

Алгебра 1 семестр ПИ,

Лекции

Собрано 26 ноября 2021 г. в 12:45

Содержание

1. Отношения и перестановки	1
1.1. Отношения	1
1.2. Отношение эквивалентности	1
1.3. Класс эквивалентности	1
1.4. Перестановка	2
1.5. Знак перестановки	3
1.6. Чётные перестановки	4
1.7. Инверсии	5
2. Теория чисел	6
2.1. Делимость	6
2.2. Наибольший общий делитель	7
2.3. Наименьшее общее кратное	8
2.4. Математическая индукция	9
2.5. Простые числа	9
2.6. Основная теорема арифметики	10
2.7. Непрерывные дроби (Цепные дроби)	11
3. Теория сравнений	12
3.1. Начала теории сравнений	12
3.2. Классы вычетов	13
3.3. Кольцо классов вычетов	14
3.4. Приведенная система вычетов	15
3.5. Функция Эйлера	15
3.6. Сравнения с одним неизвестным	16
3.7. Диофантовы уравнения	17
3.8. Системы сравнений	17
4. Комплексные числа	19
4.1. Алгебраическая форма записи комплексного числа	19
4.2. Геометрическое представление комплексных чисел	20
4.3. Тригонометрическая форма записи комплексного числа	20
4.4. Извлечение корней из комплексных чисел	21
4.5. Корни из единицы	21
4.6. Показательная форма записи комплексного числа	22
5. Многочлены	24
5.1. Корни многочлена	26
5.2. Наибольший общий делитель	27

5.3. Факториальность кольца многочленов	27
5.4. Каноническое разложение многочлена над \mathbb{C}	28
5.5. Каноническое разложение многочлена над \mathbb{R}	29
5.6. Уравнения 3-й степени	31
5.7. Уравнения 4-й степени	31
5.8. Отделение кратных корней	31
5.9. Характеристика поля	32
5.10. Формула Тейлора для многочлена	33
5.11. Интерполяция	33
5.12. Поле частных (поле отношений)	34
5.12.1. Поле дробно-рациональных функций	34
5.13. Разложение рациональной дроби над \mathbb{R}	36
6. Линейная алгебра	37
6.1. Матрицы	37
6.2. Действия над матрицами	37
6.3. Умножение матриц	38
6.4. Транспонирование	39
6.5. Формальный степенной ряд	40
6.6. Многочлены от нескольких переменных	40

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. $X = \mathbb{Z} \quad x \omega y \Leftrightarrow x - y : 5$

1. $x - x : 5$ — рефлексивно
 2. $x - y : 5 \Rightarrow y - x : 5$ — симметрично
 3. $x - y : 5, y - z : 5 \Rightarrow x - z : 5$ — транзитивно
- $\Rightarrow \omega$ — отношение эквивалентности

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. $X_1 \cup X_2 \cup \dots = X$
2. $\forall i, j : i \neq j, X_i \cap X_j = \emptyset$

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 $x \in X \Rightarrow X = X_1 \cup X_2 \cup \dots \cup X_n \cup \dots$

$X_i, X_j : X_i = [x_i], X_j = [x_j]$ 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 $X = \{1, 2, \dots, n\}$ 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. $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ — тождественная перестановка

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

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

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

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

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

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

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. $\begin{pmatrix} 1 & i_1 & i_2 & \dots & i_k \\ i_1 & i_2 & i_3 & \dots & 1 \end{pmatrix}$ — k -цикл

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

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

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

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

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

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 $\Rightarrow X = X_1 \cup \dots \cup X_s \Rightarrow \forall X_i$ соответствует цикл, длина которого равна $|X_i|$

Пусть $j \in X_i$, тогда $\begin{pmatrix} j & \sigma(j) & \sigma^2(j) & \dots & \sigma^p(j) \\ \sigma(j) & \sigma^2(j) & \sigma^3(j) & \dots & j \end{pmatrix} \Rightarrow$ 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.

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

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

1.5. Знак перестановки

Def 1.5.1. $\sigma = \tau_1, \tau_2, \dots, \tau_k, \tau_i, 1 \leq i \leq k$ - 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. $\sigma = \tau_1 \tau_2 \dots \tau_k = \tau'_1 \tau'_2 \dots \tau'_s, \tau_i, \tau'_j$ - транспозиции.

$$\Rightarrow \tau_1 \tau_2 \dots \tau_k \tau'_s = \tau'_1 \tau'_2 \dots \tau'_{s-1} \Rightarrow \tau_1 \tau_2 \dots \tau_k \tau'_s \tau'_{s-1} = \tau'_1 \tau'_2 \dots \tau'_{s-2} \Rightarrow e = \tau_1 \tau_2 \dots \tau_k \tau'_s \dots \tau'_1.$$

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

$$e = \tau_1 \tau_2 \dots (ij) \dots$$

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 $i \rightarrow t$, что невозможно. \Rightarrow обязательно будет 1 \Rightarrow число транспозиций уменьшится на 2

Было $k + s$ транспозиций. $k + s - 2, k + s - 4, \dots = 0 \Rightarrow k + s$ - чётное.

$$2. \varepsilon_{\sigma}\varepsilon_{\tau} = \varepsilon_{\sigma\tau}$$

$$\sigma = \tau_1 \dots \tau_k, \tau = \tau'_1 \dots \tau'_s$$

$$\varepsilon_{\sigma}\varepsilon_{\tau} = (-1)^k \cdot (-1)^s = (-1)^{k+s}$$

$$\varepsilon_{\sigma\tau} = (-1)^{k+s}$$

■

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

1.6. Чётные перестановки

$$A_n = \{\text{чётные перестановки в } S_n\}$$

$$\overline{A_n} = S_n \setminus A_n$$

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

Доказательство. Пусть $\tau = (ij), \sigma \in A_n, \varphi: A_n \rightarrow \overline{A_n}, \varphi(\sigma) = \tau\sigma \in \overline{A_n}$

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

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

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: $H \leq G$

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

Def 1.6.5. A_n - знакопеременная группа (alternating)

1.7. Инверсии

Def 1.7.1. $\sigma = \begin{pmatrix} 1 & \dots & s & \dots & t & \dots & n \\ i & \dots & i_s & \dots & i_t & \dots & i_n \end{pmatrix}$. 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 $\sigma = \begin{pmatrix} \dots & s & t & \dots \\ \dots & i & j & \dots \end{pmatrix}, \tau = \begin{pmatrix} i & i+1 \\ i+1 & i \end{pmatrix}, j = i+1$ Хотим узнать, как меняется количество инверсий при умножении на τ .

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

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. $\tau = (ij)$ - произвольная транспозиция. σ - произвольная перестановка.

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

3. $\sigma = \sigma_1\sigma_2\dots\sigma_le$, где σ_i – независимые циклы.

Если σ_l раскладывается в чётное число транспозиций, то в σ_le чётное число инверсий (т.к. каждая транспозиция меняет $inv(\sigma_l)$ на нечетное число).

Если σ_l раскладывается в нечётное число транспозиций, то в σ_le нечётное число инверсий. ■

Раздел #2: Теория чисел

2.1. Делимость

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

Свойства:

1. Рефлексивность. $a:a, a \neq 0$
2. Антисимметричность на \mathbb{N} . $a:b, b:a \Rightarrow a = b$
3. Транзитивность. $a:b, b:c \Rightarrow a:c$
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. $a|b \Rightarrow \forall c \rightarrow a|bc$

6. Пусть $a|b_i, i = 1, \dots, n, a|(b_1 + \dots + b_n + c) \Rightarrow a|c$

Доказательство. $b_1 + \dots + b_n + c = aq, aq_1 + aq_2 + \dots + aq_n + c = aq \Rightarrow c = a(q - q_1 - \dots - q_n) \Rightarrow a|c$ ■

7. $a|b \Rightarrow \forall k \neq 0 \rightarrow ka|kb$

8. $ka|kb \Rightarrow a|b$

Теорема 2.1.2 (О делении с остатком).

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

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 $r = a - bq \geq 0 \Rightarrow a = bq + r$. По выбору $q \rightarrow a - b(q + 1) < 0 \Rightarrow a < b(q + 1) \Rightarrow r = a - bq < b(q + 1) - bq = b$.

Единственность. Преположим, что $a = bq_1 + r_1 = bq_2 + r_2, 0 \leq r_1, r_2 < b$

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

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

2.2. Наибольший общий делитель

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

Def 2.2.2. Наибольший общий делитель a_1, a_2, \dots, a_n называется d такое, что

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

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

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).

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

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

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

...

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

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

Теорема 2.2.5. $r_n = \gcd(a, b)$

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

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

■

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. $(a, b) = (d \cdot \frac{a}{d}, d \cdot \frac{b}{d}) = d \cdot \left(\frac{a}{d}, \frac{b}{d}\right)$ ■

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, \dots, a_n называется число $M > 0 : a_i|M \forall i = 1, \dots, n$
Наименьшее из общих кратных – НОК.

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

Доказательство. $a = a_1d, b = b_1d, (a_1, b_1) = 1$

$$M = at = bs \Rightarrow \frac{M}{b} = \frac{at}{b} = \frac{a_1dt}{b_1d} = \frac{a_1t}{b_1} \Rightarrow M = \frac{b \cdot a_1t}{b_1}$$

t делится на b_1 , т.е. $t = b_1k$

$$M = \frac{ba_1b_1k}{b_1} = ba_1k - \text{минимально при } k = 1 \Rightarrow M = ba_1 = \frac{ba_1d}{d} = \frac{ab}{\text{gcd}(a, b)}$$
 ■

2.4. Математическая индукция

1. Аксои́ма. \forall подмножество \mathbb{N} имеет наши элементы \Rightarrow ММИ.

2. Аксио́ма. $A_1, A_n \Rightarrow A_{n+1} \Rightarrow \forall A_n$

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

Доказательство. $n = 2$. $\text{lcm}(a_1, a_2) = \frac{a_1 a_2}{\gcd(a_1, a_2)} = a_1 \cdot a_2$

Пусть верно для n . Тогда для $n + 1$

$$\begin{aligned} (a_i, a_n a_{n+1}) &= (a_i, a_{n+1}) = 1 \Rightarrow a_1, a_2, \dots, a_{n-1}, a_n a_{n+1} \Rightarrow \\ \Rightarrow \text{lcm}(a_1, \dots, a_{n-1}, a_n \cdot a_{n+1}) &= a_1 \cdot a_2 \cdot \dots \cdot a_{n-1} \cdot a_n \cdot a_{n+1} \end{aligned}$$

■

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. $M = \{d | d > 1, d | a\} \neq \emptyset$ 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 $n \Rightarrow p \leq \sqrt{n}$

Доказательство.

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

■

Теорема 2.5.4 (Теорема Евклида). Простых чисел бесконечно много

Доказательство. Пусть p_1, p_2, \dots, p_n - все простые числа, $a = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$. 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 $\Rightarrow \forall a > 1 \rightarrow p|a \vee (p, a) = 1$

Доказательство.

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

■

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

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

Теорема 2.6.3 (Основная теорема арифметики). 1. $\forall a > 1 \rightarrow a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}, p_1, p_2, \dots, p_k$ - различные простые, $\alpha_1, \alpha_2, \dots, \alpha_k \geq 1$

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 - $p_2 \Rightarrow a_1 = p_2 \cdot a_2$ и т.д.

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

2. Предположим, что представление не одно, то есть

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

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

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 $a = p_a^{\alpha_1} \dots p_k^{\alpha_k}$ имеет вид $b = p_1^{\beta_1} \cdot \dots \cdot p_k^{\beta_k}, 0 \leq \beta_i \leq \alpha_i$

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

Следствие 2.6.6. $\gcd(a_1, \dots, a_n)$ имеет вид $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, где

$a_i = \min \{ \text{показатель степени } p_i, \text{ с которым } p_i \text{ входит в разложение } a_1, a_2, \dots, a_n \}$

Следствие 2.6.7. $\text{lcm}(a_1, \dots, a_n)$ имеет вид $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, где

$a_i = \max \{ \text{показатель степени } p_i, \text{ с которым } p_i \text{ входит в разложение } a_1, a_2, \dots, a_n \}$

2.7. Непрерывные дроби (Цепные дроби)

Def 2.7.1. *Выражение вида*

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

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

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. $a > b$

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

где

$$\begin{aligned} a &= b \cdot a_0 + r_1 \\ b &= r_1 \cdot a_1 + r_2 \\ r_1 &= r_2 \cdot a_2 + r_3 \end{aligned}$$

■

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). $\delta_k = \frac{p_k}{q_k}, p_{-1} = 1, q_{-1} = 0, p_0 = a_0, q_0 = 1$

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

Доказательство. $\delta_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1 \cdot 1 + 0} = \frac{a_1 p_0 + p_{-1}}{a_1 q_0 + q_{-1}}$

Предположим, что для k верно. Тогда для $k+1$

$$\begin{aligned} \delta_{k+1} &= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_k + \frac{1}{a_{k+1}}}}} = \frac{(a_k + \frac{1}{a_{k+1}}) \cdot p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}}) \cdot q_{k-1} + q_{k-2}} = \\ &= \frac{(a_{k+1} \cdot a_k + 1) \cdot p_{k-1} + p_{k-2} \cdot a_{k+1}}{(a_{k+1} \cdot a_k + 1) \cdot q_{k-1} + q_{k-2} \cdot a_{k+1}} = \frac{a_{k+1}(a_k \cdot p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1} \cdot p_k + p_{k-1}}{a_{k+1} \cdot q_k + q_{k-1}} \end{aligned}$$

■

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

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

Утверждение 3.1.2.

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

Доказательство. 1) \Rightarrow 2)

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

2) \Rightarrow 3)

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

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

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

$$\begin{aligned} 3) : a = b + mt &\Rightarrow mq_1 + r_1 = mq_2 + r_2 + mt \Rightarrow \\ &\Rightarrow m(q_1 - q_2 - t) = r_2 - r_1 \Rightarrow m | r_2 - r_1 \Rightarrow r_2 - r_1 = 0 \end{aligned}$$

■

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.

$$a - c = a - b + b - c : m$$

■

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.

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

■

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

Доказательство.

$$a - b = a_1d - b_1d = my = m_1dt \Rightarrow a_1 - b_1 = m_1t$$

■

$$7. a \equiv b \pmod{m} \Rightarrow ka \equiv kb \pmod{m}$$

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

Доказательство.

$$a = a_1d, b = b_1d, a - b : m \Rightarrow (a_1 - b_1) \cdot d : m \Rightarrow a_1 - b_1 : \frac{m}{d}$$

■

$$9. d|m, a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{d}$$

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

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 $(\text{mod } m)$ называется множество чисел, сравнимых с a по модулю m

$$m = 7, \bar{1} = \{-6, 8, 1, 15, \dots\}$$

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

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

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

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 $(\text{mod } m) \Rightarrow \forall b \rightarrow ax + b$ тоже пробегает полную систему вычетов по $(\text{mod } m)$

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 .

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

Lm 3.3.2. Сложение и умножение определены корректно

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

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

■

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

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

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

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

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

■

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

1. $\forall x, y, z \rightarrow (x + y) + z = x + (y + z)$
2. $\exists 0 \in R : \forall x \in R \rightarrow x + 0 = x$
3. $\forall x \in R \exists (-x) \in R : x + (-x) = 0$
4. $\forall x, y \in R \rightarrow x + y = y + x$
5. $\forall x, y, z \in R \rightarrow (y + z) = xy + xz, (x + y)z = xz + yz$
6. $\forall x, y, z \in R \rightarrow (xy)z = x(yz)$

Замечание 3.3.6. $\exists 1 \in R : \forall x \in R \rightarrow x \cdot 1 = 1 \cdot x = x$ – кольцо с единицей

$\forall x, y \in R \rightarrow xy = yx$ – коммутативное кольцо

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

Доказательство.

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

и т.д.

■

Def 3.3.8. Кольца R , в котором $\forall a, b \rightarrow (ab = 0 \Rightarrow a = 0 \vee b = 0)$ 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.

Теорема 3.3.10. 1. \mathbb{Z}_m имеет делители нуля $\Leftrightarrow m$ – составное число

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

Доказательство. " \Rightarrow ". $m = n \cdot k, \bar{n} \cdot \bar{k} = \bar{0}$ в \mathbb{Z}_m

" \Leftarrow ". $\bar{n} \cdot \bar{k} = \bar{0} \Rightarrow n \cdot k \equiv 0 \pmod{m}$

Предположим, что m – простое $\Rightarrow m|n \vee m|k \Rightarrow \bar{n} = \bar{0} \vee \bar{k} = \bar{0}$. Но \bar{n} и \bar{k} – делители нуля, т.е. $\bar{n}, \bar{k} \neq \bar{0} \Rightarrow m$ – 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 образуют приведенную систему вычетов

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

Lm 3.4.3. Если p – простое, то

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

Теорема 3.4.4. $(a, m) = 1, x$ пробегает приведенную систему вычетов $\Rightarrow ax$ тоже пробегает приведенную систему вычетов по \pmod{m}

Доказательство. $x \rightarrow \varphi(m), ax \rightarrow \varphi(m)$

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

3.5. Функция Эйлера

Lm 3.5.1. p – простое, $\alpha > 0$

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

Доказательство. $1, 2, 3, \dots, p, 2p, 3p, \dots, p \cdot p, \dots, p^\alpha - 1$. 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. Функция $\Theta : \mathbb{N} \rightarrow \mathbb{N}$ называется мультипликативной, если

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

Теорема 3.5.3 (Мультипликативность функции Эйлера). φ мультипликативна

Доказательство. $(a, b) = 1$

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

Количество чисел, взаимно-простых с $b : \forall$ строка : $kb+r, k=0, \dots, a-1, 1 \leq r \leq b$. 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 : $xb+r, x=0, \dots, a-1 \Rightarrow xb+r$ – 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. $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ – каноническое разложение $\Rightarrow \varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdot \dots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k-1})$

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

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

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

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

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

■

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. $\mathbb{Z}_m^* = \{r : 0 \leq r < m, (r, m) = 1\}$ – 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. $d \nmid b \Rightarrow$ решений нет.

2. $d \mid b \Rightarrow \exists d$ решений : $x = x_0 + m_1 t, t = 0, 1, \dots, d - 1, m_1 = \frac{m}{d}, x_0$ – 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. $0 \leq x_0 + m_1 t < m$.

Ясно, что такие решения будут при $t = 0, 1, \dots, d - 1$.

■

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

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b$$

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 $c - ax : b \Rightarrow \frac{c - ax_0}{b} \in \mathbb{Z}$

■

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

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

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

1. Решение системы существует:

$$x \equiv \frac{M}{m_1} \cdot M'_1 b_1 + \frac{M}{m_2} \cdot M'_2 b_2 + \dots + \frac{M}{m_k} \cdot M'_k b_k \pmod{M}$$

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

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

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

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

" \Leftarrow ". Предположим, что

$$k|p, k > 1, k \neq p \Rightarrow k < p \Rightarrow 1 \cdot 2 \cdot \dots \cdot (p-1) \not\equiv k \pmod{p} \Rightarrow (p-1)! \equiv 0 \pmod{p}$$
■

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 множеством 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

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

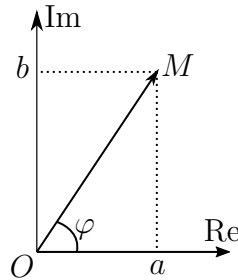
4.2. Геометрическое представление комплексных чисел

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 . $\varphi = (\operatorname{Re}, OM)$ – 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. $a = \rho \cos \varphi, b = \rho \sin \varphi \Rightarrow z = a + bi = \rho(\cos \varphi + i \sin \varphi)$

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

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

1. $|z_1 + z_2| \leq |z_1| + |z_2|$
2. $|z_1 - z_2| \geq ||z_1| - |z_2||$

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

$$\begin{aligned} |z_1 + z_2|^2 &= |\rho_1 \cos \varphi_1 + \rho_2 \cos \varphi_2 + i(\rho_1 \sin \varphi_1 + \rho_2 \sin \varphi_2)|^2 = \\ &= \rho_1^2 \cos^2 \varphi_1 + 2\rho_1 \rho_2 \cos \varphi_1 \cos \varphi_2 + \rho_2^2 \cos^2 \varphi_2 + \rho_1^2 \sin^2 \varphi_1 + 2\rho_1 \rho_2 \sin \varphi_1 \sin \varphi_2 + \rho_2^2 \sin^2 \varphi_2 = \\ &= \rho_1^2 + 2\rho_1 \rho_2 \cos(\varphi_1 - \varphi_2) = \rho_2^2 \leq \rho_1^2 + 2\rho_1 \rho_2 + \rho_2^2 = (\rho_1 + \rho_2)^2 = (|z_1| + |z_2|)^2 \end{aligned}$$

2.

$$|z_1| = |z_1 - z_2 + z_2| \leq |z_1 - z_2| + |z_2| \Rightarrow |z_1| - |z_2| \leq |z_1 - z_2| \Rightarrow ||z_1| - |z_2|| \leq |z_1 - z_2|$$

■

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. $n \geq 0$. По индукции: $n = 1$ очевидно.

$n - 1 \rightarrow n$:

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

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 $z_k, k = 0, 1, \dots, n-1$

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

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. $\forall m : 0 < m < n \rightarrow \varepsilon^m \neq 1$

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 $\varepsilon_k^m = 1 \Rightarrow \cos \frac{2\pi k m}{n} = 1, \sin \frac{2\pi k m}{n} = 0$

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

■

Свойства:

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

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

■

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.

$u_n = \{\varepsilon_k, \varepsilon_k^2, \dots, \varepsilon_k^{n-1}, 1\}, \varepsilon_k$ – первообразный корень.

Def 4.5.3. Группа G называется циклической, если $G = \{a, a^2, a^3, \dots\}$. 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 $\exists \varphi : G_1 \rightarrow G_2$:

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

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

Доказательство. ε – первообразный корень, т.е. $u_n = \{\varepsilon^k\}, k = 0, \dots, n-1$

$\varphi : \mathbb{Z}_n \rightarrow u_n, \varphi(k) = \varepsilon^k, \varphi$ – 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. $z + \bar{z} \in \mathbb{R}$

5. $i(z - \bar{z}) \in \mathbb{R}$

Раздел #5: Многочлены

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

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

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

4. $\forall a \in R \rightarrow a = (a, 0, 0, \dots)$

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

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

$$\Rightarrow x^k = (0, 0, \dots, 1, 0, \dots)$$

Тогда

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

Обозначение: $R[x] = \{a_0 + a_1 x + \dots + a_n x^n\}$ – 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 $n \geq 1$, 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. $\deg(f + g) \leq \max\{\deg f, \deg g\}$
2. $\deg(f \cdot g) \leq \deg f + \deg g$

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

$$f + g = a_nx^n + \dots \Rightarrow \deg(f + g) \leq \deg n$$

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

■

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. $f = a_nx^n + \dots, g = b_mx^m + \dots \Rightarrow f \cdot g = a_nb_mx^{n+m} + \dots, a_n \cdot b_m \neq 0$ 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. $\deg f = n, \deg g = m, n < m \Rightarrow f = g \cdot 0 + f$

$n \geq m$. Индукция по n . $n = 0 \Rightarrow a_0 = b_0(b_0^{-1}a_0) + 0$.

$n - 1 \mapsto n$. $f = a_nx^n + \dots + a_0, g = b_mx^m + \dots + b_0$. Рассмотрим

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

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

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

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 $\deg(g(q_1 - q_2)) \geq m, \deg(r_2 - r_1) < m$ – противоречие. ■

Def 5.0.11. $f = a_nx^n + \dots + a_0, c \in R$. Тогда $f(c) = a_nc^n + \dots + a_1c + a_0$ – 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. $f : x - a \Leftrightarrow f(a) = 0$

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 $(x - c)^k | f, (x - c)^{k+1} \nmid f$, то c – корень кратности k .

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

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 $g \leq n - k \Rightarrow$ корней $f \leq k + n - k = n.$ ■

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

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

Формальное равенство многочленов.

$$f = g = a_n x^n + \dots + a_1 x + a_0$$

Функциональное равенство многочленов.

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

Пример 5.1.4. $\mathbb{Z}_5. f = x^5 + x^4, g = x^4 + x.$

$$f - g = x^5 - x, x^5 \equiv x \pmod{5} \Rightarrow x^5 - x = 0 \quad \forall x \in \mathbb{Z}_5 \Rightarrow f(x) = g(x)$$

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 ассоциированы.

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 $R \forall a \in R \setminus \{0\} \exists a = \varepsilon \cdot p_1 \cdot \dots \cdot p_s, \varepsilon \in R^*, p_1, \dots, p_s$ – 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. $f \in K[x]$, φ – 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. **TODO**

3. $f, g, \varphi \in K[x]$, φ – неприводим, $\varphi|fg \Rightarrow \varphi|f \vee \varphi|g$

Доказательство. $\varphi \nmid f \Rightarrow (\varphi, f) = 1 \Rightarrow \exists h_1, h_2 \in K[x] : h_1\varphi + h_2f = 1 \Rightarrow h_1\varphi g + h_2fg = g \Rightarrow \varphi|(h_1\varphi g + h_2fg) \Rightarrow \varphi|g$ ■

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

Lm 5.3.7. $\forall f \in K[x] : \deg f \geq 1$ 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 $f_1 \Rightarrow \varphi|f$. ■

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. $\Rightarrow f = \varphi_1 \cdot \varphi_2 \cdot \dots \cdot \varphi_k$

Единственность. $f = \varepsilon \varphi_1 \varphi_2 \dots \varphi_k = \eta \psi_1 \psi_2, \dots, \psi_s, \varepsilon, \eta \in K^*, \varphi_i, \psi_j$ – неприводимы. $k \leq s \Rightarrow \varphi_1|\eta \psi_1 \psi_2 \dots \psi_s \Rightarrow \varphi_1|\psi_j \Rightarrow \varphi_1 = \psi_j \Rightarrow \varepsilon^{-1} \eta \psi_{s-k} \dots \psi_s = 1 \Rightarrow \varepsilon = \eta, \psi_{s-k} \dots \psi_s = 1$ ■

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

5.4. Каноническое разложение многочлена над \mathbb{C}

Def 5.4.1. Поле K называется алгебраически замкнутым, если любой многочлен $\deg \geq 1$ 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}

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

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

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 $\varphi : R_1 \rightarrow R_2$:

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. $id : R \rightarrow R$ – изоморфизм.

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

Доказательство.

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

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

$$\varphi(1) = 1$$

$\Rightarrow \varphi$ – гомоморфизм.

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

3. $\varphi : R \rightarrow R[x], \varphi(r) = r$ – 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 $\varphi : K \rightarrow K$ (K – поле) называется автоморфизмом.

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

$$\varphi(n) = \varphi(\underbrace{1 + 1 + \dots + 1}_n) = \underbrace{\varphi(1) + \dots + \varphi(1)}_n = n$$

$$\Rightarrow \varphi(-n) = -n \Rightarrow \varphi|_{\mathbb{Z}} = id$$

$$q \cdot \varphi\left(\frac{1}{q}\right) = \varphi\left(\frac{1}{q}\right) + \dots + \varphi\left(\frac{1}{q}\right) = \varphi\left(\frac{1}{q} + \dots + \frac{1}{q}\right) = \varphi(1) = 1 \Rightarrow \varphi\left(\frac{1}{q}\right) = \frac{1}{q} \Rightarrow \varphi\left(\frac{p}{q}\right) =$$

$$p \cdot \varphi\left(\frac{1}{q}\right) = \frac{p}{q} \Rightarrow \text{автоморфизмы } \mathbb{Q} = \{id\}$$

2. автоморфизмы $\mathbb{R} = \{id\}$

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

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

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

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

$$\begin{aligned} \varphi(f) &= \varphi(a_n x^n + \dots + a_0) = \varphi(a_n) \cdot \varphi(x^n) + \dots + \varphi(a_1) \varphi(x) + \varphi(a_0) = \\ &= a_n \varphi(x)^n + \dots + a_1 \varphi(x) + a_0 = f(\varphi(x)) \end{aligned}$$

$x = c : \varphi(f(c)) = \varphi(0) = 0$. 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 $\mathbb{R}, \deg f \geq 2$, корней из \mathbb{R} нет. Пусть $\alpha + \beta i$ – комплексный корень f ($\beta \neq 0$). По лемме $\alpha - \beta i$ – тоже корень $\Rightarrow f \div (x - \alpha - \beta i)(x - \alpha + \beta i)$.

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

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

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

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

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

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. $x = y - \frac{b'}{4} \Rightarrow y^4 + \alpha y^2 + \beta y + \gamma = 0$

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 $u : (\alpha + u)y^2 + \beta y + (u + \alpha)^2 - \gamma - \text{полный квадрат} \Leftrightarrow \beta^2 - u(\alpha + u)((u + \alpha)^2 - \gamma) = 0$
– 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. $f \in K[x], f = a_n x^n + \dots + a_1 x + a_0$. Производной многочлена f называется $f' = na_n x^{n-1} + \dots + a_1$

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. $(f_1 \cdot f_2 \cdot \dots \cdot f_k)' = f_1' f_2 \dots f_k + f_1 f_2' \dots f_k + \dots + f_1 f_2 \dots f_k'$

6. $(f^k)' = k \cdot f^{k-1} \cdot f'$

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

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

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

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

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

$$f = a_n x^n + \dots + a_1 x + a_0, g = b_m x^m + \dots + b_1 x + b_0 \quad a_k x^k \cdot g - \text{верно} \Rightarrow \text{верно и для } f \cdot g$$

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 ". $\deg f \geq 2, f$ 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. $1 + 1 + 1 + \dots = 0 \vee \infty$

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

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

Доказательство. Предположим, что $n = tk, 1 < t, k < n \Rightarrow n \cdot 1 = t \cdot k \cdot 1 = 0 \Rightarrow t = 0$ или $k = 0$ – противоречие. ■

Теорема 5.9.3. K – поле, $\text{char } K = 0. f \in K[x], \varphi \in K[x]$ – 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

$$(\varphi, \varphi'g) = 1 \Rightarrow (\varphi, h) = 1. \quad \blacksquare$$

Теорема 5.9.4 (Критерий кратности корня). $\text{char } K = 0, f \in K[x], c \in L \supset K$. Тогда c – корень кратности k многочлена $f \Leftrightarrow f(c) = f'(c) = \dots = f^{(k-1)}(c) = 0$ 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. $\Rightarrow f'(c) = \dots = f^{(k-1)}(c) = 0$, 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. $\text{char } K = 0, f = a\varphi_1^{k_1}\varphi_2^{k_2}\dots\varphi_s^{k_s}$ – каноническое разложение $\Rightarrow \gcd(f, f') = \varphi_1^{k_1-1}\varphi_2^{k_2-1}\dots\varphi_s^{k_s-1}$

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

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

5.10. Формула Тейлора для многочлена

Теорема 5.10.1 (Разложение по степеням другого многочлена). K – поле, $\text{char } K = 0, f, g \in K[x], \deg g \geq 1 \Rightarrow f = h_n g^n + h_{n-1} g^{n-1} + \dots + h_1 g + h_0$, 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 существования, и для единственности.

Индукционный переход: $\deg f \geq \deg g, f = g \cdot q + r, \deg r \leq \deg g, \deg q < \deg f \Rightarrow q = h_n g^n + \dots + h_1 g + h_0 \Rightarrow f = gq + r = h_n g^{n+1} + \dots + h_1 g^2 + h_0 g + r, \deg h_i < \deg g \Rightarrow$ существование доказано. Предположим, что разложение не единственно, т.е. $f = h_n g^n + \dots + h_1 g + h_0 = h'_n g^n + \dots + h'_1 g + h'_0$

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

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). $\text{char } K = 0, f \in K[x], c \in K \Rightarrow$

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

Доказательство. $g = x - c \Rightarrow f = r_n(x - c)^n + r_{n-1}(x - c)^{n-1} + \dots + r_1(x - c) + r_0$. Т.к. $\deg r_i < \deg g = 1 \Rightarrow r_i \in K$

$$x = c \quad f(c) = r_0, f^{(k)}(c) = k! \cdot r_k \Rightarrow r_k = \frac{f^{(k)}(c)}{k!}$$

5.11. Интерполяция

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

Задача:

x_0	x_1	\dots	x_n
y_0	y_1	\dots	y_n

 – узлы интерполяции. Требуется найти $P_n \in K[x] : P_n(x_i) = y_i, i = 0, \dots, n$.

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

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

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.

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

■

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

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

$$x = x_0 \quad P_n(x_0) = a_0 = y_0$$

$$x = x_1 \quad P_n(x_1) = y_1 = y_0 + a_1(x_1 - x_0) \Rightarrow a_1 \text{ и т.д.}$$

5.12. Поле частных (поле отношений)

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

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. $\forall a \in R \quad a = (a, 1)$

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

$$R = K[x] \rightarrow Q(K[x]) = \left\{ \frac{f}{g}, f, g \in K[x], g \neq 0 \right\}$$

$K(x)$ – 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 $\frac{f}{g} = h_1 + \frac{r_1}{g} \Leftrightarrow \frac{f}{g} = \frac{h_1g + r_1}{g} \Rightarrow f = h_1g + r_1$ – однозначно определено. ■

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

Доказательство. $(f, g) = 1 \Rightarrow \exists h'_1, h'_2 : h'_1g + h'_2f = 1$

$$\Rightarrow hh'_1g + hh'_2f = h \Rightarrow \frac{h}{fg} = \frac{hh'_1g + hh'_2f}{fg} = \frac{hh'_1}{f} + \frac{hh'_2}{g}$$

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

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

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

$$\Rightarrow \frac{f}{g} = h + \underbrace{\frac{f'_1}{\varphi_1^{k_1}} + \dots + \frac{f'_s}{\varphi_s^{k_s}}}_{\text{правильные дроби}} \Rightarrow h = 0$$

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

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

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

$\Rightarrow \exists$ 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.

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

Раздел #6: Линейная алгебра

6.1. Матрицы

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

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

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

Виды матриц:

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

6.2. Действия над матрицами

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

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

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

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

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 6.2.1. $M(m, n, K)$ – 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.

$$(c_1 + c_2) \cdot A = c_1 A + c_2 A$$

6. Дистрибутивность относительно сложения матриц.

$$c(A + B) = cA + cB$$

7. $c_1, c_2 \in K$

$$c_1(c_2 A) = (c_1 c_2) A$$

8. $1 \cdot A = A$

6.3. Умножение матриц

Def 6.3.1. $B = \begin{pmatrix} b_1 & b_2 & \dots & b_n \end{pmatrix}, A = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix}$

$$B \cdot A = b_1 a_1 + b_2 a_2 + \dots + b_n a_n$$

Def 6.3.2 (Умножение матриц). $A - m \times k, B - k \times n$. Тогда определено произведение $A \cdot B = C - m \times n$.

$$C = (c_{ij}), 1 \leq i \leq m, 1 \leq j \leq n, c_{ij} = A_i \cdot B^j = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{ik}b_{kj}$$

A_i – i -я строка A , B^j – j -й столбец B .

Замечание 6.3.3. 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 $\in K$.

$$4. \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 b_1 & a_1 b_2 & \dots & a_1 b_n \\ a_2 b_1 & a_2 b_2 & \dots & a_2 b_n \\ \dots & \dots & \dots & \dots \\ a_n b_1 & a_n b_2 & \dots & a_n b_n \end{pmatrix}$$

5. $B = \begin{pmatrix} B^1 & B^2 & \dots & B^n \end{pmatrix}$, B^j – столбцы.

$$A \cdot B = \begin{pmatrix} AB^1 & AB^2 & \dots & AB^n \end{pmatrix}$$

6. $M(n, n, K) = M(n, K)$ – квадратные матрицы порядка n . $E = E_n \in M(n, K)$ – единичная матрица.

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

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 $\Rightarrow C - l \times n \Rightarrow (AB)C - m \times n$.

$BC - (k \times l) \cdot (l \times n) = (k \times n)$. $A(BC) - (m \times k) \cdot (k \times n) = (m \times n)$. $C = \begin{pmatrix} C^1 & C^2 & \dots & C^n \end{pmatrix}$ – столбцы. Тогда $A(BC) = A \begin{pmatrix} BC^1 & BC^2 & \dots & BC^n \end{pmatrix} = \begin{pmatrix} ABC^1 & ABC^2 & \dots & ABC^n \end{pmatrix}$
 $(AB)C = (AB) \begin{pmatrix} C^1 & C^2 & \dots & C^n \end{pmatrix} = \begin{pmatrix} ABC^1 & ABC^2 & \dots & ABC^n \end{pmatrix}$ ■

Теорема 6.3.4. $M(n, K)$ – кольцо с 1.

6.4. Транспонирование

Def 6.4.1. $A = (a_{ij}) - m \times n$.

$$A^T = (a_{ji}), 1 \leq j \leq n, 1 \leq i \leq m$$

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. $A - m \times k, B - k \times n \Rightarrow (AB)^T - n \times m$. $B^T - n \times k, A^T - k \times m \Rightarrow B^T A^T - n \times m$.

$A = (a_{ij}), 1 \leq i \leq m, 1 \leq j \leq k$. $B = (b_{ij}), 1 \leq i \leq k, 1 \leq j \leq n$.

$A^T = C = (c_{ij}), 1 \leq i \leq k, 1 \leq j \leq m$.

$B^T = D = (d_{ij}), 1 \leq i \leq n, 1 \leq j \leq k$.

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

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

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

■

6.5. Формальный степенной ряд

R – коммутативное кольцо с 1.

Def 6.5.1.

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$$

$a_n \in R$, 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.

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

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

6.6. Многочлены от нескольких переменных

R – коммутативное кольцо с 1. $S = R[x_1], S[x_2] = R[x_1, x_2]$ и т.д.

$R[x_1, x_2, \dots, x_n]$ – кольцо многочленов от переменных x_1, x_2, \dots, x_n над R .

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

Def 6.6.1. *Мономом называется многочлен, у которого только один ненулевой коэффициент. $a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}, i_1 + i_2 + \dots + i_n$ – степень монома.*

Def 6.6.2. *Многочлен от n переменных называется однородным, если он равен сумме мономов степени m .*

Def 6.6.3. *Элементарными симметрическими многочленами порядка k называются*
 $\sigma_1(x_1, \dots, x_n) = x_1 + \dots + x_n$
 $\sigma_2(x_1, \dots, x_n) = \sum_{1 \leq i < j \leq n} x_i x_j$
 $\sigma_k(x_1, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k}$

Теорема 6.6.4 (Теорема Виета). $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$, имеющий n корней.

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