Алгебра 1 семестр ПИ,
Лекции

Собрано 5 января 2022 г. в 12:42

Содержание

Раздел #1: Отношения и перестановки

1.1. Отношения

Def 1.1.1. *Отношением ω на $X \times Y$ называется любое подмножество $X \times Y$.*

Если $X = Y$, то говорят про отношение на X.
Отношение на X называется:

1. рефлексивным, если $\forall x \in X (x, x) \in \omega$
2. антирефлексивным, если $(x, y) \in \omega \Rightarrow x \neq y$
3. симметричным, если $(x, y) \in \omega \Rightarrow (y, x) \in \omega$
4. антисимметричным, если $(x, y), (y, x) \in \omega \Rightarrow y = x$
5. транзитивным, если $(x, y), (y, z) \in \omega \Rightarrow (x, z) \in \omega$

1.2. Отношение эквивалентности

Def 1.2.1. *Отношение на X, которое является рефлексивным, симметричным, транзитивным, называется эквивалентностью и обозначается $x \sim y$*

Пример 1.2.2. $X = \mathbb{Z}\ x \omega y \Leftrightarrow x - y \vdots 5$

1. $x - x \vdots 5$ — рефлексивно
2. $x - y \vdots 5 \Rightarrow y - x \vdots 5$ — симметрично
3. $x - y \vdots 5$, $y - z \vdots 5$ $x - z = (x - y) + (y - z) \vdots 5 \Rightarrow x - z \vdots 5$ — транзитивно

$\Rightarrow \omega$ — отношение эвивалентности

1.3. Класс эквивалентности

Def 1.3.1. *Классом эквивалентности, содержащим $a \in X$, называется $[a] = \{x : x \in X, x \sim a\}$*

Def 1.3.2. *Разбиением множества X называется $\pi(X) = \{X_i\}$:*

1. $X_1 \cup X_2 \cdots = X$
2. $\forall i, j : i \neq j, X_i \cap X_j = \varnothing$

Теорема 1.3.3. Связь эквивалентности и разбиения множества

1. Отношения эквивалентности на X задаёт разбиение множества $\pi(X)$, X_i — классы эквивалентности
2. Разбиение $\pi(X)$ задаёт эквивалентность на X

Доказательство. 1. $X_i = [x] = \{y \in X : y \sim x\}$ — перебираем все $x \in X \Rightarrow X = X_1 \cup X_2 \cup \cdots X_n \cup \cdots$

$X_i, X_j : X_i = [x_i], X_j = [x_j]$ предположим, что $a \in X_i \cap X_j \Rightarrow a \sim x_i, a \sim x_j \Rightarrow x_i \sim x_j \Rightarrow X_i = X_j \Rightarrow [x_i]$ задают разбиения

2. $\sim$: $x \sim y \Leftrightarrow x, y \in X_i$, проверить, что $\sim$ — эквивалентность:

   1. $x, x \in X_i \Rightarrow x \sim x$
   2. $x, y \in X_i \Rightarrow y, x \in X_i$
   3. $x, y, y, z \in X_i \Rightarrow x, z \in X_i$

   $\Rightarrow \sim$ — эквивалентность

■

Def 1.3.4. $\sim$ *на* X, *тогда фактормножество* $(X/\sim)$ — *множество, состоящее из классов эквивалентности*

1.4. Перестановка — биективное отображение $X = \{1, 2, \cdots, n\}$ в X

Запись перестановки: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

Def 1.4.1. *Композиция перестановок. (σ, τ)*
$\sigma, \tau \Rightarrow \sigma \circ \tau = \sigma\tau$ — *выполняется справа налево.*

Def 1.4.2. $e = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}$ — *тождественная перестановка*

Утверждение 1.4.3. $\forall \sigma \to \exists \sigma^{-1}$

Множество всех перестановок $X = \{1, 2, ..., n\}$ обозначается S_n

Def 1.4.4. *Группой называется некоторое множество* G, *на котором определена бинарная операция:* $\forall x, y \in G \to xy \in G$. *При этом выполняются следующие аксиомы*

1. $\forall x, y, z \in G \to (xy)z = x(yz)$ *- ассоциативность.*

2. $\forall x \in G \to \exists e \in G : xe = ex = x$ *- нейтральный элемент*

3. $\forall x \in G \to \exists x^{-1} \in G : xx^{-1} = x^{-1}x = e$

Теорема 1.4.5. S_n относительно композиции является группой.

Def 1.4.6. *Порядком группы* G *называется количество элементов в* G
Обозначается $|G|$

Def 1.4.7. $\begin{pmatrix} 1 & i_1 & i_2 & ... & i_k \\ i_1 & i_2 & i_3 & ... & 1 \end{pmatrix}$ – k*-цикл*

$\begin{pmatrix} i & j \\ j & i \end{pmatrix} = (ij)$ – *транспозиция.*

Пример 1.4.8. $\sigma = \begin{pmatrix} 1 & 5 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}$

$\sigma^2 = \begin{pmatrix} 1 & 5 & 3 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 5 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 & 5 & 4 \end{pmatrix}$

Теорема 1.4.9. $\forall \sigma \in S_n$ может быть разложена в произведение независимых циклов.

Доказательство. $1 \leqslant i, j \leqslant n$. $i \sim j \Leftrightarrow \exists p \in \mathbb{Z} : \sigma^p(i) = j$

1. $\sigma^0(i) = i$ - рефлексивность
2. $\sigma^p(i) = j \Rightarrow \sigma^{-p}(j) = i$ - симметричность
3. $\sigma^p(i) = j, \sigma^q(j) = k \Rightarrow \sigma^{p+q}(i) = k$ - транзитивность

$\Rightarrow$ по теореме о разбиении множества $\Rightarrow X = X_1 \cup ... \cup X_s \Rightarrow \forall X_i$ соответствует цикл, длина которого равна $|X_i|$
Пусть $j \in X_i$, тогда $\begin{pmatrix} j & \sigma(j) & \sigma^2(j) & ... & \sigma^p(j) \\ \sigma(j) & \sigma^2(j) & \sigma^3(j) & ... & j \end{pmatrix} \Rightarrow$ все такие циклы независимы.
Замечание 1.4.10. Можно доказать, что это разложение единственно с точностью до порядка.

■

Следствие 1.4.11. $\forall \sigma \in S_n$ раскладывается в произведение транспозиций

Доказательство. Рассмотрим какой-то k-цикл.

$$\begin{pmatrix} i_1 & i_2 & i_3 & ... & i_k \\ i_2 & i_3 & i_4 & ... & i_1 \end{pmatrix} = \begin{pmatrix} i_1 & i_k \\ i_k & i_1 \end{pmatrix} \begin{pmatrix} i_1 & i_{k-1} \\ i_{k-1} & i_1 \end{pmatrix} ... \begin{pmatrix} i_1 & i_3 \\ i_3 & i_1 \end{pmatrix} \begin{pmatrix} i_1 & i_2 \\ i_2 & i_1 \end{pmatrix}$$

■

Замечание 1.4.12. Разложение перестановки в произведение транспозиций не является единственным.

1.5. Знак перестановки

Def 1.5.1. $\sigma = \tau_1, \tau_2, ..., \tau_k, \tau_i, 1 \leqslant i \leqslant k$ - *транспозиции.*
Знаком перестановки σ *называется* $\varepsilon_\sigma = (-1)^k$

Замечание 1.5.2. Если $\tau = (ij) \Rightarrow \tau^2 = (ij)^2 = e$

Теорема 1.5.3. О знаке перестановки

1. ε_σ не зависит от способа разложения σ на произведение транспозиций
2. $\varepsilon_\sigma \varepsilon_\tau = \varepsilon_{\sigma\tau}$

Доказательство. 1. $\sigma = \tau_1\tau_2...\tau_k = \tau_1'\tau_2'...\tau_s', \tau_i, \tau_j'$ - транспозиции.
$\Rightarrow \tau_1\tau_2...\tau_k\tau_s' = \tau_1'\tau_2'...\tau_{s-1}' \Rightarrow \tau_1\tau_2...\tau_k\tau_s'\tau_{s-1}' = \tau_1'\tau_2'...\tau_{s-2}' \Rightarrow e = \tau_1\tau_2...\tau_k\tau_s'...\tau_1'$.
Если k, s одной четности $\Rightarrow e$ раскладывается в четное число транспозиций
k, s разной четности $\Rightarrow e$ раскладывается в нечетное число транспозиций.
Докажем, что e не может быть разложена в нечётное число транспозиций. Найдем транспозицию, содержащую i и будем двигать её влево
$e = \tau_1\tau_2...(ij)...$

Смотрим транспозицию слева от (ij):

$$(ij)(ij) = e \Rightarrow$$

число транспозиций уменьшилось на 2

$$(ik)(ij) = (ij)(jk)$$

$$(jk)(ij) = (ik)(jk)$$

$$(kl)(ij) = (ij)(kl)$$

$\Rightarrow$ если не будет пункта 1 $\Rightarrow e = (it)...$
$e(i) = i$. Однако правая часть $i \to t$, что невозможно. $\Rightarrow$ обязательно будет 1 $\Rightarrow$ число транспозиций уменьшится на 2
Было $k+s$ транспозиций. $k+s-2, k+s-4, ... = 0 \Rightarrow k+s$ - чётное.

2. $\varepsilon_\sigma \varepsilon_\tau = \varepsilon_{\sigma\tau}$
   $\sigma = \tau_1...\tau_k, \tau = \tau'_1...\tau'_s$
   $\varepsilon_\sigma \varepsilon = (-1)^k \cdot (-1)^s = (-1)^{k+s}$
   $\varepsilon_{\sigma\tau} = (-1)^{k+s}$

■

Def 1.5.4. *Если $\varepsilon = +1$, то перестановка называется четной*

1.6. Чётные перестановки

$A_n = \{$чётные перестановки в $S_n\}$
$\overline{A_n} = S_n \setminus A_n$

Утверждение 1.6.1. $|A_n| = |\overline{A_n}| = \frac{n!}{2}$

Доказательство. Пусть $\tau = (ij), \sigma \in A_n, \varphi : A_n \to \overline{A_n}, \varphi(\sigma) = \tau\sigma \in \overline{A_n}$
Инъективность: $\sigma_1 \neq \sigma_2 \in A_n, \varphi(\sigma_1) = \tau\sigma_1, \varphi(\sigma_2) = \tau\sigma_2$
Если $\tau\sigma_1 = \tau\sigma_2 \Rightarrow \sigma_1 = \sigma_2$ - противоречие
Сюръективность: Пусть $\rho \in \overline{A_n} \Rightarrow \tau\rho \in A_n \Rightarrow \varphi(\tau\rho) = \tau(\tau\rho) = \rho \Rightarrow \varphi$ - биективно $\Rightarrow |A_n| = |\overline{A_n}|$ ■

Замечание 1.6.2. $e \in A_n, \sigma, \rho \in A_n \Rightarrow \sigma\rho \in A_n$.

$$\sigma = \tau_1\tau_2...\tau_k, \sigma^{-1} = \tau_k\tau_{k-1}...\tau_1 \in A_n$$

Значит A_n - группа относительно композиции.

Def 1.6.3. *G - группа. Множество $H \subseteq G$ называется подгруппой G, если оно также образует группу. Обозначение: $H \leqslant G$*

Теорема 1.6.4. $A_n \leqslant S_n \Rightarrow |A_n| = \frac{n!}{2}$

Def 1.6.5. *A_n - знакопеременная группа (alternating)*

1.7. Инверсии

Def 1.7.1. $\sigma = \begin{pmatrix} 1 & ... & s & ... & t & ... & n \\ i & ... & i_s & ... & i_t & ... & i_n \end{pmatrix}$. *Говорят, что* (s, t) *образуют инверсию, если* $s < t \wedge i_s > i_t$. *Количество всех инверсий равно* $inv(\sigma)$

Теорема 1.7.2 (Инверсии и четность и перестановки)**.** σ – четная (нечетная) $\Leftrightarrow$ $inv(\sigma)$ четно (нечетно)

Доказательство. 1. Пусть $\sigma = \begin{pmatrix} ... & s & t & ... \\ ... & i & j & ... \end{pmatrix}, \tau = \begin{pmatrix} i & i+1 \\ i+1 & i \end{pmatrix}, j = i+1$ Хотим узнать, как меняется количество инверсий при умножении на τ.

$$\tau\sigma = \begin{pmatrix} i & i+1 \\ i+1 & i \end{pmatrix} \begin{pmatrix} ... & s & ... & t & ... \\ ... & i & ... & i+1 & ... \end{pmatrix} \Rightarrow$$

количество инверсий изменится на 1.
Число инверсий в парах без s и t не поменялось. $(k, s), (m, t)$ - тоже не поменялось. (s, t) - изменилось на 1.

2. $\tau = (ij)$ - произовальная транспозиция. σ - произовальная перестановка.
$\tau = \begin{pmatrix} i & i+1 \end{pmatrix} \begin{pmatrix} i+1 & i+2 \end{pmatrix} ... \begin{pmatrix} i+k-1 & j \end{pmatrix} \begin{pmatrix} i+k-2 & i+k-1 \end{pmatrix} ... \begin{pmatrix} i+1 & i+2 \end{pmatrix} \begin{pmatrix} i & i+1 \end{pmatrix}$
$\Rightarrow \tau$ раскладывается в $2(k-1)+1$ транспозицию соседних элементов $\Rightarrow$ число инверсий $\tau\sigma$ изменится на нечётное число.

3. $\sigma = \sigma_1\sigma_2...\sigma_l e$, где σ_i – независимые циклы.
Если σ_l раскладывается в чётное число транспозиций, то в $\sigma_l e$ чётное число инверсий (т.к. каждая транспозиция меняет $inv(\sigma_l)$ на нечетное число).
Если σ_l раскладывается в нечётное число транспозиций, то в $\sigma_l e$ нечётное число инверсий.

∎

Раздел #2: Теория чисел

2.1. Делимость

Def 2.1.1. $a \vdots b$ *или* $b | a \Leftrightarrow \exists q : a = b \cdot q, b \neq 0$

Свойства:

1. Рефлексивность. $a \vdots a, a \neq 0$
2. Антисимметричность на $\mathbb{N}$. $a \vdots b, b \vdots a \Rightarrow a = b$
3. Транзитивность. $a \vdots b, \vdots c \Rightarrow a \vdots c$
4. $a | b, a | c \Rightarrow a | (b \pm c)$.

   Доказательство. $b = a \cdot q_1, c = aq_2 \Rightarrow b \pm c = aq_1 \pm aq_2 = a(q_1 \pm q_2)$ ■
5. $a | b \Rightarrow \forall c \to a | bc$
6. Пусть $a | b_i, i = 1, ..., n, a | (b_1 + ... + b_n + c) \Rightarrow a | c$

   Доказательство. $b_1 + ... + b_n + c = aq, aq_1 + aq_2 + ... + aq_n + c = aq \Rightarrow c = a(q - q_1 - ... - q_n)$ $\Rightarrow a | c$ ■
7. $a | b \Rightarrow \forall k \neq 0 \to ka | kb$
8. $ka | kb \Rightarrow a | b$

Теорема 2.1.2 (О делении с остатком)**.**

$$\forall a \wedge \forall b > 0 \ \exists! q, r, 0 \leqslant r < b : a = bq + r$$

Def 2.1.3. *a - делимое, b - делитель, q - частное (неполное частное), r - остаток*

Доказательство. $\exists$-ние. Рассмотрим $a - bq$. Выберем q так, чтобы $a - bq > 0$ было наименьшим. Положим $r = a - bq \geqslant 0 \Rightarrow a = bq + r$. По выбору $q \to a - b(q+1) < 0 \Rightarrow a < b(q+1) \Rightarrow$
$r = a - bq < b(q+1) - bq = b$.
Единственность. Преположим, что $a = bq_1 + r_1 = bq_2 + r_2, 0 \leqslant r_1, r_2 < b$

$$|r_1 - r_2| < b, bq_1 + r_1 = bq_2 + r_2 \Rightarrow b(q_1 - q_2) = r_2 - r_1 \Rightarrow |b(q_1 - q_2)| \geqslant b$$

Но $|r_1 - r_2| < b$ - противоречие. ■

2.2. Наибольший общий делитель

Def 2.2.1. *Общим делителем* $a_1, a_2, ..., a_n$ *называется* $d : d|a_i, i = 1, ..., n$.

Def 2.2.2. *Наибольший общий делитель* $a_1, a_2, ..., a_n$ *называется* d *такое, что*

1. $d > 0$
2. $d|a_i, i = 1, ..., n$
3. *если* $d'|a_i, i = 1, ..., n$, *то* $d'|d$

Обозначается $\gcd(a_1, a_2, ..., a_n) = (a_1, a_2, ..., a_n)$

Замечание 2.2.3. По определению $\gcd(0, 0) = 0$. $a \neq 0$, то $\gcd(a, 0) = 0$

Свойства:

1. $b|a \Rightarrow (a, b) = b$

   Доказательство. Докажем, что множество делителей (a, b) совпадает с множество делителей b.

$$d|(a, b) \Rightarrow d|b$$

$$d|b \Rightarrow d|a(\text{по транзитивности}) \Rightarrow d|(a, b)$$

■

2. $a = bq + c \Rightarrow (a, b) = (b, c)$
3.

   Алгоритм 2.2.4 (Алгоритм Евклида).

$$a = bq_1 + r_1, 0 \leqslant r_1 < b$$

$$b = r_1q_1 + r_2, 0 \leqslant r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, 0 \leqslant r_3 < r_2$$

$$...$$

$$r_{n-2} = r_{n-1}q_n + r_n, 0 \leqslant r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1}$$

   Теорема 2.2.5. $r_n = \gcd(a, b)$

   Доказательство. $r_1 > r_2 > r_3 > ... \geqslant 0 \Rightarrow \exists r_{n+1} = 0$. $r_n|r_{n-1}$.

$$r_n = (r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = ... = (r_2, r_1) = (b, r_1) = (a, b)$$

■

4. $(ma, mb) = m \cdot (a, b)$
5. $d|a, d|b \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$

   Доказательство. $(a, b) = \left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = d \cdot \left(\frac{a}{d}, \frac{b}{d}\right)$ ■
6. $(a, b) = 1 \Rightarrow (a, bc) = (a, c)$

   Доказательство. Докажем, что $(a, bc)|(a, c)$

   $$(a, bc)|a, (a, bc)|ac, (a, bc)|bc \Rightarrow (a, bc)|(ac, bc) \Rightarrow (a, bc)|(a, b) \cdot c = c \Rightarrow (a, bc)|(a, c)$$

   Теперь докажем, что $(a, c)|(a, bc)$

   $$(a, c)|a, (a, c)|c \Rightarrow (a, c)|bc \Rightarrow (a, c)|(a, bc) \Rightarrow (a, bc) = (a, c)$$

   ■
7. $(a, b) = 1, b|ac \Rightarrow b|c$

   Доказательство.

   $$b|bc, b|ac \Rightarrow b|(bc, ac) = c$$

   ■
8. $(a, b) = (a - b, b)$

Теорема 2.2.6 (Линейное представление НОД)**.**

$$(a, b) = d \Rightarrow \exists u, v : u \cdot a + v \cdot b = d$$

Доказательство. Из алгоритма Евклида:

$$r_{n-2} = r_{n-1} \cdot q_n + r_n \Rightarrow d = r_n = r_{n-2} - r_{n-1} \cdot q_n$$

$$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1} \Rightarrow d = r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1})q_n$$

Из следующей строки выражаем r_{n-2} и т.д. $\Rightarrow$ останутся a и $b \Rightarrow d = u \cdot a + v \cdot b$ ■

2.3. Наименьшее общее кратное

Def 2.3.1. *Общим кратным $a_1, a_2, ..., a_n$ называется число $M > 0 : a_i|M \ \forall i = 1, ..., n$*
Наименьшее из общих кратных – НОК.

Теорема 2.3.2. $\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$

Доказательство. $a = a_1 d, b = b_1 d, (a_1, b_1) = 1$

$$M = at = bs \Rightarrow \frac{M}{b} = \frac{at}{b} = \frac{a_1 dt}{b_1 d} = \frac{a_1 t}{b_1} \Rightarrow M = \frac{b \cdot a_1 t}{b_1}$$

t делится на b_1, т.е. $t = b_1 k$

$$M = \frac{b a_1 b_1 k}{b_1} = b a_1 k \text{ - минимально при } k = 1 \Rightarrow M = b a_1 = \frac{b a_1 d}{d} = \frac{ab}{\gcd(a, b)}$$

■

2.4. Математическая индукция

1. Аксоима. $\forall$ подмножество $\mathbb{N}$ имеет наши элементы $\Rightarrow$ ММИ.
2. Аксиома. $A_1, A_n \Rightarrow A_{n+1} \Rightarrow \forall A_n$

Следствие 2.4.1. Пусть $a_1, a_2, ..., a_n$ – попарно взаимно-простые $\Rightarrow \operatorname{lcm}(a_1, a_2, ..., a_n) = a_1 \cdot a_2 \cdot \ldots \cdot a_n$

Доказательство. $n = 2$. $\operatorname{lcm}(a_1, a_2) = \frac{a_1 a_2}{\gcd(a_1, a_2)} = a_1 \cdot a_2$
Пусть верно для n. Тогда для $n + 1$

$$(a_i, a_n a_{n+1}) = (a_i, a_{n+1}) = 1 \Rightarrow a_1, a_2, ..., a_{n-1}, a_n a_{n+1} \Rightarrow$$

$$\Rightarrow \operatorname{lcm}(a_1, ..., a_{n-1}, a_n \cdot a_{n+1}) = a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} \cdot a_n \cdot a_{n+1}$$

■

2.5. Простые числа

Def 2.5.1. *Число $p > 1$ называется простым, если оно делится только на 1 и на p. Иначе число называется составным.*

Теорема 2.5.2 (о наименьшем делителе)**.** Наименьший делитель $a > 1$ – простое число

Доказательство. $M = \{d | d > 1, d | a\} \neq \varnothing$ Пусть p - наименьший элемент M. Предположим, что p – составное, т.е. $p = bq, q < p, q | p, p | a \Rightarrow q | a$ – противоречие. ■

Теорема 2.5.3. p - наименьший делитель > 1 числа $n \Rightarrow p \leqslant \sqrt{n}$

Доказательство.

$$n = mp, p \leqslant m \Rightarrow np \leqslant nm \Rightarrow mp \cdot p \leqslant nm \Rightarrow p^2 \leqslant n \Rightarrow p \leqslant \sqrt{n}$$

■

Теорема 2.5.4 (Теорема Евклида)**.** Простых чисел бесконечно много

Доказательство. Пусть $p_1, p_2, ..., p_n$ – все простые числа, $a = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$. Если $a \vdots p_i$, то $1 \vdots p_i \Rightarrow a$ – новое простое число. ■

2.6. Основная теорема арифметики

Lm 2.6.1. p – простое $\Rightarrow \forall a > 1 \to p|a \vee (p, a) = 1$

Доказательство.

$$(p, a)|p \Rightarrow (p, a) = 1 \vee (p, a) = p$$

■

Lm 2.6.2. p – простое, $p|a_1 \cdot a_2 \cdot ... \cdot a_n \Rightarrow \exists i = 1, ..., n : p|a_i$

Доказательство. Если $(p, a_i) = 1, i = 1, ..., n \Rightarrow 1 = (p, a_1) = (p, a_1 a_2) = (p, a_1 a_2 a_3) = (p, a_1 \cdot ... \cdot a_n) = 1 \Rightarrow \exists a_i : p|a_i$ ■

Теорема 2.6.3 (Основная теорема арифметики)**.** 1. $\forall a > 1 \to a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}, p_1, p_2, ..., p_k$ – различные простые, $\alpha_1, \alpha_2, ..., \alpha_k \geqslant 1$

2. с точностью до перестановки множителей это представление единственно

Доказательство. 1. из всех делителей a выбираем наименьший – p_1 - простое $\Rightarrow a = p_1 \cdot a_1$. Рассмотрим a_1 – наименьший делитель - $p_2 \Rightarrow a_1 = p_1 \cdot p_2 \cdot a_2$ и т.д.

$$a_1 > a_2 > a_3 > ... \Rightarrow \exists a_n = 1 \Rightarrow a = \text{ разложение на простые}$$

2. Предположим, что представление не одно, то есть

$$a = p_1 \cdot p_2 \cdot ... \cdot p_s = q_1 \cdot q_2 \cdot ... \cdot q_n$$

Не умаляя общности, пусть $n \geqslant s \Rightarrow p_1 | q_1 ... q_n$. Тогда, по лемме 2 $p_1 | q_i \Rightarrow p_1 = q_i$. Перенумеруем $i = 1 \Rightarrow p_2 p_3 ... p_s = q_2 q_3 ... q_n \Rightarrow$ все p_s сократятся, т.е. $1 = q_{s+1} ... q_n \Rightarrow s = n$

■

Def 2.6.4. $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_k^{\alpha_k}$ – *каноническое разложение числа a*

Следствие 2.6.5. Любой делитель $a = p_a^{\alpha_1} ... p_k^{\alpha_k}$ имеет вид $b = p_1^{\beta_1} \cdot ... \cdot p_k^{\beta_k}, 0 \leqslant \beta_i \leqslant \alpha_i$

Доказательство. $b|a \Rightarrow b$ содержит в разложении p_i ■

Следствие 2.6.6. $\gcd(a_1, ..., a_n)$ имеет вид $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, где
$a_i = \min\{$показатель степени p_i, с которым p_i входит в разложение $a_1, a_2, ..., a_n\}$

Следствие 2.6.7. $\mathrm{lcm}(a_1, ..., a_n)$ имеет вид $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, где
$a_i = \max\{$показатель степени p_i, с которым p_i входит в разложение $a_1, a_2, ..., a_n\}$

2.7. Непрерывные дроби (Цепные дроби)

Def 2.7.1. *Выражение вида*

$$a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + ...}}}$$

называется непрерывной дробью. Обозначение: $[a_0, a_1, a_2, ...]$

Теорема 2.7.2. Любое вещественное число может быть представлено в виде непрерывной дроби.
Если число иррационально – в виде бесконечной дроби, если рациональное – в виде конечной.

Доказательство. $a > b$

$$\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\frac{b}{r_1}} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{r_3}{r_2}}} \text{ и т.д.}$$

где

$$a = b \cdot a_0 + r_1$$
$$b = r_1 \cdot a_1 + r_2$$
$$r_1 = r_2 \cdot a_2 + r_3$$

∎

Def 2.7.3. *Для* $\frac{a}{b}$ $\delta_0 = \frac{a_0}{1}, \delta_1 = a_0 + \frac{1}{a_1}, \delta_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}}$ *и т.д. называются подходящими дробями.*

Теорема 2.7.4 (Формулы подходящих дробей). $\delta_k = \frac{p_k}{q_k}, p_{-1} = 1, q_{-1} = 0, p_0 = a_0, q = 1$

$$\Rightarrow \begin{cases} p_k = a_k \cdot p_{k-1} + p_{k-2} \\ q_k = a_k \cdot q_{k-1} + q_{k-2} \end{cases}$$

Доказательство. $\delta_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1 \cdot 1 + 0} = \frac{a_1 \cdot p_0 + p_{-1}}{a_1 \cdot q_0 + q_{-1}}$
Предположим, что для k верно. Тогда для $k+1$

$$\delta_{k+1} = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + ... \frac{1}{a_k + \frac{1}{a_{k+1}}}}} = \frac{(a_k + \frac{1}{a_{k+1}}) \cdot p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}}) \cdot q_{k-1} + q_{k-2}} =$$

$$= \frac{(a_{k+1} \cdot a_k + 1) \cdot p_{k-1} + p_{k-2} \cdot a_{k+1}}{(a_{k+1} \cdot a_k + 1) \cdot q_{k-1} + q_{k-2} \cdot a_{k+1}} = \frac{a_{k+1}(a_k \cdot p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1} \cdot p_k + p_{k-1}}{a_{k+1} \cdot q_k + q_{k-1}}$$

∎

Раздел #3: Теория сравнений

3.1. Начала теории сравнений

Def 3.1.1. *a и b называются сравнимыми по модулю $m > 0$, если они имеют одинаковые остатки при делении на m*

$$a \equiv b \pmod m, a \equiv b(m), a \overset{m}{\equiv} b$$

Утверждение 3.1.2.

$$\Leftrightarrow \begin{cases} a \equiv b \pmod m \\ a - b \vdots m \\ a \equiv b + mt \end{cases}$$

Доказательство. 1) $\Rightarrow$ 2)

$$a = mq_1 + r, b = mq_2 + r \Rightarrow a - b = m(q_1 - q_2) \vdots m$$

2) $\Rightarrow$ 3)

$$a - b \vdots m \Rightarrow a - b = mt \Rightarrow a = b + mt$$

3) $\Rightarrow$ 1). Поделим a и b на m:

$$a = mq_1 + r_1, b = mq_2 + r_2$$

$$3) : a = b + mt \Rightarrow mq_1 + r_1 = mq_2 + r_2 + mt \Rightarrow$$
$$\Rightarrow m(q_1 - q_2 - t) = r_2 - r_1 \Rightarrow m | r_2 - r_1 \Rightarrow r_2 - r_1 = 0$$

■

Свойства:

1. Рефлексивность. $a \equiv a \pmod m$
2. Симметричность. $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$
3. Транзитивность. $a \equiv b \pmod m \Rightarrow b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

   Доказательство.

   $$a - c = a - b + b - c \vdots m$$

   ■

4. $a \equiv b \pmod m, c \equiv d \pmod m \Rightarrow a + c \equiv b + d \pmod m$
5. $a \equiv b \pmod m, c \equiv d \pmod m \Rightarrow ac \equiv bd \pmod m$

   Доказательство.

   $$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) \vdots m$$

   ■

6. $d|a, d|b, d|m, a \equiv b \pmod{m} \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

   Доказательство.

$$a - b = a_1 d - b_1 d = my = m_1 dt \Rightarrow a_1 - b_1 = m_1 t$$

■

7. $a \equiv b \pmod{m} \Rightarrow ka \equiv kb \pmod{m}$
8. $d|a, d|b, (m, d) = 1, a \equiv b \pmod{m} \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{m}$

   Доказательство.

$$a = a_1 d, b = b_1 d, a - b \vdots m \Rightarrow (a_1 - b_1) \cdot d \vdots m \Rightarrow a_1 - b_1 \vdots m$$

■

9. $d|m, a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{d}$
10. $a \equiv b \pmod{m} \Rightarrow (a, m) = (b, m)$

    Доказательство.

$$a \equiv b \pmod{m} \Rightarrow a = b + mt \Rightarrow (a, m) = (b, m)$$

■

3.2. Классы вычетов

Def 3.2.1. *Классом вычетов по* $\pmod{m}$ *называется множество чисел, сравнимых с a по модулю m*

$$m = 7, \overline{1} = \{-6, 8, 1, 15, ...\}$$

$$\overline{a} = \{x | x \equiv a \pmod{m}\}$$

Элементы классов вычетов – ***вычеты****. Обычно рассматривают наименьший неотрицательный вычет.*

Def 3.2.2. *Множество вычетов, взятых по одному из разных классов образуют полную систему вычетов. Например*

$$\{0, 1, 2, ..., m - 1\}$$

Lm 3.2.3. Множество из m чисел, попарно несравнимых по модулю m, образуют полную систему вычетов.

Теорема 3.2.4. $(a, m) = 1$. Если x пробегает полную систему вычетов по $\pmod{m} \Rightarrow \forall b \to ax + b$ тоже пробегает полную систему вычетов по $\pmod{m}$

Доказательство. x принадлежит m значений $\Rightarrow ax + b$ принадлежит m значений.
Пусть $x_1 \not\equiv x_2 \pmod{m}$. Предположим, что $ax_1 + b \equiv ax_2 + b \pmod{m} \Rightarrow ax_1 \equiv ax_2 \pmod{m} \Rightarrow x_1 \equiv x_2 \pmod{m}$ ■

3.3. Кольцо классов вычетов

Def 3.3.1. *Определим сложение и умножение вычетов по фиксированному модулю m.*

$$\overline{a}+\overline{b}=\overline{a+b}, \overline{a}\cdot\overline{b}=\overline{ab}$$

Lm 3.3.2. Сложение и умножение определены корректно

Доказательство. $a \equiv a_1 \pmod{m}, b \equiv b_1 \pmod{m}$

$$\Rightarrow a+b=a_1+b_1 \pmod{m}, a\cdot b=a_1\cdot b_1 \pmod{m} \Rightarrow \overline{a}+\overline{b}=\overline{a}_1+\overline{b}_1, \overline{a}\cdot\overline{b}=\overline{a}_1\cdot\overline{b}_1$$

■

Def 3.3.3. *Группа G называется коммутативной (абелевой), Если*

$$\forall x,y\in G\to xy=yx$$

Теорема 3.3.4. $\mathbb{Z}_m$ образует коммутативную группу относительно сложения

Доказательство. $\overline{a}+\overline{b}=\overline{a+b}\in\mathbb{Z}_m$

1. $(\overline{a}+\overline{b})+\overline{c}=\overline{a+b}+\overline{c}=\overline{a+b+c}$
   $\overline{a}+(\overline{b}+\overline{c})=\overline{a}+\overline{b+c}=\overline{a+b+c}$
2. $\overline{0}$. $\overline{a}+\overline{0}=\overline{a+0}=\overline{a}$
3. $-\overline{a}=\overline{m-a}\Rightarrow\overline{a}-\overline{a}=\overline{a+m-a}=\overline{0}$
4. $\overline{a}+\overline{b}=\overline{b}+\overline{a}$

■

Def 3.3.5. *(Ассоциативным) кольцом называется множество R, на котором заданы бинарные операции:*

1. $\forall x,y,z\to(x+y)+z=x+(y+z)$

2. $\exists 0\in R:\forall x\in R\to x+0=x$

3. $\forall x\in R\ \exists(-x)\in R: x+(-x)=0$

4. $\forall x,y\in R\to x+y=y+x$

5. $\forall x,y,z\in R\to(y+z)=xy+xz, (x+y)z=xz+yz$

6. $\forall x,y,z\in R\to(xy)z=x(yz)$

Замечание 3.3.6. $\exists 1\in R:\forall x\in R\to x\cdot 1=1\cdot x=x$ – кольцо с единицей
$\forall x,y\in R\to xy=yx$ – коммутативное кольцо

Теорема 3.3.7. $\mathbb{Z}_m$ – коммутативное кольцо с единицей.

Доказательство.

$$\overline{a}(\overline{b}+\overline{z})=\overline{a}\cdot\overline{b+c}=\overline{a(b+c)}=\overline{ab+ac}$$

и т.д. ■

Def 3.3.8. *Кольца R, в котором $\forall a,b\to(ab=0\Rightarrow a=0\vee b=0)$ называется кольцом без делителей нуля.*
Если $ab=0$ и $a,b\neq 0$, то a,b – делители нуля

Def 3.3.9. *Коммутативное кольцо без делителей нуля – область целостности.*

<u>**Теорема**</u> **3.3.10.** 1. $\mathbb{Z}_m$ имеет делители нуля $\Leftrightarrow m$ – составное число

2. $\mathbb{Z}_p, p$ - простое – область целостности.

Доказательство. "$\Rightarrow$". $m = n \cdot k, \overline{n} \cdot \overline{k} = \overline{0}$ в $\mathbb{Z}_m$
"$\Leftarrow$". $\overline{n} \cdot \overline{k} = \overline{0} \Rightarrow n \cdot k \equiv 0 \pmod m$
Предположим, что m – простое $\Rightarrow m|n \vee m|k \Rightarrow \overline{n} = \overline{0} \vee \overline{k} = \overline{0}$. Но $\overline{n}$ и $\overline{k}$ – делители нуля, т.е. $\overline{n}, \overline{k} \neq 0 \Rightarrow m$ – составное.
1) $\Rightarrow$ 2) ■

3.4. Приведенная система вычетов

Def 3.4.1. *Вычеты, выбранные из полной системы вычетов и взаимно-простые с модулем m обрузуют приведенную систему вычетов*

Def 3.4.2. *Количество вычетов в приведенной системе вычетов обозначается $\varphi(m)$ – функция Эйлера.*

<u>**Lm**</u> **3.4.3.** Если p – простое, то

$$\varphi(p) = p - 1$$

<u>**Теорема**</u> **3.4.4.** $(a, m) = 1, x$ пробегает приведенную систему вычетов $\Rightarrow ax$ тоже пробегает приведенную систему вычетов по $\pmod m$

Доказательство. $x \to \varphi(m), ax \to \varphi(m)$
$(ax, m) = (a, m) = 1 \Rightarrow ax$ набор чисел из $\varphi(m)$, взаимно-простых с $m \Rightarrow \{ax\}$ – приведенная система вычетов. ■

3.5. Функция Эйлера

<u>**Lm**</u> **3.5.1.** p – простое, $\alpha > 0$

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

Доказательство. $1, 2, 3, ..., p, 2p, 3p, ..., p \cdot p, ..., p^\alpha - 1$. Выбросим из этого множества числа, делящиеся на p. Таких чисел будет ровно количество коэффициентов при p до p^α, т.е. $p^{\alpha-1}$ ■

Def 3.5.2. *Функия $\Theta : \mathbb{N} \to \mathbb{N}$ называется мультипликативной, если*

$$(a, b) = 1 \Rightarrow \Theta(ab) = \Theta(a) \cdot \Theta(b)$$

<u>**Теорема**</u> **3.5.3** (Мультипликативность функции Эйлера)**.** φ мультипликативна

Доказательство. $(a, b) = 1$

$$\begin{array}{ccccc} 1 & 2 & 3 & ... & b \\ b+1 & b+2 & b+3 & ... & 2b \\ ... & ... & ... & ... & ... \\ (a-1)b+1 & (a-1)b+2 & (a-1)b+3 & ... & ab \end{array}$$

Количество чисел, взаимно-простых с $b : \forall$ строка : $kb + r, k = 0, ..., a-1, 1 \leqslant r \leqslant b$. Рассмотрим k-ю строку: $(kb+r, b) = 1 \Rightarrow (r, b) = 1$. Количество чисел $kb+r : (kb+r, b) = 1 = \varphi(b) \Rightarrow$ есть $\varphi(b)$ столбцов, в которых числа $(kb + r, b) = 1$. Найдем в этих столбцах числа, взаимно-простые с a. $\forall$ столбец : $xb+r, x = 0, ..., a-1 \Rightarrow xb+r$ – полная система вычетов по $\pmod a \Rightarrow$ среди $\{xb+r\}$ чисел, взаимно-простых с $a = \varphi(a) \Rightarrow$ всего чисел, взаимно-простых с $ab = \varphi(a) \cdot \varphi(b)$ ■

Следствие 3.5.4. $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k}$ – каноническое разложение $\Rightarrow \varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdot ... \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$

Замечание 3.5.5. $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdot ... \cdot (1 - \frac{1}{p_k})$

Теорема 3.5.6 (Теорема Эйлера)**.** $(m, a) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$

Доказательство. $r_1, r_2, ..., r_{\varphi(m)}$ – приведенная система вычетов по $\pmod m$
$\Rightarrow ar_1, ar_2, ..., ar_{\varphi(m)}$ – приведенная система вычетов по $\pmod m$. Пусть $ar_i = \rho_i$

$$\Rightarrow ar_1 \cdot ar_2 \cdot ...ar_{\varphi(m)} = \rho_1 \rho_2 \cdot ... \cdot \rho_{\varphi(m)}$$

$$a^{\varphi(m)} r_1 \cdot r_2 \cdot ... \cdot r_{\varphi(m)} = \rho_1 \cdot \rho_2 \cdot ... \cdot \rho_{\varphi(m)} \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m$$

■

Теорема 3.5.7 (Теорема Ферма)**.** p – простое, $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod p$

Доказательство. $\varphi(p) = p - 1$ ■

Def 3.5.8. $\mathbb{Z}_m^* = \{r : 0 \leqslant r < m, (r, m) = 1\}$ – *приведенная система вычетов по* $\pmod m$

Теорема 3.5.9. $\mathbb{Z}_m^*$ – коммутативная группа по умножению

Доказательство. $r_1, r_2 \in \mathbb{Z}_m^*$. $(r_1, m) = (r_2, m) = 1 \Rightarrow (r_1 \cdot r_2, m) = 1 \Rightarrow r_1 \cdot r_2 \in \mathbb{Z}_m^*, 1 \in \mathbb{Z}_m^*$
$r \in \mathbb{Z}_m^*$, то $r^{-1} = r^{\varphi(m)-1} \Rightarrow r^{\varphi(m)-1} \cdot r = r^{\varphi(m)} \equiv 1 \pmod m$ ■

3.6. Сравнения с одним неизвестным

Def 3.6.1. $f(x) \equiv 0 \pmod m$. *Решением этого сравнения называется* $x_0 : f(x_0) \equiv 0 \pmod m$.
Решения x_1 *и* x_2 *называются эквивалентными, если* $x_1 \equiv x_2 \pmod m$
Решить сравнение – найти решений из полной системы вычетов.

Теорема 3.6.2 (Решение линейного сравнения)**.** $ax \equiv b \pmod m, (a, m) = d$

1. $d \not| \, b \Rightarrow$ решений нет.
2. $d | b \Rightarrow \exists d$ решений : $x = x_0 + m_1 t, t = 0, 1, ..., d - 1, m_1 = \frac{m}{d}, x_0$ – какое-то решение

Доказательство. 1. Очевидно

2. Если $(a, m) = 1, x$ пробегает полную систему вычетов по $\pmod m$ $\Rightarrow ax$ – полная система вычетов по $\pmod m$ $\Rightarrow \exists x_0 : ax_0 \equiv b \pmod m$
   Если $(a, m) = d, a = a_1 d, m = m_1 d, b = b_1 d, (a_1, m_1) = 1$
   $a_1 x \equiv b_1 \pmod{m_1}$ – $\exists$ решение $x_0 : a_1 x_0 \equiv b_1 \pmod{m_1}$. $x = x_0 + m_1 t$ – решение $ax \equiv b \pmod m$

$$a(x_0 + m_1 t) = a_1 d x_0 + a_1 d m_1 t \equiv b_1 d \pmod m$$

   Посмотрим, какие решения принадлежат полной системе вычетов, т.е. $0 \leqslant x_0 + m_1 t < m$. Ясно, что такие решения будут при $t = 0, 1, ..., d - 1$.

■

Теорема 3.6.3 (Методы решения $ax \equiv b \pmod m, (a,m) = 1$)**.** 1. $ax \equiv b \pmod m \Rightarrow x \equiv a^{\varphi(m)-1} \cdot b \pmod m$

2. $ax \equiv b \pmod m \Rightarrow x \equiv (-1)^n p_{n-1} \cdot b \pmod m$
   $\frac{m}{a}$ – непрерывная дробь, p_{n-1} – числитель $(n-1)$-й подходящей дроби, $\frac{p_n}{q_n} = \frac{m}{a}$

Доказательство. $p_k \cdot q_{k-1} - p_{k-1} \cdot q_k = (-1)^{k-1}$. $k = n$

$$m \cdot q_{n-1} - p_{n-1} \cdot a = (-1)^{n-1} \Rightarrow -p_{n-1} \cdot a \equiv (-1)^{n-1} \pmod m$$

$$ap_{n-1}b = (-1)^n b \pmod m \Rightarrow a \cdot (-1)^n p_{n-1} \cdot b \equiv b \pmod m \Rightarrow x \equiv (-1)^n p_{n-1} \cdot b \pmod m$$

■

3.7. Диофантовы уравнения

Def 3.7.1. *Уравнение вида*

$$a_1x_1 + a_2x_2 + ... + a_nx_n = b$$

где $a_i \in \mathbb{Z}, x_i$ *– переменные и* $\exists i : a_i \neq 0$, *называется диофантовым.*

Lm 3.7.2. $ax + by = c, a, b \neq 0$. Если $x_0 : ax_0 \equiv c \pmod b \Rightarrow (x_0, \frac{ax_0 - c}{b})$ – решения уравнения

Доказательство. $by \equiv c - ax$ при $x = x_0$ и $c - ax \,\vdots\, b \Rightarrow \frac{c - ax_0}{b} \in \mathbb{Z}$ ■

Теорема 3.7.3. $ax + by = c, d = (a,b), d|c$. Пусть (x_0, y_0) – какое-то решение $\Rightarrow$ все решения:

$$\begin{cases} x = x_0 - \frac{b}{d}t \\ y = y_0 + \frac{a}{d}t \end{cases}, t \in \mathbb{Z}$$

3.8. Системы сравнений

$$\begin{cases} x \equiv b_1 \pmod m_1 \\ x \equiv b_2 \pmod m_2 \\ ... \\ x \equiv b_k \pmod m_k \end{cases}$$

Теорема 3.8.1 (Китайская теорема об остатках)**.** $(m_i, m_j) = 1, i \neq j$. Тогда

1. Решение системы существует:

$$x \equiv \frac{M}{m_1} \cdot M_1' b_1 + \frac{M}{m_2} \cdot M_2' b_2 + ... + \frac{M}{m_k} M_k' b_k \pmod M$$

   $M = m_1 \cdot m_2 \cdot ... \cdot m_k, M_i' : M_i' \cdot \frac{M}{m_i} \equiv 1 \pmod m_i$

2. Решение единственно

Доказательство. 1. Подставим в i-е уравнение:

$$x \equiv \frac{M}{m_i} M_i' b_i \pmod{m}_i \Rightarrow x \equiv b_i \pmod{m}_i$$

2. Без доказательства.

■

Теорема 3.8.2 (Теорема Вильсона)**.** p – простое $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$

Доказательство. "$\Rightarrow$". $\mathbb{Z}_p^* = \{1, 2, ..., p-1\}$ – группа, $a \in \mathbb{Z}_p^*$

$$a^2 = 1 \Rightarrow a = \pm 1, 1 \cdot 2 \cdot ... \cdot (p-1) \Rightarrow 1 \cdot (p-1) \equiv -1 \pmod{p}$$

$$a \neq a^{-1} \Rightarrow 2 \cdot ... \cdot (p-2) = 1$$

"$\Leftarrow$". Предположим, что

$$k|p, k > 1, k \neq p \Rightarrow k < p \Rightarrow 1 \cdot 2 \cdot ... \cdot (p-1) \vdots k \Rightarrow (p-1)! \equiv 0 \pmod{p}$$

■

Алгоритм 3.8.3 (Алгоритм RSA)*.* 1. Выбираем p, q – простые
2. $n = p \cdot q, \varphi(n) = (p-1)(q-1)$
3. Выбираем $e : (e, \varphi(n)) = 1$
4. Решаем $e \cdot d \equiv 1 \pmod{\varphi(n)} \Rightarrow$ находим d
Шифрование:

1. m – текст (в виде цифрового кода)
2. $c \equiv m^e \pmod{n} \Rightarrow c$ – шифр

Ключи:

- (e, n) – открытый ключ
- (d, n) – закрытый ключ

Дешифрование:

$$c^d \equiv m^{ed} \equiv m \pmod{n}$$

Трудность $n = p \cdot q$.

Раздел #4: Комплексные числа

Def 4.0.1. *Множество* $\{(a, b)|a, b \in \mathbb{R}\}$ *называется множество комплексных чисел, если:*

1. $(a, b) = (c, d) \Leftrightarrow a = c, b = d$
2. $(a, b) + (c, d) = (a + c, b + d)$
3. $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$
4. $a = (a, 0)$

Проверим корректность:

- *1 и 4:* $a = b \Leftrightarrow (a, 0) = (b, 0)$
- *2 и 4:* $a + b = (a, 0) + (b, 0) = (a + b, 0) = a + b$
- *3 и 4:* $a \cdot b = (a, 0) \cdot (b, 0) = (ab, 0) = ab$

Теорема 4.0.2. $\mathbb{C}$ образует коммутативное кольцо с единицей.

Доказательство. $(0, 0)$ – нейтральный элемент по сложению. $(a, b) : -(a, b) = (-a, -b)$ – обратный элемент по сложению. Остальные свойства несложно проверяются. ■

Def 4.0.3. *Множество* K *называется полем, если* K *является коммутативным кольцом с единицей и*

$$\forall x \in K^* = K \setminus \{0\}\ \exists x^{-1} \in K : x \cdot x^{-1} = 1$$

Теорема 4.0.4. $\mathbb{Z}_p$(p – простое)$, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ – поля.

Доказательство. $\mathbb{Q}, \mathbb{R}$ – поля.
$\mathbb{Z}_p$ – коммутативное кольцо с единицей, $\mathbb{Z}_p^*$ – мультипликативная группа $\Rightarrow \mathbb{Z}_p$ – поле.
$(a, b) \in \mathbb{C}^*, (a, b)^{-1} = \frac{(a,-b)}{a^2+b^2} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$

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

■

Def 4.0.5. (a, b) *и* $(a, -b)$ *– комплексно-сопряженные числа.*
$|(a, b)| = \sqrt{a^2 + b^2}$ *– модуль комплексного числа. Заметим, что* $|(a, 0)| = \sqrt{a^2 + 0} = \sqrt{a^2} = |a|$
$(a, b) \cdot (a, -b) = a^2 + b^2 = |(a, b)|^2$

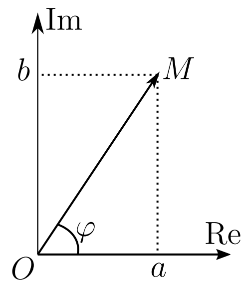
4.1. Алгебраическая форма записи комплексного числа

Def 4.1.1. *Положим* $i = (0, 1)$*. Тогда*

$$(a, b) = (a, 0) + (0, b) = (a, 0) \cdot (1, 0) + (b, 0) \cdot (0, 1) = a + bi$$

4.2. Геометрическое представление комплексных чисел

Def 4.2.1. $z = a + bi$. $\operatorname{Re} z = a$ – *вещественная часть числа* z, $\operatorname{Im} z = b$ – *мнимая часть.* $z = a + bi \mapsto$ *точка на комплексной плоскости.* (a, b) – *радиус-вектор* OM.
$\rho = |z| = \sqrt{a^2 + b^2}$ – *длина вектора* OM. $\varphi = (\widehat{\operatorname{Re}, OM})$ – *аргумент комплексного числа.* $\arg z = \varphi, \varphi = \varphi_0 + 2\pi k, \varphi_0 \in [0; 2\pi)$ *или* $\varphi_0 \in (-\pi; \pi]$.



4.3. Тригонометрическая форма записи комплексного числа

Def 4.3.1. $a = \rho\cos\varphi, b = \rho\sin\varphi \Rightarrow z = a + bi = \rho(\cos\varphi + i\sin\varphi)$

$$\operatorname{tg}\varphi = \frac{b}{a} \Rightarrow \varphi = \begin{cases} \operatorname{arctg}\frac{b}{a}, z \in \ \textit{I и II четверти} \\ \operatorname{arctg}\frac{b}{a} + \pi, z \in \textit{III и IV четверти} \end{cases}$$

Def 4.3.2 (Неравенство треугольника)**.** $z_1, z_2 \in \mathbb{C}$

1. $|z_1 + z_2| \leqslant |z_1| + |z_2|$

2. $|z_1 - z_2| \geqslant ||z_1| - |z_2||$

Доказательство. 1. $z_1 = \rho_1(\cos\varphi_1 + i\sin\varphi_1), z_2 = \rho_2(\cos\varphi_2 + i\sin\varphi_2)$

$$|z_1 + z_2|^2 = |\rho_1\cos\varphi_1 + \rho_2\cos\varphi_2 + i(\rho_1\sin\varphi_1 + \rho_2\sin\varphi_2)|^2 =$$
$$= \rho_1^2\cos^2\varphi_1 + 2\rho_1\rho_2\cos\varphi_1\cos\varphi_2 + \rho_2^2\cos^2\varphi_2 + \rho_1^2\sin^2\varphi_1 + 2\rho_1\rho_2\sin\varphi_1\sin\varphi_2 + \rho_2^2\sin^2\varphi_2 =$$
$$= \rho_1^2 + 2\rho_1\rho_2\cos(\varphi_1 - \varphi_2) + \rho_2^2 \leqslant \rho_1^2 + 2\rho_1\rho_2 + \rho_2^2 = (\rho_1 + \rho_2)^2 = (|z_1| + |z_2|)^2$$

2.
$$|z_1| = |z_1 - z_2 + z_2| \leqslant |z_1 - z_2| + |z_2| \Rightarrow |z_1| - |z_2| \leqslant |z_1 - z_2| \Rightarrow ||z_1| - |z_2|| \leqslant |z_1 - z_2|$$

■

Замечание 4.3.3. $|z_1 + z_2| = |z_1| + |z_2| \Leftrightarrow z_1 \parallel z_2$

Теорема 4.3.4 (Умножение комплексных чисел в тригонометрической форме). $z_1 = \rho_1(\cos\varphi_1 + i\sin\varphi_1), z_2 = \rho_2(\cos\varphi_2 + i\sin\varphi_2)$. Тогда

$$z_1 \cdot z_2 = \rho_1 \cdot \rho_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$$

Доказательство. Достаточно перемножить, заметить формулу косинуса суммы и синуса суммы ■

Следствие 4.3.5 (Формула Муавра). $z = \rho(\cos\varphi + i\sin\varphi) \Rightarrow z^n = \rho^n(\cos n\varphi + i\sin n\varphi)$

Доказательство. 1. $n \geqslant 0$. По индукции: $n = 1$ очевидно.
$n - 1 \to n:$

$$z^n = z^{n-1} \cdot z = \rho^{n-1}(\cos(n-1)\varphi + i\sin(n-1)\varphi) \cdot \rho(\cos\varphi + i\sin\varphi) = \rho^n(\cos n\varphi + i\sin n\varphi)$$

2. $n < 0$. Пусть $n = -m, m > 0$. Тогда

$$z^n = \frac{1}{z^m} = \frac{1}{\rho^m(\cos m\varphi + i\sin m\varphi)} = \rho^{-m}\frac{\cos m\varphi - i\sin m\varphi}{1} = \rho^n(\cos n\varphi + i\sin n\varphi)$$

■

4.4. Извлечение корней из комплексных чисел

Def 4.4.1. *Корнем n-й степени из комплексного числа z называется $w \in \mathbb{C} : w^n = z$*

Теорема 4.4.2. $\forall z \in \mathbb{C}^* \; \exists n$ корней n-й степени $z_k, k = 0, 1, ..., n-1$

$$z_k = \sqrt[n]{\rho}(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}), z = \rho(\cos\varphi + i\sin\varphi)$$

Доказательство. $w^n = z, w = R(\cos\Theta + i\sin\Theta)$

$$\Rightarrow (w^n = z) : R^n(\cos(n\Theta) + i\sin(n\Theta)) = \rho(\cos\varphi + i\sin\varphi) \Rightarrow$$
$$\Rightarrow R = \sqrt[n]{\rho}, \cos(n\Theta) = \cos\varphi, \sin(n\Theta) = \sin\varphi \Rightarrow$$
$$\Rightarrow n\Theta = \varphi + 2\pi k \Rightarrow \Theta = \frac{\varphi + 2\pi k}{n} \Rightarrow \text{ любой корень имеет вид } z_k$$

■

4.5. Корни из единицы

Def 4.5.1. *Корень из 1 n-й степени ε_k называется первообразным, если он принадлежит показателю, т.е. $\forall m : 0 < m < n \to \varepsilon^m \neq 1$*

Теорема 4.5.2 (О первообразном корне). Корень из 1 n-й степени является первообразным $\Leftrightarrow (k, n) = 1$.

Доказательство. "$\Rightarrow$". ε_k – первообразный корень. Предположим, что $(k,n) = d > 1, k = k_1 d, n = n_1 d, n_1 < n$. Тогда

$$\varepsilon_k^{n_1} = \cos\frac{2\pi k n_1}{n} + i\sin\frac{2\pi k n_1}{n} = \cos\frac{2\pi k_1 d n_1}{n} + i\sin\frac{2\pi k_1 d n_1}{n} = 1?! \Rightarrow d = 1$$

"$\Leftarrow$". $(k,n) = 1$. Предположим, что $\varepsilon_k^m = 1 \Rightarrow \cos\frac{2\pi km}{n} = 1, \sin\frac{2\pi km}{n} = 0$

$$\Leftrightarrow \frac{2\pi km}{n} = 2\pi s \Rightarrow \frac{km}{n} \in \mathbb{Z} \Rightarrow n | m \Rightarrow m \geqslant n$$

■

Свойства:

1. α – корень из 1 степени n, β – корень из 1 степени $m \Rightarrow \alpha\cdot\beta$ – тоже корень из 1.

   Доказательство. $(\alpha\beta)^{\mathrm{lcm}(m,n)} = 1$ ■

2. Если α – корень из 1 степени n, то α^{-1} – корень из 1 степени n

   Доказательство. $(\alpha^{-1})^n = \frac{1}{\alpha^n} = 1$ ■

3. $u_n = \{z \in \mathbb{C} : z^n = 1\}$ – мультипликативная коммутативная группа.
   $u_n = \{\varepsilon_k, \varepsilon_k^2, ..., \varepsilon_k^{n-1}, 1\}, \varepsilon_k$ – первообразный корень.

Def 4.5.3. *Группа G называется циклической, если $G = \{a, a^2, a^3, ...\}$. Пишут $G = \langle a\rangle$ – группа G порождается элементом a.*

Def 4.5.4. *G_1 – группа с операцией $*_1, G_2$ – группа с операцией $*_2$. Говорят, что группы G_1 и G_2* ***изоморфны****, если $\exists\varphi : G_1 \to G_2$:*

- *φ – биективно*
- *$\forall x, y \in G_1 \to \varphi(x *_1 y) = \varphi(x) *_2 \varphi(y)$*

Теорема 4.5.5. *$u_n \simeq \mathbb{Z}_n$*

Доказательство. ε – первообразный корень, т.е. $u_n = \{\varepsilon^k\}, k = 0, ..., n-1$
$\varphi : \mathbb{Z}_n \to u_n, \varphi(k) = \varepsilon^k, \varphi$ – биекция

$$\varphi(k+m) = \varepsilon^k \cdot \varepsilon^m = \varphi(k)\cdot\varphi(m)$$

■

4.6. Показательная форма записи комплексного числа

Def 4.6.1. *$e^{i\varphi} = \cos\varphi + i\sin\varphi$ – показательная форма записи комплексного числа.*

Def 4.6.2 (Формула Эйлера)**.** *$e^{i\varphi} = \cos\varphi + i\sin\varphi, e^{-i\varphi} = \cos\varphi - i\sin\varphi$. Тогда*

$$\cos\varphi = \frac{e^{i\varphi} + e^{-i\varphi}}{2}$$
$$\sin\varphi = \frac{e^{i\varphi} - e^{-i\varphi}}{2i}$$

Свойства комплексных чисел:

1. $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$
2. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$
3. $\overline{z_1 \pm z_2} = \overline{z_1} \pm \overline{z_2}$
4. $z + \overline{z} \in \mathbb{R}$
5. $i(z - \overline{z}) \in \mathbb{R}$

Раздел #5: Многочлены

Def 5.0.1. *R – коммутативное кольцо с 1. Множество $\{(a_0, a_1, ..., a_n, ...), \exists n : \forall m > n \to a_m = 0\}$*

1. *$\alpha \in R \to \alpha(a_0, a_1, ..., a_n, ...) = (\alpha a_0, \alpha a_1, ..., \alpha a_n, ...)$*
2. *$(a_0, a_1, ..., a_n, ...) + (b_0, b_1, ..., b_n) = (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, ...)$*
3. *$(a_0, a_1, ..., a_n) \cdot (b_0, b_1, ..., b_n, ...) = (c_0, c_1, ..., c_n, ...)$, где*

$$c_k = \sum_{s+t=k} a_s b_t$$

4. *$\forall a \in R \to a = (a, 0, 0, ...)$*

Это множество называется многочленами над R.

Корректность определения:

- все действия 1, 2, 3 не выводят из множества.
- Согласование 1 и 4, 2 и 4, 3 и 4.

Теорема 5.0.2. Множество многочленов над R – коммутативное кольцо с 1

Доказательство. $(0, 0, ...)$ – нулевой элемент, $(1, 0, 0, ...)$ – единица. Ассоциативность несложно доказывается. ■

Def 5.0.3. *Введём $x = (0, 1, 0, ...)$. Тогда $x^2 = (0, 1, 0, 0, ...) \cdot (0, 1, 0, 0, ...) = (0, 0 \cdot 1 + 1 \cdot 0, 0 \cdot 0 + 1 \cdot 1, 0, ...) = (0, 0, 1, 0, ...)$*

$$\Rightarrow x^k = (\underset{0}{0}, \underset{1}{0}, ..., \underset{k}{1}, \underset{k+1}{0}, ...)$$

Тогда

$$(a_0, a_1, ..., a_n, ...) = (a_0, 0, ...) + (0, a_1, 0, ...) + ... + (0, ..., a_k, ...) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$$

Обозначение: $R[x] = \{a_0 + a_1 x + ... + a_n x^n\}$ – кольцо многочленов над R от переменной x.

Def 5.0.4. *Коэффициент $a_n \neq 0 : a_m = 0, m > n$ называется старшим коэффициентом. Если $n \geqslant 1$, то n – степень многочлена.*

$$\deg(f) = n$$

Если a_0 – старший коэффициент. Если $a_0 \neq 0$, то $\deg(f) = 0$. Если $a_0 = 0$, то $\deg(f) = -\infty$

Теорема 5.0.5. $f, g \in R[x]$

1. $\deg(f + g) \leqslant \max\{\deg f, \deg g\}$
2. $\deg(f \cdot g) \leqslant \deg f + \deg g$

Доказательство. $f = a_0 + a_1x + ... + a_nx^n, g = b_0 + b_1x + ...b_mx^m$. Тогда если $n > m$, то

$$f + g = a_nx^n + ... \Rightarrow \deg(f+g) \leqslant \deg n$$

$$f \cdot g = a_n \cdot b_mx^{n+m} + ... \Rightarrow \deg(f \cdot g) \leqslant n + m$$

■

Пример 5.0.6. $\mathbb{Z}_6[x]$. $f = 2x^2 + 1, g = 3x + 2$

$$f \cdot g = 6x^3 + 4x^2 + 3x + 2 = 4x^2 + 3x + 2 \Rightarrow \deg(f \cdot g) = 2 < \deg f + \deg g = 3$$

Def 5.0.7. *Коммутативное кольцо с 1 без делителей нуля называется областью целостности.*

Теорема 5.0.8. R – область целостности $\Rightarrow R[x]$ – область целостности.

Доказательство. $f = a_nx^n + ..., g = b_mx^m + ... \Rightarrow f \cdot g = a_nb_mx^{n+m} + ..., a_n \cdot b_m \neq 0$ т.к. R – область целостности $\Rightarrow R[x]$ – область целостности. ■

Lm 5.0.9 (О сокращении)**.** R – область целостности, $a, b, c \in R, a \neq 0$. Тогда $ab = ac \Rightarrow b = c$.

Доказательство. $ab = ac \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0$ ■

Теорема 5.0.10 (О делении с остатком)**.** R – область целостности, $\forall f \in R[x], \forall g \in R[x]$ с обратимым старшим коэффициентом $\exists!\ q, r \in R[x] : f = g \cdot q + r, \deg r < \deg g$

Доказательство. Существование. $\deg f = n, \deg g = m, n < m \Rightarrow f = g \cdot 0 + f$
$n \geqslant m$. Индукция по n. $n = 0 \Rightarrow a_0 = b_0(b_0^{-1}a_0) + 0$.
$n - 1 \mapsto n$. $f = a_nx^n + ... + a_0$, $g = b_mx^m + ... + b_0$. Рассмотрим

$$\overline{f} = f - a_nb_m^{-1}x^{n-m} \cdot g \Rightarrow \deg \overline{f} < n$$

$\Rightarrow$ по предположению индукции $\overline{f} = g \cdot q + r \Rightarrow f - a_nb_m^{-1}x^{n-m}g = g \cdot q + r$

$$\Rightarrow f = (g + a_nb_m^{-1}x^{n-m})g + r, \deg r \leqslant \deg g$$

Единственность. Предположим, что

$$f = g \cdot q_1 + r_1, f = g \cdot q_2 + r_2$$

$\Rightarrow g(q_1 - q_2) = r_2 - r_1$. Если $q_1 \neq q_2, r_1 \neq r_2$, то $\deg(g(q_1 - q_2)) \geqslant m, \deg(r_2 - r_1) < m$ – противоречие. ■

Def 5.0.11. $f = a_nx^n + ... + a_0, c \in R$. *Тогда* $f(c) = a_nc^n + ... + a_1c + a_0$ *– значение многочлена в точке* c.
Если $f(c) = 0$, *то* c *– корень многочлена.*

Теорема 5.0.12 (Теорема Безу)**.** R – область целостности, $a \in R, f \in R[x]$

$$\Rightarrow f = (x - a) \cdot q(x) + f(a)$$

Доказательство. $f = (x-a)q+r, \exists! q, r, \deg r < 1 \Rightarrow r \in R$. $x = a \Rightarrow f(a) = 0+r \Rightarrow r = f(a)$. ■

Следствие 5.0.13. $f \vdots x - a \Leftrightarrow f(a) = 0$

Def 5.0.14. *Многочлен $f \in R[x]$ со старшим коэффициентом 1 называется нормализованным.*

5.1. Корни многочлена

Def 5.1.1. *Если многочлен $f = (x-c)^k q, q(c) \neq 0$, то c – корень кратности k.*
Иначе, если $(x-c)^k | f, (x-c)^{k+1} \not| f$, то c – корень кратности k.

Теорема 5.1.2 (О количестве корней многочлена)**.** Число корней многочлена f с учетом их кратности $\leqslant \deg f$

Доказательство. Индукция по $\deg f$
$\deg f = 0 \Rightarrow$ всё верно. Если нет корней $\Rightarrow$ всё верно.
Пусть для $\deg f < n$ доказано. Докажем для $\deg f = n$.
c_1 – корень $f \Rightarrow f = (x-c_1)^k g(x)$, если $c_2 \neq c_1$ – другой корень $\Rightarrow f(c_2) = (c_2-c_1)^k g(c_1) = 0 \Rightarrow c_2$ – корень g. $\deg g = n - k < n \Rightarrow$ корней $g \leqslant n - k \Rightarrow$ корней $f \leqslant k + n - k = n$. ■

Следствие 5.1.3. $f, g \in R[x]$. Пусть $\max\{\deg f, \deg g\} = n$. Предположим, что $\exists c_1, ..., c_{n+1} \in R$: $f(c_i) = g(c_i) \Rightarrow f$ совпадает с g

Доказательство. $h = f - g, \deg h \leqslant n, h(c_i) = 0, i = 1, ..., n+1 \Rightarrow h \equiv 0$ ■

Формальное равенство многочленов.

$$f = g = a_n x^n + ... + a_1 x + a_0$$

Функциональное равенство многочленов.

$$f(x) = g(x) \ \forall x \in R$$

Пример 5.1.4. $\mathbb{Z}_5$. $f = x^5 + x^4, g = x^4 + x$.
$f - g = x^5 - x, x^5 \equiv x \pmod 5 \Rightarrow x^5 - x = 0 \ \forall x \in \mathbb{Z}_5 \Rightarrow f(x) = g(x)$

Замечание 5.1.5. R – бесконечно, то $\forall x \in R \ f(x) = g(x) \Leftrightarrow f = g$

Упражнение 5.1.6. Доказать утверждение выше

5.2. Наибольший общий делитель

Пусть $R = K$ – поле.

Def 5.2.1. *R – область целостности, $a, b \in R$. $d = \gcd(a, b)$, если*

1. $d|a, d|b$
2. $c|a, c|b \Rightarrow c|d$

Теорема 5.2.2 (О НОД для многочленов)**.** $\forall f, g \in K[x]$

1. $\exists d = \gcd(f, g)$ определен однозначно с точностью до ассоциированного элемента
2. $\exists h_1, h_2 \in K[x] : h_1 f + h_2 g = d$

Доказательство. Полностью аналогично доказательству о существовании нод над $\mathbb{Z}$ ■

Def 5.2.3. *R – область целостности. R^* – обратимые элементы. Если $a, b \in R, a = \varepsilon b, \varepsilon \in R^*$, то a, b – ассоциированные.*

Пример 5.2.4. K – поле, $K^* = K \setminus \{0\} \Rightarrow$ все элементы ассоциированны.

Пример 5.2.5. $\mathbb{Z}, \mathbb{Z}^* = \{-1, 1\}, a = -b$

Пример 5.2.6. $\mathbb{Z}_n, \mathbb{Z}_n^* = \{m \in \mathbb{Z} : (m, n) = 1\}$

Упражнение 5.2.7. Доказать.

Пример 5.2.8. $K[x], (K[x])^* = K^*$

Def 5.2.9. *$f, g \in K[x]$ – взаимно-простые, если $(f, g) = 1$*

5.3. Факториальность кольца многочленов

Def 5.3.1. *R – область целостности. $p \in R$:*

1. $p \notin R^*$
2. $p = ab \Rightarrow a$ *или* $b \in R^*$

Тогда p – простой (неразложимый) элемент R.

Def 5.3.2. *Если в области целостности R $\forall a \in R \setminus \{0\}$ $\exists a = \varepsilon \cdot p_1 \cdot ... \cdot p_s, \varepsilon \in R^*, p_1, ...p_s$ – простые, определенное с точностью до порядка и умноженное на ε, то R – факториальное кольцо.*

Def 5.3.3. *Простой элемент кольца $K[x]$ называется неприводимым многочленом.*

Пример 5.3.4. $x^2 - 2$ – неприводим над $\mathbb{Q}$

Пример 5.3.5. $\forall$ многочлен $x - a$ неприводим.

Упражнение 5.3.6. Над бесконечным полем K существует бесконечно много неприводимых многочленов.

Свойства:

1. $f \in K[x], \varphi$ – неприводим над $K \Rightarrow$ либо $\varphi | f$, либо $(f, \varphi) = 1$.

   Доказательство. $d = (f, \varphi)$. Если $d \neq 1 \Rightarrow d|f, d|\varphi \Rightarrow d = \varepsilon \cdot \varphi ..., \varepsilon \in K^* \Rightarrow \varphi | f$ ∎

2. $\varphi_1, \varphi_2 \in K[x]$ – неприводимы $\Rightarrow (\varphi_1, \varphi_2) = 1$ или $\varphi_1 = \varepsilon \varphi_2, \varepsilon \in K^*$.
3. $f, g, \varphi \in K[x], \varphi$ – неприводим, $\varphi | fg \Rightarrow \varphi | f \vee \varphi | g$

   Доказательство. $\varphi \not| f \Rightarrow (\varphi, f) = 1 \Rightarrow \exists h_1, h_2 \in K[x] : h_1\varphi + h_2 f = 1 \Rightarrow h_1 \varphi g + h_2 f g = g \Rightarrow \varphi | (h_1 \varphi g + h_2 f g) \Rightarrow \varphi | g$ ∎

4. $\varphi \in K[x]$ – неприводим, $f_1, ..., f_s \in K[x]$, $\varphi | f_1 \cdot ... \cdot f_s \Rightarrow \exists i, 1 \leqslant i \leqslant s : \varphi | f_i$

Lm 5.3.7. $\forall f \in K[x] : \deg f \geqslant 1$ делится хотя бы на один неприводимый многочлен.

Доказательство. $\deg f = n$. $n = 1$ – верно. Предположим, что для $m < n$ тоже всё верно. f – приводим $\Rightarrow f = f_1 \cdot g, \deg f_1 < n \Rightarrow \exists$ неприводимый многочлен φ, который делит $f_1 \Rightarrow f_1 | f$. ∎

Теорема 5.3.8. K – поле. $K[x]$ – факториальное кольцо.

Доказательство. Существование. $f \in K[x]$. Если f – неприводим, то очевидно. Если $f = \varphi_1 \cdot f_1, \varphi$ – неприводим; $f_1 = \varphi_2 \cdot f_2$ и т.д. $\Rightarrow f = \varphi_1 \cdot \varphi_2 \cdot ... \cdot \varphi_k$
Единственность. $f = \varepsilon \varphi_1 \varphi_2 ... \varphi_k = \eta \psi_1 \psi_2, ..., \psi_s, \varepsilon, \eta \in K^*, \varphi_i, \psi_j$ – неприводимы. $k \leqslant s \Rightarrow \varphi_1 | \eta \psi_1 \psi_2 ... \psi_s \Rightarrow \varphi_1 | \psi_j \Rightarrow \varphi_1 = \psi_j \Rightarrow \varepsilon^{-1} \eta \psi_{s-k} ... \psi_s = 1 \Rightarrow \varepsilon = \eta, \psi_{s-k} ... \psi_s = 1$ ∎

Def 5.3.9. *$f = \varepsilon \cdot \varphi_1^{k_1} \cdot ... \cdot \varphi_s^{k_s}$, где $\varepsilon \in K^*, \varphi_1, \varphi_2, ..., \varphi_s$ – различные неприводимые многочлены над K, $k_1, k_2, ..., k_s \geqslant 1 \in \mathbb{Z}$ – каноническое разложение многочлена f.*

5.4. Каноническое разложение многочлена над $\mathbb{C}$

Def 5.4.1. *Поле K называется алгебраически замкнутым, если любой многочлен* $\deg \geqslant 1$ *имеет хотя бы один корень.*

Пример 5.4.2. $\mathbb{Q}(x^2 - 2), \mathbb{R}(x^2 + 1), \mathbb{Z}_p$ не являются алгебраически замкнутыми.

Теорема 5.4.3 (Основная теорема высшей алгебры). $\mathbb{C}$ – алгебраически замкнуто.

Следствие 5.4.4. Каноническое разложение многочлена над $\mathbb{C}$

$$f = a_n (x - z_1)^{k_1} (x - z_2)^{k_2} ... (x - z_s)^{k_s}$$

$z_1, ..., z_s \in \mathbb{C}, a_n \in \mathbb{C}$

5.5. Каноническое разложение многочлена над $\mathbb{R}$

Def 5.5.1. *R_1, R_2 – кольца с 1. Гомоморфизмом колец R_1 и R_2 называется $\varphi : R_1 \to R_2$:*

1. $\forall x, y \in R_1 \ \varphi(x+y) = \varphi(x) + \varphi(y)$
2. $\forall x, y \in R_1 \ \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$
3. $\varphi(1) = 1$

Def 5.5.2. *Биективный гомоморфизм колец – **изоморфизм**, при этом сами кольца называются **изоморфными**.*

Пример 5.5.3. 1. $id : R \to R$ – изоморфизм.

2. $\varphi : \mathbb{Z} \to \mathbb{Z}_n, \varphi(a) = a \pmod n$ – гомоморфизм.

Доказательство.

$$\varphi(a+b) = a+b \pmod n = \begin{cases} a+b, 0 \leqslant a+b < n \\ a_0 + b_0 \equiv a+b \pmod n \end{cases} = a \pmod n + b \pmod n = \varphi(a) + \varphi(b)$$

$$ab \equiv a_0 b_0 \pmod n \Rightarrow \varphi(ab) = ab \pmod n = (a \pmod n) \cdot (b \pmod n) = \varphi(a) \cdot \varphi(b)$$
$$\varphi(1) = 1$$

$\Rightarrow \varphi$ – гомоморфизм.
$\varphi(kn) = 0 \Rightarrow$ не инъективно $\Rightarrow$ не изоморфизм. ■

3. $\varphi : R \to R[x], \varphi(r) = r$ – вложение - гомоморфизм.

Свойства:

1. $\varphi(0) = 0$

Доказательство. $\varphi(x) = \varphi(x+0) = \varphi(x) + \varphi(0) \Rightarrow \varphi(0) = \varphi(x) - \varphi(x) = 0$ ■

2. $\varphi(-x) = -\varphi(x)$

Доказательство. $0 = \varphi(x-x) = \varphi(x) + \varphi(-x) \Rightarrow \varphi(-x) = -\varphi(x)$ ■

Замечание 5.5.4. Противоположный элемент в кольце определен однозначно.

Доказательство. Пусть x имеет y и z – противоположные элементы. Тогда

$$z = 0 + z = y + x + z = y + 0 = y$$

■

Def 5.5.5. *Поле K_1 и K_2 называются изоморфными, если они изоморфны как кольца.*

Замечание 5.5.6. При этом $\forall x \in K, \varphi(x^{-1}) = \varphi(x)^{-1}$

$$1 = \varphi(x \cdot x^{-1}) = \varphi(x) \cdot \varphi(x^{-1}) \Rightarrow \varphi(x^{-1}) = \varphi(x)^{-1}$$

Обратный элемент определен однозначно: если y, z – обратные к x

$$(yx = zx = 1) \Rightarrow y = yxz = z$$

Def 5.5.7. *Изоморфизм $\varphi : K \to K$ (K – поле) называется автоморфизмом.*

Пример 5.5.8. 1. Найдем все автоморфизмы $\mathbb{Q} \to \mathbb{Q}$. $\varphi : \mathbb{Q} \to \mathbb{Q}$ – произвольный автоморфизм. $\varphi(1) = 1 \Rightarrow n \in \mathbb{Z}, n > 0$

$$\varphi(n) = \varphi(\underbrace{1 + 1 + ... + 1}_{n}) = \underbrace{\varphi(1) + ... + \varphi(1)}_{n} = n$$

$\Rightarrow \varphi(-n) = -n \Rightarrow \varphi|_{\mathbb{Z}} = id$
$q \cdot \varphi\left(\frac{1}{q}\right) = \underbrace{\varphi\left(\dfrac{1}{q}\right) + ... + \varphi\left(\dfrac{1}{q}\right)}_{q} = \varphi\left(\frac{1}{q} + ... + \frac{1}{q}\right) = \varphi(1) = 1 \Rightarrow \varphi\left(\frac{1}{q}\right) = \frac{1}{q} \Rightarrow \varphi\left(\frac{p}{q}\right) = p \cdot \varphi\left(\frac{1}{q}\right) = \frac{p}{q} \Rightarrow$ автоморфизмы $\mathbb{Q} = \{id\}$

2. автоморфизмы $\mathbb{R} = \{id\}$
3. $\mathbb{C}$, автоморфизмы: $id, \varphi(z) = \overline{z}$

Def 5.5.9. *K – поле, тогда k – подполе поля K, если $k \subset K$ и k – поле.*

Lm 5.5.10. $f \in k[x], c \in K, k \subset K, f(c) = 0, \varphi : K \to K$ – автоморфизм, $\varphi|_k = id \Rightarrow \varphi(c)$ – корень f.

Доказательство. $f = a_n x^n + ... + a_0, a_i \in k, i = 0, ..., n$

$$\varphi(f) = \varphi(a_n x^n + ... + a_0) = \varphi(a_n) \cdot \varphi(x^n) + ... + \varphi(a_1)\varphi(x) + \varphi(a_0) =$$

$$= a_n \varphi(x)^n + ... + a_1\varphi(x) + a_0 = f(\varphi(x))$$

$x = c : \varphi(f(c)) = \varphi(0) = 0$. С другой стороны $\varphi(f(c)) = f(\varphi(c)) \Rightarrow \varphi(c)$ корень f. ■

Теорема 5.5.11 (Неприводимые многочлены над $\mathbb{R}$)**.** Неприводимые многочлены над $\mathbb{R}$

1. $x - \alpha, \alpha \in \mathbb{R}$
2. $ax^2 + bx - c, b^2 - 4ac < 0$

Доказательство. f – неприводимый многочлен над $\mathbb{R}, \deg f \geqslant 2$, корней из $\mathbb{R}$ нет. Пусть $\alpha + \beta i$ – комплексный корень f ($\beta \neq 0$). По лемме $a - \beta i$ – тоже корень $\Rightarrow f \vdots (x - \alpha - \beta i)(x - \alpha + \beta i)$.

$$(x - \alpha - \beta i)(x - \alpha + \beta i) = (x - \alpha)^2 + \beta^2 = x^2 - 2\alpha x + \alpha^2 + \beta^2 \in \mathbb{R}[x] - \text{неприводим}$$

$\Rightarrow f = a(x^2 - 2\alpha x + \alpha^2 + \beta^2), a \in \mathbb{R}^*$ ■

Следствие 5.5.12. Каноническое разложение над $\mathbb{R}$.

$$f = a(x - \alpha_1)^{k_1}...(x - \alpha_s)^{k_s}(x^2 + p_1 x + q_1)^{r_1}...(x^2 + p_t x + q_t)^{r_t}$$

где $p_i^2 - 4q_i < 0, i = 1, ..., t$.

5.6. Уравнения 3-й степени

$ax^3 + bx^2 + cx + d = 0$

Теорема 5.6.1 (Метод Кардано)**.** 1. $x^3 + b'x^2 + c'x + d' = 0$ (поделили на a)

2. $x = y - \frac{b'}{3} \Rightarrow y^3 + py + q = 0$

3. $y = u + v : (u+v)^3 + p(u+v) + q = 0$

$$u^3 + 3u^2v + 3uv^2 + v^3 + p(u+v) + q = 0 \Leftrightarrow (u+v)(3uv+p) + u^3 + v^3 + q = 0$$

$$\Rightarrow \begin{cases} 3uv + p = 0 \\ u^3 + v^3 + q = 0 \end{cases} \Leftrightarrow \begin{cases} v = -\frac{p}{3u} \\ u^3 - \frac{p}{27u^3} + q = 0 \end{cases} \Leftrightarrow \begin{cases} v = -\frac{p}{3u} \\ 27u^6 + 27qu^3 - p^3 = 0 \end{cases}$$

$\Rightarrow$ получим три несимметричных решения (u, v)

4. Находим y и x.

5.7. Уравнения 4-й степени

$ax^4 + bx^3 + cx^2 + dx + e = 0$

Теорема 5.7.1 (Метод Феррари)**.** 1. $x^4 + b'x^3 + c'x^2 + d'x + e' = 0$ (поделим на a)

2. $x = y - \frac{b'}{4} \Rightarrow y^4 + \alpha y^2 + \beta y + \gamma$

3. Введем $u : (y^2 + \alpha + u)^2 - (\alpha y^2 + uy^2 + 2\alpha u - \beta y - \gamma + u^2 + \alpha^2) = 0$
Выбираем $u : (\alpha + u)y^2 + \beta y + (u + \alpha)^2 - \gamma$ – полный квадрат $\Leftrightarrow \beta^2 - u(\alpha + u)((u+\alpha)^2 - \gamma) = 0$ – уравнение третьей степени. Находим u.

4. Раскладываем разность квадратов: 2 квадратных уравнения относительно y

5. Находим x.

5.8. Отделение кратных корней

Def 5.8.1. $f \in K[x], f = a_n x^n + ... + a_1 x + a_0$. *Производной многочлена* f *называется* $f' = na_n x^{n-1} + ... + a_1$

Свойства:

1. $\deg f = 0 \Rightarrow f' = 0$
2. $(f + g)' = f' + g'$
3. $(c \cdot f)' = c \cdot f', c \in K$
4. $(f \cdot g)' = f'g + fg'$
5. $(f_1 \cdot f_2 \cdot ... \cdot f_k)' = f_1' f_2 ... f_k + f_1 f_2' ... f_k + f_1 f_2 ... f_k'$
6. $(f^k)' = k \cdot f^{k-1} \cdot f'$

Доказательство. 4. $f = a_n x^n, g = b_m x^m$

$$(a_n x^n \cdot b_m x^m)' = (n+m) a_n b_m x^{n+m-1}$$

$$(a_n x^n)' \cdot b_m x^m + a_n x^n \cdot (b_m x^m)' = a_n b_m (n+m) x^{n+m-1}$$

$f = a_n x^n, g = b_m x^m + ... + b_1 x + b_0$

$$(fg)' = \left(\sum\right)' = \sum ()' = f'g + fg'$$

$f = a_n x^n + ... + a_1 x + a_0, g = b_m x^m + ... + b_1 x + b_0$ $a_k x^k \cdot g$ – верно $\Rightarrow$ верно и для $f \cdot g$
5. Индукция
5. $\Rightarrow$ 6. ∎

Def 5.8.2. *Корни кратности 1 – простые корни, корни кратности > 1 – кратные корни.*

Теорема 5.8.3 (Критерий кратности корня)**.** $f \in K[x]$. c – кратный корень $f \Leftrightarrow f(c) = f'(c) = 0$

Доказательство. "$\Rightarrow$". $f = (x-c)^2 \cdot g, f(c) = 0$. $f'(c) = 2(x-c)g + (x-c)^2 \cdot g' \Rightarrow f'(c) = 0$.
"$\Leftarrow$". $\deg f \geqslant 2, f$ делим на $(x-c)^2 \Rightarrow f = (x-c)^2 \cdot g + ax + b$

$$\Rightarrow f = (x-c)^2 g + a(x-c) + r$$

$f(c) = 0 \Rightarrow r = 0$

$$f' = 2(x-c)g + (x-c)^2 g' + a, f'(c) = 0 \Rightarrow a = 0 \Rightarrow f = (x-c)^2 g$$

∎

5.9. Характеристика поля

K – поле. $1 + 1 + 1 + ... = 0 \vee \infty$

Def 5.9.1. *Наименьшее целое положительное* $n : \forall x \in K\ nx = 0$ *называется характеристикой поля:* $\operatorname{char} K = n$ *Если такого* n *не существует, то* $\operatorname{char} K = 0$

Lm 5.9.2. K – поле, $\operatorname{char} K = n > 0 \Rightarrow n = p$ – простое.

Доказательство. Предположим, что $n = mk, 1 < m, k < n \Rightarrow n \cdot 1 = m \cdot k \cdot 1 = 0 \Rightarrow m = 0$ или $k = 0$ – противоречие. ∎

Теорема 5.9.3. K – поле, $\operatorname{char} K = 0$. $f \in K[x], \varphi \in K[x]$ – неприводимый многочлен. $f = \varphi^k \cdot g, (\varphi, g) = 1$. Тогда $f' = \varphi^{k-1} h, (\varphi, h) = 1$

Доказательство. $f' = k\varphi^{k-1}\varphi' g + \varphi^k g' = \varphi^{k-1}(\underbrace{k\varphi' g + \varphi g'}_{h})$. Если $\varphi | h \Rightarrow \varphi | k\varphi' g$, но $(\varphi, \varphi' g) = 1 \Rightarrow (\varphi, h) = 1$. ∎

Теорема 5.9.4 (Критерий кратности корня)**.** $\operatorname{char} K = 0, f \in K[x], c \in L \supset K$. Тогда c – корень кратности k многочлена $f \Leftrightarrow f(c) = f'(c) = ... = f^{(k-1)}(c) = 0$ и $f^{(k)}(c) \neq 0$.

Доказательство. "$\Rightarrow$". $f = (x-c)^k g, g(c) \neq 0$, из предыдущей теоремы $\Rightarrow f' = (x-c)^{k-1} g_1, g_1(c) \neq 0$ и т.д. $\Rightarrow f'(c) = ... = f^{(k-1)}(c) = 0$, но $f^{(k-1)} = (x-c)g_{k-1}, g_{k-1}(c) \neq 0 \Rightarrow f^{(k)}(c) \neq 0$.
"$\Leftarrow$". c – кратный корень : $f = (x-c)^s \cdot g, g(c) \neq 0$. Дифференцируем $\Rightarrow s = k, f^{(k)} = h, h(c) \neq 0$. ■

Следствие 5.9.5. $\operatorname{char} K = 0, f = a\varphi_1^{k_1}\varphi_2^{k_2}...\varphi_s^{k_s}$ – каноническое разложение $\Rightarrow \gcd(f, f') = \varphi_1^{k_1-1}\varphi_2^{k_2-1}...\varphi_s^{k_s-1}$

Доказательство. $f = \varphi_i^{k_i} \cdot g \Rightarrow f' = \varphi_i^{k_i-1} \cdot h$ ■

Следствие 5.9.6 (Отделение кратных корней). $\operatorname{char} K = 0, f \in K[x] \Rightarrow g = \frac{f}{(f,f')}$ не имеет кратных корней.

5.10. Формула Тейлора для многочлена

Теорема 5.10.1 (Разложение по степеням другого многочлена)**.** K – поле, $\operatorname{char} K = 0, f, g \in K[x], \deg g \geqslant 1 \Rightarrow f = h_n g^n + h_{n-1} g^{n-1} + ... + h_1 g + h_0$, где $h_i \in K[x], \deg h_i < \deg g$ и это разложение единственно.

Доказательство. Существование. $\deg f < \deg g \Rightarrow f = f, h_0 = f$. $\deg f = \deg h_n + n \cdot \deg g \Rightarrow n = 0, \deg f = \deg h_0 \Rightarrow$ база индукции верна и для существовавния, и для единственности.
Индукционный переход: $\deg f \geqslant \deg g, f = g \cdot q + r, \deg r \leqslant \deg g, \deg q < \deg f \Rightarrow q = h_n g^n + ... + h_1 g + h_0 \Rightarrow f = gq + r = h_n g^{n+1} + ... + h_1 g^2 + h_0 g + r, \deg h_i < \deg g \Rightarrow$ существование доказано.
Предположим, что разложение не едиственно, т.е. $f = h_n g^n + ... + h_1 g + h_0 = h'_n g^n + ... + h'_1 g + h'_0$

$$\Rightarrow (h_n g^{n-1} + ... + h_1)g + h_0 = (h'_n g^{n-1} + ... + h'_1)g + h'_0$$

По теореме о делении с остатком, частное и остаток определены однозначно $\Rightarrow$ неполные частные тоже равны $\Rightarrow$ по индукционному предположению $h_i = h'_i \ \forall i$ ■

Теорема 5.10.2 (Формула Тейлора)**.** $\operatorname{char} K = 0, f \in K[x], c \in K \Rightarrow$

$$\Rightarrow f = \sum_{k=0}^{n} \frac{f^{(k)}(c)}{k!}(x-c)^k$$

Доказательство. $g = x - c \Rightarrow f = r_n(x-c)^n + r_{n-1}(x-c)^{n-1} + ... + r_1(x-c) + r_0$. Т.к. $\deg r_i < \deg g = 1 \Rightarrow r_i \in K$
$x = c \ f(c) = r_0, f^{(k)}(c) = k! \cdot r_k \Rightarrow r_k = \frac{f^{(k)}(c)}{k!}$ ■

5.11. Интерполяция

f – функция. $x_0, ..., x_n \ f(x_i) = y_i$ – известно. Картинка: TODO.

Задача: $\begin{array}{c|c|c|c} x_0 & x_1 & ... & x_n \\ \hline y_0 & y_1 & ... & y_n \end{array}$ – узлы интерполяции. Требуется найти $P_n \in K[x] : P_n(x_i) = y_i, i = 0, ..., n$.

Def 5.11.1. $\omega(x) = \prod_{i=0}^{n}(x - x_i)$

$$\omega'(x_i) = (x_i - x_0)...(x_i - x_{i-1})(x_i - x_{i+1})...(x_i - x_n)$$

Теорема 5.11.2 (Интерполяционный многочлен Лагранжа)**.**

$$P_n(x) = \sum_{i=0}^{n} \frac{\omega(x)}{(x-x_i)\omega'(x_i)} y_i$$

– искомый многочлен.

Доказательство.

$$\frac{\omega(x)}{(x-x_i)(\omega'(x_i))} \Rightarrow P_n(x_i) = 0 + ... + 0 + 1 \cdot y_i + 0 + ... + 0 = y_i$$

■

Теорема 5.11.3 (Интерполяционный многочлен Ньютона)**.** $\begin{array}{c|c|c|c} x_0 & x_1 & ... & x_n \\ \hline y_0 & y_1 & ... & y_n \end{array}$ – узлы.

$$P_n(x) = a_0 + a_1(x-x_0) + a_2(x-x_0)(x-x_1) + ... + a_n(x-x_0)...(x-x_{n-1})$$

$x = x_0$ $P_n(x_0) = a_0 = y_0$
$x = x_1$ $P_n(x_1) = y_1 = y_0 + a_1(x_1 - x_0) \Rightarrow a_1$ и т.д.

5.12. Поле частных (поле отношений)

$\mathbb{Z} \to \mathbb{Q} = \left\{\frac{p}{q}, q \neq 0, p, q \in \mathbb{Z}\right\}$

Def 5.12.1. *R – область целостности. $Q(R) = \{(a,b), a, b \in R, b \neq 0\}$:*

1. $(a,b) = (c,d) \Leftrightarrow ad = bc$
2. $(a,b) + (c,d) = (ad + bc, bd)$
3. $(a,b) \cdot (c,d) = (a \cdot c, b \cdot d)$
4. $\forall a \in R$ $a = (a, 1)$

Корректность: 1 и 4, 2 и 4, 3 и 4 согласованы.

Теорема 5.12.2. $Q(R)$ – поле.

Def 5.12.3. *Поле $Q(R)$ называется поле частных кольца R.*

5.12.1. Поле дробно-рациональных функций

$R = K[x] \to Q(K[x]) = \left\{\frac{f}{g}, f, g \in K[x], g \neq 0\right\}$
$K(x)$ – поле дробно-рациональных функций над K.
Замечание 5.12.4. В $K(x)$ $\frac{x^2-1}{x+1} = x - 1$

Def 5.12.5. $\frac{f}{g}$ *– степенью этой дроби называется* $\deg f - \deg g$

Def 5.12.6. $\frac{f}{g}$ *– **правильная** , если* $\deg f < \deg g$*, иначе* $\frac{f}{g}$ *– **неправильная**.*

Def 5.12.7. $\frac{f}{\varphi^k}$, *где* φ *– неприводим,* $\deg f < \deg\varphi$, *называется простейшей.*

Теорема 5.12.8 (Выделение целой части)**.** $\frac{f}{g}$ – неправильная дробь

$$\Rightarrow \frac{f}{g} = h + \frac{r}{g}$$

где $\frac{r}{g}$ – правильная дробь и это представление единственно.

Доказательство. $f = h \cdot g + r, \deg r < \deg g$

$$\Rightarrow \frac{f}{g} = \frac{hg + r}{g} = h + \frac{r}{g}$$

Если $\frac{f}{g} = h_1 + \frac{r_1}{g} \Leftrightarrow \frac{f}{g} = \frac{h_1 g + r_1}{g} \Rightarrow f = h_1 g + r_1$ – однозначно определено. ■

Lm 5.12.9. $(f, g) = 1 \Rightarrow \frac{h}{fg} = \frac{h_1}{f} + \frac{h_2}{g}$

Доказательство. $(f, g) = 1 \Rightarrow \exists h_1', h_2' : h_1' g + h_2' f = 1$

$$\Rightarrow hh_1' g + hh_2' f = h \Rightarrow \frac{h}{fg} = \frac{hh_1' g + hh_2' f}{fg} = \frac{hh_1'}{f} + \frac{hh_2'}{g}$$

■

Теорема 5.12.10 (Разложение дроби на простейшие)**.** Любая правильная дробно-рациональная функция может быть разложена единственным образом на простейшие.

Доказательство. $\frac{f}{g}$ – правильная дробь. $g = \varphi_1^{k_1}\varphi_2^{k_2}...\varphi_s^{k_s}$ – каноническое разложение, $(\varphi_i, \varphi_j) = 1, i \neq j$. Тогда

$$\frac{f}{\varphi_1^{k_1}...\varphi_s^{k_s}} = \frac{f_1}{\varphi_1^{k_1}} + ... + \frac{f_s}{\varphi_s^{k_s}}$$

Докажем, что все дроби $\frac{f_i}{\varphi_i^{k_i}}$ – правильные. Если есть неправильные дроби $\Rightarrow$ выделим целую часть

$$\Rightarrow \frac{f}{g} = h + \underbrace{\frac{f_1'}{\varphi_1^{k_1}} + ... + \frac{f_s'}{\varphi_s^{k_s}}}_{\text{правильные дроби}} \Rightarrow h = 0$$

Рассмотрим правильную дробь $\frac{f_i}{\varphi_i^{k_i}}, \deg f_i < \deg \varphi_i^{k_i}$.

$$f_i = h_n\varphi_i^n + h_{n-1}\varphi_i^{n-1} + ... + h_1\varphi_i + h_0, \deg h_s < \deg\varphi_i \Rightarrow n \leqslant k_i$$

$$\frac{f_i}{\varphi_i^{k_i}} = \frac{h_{k_i}\varphi_i^{k_i} + h_{k_i-1}\varphi_i^{k_i-1} + ... + h_0}{\varphi_i^{k_i}}$$

$\Rightarrow \exists$ разложение доказано. Единственность без доказательства. ■

5.13. Разложение рациональной дроби над $\mathbb{R}$

$\frac{f}{\varphi^k}, \deg f < \deg \varphi$
$\frac{a}{(x-m)^k}, \frac{bx+c}{(x^2+px+q)^k}, p^2 - 4q < 0$

Пример 5.13.1.

$$\frac{x^4+5x^3+6x^2+7x-8}{(x-2)^3(x^2+x+1)^2(x+4)^2} = \frac{a_1}{x-2}+\frac{a_2}{(x-2)^2}+\frac{a_3}{(x-2)^3}+\frac{b_1x+c_1}{x^2+x+1}+\frac{b_2x+c_2}{(x_2+x+1)^2}+\frac{d_1}{x+4}+\frac{d_2}{(x+4)^2}$$

5.14. Формальный степенной ряд

R – коммутативное кольцо с 1.

Def 5.14.1.

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1x + a_2x^2 + ... + a_nx^n + ...$$

$a_n \in R$, называется формальным степенным рядом.

1. Сложение.

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{m=0}^{\infty} b_m x^m = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

2. Умножение.

$$\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{m=0}^{\infty} b_m x^m\right) = \sum_{k=0}^{\infty}\left(\sum_{n+m=k}^{a_nb_m} x^k\right)$$

Множество $R[[x]] = \{\sum_{n=0}^{\infty} a_nx^n, a_n \in R\}$ образует коммутативное кольцо с 1.

5.15. Многочлены от нескольких переменных

R – коммутативное кольцо с 1. $S = R[x_1], S[x_2] = R[x_1, x_2]$ и т.д.
$R[x_1, x_2, ..., x_n]$ – кольцо многочленов от переменных $x_1, x_2, ..., x_n$ над R.

$$R[x_1, ..., x_n] = \left\{\sum_{i_1,...i_n=0} a_{i_1,...,i_n} x_1^{i_1} x_2^{i_2} ... x_n^{i_n}\right\}$$

Def 5.15.1. *Мономом называется многочлен, у которого только один ненулевой коэффициент. $a_{i_1,...,i_n} x_1^{i_1} ... x_n^{i_n}, i_1 + i_2 + ... + i_n$ – степень монома.*

Def 5.15.2. *Многочлен от n переменных называется однородным, если он равен сумме мономов степени m.*

Def 5.15.3. *Элементарными симметрическими многочленами порядка k называются*
$\sigma_1(x_1, ..., x_n) = x_1 + ... + x_n$
$\sigma_2(x_1, ..., x_n) = \sum_{1 \leqslant i < j \leqslant n} x_i x_j$
$\sigma_k(x_1, ..., x_n) = \sum_{1 \leqslant i_1 < i_2 < ... < i_k \leqslant n} x_{i_1} ... x_{i_k}$

Теорема 5.15.4 (Теорема Виета)**.** $f = a_nx^n + a_{n-1}x^{n-1} + ... + a_0$, имеющий n корней.

$$\Rightarrow \sigma_k(x_1, ..., x_n) = (-1)^k \frac{a_{n-k}}{a_n}$$

Раздел #6: Линейная алгебра

6.1. Матрицы

Def 6.1.1. *Матрицей называется таблица размера $m \times n$ элементов.*

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

$A = (a_{ij}), 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n, a_{ij} \in K, K$ – *поле*

Виды матриц:

1. Матрица 1×1
2. Матрица $1 \times n \Rightarrow (a_1, ..., a_n)$ – строка
3. Матрица $m \times 1 \Rightarrow \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ – столбец
4. Нулевая матрицы $0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$
5. Квадратная матрица: $m = n$

6.1.1. Действия над матрицами

1. Сложение. $A = (a_{ij}) - m \times n, B = (b_{ij}) - m \times n$

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & ... & a_{1n} + b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & ... & a_{mn} + b_{mn} \end{pmatrix}$$

2. Умножение на элемент поля K, $c \in K, A = (a_{ij}) - m \times n$

$$c \cdot A = \begin{pmatrix} c \cdot a_{11} & c \cdot a_{12} & \cdots & c \cdot a_{1n} \\ c \cdot a_{21} & c \cdot a_{22} & \cdots & c \cdot a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c \cdot a_{m1} & c \cdot a_{m2} & \cdots & c \cdot a_{mn} \end{pmatrix}$$

Свойства:

1. Ассоциативность сложения.
$$(A+B)+C = A+(B+C)$$
2. Коммутативность сложения.
$$A+B = B+A$$
3. Нейтральный элемент.
$$A+0 = A$$
4. Существование противоположной матрицы.
$$A+(-1)\cdot A = 0$$

Замечание 6.1.2. $M(m,n,K)$ – множество матриц размера $m\times n$ над полем K. $M(m,n,K)$ – коммутативная группа по сложению.

5. $c_1, c_2 \in K$. Дистрибутивность.
$$(c_1+c_2)\cdot A = c_1A + c_2A$$
6. Дистрибутивность относительно сложения матриц.
$$c(A+B) = cA + cB$$
7. $c_1, c_2 \in K$
$$c_1(c_2A) = (c_1c_2)A$$
8. $1\cdot A = A$

6.1.2. Умножение матриц

Def 6.1.3. $B = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \end{pmatrix}, A = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$
$$B\cdot A = b_1a_1 + b_2a_2 + ... + b_na_n$$

Def 6.1.4 (Умножение матриц)**.** $A - m\times k, B - k\times n$. *Тогда определено произведение* $A\cdot B = C$ *–* $m\times n$ *.*
$$C = (c_{ij}), 1\leqslant i\leqslant m, 1\leqslant j\leqslant n, c_{ij} = A_i\cdot B^j = a_{i1}b_{1j} + a_{i2}b_{2j} + ... + a_{ik}b_{kj}$$
A_i *–* i*-я строка* A*,* B^j *–* j*-й столбец* B*.*

Замечание 6.1.5. 1. Если определено $A\cdot B$, то $B\cdot A$ может быть не определено.

2. Если $A\cdot B$ и $B\cdot A$ определены: как правило $AB\neq BA$.

3. Строка $\cdot$ столбец $\in K$.

4. $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}\cdot\begin{pmatrix} b_1 & b_2 & \cdots & b_n \end{pmatrix} = \begin{pmatrix} a_1b_1 & a_1b_2 & \cdots & a_1b_n \\ a_2b_1 & a_2b_2 & \cdots & a_2b_n \\ \vdots & \vdots & \ddots & \vdots \\ a_nb_1 & a_nb_2 & \cdots & a_nb_n \end{pmatrix}$

5. $B = \begin{pmatrix} B^1 & B^2 & \cdots & B^n \end{pmatrix}, B^j$ – столбцы.
$$A \cdot B = \begin{pmatrix} AB^1 & AB^2 & \cdots & AB^n \end{pmatrix}$$
6. $M(n, n, K) = M(n, K)$ – квадратные матрицы порядка n. $E = E_n \in M(n, K)$ – единичная матрица.
$$E = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Свойства:

1. $c \in K, A, B$
$$(cA)B = c(AB)$$
2. $(A + B)C = AC + BC$
3. $A(B + C) = AB + AC$
4. $(AB)C = A(BC)$

   Доказательство. Если $(AB)C$ – определено, то $A(BC)$ – определено. $A - m \times k, B - k \times l \Rightarrow AB$ – определено, $m \times l$. $(AB)C$ – определено $\Rightarrow C - l \times n \Rightarrow (AB)C - m \times n$.
   $BC - (k \times l) \cdot (l \times n) = (k \times n)$. $A(BC) - (m \times k) \cdot (k \times n) = (m \times n)$. $C = \begin{pmatrix} C^1 & C^2 & \cdots & C^n \end{pmatrix}$ – столбцы. Тогда $A(BC) = A\begin{pmatrix} BC^1 & BC^2 & \cdots & BC^n \end{pmatrix} = \begin{pmatrix} ABC^1 & ABC^2 & \cdots & ABC^n \end{pmatrix}$
   $(AB)C = (AB)\begin{pmatrix} C^1 & C^2 & \cdots & C^n \end{pmatrix} = \begin{pmatrix} ABC^1 & ABC^2 & \cdots & ABC^n \end{pmatrix}$ ■

Теорема 6.1.6. $M(n, K)$ – кольцо с 1.

6.1.3. Транспонирование

Def 6.1.7. $A = (a_{ij}) - m \times n$.
$$A^T = (a_{ji}), 1 \leqslant j \leqslant n, 1 \leqslant i \leqslant m$$
называется транспонированной. Замена в матрице A строк на столбцы называется транспонированием.

Свойства:

1. $(A^T)^T = A$
2. $(A + B)^T = A^T + B^T$
3. $c \in K, (cA)^T = cA^T$
4. $(AB)^T = B^T \cdot A^T$

   Доказательство. $A - m \times k, B - k \times n \Rightarrow (AB)^T - n \times m$. $B^T - n \times k, A^T - k \times m \Rightarrow B^T A^T - n \times m$.
   $A = (a_{ij}), 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant k$. $B = (b_{ij}), 1 \leqslant i \leqslant k, 1 \leqslant j \leqslant n$.

$A^T = C = (c_{ij}), 1 \leqslant i \leqslant k, 1 \leqslant j \leqslant m.$
$B^T = D = (d_{ij}), 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant k.$

$$AB = F = (f_{ij}), f_{ij} = \sum_{s=1}^{k} a_{is} b_{sj}$$

$$B^T A^T = G = (g_{ij}), g_{ij} = \sum_{t=1}^{k} d_{it} c_{tj}$$

$$g_{ij} = \sum_{t=1}^{k} d_{it} c_{tj} = \sum_{t=1}^{k} b_{ti} a_{jt} = \sum_{t=1}^{k} a_{jt} b_{ti} = f_{ji}$$

$\blacksquare$

6.2. Теория определителей

Рассмотрим систему из двух линейных уравнений с двумя неизвестными.

$$\begin{cases} a_{11}x + a_{12}y = b_1 \\ a_{21}x + a_{22}y = b_2 \end{cases} \Leftrightarrow \begin{cases} -a_{11}a_{21}x - a_{21}a_{12} = -a_{21}b_1 \\ a_{11}a_{21}x + a_{11}a_{22}y = a_{11}b_2 \Rightarrow \end{cases}$$

$$\Rightarrow (a_{11}a_{22} - a_{12}a_{21})y = a_{11}b_2 - a_{21}b_1 \Rightarrow \begin{cases} y = \frac{a_{11}b_2 - a_{21}b_1}{a_{11}a_{22} - a_{12}a_{21}} \\ x = \frac{b_1 a_{22} - b_2 a_{12}}{a_{11}a_{22} - a_{12}a_{21}} \end{cases}$$

$$\Delta = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12}, \Delta_1 = \begin{vmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{vmatrix}, \Delta_2 = \begin{vmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{vmatrix}$$

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

6.2.1. Определение определителя

Квадратная матрица $n \times n$ – матрица порядка n.

Def 6.2.1. *Определителем матрицы порядка n называется*

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \sum_{(i_1, i_2, \ldots, i_n)} \pm a_{1i_1} a_{2i_2} \ldots a_{ni_n} = \sum \varepsilon_\sigma a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)} =$$

где ε_σ – знак перестановки. $\varepsilon = (-1)^{\operatorname{inv}(i_1, i_2, \ldots, i_n)}$

$$= \sum_{(i_1, i_2, \ldots, i_n) \in S_n} (-1)^{\operatorname{inv}(i_1, i_2, \ldots, i_n)} a_{1i_1} a_{2i_2} \ldots a_{ni_n}$$

6.2.2. Свойства определителя

1. Знак $(a_{i_1j_1} \cdot a_{i_2j_2} \cdot ... \cdot a_{i_nj_n}) = (-1)^{\mathrm{inv}(i_1,i_2,...,i_n)+\mathrm{inv}(j_1,j_2,...,j_n)}$

   Доказательство. $a_{i_1j_1}a_{i_2j_2}...a_{i_nj_n} \to a_{1j'_1}a_{2j'_2}...a_{nj'_n}$. $(i_1,...,i_n),(j_1,...,j_n)$ совершали 2 транспозиции $\Rightarrow \mathrm{inv}(i_1,...,i_n)+\mathrm{inv}(j_1,...,j_n)$ – четность осталась та же самая

   $$\Rightarrow (-1)^{\mathrm{inv}(i_1,...,i_n)+\mathrm{inv}(j_1,...,j_n)} = (-1)^{\mathrm{inv}(1,...,n)+\mathrm{inv}(j'_1,...,j'_n)} = (-1)^{\mathrm{inv}(j'_1,...,j'_n)}$$

   ■

2. $\det A = \det A^T$

   Доказательство. $\det A = \sum \pm a_{1i_1}...a_{ni_n}$. В $\det A^T$ слагаемые без учета знака будут одинаковые.

   $$(-1)^{\mathrm{inv}(1,...,n)+\mathrm{inv}(j'_1,...,j'_n)} = (-1)^{\mathrm{inv}(i'_1,...,i'_n)+\mathrm{inv}(1,...,n)} = (-1)^{\mathrm{inv}(i_1,...,i_n)+\mathrm{inv}(j_1,...,j_n)}$$

   ■

3. $A = \begin{pmatrix} A_1 & \cdots & A_n \end{pmatrix}$, A_i – строки $1 \leqslant i \leqslant n$.
   $\begin{pmatrix} A_1 \\ \vdots \\ A_n \end{pmatrix}$, $A = \begin{pmatrix} A^1 & \cdots & A^n \end{pmatrix}$, A^j – столбцы, $1 \leqslant j \leqslant n$.

   Замечание 6.2.2. Все свойства, которые верны для строк матрицы, будут верны и для столбцов.

   $$\det(A_1,...,A'_i+A''_i,...,A_n) = \det(A_1,...,A'_i,...,A_n) + \det(A_1,...,A''_i,...,A_n)$$
   $$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ b_1+c_1 & b_2+c_2 & b_3+c_3 \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ b_1 & b_2 & b_3 \\ a_{31} & a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ c_1 & c_2 & c_3 \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

   Доказательство. $\det A = \sum_\sigma \varepsilon_\sigma a_{1\sigma(1)}...(a'_{i\sigma(i)} + a''_{i\sigma(i)})...a_{n\sigma(n)} = \sum \varepsilon_\sigma a_{1\sigma(1)}...a'_{i\sigma(i)}...a_{n\sigma(n)} + \sum \varepsilon_\sigma a_{1\sigma(i)}...a''_{i\sigma(i)}...a_{n\sigma(n)} =$

   $$= \det(A_1,...,A'_i,...,A_n) + \det(A_1,...,A''_i,...,A_n)$$

   ■

4. $\det(A_1,...,\lambda A_i,...,A_n) = \lambda\det(A_1,...,A_n)$
5. $\det(A_1,...,\underbrace{A_i}_{i},...,\underbrace{A_i}_{j},...,A_n) = 0$

Доказательство.

$$\det A = \begin{array}{c} i \\ \\ j \end{array}\begin{vmatrix} a_{i1} & \cdots & a_{in} \\ \vdots & \ddots & \vdots \\ a_{j1} & \cdots & a_{jn} \end{vmatrix} = \sum_{\sigma \text{ -- чет.}} a_{1\sigma(1)}...a_{n\sigma(n)} - \sum_{\sigma \text{ -- неч.}} a_{1\sigma(1)}...a_{n\sigma(n)}$$

Все нечетные перестановки получаются из четных, если сделать одну транспозицию $\Rightarrow$ сделав транспозицию $(ij) \Rightarrow$ из четной получим нечетную. ■

6.
$$\det(A_1, ..., A_i, ..., A_j, ...A_n) = -\det(A_1, ..., A_j, ..., A_i, ..., A_n)$$

Доказательство. $0 = \det(A_1, ..., \underbrace{A_i + A_j}_{i}, ..., \underbrace{A_i + A_j}_{j}, ..., A_n) = \det(A_1, ..., A_i, ...A_i, ..., A_n) + \det(A_1, ..., A_i, ..., A_j, ..., A_n) + \det(A_1, ..., A_j, ..., A_i, ..., A_n) + \det(A_1, ..., A_j, ..., A_j, ..., A_n)$

$$\Rightarrow \det(A_1, ..., A_i, ..., A_j, ..., A_n) = \det(A_1, ..., A_j, ..., A_i, ..., A_n) = 0$$

■

7. Определитель с двумя пропорциональными строками равен нулю.

$$\det(A_1, ..., A_n) = 0 \Leftarrow A_i = \lambda A_j, 1 \leqslant i \neq j \leqslant n$$

8. Определитель не изменится, если к одной строке прибавить другую, умноженную на λ.

$$\det(A_1, ..., A_n) = \det(A_1, ..., A_i + \lambda A_j, ..., A_n)$$

Доказательство.

$$\det(A_1, ..., A_i+\lambda A_j, ..., A_j, ..., A_n) = \det(A_1, ..., A_i, ...A_j, ...A_n) + \underbrace{\det(A_1, ..., \lambda A_j, ..., A_j, ..., A_n)}_{0} = \det A$$

■

6.2.3. Алгебраические дополнения и миноры

Def 6.2.3. *Определитель матрицы, полученной вычеркиванием из матрицы A k строк и k столбцов, называется минором $(n-k)$-го порядка.*

Def 6.2.4. *Минор $(n-1)$-го порядка называется главным.*

$$\Delta_{ij} = \begin{array}{c} \\ i \\ \\ \\ \end{array}\begin{vmatrix} a_{11} & & \vdots & a_{1n} \\ \cdots & \cdots & \vdots & \cdots \\ & & \vdots & \\ a_{n1} & & \vdots & a_{nn} \\ & & j & \end{vmatrix}$$

Def 6.2.5. $A_{ij} = (-1)^{i+j}\Delta_{ij}$ – *алгебраическое дополнение к* a_{ij}

Lm 6.2.6. 1. $\begin{vmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = a_{11}A_{11}$

2. $\begin{vmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{in} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & a_{ij} & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{vmatrix} = a_{ij}A_{ij}$

Доказательство. 1. $\det A = \sum_{\sigma(i)\neq 1} \varepsilon_\sigma a_{11}a_{2\sigma(2)}...a_{n\sigma(n)} = a_{11}\Delta_{11} = a_{11}A_{11}$

2. $\begin{vmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & a_{ij} & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{vmatrix} = \varepsilon \cdot \begin{vmatrix} a_{ij} & 0 & \cdots & 0 \\ a_{1j} & a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{nj} & a_{n1} & \cdots & a_{nn} \end{vmatrix} = \varepsilon \cdot a_{ij} \cdot \Delta_{ij} = (-1)^{i+j}a_{ij}\Delta_{ij} = a_{ij}A_{ij}$

■

Теорема 6.2.7 (Разложение определителя по строке)**.** $\forall i, 1 \leqslant i \leqslant n$

$$\det A = a_{i1}A_{i1} + ... + a_{in}A_{in}$$

Доказательство.

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{i1} & 0 & \cdots & 0 \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{i2} & \cdots & 0 \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \cdots + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & 0 & \cdots & a_{in} \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} =$$

$$= a_{i1}A_{i1} + a_{i2}A_{i2} + ... + a_{in}A_{in}$$

■

Следствие 6.2.8. $a_{i1}A_{j1} + ... + a_{in}A_{jn} = 0, i \neq j$

Доказательство.

$$x_1A_{j1} + ... + x_nA_{jn} = \begin{array}{c} i \\ \\ j \end{array} \begin{vmatrix} a_{i1} & \cdots & a_{in} \\ \vdots & \ddots & \vdots \\ x_1 & \cdots & x_n \end{vmatrix} = 0$$

■

Пример 6.2.9 (Определитель Вондермонда)**.**

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{1\leqslant j<i\leqslant n}(x_i - x_j)$$

Доказательство. Докажем по индукции.
$n = 2: \begin{vmatrix} 1 & x_1 \\ 1 & x_2 \end{vmatrix} = x_2 - x_1.$
Индукционный переход: домножаем k-й столбец на x_1 и вычитаем его из $(k+1)$-го столбца, $k = n-1, ..., 1$.

$$\begin{vmatrix} 1 & x_1 & \cdots & x_1^{n-2} & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-2} & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_n & \cdots & x_n^{n-2} & x_n^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & x_1 & \cdots & x_1^{n-2} & 0 \\ 1 & x_2 & \cdots & x_2^{n-2} & x_2^{n-1} - x_1 \cdot x_2^{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_n & \cdots & x_n^{n-2} & x_n^{n-1} - x_1 \cdot x_n^{n-2} \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & x_2 - x_1 & x_2^2 - x_2x_1 & \cdots & x_2^{n-1} - x_2^{n-2}x_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n - x_1 & x_n^2 - x_nx_1 & \cdots & x_n^{n-1} - x_n^{n-2}x_1 \end{vmatrix} = a_{11}A_{11} =$$

$$= (x_2 - x_1)(x_3 - x_1)...(x_n - x_1) \cdot \begin{vmatrix} 1 & x_2 & \cdots & x_2^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{n-2} \end{vmatrix}$$

■

6.2.4. Геометрическая интерпретация

$A_1, ..., A_n$ – векторы в пространстве $\mathbb{R}^n$ (строки). $A = (A_1, ..., A_n)$
$\Pi = \{\alpha_1 A_1 + ... + \alpha_n A_n, 0 \leqslant \alpha_i \leqslant 1, 1 \leqslant i \leqslant n\}$ – n-мерный параллелепипед.

$$|\det(A)| = V(\Pi)$$

6.2.5. Определитель ступенчатой матрицы

Def 6.2.10. *Матрица вида*

$$M = \begin{pmatrix} A & O \\ B & C \end{pmatrix} - n \times n,$$

где $A - k \times k, C - (n-k) \times (n-k), B - (n-k) \times k, O$ *– нулевая матрица* $k \times (n-k)$ *, называется* ***ступенчатой***

Теорема 6.2.11 (Определитель ступенчатой матрицы)**.**

$$\det M = \det A \cdot \det C$$

Доказательство. Индукция по k. $k = 1$

$$\begin{vmatrix} a_{11} & 0, ..., 0 \\ B & C \end{vmatrix} = a_{11} \cdot \det C$$

Выполним индукционный переход: $k - 1 \mapsto k$.

$$\det M = a_{11} \cdot M_{11} + a_{12} \cdot M_{12} + ... + a_{1k} \cdot M_{1k}$$

По индукционному предположению, $M_{1j} = A_{1j} \cdot \det C \Rightarrow \det M = (a_{11} \cdot A_{11} + ... + a_{1k} \cdot A_{1k}) \cdot \det C = \det A \cdot \det C$. ■

Следствие 6.2.12 (Определитель произведения матриц).

$$\det(AB) = \det A \cdot \det B$$

Доказательство.

$$M = \begin{pmatrix} A & O \\ -E & B \end{pmatrix} - 2n \times 2n$$

По теореме $\det M = \det A \cdot \det B$. С другой стороны:

$$\begin{vmatrix} A & O \\ -E & B \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1n} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} & 0 & \cdots & 0 \\ -1 & \cdots & 0 & b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & -1 & b_{n1} & \cdots & b_{nn} \end{vmatrix} = \begin{vmatrix} A & C \\ -E & O \end{vmatrix} =$$

$c_{11} = a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} + ... + a_{1n}b_{n1} \Rightarrow c_{ij} = a_{i1}b_{1j} + ... + a_{in}b_{nj} \Rightarrow C = AB$

$$= \begin{vmatrix} -E & O \\ A & C \end{vmatrix} = (-1)^n \det(-E) \det C = (-1)^n \cdot (-1)^n \cdot \det C = \det C \Rightarrow \det C = \det A \det B$$

■

6.2.6. Обратная матрица

Def 6.2.13. *Для матрицы $A - n \times n$ матрица B называется обратной, если $A \cdot B = B \cdot A = E_n$*

Def 6.2.14. $\widetilde{A} = (A_{ij})^T$ *– взаимная матрица к A.*

Теорема 6.2.15 (Об обратной матрице)**.**

$$\exists!\ A^{-1}, A^{-1} = \frac{1}{\det A} \cdot \widetilde{A} \Leftrightarrow \det A \neq 0$$

Доказательство. “$\Rightarrow$”. $A \cdot A^{-1} = E \Rightarrow \det(A \cdot A^{-1}) = \det A \cdot \det A^{-1} = 1 \Rightarrow \det A \neq 0$.
“$\Leftarrow$”.

$$A \cdot \widetilde{A} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & & \end{pmatrix} \begin{pmatrix} A_{11} \\ \vdots \\ A_{1n} \end{pmatrix} = \begin{pmatrix} \det A & 0 & \dots & 0 \\ 0 & \det A & \dots & 0 \\ 0 & 0 & \dots & \det A \end{pmatrix} \Rightarrow A \cdot A^{-1} = E$$

Единственность. Пусть B_1, B_2 – обратные матрицы к A.

$$B_1 = B_1 \cdot A \cdot B_2 = B_2$$

■

Свойства обратной матрицы:

1. $(A^{-1})^{-1} = A$
2. $(AB)^{-1} = B^{-1}A^{-1}$
3. $\det A^{-1} = (\det A)^{-1}$
4. $(A^T)^{-1} = (A^{-1})^T$

Доказательство. 1. $A^{-1} \cdot A = E$

2. $AB \cdot B^{-1} \cdot A^{-1} = E \Rightarrow (AB)^{-1} = B^{-1}A^{-1}$

3. $\det(AA^{-1}) = \det A \cdot \det A^{-1} = \det E \Leftrightarrow \det A^{-1} = (\det A)^{-1}$

4. $A \cdot A^{-1} = E \Rightarrow (A \cdot A^{-1})^T = E^T \Rightarrow (A^{-1})^T A^T = E$

■

6.2.7. Формулы Крамера

Система линейных уравнений $n \times n$:

$$(*) = \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{n1}x_1 + \dots + a_{nn}x_n = b_n \end{cases}$$

$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$ – матрица коэффициентов, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ – столбец свободных членов, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ – столбец неизвестных. Тогда в матричном виде СЛУ : $Ax = b$.

Теорема 6.2.16 (Формула Крамера)**.** Если $\det A \neq 0 \Rightarrow$ решение $(*)$ $\exists!$ и

$$x_i = \frac{\Delta_i}{\Delta}, \Delta = \det A, \Delta_i = \begin{vmatrix} a_{11} & \cdots & b_1 & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & b_n & \cdots & a_{nn} \end{vmatrix}$$

Доказательство. $Ax = b \Rightarrow A^{-1} \cdot Ax = A^{-1}b \Rightarrow x = A^{-1}b$

$$\Rightarrow \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \frac{1}{\Delta} \cdot \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \frac{1}{\Delta}(A_{1i}b_1 + A_{2i}b_2 + ... + A_{ni}b_n) = \begin{pmatrix} \frac{\Delta_1}{\Delta} \\ \vdots \\ \frac{\Delta_n}{\Delta} \end{pmatrix}$$

■

6.3. Векторные пространства

Def 6.3.1. *Векторным (линейным) пространством над полем K называется множество V элементов, называемых векторами, на котором определены две операции:*

1. $\forall x, y \in V \to x + y \in V$ *(сумма векторов)*
2. $\forall \alpha \in K, \forall x \in V \ \alpha x \in V$ *(умножение вектора на элемент поля)*

которые подчиняются следующим аксиомам:

1. $x + y = y + x$
2. $(x + y) + z = x + (y + z)$
3. $\exists 0 \in V : x + 0 = x \ \forall x \in V$
4. $\forall x \in V \ \exists(-x) \in V : x + (-x) = 0$
5. $1 \cdot x = x \ \forall x \in V$ *(унитарность)*
6. $(\alpha\beta)x = \alpha(\beta x), \forall \alpha, \beta \in K, \forall x \in V$
7. $(\alpha + \beta)x = \alpha x + \beta x$
8. $\alpha(x + y) = \alpha x + \alpha y$

Замечание 6.3.2. 1. V – коммутативная группа по сложению векторов

2. $\alpha \in K, x \in V, \alpha x$, слева из K, справа из V.

3. $+$ и $\cdot$ условны.

4. Разность $x - y = x + (-y)$

Следствие 6.3.3. 1. $0 \cdot x = 0$ ($0 \cdot \overline{x} = \overline{0}$) $\forall x \in V$

Доказательство. $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x \Rightarrow 0 = 0 \cdot x$ ■

2. $\alpha \cdot 0 = 0 \ \forall \alpha \in K$

Доказательство. $\alpha \cdot 0 = \alpha(0 + 0) = \alpha \cdot 0 + \alpha \cdot 0 \Rightarrow \alpha \cdot 0 = 0$ ■

3. $\alpha x = 0 \Rightarrow \alpha = 0 \vee x = 0$

Доказательство. $\alpha \neq 0 \Rightarrow \exists \alpha^{-1} \Rightarrow \alpha^{-1}(\alpha x) = \alpha^{-1} \cdot 0 \Rightarrow x = 0.$ ■

4. $(-1) \cdot x = -x$

Доказательство. $x+(-1)\cdot x = 1\cdot x+(-1)\cdot x = (1-1)\cdot x = 0 \Rightarrow$ по единственности обратного $\Rightarrow (-1)\cdot x = -x$ ■

Пример 6.3.4. 1. Пространство столбцов (координатное пространство)

$$K^n = \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \alpha_i \in K \right\}$$

– векторное пространство

2. Пространство строк

$$^nK = \{(\alpha_1, ..., \alpha_n), \alpha_i \in K\}$$

3. $M(m, n, K)$ – матрицы $m \times n$
4. E – векторы на плоскости или в пространстве ($\mathbb{R}^2, \mathbb{R}^3$)
5. $K[x]$ – пространство многочленов
6. $K[x]_n$ – пространство многочленов степени не выше n

Замечание 6.3.5. Множество многочленов степени n не образует векторного пространства.

6.3.1. Линейная зависимость

Def 6.3.6. $\alpha_1, .., \alpha_n \in K, v_1, ..., v_n \in V$. *Тогда*

$$\alpha_1 v_1 + ... + \alpha_n v_n \text{ – линейная комбинация } v_1, ..., v_n$$

Множество всех линейных комбинаций $v_1, ..., v_n$*:*

$$\langle v_1, ..., v_n \rangle = \{\alpha_1 v_1 + ... \alpha_n v_n, \alpha_i \in K, i = 1, ..., n\}$$

и называется ***линейной оболочкой*** *векторов* $v_1, ..., v_n$.

Def 6.3.7. *Говорят, что векторы* $v_1, ..., v_n$ *порождают векторное пространство* V*, если* $\langle v_1, ..., v_n \rangle = V$.

Def 6.3.8. *Пространство* V *называется конечномерным, если оно порождается конечным числом векторов. Иначе,* V *– бесконечномерное.*

Пример 6.3.9. 1. $\mathbb{R}^3 = \left\{ \alpha_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \alpha_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\} = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$

2. $K[x] = \langle 1, x, x^2, ..., \rangle$ – бесконечномерное пространство.

Def 6.3.10. *Множество векторов* $v_1, ..., v_n \in V$ *называется линейно независимым (ЛНЗ), если* $\alpha_1 v_1 + ... + \alpha_n v_n = 0 \Rightarrow \alpha_1 = \alpha_2 = ... = \alpha_n = 0$
Линейная комбинация $0 \cdot v_1 + ... + 0 \cdot v_n$ *называется тривиальной.*

Def 6.3.11. *Если* $\exists \alpha_1, ..., a_n \in K$*, не все равные 0, что* $\alpha_1 v_1 + ... + \alpha_n v_n = 0$*, то* $v_1, ..., v_n$ *называется линейно зависимым (ЛЗ).*

Пример 6.3.12. 1. $e_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}, e_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}, e_3 = \begin{pmatrix}0\\0\\1\end{pmatrix}$

$$\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 = \begin{pmatrix}0\\0\\0\end{pmatrix} = \begin{pmatrix}\alpha_1\\\alpha_2\\\alpha_3\end{pmatrix} \Leftrightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0$$

2.

$$1 \cdot \begin{pmatrix}1\\2\\3\end{pmatrix} + 1 \cdot \begin{pmatrix}2\\1\\0\end{pmatrix} - 3 \cdot \begin{pmatrix}1\\1\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix}$$

3. $K[x]_n, \{1, x, ..., x^n\}$ – ЛНЗ.

Теорема 6.3.13 (Свойства ЛЗ и ЛНЗ)**.** 1. $v_1, ..., v_n$ – ЛЗ $\Leftrightarrow$ $\exists i : v_i$ = линейная комбинация остальных.

2. Множество векторов, содержащее 0 – ЛЗ.

3. X, Y – множества векторов, $X \subset Y$. Если Y – ЛНЗ, то X – ЛНЗ. Если X – ЛЗ, то Y – ЛЗ.

Доказательство. 1. $\exists \alpha_i \neq 0, \alpha_1 v_1 + ... + \alpha_i v_i + ... + \alpha_n v_n = 0 \Rightarrow v_i$ выражается.

2. $1 \cdot 0 + 0 \cdot v_1 + ... + 0 \cdot v_n = 0$

3. самостоятельно.

■

Lm 6.3.14. $v_1, ..., v_n$ – ЛЗ, $v_1 \neq 0 \Rightarrow \exists i, 2 \leqslant i \leqslant n :$

1. $v_i \in \langle v_1, ..., v_{i-1} \rangle$

2. $\langle v_1, ..., v_n \rangle = \langle v_1, ..., \widehat{v}_i, ..., v_n \rangle$

Доказательство. 1. Рассмотрим $\alpha_1 v_1 + ... + \alpha_i v_i, i$ – наименьший индекс $i : v_1, ..., v_i$ – ЛЗ $\Rightarrow$ $\alpha_1 v_1 + ... + \alpha_i v_i = 0$. Если $\alpha_i = 0 \Rightarrow v_1, ..., v_{i-1}$ – ЛЗ $\Rightarrow a_i \neq 0 \Rightarrow v_i \in \langle v_1, ..., v_{i-1} \rangle$.

2. $\langle v_1, ..., \widehat{v}_i, ..., v_n \rangle = \langle v_1, ..., v_n \rangle \subseteq$.
Возьмем произвольный $u \in \langle v_1, ..., v_n \rangle = \beta_1 v_1 + ... + \beta_i v_i + ... + \beta_n v_n = \beta_1 v_1 + ... + \beta_i(\alpha'_1 v_1 + ... + \alpha'_{i-1} v_{i-1}) + ... + \beta_n v_n$.

■

Следствие 6.3.15. $v_1, ... v_n$ – ЛНЗ, $v \in V$. Тогда $v_1, ..., v_n, v$ – ЛЗ $\Leftrightarrow v \in \langle v_1, ..., v_n \rangle$

Теорема 6.3.16 (Количество ЛНЗ $\leqslant$ к-во порождающих)**.** V – конечномерное векторное пространство. Пусть $u_1, ..., u_m$ – ЛНЗ векторы, $V = \langle v_1, ..., v_n \rangle \Rightarrow m \leqslant n$

Доказательство. Если к $v_1, ..., v_n$ добавить $\forall u \in V$ – ЛЗ. Рассмотрим $u_1, v_1, ..., v_n$ – ЛЗ $\Rightarrow$ по лемме $\exists i : 1 \leqslant i \leqslant n : \langle u_1, v_1, ..., v_n \rangle = \langle u_1, v_1, ..., \widehat{v}_i, ..., v_n \rangle$ и далее: $\langle u_1, u_2, v_1, ..., \widehat{v}_i, ..., v_n \rangle \Rightarrow \exists j :$ можно убрать v_j и т.д. и получаем $\langle u_i, ..., \rangle = V$. Если $m > n \Rightarrow u_1, ..., u_n$ – порождает все $V \Rightarrow u_1, ..., u_n, u_{n+1}$ – ЛЗ – противоречие. ■

6.4. Базис и размерность

V – конечномерное векторное пространство над полем K.

Def 6.4.1. *Система векторов* $e_1, ..., e_n$ *называется базисом пространства* V *если выполняются:*

1. $\langle e_1, ..., e_n \rangle = V$
2. $e_1, ..., e_n$ – *ЛНЗ*

Теорема 6.4.2 (Существование базиса)**.** 1. Любая линейная оболочка обладает базисом.

2. Все базисы V состоят из одинакового количества векторов.
3. Разложение любого $v \in V$ по базису $v = \alpha_1 e_1 + ... + \alpha_n e_n$ единственно.

Доказательство. 1. $u_1, ..., u_k \in V$. $U = \langle u_1, ..., u_k \rangle$. Возьмем из $u_1, ..., u_k$ максимальное число ЛНЗ векторов $u_1, ..., u_s \Rightarrow u_1, ..., u_s, u_{s+1}$ – ЛЗ $\Rightarrow \langle u_1, ..., u_s \rangle = \langle u_1, ..., u_{s+1} \rangle \Rightarrow \langle u_1, ..., u_s \rangle = U$.

2. Пусть $e_1, ..., e_n$ – базис, $e'_1, ...e'_k$ – базис. $e_1, ..., e_n$ – ЛНЗ, $e'_1, ..., e'_k$ – порождающие векторы $\Rightarrow n \leqslant k$. Аналогично, $e'_1, ..., e'_k$ – ЛНЗ, $e_1, ..., e_n$ – порождающие $\Rightarrow k \leqslant n$.
3. $v = \alpha_1 e_1 + ... + \alpha_n e_n = \alpha'_1 e_1 + ... + \alpha'_n e_n \Rightarrow (\alpha_1 - \alpha'_1)e_1 + ... + (\alpha_n - \alpha'_n)e_n = 0$.

■

Def 6.4.3. *Коэффициенты* $(\alpha_1, ..., \alpha_n)$ *в разложении* $v = \alpha_1 e_1 + ...\alpha_n e_n$ *называются координатами вектора* v *в базисе* $e_1, ..., e_n$.

Def 6.4.4. *Количество векторов в базисе – размерность* V – $\dim V$.

Теорема 6.4.5 (Три равносильных определения базиса)**.** V – конечномерное векторное пространство над K

1. $e_1, ..., e_n$ – базис V
2. $e_1, ..., e_n$ – максимальный ЛНЗ набор векторов.
3. $e_1, ..., e_n$ минимальный порождающий набор векторов.

Доказательство. 1) $\Rightarrow$ 2). $e_1, ..., e_n, f \Rightarrow f$ выражается через $e_1, ..., e_n \Rightarrow e_1, ..., e_n, f$ – ЛЗ.
2) $\Rightarrow$ 1). $e_1, ..., e_n$ – максимальный $\Rightarrow \forall v \in V$ $e_1, ..., e_n, v$ – ЛЗ $\Rightarrow v \in \langle e_1, ..., e_n \rangle$.
1) $\Rightarrow$ 3). $\langle u_1, ..., u_k \rangle = V$. $e_1, ..., e_n$ – ЛНЗ, порождающие $\Rightarrow n \leqslant k \Rightarrow n$ – минимально.
3) $\Rightarrow$ 1). Если $e_1, ..., e_n$ – ЛЗ $\Rightarrow \exists i : \langle e_1, ..., e_n \rangle = \langle e_1, ..., \widehat{e_i}, ..., e_n \rangle$ – противоречие. ■

6.4.1. Подпространства

Def 6.4.6. $U \subset V$ *называется подпространством, если оно само является векторным пространством над* K.

Замечание 6.4.7. U – подпространство достаточно проверить $\forall v, u \in U, \forall \lambda \in K \Rightarrow v + u, \lambda u \in U$.

Lm 6.4.8. $U_1, U_2 \subset V$ – подпространства $\Rightarrow U_1 \cap U_2 \subset V$ – подпространство.

Доказательство. $x, y, \lambda x \in U_1 \cap U_2 \Rightarrow x + y \in U_1, x + y \in U_2 \Rightarrow x + y \in U_1 \cap U_2, \lambda x \in U_1, U_2$ ■

Замечание 6.4.9. 1. $\bigcap_{i \in I} U_i$ – подпространство

2. $U_1, U_2 \subset V$ – подпространства $\Rightarrow U_1 \cup U_2$ – необязательно подпространство.

Def 6.4.10. *Суммой подпространств называется* $U_1 + U_2 = \{u_1 + u_2, u_1 \in U_1, u_2 \in U_2\}$

Lm 6.4.11 (О дополнении до базиса)**.** Любой ЛНЗ набор векторов можно дополнить до базиса.

Доказательство. $e_1, ..., e_k$ – ЛНЗ, $\dim V = n, k < n$. $\langle e_1, ..., e_k\rangle \subset V \Rightarrow \exists v \in V : v \notin \langle e_1, ..., e_k\rangle \Rightarrow e_1, ..., e_k, v$ – ЛНЗ и т.д. ■

Теорема 6.4.12 (Размерность суммы подпространств)**.** $U, W \in V$ – подпространства.

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

Доказательство. $\dim(U \cap W) = m, \dim U = k, \dim W = l, e_1, ..., e_m$ – базис $U \cap W, U \cap W \subset U$. Дополним базис $e_1, ..., e_m$ до $U : u_1, ..., u_{k-m}$. $U \cap W \subset W$ $e_1, ..., e_m, w_1, ..., w_{l-m}$ – базис W. Докажем, что $e_1, ..., e_m, u_1, ..., u_{k-m}, w_1, ..., w_{l-m}$ – базис $U + W$. $\langle e_1, ..., e_m, u_1, ..., u_{k-m}, w_1, ..., w_{l-m}\rangle = U + W \Rightarrow$ надо доказать ЛНЗ. Предположим, что набор ЛЗ:

$$\sum_{i=1}^{m} \alpha_i e_i + \sum_{j=1}^{k-m} \beta_j u_j + \sum_{t=1}^{l-m} \gamma_t w_t = 0 \Rightarrow \underbrace{-\sum_{t=1}^{l-m} \gamma_t w_t}_{\in W} = \underbrace{\sum_{i=1}^{m} \alpha_i e_i + \sum_{j=1}^{k-m} \beta_j u_j}_{\in U}$$

$$\Rightarrow \sum_{t=1}^{l-m} \gamma_t w_t \in U \cap W \Rightarrow \sum_{t=1}^{l-m} \gamma_t w_t = \sum_{s}^{m} \delta_s e_s$$

Но $e_1, ..., e_m, w_1, ..., w_{l-m}$ – базис $W \Rightarrow \gamma_1 = ... = \gamma_{l-m} = 0$.

$$\Rightarrow \sum_{i}^{m} \alpha_i e_i + \sum_{j}^{k-m} \beta_j u_j = 0$$

e_i, u_j – базис $\Rightarrow \alpha_i, \beta_j = 0\ \forall i, \forall j \Rightarrow e_1, ..., e_m, u_1, ..., u_{k-m}, w_1, ..., w_{l-m}$ – базис

$$\Rightarrow \dim(U + W) = m + k - m + l - m = k + l - m$$

■

Замечание 6.4.13. Если $\dim U + \dim W > \dim V \Rightarrow U \cap W \neq \{0\}$

6.4.2. Прямая сумма подпространств

Def 6.4.14. $U, W \subset V$. *Сумма* $U + W$ *называется прямой, если* $\forall v \in U + W$ *представляется* $v = u + w, u \in U, w \in W$ *единственными образом.*

$$U \oplus W$$

Замечание 6.4.15. Достаточно проверить, что 0 представляется единственным образом. $v = u_1 + w_1 = u_2 + w_2 \Leftrightarrow (u_1 - u_2) + (w_1 - w_2) = 0 = \underbrace{0}_{\in U} + \underbrace{0}_{\in W}$

Теорема 6.4.16 (Критерий прямой суммы)**.** $U, W \in V$ – подпространства. $U + W$ – прямая $\Leftrightarrow U \cap W = \{0\}$.

Доказательство. $\Rightarrow$. Предположим, что $u \in U \cap W \Rightarrow 0 = \underbrace{u}_{\in U} + \underbrace{(-u)}_{\in W} \Rightarrow U + W$ – не прямое – противоречие.
$\Leftarrow$. Предположим, что $U + W$ – не прямая $v = u_1 + w_1 = u_2 + w_2 = 0 \Rightarrow \underbrace{u_1 - u_2}_{\in U} = \underbrace{w_2 - w_1}_{\in W} \Rightarrow$ $u_1 - u_2, w_2 - w_1 \in U \cap W = \{0\} \Rightarrow u_1 = u_2, w_1 = w_2$. ■

Def 6.4.17. *$U_i \subset V, i = 1, ..., k$ – подпространства. Сумма $\sum_{i=1}^k U_i$ называется прямой, если $\forall v \in \sum_{i=1}^k U_i$ представляется единственным образом.*

Теорема 6.4.18. $\sum_{i=1}^k U_i$ – прямая $\Leftrightarrow U_j \cap (U_1 + ... + \widehat{U}_j + ... + U_k) = \{0\}\ \forall j = 1, ..., k$.

Доказательство. Аналогично, упражнение. ■

Теорема 6.4.19 (Размерность прямой суммы)**.** $\sum_{i=1}^k U_i$ – прямая сумма $\Leftrightarrow \dim\left(\sum_{i=1}^k U_i\right) = \sum_{i=1}^k \dim U_i$.

Доказательство. $\Rightarrow$. Индукция $k = 2 : \dim(U_1 \oplus U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$.
Индукционный переход: $U_1 + ... + U_{k-1} + U_k = \overline{U} + U_k$ – прямая сумма $\Rightarrow \dim(\overline{U} + U_k) = \dim \overline{U} + \dim U_k = \sum_{i=1}^{k-1} \dim U_i + \dim U_k$.
$\Leftarrow$. Возьмем базисы в $\forall U_i$ из $\dim \sum U_i = \sum \dim U_i \Rightarrow$ базисы не пересекаются $\Rightarrow$ их объединение базис $\sum U_i$, сумма – прямая. ■

Теорема 6.4.20 (О дополнительном подпространстве)**.** V – векторное пространство $\Rightarrow \exists W \subset V : V = U \oplus W$.

Доказательство. $U = \langle e_1, ..., e_k \rangle$ – базис, дополним до V $e_1, ..., e_n \Rightarrow W = \langle e_{k+1}, ..., e_n \rangle \Rightarrow V = U \oplus W$. ■

6.4.3. Изоморфизм векторных пространств

Def 6.4.21. *V, U – векторные пространства над K. Изоморфизмом $\varphi : V \to U$ таких, что*

1. *φ – биекция*
2. *$\varphi(x + y) = \varphi(x) + \varphi(y)\ \forall x, y, \in x, y \in V$*
3. *$\varphi(\lambda x) = \lambda\varphi(x)\ \forall \lambda \in K, x \in V$*

Теорема 6.4.22 (Об изоморфизме векторных пространств)**.** V – векторное пространство над $K, \dim V = n \Rightarrow V \simeq K^n$.

Доказательство. $V = \langle e_1, ..., e_n \rangle, \forall x \in V\ x = \alpha_1 e_1 + ... + \alpha_n e_n$. $\varphi(x) = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ – биекция.

$$\varphi(x + y) = \varphi(\alpha_1 e_1 + ... + \alpha_n e_n + \beta_1 e_1 + ... + \beta_n e_n) = \varphi((\alpha_1 + \beta_1)e_1 + ... + (\alpha_n + \beta_n)e_n) =$$
$$= \begin{pmatrix} \alpha_1 + \beta_1 \\ \vdots \\ \alpha_n + \beta_n \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} + \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \varphi(x) + \varphi(y)$$

■

6.4.4. Факторпространство

$U \subset V, x, y \in V$ сравнимы по подпространству U, если $x - y \in U$. $x \equiv y(U)$.
Если $x \equiv y(U), y \equiv z(U) \Rightarrow x \equiv z(U)$, т.е. отношение эквивалентности.

$$x \equiv y(U), z \equiv w(U) \Rightarrow \alpha x + \beta z \equiv \alpha y + \beta w(U)$$

$\Rightarrow$ классы эквивалентности образуют векторные пространства.

Def 6.4.23. *Факторпространством V/U называется множество $\{x + U, x \in V\}$, т.е. классов эквивалентности по U.*

$$\overline{v} + v/u, \overline{0} = U, \overline{x} = x + U$$

x – представитель класса.

Теорема 6.4.24. $V = U \oplus W \Rightarrow V/U \simeq W$.

Доказательство. Построим $\varphi : W \to V/U, w \to w + U$.

1. Линейность $\varphi(w_1 + w_2) = w_1 + w_2 + U = w_1 + U + w_2 + U = \varphi(w_1) + \varphi(w_2), \varphi(\alpha w) = \alpha w + U = \alpha(w + U) = \alpha\varphi(w)$
2. Сюръективность $v + U \in V/U, v = w + u \Rightarrow v + U = w + u + U = w + U \Rightarrow \varphi(w) = w + U = v + U$
3. Инъективность $w_1 \neq w_2$, но $\varphi(w_1) = \varphi(w_2) \Rightarrow w_1 + U = w_2 + U \Rightarrow w_1 - w_2 \in U$, но $W \cap U = \{0\} \Rightarrow w_1 - w_2 = 0$

■

Следствие 6.4.25 (Размерность факторпространства). $\dim V/U = \dim V - \dim U, U \subset V$

Доказательство. $\forall u \in V\ \exists W \subset V : V = U \oplus W, \dim W = \dim V - \dim U$. По теореме $W \simeq V/U$. ■