Алгебра

Лектор: Жуков Игорь Борисович

Содержание

1 Элементы теории 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

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

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

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

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 $m \mid (a - b)$.

Свойства.

1. $\underset{m}{\equiv}$ — рефлексивно
2. $\underset{m}{\equiv}$ — симметрично
3. $\underset{m}{\equiv}$ — транзитивно
4. $a \underset{m}{\equiv} b, d \mid m \implies a^d \underset{m}{\equiv} b$
5. $a \underset{m}{\equiv} b, k \in \mathbb{Z} \implies ka \underset{km}{\equiv} kb$
6. $a \underset{m}{\equiv} b, k \in \mathbb{Z} \implies ka \underset{m}{\equiv} kb$
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. $a_1 \underset{m}{\equiv} b_1, a_2 \underset{m}{\equiv} b_2 \implies a_1 a_2 \underset{m}{\equiv} b_1 b_2$

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

      $r \geqslant m \implies r - m \underset{m}{\equiv} a, r - m \geqslant 0, r - m < r$. Противоречие с выбором r.

      Значит $r < m$, тоесть r — искомое.

   b) $a < 0,\ a' = a \pm (-a)m = a(1-m) \geqslant 0$

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

   $|r' - r| < m \implies m \mid (r - r') \implies r' - r = 0$

Следствие.

Теорема о делениии с остатком — $\exists a \in \mathbb{Z}, b \in \mathbb{N} \implies \exists! q, r \in \mathbb{Z}$

1. $a = bq + r,\ 0 \leqslant r < b$
2. $0 \leqslant r < b$

Доказательство.

Существование:

В $\mathbb{Z}/b\mathbb{Z}$ рассмотрим $\overline{a} \in \{\overline{0}, \overline{1}, \ldots, \overline{b-1}\}$, тогда если $\overline{a} = \overline{r},\ 0 \leqslant r < b$

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

Единственность:

$\exists a = bq + r = bq' + r',\ 0 \leqslant r, r' < b \iff \overline{bq + r} = \overline{bq' + r'} \iff \overline{r} = \overline{r'} \iff r = r' \implies bq = bq' \implies q = q'$

***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 — бинарная операция $M \times M \to M$

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

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

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

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

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

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

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

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 выполнены свойство 5.

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

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

***Определение* 4.9.** $\forall x \in \mathbb{R} \exists y \in \mathbb{R} : x + y = n \implies n$ — нейтральный элемент относительно сложения.

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

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

Предложение 4.2. В нашем курсе все кольца будут ассоциативные с единицей.

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

Доказательство.

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

$\exists 0 \cdot A \neq 0 \implies \exists b : b + 0 \cdot A = 0$

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

***Определение* 4.10.** A^* — множество обратимых элементов A.

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, d_2 — ассоциированны.
2. $\exists d_1$ — наибольший общий делитель, d_2 ассоциированн с d_1, тогда d_2 — тоже наибольший общий делитель.

Доказательство.

1. По свойству 2. $d_1 \mid d_2,\ d_2 \mid d_1 \implies d_1,\ d_2$ — ассоциированны.
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 $\exists d' > d_2$.

   $d' \mid a,\ d' \mid b \implies d' \mid d_1$

   $d' \mid d_1,\ d_1 \mid d_2 \implies d' \mid d_2$

   Противоречие

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

1. $\exists d \in \mathbb{Z}: \ a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$
2. при этом d — наибольший общий делитель a, b.

Доказательство.

1. $I = a\mathbb{Z} + b\mathbb{Z}$, заметим что $0 \in I$, так как $0a + 0b = 0$.

   $I = \{0\} \implies I = 0\mathbb{Z}$

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

   То есть в I есть положительные числа.

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

   "$\subset$":

   $d \in I \implies d = ax_0 + by_0, x_0, y_0 \in \mathbb{Z} \implies$

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

   "$\supset$":

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

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

   $d = ax_0 + by_0, x_0, y_0 \in \mathbb{Z}$

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

   Но $r < d \overset{defn(d)}{\implies} r = 0 \implies c \in d\mathbb{Z}$
2. $a = a1 + b0 \in I = d\mathbb{Z} \implies d \mid a$

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

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

   $d' \mid ax_0, \ d' \mid by_0 \implies d' \mid d$

Следствие.

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

Доказательство.

1. Доказали в двух частях предложения.
2. $\exists d_0$ — 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$(a, b) = \gcd(a, b)$ — 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. (!) $\{c : c \mid a_1, c \mid b\} = \{c : c \mid a_2, c \mid b\}$

"$\subset$":

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

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

"$\supset$":

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

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

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

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

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

***Определение* 5.3.** Алгоритм Евклида

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

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. $a_1, \dots, a_m, b_1, \dots, b_n \in \mathbb{Z}$ и $\forall i, j : a_i \perp b_j \implies a_1 \dots a_m \perp b_1 \dots b_n$.
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. $a_1 \perp b, \dots,\ a_n \perp b \implies a_1 \dots a_n \perp b$

   $a_1 \dots a_n \perp b_1, \dots,\ a_1 \dots a_n \perp b_n \implies a_1 \dots a_n \perp b_1 \dots b_n$
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. $d \mid a, d \mid b \implies a = da',\ b = db' : a', b' \in \mathbb{Z}$

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

   $d = 0 \implies a' = b' = 1 = da'm + db'm$

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

7 Линейные диофантовы уравнения

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

Для решения нужно найти пару $(x, y) \in \mathbb{Z}^2 : ax + by = c$.

Пример. $12x + 21y = 5$ — уравнение не имеет решений.

Если $\gcd(a, b) \mid c$, то решение существует, иначе — нет.

TODO: нужно доделать параграф

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

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

Индукция по k:

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

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

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

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

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

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

***Определение* 9.1.** Каноническое разложение(факторизация) числа n — это представление n в виде $p_1^{r_1} \dots p_s^{r_s}$, 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. $\exists a = p_1^{r_1} \dots p_s^{r_s}, b = p_1^{t_1} \dots p_s^{t_s}$

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

Доказательство. "$\Rightarrow$":

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

"$\Leftarrow$":

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

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

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

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

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

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

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

***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

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

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

Доказательство. Проверим корректность:

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

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

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

Для умножения аналогично.

Проверим сюръективность φ

$X = ([a_1]_{m_1}, [a_2]_{m_2})$

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

про сюръективность $\implies$ биекция:

$|Y| = |Z| < \infty$

$\varphi : Y \to Z$

Тогда φ инъективна $\iff$ φ сюръективна

что-то про принцип дирихле и готово)

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 $\forall a \in \{1, 2, \dots, m-1\} \implies$

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

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.** $\mathbb{F}_{p^r}$ — поле из n элементов $\iff$ $n = p^r,\ p \in \mathbb{P},\ r \in \mathbb{N}$

(хз что это)

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

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 11.3. $\exists m, n \in \mathbb{N},\ (m,n) = 1.$

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

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

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

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

Проверка корректности:

$[a]_{mn} = [a']_{mn} \implies ([a]_m, [a]_n) = ([a']_m, [a']_n)$?

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

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

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

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

$\lambda([a]_{mn}) = ([a]_m, [a]_n) = ([b]_m, [c]_n) \implies \lambda$ — 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. $\exists n = p_1^{r_1}, \dots, p_s^{r_s}$ — разложение числа n на простые множители.

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

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

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 $(\mathbb{Z}/m\mathbb{Z})^*$

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

$A^2 = \overline{1} \iff A^2 - \overline{1}^2 = \overline{0} \iff (A-\overline{1})(A+\overline{1}) = \overline{0} \overset{\mathbb{Z}/p\mathbb{Z}-field}{\iff} A - \overline{1} = \overline{0}, A + \overline{1} = \overline{0} = \prod\limits_{A^2=\overline{1}}$

$p \neq 2 \implies \overline{1} \cdot \overline{-1} = \overline{-1}$

$p = 2 \implies \overline{1} = \overline{-1}$

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 $\mathbb{C}$: $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1)$

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.
- $(a, b) z_1 z_2 = (1, 0): \ z_1 = (a, -b), \ z_2 = \frac{1}{a^2+b^2}$

***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

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

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

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

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 $k, l : z_k = z_l$?

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

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

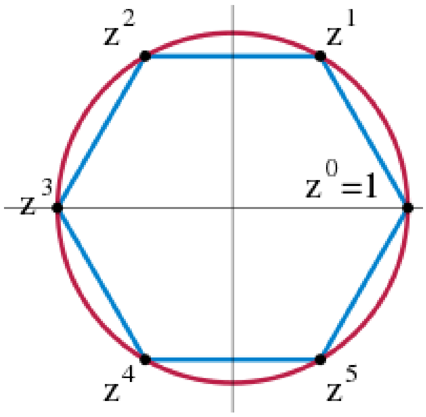
Таким образом, мы доказали:

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

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

$\implies G = \langle g \rangle$

***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 $\varphi_b : A[x] \to B$

$a_nX^n + \ldots + a_1X + a_0 \mapsto a_nb^n + \ldots + a_1b + a_0$ является гомоморфизмом колец.

Доказательство.

Если $f = a_nX^n + \ldots + a_1X + a_0$, то $f(b) = a_nb^n + \ldots + a_1b + a_0 = \varphi_b(f)$

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 $f + g$.

$f = \sum\limits_{i=0}^{n} a_iX^i, g = \sum\limits_{i=0}^{m} c_iX^i$

$fg = \sum\limits_{k=0}^{n+m} d_kX^k, d_k = \sum\limits_{i+j=k} a_ic_j$

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

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

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

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. $A \to A$

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

   $f \xmapsto{\beta} f(0, x_1, x_2, x_3, \ldots)$ — 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. $R = \mathbb{Z}/3\mathbb{Z}$, $f = X, g = X^3$

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