Алгебра

Лектор: Жуков Игорь Борисович

Содержание

1 Теория чисел

1 Делимость

***Определение* 1.1.** $a, b \in \mathbb{Z}, a \mid b \iff \exists c \in \mathbb{Z} : b = ac$

Свойства.

1. $a \mid a$ — рефлексивность
2. $a \mid b,\ b \mid c \implies \exists c \in \mathbb{Z} : b = ac$ — транзитивность
3. $a \mid b,\ k \in \mathbb{Z} \implies ka \mid kb$
4. $a \mid b_1,\ a \mid b_2 \implies a \mid (b_1 \pm b_2)$
5. $\pm 1 \mid a$
6. $\begin{cases} ka \mid kb \\ k \neq 0 \end{cases} \implies a \mid b$

***Определение* 1.2.** a, b называются *ассоциированными*, если $a \mid b$ и $b \mid a$. Иногда такое отношение обозначают $a \sim b$:

$$a \sim b \iff a \mid b \ \wedge \ b \mid a$$

Свойства.

1. Пусть $a \sim a'$, $b \sim b'$. Тогда $a \mid b \iff a' \mid b'$.

2 Отношение эквивалентности и разбиение на классы

***Определение* 2.1.** Отношение эквивалентности — бинарное отношение, удовлетворяющее следующим свойствам: рефлексивность, симметричность, транзитивность.

***Определение* 2.2.** Разбиение на классы множества M — это представление M в виде $M = \bigcup\limits_{i \in I} M_i$, где M_i — классы, I — индексное множество, $M_i \cap M_j = \varnothing$ при $i \neq j$.

Теорема 2.1. Пусть $M = \bigcup\limits_{i \in I} M_i$ — разбиение на классы. Введем отношение $\sim$ над M так, что $a \sim b \iff \exists i \in I : a, b \in M_i$. Тогда $\sim$ — отношение эквивалентности.

Доказательство.

Рефлексивность и симметричность очевидны. Докажем транзитивность.

$$a \sim b,\ b \sim c \implies \exists i, j : \begin{cases} a, b \in M_i \\ b, c \in M_j \end{cases}$$

Тогда $b \in M_i \cap M_j$, но так как $M_i \cap M_j \neq \varnothing$ при неравных i и j, $i = j$. Значит $a, b, c \in M_i$.

Теорема 2.2. Пусть $\sim$ — отношение эквивалентности на M. Значит существует разбиение на классы $M = \bigcup\limits_{i \in I} M_i$ такое, что $\forall a, b \in M : a \sim b \iff \exists i : a, b \in M_i$.

Доказательство.

Рассмотрим $a \in M$. Назовем классом элемента a множество

$$[a] = \{b \in M \mid a \sim b\}.$$

Докажем, что для любых элементов a и b, либо $[a] = [b]$, либо $[a] \cap [b] = \varnothing$.

Пусть $[a] \cap [b] \neq \varnothing$. Тогда

$$\exists x \in [a] \cap [b] \implies \begin{cases} x \in [a] \\ x \in [b] \end{cases} \overset{\text{опр. класса}}{\implies} \begin{cases} x \sim a \\ x \sim b \end{cases} \overset{\text{транзитивность} \sim}{\implies} a \sim b.$$

$$(\forall c \in [a]\ c \sim a \overset{a \sim b}{\implies} c \sim b \implies c \in [b]) \implies [a] \subset [b] \tag{1}$$

$$(\forall c \in [b]\ c \sim b \overset{a \sim b}{\implies} c \sim a \implies c \in [a]) \implies [b] \subset [a] \tag{2}$$

Из (1) и (2) получаем $[a] = [b]$.

Тогда искомое разбиение можно построить как

$$X = \{[a] \mid a \in M\}.$$

Действительно $\forall a \in M$, так как $a \in [a]$, то $M = \bigcup\limits_{\alpha \in I} M_i$, а так как различные классы не пересекаются (доказано выше) $\forall a, b\ [a] \neq [b]$.

***Определение* 2.3.** Построенное множество X называют *фактор-множеством* множества M по отношению эквивалентности $\sim$, обозначение: $M/\sim$.

Пример. $\mathbb{Z}/\sim = \{[z] \mid z \in \mathbb{Z}\} = \{[0], [1], [2], \dots\}$

3 Сравнение по модулю

***Определение* 3.1.** $\exists a, b, m \in \mathbb{Z}$. Говорят, что

$$\begin{aligned} a \underset{m}{\equiv} b &\iff \\ a \equiv_m b &\iff \\ a \equiv b \pmod m &\iff m \mid (a - b) \end{aligned}$$

Свойства.

1. $\underset{m}{\equiv}$ — рефлексивно
2. $\underset{m}{\equiv}$ — симметрично
3. $\underset{m}{\equiv}$ — транзитивно
4. $a \underset{m}{\equiv} b,\ d \mid m \implies a \underset{d}{\equiv} b$
5. $a \underset{m}{\equiv} b,\ k \in \mathbb{Z} \implies ka \underset{km}{\equiv} kb$
6. $a \underset{m}{\equiv} b,\ k \in \mathbb{Z} \implies ka \underset{m}{\equiv} kb$ (ослабленная версия предыдущего свойства)

7. $a_1 \underset{m}{\equiv} b_1,\ a_2 \underset{m}{\equiv} b_2 \implies a_1 \pm a_2 \underset{m}{\equiv} b_1 \pm b_2$
8. $a_1 \underset{m}{\equiv} b_1,\ a_2 \underset{m}{\equiv} b_2 \implies a_1 a_2 \underset{m}{\equiv} b_1 b_2$

Замечание. Сравнение по модулю — отношение эквивалентности.

4 Кольцо классов вычетов

***Определение* 4.1.** Множество классов вычетов по модулю m — это множество всех вычетов по модулю m.

Обозначается как $\mathbb{Z}/m\mathbb{Z} \iff \mathbb{Z}/m \iff \mathbb{Z}/\underset{m}{\equiv}$

Теорема 4.1. $\exists m \in \mathbb{N}$. Тогда

1. $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$
2. $|\mathbb{Z}/m\mathbb{Z}| = m$

Доказательство.

1. $\exists a \in \mathbb{Z}$, (!) $\overline{a} = \overline{r}, \quad 0 \leqslant r < m$
   a) Случай $a \geqslant 0$: $\exists r$ — наименьшее число, такое что $r \geqslant 0$ и $a \underset{m}{\equiv} r$.

   Если $r \geqslant m$, то $r - m \underset{m}{\equiv} a,\ r - m \geqslant 0,\ r - m < r$. То есть $r - m$ подходит под условие для r и меньше. Противоречие с выбором r.

   Значит $r < m$, то есть r — искомое.

   b) Случай $a < 0$:

   Рассмотрим $a' = a \pm (-a)m = a(1-m)$. Тогда $a < 0,\ 1 - m \geqslant 0$, и $a' \geqslant 0$.

   $\overline{a} = \overline{a'} = \overline{r},\ 0 \leqslant r < m$
2. предположим $\overline{r} = \overline{r'},\ 0 \leqslant r, r' < m$.

$$\begin{cases} |r' - r| < m \\ m \mid (r - r') \end{cases} \implies r' - r = 0 \implies r = r'.$$

Следствие. Теорема о делениии с остатком

Пусть $a \in \mathbb{Z},\ b \in \mathbb{N}$. Тогда

$$\exists!\, q, r \in \mathbb{Z} : \begin{cases} a = bq + r \\ \leqslant r < b \end{cases}$$

Доказательство.

Существование:

В $\mathbb{Z}/b\mathbb{Z}$ рассмотрим $\overline{a} \in \{\overline{0}, \overline{1}, \ldots, \overline{b-1}\}$, тогда по теореме выше найдется $0 \leqslant r < b$ для которого $\overline{a} = \overline{r}$:

$$a \underset{b}{\equiv} r \iff a = bq + r, \quad q \in \mathbb{Z}.$$

Единственность: Пусть нашлось два таких $q, q' \in \mathbb{Z}$ и $r, r' \in \mathbb{Z}$ для которых $a = bq + r, a = bq' + r'$. Тогда

$$bq + r \underset{b}{\equiv} bq' + r' \iff r \underset{b}{\equiv} r' \overset{0 \geqslant r, r' < b}{\iff} r = r' \implies bq = bq' \iff q = q'.$$

Напомню, что вторая равносильнось выполняется благодаря единственности класса вычетов $\overline{r}$.

***Определение* 4.2.** q — *неполное частное* при делении a на b, r — *остаток* при делении a на b.

***Определение* 4.3.** *Операция* на множестве M — бинарное отображение $M \times M \to M$.

На $\mathbb{Z}/m\mathbb{Z}$ определим операцию сложения и умножения по модулю m:

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

Предложение 4.1. Это правда операции над множеством $\mathbb{Z}/m\mathbb{Z}$:

Доказательство. То, что за пределы множества при сложении и умножении мы не выходим, очевидно. Надо доказать, что при подстановке одинаковых классов, получаеются одинаковые результаты, то есть:

$$(!)\ \overline{a} = \overline{a'},\ \overline{b} = \overline{b'} \implies \overline{a + b} = \overline{a' + b'},\ \overline{a \cdot b} = \overline{a' \cdot b'}$$

распишем условия через сравнения по модулю:

$$\overline{a} = \overline{a'},\ \overline{b} = \overline{b'} \implies a \underset{m}{\equiv} a',\ b \underset{m}{\equiv} b'$$

Воспользуемся свойствами сравнения:

$$a \underset{m}{\equiv} a',\ b \underset{m}{\equiv} b' \implies a + b \underset{m}{\equiv} a' + b',\ a \cdot b \underset{m}{\equiv} a' \cdot b'$$

И перейдем обратно к классам:

$$a + b \underset{m}{\equiv} a' + b',\ a \cdot b \underset{m}{\equiv} a' \cdot b' \implies \overline{a + b} = \overline{a' + b'}, \quad \overline{a \cdot b} = \overline{a' \cdot b'}$$

Пример. $m = 4,\ \mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

***Определение* 4.4.** $e \in M$ — *нейтральный элемент* относительно операции $*$ на M, если $\forall a \in M$ справедливо $a * e = e * a = a$.

Предложение 4.2. Операции сложения и умножения на $\mathbb{Z}/m\mathbb{Z}$ обладают следующими свойствами:

$\forall A,\ B,\ C \quad \exists A'$:

1. $A + B = B + A$ — коммутативность сложения
2. $(A + B) + C = A + (B + C)$ — ассоциативность сложения
3. $A + \overline{0} = A$— существование нейтрального элемента относительно сложения
4. $A + A' = \overline{0}$ — существование обратного элемента относительно сложения
5. $AB = BA$ — коммутативность умножения
6. $(AB)C = A(BC)$ — ассоциативность умножения
7. $A \cdot \overline{1} = A$ — существование нейтрального элемента относительно умножения
8. $A \cdot (B + C) = A \cdot B + A \cdot C$ — дистрибутивность умножения относительно сложения.
9. $(B + C) \cdot A = B \cdot A + C \cdot A$ — дистрибутивность сложения относительно умножения.

***Определение* 4.5.** *Кольцом* называется множество M с операциями сложения и умножения, для которых выполнены аналоги свойств 1-4 и 8-9.

***Определение* 4.6.** Кольцо *коммутативное*, если выполнено свойство 5.

***Определение* 4.7.** Колько *ассоциативное*, если выполнено свойство 6.

***Определение* 4.8.** Кольцо *с единицей*, если выполнено свойство 7.

***Определение* 4.9.** Я оставлю это для полноты картины, но wtf is this?
~~$\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R} : x + y = n \implies n$ — нейтральный элемент относительно сложения.~~

Замечание. Если $*$ — операция на M, то существует единственный нейтральный элемент относительно $*$.

Доказательство. $e,\ e'$ — нейтральные элементы относительно $*$, тогда $e = e * e' = e'$.

Типа просто в определение нейтрального элемента подставили и получилось.

Предложение 4.3. В нашем курсе все кольца будут ассоциативные с единицей.

Лемма 4.1. В любом кольце $0 \cdot a = 0$.

Доказательство.

Предположим противное. Покажем, что $0 \cdot a + 0 \cdot a = 0 \cdot a$.

$$0 + 0 = 0 \overset{\exists 0}{\Longrightarrow} (0 + 0) \cdot a = 0 \cdot a \overset{\text{дистр.}}{\Longrightarrow} 0 \cdot a + 0 \cdot a = 0 \cdot a$$

Теперь вычтем $0 \cdot a$. Так как $\exists b : \ b + (0 \cdot a) = 0$, то

$$0 = b + (0 \cdot a) = b + (0 \cdot a + 0 \cdot a) = (b + 0 \cdot a) + (0 \cdot a) = 0 + (0 \cdot a) = 0 \cdot a$$

Противоречие.

***Определение* 4.10.** A^* — множество обратимых элементов кольца A (по умножению, разумеется).

Примеры.

- $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$
- $\mathbb{Z}^* = \{-1, 1\}$
- $(\mathbb{Z}/4\mathbb{Z})^* = \{\overline{1}, \overline{3}\}$
- $(\mathbb{Z}/5\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

***Определение* 4.11.** *Полем* называется коммутативное кольцо F, такое что $F^* = F \setminus \{0\}$.

5 Наибольший общий делитель

***Определение* 5.1.** R — коммутативное кольцо, $a, b \in R$.

Элемент d называется наибольшим общим делителем, если:

1. $d \mid a,\ d \mid b$
2. $d' \mid a,\ d' \mid b \implies d' \mid d$

Предложение 5.1.

1. $d_1,\ d_2$ — наибольшие общие делители, тогда $d_1 \sim d_2$.
2. $\exists d_1$ — наибольший общий делитель, $d_2 \sim d_1$, тогда d_2 — тоже наибольший общий делитель.

Доказательство.

1. По свойству $2: d_1 \mid d_2,\ d_2 \mid d_1 \implies d_1 \sim d_2$.
2. $d_2 \mid d_1,\ d_1 \mid a,\ d_1 \mid b \implies d_2 \mid a,\ d_2 \mid b$

   Пусть d_2 не наибольший, тогда $\exists d' > d_2$.

   $d' \mid a,\ d' \mid b \implies d' \mid d_1$, так как d_1 наибольший общий делитель,

   $d' \mid d_1,\ d_1 \mid d_2 \implies d' \mid d_2$, противоречие, так как $d' > d_2$.

Предложение 5.2. $\exists a, b \in \mathbb{Z} \implies$

1. $\exists d \in \mathbb{Z}:\ a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, иначе говоря: $\forall x, y \in \mathbb{Z}\ \exists d, z \in \mathbb{Z} : ax + by = dz$
2. при этом d — наибольший общий делитель a, b.

Доказательство.

1. Пусть $I = a\mathbb{Z} + b\mathbb{Z}$.

   Заметим что $0 \in I$, так как $0a + 0b = 0$.

   Если $I = \{0\}$, то $I = 0\mathbb{Z}$.

   Иначе $I \neq \{0\} \implies c \in I \implies -c \in I$, так как $-(ax + by) = a \cdot -x + b \cdot -y$

   То есть в I есть положительные числа.

Пусть $d = \min\{c \mid c \in I,\ c > 0\}$, и докажем что $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

«$\supset$»:

$d \in I$ (по определению) $\implies d = ax_0 + by_0, \quad x_0, y_0 \in \mathbb{Z} \implies$

$\forall z \in \mathbb{Z}:\ dz = a(x_0 z) + b(y_0 z) \in I$, значит $d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$

«$\subset$»:

$\exists c \in I,\ d \in \mathbb{N} \implies \exists q, r \in \mathbb{Z}:\ c = dq + r, \quad 0 \leqslant r < d$

$c \in I$, значит $c = ax_1 + by_1, \quad x_1, y_1 \in \mathbb{Z}$

Мы уже знаем, что $d \in I$, значит $d = ax_0 + by_0, \quad x_0, y_0 \in \mathbb{Z}$

$r = c - dq = a(x_1 - x_0 q) + b(y_1 - y_0 q) \in I$

По определению остатка: $\begin{cases} r \geqslant 0, \\ r < d \end{cases}$, но $d = \min\{c \mid c \in I,\ c > 0\} \implies$

$\implies c \in d\mathbb{Z} \implies a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$

2. Пусть d — наибольший общий делитель a, b.

   $a = a1 + b0 \in I = d\mathbb{Z} \implies d \mid a$

   $b = a0 + b1 \in I = d\mathbb{Z} \implies d \mid b$

   $\exists d' \mid a,\ d' \mid b,\ d = ax_0 + by_0$

   $d' \mid ax_0,\ d' \mid by_0 \implies d' \mid d$, значит d действительно наибольший общий делитель a, b.

Следствие.

1. $a, b \in \mathbb{Z}$: Тогда наибольший общий делитель a, b существует.
2. Если d — наибольший общий делитель a, b, то $\exists x, y \in \mathbb{Z}:\ d = ax + by \quad$ (*Линейное представление наибольшего общего делителя*).

Доказательство.

1. Доказали в двух частях предложения.
2. Из первой части знаем, что существует d_0 — наибольший общий делитель a, b, то есть $d_0 = ax_0 + by_0$

   d ассоциирован с $d_0 \implies d = d_0\mathbb{Z},\ z \in \mathbb{Z} \implies d = a(x_0 z) + b(y_0 z)$

***Определение* 5.2.** НОД$(a, b) \iff \gcd(a, b)$ — неотрицательный наибольший общий делитель a, b.

Предложение 5.3. $\exists a_1, a_2, b \in \mathbb{Z}:\ a_1 \underset{b}{\equiv} a_2$

Тогда $\gcd(a_1, b) = \gcd(a_2, b)$.

Доказательство. (!) $\{c : c \mid a_1,\ c \mid b\} = \{c : c \mid a_2,\ c \mid b\}$

«$\subset$»:

$a_2 - a_1 = bm \implies a_2 = a_1 + bm$

$c \mid a_1,\ c \mid b \implies c \mid a_2$

«$\supset$»:

$a_1 - a_2 = bm \implies a_1 = a_2 + bm$

$c \mid a_2,\ c \mid b \implies c \mid a_1$

Получается, что:

$\forall x \in \{c : c \mid a_1, c \mid b\} :\ x \mid \gcd(a_1, b)$

$\forall x \in \{c : c \mid a_2, c \mid b\} :\ x \mid \gcd(a_2, b)$

$\gcd(a_1, b) = \gcd(a_2, b)$

***Определение* 5.3.** Алгоритм Евклида

$\gcd(a, b) = \gcd(b, a \mod b)$, если $b \neq 0$

```
int gcd(int a, int b) {
    if (b == 0) return a;
    return gcd(b, a % b);
}
```

6 Взаимно простые числа

***Определение* 6.1.** Числа a и b называются взаимно простыми, если $\gcd(a, b) = 1$.

Предложение 6.1.

1. $\exists a, b \in \mathbb{Z}$, тогда $a \perp b \iff \exists m, n \in \mathbb{Z} : am + bn = 1$.
2. $a_1 \perp b, a_2 \perp b \implies a_1 a_2 \perp b$.
3. $a_1, \ldots, a_m, b_1, \ldots, b_n \in \mathbb{Z}$ и $\forall i, j : a_i \perp b_j \implies a_1 \ldots a_m \perp b_1 \ldots b_n$.
4. $a \mid bc,\ a \perp b \implies a \mid c$.
5. $ax \underset{m}{\equiv} ay,\ a \perp m \implies x \underset{m}{\equiv} y$.
6. $\gcd(a, b) = d \implies a = da',\ b = db', a' \perp b'$.

Доказательство.

1. m и n существуют согласно линейному представлению НОД.

   $d = \gcd(a, b), d \mid a, d \mid b \implies d \mid (am + bn) = 1 \implies d \mid 1 \implies d = 1$.
2. $1 = a_1 m_1 + b n_1, 1 = a_2 m_2 + b n_2 \implies 1 = a_1 a_2 (m_1 m_2) + b(a_1 m_1 n_2 + a_2 m_2 n_1 + b n_1 n_2) \implies a_1 a_2 \perp b$.
3. $a_1 \perp b, \ldots,\ a_n \perp b \implies a_1 \ldots a_n \perp b$

   $a_1 \ldots a_n \perp b_1, \ldots,\ a_1 \ldots a_n \perp b_n \implies a_1 \ldots a_n \perp b_1 \ldots b_n$
4. $1 = am + bn, c = acm + bcn$

   $a \mid acm,\ a \mid bcn \implies a \mid c$.
5. $m \mid (ax - ay), a \perp m \implies m \mid (x - y) \implies x \underset{m}{\equiv} y$.

6. $d \mid a, d \mid b \implies a = da',\ b = db' : a', b' \in \mathbb{Z}$

   $d = am + bn,\ m, n \in \mathbb{Z}$

   $d = 0 \implies a' = b' = 0 = da'm + db'm$

   $d \neq 0 \implies 1 = a'm + b'n \implies a' \perp b'.$

7 Линейные диофантовы уравнения

***Определение* 7.1.** Линейным диофантовым уравнением с двумя неизвестными называется уравнение вида $ax + by = c$, где $a, b, c \in \mathbb{Z}$.

Решение уравнения - множество всех пар $(x, y) \in \mathbb{Z}^2 : ax + by = c$.

Если $\gcd(a, b) \nmid c$, то решение — пустое множество, так как все линейные комбинации a, b делятся на $\gcd(a, b)$.

Теперь заметим сдедующее: если $ax_1 + by_1 = c$ и $ax_2 + by_2 = c$, то $a(x_1 - x_2) + b(y_1 - y_2) = 0$.

Иными словами, разность двух решений линейного диофантова уравнения - решение соответствующего однородного уравнения.

А значит все решения линейного диофантова уравнения можно найти, решив однородное уравнение и прибавив ко всем его решениям какое-то решение исходного уравнения.

Решим однородное уравнение:

$$ax + by = 0 \iff ax = -by \overset{\text{поделим a, b на их gcd}}{\iff} a'gcd(a,b)x = -b'gcd(a,b)y \iff a'x = -b'y \overset{(\star)}{\iff} \begin{cases} x = b'k \\ y = -a'k \end{cases} \quad k \in \mathbb{Z}$$

$(\star)\ \gcd a', b' = 1 \implies a' \mid y,\ b' \mid x \implies x = b'k,\ k \in \mathbb{Z} \implies y = -a'k$

Теперь найдём какое-то решение исходного уравнения, вспомнив о линейном представлении gcd:

$\gcd(a, b) = ax_0 + by_0 \implies c = c' \gcd(a, b) = a(c'x_0) + b(c'y_0)$

Такимо образом, решение исходного уравнения:

$\{(c'x_0 + b'k, c'y_0 - a'k) \mid k \in \mathbb{Z}\}$, где x_0, y_0 - коэффициенты при a, b в линейном представлении $\gcd(a, b)$, $a' = \frac{a}{\gcd(a,b)}$, $b' = \frac{b}{\gcd(a,b)}$, $c' = \frac{c}{\gcd(a,b)}$

TODO: Вставить код

8 Простые числа

***Определение* 8.1.** Число $p \in \mathbb{Z}$ называется простым, если $p \notin \{-1, 0, 1\}$ и все делители p — это ± 1 и p.

Свойства.

1. p — простое $\iff -p$ — простое.
2. p — простое, $a \in \mathbb{Z} \implies p | a$ или $p \perp a$.
3. p, q — простые $\implies p, q$ — ассоциированны или $p \perp q$.
4. $p \mid ab \implies p \mid a$ или $p \mid b$.

Предложение 8.1. $\exists a \neq \pm 1$, тогда существует простое число $p : p \mid a$.

Доказательство. $a = 0 \implies p = 239$

$a = 1 \implies a > 0$

Индукция по a:

a — простое $\implies p = a, p \mid a$

a — не простое, $\exists d : 1 < d < a, d \mid a$

$a = dd'$, тогда по индукционному переходу существует простое число $p : p \mid d$

$p \mid d, d \mid a \implies p \mid a$

***Определение* 8.2.** Составное число — это число отличное от 0, и не являющееся простым.

Решето Эратосфена

2, 3, 4, 5, 6, 7, 8, 9, …, 100

- 2 — простое, вычеркиваем все числа кратные 2
- 3 — простое, вычеркиваем все числа кратные 3
- 4 — составное, пропускаем
- и т. д.

Теорема 8.1. (Теорема Евклида) Существует бесконечно много простых чисел

Доказательство. $\exists p_1, p_2, \dots p_n$ — все простые числа

$N = p_1 p_2 \dots p_n + 1 \implies$

$\exists$ простое число $p : p \mid N, p > 0 \implies \exists j : p = p_j \implies p \mid (N - 1) \implies p \mid 1 \implies p = \pm 1$

Противоречие

9 Основная теорема арифметики

Теорема 9.1. $\exists n \geqslant 2$. Тогда n можно представить в виде произведения простых чисел, и такое представление единственно с точностью до порядка сомножителей.

Доказательство.

Существование:

$\exists n_0$ — наименьшее число ($\geqslant 2$), для которого такого представления нету.

n_0 — составное число $\implies n_0 = ab, 2 \leqslant a, b < n_0$

По минимальности $\implies a = p_1 \dots p_k, b = q_1 \dots q_l$, все p_i, q_j — простые.

$\implies n_0 = p_1 \dots p_k q_1 \dots q_l$ — Противоречие

Единственность:

$n = p_1 \dots p_k = q_1 \dots q_l$, p_i, q_j — простые.

Нудно доказать: $k = l,\ q_1, \ldots, q_k$ совпадают с $p_1, \ldots, p_k$ с точностью до порядка.

Не умаляя общности иожно считать: $k \leqslant l$.

Индукция по k:

$k = 1$: $p_1 = q_1 \ldots q_l$, p_1 — простое $\implies l = 1, p_1 = q_1$

k > 1: $p_k \mid n \implies p_k \mid (q_1 \ldots q_l) \implies \exists j : p_k \mid q_j \implies p_k \sim q_j \implies p_k = q_j \implies$

$p_1 \ldots p_{k-1} = q_1 \ldots \hat{q}_j \ldots q_l,\ k - 1 \leqslant l - 1$

$k - 1 < k \implies$ применим индукционный переход:

$k - 1 = l - 1$ и $q_1, \ldots, \hat{q}_j, \ldots, q_k$ — это $p_1, \ldots, p_{k-1}$ с точностью до порядка. $\implies$

$q_1, \ldots, (q_j = p_k), \ldots, q_k$ — это $p_1, \ldots, p_k$ с точностью до порядка.

***Определение* 9.1.** Каноническое разложение(факторизация) числа n — это представление n в виде $p_1^{r_1} \ldots p_s^{r_s}$, где p_i — разложение n на простые множители, $r_i \in \mathbb{N}$

Примеры.

- $n = 112 = 2^4 \cdot 7$
- $n = 6006 = 2^1 \cdot 3^1 \cdot 7^1 \cdot 11^1 \cdot 13^1$

Предложение 9.1. $\exists a = p_1^{r_1} \ldots p_s^{r_s}, b = p_1^{t_1} \ldots p_s^{t_s}$

Тогда $a \mid b \iff r_i \leqslant t_i\ \forall i \in \{1, \ldots, s\}$

Доказательство. "$\Rightarrow$":

$b = a \cdot p_1^{t_1 - r_1} \ldots p_s^{t_s - r_s}$

"$\Leftarrow$":

$b = ac\ c = p_1^{m_1} \ldots p_s^{m_s} p_{s+1}^{m_{s+1}} \ldots p_n^{m_n}$

$p_1^{t_1} \ldots p_s^{t_s} = p_1^{r_1 + m_1} \ldots p_s^{r_s + m_s} p_{s+1}^{m_{s+1}} \ldots p_n^{m_n} \implies$

$t_i = r_i + m_i\ \forall i \in \{1, \ldots, s\}, m_{s+1} = \ldots = m_n = 0 \implies t_i \geqslant r_i\ \forall i \in \{1, \ldots, s\}$

Следствие. $\exists a = p_1^{r_1} \ldots p_s^{r_s}$

Тогда $\{d > 0 : d \mid a\} = \{p_1^{t_1} \ldots p_s^{t_s} \mid 0 \leqslant t_i \leqslant r_i,\ \forall i \in \{1, \ldots, s\}\}$

Следствие. $\exists a = p_1^{r_1} \ldots p_s^{r_s},\ b = p_1^{t_1} \ldots p_s^{t_s}$

Тогда $\gcd(a, b) = p_1^{min(r_1, t_1)} \ldots p_s^{min(r_s, t_s)}$

***Определение* 9.2.** $\exists a, b \in \mathbb{Z}$. Число $c \in \mathbb{Z}$ называется наименьшим общим кратным чисел a и b, если

1. $a \mid c, b \mid c$
2. Если $a \mid c', b \mid c'$, то $c \mid c'$

Предложение 9.2. $\exists a = p_1^{r_1} \dots p_s^{r_s}, b = p_1^{t_1} \dots p_s^{t_s}$

Тогда $c = p_1^{max(r_1,t_1)} \dots p_s^{max(r_s,t_s)}$ — наименьшее общее кратное чисел a и b

Доказательство. $a \mid c, b \mid c$ — очевидно

$\exists a \mid c', b \mid c', c' = p_1^{m_1} \dots p_s^{m_s} p_{s+1}^{m_{s+1}} \dots p_n^{m_n}$

$a \mid c',\ b \mid c' \implies r_i \leqslant m_i,\ t_i \leqslant m_i,\ \forall i \in \{1, \dots, s\} \implies$

$max(r_i, t_i) \leqslant m_i,\ \forall i \in \{1, \dots, s\} \implies c \mid c'$

***Определение* 9.3.** НОК$(a, b) = \operatorname{lcm}(a, b)$ — положительное значение наименьшего общего кратного чисел a и b.

Следствие. $\exists a, b \in \mathbb{N}$

Тогда $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = ab$

Доказательство. $min(r_i, t_i) + max(r_i, t_i) = r_i + t_i$

10 Китайская теорема об остатках

Теорема 10.1. Пусть $(m_1, m_2) = 1$; $a_1, a_2 \in \mathbb{Z}$.

1. $\exists x \in \mathbb{Z}$: $\begin{cases} x_0 \underset{m_1}{\equiv} a_1 \\ x_0 \underset{m_2}{\equiv} a_2 \end{cases}$
2. $\exists x_0$ удовлетворяет системе выше

   Тогда для $x \in \mathbb{Z}$: x удовлетворяет системе выше $\iff x \underset{m_1 m_2}{\equiv} x_0$

Доказательство.

1. $x_0 = a_1 + km_1 = a_2 + lm_2 \implies km_1 - lm_2 = a_2 - a_1$ — линейное диофантово уравнение с дыумя неизвестными k, l

   $(m_1, m_2) = 1 \implies$ у него есть решение (k_0, l_0)

   $x_0 = a_1 + k_0 m_1$ — искомое
2. "$\Rightarrow$": $x \underset{m_1 m_2}{\equiv} x_0 \implies \begin{cases} x \underset{m_1}{\equiv} x_0 \\ x \underset{m_2}{\equiv} x_0 \end{cases} \implies \begin{cases} x \underset{m_1}{\equiv} a_1 \\ x \underset{m_2}{\equiv} a_2 \end{cases}$

   "$\Leftarrow$": x удовлетворяет системе из теоремы $\implies \begin{cases} x \underset{m_1}{\equiv} x_0 \\ x \underset{m_2}{\equiv} x_0 \end{cases} \implies \begin{cases} m_1 \mid (x - x_0) \\ m_2 \mid (x - x_0) \end{cases} \implies$
   $m_1 m_2 \mid (x - x_0)$

***Определение* 10.1.** $\exists R, S$ — кольца с единицей. Отображение $\varphi : R \to S$ называется изоморфизмом колец, если: φ биекция.

1. $\forall r_1, r_2 : \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$
2. $\forall r_1, r_2 : \varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$

Предложение 10.1. $\exists (m_1, m_2) = 1$

Тогда существует изоморфизм

$\mathbb{Z}/m_1m_2\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$

$[a]_{m_1m_2} \mapsto ([a]_{m_1}, [a]_{m_2})$

Доказательство. Проверим корректность:

$$\exists [a]_{m_1m_2} = [a']_{m_1m_2} \implies a \underset{m_1m_2}{\equiv} a' \implies \begin{cases} a \underset{m_1}{\equiv} a' \\ a \underset{m_2}{\equiv} a' \end{cases} \implies ([a]_{m_1}, [a]_{m_2}) = ([a']_{m_1}, [a']_{m_2})$$

$\varphi([a]_{m_1m_2} + [b]_{m_1m_2}) = \varphi([a+b]_{m_1m_2}) = ([a+b]_{m_1}, [a+b]_{m_2}) =$

$([a]_{m_1}, [a]_{m_2}) + ([b]_{m_1}, [b]_{m_2}) = \varphi([a]_{m_1m_2}) + \varphi([b]_{m_1m_2})$

Для умножения аналогично.

φ - отображение между конечными равномощными множествами, поэтому оно биективно $\iff$ оно сюръективно $\iff$ оно инъективно.

Действительно, если $\varphi : A \to B,\ |A| = |B| < \infty$ инъективно, то полный прообраз любого элемента из B состоит из не более чем одного элемента из A (определение инъективности).

А если сложить количества прообразов у всех элементов из B, то должно получиться в точности $|A|$, так как каждый прообраз - чей-то образ.

Но тогда каждый прообраз состоит из в точности одного элемента, т. е. φ - биекция.

Аналогично можно рассуждать и про сюрьективное отображение.

Проверим сюръективность φ

По китайской теореме об остатках $\forall a_1, a_2 \in \mathbb{Z}\ \exists a \in \mathbb{Z} : \begin{cases} a \underset{m_1}{\equiv} a_1 \\ a \underset{m_2}{\equiv} a_2 \end{cases}$

Таким образом φ - биекция.

11 Функция Эйлера

Предложение 11.1. $\exists m \in \mathbb{N};\ a \in \mathbb{Z}$

$[a]_m \in (\mathbb{Z}/m\mathbb{Z})^* \iff (a, m) = 1$

Доказательство.

$[a]_m \in (\mathbb{Z}/m\mathbb{Z})^* \iff \exists [b]_m :\ [a]_m \cdot [b]_m = [1]_m \iff$

$\exists b \in \mathbb{Z} :\ ab \underset{m}{\equiv} 1 \iff$

$\exists b, c \in \mathbb{Z} :\ ab = 1 + mc \iff$

$\exists b, c \in \mathbb{Z} :\ ab - mc = 1 \iff (a, m) = 1$

Следствие. $\mathbb{Z}/m\mathbb{Z}$ - поле $\iff$ m — простое число.

Доказательство. считаем $m \geqslant 1$

$m = 1$: $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$

m — простое: $(a, m) = 1$ для $\forall a \in \{1, 2, \ldots, m-1\} \implies$

$(\mathbb{Z}/m\mathbb{Z})^* = \{\overline{1}, \overline{2}, \ldots, \overline{m-1}\}$

m — составное: $m = ab,\ 2 \leqslant a \leqslant m-1$

$(a, m) \neq 1 \implies \overline{a} \notin (\mathbb{Z}/m\mathbb{Z})^*$

***Определение* 11.1.** $\mathbb{F}_n$ — поле из n элементов.

Предложение 11.2. $\mathbb{F}_n$ — поле из n элементов $\iff n = p^r,\ p \in \mathbb{P},\ r \in \mathbb{Z}_+$.

p - характеристика $\mathbb{F}_n$.

Доказательство. **TODO:** Пока без доказательства.

***Определение* 11.2.** $\exists m \in \mathbb{N} : \varphi(n) = |(\mathbb{Z}/m\mathbb{Z})^*|$

Функция $\varphi \times \mathbb{N} \to \mathbb{N}$ — функция Эйлера.

Предложение 11.3. $\exists p \in \mathbb{P},\ r \in \mathbb{N}$.

Тогда $\varphi(p^r) = p^r - p^{r-1}$.

Доказательство. $\varphi(p^r) = |\{a \mid 0 \leqslant a \leqslant p^r - 1,\ (a, p^r) = 1\}| =$

$p^r - |\{a \mid 0 \leqslant a \leqslant p^r - 1,\ (a, p) \neq 1\}| =$

$p^r - |\{a \mid 0 \leqslant a \leqslant p^r - 1,\ p \mid a\}| = p^r - p^{r-1}$

Предложение 11.4. Мультипликативность функции Эйлера.
$\exists m, n \in \mathbb{N},\ (m, n) = 1$.

Тогда $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Доказательство. Построим отображение $\lambda : (\mathbb{Z}/mn\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$:

$[a]_{mn} = A \in (\mathbb{Z}/mn\mathbb{Z})^* \mapsto ([a]_m, [a]_n)$

$$[a]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^* \implies (a, mn) = 1 \implies \begin{cases} (a, m) = 1 \\ (a, n) = 1 \end{cases} \quad \begin{cases} [a]_m \in (\mathbb{Z}/m\mathbb{Z})^* \\ [a]_n \in (\mathbb{Z}/n\mathbb{Z})^* \end{cases}$$

Проверка корректности:

$$[a]_{mn} = [a']_{mn} \implies a \underset{mn}{\equiv} a' \implies \begin{cases} a \underset{m}{\equiv} a' \\ a \underset{n}{\equiv} a' \end{cases} \implies \begin{cases} [a]_m = [a']_m \\ [a]_n = [a']_n \end{cases} \implies ([a]_m, [a]_n) = ([a']_m, [a']_n)$$

Проверим что λ — биекция:

Инъективность:

$$\lambda([a]_{mn}) = \lambda([b]_{mn}) \implies \begin{cases} [a]_m = [b]_m \\ [a]_n = [b]_n \end{cases} \overset{\text{КТО}}{\implies} a \underset{mn}{\equiv} b \implies [a]_{mn} = [b]_{mn}$$

Сюръективность:

Рассмотрим $([b]_m, [c]_n) \in (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$.

$(m,n) = 1 \overset{\text{КТО}}{\Longrightarrow} \exists a : \begin{cases} a \underset{m}{\equiv} b \\ a \underset{n}{\equiv} c \end{cases}$

$\begin{cases} (b,m) = 1 \implies (a,m) = 1 \\ (c,n) = 1 \implies (a,n) = 1 \end{cases} \implies (a, mn) = 1 \implies [a]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^*$

$\lambda([a]_{mn}) = ([a]_m, [a]_n) = ([b]_m, [c]_n) \implies \lambda$ — биекция.

λ — биекция $\implies |(\mathbb{Z}/mn\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*| \implies \varphi(mn) = \varphi(m) \cdot \varphi(n)$

Следствие. $\exists m_1, \ldots, m_k$ — попарно взаимно простые числа.

Тогда $\varphi(\prod\limits_{i=1}^{k} m_i) = \prod\limits_{i=1}^{k} \varphi(m_i)$.

Доказательство. Индукция по k.

База: $k = 1 \implies \varphi(m_1) = \varphi(m_1)$

Переход: $n - 1 \to n$

$(m_n, m_1) = \ldots = (m_n, m_{n-1}) = 1 \implies (m_1, \ldots, m_n) = 1 \implies$

$\varphi(m_1 \ldots m_n) = \varphi(m_1 \ldots m_{n-1})\varphi(m_n) = \varphi(m_1) \ldots \varphi(m_{n-1})\varphi(m_n)$

Следствие. $\exists n = p_1^{r_1}, \ldots, p_s^{r_s}$ — разложение числа n на простые множители.

$\implies \varphi(n) = \prod\limits_{i=1}^{s} (p_i^{r_i} - p_i^{r_i - 1})$

Доказательство. По следствию: $\varphi(n) = \varphi(\prod\limits_{i=1}^{s} p_i^{r_i}) = \prod\limits_{i=1}^{s} \varphi(p_i^{r_i}) = \prod\limits_{i=1}^{s} (p_i^{r_i} - p_i^{r_i - 1})$

Теорема 11.1. $\exists m \in \mathbb{N}, a \in \mathbb{Z}, (a,m) = 1 \implies a^{\varphi(m)} \underset{m}{\equiv} 1$ — теорема Эйлера.

Лемма 11.1.

Пусть R — ассоциативное кольцо с единицей.

1. $a, b \in R^* \implies ab \in R^*$
2. $a \in R^*,\ x, y \in R \implies ax = ay \implies x = y,\ xa = ya \implies x = y$

Доказательство.

1. a' — обратный к a элемент, b' — обратный к b элемент.

   $(ab)(b'a') = a(bb')a' = aa' = 1$

   $(b'a)(ab) = b'(aa')b = bb' = 1$

2. a' — обратный к a элемент.

   $ax = ay \implies a'ax = a'ay \implies x = y$

$xa = ya \implies xaa' = yaa' \implies x = y$

Доказательство. (теоремы Эйлера)

$(\mathbb{Z}/m\mathbb{Z})^* = \{A_1, A_2, \dots, A_{\varphi(m)}\}$

$[a]_m A_j \in (\mathbb{Z}/m\mathbb{Z})^* \overset{lemma-1}{\implies}$

$[a]_m A_1, \dots, [a]_m A_{\varphi(m)}$ — различные элементы

$([a]_m A_j = [a]_m A_k \overset{lemma-2}{\implies} A_j = A_k) \implies$

$\{[a]_m A_1, \dots, [a]_m A_{\varphi(m)}\} = (\mathbb{Z}/m\mathbb{Z})^* \implies$

$[a]_m A_1 \cdot \ldots \cdot [a]_m A_{\varphi(m)} = A_1 A_2 \dots A_{\varphi(m)} \implies$

$[a]_m^{\varphi(m)} A_1 A_2 \dots A_{\varphi(m)} = [1]_m A_1 A_2 \dots A_{\varphi(m)} \overset{lemma-2}{\implies}$

$[a]_m^{\varphi(m)} = [1]_m \implies [a^{\varphi(m)}]_m = [1]_m \implies a^{\varphi(m)} \underset{m}{\equiv} 1$

Теорема 11.2. (Малая теорема Ферма)

$\exists p \in \mathbb{P}, a \in \mathbb{Z} \implies a^p \underset{p}{\equiv} a$

Доказательство.

$(a, p) = 1 \implies a^{p-1} \underset{p}{\equiv} 1 \implies a^{p-1} a \underset{p}{\equiv} 1a \implies a^p \underset{p}{\equiv} a$

$(a, p) \neq 1 \implies a \underset{p}{\equiv} 0 \implies a^p \underset{p}{\equiv} 0 \implies a^p \underset{p}{\equiv} a$

Теорема 11.3. (Теорема Вильсона)

$p \in \mathbb{P} \implies (p-1)! \underset{p}{\equiv} -1$

Доказательство.

В $(\mathbb{Z}/m\mathbb{Z})^*$

$\overline{(p-1)!} = \overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{p-1} = \prod\limits_{A \in (\mathbb{Z}/m\mathbb{Z})^*} A = \prod\limits_{A^2 = \overline{1}} A \cdot \prod\limits_{A^2 \neq \overline{1}} A = (\prod\limits_{A^2 = \overline{1}} A) \cdot (A_1 \cdot A_1' \cdot \ldots) = (\prod\limits_{A^2 = \overline{1}} A) \cdot \overline{1} = \prod\limits_{A^2 = \overline{1}} A$

$A^2 = \overline{1} \iff A^2 - \overline{1}^2 = \overline{0} \iff (A - \overline{1})(A + \overline{1}) = \overline{0} \overset{\mathbb{Z}/p\mathbb{Z}-\text{ОЦ}}{\iff} A - \overline{1} = \overline{0}$ или $A + \overline{1} = \overline{0} \implies$
$$\begin{cases} p = 2 & \prod\limits_{A^2 = \overline{1}} A = \overline{1} = \overline{-1} \\ p \neq 2 & \prod\limits_{A^2 = \overline{1}} A = \overline{-1} \end{cases}$$

2 Комплексные числа

1 Построение поля комплексных чисел

***Определение* 1.1.** $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}$

***Определение* 1.2.**

- Сложение на $\mathbb{C}$: $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$
- Умножение на $\mathbb{C}$: $(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)$

Предложение 1.1. $(\mathbb{C}, +, \cdot)$ - поле.

Доказательство.

- Коммутативность сложения — очевидно.
- Ассоциативность сложения — очевидно.
- $(0, 0)$ — нейтральный элемент сложения.
- $(-a, -b)$ — обратный элемент к (a, b).
- Коммутативность умножения — очевидно.
- Ассоциативность умножения — проверяется.
- Дистрибутивность — проверяется.
- $(1, 0)$ — нейтральный элемент умножения.
- $(a, b)z_1z_2 = (1, 0):\ z_1 = (a, -b),\ z_2 = \frac{1}{a^2+b^2}$

***Определение* 1.3.** $\mathbb{C}$ — поле комплексных чисел.

***Определение* 1.4.** $c \in \mathbb{C}$ — комплексное число.

Предложение 1.2. $\mathbb{R}' = \{(a, 0) \mid a \in \mathbb{R}\}$

R' замкнуто относительно сложения, вычитания, умножения, содержит единицу, то есть является подкольцом поля $\mathbb{C}$.

$\implies \mathbb{R}'$ — само является кольцом относительно сложения, умножения, ограниченных на $\mathbb{R}'$.

$\mathbb{R} \xrightarrow{\varphi} \mathbb{R}'(a \mapsto (a, 0))$, $\varphi(a)$ — изоморфизм колец, т.е. φ — биекция и $\varphi(a + b) = \varphi(a) + \varphi(b)$; $\varphi(ab) = \varphi(a)\varphi(b)$.

Отождествим $(a, 0)$ с вещественным числом a.

$(a, 0) \cdot (0, 1) = (0, a)$

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

***Определение* 1.5.** $z = a + bi$ — комплексное число. $a = Re(z)$, $b = Im(z)$ — действительная и мнимая части комплексного числа z. В геометрическом виде это вектор $z = (a, b)$.

***Определение* 1.6.** $z = a + bi$ — комплексное число. $\overline{z} = a - bi$ — сопряженное к z.

***Определение* 1.7.** Автоморфизм — изоморфизм на себя.

Отступление про отображения

***Определение* 1.8.** $id_M : M \to M,\ x \mapsto x$ — тождественное отображение на M.

***Определение* 1.9.** $\exists \alpha : M \to N,\ \beta : N \to P$ — отображения

Тогда $\alpha \circ \beta : M \to P,\ x \mapsto \alpha(\beta(x))$ — композиция отображений.

***Определение* 1.10.** $\exists \alpha : M \to N$ — отображение

Отображение $\beta : N \to M$ — обратное к α, если $\beta \circ \alpha = id_M$.

Предложение 1.3. У отображения $\alpha : M \to N$ есть обратное отображение, если и только если α — биекция.

Доказательство.

"$\Rightarrow$":

Инъективность:

$\beta \circ \alpha = id_M,\ \alpha(x) = \alpha(y) \implies \beta(\alpha(x)) = \beta(\alpha(y)) \implies x = y$

Сюръективность:

$y \in N,\ y = \alpha(\beta(y)) \in Im(\alpha)$(Im это прообраз)

"$\Leftarrow$":

Пусть α — биекция, назовем $\beta : N \to M$ — обратныи, если $\forall y \in N \alpha^{-1}(y) = \{x\},\ x \in M$

Положим $\beta(y) = x,\ \alpha \circ \beta = id_N,\ \beta \circ \alpha = id_M$

Продолжение

Предложение 1.4. $\sigma : \mathbb{C} \to \mathbb{C},\ z \mapsto \overline{z}$ — автоморфизм.

Доказательство.

σ — биекция, т.к. $\sigma \circ \sigma = id_{\mathbb{C}}$

$\sigma(z_1 + z_2) = \sigma(z_1) + \sigma(z_2)$ — очевидно

$\sigma(z_1 z_2) = \sigma(z_1)\sigma(z_2)$

$\sigma(1) = 1$ — очевидно

$z_1 = a_1 + b_1 i,\ z_2 = a_2 + b_2 i$

$\sigma(z_1 z_2) = \overline{a_1 a_2 - b_1 b_2 + i(a_1 b_2 + a_2 b_1)} = a_1 a_2 - b_1 b_2 + i(a_1 b_2 + a_2 b_1)$

$\sigma(z_1)\sigma(z_2) = \overline{(a_1 - ib_1)(a_2 - ib_2)} = a_1 a_2 - b_1 b_2 + i(a_1 b_2 + a_2 b_1)$

2 Тригонометрическая форма комплексного числа

***Определение* 2.1.** $a + bi = r(\cos\varphi + i\sin\varphi)$

$a = r\cos\varphi$

$b = r\sin\varphi$

***Определение* 2.2.** Модулем комплексного числа $z = a + bi \in \mathbb{C}$ назовем:

$|z| = \sqrt{a^2 + b^2}$

Предложение 2.1.

1. $|z| \geqslant 0,\ |z| = 0 \iff z = 0$
2. $|z_1 z_2| = |z_1||z_2|$
3. $|z_1 + z_2| \leqslant |z_1| + |z_2|$
4. $|\overline{z}| = |z|$
5. $z\overline{z} = |z|^2$

Доказательство.

1. очевидно
2. $z_1 = a_1 + b_1 i,\ z_2 = a_2 + b_2 i$

   $|z_1 z_2|^2 = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + a_2b_1)^2 = a_1^2a_2^2 + b_1^2b_2^2 + a_1^2b_2^2 + a_2^2b_1^2 =$

   $(a_1^2 + b_1^2)(a_2^2 + b_2^2) = |z_1|^2|z_2|^2$
3. $\iff |z_1 + z_2|^2 \leqslant (|z_1| + |z_2|)^2$

   $\iff (a_1 + a_2)^2 + (b_1 + b_2)^2 \leqslant a_1^2 + b_1^2 + a_2^2 + b_2^2 + 2|z_1||z_2|$

   $\iff a_1a_2 + b_1b_2 \leqslant \sqrt{(a_1^2 + b_1^2)(a_2^2 + b_2^2)}$

   $\Leftarrow |a_1a_2 + b_1b_2| \leqslant \sqrt{(a_1^2 + b_1^2)(a_2^2 + b_2^2)}$

   $\iff a_1^2a_2^2 + b_1^2b_2^2 + 2a_1a_2b_1b_2 \leqslant (a_1^2 + b_1^2)(a_2^2 + b_2^2)$

   $\iff 2a_1a_2b_1b_2 \leqslant b_1^2a_2^2 + a_1^2b_2^2$

   $\iff (b_1a_2 - b_2a_1)^2 \geqslant 0$
4. очевидно
5. $z = a + bi \implies \overline{z} = a - bi$

   $z\overline{z} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2 = |z|^2$

Замечание. $z^{-1} = \frac{\overline{z}}{|z|^2} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$

***Определение* 2.3.** Пусть $z \in \mathbb{C}$. Аргументом z назовем такое $\varphi \in \mathbb{R}$, что $z = |z|(\cos\varphi + i\sin\varphi)$

Предложение 2.2.

1. Если $z = 0$, то любой $\varphi \in \mathbb{R}$ - аргумент z
2. Если $z \neq 0$, то:
   (a) аргумент существует
   (b) если φ_0 - аргумент z, то φ - аргумент $z \iff \varphi = \varphi_0 + 2\pi k,\ k \in \mathbb{Z}$

Доказательство.

1. тривиально
2. $z_0 = \frac{1}{|z|} \cdot z$

   $|z_0| = \left|\frac{1}{|z|}\right| \cdot |z| = \frac{1}{|z|} \cdot |z| = 1$

   $z_0 = a_0 + ib_0,\ |z_0| = a_0^2 + b_0^2 = 1 \implies \exists \varphi_0 : \begin{cases} a_0 = \cos\varphi_0 \\ b_0 = \sin\varphi_0 \end{cases}$

   $z = |z| \cdot z_0 = |z|(\cos\varphi_0 + i\sin\varphi_0)$

   $\varphi = \varphi_0 + 2\pi k \implies \begin{cases} \cos\varphi = \cos\varphi_0 \\ \sin\varphi = \sin\varphi_0 \end{cases} \implies \varphi$ - аргумент

   φ - аргумент $\implies z = |z|(\cos\varphi + i\sin\varphi) \implies \begin{cases} \cos\varphi = \cos\varphi_0 \\ \sin\varphi = \sin\varphi_0 \end{cases} \implies \varphi - \varphi_0 = 2\pi k,\ k \in \mathbb{Z}$

***Определение* 2.4.** $arg(z) = \varphi$ означает φ - один из аргументов z

Замечание. Предположим оказалось, что $z = r(\cos\varphi + i\sin\varphi)$ для некоторых $r \geqslant 0,\ \varphi \in \mathbb{R}$. Тогда $r = |z|,\ \varphi = \arg z$

Доказательство. $|z| = \sqrt{(r\cos\varphi)^2 + (r\sin\varphi)^2} = \sqrt{r^2} = r \implies \varphi$ - аргумент по определению

Предложение 2.3.

1. $\arg\overline{z} = -\arg z$
2. $z \in \mathbb{R} \iff \arg z = k\pi,\ k \in \mathbb{Z}$
3. $\arg(z_1 z_2) = \arg z_1 + \arg z_2$
4. $\exists z_2 \neq 0 \implies \arg\frac{z_1}{z_2} = \arg z_1 - \arg z_2$

Доказательство.

1. $\arg z = \varphi$

   $z = |z|(\cos\varphi + i\sin\varphi)$

   $\overline{z} = |z|(\cos\varphi - i\sin\varphi) = |\overline{z}|(\cos(-\varphi) + i\sin(-\varphi)) \implies$

   $\arg\overline{z} = -\varphi$
2. "$\Rightarrow$":

   $z > 0$:

$z = |z| \cdot 1 = |z|(\cos 0 + i \sin 0) \implies \arg z = 0$

$z < 0$:

$z = |z| \cdot (-1) = |z|(\cos \pi + i \sin \pi) \implies \arg z = \pi$

"$\Leftarrow$":

$\sin(k\pi) = 0$

3. $\arg z_1 = \varphi_1,\ \arg z_2 = \varphi_2 \implies$

   (!) $\varphi_1 + \varphi_2 = \arg(z_1 z_2)$

   $z_1 = |z_1|(\cos \varphi_1 + i \sin \varphi_1),\ z_2 = |z_2|(\cos \varphi_2 + i \sin \varphi_2) \implies$

   $z_1 z_2 = |z_1| \cdot |z_2|(\cos \varphi_1 \cdot \cos \varphi_2 - \sin \varphi_1 \cdot \sin \varphi_2 + i(\sin \varphi_1 \cdot \cos \varphi_2 + \cos \varphi_1 \cdot \sin \varphi_2)) =$

   $|z_1 z_2|(\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)) \implies \arg(z_1 z_2) = \varphi_1 + \varphi_2$

4. $z_1 = \frac{z_1}{z_2} \cdot z_2 \implies \arg z_1 = \arg \frac{z_1}{z_2} + \arg z_2 \implies \arg \frac{z_1}{z_2} = \arg z_1 - \arg z_2$

Следствие. (Формула Муавра)

Пусть $z \in \mathbb{C},\ |z| = r,\ \arg z = \varphi,\ n \in \mathbb{Z}.$

Тогда $z^n = r^n(\cos(n\varphi) + i \sin(n\varphi))$

Доказательство.

$n > 0$ — индукция по n

База: $n = 1$ — тривиально

Переход: $n - 1 \to n$

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

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

$r^n(\cos((n-1)\varphi + \varphi) + i \sin((n-1)\varphi + \varphi)) =$

$r^n(\cos(n\varphi) + i \sin(n\varphi))$

$n = 0,\ 1 = r^0(\cos(0) + i \sin(0)) = 1$

$n < 0$: $n = -k,\ k \in \mathbb{N}$

$z^n = \frac{1}{z^k}$

$|z^n| = \frac{1}{|z^k|} = \frac{1}{|z|^k} = |z|^{-k} = |z|^n$

$\arg z^n = \arg 1 - \arg z^k = 0 - k\varphi = n\varphi$

3 Корни из комплексных чисел

$z^n = w,\ n \in \mathbb{N},\ w \in \mathbb{C}$

$w = 0 \implies z = 0$

$w \neq 0,\ w = r(\cos \varphi + i \sin \varphi),\ r > 0,\ \varphi \in \mathbb{R},\ z = p(\cos \alpha + i \sin \alpha),\ p > 0,\ \alpha \in \mathbb{R}$

$z^n = w \iff p^n(\cos n\alpha + i\sin n\alpha) = r(\cos\varphi + i\sin\varphi) \iff \begin{cases} p^n = r \\ n\alpha = \varphi + 2\pi k, \ k \in \mathbb{Z} \end{cases} \iff$

$\begin{cases} p = \sqrt[n]{r} \\ \alpha = \frac{\varphi+2\pi k}{n}, \ k \in \mathbb{Z} \end{cases}$

$z^n = w \iff z = \underbrace{\sqrt[n]{r}\left(\cos\dfrac{\varphi+2\pi k}{n} + i\sin\dfrac{\varphi+2\pi k}{n}\right)}_{z_k}, \ k \in \mathbb{Z}$

При каких $k, l : z_k = z_l$?

$z_k = z_l \iff \frac{\varphi+2\pi k}{n} = \frac{\varphi+2\pi l}{n} + 2\pi s, \ s \in \mathbb{Z} \iff \frac{k}{n} + \frac{l}{n} + s, \ s \in \mathbb{Z} \iff$

$k = l + ns, \ s \in \mathbb{Z} \iff k \underset{n}{\equiv} l \iff z \in \{z_0, z_1, \ldots, z_{n-1}\}$

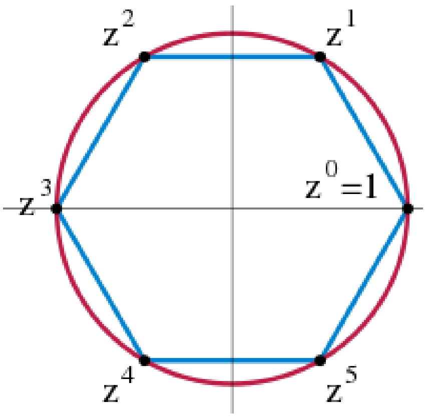
Таким образом, мы доказали:

Теорема 3.1. $\exists n \in \mathbb{N}, \ w \in \mathbb{C}$

1. Если $w = 0$, То уравнение $z^n = w$ имеет единственный корень $z = 0$.
2. Если $w \neq 0$, То уравнение $z^n = w$ имеет ровно n различных корней:

$$z_k = \sqrt[n]{r}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right), \ k = 0, 1, \ldots, n-1$$

Изображение на окружности



Комплексные корни образуют праильный n-угольник на окружности.

Лемма 3.1. Пусть $z_0, z_1, \ldots, z_{n-1}$ — все корни $z^n = w, \ n > 1$

Тогда $z_0 + z_1 + \ldots + z_{n-1} = 0$

Доказательство.

$z_k = z_{k-1}\underbrace{\left(\cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}\right)}_{\xi}$

$S = z_0 + z_1 + \ldots + z_{n-1}$

$z_k = z_0 \cdot \xi^k$

$\xi \cdot S = z_1 + z_2 + \ldots + \underbrace{z_n}_{=z_0} = S \implies (\xi - 1)S = 0$

$n \neq 1 \implies \xi \neq 1$

$(\xi - 1)S = 0 \implies S = 0$

***Определение* 3.1.** Группа — это множество G с операцией $* : G \times G \to G$ такая, что:

1. $*$ — ассоциативна: $(a * b) * c = a * (b * c)$
2. Существует нейтраальный элемент $e \in G$ такой, что $a * e = e * a = a$ для любого $a \in G$
3. У любого элемента $a \in G$ существует обратный элемент $a^{-1} \in G$ такой, что $a * a^{-1} = a^{-1} * a = e$

Примеры.

1. $(\mathbb{Z}, +)$
2. $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$
3. Если R — ассоциативное кольцо с 1, то $R^* = \{r \mid \exists s \in R : rs = sr = 1\}$ — группа относительно умножения.

Проверить замкнутость относительно умножения.

Зафиксируем $n \in \mathbb{N}$

$\mu_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{\underbrace{\cos\dfrac{2\pi k}{n} + i \sin\dfrac{2\pi k}{n}}_{\xi_k} \mid k = 0, 1, \ldots, n-1\}$ — группа относительно умножения

$z, w \in \mu_n \implies zw \in \mu_n$ — замкнутость относительно умножения

$(zw)^n = z^n w^n = 1 \cdot 1 = 1$

Доказательство, что μ_n — группа:

- Ассоциативность — так как есть ассоциативность в $\mathbb{C}$
- $1 \in \mu_n$ $(1 = \xi_0)$
- $\xi_k \cdot \xi_{-k} = \left(\cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}\right)\left(\cos\frac{2\pi(-k)}{n} + i \sin\frac{2\pi(-k)}{n}\right) = 1$

Лемма 3.2. $\xi_k = \xi_1^k$

Доказательство. $\left(1 \cdot \cos\frac{2\pi k}{n} + i \sin\frac{2\pi}{n}\right)^k = 1 \cdot \left(\cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}\right)$ (по формуле Муавра)

***Определение* 3.2.** G — группа с операцией $*$, $g \in G$, $n \in \mathbb{Z}$

$$g^n = \begin{cases} g * g * \ldots * g & n > 0 \\ e & n = 0 \\ g^{-1} * g^{-1} * \ldots * g^{-1} & n < 0 \end{cases}$$

***Определение* 3.3.** Группа G называется циклической, если $\exists g \in G : G = \{g^n \mid n \in \mathbb{Z}\}$

Пишут: $G = \langle g \rangle$

***Определение* 3.4.** g — образующий элемент группы G

Примеры.

- $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ (по сложению) $g^n = \begin{cases} 1 + 1 + \ldots + 1 & n > 0 \\ 0 & n = 0 \\ -1 + -1 + \ldots + -1 & n < 0 \end{cases}$
- $\mathbb{Z}/5\mathbb{Z} = \langle \overline{1} \rangle = \langle \overline{2} \rangle = \langle \overline{3} \rangle = \langle \overline{4} \rangle$ (по сложению)
- $\mathbb{Z}/6\mathbb{Z} = \langle \overline{1} \rangle = \langle \overline{5} \rangle$ (по сложению)
- $(\mathbb{Z}/5\mathbb{Z})^* = \langle \overline{2} \rangle = \langle \overline{3} \rangle$ (по умножению)
- $(\mathbb{Z}/8\mathbb{Z})^*$ — не циклическая группа $g^2 = e \implies g^{2k} = e,\ g^{2k+1} = g$

***Определение* 3.5.** G — группа, $g \in G$

Если $\forall n \in \mathbb{N} : g^n \neq e$, то говорят, что g — бесконечный порядок

Если $\exists n \in \mathbb{N} : g^n = e$, то минимальное такое n называют порядком g (пишут: $\operatorname{ord} g = n$)

Пример. $\mathbb{Z}/5\mathbb{Z}$

$\operatorname{ord} \overline{1} = 1$

$\operatorname{ord} \overline{2} = 4$

$\operatorname{ord} \overline{3} = 4$

$\operatorname{ord} \overline{4} = 2$

Предложение 3.1. Пусть G — конечная группа, $|G| = n,\ g \in G$.

Тогда: $G = \langle g \rangle \iff \operatorname{ord} g = n$

Доказательство. "$\Rightarrow$":

$\exists k, l : g^k = g^l,\ k, l \in \{0, 1, \ldots, n\},\ k \neq l$ (так как G конечная)

$k < l$: $g^{-k} \cdot g^k = g^{-k} \cdot g^l = g^{l-k} = e$

$0 < l - k \leqslant n$

Таким образом, порядок g не превосходит n

Предположим, $\operatorname{ord} g = m < n$

$G = \{g^k \mid k \in \mathbb{Z}\} = \{g^{mq+r} \mid q \in \mathbb{Z},\ 0 \leqslant r < m\} = \{g^0, g^1, \ldots, g^{m-1}\}$ — противоречие, так как $|G| \leqslant m < n$

"$\Leftarrow$":

$\operatorname{ord} g = n$

$\implies g^0, g^1, g^2, \ldots, g^{n-1}$ — они попарно различны

$\implies \{g^0, g^1, \ldots, g^{n-1}\} = G$

$\implies G = \langle g \rangle$

***Определение* 3.6.** Первообразным корнем из 1 степени n называется такой элемент $z \in \mathbb{C}^*$, что $\operatorname{ord} z = n$

Пример. $\mu_6 = \{1, \xi_1, \xi_2, \xi_3, \xi_4, \xi_5\}$

$\operatorname{ord} 1 = 1$, $\operatorname{ord} \xi_1 = 6$, $\operatorname{ord} \xi_2 = 3$, $\operatorname{ord} \xi_3 = 2$, $\operatorname{ord} \xi_4 = 3$, $\operatorname{ord} \xi_5 = 6$

ξ_2 — первообразный корень из 1 степени 3

3 Многочлены

1 Многочлены и формальные степенные ряды

***Определение* 1.1.** Последовательность финитная $\iff \exists N : \forall n \geqslant N : a_n = 0.$

***Определение* 1.2.** Многочленом над R (от одной переменной) называется финитная последовательность $(a_i),\ a_i \in \mathbb{R},\ i = 0, 1, 2, \ldots$.

***Определение* 1.3.** R — коммутативное кольцо с 1.

$R[x] = \{(a_i) \mid a_i \in R, i = 0, 1, \ldots; a_i = 0$ при $i \to \infty\}$ — кольцо многочленов над R.

Введём сложение и умножение на $R[x]$

$(a_i) + (b_i) = (a_i + b_i)$

$(a_i) \cdot (b_i) = (p_i)$, где $p_k = \sum\limits_{i=0}^{k} a_i b_{k-i}$

$\exists a \in R,\ [a] = (a, 0, 0, \ldots)$ — многочлен, равный a.

$[a] + [b] = [a + b]$

$[a] \cdot [boba] = (aboba, 0, 0, \ldots) = [aboba]$

Отождествим $[a]$ с a.

$[a] \cdot (b_0, b_1, \ldots) = (ab_0, ab_1, \ldots)$

$(a_0, a_1, \ldots, a_n, 0, 0, \ldots) = (a_0, 0, 0, \ldots) + (0, a_1, 0, 0, \ldots) + \ldots + (0, 0, \ldots, a_n, 0, 0, \ldots) =$

$a_0 \cdot \underbrace{(1, 0, 0, \ldots)}_{x_0} + a_1 \cdot \underbrace{(0, 1, 0, \ldots)}_{x_1} + \ldots + a_n \cdot \underbrace{(0, 0, \ldots, 1, 0, 0, \ldots)}_{x_n} =$

$a_0 + a_1 \cdot x_1 + \ldots + a_n \cdot x_n$

$x_j \cdot x_1 = (0, \ldots, 1, 0, 0, \ldots) \cdot (0, 1, 0, 0, \ldots) = (0, \ldots, 0, 1, 0, 0, \ldots) = x_{j+1} \implies$

$\forall m \in \mathbb{N} : x_m = x_1^m$

$x_1 = x \implies x_m = x_1^m = x^m$

Значит получили стандартную запись многочленов $(a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n)$

***Определение* 1.4.** $\exists f \in R[x],\ f \neq 0$ (то есть не (0))

Тогда степенью f называется максимальное j такое что $a_j \neq 0$

Обозначим $\deg(f) = j$.

Если $f = 0$, то $\deg(f) \in \{-1, -\infty\}$ (по разному обозначают).

***Определение* 1.5.** $d = \deg f \implies a_d$ называется старшим коэффициентом f.

***Определение* 1.6.** Константой называется множество f такое что $\deg(f) \leqslant 0$.

***Определение* 1.7.** Мономом называется множество вида ax^j.

Предложение 1.1. $R[x]$ — коммутативное ассоциативное кольцо с 1.

Доказательство. Аксиомы относящиеся к сложению очевидны.

Проверим коммутативность умножения и дистрибутивность.

$(f \cdot g) \cdot h = f \cdot (g \cdot h)$ — сводится к сложению, f, g, h — мономы.

$$\begin{cases} (aX^i \cdot bX^j) \cdot cX^k = abX^{i+j} \cdot cX^k = abc \cdot X^{i+j+k} \\ aX^i \cdot (bX^j \cdot cX^k) = aX^i \cdot bcX^{j+k} = abc \cdot X^{i+j+k} \end{cases}$$

$(fg)h = f(gh)$

$f = \sum\limits_{i=0}^{k} f_i,\ g = \sum\limits_{j=0}^{l} g_j,\ h = \sum\limits_{m=0}^{n} h_m$

$(fg)h = (\sum f_i \cdot \sum g_j) \cdot \sum h_k = \sum(f_i \cdot g_j) \cdot \sum h_k \overset{\text{ассоц. для мономов}}{=} \sum f_i \cdot \sum(g_j \cdot h_k) = f(gh)$

***Определение* 1.8.** $R[[x]] = \{(a_i) \mid a_i \in R, i = 0, 1, \ldots\}$ — множество формальных степенных рядов над R.

$(a_i) = \sum\limits_{i=0}^{\infty} a_i X^i$

Упражнение. $R[[x]]$ — коммутативное ассоциативное кольцо с 1.

2 Свойства степени

Предложение 2.1. $f, g \in R[x],\ \deg f = m,\ \deg g = n$

1. $\deg(f + g) \leqslant \max(m, n)$

   При этом: $m \neq n \implies \deg(f + g) = \max(m, n)$
2. $\deg(fg) \leqslant m + n$

Доказательство.

1. $f = \sum\limits_{i=0}^{m} a_i X^i,\ g = \sum\limits_{i=0}^{n} b_i X^i,\ d = \max(m, n)$

   $f = \sum\limits_{i=0}^{d} a_i X^i,\ g = \sum\limits_{i=0}^{d} b_i X^i$

   $f + g = \sum\limits_{i=0}^{d} (a_i + b_i) X^i \implies \deg(f + g) \leqslant d$

   $m \neq n \implies \begin{cases} a_d = 0 \\ b_d \neq 0 \end{cases}$ или $\begin{cases} a_d \neq 0 \\ b_d = 0 \end{cases} \implies a_d + b_d \neq 0 \implies \deg(f + g) = d$
2. $\left(\sum\limits_{i=0}^{m} a_i X^i\right)\left(\sum\limits_{j=0}^{n} b_j X^j\right) = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + \ldots + a_m b_n X^{m+n} \implies \deg fg \leqslant m + n$

Замечание. $\deg fg < m + n$, если $a_m \neq 0$ или $b_n \neq 0$ и $a_m b_n = 0$

Замечание. Будем считать, что $\deg 0 = -\infty$

***Определение* 2.1.** Область целостности (целостное кольцо, область) — коммутативное ассоциативное кольцо с $1 \neq 0$ и без делителей нуля.

$$a \neq 0 \text{ так чтобы } \exists b \neq 0 : ab = 0$$

Предложение 2.2. Пусть R — ОЦ(область целостности).

1. $\forall f, g \in R[x] : \deg(fg) \leqslant \deg f + \deg g$
2. $R[x]$ — ОЦ

Доказательство.

1. В предыдущем доказательстве $\begin{cases} a_m \neq 0 \\ b_n \neq 0 \end{cases} \implies a_m b_n \neq 0 \implies \deg(fg) = m + n$
2. $f \neq 0 \implies \deg f \geqslant 0, \ g \neq 0 \implies \deg g \geqslant 0 \implies \deg(fg) \geqslant 0 \implies fg \neq 0$

Следствие. Пусть R — ОЦ: тогда $R[x]^* = R^*$

Доказательство. Очевидно $R^* \subset R[x]^*$

Обратно, пусть $f \in R[x]^* \implies$

$\exists g \in R[x] : f \cdot g = 1 (\implies f, g \neq 0)$

$\deg(fg) = 0 = \deg f + \deg g \implies \deg f = \deg g = 0 \implies f \in R^*$

Примеры.

1. $\mathbb{Z}[x]^* = \{\pm 1\}$
2. $\mathbb{R}[x]^* = \mathbb{R} \setminus \{0\}$
3. $(\mathbb{Z}/4\mathbb{Z})[x]^*$ — бесконечное множество

Упражнение. $R[[x]]^* = \{\sum\limits_{i=0}^{\infty} a_i X^i \mid a_0 \in R^*\}$

3 Деление с остатком

Теорема 3.1 (о делении с остатком для многочленов)**.** R — ОЦ.

Пусть $f, g \in R[x], \ g \neq 0$ и старший коэффициент g обратим.

Тогда $\exists! \ q, r \in R[x]$:

1. $f = gq + r$
2. $\deg r < \deg g$

Доказательство. $\deg g = d, \ g = b_d X^d + \ldots$

1. Существование q и r

   Индукция по $\deg f$: $\deg f < d \implies$ подходит $q = 0, r = f$

   Пусть $\deg f = n \geqslant d$

   $f_1 = f - g \cdot a_n \cdot b_d^{-1} \cdot X^{n-d}$, где b_d — старший коэффициент g

   $g \cdot a_n \cdot b_d^{-1} \cdot X^{n-d} = (b_d X^d + \ldots) \cdot a_n \cdot b_d^{-1} \cdot X^{n-d} = a_n X^n + \ldots \implies \deg f_1 < n$

   По индукционному предположению $\exists q_1, r_1 \in R[x]$ такие, что:

   (a) $f_1 = gq_1 + r_1$

   (b) $\deg r_1 < d$

   $f = g \cdot a_n \cdot b_d^{-1} \cdot X^{n-d} + f_1 = g\underbrace{(a_n \cdot b_d^{-1} \cdot X^{n-d} + q_1)}_{q} + \underbrace{r_1}_{r}$

2. Предположим $f = g \cdot q_1 + r_1 = g \cdot q_2 + r_2,\ \deg r_1 < d, \deg r_2 < d$

   $g(q_1 - q_2) = r_2 - r_1$

   Предположим $q_1 \neq q_2 \implies \deg g \cdot (q_1 - q_2) = \underbrace{\deg g}_{d} + \underbrace{\deg q_1 - q_2}_{\geqslant 0} \geqslant d,\ \deg(r_2 - r_1) < d$

Замечание. Условие R — ОЦ не существенно.

$g = b_d X^d + \ldots,\ b_d \in R^*$

$b_d \cdot a = 0 \implies b_d^{-1}(b_d a) = 0 \implies a = 0$ (что это значит?)

4 Гомоморфизм подстановки

***Определение* 4.1.** Пусть R, S – кольца. Гомоморфизм из кольца R в кольцо S называется отображение $\varphi : R \to S$ так что:

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\forall a, b \in R$;
2. $\varphi(ab) = \varphi(a)\varphi(b)$
3. $\varphi(1_R) = 1_S$

Предложение 4.1 (свойства гомоморфизма)**.**

1. $\varphi(0_R) = 0_S$
2. $\forall a \in R : \varphi(-a) = -\varphi(a)$
3. $\forall a, b \in R : \varphi(a - b) = \varphi(a) - \varphi(b)$

Доказательство.

1. $0_R = 0_R + 0_R \implies \varphi(0_R) = \varphi(0_R) + \varphi(0_R) \implies \underbrace{\varphi(0_R) + (-\varphi(0_R))}_{0_S} = \varphi(0_R) + \underbrace{\varphi(0_R) + (-\varphi(0_R))}_{0_S} \implies$

   $0_S = \varphi(0_R) + 0_S \implies \varphi(0_R) = 0_S$
2. $a + (-a) = 0_R \implies \varphi(a) + \varphi(-a) = \varphi(0_R) = 0_S \implies \varphi(-a) = -\varphi(a)$
3. $\varphi(a - b) = \varphi(a) + \varphi(-b) = \varphi(a) - \varphi(b)$

***Определение* 4.2.** Пусть S-кольцо, $R \subset S$. R называется подкольцом S, если:

1. $\forall a, b \in R : a - b \in R$
2. $\forall a, b \in R : ab \in R$
3. $1_S \in R$

Замечание. Этих условий достаточно (остальные выражаются)

$1 \in R \implies 0 = 1 - 1 \in R$

$a \in R \implies -a = 0 + (-a) = 0 - a \in R$

$a, b \in R \implies a + (-(-b)) = a - (-b) \in R$

Примеры.

1. Пусть R — подкольцо в S. Тогда $i_R : R \to S$ — гомоморфизм, $a \mapsto a$.
2. $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ — гомоморфизм, $a \mapsto \overline{a}$
3. $\mathbb{C} \to \mathbb{C}$ — гомоморфизм, $z \mapsto \overline{z}$

Теорема 4.1. Пусть B - кольцо, A - подкольцо такое что, $\forall a \in A\ \forall b \in B : ab = ba$

Зафиксируем $b \in B$. Тогда отображение $\varphi_b : A[x] \to B$

$a_n X^n + \ldots + a_1 X + a_0 \mapsto a_n b^n + \ldots + a_1 b + a_0$ является гомоморфизмом колец.

Доказательство.

Если $f = a_n X^n + \ldots + a_1 X + a_0$, то $f(b) = a_n b^n + \ldots + a_1 b + a_0 = \varphi_b(f)$

Нужно проверить: $(f+g)(b) = f(b) + g(b)$

$(fg)(b) = f(b)g(b)$

$1(b) = 1$ — тривиально

$(f+g)(b) = f(b) + g(b)$ — очевидно из определения $f + g$.

$f = \sum\limits_{i=0}^{n} a_i X^i, g = \sum\limits_{i=0}^{m} c_i X^i$

$fg = \sum\limits_{k=0}^{n+m} d_k X^k, d_k = \sum\limits_{i+j=k} a_i c_j$

$(fg)(b) = \sum\limits_{k=0}^{n+m} d_k b^k$

$$f(b)g(b) = \left(\sum_{i=0}^{n} a_i b^i\right)\left(\sum_{j=0}^{m} c_j b^j\right) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b^i c_j b^j \overset{\text{коммут.}}{=}$$

$$\sum_{i=0}^{n}\sum_{j=0}^{m} a_i c_j b^{i+j} = \sum_{k=0}^{n+m} \underbrace{\left(\sum_{i,j\geqslant 0, i+j=k} (a_i c_j)\right)}_{d_k} b^k = (fg)(b)$$

Примеры.

1. A — любое коммутативное кольцо, $B = A[x]$

   A - подкольцо в $B = A[x] \implies$ можно рассмотреть $f(g)$, где $f, g \in A[x]$

2. $\mathbb{R}[x] \xrightarrow{\varphi} \mathbb{R}[x]$, $f \mapsto f(5)$

   $\operatorname{Im}\varphi = \mathbb{R} \neq \mathbb{R}[x]$

3. $A \to A$

   $f \overset{\alpha}{\longmapsto} f(x_2, x_3, x_4, \ldots)$ — инъективный, но не сюръективный

   $f \overset{\beta}{\longmapsto} f(0, x_1, x_2, x_3, \ldots)$ — сюръективный, но не инъективный

Упражнение.

1. Найти все автоморфизмы $\mathbb{Q}$
2. Найти все автоморфизмы $\mathbb{R}$
3. Найти все автоморфизмы $\mathbb{R}[x]$

Теорема 4.2 (Безу)**.** Пусть $f \in R[X],\ c \in R$. Тогдаа остаток при делении f на $X - c$ есть $f(c)$.

Доказательство.

$f = (X - c) \cdot q + r$, по теореме о делении с остатком $\deg r < \deg(X - c) = 1 \implies$

$f(c) = (c - c) \cdot q(c) + r(c) = r(c)$

Следствие. Пусть $f \in R[X],\ c \in R$. Тогда $f(c) = 0 \iff (X - c) \mid f$

***Определение* 4.3.** Пусть R — подкольцо S, элементы R коммутируют с элементами S. Тогда $s \in S$, такой что $f(s) = 0$, где $f \in R[x]$ — называется корнем из f в R.

Примеры.

1. $f = x^4 - 2$ в $\mathbb{Z}[x]$

   f не имеет корней в $\mathbb{Z}$

   f имеет 2 корня в $\mathbb{R}$

   f имеет 4 корня в $\mathbb{C}$

Предложение 4.2. Пусть R – область целостности, $f \in R[x]$, $\deg f = d \geqslant 0$. Тогда число корней f в R не превосходит d.

Доказательство. Индукция по d

База: $d = 0 \implies f$ ненулевой $d \implies$ корней нет

Переход: $d > 0$

У f нет корней в $R \implies$ утверждение выполнено

У f есть корни в R, пусть $c \in R$ — какой-либо из корней f

$f(c) = 0 \implies f = (X - c) \cdot g$, где $g \in R[x]$

$\deg f = \deg(X - c) + \deg g \implies \deg g = d - 1$

Пусть $c_1, \ldots, c_l$ — все корни g в R

По предположению индукции: $l \leqslant d - 1$

Утверждение: $\{c_1, \ldots c_l, c\}$ — все корни f в R

$f(c_1) = \ldots = f(c_l) = f(c) = 0$

Предположим $\exists c' \notin \{c_1, \ldots, c_l, c\}$, такой что $f(c') = 0$

$\implies (c' - c) \cdot g(c') = 0$ — противоречие с тем, что R – область целостности

$\implies$ у f не более $l + 1 \leqslant d$ корней в R.

Пример. $x^2 - 1$ имеет 4 корня в $\mathbb{Z}/8\mathbb{Z}$ или в $\mathbb{Z}/5\mathbb{Z}$

$$x^2 \underset{77}{\equiv} 1 \iff \begin{cases} x^2 \underset{7}{\equiv} 1 \\ x^2 \underset{11}{\equiv} 1 \end{cases} \iff \begin{cases} x \underset{7}{\equiv} 1 \text{ или } x \underset{7}{\equiv} -1 \\ x \underset{11}{\equiv} 1 \text{ или } x \underset{11}{\equiv} -1 \end{cases}$$

Предложение 4.3 (формальное и функциональное равенство многочленов)**.**

Пусть R – бесконечная область: $f, g \in R[x]$

таковы, что $\forall a \in R : f(a) = g(a)$

Тогда $f = g$

Доказательство.

$h = f - g$, предположим, что $h \neq 0 \implies \deg h = d \geqslant 0 \implies$ у h есть $\leqslant d$ корней.

Но $\forall a \in R : h(a) = f(a) - g(a) = 0$, R - бесконечная область, противоречие. Так как их не больше чем d, но R бесконечно.

Пример. $R = \mathbb{Z}/3\mathbb{Z}$, $f = X, g = X^3$

$\forall A \in \mathbb{Z} : a^3 \underset{3}{\equiv} a \implies \forall \alpha \in \mathbb{Z}/3\mathbb{Z} : f(\alpha) = g(\alpha)$

5 Евклидовы области

***Определение* 5.1.** *Евклидовой областью целостности* (*евклидовой областью, евклидовым кольцом*) называется область целостности R, для которой существует функция $\nu : R \setminus \{0\} \to \mathbb{Z}_{\geqslant 0}$, называемая *евклидовой нормой*, такая что:

1. Если $d \mid a$, то $\nu(d) \leqslant \nu(a)$, причем $\nu(d) = \nu(a) \iff d \sim a$.
2. Для любых $a, b \in R,\ b \neq 0$: существует представление $a = bq + r$, где $r = 0$ или $\nu(r) < \nu(b)$.

Замечание: свойство один можно убрать, но доказательства будут сложнее.

Примеры.

1. $R = K[x]$, (K - поле), где $\nu(P) = \deg P$
2. $R = \mathbb{Z}$, где $\nu(a) = |a|$

3. $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, где $\nu(a+bi) = a^2 + b^2$ (подробнее в книжке Аейрленд, Роузен - «Классическое введение в современную теорию чисел»)

4. $R = K[[x]]$, (K - поле)

   $R^* = \{a_0 + a_1 x + a_2 x + \ldots \mid a_0 \neq 0\}$

   $\operatorname{ord} f = \min\{j \mid a_j \neq 0\}$

   $f = x^{\operatorname{ord} f} \cdot (a_j + a_{j+1} x + \ldots) \sim x^{\operatorname{ord} f}$

   Упражнение. Докажите, что это евклидова область.

5. $R = \mathbb{Z}_{(5)} = \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ 5 \nmid b\}$

   Упражнение. Докажите, что это евклидова область.

Лемма 5.1. Пусть R - область целостности, $a, b \in R$. Тогда $a \sim b \iff a = \varepsilon b,\ \varepsilon \in R^*$

Доказательство.

«$\Longleftarrow$»:

Пусть $a = \varepsilon b \implies b$. Так как ε — обратим, $b = \varepsilon^{-1} a$.

$$\left.\begin{array}{l} a = \varepsilon b \implies a \mid b \\ b = \varepsilon^{-1} a \implies b \mid a \end{array}\right\} \iff a \sim b$$

«$\Longrightarrow$»:

$$a \sim b \implies \begin{cases} a \mid b \\ b \mid a \end{cases} \implies \begin{cases} b = \varepsilon a \\ a = \varepsilon' b \end{cases} \implies b = \varepsilon\varepsilon' b \implies (\varepsilon\varepsilon' - 1) b = 0 \implies \varepsilon \text{ — обратим.}$$

***Определение* 5.2.** R — коммутативное кольцо, $I \subset R$ называется *идеалом* в R, если:

1. $I \neq \varnothing$
2. $\forall a, b \in I : a + b \in I$
3. $\forall a \in I\ \forall b \in R : ab \in I$

Примеры.

1. $R = \mathbb{Z},\ I = 2\mathbb{Z}$
2. $R = K[X],\ I = \{f \in R \mid f(0) = 0\}$
3. $R = C[0,1]$ (непрерывные функции на отрезке [0, 1]), $I = \{f \in R \mid f(0) = 0\}$

***Определение* 5.3.** Пусть R — коммутативное кольцо, $r \in R$. Из свойств кольца очевидно, что $\langle r \rangle \rightleftharpoons (r) \rightleftharpoons \{rs \mid s \in R\}$ — идеал в R.

Тогда (r) называется *главным идеалом* порожденный элементом r.

Замечание. $(r) = (r') \iff r \sim r'$

Пример. Пример неглавного идеала:

$$R = \mathbb{Z}[X],\ I = \{f : 2 \mid f(0)\}$$

Предложение 5.1. В евклидовой области все идеалы главные.

Доказательство. Пусть I - идеал в области целостности R.

Случай $I = \{0\}$ — тривиален, тогда $I = (0)$. Пусть $I \neq \{0\}$.

Зафиксируем норму ν и рассмотрим $c \in I$ с минимальной нормой. Докажем, что $I = ()$.

«$\supset$»:

Так как для любого $b \in R$ должно быть выполнено $cb \in I$, то $I \supset (c)$.

«$\subset$»:

Предположим, $\exists a \in I \setminus (c)$. Представим евклидову норму в виде $a = cq + r,\ q, r \in R$. Если $r = 0$, то $a \in (c)$ по определению главного идеала. Но иначе $\nu(r) < \nu(c)$. Выразим r:

$$r = a - cq = a + c(-q).$$

Так как $c \in I$ и $a \in I$, то и $c(-q) \in I$, следовательно $r \in I$. Но $\nu(r) < \nu(c)$, что противоречит минимальности нормы $\nu(c)$

***Определение* 5.4.** Область целостности, в которых все идеалы главные, называется *областью главных идеалов (ОГИ).*

Предложение 5.2. Пусть R — область главных идеалов. Тогда:

1. $a, b \in R \implies$ у a и b существует наибольший общий делитель
2. Если d - наибольший общий делитель a и b, то $d = am + bn,\ m, n \in R$

Доказательство.

Можно считать $a \neq 0$ или $b \neq 0$, если $a = b = 0$, то $d = 0$ подходит, $d \neq 0$ не подходит.

1. Рассмотрим множество $I = \{am + bn \mid m, n \in R\}$ — идеал в R. Тогда можно записать $I = (d)$.

   Заметим, что d — общий делитель a и b.

   $$\begin{cases} a = a \cdot 1 + b \cdot 0 \in I = (d) \\ b = a \cdot 0 + b \cdot 1 \in I = (d) \end{cases} \implies \begin{cases} d \mid a \\ d \mid b \end{cases}$$

   Покажем, что d - наибольший общий делитель a и b. То есть, что

   $$\begin{cases} d' \mid a \\ d' \mid b \end{cases} \overset{(!)}{\implies} d' \mid d$$

   Так как $d \in I$, $d = am_0 + bn_0,\ m_0, n_0 \in R$.

   $$\begin{cases} d' \mid a \\ d' \mid b \end{cases} \implies \begin{cases} d' \mid am_0 \\ d' \mid bn_0 \end{cases} \implies d' \mid d.$$

   Что и требовалось доказать.

2. Если d' - наибольший общий делитель a и b, то:
$$d' \sim d \in I \implies d' \in I \implies d' = am + bn,\ m, n \in R.$$

Замечание. Наибольший общий делитель в ОГИ обозначают (a, b).

***Определение* 5.5.** Элементы ОГИ a и b называют *взаимно простыми*, если $(a, b) = 1$.

Предложение 5.3. $(a, b) = 1 \iff m, n \in R : am + bn = 1$

Доказательство. «$\Longrightarrow$»: Из предыдущего предложения

«$\Longleftarrow$»: $d = (a, b) \implies d \mid a, d \mid b \implies d = 1 \implies d \sim 1$

6 Факториальность области главных идеалов

***Определение* 6.1.** Пусть R - коммутативное кольцо. Элемент a называется *неприводимым*, если $a \neq 0$, $a \notin R^*$ и $a = bc \implies b \in R : *$ или $c \in R^*$.

То есть неприводимый элемент — необратимый элемент, который не раскладывается в произведение двух обратимых.

***Определение* 6.2.** *Приводимый элемент* — не 0, не обратный, не неприводимый.

Примеры.

1. $R = K[x]$, (K - поле)

   $\deg f = 1 \implies f$ - неприводимый, так как $f = bc, \deg f = \deg b + \deg c = 1 + 0 = 0 + 1 = 1$

2. $\mathbb{R}[x]$:

   $x^2 - 4$ приводим $x^2 - 4 = (x-2)(x+2)$

   $x^2 + 1$ неприводим, иначе имел бы корень в $\mathbb{R}$

Лемма 6.1. Пусть $f \in K[x]$ — многочлен степени 2 или 3. Тогда f приводим $\iff$ у него есть корень в K.

Доказательство.

«$\Longrightarrow$»:

a - корень $f \overset{\text{т. Безу}}{\implies} (X - a) \mid f$. Рассмотрим разложение $f = (X-a) \cdot g$. Так как $\deg g = \deg f - 1 \geqslant 1$, оно нетривиально и f — приводимый.

«$\Longleftarrow$»:

Пусть $f = gh$ и $\deg g,\ \deg h \geqslant 1$, не умаляя общности, $\deg g \geqslant \deg h$. Тогда:
$$\underbrace{\deg f}_{2 \text{ или } 3} = \deg g + \deg h$$

Есть два стула: $2 = 1 + 1$ и $3 = 2 + 1$ (на какой сам сядешь, на какой друга посадишь?)
$$\deg h = 1 \implies h = aX + b \implies h\left(-\frac{b}{a}\right) = 0 \implies f\left(-\frac{b}{a}\right) = 0.$$

Значит $-\frac{b}{a}$ — корень f.

Замечание. Многочлены большей степени могут быть приводимыми, но не иметь корней в K.

Пример. Рассмотрим $f = x^4 + x^2 + 1$ в $\mathbb{R}[x]$:

$$f = (x^2+1)^2 = (x^2+x+1)(x^2-x+1).$$

Замечание. R — ОГИ

Лемма 6.2. Пусть $p, f \in R$. p - неприводимый элемент. Тогда $p \mid f$ либо $(p, f) = 1$.

Доказательство. $(p, f) \mid p \implies (p, f) = 1$ или $(p, f) = p \implies (p, f) = 1$ или $p \mid f$.

Предложение 6.1. Пусть p - неприводимый, $p \mid ab \implies p \mid a$ или $p \mid b$.

Доказательство. Пусть $p \nmid a, p \nmid b \implies (p, a) = (p, b) = 1 \implies$

$pm + an = 1, pm' + an' = 1 \overset{\text{перемножим}}{\implies} p(pmm' + mbn' + anm') + abnn' = 1 \implies p \mid 1$

***Определение* 6.3.** Область целостности R называют факториальным кольцом, если:

1. Любой $a \in \mathbb{R}$ отличный от 0 и не являющийся обратимым можно представить в виде $a = p_1 \dots p_s, s \geqslant 1$ и $p_1, \dots, p_s$ - неприводимые элементы.
2. Если $p_1 \dots p_s = q_1 \dots q_t$, где все p_i, q_i - неприводимые элементы, то $s = t$ и после перенумерации q_j выполнено $q_1 \sim p_1, \dots, q_s \sim p_s$.

Теорема 6.1. Область главных идеалов является факториальным кольцом.

Доказательство. Есть элемент a, докажем что существует неприводимый p такой, что $p \mid a$.

Возьмем a, если он неприводимый, то доказывать нечего (т.к. $a \mid a$), иначе: $a = a_1 b_1$, где $a_1, b_1 \notin R^*$ (не являются обратимыми)

a_1 – неприводимый, следовательно утверждение доказано, иначе $a_1 = a_2 b_2$, где $a_2, b_2 \notin R^*$

и так далее

Предположим, утверждение неверно. Обозначим $I = \bigcup\limits_{i=1}^{\infty}(a_i)$

$x, y \in I \implies x + y \in I$

Можно заметить, что $a_2 \mid a_1, a_3 \mid a_2, \dots \implies (a_1) \subset (a_2) \subset \dots$

$x \in (a_i), y \in (a_j)$, не умаляя общности $i \leqslant j$

$x, y \in (a_j) \implies x + y \in (a_j) \subset I$

$x \in I \implies x \in (a_i)$ для некоторого i

$a \in R \implies ax \in (a_i) \subset I$

$I = (c), c \in I \implies c \in (a_i)$ для некоторого i

$a_{i+1} \in I \implies c \mid a_{i+1}$

$a_i \mid c \implies a_i \mid a_{i+1}$

$a_i = a_{i+1} \cdot b_{i+1} \implies b_{i+1} \in R^*$

Значит любой обратимый элемент делится на неприводимый.

$a \in R, a \neq 0, a \notin R^*$

a неприводимый $\implies$ все доказано, иначе $a = p_1 a_1,\ p_1 \notin R^*$, p_1 – неприводимый

a_1 неприводимый $\implies$ все доказано, иначе $a_1 = p_2 a_2,\ p_2 \notin R^*$, p_2 – неприводимый

и так далее

Можно заметить, что $a_2 \mid a_1, a_3 \mid a_2, \ldots \implies (a_1) \subset (a_2) \subset \ldots$

Аналогично доказывается, что существуют $a_i \sim a_{i+1}$ ассоциированные $\implies p_{i+1} \in R^*$. Противоречие.

Единственность разложения:

Пусть $p_1 \ldots p_s = q_1 \ldots q_t$, где все p_i, q_i, не умаляя общности $s \leqslant t$

Индукция по S

База: $s = 1$

$p_1 = q_1 \ldots q_t$. p_1 - неприводимый $\implies t = 1,\ q_1 = p_1$.

Переход: $s > 1$

$p_s \mid (p_1 \ldots p_s) \implies p_s \mid (q_1 \ldots q_t) \implies \exists j : p_s \mid q_j$

Перенумеруем, так чтобы $j = t$. $q_t = p_s \cdot \varepsilon$, но q_t неприводим $\implies \varepsilon \in R^*$

$$p_1 \ldots p_s = q_1 \ldots q_{t-1} \cdot \varepsilon p_s \implies p_1 \ldots p_{s-1} = q_1 \ldots q_{t-1} \cdot \varepsilon = \underbrace{(\varepsilon q_1)}_{\text{неприводимый}} \cdot q_2 \ldots q_{t-1}$$

По индукционному предположению $p_1 \ldots p_{s-1}$ совпадает с $(\varepsilon q_1) \cdot q_2 \ldots q_{t-1}$ с точностью до порядка и ассоциировнности.

Примеры.

1. R — факториальное кольцо $\implies R[X]$ — факториальное кольцо.
2. $\mathbb{Z}[X]$ — факториальное кольцо.
3. $K[X][Y] = K[X, Y] \implies K[X, Y]$ — факториальное кольцо.

7 Кратные корни и производные

***Определение* 7.1.** Пусть $f \in R[x]$ и $f \neq 0$. Пусть $a \in R$ — корень.

$(X - a) \mid f$ по теореме Безу.

Наибольший n, такой что $(X - a)^n \mid f$, называется кратностью корня a. Можно заметить, что $n \leqslant \deg f$, поэтому он всегда существует.

Корни кратности 1 называются простыми корнями f,

корни кратности $\leqslant 2$ называются кратными корнями f,

корни кратности 2 — двойными, 3 — тройными

Теорема 7.1. Пусть K поле, $f \in K[X]$, $d = \deg f > 0$

$a_1, \ldots, a_s$ — его корни, $n_1, \ldots, n_s$ — их кратности.

Тогда $n_1 + \ldots + n_s \leqslant d$.

Доказательство. Разложим f на неприводимые множители.

$X - a_j$ — неприводимые

$f = (X - a_1)^{m_1} \ldots (X - a_s)^{m_s} \cdot g,\ g \in K[x]$

$(X - a_1) \neq g, \ldots, (X - a_s) \neq g$

$m_1 \leqslant n_1, \ldots, m_s \leqslant n_s$

Предположим, при некотором j: $n_j > m_j \implies$

$(X - a_j)^{m_j+1} \mid f \implies (X - a_j)^{m_j+1} \cdot h = (X - a_1)^{m_1} \ldots (X - a_s)^{m_s} \cdot g \implies$

$(X - a_j) \cdot h = (X - a_1)^{m_1} \ldots \widehat{(X - a_j)}^{m_j} \ldots (X - a_s)^{m_s} \cdot g \implies$

$(X - a_j) \mid (X - a_1)^{m_1} \ldots \widehat{(X - a_j)}^{m_j} \ldots (X - a_s)^{m_s} \cdot g \implies$

Очевидно, $(X - a_j) \mid (X - a_i)$, $(i \neq j)$.

$(X - a_j) \nmid g$ — противоречие.

Т.о. $m_j = n_j, j = 1, \ldots, s$.

$d = \deg f = m_1 + \ldots + m_s + \underbrace{\deg g}_{\geqslant 0} \geqslant n_1 + \ldots + n_s$

***Определение* 7.2.** Пусть $f \in K[X]$, $f = a_n X_n + a_{n-1} X_{n-1} + \ldots + a_1 X_1 + a_0$

Его производной будет называться многочлен $f' \in K[X]$, $f' = n a_n X_{n-1} + (n-1) a_{n-1} X_{n-2} + \ldots + a_1$

Предложение 7.1.

1. $(f + g)' = f' + g'$
2. $(fg)' = f'g + fg'$
3. $(f^n)' = n f^{n-1} f'$

Доказательство.

1. лёгкая непосредственная проверка (сначала очевидно, потом тривиально)
2. Пусть f, g — мономы, то есть $f = aX^n,\ g = bX^m$

   $(fg)' = (abX^{n+m})' = (n+m)abX^{n+m-1} = n \cdot abX^{n+m-1} + m \cdot abX^{n+m-1} =$

   $$\underbrace{naX^{n-1}}_{f'} \cdot \underbrace{bX^m}_{g} + \underbrace{aX^n}_{f} \cdot \underbrace{mbX^{m-1}}_{g'}$$

   $f = \sum f_i,\ g = \sum g_i, f_i, g_i$ — мономы

   $(fg)' = \left(\sum\limits_{i,j} f_i g_j \right) = \sum\limits_{i,j} (f_i g_j)' = \sum\limits_{i,j} (f_i' g_j + f_i g_j') = \sum\limits_{i,j} f_i' g_j + \sum\limits_{i,j} f_i g_j' = \sum\limits_i f_i' \sum\limits_j g_j + \sum\limits_i f_i \sum\limits_j g_j' =$
   $f'g + fg'$

3. Индукция по n

   База: $n = 1$

   $f' = f'$

   Переход: $n > 1$

   $(f^n)' = (f^{n-1} \cdot f)' = (f^{n-1})' \cdot f + f^{n-1} \cdot f' \overset{\text{ИП}}{=} ((n-1) \cdot f' \cdot f^{n-2}) \cdot f + f^{n-1} \cdot f' = (n-1)f' \cdot f^{n-1} + f' \cdot f^{n-1} = nf^{n-1}f'$

Предложение 7.2. K-поле. $f \in K[X], f \neq 0, a \in K$

Тогда a кратный корень $f \iff f(a) = f'(a) = 0$

Доказательство.

«$\Longrightarrow$»:

a кратный корень $f \implies (X-a)^2 \mid f \implies f = (X-a)^2 \cdot g, g \in K[X]$

$f' = ((X-a)^2)' \cdot g + (X-a)^2 \cdot g' = 2(X-a) \cdot g + (X-a)^2 \cdot g' \implies f'(a) = 0$

«$\Longleftarrow$»:

Пусть $f(a) = f'(a) = 0$.

$f(a) = 0 \overset{\text{т.Безу}}{\Longrightarrow} f = (X-a) \cdot g, g \in K[X] \implies$

$f' = g + (X-a)g'$

$f'(a) = 0 \implies g(a) = 0 \implies (X-a) \mid g \implies (X-a)^2 \mid f \implies a$ кратный корень f

Следствие. K-поле. $f \in K[X], f \neq 0, a \in K$

Пусть $D = (f, f')$

Тогда a кратный корень $f \iff D(a) = 0$

Доказательство. a кратный корень $\iff f(a) = f'(a) = 0 \overset{\text{т.Безу}}{\iff} (X-a) \mid f$ и $(X-a) \mid f' \iff (X-a) \mid D \overset{\text{т.Безу}}{\iff} D(a) = 0$

Предложение 7.3. K-поле. Характеристика 0, то есть $\underbrace{1 + \ldots + 1}_{n} \neq 0, \forall n \in \mathbb{N}$

$f \in K[X], a \in K$ — корень f кратности $s \geqslant 2$.

Тогда a — корень f' кратности $s - 1$

Доказательство. $f = (X-g)^s g$

$(X-a) \nmid g \overset{\text{т.Безу}}{\Longrightarrow} g(a) \neq 0$

$f' = ((X-a)^s)' \cdot g + (X-a)^s \cdot g' = s(X-a)^{s-1} \cdot g + (X-a)^s \cdot g' = (X-a)^{s-1} \cdot h$, где $h = s \cdot g + (X-a)g'$

$h(a) = s \cdot g(a) \neq 0 \implies (X-a) \nmid h$

8 Формула Тейлора

Предложение 8.1. K - поле, $f, g \in K[x], f \neq 0, d = \deg(g) \geqslant 1$.

Тогда f можно представить единственным образом:

$f = h_n g^n + \dots + h_1 g + h_0$,

где $n \geqslant 0, h_i \in K[x], h_n \neq 0, \deg(h_i) < d, i = 0, \dots, n$.

Доказательство. Индукция по $l = \deg f$.

$l < d: \; n = 0, h_0 = f$.

$l >= d: \; f = gq + r, \; \deg(r) < d, \; q \neq 0$.

$\deg gq \geqslant \deg g > \deg r$

$\implies \deg f = \deg gq \implies \deg q = l - d$

По ИП: $q = h_n g^n + \dots + h_1 g + h_0, \; h_n \neq 0, \; \deg(h_i) < d, \; i = 0, \dots, n$.

$\implies f = h_n g^{n+1} + \dots + h_0 g + r$.

Единственность.

Индукция по $l = \deg f$.

$l < d$:

$\deg h_n g^n \geqslant nd > deg h_i g^i, \; i = 0, \dots, n-1 \implies \deg f = \deg h_n g^n \implies \deg h_n g^n < d$.

$nd + d - 1 \geqslant l \geqslant nd \implies n$ - неполное частное при делении l на d.

База $l < d \; n = 0 \implies h_0 = f$.

Предположим, то есть еще разложение $f = \hat{h_n} g^n + \dots + \hat{h_1} g + \hat{h_0}$.

$f = g(h_n g^{n-1} + \dots + h_1) + h_0 = g(\hat{h_n} g^{n-1} + \dots + h_1) + h_0, \; \deg h_0, \; \deg \hat{h_0} < d$

Тогда $h_0 = \hat{h_0}$.

По ИП: $\deg f_1 = h_n g^{n-1} + \dots + h_1 < \deg f \implies h_i = \hat{h_i}, \; i = 1, \dots, n-1$.

Предложение 8.2. $char K = 0, \; f \in K[x], \; f \neq 0, \; d = \deg(f) = n \geqslant 0, \; a \in K$.

$\implies f = \sum\limits_{i=0}^{n} \frac{f^{(i)}(x-a)^i}{i!}, \; f_i \in K[x], \; \deg(f_i) < d, \; i = 0, \dots, n$.

Напоминание: $\operatorname{char} K = \min\{l \mid \underbrace{1 + 1 + \dots 1}_{\text{l раз}} = 0\}$.

Доказательство. $f = \sum_{i=0}^{n} c_i (x-a)^i, \; c_i \in K, \; i = 0, \dots, n, \; c_n \neq 0$.

$f^{(i)} = \sum\limits_{j=i}^{n} c_j j! (x-a)^{j-i}, \; i = 0, \dots, n$.

$f^{(j)}(a) = c_j j!$

$c_i = \frac{f^{(i)}(a)}{i!}$.

9 Алгебраически замкнутые поля. Каноническое разложение над $\mathbb{C}$ и над $\mathbb{R}$.

***Определение* 9.1.** Поле K называется *алгебраически замкнутым*, если любой $f \in K[x]$ имеет корень в K.

Теорема 9.1. Основная теорема алгебры.

$\mathbb{C}$ алгебраически замкнуто.

Доказательство. Не будет в курсе.

Идея доказательства:

$f = a_n x^n + \dots + a_1 x + a_0,\ z \in \mathbb{C},\ f(z) = 0.$

$r > max\{|a_0|, \dots, |a_n|\}.$

$f(r(\cos(\varphi) + i\sin(\varphi))) = r^n(\cos(n\varphi) + i\sin(n\varphi)) + g(r(\cos(\varphi) + i\sin(\varphi))).$

$|g(r(\cos(\varphi) + i\sin(\varphi)))| < r^{n-1}(|a_{n-1}| + \ldots + |a_1| + |a_0|) < r^n.$

$\implies \Delta \arg f(r(\cos(\varphi) + i\sin(\varphi))) = 2\pi n.$

$D = \{z \in \mathbb{C} \mid |z| \geqslant r\}$

$\overset{\text{Топология}}{\implies} f(D)$ - односвязная область.

$\implies 0 \in f(D) \implies \exists z\ f(z) = 0.$

Замечание. Любое поле можно вложить в алгебраически замкнутое поле.

Всегда есть минимальное такое поле.

Для $\mathbb{Q}$ это поле алгебраических чисел.

Алгебраическое число - комплексный корень многочлена над $\mathbb{Q}$.

Предложение 9.1. K - алгебраически замкнутое поле, $f \in K[x]$.

Тогда f - неприводим $\iff \deg f = 1$.

Доказательство. Все многочлены $\deg = 1$ неприводимы.

$\deg f \neq 1 \implies \exists x \in K : f(x) = 0$

$\overset{\text{Т. Безу}}{\implies} (x - c) \mid f$

Таким образомб если $f \in K[x], \deg f \geqslant 1$, то его каноническое разложение имеет вид:

$f = c_0 \prod\limits_{i=1}^{n} (x - c_i)^{d_i}$, где $c_i \in K,\ d_i \in \mathbb{Z}_+$.

Предложение 9.2. $f \in \mathbb{R}[x],\ a \in CC$ - его корень.

Тогда $\bar{a}$ - корень f той же кратности.

Доказательство. l - кратность a.

В $\mathbb{C}[x]$ $f = (x - a)^l g,\ g \in \mathbb{C}[x],\ g(a) \neq 0.$

Пусть $g = b_n x^n + \dots + b_1 x + b_0$.

Рассмотрим $\bar{g} = \bar{b_n} x^n + \dots + \bar{b_1} x + \bar{b_0}$.

Тогда $f = \bar{f} = \overline{(x-a)^l}\bar{g} = (x-\bar{a})^l \bar{g} \implies f(\bar{a}) = 0$

$g(a) = \overline{\bar{g}(\bar{a})} \implies x - \bar{a} \nmid \bar{g}$

$\implies \bar{a}$ - корень f кратности l

$\implies$ все корни входят парами

$\implies f = r_0 \left(\prod\limits_{i=1}^{n}(x-r_i)^{d_i}\right) \cdot \left(\prod\limits_{i=1}^{m}((x-c_i)(x-\bar{c_i}))^{p_i}\right)$, где $r_i \in \mathbb{R},\ d_i \in Z_+,\ c_i \in \mathbb{C},\ p_i \in \mathbb{Z}_+$.

$\implies f = r_0 \left(\prod\limits_{i=1}^{n}(x-r_i)^{d_i}\right) \cdot \left(\prod\limits_{i=1}^{m} B_i^{p_i}\right)$, B_i - квадратичные многочлены, неприводимые в $\mathbb{R}$.

Предложение 9.3. Унитарные неприводимые многочлены в $\mathbb{R}$ - это:

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

Доказательство. С многочленами степени 1 и 2 все ясно.

Если степень многочлена больше 2, то справедливо разложение 9.2, значит он приводим.

10 Рациональные дроби

***Определение* 10.1.** Пусть R область целостности. Мы вложим R в поле $Q(R)$, назовем её полем частных.

Рассмотрим $M = R \times (R \setminus \{0\})$ и введём на M отношение $\sim$:

$(a,b) \sim (a',b') \iff ab' = a'b$

Проверим: $\sim$ — отношение эквивалентности

рефлексивность и симметричность очевидны

транзитивность: $\begin{cases}(a,b) \sim (a',b') \\ (a',b') \sim (a'',b'')\end{cases} \implies ab'b'' = a'bb'' = a''bb' \implies b'(ab'' - a''b) = 0$

$b \neq 0 \implies ab'' - a''b \implies ab'' = a''b \implies (a,b) \sim (a'',b'')$

То есть $\sim$ — это отношение эквивалентности на M.

$Q(R) = M/\sim = \{[(a,b)] \mid a \in R, b \in R \setminus \{0\}\}$

***Определение* 10.2.** Обозначим $\frac{a}{b}$ — это $[(a,b)] \in Q(R)$.

Введём в $Q(R)$ операции сложения и умножения:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$
$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

Замечание. $(a,b)\sim(ac,bc)\quad\forall c\in R\setminus\{0\}$

Такая замена не изменит результат.

Замечание. $(a,b)\sim(a',b')\iff(ab',bb')=(a'b,b'b)$

Предложение 10.1. Операции на $Q(R)$ определены корректно, при этом $Q(R)$ с этими операциями — поле.

Доказательство. Коммутативность и ассоциативность сложения очевидны в случае одинакового знаменателя.

$\frac{a_1}{b}+\frac{a_2}{b}=\frac{a_1b+a_2b}{b^2}=\frac{a_2b+a_1b}{b^2}=\frac{a_2}{b}+\frac{a_1}{b}$

Но любые 2 дроби можно привести к общему знаменателю:

$\frac{a_1}{b_1}=\frac{a_1b_2}{b_1b_2}\quad\frac{a_2}{b_2}=\frac{a_2b_1}{b_1b_2}$

Нейтральный по сложению элемент — это $\frac{0}{1}$

Противоположный по сложению элемент к $\frac{a}{b}$ — это $\frac{-a}{b}$

Дистрибутивность: $\left(\frac{a_1}{b}+\frac{a_2}{b}\right)\frac{a'}{b'}=\frac{a_1+a_2}{b}\frac{a'}{b'}=\frac{(a_1+a_2)a'}{bb'}=\frac{a_1a'+a_2a'}{bb'}=\frac{a_1}{b}\frac{a'}{b'}+\frac{a_2}{b}\frac{a'}{b'}=\frac{a_1}{b}\frac{a'}{b'}+\frac{a_2}{b}\frac{a'}{b'}$

Нейтральный по умножению элемент — это $\frac{1}{1}$

$\frac{a}{b}\neq\frac{0}{1}\implies a\cdot 1\neq b\cdot 0\iff a\neq 0$

Обратный по умножению элемент к $\frac{a}{b}$ — это $\frac{b}{a}$

$R\overset{\varepsilon}{\hookrightarrow}Q(R),\ r\mapsto\frac{r}{1}$

То есть, считаем $R\subset Q(R)$

***Определение* 10.3.** Пусть K-поле. Тогда поле $K(x)=Q(K[x])$ назовем полем рациональных дробей (дробно-рациональных функций) над полем K.

Предложение 10.2 (Несократимое представление)**.** Пусть R — факториальное кольцо. Тогда любой $S\in Q(R)$ представимых в виде $s=\frac{p}{q},\ (p,q)=1$. Такое представление единственно с точностью до умножения p и q на $\varepsilon\in R^*$.

Доказательство. $s=\frac{a}{b},\ d=\gcd(a,b)\implies a=da',b=db'\implies s=\frac{a'}{b'},\ (a',b')=1$

$\frac{p}{q}=\frac{p'}{q'},(p,q)=(p',q')=1$

$\begin{cases}p\mid(p'q)\\(p,q)=1\end{cases}\implies p\mid p'$, аналогично $p'\mid p$

То есть p и p' ассоциативны $\implies p'=\varepsilon p,\ \varepsilon\in R^*$

$pq'=\varepsilon pq\implies q'=\varepsilon q$

Лемма 10.1. Пусть $s\in K(x),\ s=\frac{p}{q},p,q\in K[x]$

Тогда $\deg p-\deg q$ — инвариант s.

Доказательство. $\frac{p}{q} = \frac{p'}{q'} \implies pq' = p'q \implies \deg p + \deg q' = \deg p' + \deg q \implies \deg p - \deg q = \deg p' - \deg q'$

$\deg \frac{p}{q} = \deg p - \deg q$

***Определение* 10.4.** $s \in K(x)$ называется правильной дробью, если $\deg s < 0$

В частности 0 — правильная дробь

Замечание. Очевидно сумма и произведение правильных дробей — правильная дробь

Лемма 10.2. Любая рациональная дробь однозначно представляется в виде суммы многочленов и правильной дроби.

Доказательство. $s = \frac{p}{q}$

$p = q \cdot t + r$, где $r = 0$ или $\deg r < \deg q$

$\implies \frac{p}{q} = t + \frac{r}{q},\ t \in K[x],\ \frac{r}{q}$ — правильная дробь

$t + \frac{r}{q} = t_1 + \frac{r_1}{q_1}, t_1 \in K[x], \frac{r_1}{q_1}$ — правильная дробь

$t - t_1 = \frac{r_1}{q_1} - \frac{r}{q}$ — правильная дробь

$t - t_1 = \frac{t - t_1}{1} \implies \deg(t - t_1) < 0 \implies t - t_1 = 0$

Лемма 10.3. Пусть $(f, g) = 1$. Тогда любую дробь со знаменателем fg можно представить как сумму дробей со знаменателем f и g.

Доказательство. $1 = cf + dg$ для некоторых $c, d \in K[x]$

$\frac{a}{fg} = \frac{a(cd+dg)}{fg} = \frac{acf}{fg} + \frac{adg}{fg} = \frac{ac}{g} + \frac{ad}{f}$

Доказательство. Дробь s называется примарной (p-примарной), если $s = \frac{a}{p^n}$, p — неприводимый многочлен, $n \in \mathbb{N}$

Предложение 10.3. Любую правильную дробь можно однозначно представить в виде суммы нескольких отличных от 0 правильных p-примарных дробей, где p-различные унитарные неприводимые многочлены.

Доказательство. «Существование»:

Запишем значение s в виде $p_1^{m_1} \dots p_t^{m_t}$, где p_i — унитарные неприводимые многочлены

$p_1^{m_1} \dots p_t^{m_t} = (p_1^{m_1} \dots p_{t-1}^{m_{t-1}}) \cdot p_t^{m_t}$ (старшие коэффиценты ушли в числитель)

По лемме

$s = \frac{\dots}{p_1^{m_1}} + \frac{\dots}{p_t^{m_t}} = \frac{a_1}{p_1^{m_1}} + \dots + \frac{a_t}{p_t^{m_t}}$ (многочлен и правильная дробь, с тем же знаменателем)

$\implies s = f + \frac{b_1}{p_1^{m_1}} + \dots + \frac{b_t}{p_t^{m_t}},\ f \in K[x],\ \frac{b_j}{p_j^{m_j}}$ — правильная дробь

$\implies f = s - \frac{b_1}{p_1^{m_1}} - \dots - \frac{b_t}{p_t^{m_t}}$

$\implies \frac{f}{1}$ — правильная дробь

$\implies \deg f < 0 \implies f = 0$

«Единственность»:

Пусть у S есть 2 различных таких разложения

Вычитаем из первого разложения второе, получим:

$\frac{c_1}{p_1^{n_1}} + \ldots + \frac{c_l}{p_l^{n_l}} = 0,\ p_i$ — унитарные неприводимые многочлены

$c_1, \ldots, c_l \neq 0$

Можно считать все эти дроби несократимыми.

$\implies \frac{c_1}{p_1^{n_1}} + \ldots + \frac{c_{l-1}}{p_{l-1}^{n_{l-1}}} = \frac{-c_l}{p_l^{n_l}}$

Приведем к общему знаменателю и сделаем их сократимыми

знаменатель будет делиться на $p_1^{n_1} \ldots p_{l-1}^{n_{l-1}}$

не может быть ассоциированно с $p_l^{n_l}$

$\frac{b_i}{p_i^{m_i}} - \frac{b_i'}{p_i^{m_i}} = \frac{\ldots}{p_i^{n_i}}$

***Определение* 10.5.** Простейшей дробью называется дробь вида $\frac{a}{p^n}$, где p — неприводимый многочлен, $n \in \mathbb{N}$, $\deg a < \deg p$

Теорема 10.1. Любая ненулувая правильная дробь единственным образом представляется в виде суммы нескольких простых дробей с различными знаменателями.

Доказательство. «Существование»:

Достаточно разложить правильную примарную дробь $\frac{a}{p^n}$

$a = r_m p^m + \ldots + r_1 p + r_0$, $\deg r_i < \deg p,\ r_m \neq 0$

$m < n$, так как $\deg a < \deg p$

$\frac{a}{p^n} = \frac{r_m}{p^{n-m}} + \frac{r_{m-1}}{p^{n-m+1}} + \ldots + \frac{r_1}{p^{n-1}} + \frac{r_0}{p^n}$ — искомое представление, если удалить нулевые слагаемые

«Единственность»:

Пусть для s есть представления в виде суммы примарных. Обозначим C_p за сумму p-примарных дробей в этом представлении.

C_p — p-примарная правильная дробь

$s = C_{p_1} + \ldots + C_{p_t} \implies$ все C_p определены однозначно

Пусть у C_p есть лва разных разложения в сумму простейших дробей со степенями p в знаменателях.

$\frac{r_n}{p_n} + \ldots + \frac{r_1}{p_1} = \frac{s_n}{p_n} + \ldots + \frac{s_1}{p_1}$, где n — максимальная показатель степени p в знаменателях

Пусть m — максимальный индекс, такой что $r_m \neq s_m$, некоторые r_i и s_i могут быть нулевыми

$\frac{r_m - s_m}{p^m} + \ldots + \frac{r_1 - s_1}{p_1} = 0$

$\implies \frac{r_m - s_m}{p} = -(r_{m-1} - s_{m-1}) - p(r_{m-2} - s_{m-2}) - \ldots \in K[X]$

11 Интерполяция

Теорема 11.1. Пусть K — поле, $n \in \mathbb{N}$: $x_1, x_2, \ldots, x_n \in K$, различные между собой. $y_1, y_2, \ldots, y_n \in K$. Тогда $\exists! f \in K[x] : \deg f \leqslant n-1$ и $f(x_i) = y_i,\ i = 1, \ldots, n$.

Доказательство.

«Единственность»:

Предположим, что существует $f, g \in K[x],\ \deg \leqslant n-1,\ \deg g \leqslant n-1, f(x_i) = g(x_i) = y_i,\ i = 1, \ldots, n$

$\exists h = f - g,\ \deg h \leqslant n-1,\ h(x_i) = 0,\ i = 1, \ldots, n$

Предположим, $h \neq 0 \implies$ у $h \leqslant n-1$ корней, но такого не может быть.

«Существование»:

Формула Лагранжа

Решим интерполяционную задачу в специальном случае, когда $y_1 = 1, y_2 = \ldots = y_n = 0$.

Найдем соответствующий многочлен f_1.

$x_1, \ldots, x_n$ — корни многочлена $f_1 \implies (x - x_2) \mid f_1, \ldots, (x - x_n) \mid f_1 \implies$

$\underbrace{(x - x_2)(x - x_3) \ldots (x - x_n)}_{\text{степени } n-1} \mid f_1 \implies f_1 = c(x - x_2) \ldots (x - x_n),\ c \in K$

$f_1(x_1) = 1 \iff c(x_1 - x_2) \ldots (x_1 - x_n) = 1 \implies c = \frac{1}{(x_1 - x_2) \ldots (x_1 - x_n)}$

Получился многочлен $f_1 = \frac{(x - x_2) \ldots (x - x_n)}{(x_1 - x_2) \ldots (x_1 - x_n)}$

Аналогичная задача с $y_i = 1, \forall_{j \neq i}\ y_j = 0$ имеет решение:

$f_i = \frac{(x - x_1) \ldots \widehat{(x - x_i)} \ldots (x - x_n)}{(x_i - x_1) \ldots \widehat{(x_i - x_i)} \ldots (x_i - x_n)} = \frac{(x - x_1) \ldots \widehat{(x - x_i)} \ldots (x - x_n)}{F'(x_i)}$

Рассмотрим $f = y_1 f_1 + y_2 f_2 + \ldots + y_n f_n$, $y_1, \ldots, y_n$ теперь произвольные.

$\deg \leqslant \max(\deg f_1, \ldots, \deg f_n) = n - 1$

Получилась такая формула $f(x_i) = y_1 \underbrace{f_1(x_i)}_{0} + y_2 \underbrace{f_2(x_i)}_{0} + \ldots + y_i \underbrace{f_i(x_i)}_{1} + \ldots + y_n \underbrace{f_n(x_i)}_{0} = y_i$

Замечание. Про связь с производной

$F = (x - x_1) \ldots (x - x_n)$

$F' = \sum\limits_{i=1}^{n} (x - x_1) \ldots \widehat{(x - x_i)} \ldots (x - x_n)$

$F'(x_j) = \sum\limits_{i=1}^{n} (x_j - x_1) \ldots \widehat{(x_j - x_i)} \ldots (x_j - x_n) = (x_j - x_1) \ldots \widehat{(x_j - x_j)} \ldots (x_j - x_n)$

Метод Ньютона

Рассмотрим интерполяционную задачу и предположим, что мы уже нашли $f_{(n-1)} \in K[x]$, такой что $f_{(n-1)}$ решение интерполяционной задачи $(x_1, \ldots, x_{n-1}; y_1, \ldots, y_{n-1})$, то есть

$\deg f_{(n-1)} \leqslant n - 2$ и $f_{(n-1)}(x_i) = y_i,\ i = 1, \ldots, n-1$

Пусть f решение интерполяционной задачи

$f = f_{(n-1)} + g,\ g =?$

$f(x_i) = y_i = f_{(n-1)}(x_i),\ i = 1, \ldots, n-1$

$g = f - f_{(n-1)},\ g(x_1) = \ldots = g(x_{n-1}) = 0$

$\deg g \leqslant n-1 \implies g = c(x - x_1)\ldots(x - x_{n-1})$

$g(x_n) = f(x_n) - f_{(n-1)}(x_n) = y_n - f_{(n-1)}(x_n) \implies$ отсюда находится c

4 Линейная алгебра

1 Матрицы

***Определение* 1.1.** R — кольцо, $m, n \in \mathbb{N}$

Матрица $m \times n$ над кольцом R — прямоугольная таблица

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \text{ где } a_{ij} \in R$$

Есть краткая запись $A = (a_{ij})_{i=1,\dots,m;\ j=1,\dots,n} = (a_{ij})$

***Определение* 1.2.** Множество матриц $m \times n$ над кольцом R обозначается как $M_{m,n}(R)$

Так же обозначают, как: $R^{m\times n}$, $M(m,n,R)$, $M_{m\times n}(R)$

Пусть $A, B \in M_{m,n}(R)$ — матрицы. $A = (a_{ij})$, $B = (b_{ij})$

Их суммой называется матрица $C = (c_{ij})$, где $c_{ij} = a_{ij} + b_{ij}$.

Пусть $A = (a_{ij}) \in M_{m,n}(R)$, $B = (b_{ij}) \in M_{n,p}(R)$

Их произведением называется матрица $C = (c_{ij}) \in M_{m,p}(R)$, где $c_{ij} = \sum\limits_{k=1}^{n} a_{ik}b_{kj}$

Пусть $c \in R$, $A \in M_{m,n}(R)$

Тогда $c \cdot A = (c \cdot a_{ij}) \in M_{m,n}(R)$

Замечание. По умолчанию R — коммутативное кольцо

***Определение* 1.3.** Транспонированная матрица $A = (a_{ij}) \in M_{m,n}(R)$ — матрица $B = (b_{ij}) \in M_{n,m}(R)$, где $b_{ij} = a_{ji}$

Обозначается как A^T

Пример. $\begin{pmatrix} 2 & 0 & -3 \\ 1 & 5 & 4 \end{pmatrix}^T = \begin{pmatrix} 2 & 1 \\ 0 & 5 \\ -3 & 4 \end{pmatrix}$

***Определение* 1.4.** Матрица $A = (a_{ij}) \in M_{m,n}(R)$ — квадратная, если $m = n$

Обозначается как $A \in M_n(R)$

Теорема 1.1 (Свойства операций над матрицами)**.**

1. $A + (B + C) = (A + B) + C$
2. $0 = (0)$, тогда $A + 0 = 0 + A = A$
3. Для любой A есть $-A$, такая что $A + (-A) = (-A) + A = 0$
4. $A + B = B + A$

5. $(AB)C = A(BC)$, нужно чтобы $A \in M_{m,n}(R)$, $B \in M_{n,p}(R)$, $C \in M_{p,q}(R)$

   Обе матрицы принадлежат $M_{m,q}(R)$
6. $A(B + C) = AB + AC$
7. $(B + C)A = BA + CA$
8. $(\lambda + \mu)A = \lambda A + \mu A,\ \lambda, \mu \in R$
9. $\lambda(A + B) = \lambda A + \lambda B,\ \lambda \in R$
10. $(\lambda A)B = \lambda(AB) = A(\lambda B),\ \lambda \in R$
11. $(\lambda\mu)A = \lambda(\mu A),\ \lambda, \mu \in R$
12. $(A + B)^T = A^T + B^T$
13. $(AB)^T = B^T A^T$

***Определение* 1.5.** Пусть $n \in \mathbb{N}$. Единичная матрицой порядка n называется:

$$E_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \in M_n(R)$$

Как кратко обозначить: $E_n = (\delta_{ij})$, где $\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$ — символ Кронекера

Предложение 1.1. Пусть $A \in M_{m,n}(R)$.

Тогда $E_m A = AE_n = A$

Доказательство.

$E_m A = (b_{ij}),\ A = (a_{ij})$

$b_{ij} = \sum\limits_{k=1}^{m} \delta_{ik} a_{kj} = a_{ij}$

То есть $E_m A = A$

$E_n A^T = A^T \implies (E_n A^T)^T = (A^T)^T \implies (A^T)^T E_n^T = (A^T)^T \implies AE_n = A$

Следствие. $M_n(R)$ — кольцо, где E_n — нейтральный элемент по умножению

Называют кольцом квадратных матриц порядка n.

Замечание. Кольцо не обязательно коммутативное при $n \geqslant 2$

$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

$B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

$A \neq B$

Замечание. $M_1(R) \cong R$

***Определение* 1.6.** $GL_n(R) = M_n(R)^* = \{A \in M_n(R) \mid \exists B \in M_n(R),\ AB = BA = E_n\}$

Такая B единственная и называется обратной к A, обозначается A^{-1}

Предложение 1.2.

1. $E_n \in GL_n(R),\ E_n^{-1} = E_n$
2. $A_1, \dots, A_k \in GL_n(R) \implies \prod\limits_{i=1}^{k} A_i \in GL_n(R),\ (A_1 \dots A_k)^{-1} = A_k^{-1} \dots A_1^{-1}$
3. $A \in GL_n(R) \implies A^T \in GL_n(R),\ (A^T)^{-1} = (A^{-1})^T$

Доказательство.

1. $E_n E_n = E_n E_n = E_n$
2. $(A_1 \dots A_k)(A_k^{-1} \dots A_1^{-1}) = A_1 \dots A_{k-1}(A_k A_k^{-1}) \dots A_1^{-1} = A_1 \dots A_{k-1} A_{k-1}^{-1} \dots A_1^{-1} = A_1 A_1^{-1} = E_n$

   $(A_k^{-1} \dots A_1^{-1})(A_1 \dots A_k) = \dots = A_k^{-1} A_k = E_n$
3. $(A^T \cdot (A^T)^{-1}) = (A^{-1} \cdot A)^T = E_n^T = E_n$

   $((A^T)^{-1} \cdot A^T) = (A \cdot A^{-1})^T = E_n^T = E_n$

***Определение* 1.7.** Матричная единица — это матрица, где все элементы нулевые, кроме одного, который равен единице.

Обозначается как e_{ij}.

Замечание. $A = (a_{ij}) = \sum\limits_{i,j} a_{ij} e_{ij}$

2 Элементарные преобразования и элементарные матрицы

***Определение* 2.1.** Элементарное преобразование 1 типа:

К i строке прибавить j строку, умноженную на $\lambda \in R$. Обозначается $T_{ij}(\lambda)$

***Определение* 2.2.** Элементарное преобразование 2 типа:

Поменять местами i и j строки. Обозначается S_{ij}

***Определение* 2.3.** Элементарное преобразование 3 типа:

Умножить i строку на $\lambda \in R,\ \lambda \neq 0$. Обозначается $D_{ij}(\lambda)$

Замечание. Аналогичные преобразования можно делать с столбцами.

***Определение* 2.4.** Матрица $A \in M_{m,n}(k)$ называется ступенчатой, если существует $0 \leqslant r \leqslant m$ и числа $j_1, \dots, j_r : 1 \leqslant j_1 < \dots < j_r \leqslant n$ такие, что:

1. $a_{kj_k} \neq 0,\ k = 1, \dots, r$
2. $a_{kj} = 0,\ k = 1, \dots, r,\ j < j_k$

3. $a_{kj} = 0,\ k > r$

Предложение 2.1. Любую матрицу можно превратить в ступенчатую с помощью преобразования строк 1 и 2 типа.

Доказательство. (короче Гаусса пишем и работает)

$A = a(i,j) \in M_{m,n}(k)$

Индукция по m.

База: $m = 1$. A ступенчатая по определению.

Переход: $m > 1$:

Если $A = 0$, то A ступенчатая по определению.

j_1 — номер первого ненулевого столбца.

$\exists i : a_{ij_1} \neq 0$

$i \neq 1 \implies$ применим S_{1i}

Таким образом можно считать $a_{1j_1} \neq 0$.

Применим $T_{21}\left(-\frac{a_{2j_1}}{a_{1j_1}}\right), T_{31}\left(-\frac{a_{3j_1}}{a_{1j_1}}\right), \dots, T_{m1}\left(-\frac{a_{mj_1}}{a_{1j_1}}\right)$

Получим $A' = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{mm} & \dots & a_{mn} \end{pmatrix}$

По индукции A' ступенчатая.

***Определение* 2.5.** Окаймленная единичная матрица — матрица вида:

$$\begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

Теорема 2.1. Пусть $A \in M_{m,n}(k)$. Тогда ее можно преобразовать в окаемленную единичную с помощью преобразования строк и столбцов.

Доказательство.

Сделаем A ступенчатой.

Превратим ступеньки разной длины в единичные. (меняя столбцы)

Применим $D_1(a_{11}^{-1}), \dots, D_r(a_{rr}^{-1})$.

Потом будем от верхней строки к нижней превращать их в строки с одной 1 и нулями. (вычитая строки)

***Определение* 2.6.** Элементарная матрица:

«Первого типа»:

Пусть $1 \leqslant i, j \leqslant n, i \neq j, \lambda \in K$

$T_{ij}(\lambda)$ — матрица вида: $\begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & \lambda \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 1 \end{pmatrix} = E_n + \lambda e_{ij}$

«Второго типа»:

$S_{ij} = E_n - e_{ii} - e_{jj} + e_{ij} + e_{ji}$

«Третьего типа»:

$D_i(\lambda) = E_n + (\lambda - 1)e_{ii}$

Предложение 2.2. Пусть $A \in M_{m,n}(k)$. Тогда при элементарных преобразованиях строк $T_{ij}(\lambda), S_{ij}, D_i(\lambda)$ из A получаются матрицы $T_{ij}A, S_{ij}A, D_iA$.

Доказательство.

$T_{ij}A =$ **TODO:** умножить

$S_{ij}, D_i(\lambda)$ — аналогично.

Следствие.

1. $T_{ij}(-\lambda)T_{ij}(\lambda) = E_n$
2. $S_{ij}S_{ij} = E_n$
3. $D_i(\lambda)D_i(\lambda^{-1}) = E_n$

Следствие. $T_{ij}(\lambda), S_{ij}, D_i(\lambda) \in GL_n(k)$ — все они обратимы.

Доказательство.

$A \longrightarrow A'$ — результат прибавления к i столбцу j-го с коэффицентом λ.

$\implies (A')^T = T_{ij}(\lambda)A^T$

$\implies A' = (T_{ij}(\lambda)A^T)^T = (A^T)^T(T_{ij}(\lambda))^T = AT_{ji}(\lambda)$

Аналогично: элементарные преобразования столбцов 2 и 3 типов сводятся к умножению справа на S_{ij} и $D_i(\lambda)$ соответственно.

Предложение 2.3. (PDQ — разложение матриц)

Пусть $A \in M_{m,n}(k)$. Тогда существуют элементарные матрицы $P_1, \dots, P_k \in GL_m(k)$, $Q_1, \dots, Q_l \in GL_n(k)$, окаймленная единичная матрица $D \in M_{m,n}(k)$, такие, что $A = P_1 \dots P_k D Q_1 \dots Q_l$.

Доказательство. Существуют элементарные преобразования строк и столбцов, превращающие A в окаймленную единичную матрицу D.

$\implies D = \underbrace{u_k \dots u_1}_{\text{обратимы}} A \underbrace{v_1 \dots v_l}_{\text{обратимы}}$, где $u_1, \dots, u_k, v_1, \dots, v_l$ — элементарные матрицы

$\implies A = u_1^{-1} \dots u_k^{-1} D v_l^{-1} \dots v_1^{-1}$

Следствие. Пусть $A \in M_n(k)$? Тогда условия эквивалентны:

1. $A \in GL_n(k)$
2. $A = P_1 \dots P_m$, где $P_1, \dots, P_m$ — элементарные матрицы

Доказательство. «2 $\implies$ 1»: так как все $P_i \in GL_n(k)$

«1 $\implies$ 2»:

$A = P_1 \dots P_k D Q_1 \dots Q_l, D = \begin{pmatrix} E_n & 0 \\ 0 & 0 \end{pmatrix}$

$\implies D = P_k^{-1} \dots P_1^{-1} A Q_l^{-1} \dots Q_1^{-1} \implies D \in GL_n(k)$

В D есть нулевая строка $\implies \forall C \in M_n(k)$: в DC есть нулевая строка $\implies DC \neq E_n \implies D = E_n \implies A = P_1 \dots P_k D Q_1 \dots Q_l$

3 Перестановки

***Определение* 3.1.** M — множество. Перестановкой M называется биекция на себя.

$S(M) = \{\text{перестановка } M\}$

$S(M) \times S(M) \to S(M)$

$(g, f) \mapsto g \circ f$

Предложение 3.1. $(S(M), \circ)$ — группа.

Доказательство.

1. Ассоциативность очевидна.
2. id_M — нейтральный элемент.
3. $f \in S(M) \implies f^{-1} \in S(M)$ — обратный элемент.

***Определение* 3.2.** S_n — симметрическая группа степени n (группа перестановок n-элементного множества)

Замечание. $|S_n| = n!$

Пример. $S_3 = \{(1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), (3,2,1)\}$

***Определение* 3.3.** Циклом $(i_1, i_2, \dots, i_k)$ называется $\sigma \in S_n$ такая что $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$, а так же $\sigma(i_j) = i_j$ для всех $j \notin \{1, 2, \dots, k\}$.

$k \geqslant 2$ — длина цикла.

Определение **3.4.** Циклы $(i_1, i_2, \ldots, i_k)$ и $(j_1, j_2, \ldots, j_l)$ называются независимыми, если $i_r \neq j_s \forall r, s$

Предложение 3.2. Любая перестановка является произведением нескольких попарно независимых циклов.