АлГем

Сергей Григорян

8 ноября 2024 г.

Содержание

1 Лекция 2

1.1 Упражняемся

$A \in M_{m*n}$ Произвольную i-ую строку будем записывать в виде:

$$A_{i*} = \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix}.$$

Определение 1.1. Линейная комбинация (ЛК) строк $A_{1*}, \cdots, A_{m*}$ наз-ся форм. алг. выр-е:

$$\alpha_1 A_{1*} + \alpha_2 A_{2*} + \cdots + \alpha_m A_{m*} \in M_{1n}.$$

Утверждение 1.1. *a) Пусть $A \in M_{m*n}, B \in M_{n*k}$. Тогда строки матрицы AB явл **ЛК** строк матрицы B с коэф. из соотв. строки матрицы A*

b) Столбцы матрицы AB явл. ЛК столбцов матрицы A с коэф. из соотв. столбцов матрицы B.

Доказательство. **b)** Пусть $C = AB \in M_{m*k}$

$$C_{*j} = \begin{pmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{mj} \end{pmatrix} = \begin{pmatrix} \sum_{s=1}^n a_{1s} b_{sj} \\ \sum_{s=1}^n a_{2s} b_{sj} \\ \vdots \\ \sum_{s=1}^n a_{ms} b_{sj} \end{pmatrix} = \sum_{s=1}^n b_{sj} \begin{pmatrix} a_{1s} \\ a_{2s} \\ \vdots \\ a_{ms} \end{pmatrix} = \sum_{s=1}^n b_{sj} A_{*s}.$$

□

1.2 Векторная алгебра

V_i - линейное пространство i-ого измерения. $(i = 1, 2, 3)$

Определение 1.2. Две точки $X, Y \in V_i$ определяют направленный отрезок, если известно, какая из этих точек первая, какая вторая.

$$\overline{XY} \text{ - направленный отрезок.}$$

$|\overline{XY}| = XY$ - длина напр. отр.

Обозначение.

$$\overline{0} \text{ - нулевой напр. отр..}$$

Определение 1.3. $\overline{XY} = \overline{X'Y'} \iff$

a) $XY = X'Y'$

b) $\overline{XY}$ и $\overline{X'Y'}$ - коллинеарны ($\exists$ прямая, $||$ им обоим)

c) $\overline{XY}$ и $\overline{X'Y'}$ - сонаправлены.

Определение 1.4. Вектор - это класс направленных отрезков, кот. равны некоторому фиксированному напр. отр.

Обозначение. $\overline{a}, \overline{b}, \overline{c}$

Утверждение 1.2. *Два напр. отр. $\overline{XY}$ и $\overline{X'Y'}$ определяют (порождают) один и тот же вектор т. и т. т., когда они равны.*

Доказательство.

a) Необходимое: Пусть $\overline{XY}$ и $\overline{X'Y'}$ опр. один и тот же вектор $\Rightarrow \overline{XY} = \overline{X'Y'} = \overline{a}$

b) Достаточное: Пусть $\overline{XY} = \overline{X'Y'} \Rightarrow$ они содерж. в одном классе $\overline{a} \Rightarrow$ они опред. один и тот же вектор. □

Определение 1.5. $\overline{XY} = \overline{a} \iff$ он порождает вектор a

1.3 Операции с векторами

1.3.1 I. Сложение

Замечание. *При данном векторе $\overline{a}$ и фикс. точке X, то найдётся напр. отр. $\overline{XY} = \overline{a}$*

Определение 1.6. Пусть напр. отр. $\overline{XY}$ опр. $\overline{a}$, $\overline{YZ}$ опр. $\overline{b}$:

Сумма векторов: вектором $\overline{a} + \overline{b}$ назыв. вектор, порожд. $\overline{XZ}$

Замечание. *Данное опр. **корректно**, и не зависит от начальной точки X*

Доказательство. ***Рисунок*** □

1.3.2 Умножение вектора на $\lambda \in \mathbb{R}$

Рассм. напр. отр. $\overline{a} = \overline{XY}$ и $\overline{XZ}$:

a) $XZ = |\lambda| * XY$

b) $\overline{XZ}$ - коллинеарен $\overline{XY}$

c) $\overline{XZ}$ сонаправлен $\overline{XY}$, при $\lambda > 0$
$\overline{XZ}$ прот. направлен. $\overline{XY}$ при $\lambda < 0$:

Вектор, определяемы напр. отр. $\overline{XZ}$, наз-ся вектором $\lambda\overline{a}$

Доказательство. to do by yourself □

Теорема 1.1. *Операции "+"и "*λ"удовл. след. св-вам:*

1. *Коммутативность сложения (Вытекает из св-в параллелограмма):*
$$\overline{a} + \overline{b} = \overline{b} + \overline{a}.$$

2. *Ассоциативность сложения:*
$$(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c}).$$

3. $\exists \overline{o}$: $\overline{o} + \overline{a} = \overline{a} + \overline{o} = \overline{a}, \forall \overline{a} \in V_i$

4. $\forall \overline{a} \in V_i\ \exists (-\overline{a}) \in V_i$: $\overline{a} + (-\overline{a}) = (\overline{-a}) + \overline{a} = \overline{o}$

5. *Унитарность:*
$$1 * \overline{a} = \overline{a}, \forall \overline{a} \in V_i.$$

6. $$(\lambda * \mu) * \overline{a} = \lambda * (\mu * \overline{a}).$$

7. $$(\lambda + \mu) * \overline{a} = \lambda\overline{a} + \mu * \overline{a}.$$

8. $$\lambda(\overline{a} + \overline{b}) = \lambda\overline{a} + \lambda\overline{b}.$$

Замечание. *Мн-во векторов является действительным линейным пространством отн-но мн-ва $\mathbb{R}$.*

1.4 Системы векторов в пр-ве V_i

$V_i, i = 1, 2, 3$

$\overline{v_1}, \overline{v_2}, \cdots, \overline{v_n} \in V_i$

Обозначение.

$$\sum_{i=1}^{n} \alpha_i \overline{v_i} \text{ - наз-ся ЛК векторов.}$$

*Если $\alpha_i = 0, \forall i = 1 \cdots n$, то такая ЛК наз-ся **тривиальной**.*

*Если $\exists i\colon \alpha_i \neq 0$, то ЛК **нетривиальная**.*

Определение 1.7 (ЛЗ система векторов)**.** Система векторов $\overline{v_1}, \overline{v_2}, \cdots, \overline{v_n}$ наз-ся **линейно зависимой (ЛЗ)**, если $\exists$ **нетривиальная ЛК** этих векторов, равная $\overline{o}$

Определение 1.8 (ЛНЗ сис. вект.)**.** Система векторов $\overline{v_1}, \overline{v_2}, \cdots, \overline{v_n}$ наз-ся **линейно независимой (ЛНЗ)**, если $\nexists$ **нетривиальной ЛК** этих векторов, равной $\overline{o}$

Пример.

$$\overline{a} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \overline{b} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \overline{c} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \text{ - ЛНЗ сист. вект..}$$

Док-во ЛНЗ: предствить, что есть коэф-ты, дающие ЛК $= \overline{o}$, и показать, что она тривиальная.

Утверждение 1.3. *Система векторов $\overline{v_1}, \overline{v_2}, \cdots, \overline{v_n}$ - ЛЗ $\iff$ хотя бы один из них представим в виде ЛК остальных.*

Доказательство. а) **Необх:** пусть $\begin{pmatrix} \overline{v_1} & \overline{v_2} & \cdots & \overline{v_n} \end{pmatrix}$ - ЛЗ:

$$\Rightarrow \exists \text{ нетрив. ЛК } : \alpha_1 \overline{v_1} + \alpha_2 \overline{v_2} + \cdots + \alpha_n \overline{v_n} = \overline{o}.$$

Пусть $\alpha_i \neq 0$:

$$\frac{\alpha_1}{\alpha_i} \overline{v_1} + \cdots + \overline{v_i} + \cdots + \frac{\alpha_n}{\alpha_i} \overline{v_n} = \overline{o}.$$

$$\overline{v_i} = -\frac{\alpha_1}{\alpha_i} \overline{v_1} - \cdots - \frac{\alpha_n}{\alpha_i} \overline{v_n}.$$

b) **Дост.:** Пусть $\overline{v_i} = \lambda_1\overline{v_1} + \dots + \lambda_n\overline{v_n}$

$$\Rightarrow \lambda_1\overline{v_1} + \dots + \lambda_n\overline{v_n} - \overline{v_i} = \overline{o}.$$

□

<u>**Замечание**</u>**.** ***НЕВЕРНО*** *было бы сформ. утв. вот так: каждый из вектор выразим в виде ЛК остальных.*

<u>**Пример**</u>**.**

$$\overline{a}, \overline{b} \text{ - неколлин..}$$

$$\Rightarrow \text{Для } \begin{pmatrix}\overline{a} & \overline{a} & \overline{b}\end{pmatrix} \text{ - это неверно, т. к. } b \text{ не выразим через } a.$$

$$\text{Но } 1 * \overline{a} + (-1) * \overline{a} + 0 * \overline{b} = \overline{o} \text{ - нетривиальная ЛК.}$$

<u>**Утверждение**</u> **1.4.** *a) Если система $\overline{v_1}, \overline{v_2}, \cdots, \overline{v_n}$ - ЛЗ $\Rightarrow$ всякая её **надсистема** тоже ЛЗ*

b) Если система $\overline{v_1}, \overline{v_2}, \cdots, \overline{v_n}$ - ЛНЗ $\Rightarrow$, то всякая её подсистема ЛНЗ.

Доказательство. a) $\exists \alpha_1, \cdots, \alpha_n,$- не все равны $\overline{o}$, тогда $\sum_{i=1}^{n} \alpha_i \overline{v_i} = \overline{o}$
$\Rightarrow \sum_{i=1}^{n} \alpha_i \overline{v_i} + \sum_{i=n+1}^{n+k} 0 * \overline{v_j} = \overline{o}$

b) Пусть подсистема $\begin{pmatrix}\overline{v_1} & \overline{v_2} & \cdots & \overline{v_k}\end{pmatrix}$ - ЛЗ (от прот.), тогда по a), $\begin{pmatrix}\overline{v_1} & \cdots & \overline{v_n}\end{pmatrix}$ - ЛНЗ $\Rightarrow$ **Противоречие**

□

<u>**Утверждение**</u> **1.5.** *Пусть $\begin{pmatrix}\overline{v_1} & \overline{v_2} & \cdots & \overline{v_n}\end{pmatrix}$ - ЛНЗ сист. векторов в V_i. Тогда каждый вектор $\overline{w} \in V_i$ выражется через $\begin{pmatrix}\overline{v_1} & \overline{v_2} & \cdots & \overline{v_n}\end{pmatrix}$ не более чем одним способом.*

Доказательство.

$$\overline{w} = \begin{pmatrix}\overline{v_1} & \overline{v_2} & \cdots & \overline{v_n}\end{pmatrix} \begin{pmatrix}\alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n\end{pmatrix} = \overline{V}\alpha = \overline{V}\beta$$

$$\Rightarrow \overline{o} = \overline{V}(\alpha - \beta).$$

□

2 Лекция 14

2.1 Алгебраические структуры

Определение 2.1. 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 2.1. *Во всякой группе G нейтральный эл-т единственный.*

Доказательство.

$$e = e * e' = e'$$

$\square$

Определение 2.2. 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 2.2. *$\forall a \in G$ 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 2.3. 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 2.4. Если в R $\exists 1 \in R$, т. ч.:

$$1 * a = a * 1 = a, \forall \in R$$

то 1 наз-ся единицей кольца.

2.2 Сравнения и вычеты

<u>Определение</u> 2.5. 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.

<u>Обозначение</u>.

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

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

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

<u>Замечание</u>. *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.

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

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

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

□

<u>Обозначение</u>.

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

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

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

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

<u>Замечание</u>.

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

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

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

Доказательство. Опер-ция опр-на и кореектна:

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

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

□

Определение 2.6. Пусть R - кольцо с 1.
Эл-т $a \in R$ - обратимый $\iff \exists b \in R\colon a * b = b * a = 1$

Определение 2.7. R^* - мн-во всех обратимых эл-ов кольца R с 1.

Утверждение 2.4. *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 $a, b \in R^* \Rightarrow a * b \in R^*$:

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

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

□

Задача 2.1. Z_n^* - мн-во всех классов вычетов, взаимно простых с n.

Утверждение 2.5. *В любом кольце R:*

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

Доказательство.

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

$$0 * a = 0$$

□

Следствие 2.1. *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!!! □

Следствие 2.2. *Если R ненулевое кольцо с 1, то $0 \notin R^*$*

Определение 2.8. 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 2.9. 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 2.6. *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 2.1. *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:

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

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 $n \not| a, \Rightarrow n|(l-k) \Rightarrow l = k!!! \Rightarrow \exists b \colon \overline{b}\overline{a} = \overline{a}\overline{b} = \overline{1}$ и $\overline{b} \neq \overline{0}$

□

3 Лекция 15

3.1 Характеристика поля

F - поле.

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

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

Положим:

$$0_F = 0$$

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

Лемма 3.1.

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

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

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 3.1. **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 3.1. *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 3.2. 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 3.2. *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 3.1. *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 3.3 (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 **3.4.** *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 $\Rightarrow \forall a, b \in F_i^* \Rightarrow a{*}b \in F_i, a^{-1} \in F_i \Rightarrow (\bigcap_i F_i^*)$ - аб. группа.

□

3.2 Гомоморфизим и изоморфизм групп.

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

Определение **3.3.** 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 **3.4.** 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 **3.5.** 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 **3.6.** Отобр. $\phi\colon X \to Y$ наз-ся биективным, если оно С + И.

Определение **3.7.** **Изоморфизм** - биективный гомоморфизм.

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

Утверждение 3.5. *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 3.2. *При гомоморфизме полей 0 и 1 первого поля переходят в 0 и 1 второго.*

3.3 Простое подполе

Определение 3.8. 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 3.2. *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 3.3 (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. $\mathbb{Z}_p \Rightarrow D_F \cong \mathbb{Z}_p$

□

4 Лекция 16

4.1 Линейные пр-ва

Пусть F - поле.

Определение 4.1. 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.*

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

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

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

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

4.1.1 Подпр-во ЛП

Пусть V - ЛП на поле F.

Определение 4.2. 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 4.1. *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 4.2 (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 4.1. *Пересечение любого числа подпр-в ЛП* V *само явл-ся подпр-вом.*

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

4.1.2 Подполе лин. объектов системы векторов

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

Определение 4.3. 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 4.3. $< S >= \{ \sum_{i=1}^{n} \alpha_i s_i \mid s_i \in S, \alpha_i \in F, n \in \mathbb{Z}_+ \}$

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

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

$\square$

Определение 4.4. Если $< S >= V$, то говорят, что V порождено S.

Определение 4.5. ЛП V наз-ся **конечно-порождённым**, если оно имеет конечное порождающее мн-во

4.1.3 Базис

Определение 4.6. 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 4.4. *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 4.5 (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:
$$\lambda_2 w_1 - \lambda_1 w_2 + 0w_3 + 0w_4 + \ldots + 0w_m = 0 \Rightarrow W \text{ - ЛЗ}$$

- 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:
$$\overline{V} = \begin{pmatrix} u_2 & \ldots & u_n \end{pmatrix}, \overline{W} = \begin{pmatrix} w_2 - w_1 \cdot \frac{\lambda_{1i}}{\lambda_{11}} & \ldots \end{pmatrix}$$
По предположению индукции: $\overline{W}$ - ЛЗ $\Rightarrow W$ - ЛЗ.

□

5 Лекция 17

5.1 Конечномерные ЛП

Определение 5.1. 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.
$$dim_F V = n \text{ } или \text{ } dim_F V = \infty$$

Теорема 5.1. *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 $\Rightarrow dim_F V = n$

□

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 5.2. *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 5.1. *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 5.3. *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 5.1. *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.

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

□

5.1.1 Изоморфизм ЛП

Определение 5.2. 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 5.4. *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 5.2 (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).

□

<u>Следствие</u> 5.3. *Если пр-ва рассм. над одним и тем же полем, то единственной существенной хар-ой этих пр-в является размерность.*

<u>Теорема</u> 5.5. *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.

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

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

□

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

Доказательство.

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

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

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

□

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

6 Лекция 18

F - поле

Определение 6.1. 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 6.2. СЛУ наз-ся **совместной**, если она имеет хотя одно решение. Если она не имеет решений, то она **несовместна**.

Определение 6.3. Совместная СЛУ наз-ся **определённой**, если она имеет **единтсвенное решение**, и **неопределённой** — иначе.

Утверждение 6.1. *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 6.1. *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 6.4. Системе:

$$AX = B$$

Соотв. **однородная** система:

$$AX = 0$$

Утверждение 6.2. *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 6.3. *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. $\supseteq$)

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

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

$\subseteq$)

$$\forall X \in V_b$$

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

$\square$

6.1 Элементарные преобразования строк матрицы

Определение 6.5. 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 6.4. *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 6.5. *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 6.1. Показать, что если совершать умножение матрицы M на матрицы ЭП нужно размера **справа**, то получатся ЭП столбцов.

Определение 6.6. 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 6.7. 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 6.1. *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.

$\square$

Определение 6.8. 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 6.2. *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 $a_{1k_1}, a_{2k_2}, \dots, a_{rk_r}$ — 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. $\square$

Теорема 6.3. *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 $(A'|B')$.

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

$\square$

6.2 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 6.9. Назовём $x_{k_1}, x_{k_2}, \ldots, x_{k_r}$ — **главными** (базисными), а остальные — **свободными** (параметрические).

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

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 $x_i = b_i$

7 Лекция 19 (СКИП)

8 Лекция 20

8.1 Применения рангов матрицы

Определение 8.1. Минор M_{ij} наз-ся **невырожденным** если $\operatorname{rk} M_{ij} =$ k

Определение 8.2. Рангом матрицы по минору наз-ся максимальный порядок среди порядков всех невырожденных миноров.

$$\operatorname{rk}_M A$$

Теорема 8.1 (Фробениуса)**.** *Для $\forall$ матрицы A:*

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

Утверждение 8.1. *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 8.3. 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 8.2. *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 8.1.

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

Теорема 8.3 (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 свою. членов. □

Теорема 8.4 (Критерий определённости совм. СЛУ)**.** *Совместная СЛУ определенна, если её ранг равен числу неизвестных.*

Теорема 8.5. *Пусть $C = AB$, тогда* $\operatorname{rk} C \le min(\operatorname{rk} A, \operatorname{rk} B)$

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

□

8.1.1 Применнеие рангов к исследованию квадр. матрицы на обратимость

Определение 8.4. $A \in M_n(\mathbb{F})$ наз-ся обратимой $\iff \exists A^{-1} \in M_n(\mathbb{F})$:

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

Определение 8.5. 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 8.6 (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 $E = n \leq min(\operatorname{rk} A, \operatorname{rk} B) \leq \operatorname{rk} A \leq n$. 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:

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

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

$5 \Rightarrow 1)$

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

$\square$

Следствие 8.2. *Вырожденные матрицы необратимы*

Следствие 8.3. *Произведение двух невырож. матриц невырожд.*

Следствие 8.4. *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. $\square$

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

8.2 Операции над подпространствами

V - конечномерн. пр-во

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

Определение 8.6. 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 8.2.

$$U \cap W \leq V$$

Доказать сам-но.

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

Определение 8.7. Алг. сумма подпр-в U, W:

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

Утверждение 8.3.

$$U + W \leq V$$

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

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

Утверждение 8.4. *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 8.9. Объединение упор. систем векторов подразумевается конкатенация этих систем (приписывание).

Утверждение 8.5. *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 8.5.

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

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

Определение 8.10. Пусть $U_i \leq V$. $\sum_{i=1}^n U_i$ наз-ся **прямой суммой подпр-в**, если $\forall x \in \sum_{i=1}^n U_i$:

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

Обозначение.

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

Определение 8.11 (ЛНЗ для подпр-в)**.** Подпр-ва $U_1, \dots U_n$ 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 8.7 (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)
$$\forall i = \{1, \dots, n\} : U_i \cap (\sum_{j=1, j\neq i}^n U_j) = \{\overline{0}\}$$

3)
$$U_1, \dots, U_n \text{ — ЛНЗ}$$

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

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