АлГем

Сергей Григорян

23 октября 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.

$\overline{XY}$ - направленный отрезок.

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

Обозначение.

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

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. $\square$

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*** $\square$

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

$V_i, i = 1, 2, 3$

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

<u>Обозначение</u>.

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

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****.*

<u>Определение</u> 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 $\overline{o}$

<u>Определение</u> 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 $\overline{o}$

<u>Пример</u>.

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

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

<u>Утверждение</u> 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. a) **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 $\overline{v_i} = \lambda_1\overline{v_1} + \cdots + \lambda_n\overline{v_n}$

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

□

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

Пример.

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

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

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

Утверждение 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**

□

Утверждение 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 12

2.1 Классификация КВП

Эллиптический тип: $a \geq b > 0$	Инварианты
1) Эллипс: $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$	$\delta > 0, I \cdot \triangle < 0$
2) Мнимый эллипс: $\frac{x^2}{a^2} + \frac{y^2}{b^2} = -1$	$\delta > 0, I \cdot \triangle > 0$
3) Пара пересек. мнимых прямых: $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 0$	$\delta > 0, \triangle = 0$

Гиперболический тип: $a > 0, b > 0$	Инварианты
4) Гипербола: $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$	$\delta < 0, \triangle \neq 0$
5) Пара пересек. действ. прямых: $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 0$	$\delta < 0, \triangle = 0$

Параболический тип: $p, a > 0$	Инварианты
6) Парабола: $y^2 = 2px$	$\delta = 0, \triangle \neq 0$
7) Пара $\|\|$ действ. прямых: $y^2 = a^2$ 8) Пара $\|\|$ мнимых прямых: $y^2 = -a^2$ 9) Пара совпад. действ. прямых: $y^2 = 0$	$\delta = 0$ $\triangle = 0$

Для различения 7-9):

$$K = \begin{vmatrix} A & D \\ D & F \end{vmatrix} + \begin{vmatrix} C & E \\ E & F \end{vmatrix}$$

2.2 Центр КВП

$$\Gamma\colon P(x,y) = Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0 \qquad (1)$$

Определение 2.1. Точка $O(x_0, y_0)$ наз-ся центром кривой Γ (а также центром её мн-на), если $\forall \overline{s} = (\alpha, \beta)$ вып-ся рав-во:

$$P(x_0+\alpha, y_0+\beta) = P(x_0-\alpha, y_0-\beta) \qquad (2)$$

Утверждение 2.1. *Пусть $O(x_0, y_0)$ - центр кривой Γ (и мн-на P). Тогда т. A принадлежит $\Gamma \iff A' \in \Gamma$ - точка, симметричная т. A отн-но центра O*

Доказательство. Пусть $A \longleftrightarrow \begin{pmatrix} x_0+\alpha \\ y_0+\beta \end{pmatrix}, A' \longleftrightarrow \begin{pmatrix} x_0-\alpha \\ y_0-\beta \end{pmatrix}$:

$$A \in \Gamma \iff P(x_0+\alpha, y_0+\beta) = 0 \iff P(x_0-\alpha, y_0-\beta) = 0 \iff A' \in \Gamma$$

□

Замечание. *Центр Γ не обязан лежать в Γ*

Утверждение 2.2. *Точка $O(x_0, y_0)$ явл-ся центром Γ (и $P(x,y)$) $\iff$:*

$$\begin{cases} Ax_0 + By_0 + D = 0 \\ Bx_0 + Cy_0 + E = 0 \end{cases} \qquad (3)$$

Доказательство.

$$P(x_0+\alpha, y_0+\beta) = A(x_0+\alpha)^2+2B(x_0+\alpha)(y_0+\beta)+C(y_0+\beta)^2+2D(x_0+\alpha)+2E(y_0+\beta)+F$$

$$P(x_0-\alpha, y_0-\beta) = A(x_0-\alpha)^2+2B(x_0-\alpha)(y_0-\beta)+C(y_0-\beta)^2+2D(x_0-\alpha)+2E(y_0-\beta)+F$$

$$P(x_0+\alpha, y_0+\beta)-P(x_0-\alpha, y_0-\beta) = 4\alpha(Ax_0+By_0+D)+4\beta(Bx_0+Cy_0+E) = 0, \forall \alpha, \beta \in \mathbb{R}$$

$$\iff \begin{cases} Ax_0 + By_0 + D = 0 \\ Bx_0 + Cy_0 + E = 0 \end{cases}$$

□

2.3 Центральные кривые

Определение 2.2. КВП наз-ся **центральной**, если она имеет единственный центр. (Этот центр **не обязан** лежать на КВП)

Утверждение 2.3. *a) Кривая* Γ *явл. центральной* $\iff$

$$\delta = \begin{vmatrix} A & B \\ B & C \end{vmatrix} \neq 0$$

b) Св-во кривой Γ *быть центральной не зависит от выбора ПДСК.*

c) Пусть Γ *- центральная кривая, содерж. хотя бы одну точку. Тогда* Γ *содержитединственный центр симметрии* O_0*, причём* $O_0 = O \longleftrightarrow \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$

Доказательство. a) По т. Крамера, $O(x_0, y_0)$ - единственный центр $\iff$

$$\delta = \begin{vmatrix} A & B \\ B & C \end{vmatrix} \neq 0$$

b) Т. к. δ - инвариант, то и св-во быть центральной также не меняется при замене ПДСК.

c) Пусть $O(x_0, y_0)$ - центр и он единств. $\iff$ $\delta \neq 0$, тогда можно сказать, что Γ имеет эллиптический или гиперболический тип. Тогда:

$$\frac{x^2}{a^2} \pm \frac{y^2}{b^2} - C = 0 \text{ - ур-е КВП}$$

$$\Rightarrow B = D = E = 0 \Rightarrow \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \text{ - решение системы (3)}$$

Тогда Γ содержит единственный центр симметрии O_0, причём $O_0 \equiv O(x_0, y_0)$

$\square$

2.4 Св-ва КВП

2.4.1 Эллипс

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

$$a \text{ - большая полуось}$$

$$b \text{ - малая полуось}$$

$$c = \sqrt{a^2 - b^2} < a \text{ - фокусное расстояние}$$

$$F_1(c, 0), F_2(-c, 0) \text{ - фокусы}$$

$$\varepsilon = \frac{c}{a} \text{ - эксцентриситет}$$

$$0 \leq \varepsilon < 1$$

При $a = b$, $\varepsilon = 0$
Директрисы:

$$d_1 \colon x = \frac{a}{\varepsilon}$$

$$d_2 \colon x = -\frac{a}{\varepsilon}$$

Утверждение 2.4. *$A \longleftrightarrow \begin{pmatrix} x \\ y \end{pmatrix} \in$ эллипсу $\iff$*

$$\iff AF_1 = |a - \varepsilon x| \iff AF_2 = |a + \varepsilon x|$$

Т. к. $|x| \leq a$ (если $\begin{pmatrix} x \\ y \end{pmatrix} \in$ эллипсу), то модули раскрываются с положительным знаком.

Доказательство.

$$0 = AF_1^2 - (a - \varepsilon x)^2 = (x-c)^2 + y^2 + a^2 + 2a\varepsilon x - \varepsilon^2 x^2 = (1-\varepsilon^2)x^2 + 2x(-c + a\varepsilon) + c^2 + y^2 - a^2 \Rightarrow$$

$$\Rightarrow 1 - \varepsilon^2 - 1 - \frac{c^2}{a^2} = \frac{a^2 - c^2}{a^2} = \frac{b^2}{a^2} \Rightarrow$$

$$= \frac{b^2}{a^2}x^2 + y^2 - b^2 = b^2(\frac{x^2}{a^2} + \frac{y^2}{b^2} - 1) = 0$$

$\square$

Теорема 2.1.

$$\frac{AF_1}{p(d_1, A)} = \varepsilon = \frac{AF_2}{p(d_2, A)}$$

Доказательство.

$$\varepsilon p(A, d_1) = \varepsilon \left| x - \frac{a}{\varepsilon} \right| = |\varepsilon x - a| = AF_1$$

□

Теорема 2.2 (Характеристической св-во эллипса)**.** *Точка* $A \begin{pmatrix} x \\ y \end{pmatrix} \in$ *эллипсу* $\iff$

$$AF_1 + AF_2 = 2a$$

Доказательство. a) Необходимость:

$$AF_1 + AF_2 = a - \varepsilon x + a + \varepsilon x = 2a$$

b) Достаточность: Пусть: $AF_1 + AF_2 = 2a$, тогда $|x| \leq a$. От прот., пусть $|x| > a \Rightarrow$

$AF_1 + AF_2 \geq |x - c| + |x + c| \geq |x - c + x + c| = |2x| > 2a$ - противоречие.

Если $|x| = a \Rightarrow$

$$\left[\begin{aligned} &x = a \\ &x = -a \end{aligned}\right. \Rightarrow A\colon a - c + a + c = 2a \text{ для } -a \text{ аналогично.}$$

(Остальное док-во...)

□

2.4.2 Гипербола

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

$c = \sqrt{a^2 + b^2}$ - фокусное расст.
$F_1(c, 0), F_2(-c, 0)$ - фокусы

$\varepsilon = \frac{c}{a} > 1$
$d_1\colon x = \frac{a}{\varepsilon}$
$d_2\colon x = -\frac{a}{\varepsilon}$

Утверждение 2.5. *Точка* $A(x$
$y) \in$ *гиперболе* $\iff$

$$AF_1 = |a - \varepsilon x|\,, AF_2 = |\varepsilon x + a|$$

$$|x| \geq a$$

$$\varepsilon\,|x| > a$$

Доказательство.

$$0 = AF_1^2 - (\varepsilon x - a)^2 = (x-c)^2 + y^2 - \varepsilon^x x^2 + 2\varepsilon a x - a^2 - a^2 = (1-\varepsilon^2)x^2 + 2x(-c+\varepsilon a) + c^2 + y^2 - a^2 =$$

$$= -\frac{b^2}{a^2}x^2 + y^2 + b^2 = 0$$

□

Следствие 2.1.

$$\frac{AF_1}{p(A, d_1)} = \varepsilon$$

Доказательство.

$$\varepsilon \cdot p(A, d_1) = \varepsilon \left| x - \frac{a}{\varepsilon} \right| = |\varepsilon x - a| = AF_1$$

□

Теорема 2.3 (Характеристическое св-во гиперб.)**.**

$$A \begin{pmatrix} x \\ y \end{pmatrix} \in \text{ гиперболы } \iff |AF_2 - AF_1| = 2a$$

Доказательство. a) Пусть $A \in$ правой ветви гиперболы:

$$|AF_2 - AF_1| = AF_2 - AF_1 = \varepsilon x + a - (\varepsilon x - a) = 2a$$

b) Пусть изв., что $AF_2 - AF_1 = 2a$, и покажем, что $A \in$ правой части.

$$\sqrt{(x+c)^2 + y^2} = \sqrt{(x-c)^2 + y^2} + 2a$$

$$(x+c)^2 + y^2 = 4a^2 + 4a\sqrt{(x-c)^2 + y^2} + (x-c)^2 + y^2$$

$$
\begin{gathered}
4xc - 4a^2 = 4a\sqrt{(x-c)^2 + y^2} \\
x^2c^2 - 2a^2cx + a^4 = a^2(x^2 - 2cx + c^2 + y^2) \\
x^2(c^2 - a^2) + a^4 - a^2c^2 - a^2y^2 = 0 \\
x^2b^2 + a^4 - a^2c^2 - a^2y^2 = 0 \\
x^2b^2 + a^4 - a^2(a^2 + b^2) - a^2y^2 = 0 \\
x^2b^2 - a^2b^2 - a^2y^2 = 0 \\
\frac{x^2}{a^2} - \frac{y^2}{b^2} - 1 = 0 \\
0 = 0
\end{gathered}
$$

□

3 Лекция 13

3.1 Св-ва гиперболы

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

Определение 3.1. Асимптотами гиперболы наз-ся гиперболы:

$$\frac{x}{a} \pm \frac{y}{b} = 0$$

Утверждение 3.1. *Пусть $A \longleftrightarrow \begin{pmatrix} x \\ y \end{pmatrix}$ - т. гиперболы, с указанным ур-ем. Тогда произведение расстояний от A до асимптот = const*

Доказательство.

$$p(A, l_1)p(A, l_2) = \frac{\left|\frac{x}{a} - \frac{y}{b}\right|}{\sqrt{\frac{1}{a^2} + \frac{1}{b^2}}} \frac{\left|\frac{x}{a} + \frac{y}{b}\right|}{\sqrt{\frac{1}{a^2} + \frac{1}{b^2}}} = \frac{\left|\frac{x^2}{a^2} - \frac{y^2}{b^2}\right|}{\frac{1}{a^2} + \frac{1}{b^2}} = \frac{1}{\frac{1}{a^2} + \frac{1}{b^2}} = \frac{a^2b^2}{a^2 + b^2}$$

□

Следствие 3.1. *Пусть т. A движется по одной из ветвей гиперболы, т. ч.:*

$$p(A, O(0,0)) \to +\infty$$

Тогда верно ***одно*** *из двух:*

$$\left[\begin{aligned} &p(A, l_1) \to 0 \\ &p(A, l_2) \to 0 \end{aligned}\right.$$

Доказательство. Для правой верхней полуветви.

$$x = a \operatorname{ch} t y = b \operatorname{sh} t$$

$$\Rightarrow \frac{a^2 \operatorname{ch}^2 t}{a^2} - \frac{b^2 \operatorname{sh}^2 t}{b^2} = 1$$

$$\Rightarrow \operatorname{ch}^2 t - \operatorname{sh}^2 t = 1 \text{ основное гиперболическое тождество}$$

$$\Rightarrow A(t) \in \text{ гиперболе}$$

$$p(A, l_2) = \frac{\left|\frac{x(t)}{a} + \frac{y(t)}{b}\right|}{\sqrt{\frac{1}{a^2} + \frac{1}{b^2}}} \to +\infty$$

$$p(A, l_1) = \frac{const}{p(A, l_2)} \Rightarrow p(A, l_1) \to 0$$

□

3.2 Св-ва параболы

Канон. ур-е:

$$y^2 = 2px, p > 0$$

$$F\left(\frac{p}{2}, 0\right)$$

$$d\colon x = -\frac{p}{2}$$

Утверждение 3.2. *Т.* $A \longleftrightarrow \begin{pmatrix} x \\ y \end{pmatrix}$ *принадлежит параболе* $y^2 = 2px \iff$

$$AF = \left|x + \frac{p}{2}\right|$$

Доказательство.

$$AF^2 - \left(x + \frac{p}{2}\right)^2 = \left(x - \frac{p}{2}\right)^2 + y^2 - \left(x + \frac{p}{2}\right)^2 = -2xp + y^2 = -2xp + 2xp = 0$$

$\square$

Следствие 3.2. *Парабола - это ГМТ A, т. ч.:*

$$\frac{p(A, F)}{p(A, d)} = 1$$

Доказательство.

$$p(A, d) = \left|x + \frac{p}{2}\right| = AF \Rightarrow \frac{AF}{AF} = 1$$

$\square$

Определение 3.2. Будем считать, что $\varepsilon_{\text{пар.}} = 1$

Теорема 3.1 (Об эксцентриситете)**.** *Для любой невырожденной КВП ($\triangle \neq 0$):*

$$\frac{p(A, F)}{p(A, d)} = \varepsilon$$

Утверждение 3.3. *Две КВП подобны тогда и только тогда, когда они имеют равный эксцентриситет.*

3.3 Диаметры невырожд. кривых

3.3.1 Гипербола

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

Пусть $A \longleftrightarrow \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ - середина хорды гиперболы, имеющей напр. вектор $\overline{v} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$:

$$\begin{cases} x = x_0 + \alpha t \\ y = y_0 + \beta t \end{cases}$$

$$\left(\frac{\alpha^2}{a^2}-\frac{\beta^2}{b^2}\right)t^2+2\left(\frac{x_0\alpha}{a}-\frac{y_0\beta}{b^2}\right)t+\frac{x_0^2}{a^2}-\frac{y_0^2}{b^2}-1=0$$

Т. к. A - середина хорды, то член при t равен 0 - необх. и дост. условие:

$$\Rightarrow \frac{\alpha}{a^2}x-\frac{\beta}{b^2}y=0 \text{ - диаметр гиперболы, сопряж. с } \overline{v}$$

3.3.2 Эллипс

Аналогично гиперболе, получаем:

$$\frac{\alpha}{a^2}x+\frac{\beta}{b^2}y=0 \text{ - диаметр эллипса, сопряж с } \overline{v} \longleftrightarrow \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

3.3.3 Параболы

$$y^2=2px$$

$$A \longleftrightarrow \begin{pmatrix}x_0\\ y_0\end{pmatrix} \text{ - середина хорды, с напр. вектором } \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

$$(y_0+\beta t)^2=2p(x_0+\alpha t)$$

$$y_0^2+2y_0\beta t+\beta^2t^2-2px_0-2p\alpha t=0$$

$$\beta^2t^2+t(2y_0\beta-2p\alpha)+y_0^2-2px_0=0$$

$$\Rightarrow y=p\frac{\alpha}{\beta} \text{ - ур-е диаметра, сопряж с вектором } \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

Вывод: любой диаметр параболы || её оси.

Теорема 3.2. *Мн-во всех середин хорд данного напр-я $\overline{v}$ невырожд. КВП всегда лежит на одной прямой, кот. наз-ся диаметром, сопряж. напр. $\overline{v}$*

Замечание. *У эллипса и гиперболы диаметр проходит через центр кривой, а у параболы диаметр параллелен её оси.*

3.4 Сопряжённые диаметры

Теорема 3.3. *Пусть* Γ *- эллипс или гипербола,* $\overline{v} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ *- задаёт напр. на пл-ти. Пусть* d *- диаметр, сопряж.* $\overline{v}$*. Пусть также* $\overline{w}$ *- напр. вектор диаметра* d*. Пусть теперь* d' *- диаметр, сопряжённый* $\overline{w}$*. Тогда* $d' || \overline{v}$

Для гиперболы. Пусть AB - хорда с напр. $\overline{v}$.

$$C = Sym_O(A)$$

$$D = Sym_O(B)$$

$$ABCD \text{ - пар-м}$$

d проходит через середины AB и $CD \Rightarrow d'$ проходит через сер-ны AD и BC. Тогда, по постр., $d' || AB || CD || \overline{v}$.

□

Определение 3.3. Построенные пары диаметров (d и d') наз-ся взаимно сопряжёнными. (Т. е. каждый из них делит пополам хорды, параллельные другому диаметру)

3.5 Касательные к КВП

$$F(x, y) = Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0 \tag{4}$$

Определение 3.4. Особая точка КВП, это центр, принадлежащий кривой.

a) Точка пересечения пары пересекающихся действ. прямых - особая.

b) Точка пересечения пары пересек. мнимых прямых - особая.

c) Каждая точка пары совпавших действ. прямых - особая.

Считается, что в особой точке, касат. к кривой не определена.

Исключая из рассм. особые точки и неособые точки, лежащие на прямой, входящей в состав Γ, мы получаем случаи эллипса, гиперболы и параболы.

<u>Определение</u> 3.5. Касательная к Γ в т. $M \longleftrightarrow \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ наз-ся предельное положение секущей, когда длина хорды секущей стремится к 0.

$$F_1(x, y) = Ax + By + C = 0$$
$$F_2(x, y) = Bx + Cy + D = 0$$

Секущ. через т. M:

$$l\colon \begin{cases} x = x_0 + \alpha t \\ y = y_0 + \beta t \end{cases}$$

$$F(x(t), y(t)) = A(x_0+\alpha t)^2+2B(x_0+\alpha t)(y_0+\beta t)+C(y_0+\beta t)^2+2D(x_0+\beta t)+2E(y_0+\beta t)+F = 0$$
$$Pt^2 + 2Qt + R = 0$$
$$P = A\alpha^2 + 2B\alpha\beta + C\beta^2 = \begin{pmatrix} \alpha & \beta \end{pmatrix} \begin{pmatrix} A & B \\ B & C \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$
$$Q = (Ax_0 + By_0 + D)\alpha + (Bx_0 + Cy_0 + E)\beta$$
$$R = F(x_0, y_0) = 0, \text{ т. к. } M \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \in \Gamma$$
$$t(Pt + 2Q) = 0 \tag{5}$$

Если $P = 0 \iff \begin{pmatrix} \alpha & \beta \end{pmatrix} \begin{pmatrix} A & B \\ B & C \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 0$, прямая l, проходя через т. $M \in \Gamma$, далее нигде с Γ не пересекается.

<u>Определение</u> 3.6. Напр. $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ наз-ся асимптотическим направлением:

$$\left[\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \text{ или } \begin{pmatrix} a \\ -b \end{pmatrix}\right]$$

<u>Утверждение</u> 3.4. *Если:*

- $\delta < 0$, *то* Γ *имеет 2 асимп. напр-я.*
- $\delta = 0$, *то* Γ *имеет 1 асимп. напр-я.*
- $\delta > 0$, *то нет асимп. напр-я.*

Пусть $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ - не асимп. напр-е:
Ур-ие (5) имеет 2 корня:

$$\left[\begin{array}{l} t_0 = 0 \\ t_1 \end{array}\right.$$

Привидение полож. секущ. т. и т. т., ...

4 Лекция 14

4.1 Алгебраические структуры

Определение 4.1. Группой наз-ся мн-во G с опред. на нём бинарной алг. операцией. (Обозначим как $*$: $G \times G \to G$ - 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* $X = \{1, 2, \dots n\}$

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

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

Утверждение 4.1. *Во всякой группе G нейтральный эл-т единственный.*

Доказательство.

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

□

Определение 4.2. 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 4.2. *$\forall a \in G$ 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. □

Определение 4.3. 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 4.4. Если в R $\exists 1 \in R$, т. ч.:

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

то 1 наз-ся единицей кольца.

4.2 Сравнения и вычеты

Определение 4.5. 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.

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

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

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 4.3. *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 4.6. Пусть R - кольцо с 1.
Эл-т $a \in R$ - обратимый $\iff \exists b \in R$: $a * b = b * a = 1$

Определение 4.7. R^* - мн-во всех обратимых эл-ов кольца R с 1.

Утверждение 4.4. *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 4.1. Z_n^* - мн-во всех классов вычетов, взаимно простых с n.

Утверждение 4.5. *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 4.1. *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 4.2. *Если R ненулевое кольцо с 1, то $0 \notin R^*$*

Определение 4.8. 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 4.9. 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 4.6. *В поле нет делителей нуля.*

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

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

$\square$

Теорема 4.1. *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 $n \nmid a, \Rightarrow n | (l-k) \Rightarrow l = k!!! \Rightarrow \exists b \colon \overline{b}\overline{a} = \overline{a}\overline{b} = \overline{1}$ и $\overline{b} \neq \overline{0}$

$\square$

5 Лекция 15

5.1 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 5.1.

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

Доказательство. $n > 0, m > 0$:

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

□

Определение 5.1. **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 5.1. *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 5.2. 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 5.2. *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 5.1. *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 5.3 (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 **5.4.** *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 $\Rightarrow \forall a, b \in F_i^* \Rightarrow a*b \in F_i, a^{-1} \in F_i \Rightarrow (\bigcap_i F_i^*)$ - аб. группа.

□

5.2 Гомоморфизм и изоморфизм групп.

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

Определение **5.3.** 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 **5.4.** 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 **5.5.** 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 **5.6.** Отобр. $\phi\colon X \to Y$ наз-ся биективным, если оно С + И.

Определение **5.7.** **Изоморфизм** - биективный гомоморфизм.

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

Утверждение 5.5. *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 5.2. *При гомоморфизме полей 0 и 1 первого поля переходят в 0 и 1 второго.*

5.3 Простое подполе

Определение 5.8. 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 5.2. *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 $M \leq D \leq F \Rightarrow M \leq F \land D \not\subset M$!!, 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 5.3 (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 $n_F = 0 \Rightarrow n = 0$

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

Это гомоморфизм, т. к.:

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

Пусть $n_F = m_F \Rightarrow (n \cdot m)_F = 0 \Rightarrow n - m = 0 \Rightarrow n = m$

□