarrow \lambda AX_1 = 0, \lambda \in F$$

$$X = 0 \in V_0$$

$$\Rightarrow V_0 \leq F^n$$

□

Утверждение 4.3. *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. $\supseteq$)

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

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

$\subseteq$)

$$\forall X \in V_b$$

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

□

4.1 Элементарные преобразования строк матрицы

Определение 4.5. 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 4.4. *ЭП строк $M \iff$ умножению M слева на одну из элементарных матриц.*

E_{ij} - матрица с 1 в $(i;j)$ 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 4.5. *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 4.1. Показать, что если совершать умножение матрицы M на матрицы ЭП нужно размера **справа**, то получатся ЭП столбцов.

Определение 4.6. 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 4.7. 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 4.1. *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 4.8. 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 4.2. *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 4.3. *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 $(A'|B')$.

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

□

4.2 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 $\widetilde{A}_{\text{ступ.}}$: $a_{1k_1}, a_{2k_2}, \ldots a_{rk_r}$

Определение 4.9. Назовём $x_{k_1}, x_{k_2}, \ldots, x_{k_r}$ — **главными** (базисными), а остальные — **свободными** (параметрические).

$$1 \le k_1 < \ldots < k_r \le n$$

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

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

Тогда $x_i = b_i$