

Конспект лекций по алгебре

Лектор: Игорь Борисович Жуков

Оглавление

Элементы теории чисел	2
1 Делимость	2
2 Отношение эквивалентности и разбиение на классы	2
3 Сравнение по модулю	3
4 Кольцо классов вычетов	4
5 Наибольший общий делитель	6
6 Взаимно простые числа	8
7 Линейные диофантовы уравнения	9
8 Простые числа	9

Элементы теории чисел

1 Делимость

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

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. a и b ассоциированы, если $a \mid b, b \mid a \implies a = \pm b$
7. a, a' и b, b' — ассоциированы, тогда $a \mid b \iff a' \mid b'$
8. $k \neq 0, ka \mid kb \iff a \mid b$

2 Отношение эквивалентности и разбиение на классы

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

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

Теорема. Пусть $M = \bigcup_{i \in I} M_i$ — разбиение на классы, тогда $a \sim b \iff \exists i : a, b \in M_i$.

Доказательство. рефлексивность, симметричность — очевидны
транзитивность: $a \sim b, b \sim c \implies \exists i, j : a, b \in M_i \text{ и } b, c \in M_j$
 $b \in M_i \cap M_j \iff M_i \cap M_j \neq \emptyset \implies i = j \implies a, c \in M_i \implies a \sim c$

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

Доказательство.

$[a] = \{b \in M \mid a \sim b\}$ — класс, $a \in M$

$\forall a_1, a_2 \in M : [a_1] \cap [a_2] = \emptyset$ или $[a_1] = [a_2] \sqsubset [a_1] \cap [a_2] \neq \emptyset \implies \exists x \in [a_1] \cap [a_2]$

$x \in [a_1], x \in [a_2] \implies x \sim a_1, x \sim a_2 \implies a_2 \sim a_1$

$[a_2] \subset [a_1], c \in [a_2] \implies c \sim a_2 \implies c \sim a_1 \implies c \in [a_1]$

$[a_1] \subset [a_2], c \in [a_1] \implies c \sim a_1 \implies c \sim a_2 \implies c \in [a_2]$

Значит $[a_1] = [a_2]$

$I = \{[a] \mid a \in M\}$

$\forall \mathfrak{A}, \mathfrak{B} \in I : \mathfrak{A} \cap \mathfrak{B} = \emptyset$

$a_1, a_2 \in \mathfrak{A} \implies [a_1] = \mathfrak{A} = [a_2] \implies a_2 \in [a_1] \implies a_2 \sim a_1$

$a_1 \in \mathfrak{A}, a_2 \in \mathfrak{B} \implies \neg(a_1 \sim a_2)$, так как иначе $a_1 \in [a_2] \implies \mathfrak{B} \in \mathfrak{A} \implies \mathfrak{A} \cap \mathfrak{B} \neq \emptyset$

Определение. Фактор-множество по отношению эквивалентности \sim — множество I , обозначим его как M/\sim

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

3 Сравнение по модулю

Определение. $\exists a, b, m \in \mathbb{Z}$. Говорят, что $m \mid (a - b)$.

Свойства:

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

4 Кольцо классов вычетов

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

Обозначается как $\mathbb{Z}/m\mathbb{Z} \iff \mathbb{Z}/m \iff \mathbb{Z}/\equiv_m$

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

1. $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$

2. $|\mathbb{Z}/m\mathbb{Z}| = m$

Доказательство.

1. $a \in \mathbb{Z} (!)\bar{a} = \bar{r}, 0 \leq r < m$

а) $a \geq 0$, $\exists r$ — наименьшее число, такое что $r \geq 0, a \equiv_m r$
 $r \geq m \implies r - m \equiv_m a, r - m \geq 0, r - m < r$. Противоречие с выбором r .
 Значит $r < m$, то есть r — искомое.

б) $a < 0$, $a' = a \pm (-a)m = a(1 - m) \geq 0$
 $\bar{a} = \bar{a'} = \bar{r}, 0 \leq r < m$

2. предположим $\bar{r} = \bar{r'}, 0 \leq r, r' < m$.
 $|r' - r| < m \implies m \mid (r - r') \implies r' - r = 0$

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

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

2. $0 \leq r < b$

Доказательство.

Существование:

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

$$a \equiv_b r \iff a = bq + r, q \in \mathbb{Z}$$

Единственность:

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

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

Определение. Операция на множестве M — бинарная операция $M \times M \rightarrow M$

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

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

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

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

Пример:

$m = 4, \mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

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

Предложение. 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. $A + \bar{0} = A$ — существование нейтрального элемента относительно сложения
4. $A + A' = \bar{0}$ — существование обратного элемента относительно сложения
5. $AB = BA$ — коммутативность умножения
6. $(AB)C = A(BC)$ — ассоциативность умножения
7. $A \cdot \bar{1} = A$ — 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. Кольцом называется множество M с операциями сложения и умножения, для которых выполнены аналоги свойств 1-4 и 8-9.

Определение. Кольцо коммутативное, если выполнены свойство 5.

Определение. Кольцо ассоциативное, если выполнено свойство 6.

Определение. Кольцо с единицей, если выполнено свойство 7.

Определение. $\forall x \in R \exists y \in R : x + y = n \implies n$ — 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. В нашем курсе все кольца будут ассоциативные с единицей.

Лемма. 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. A^* — множество обратимых элементов A .

Примеры:

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

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

5 Наибольший общий делитель

Определение. 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.

1. d_1, d_2 — наибольшие общие делители, тогда d_1, d_2 — ассоциированы.

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

Доказательство.

1. По свойству 2. $d_1 \mid d_2, d_2 \mid d_1 \implies d_1, d_2$ — ассоциированы.
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. $\exists a, b \in \mathbb{Z} \implies$

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 ":
 $d \in I \implies d = ax_0 + by_0, x_0, y_0 \in \mathbb{Z} \implies$
 $\forall z \in \mathbb{Z} : dz = a(x_0z) + b(y_0z) \in I$
 " \supset ":
 $\exists c \in I, d \in \mathbb{N} \implies \exists q, r \in \mathbb{Z} : c = dq + r, 0 \leq r < d$
 $c = ax_1 + by_1, x_1, y_1 \in \mathbb{Z}$
 $d = ax_0 + by_0, x_0, y_0 \in \mathbb{Z}$
 $r = c - dq = a(x_1 - x_0q) + b(y_1 - y_0q) \in I$
 Но $r < d \xrightarrow{\text{defn}(d)} r = 0 \implies c \in d\mathbb{Z}$
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 $d_0 \implies d = d_0\mathbb{Z}, z \in \mathbb{Z} \implies d = a(x_0z) + b(y_0z)$

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

Предложение. $\exists a_1, a_2, b \in \mathbb{Z} : a_1 \equiv_b a_2$

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. Алгоритм Евклида
 $\gcd(a, b) = \gcd(b, a \bmod b)$, если $b \neq 0$

6 Взаимно простые числа

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

Предложение.

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. $ax \equiv_m ay, a \perp m \implies x \equiv_m y$.
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. $1 = a_1m_1 + bn_1, 1 = a_2m_2 + bn_2 \implies 1 = a_1a_2(m_1m_2) + b(a_1m_1n_2 + a_2m_2n_1 + bn_1n_2) \implies a_1a_2 \perp b.$
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. $m \mid (ax - ay), a \perp m \implies m \mid (x - y) \implies x \equiv_m y.$
6. $d \mid a, d \mid b \implies a = da', b = db' : a', b' \in \mathbb{Z}$
 $d = am + bn, m, n \in \mathbb{Z}$
 $d = 0 \implies a' = b' = 1 = da'm + db'n$
 $d \neq 0 \implies 1 = a'm + b'n \implies a' \perp b'.$

7 Линейные диофантовы уравнения

Определение. 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.

нужно доделать параграф

8 Простые числа

Определение. 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, $a \in \mathbb{Z} \implies p \mid a$ или $p \perp a$.
3. p, q — простые $\implies p, q$ — ассоциированы или $p \perp q$.

4. $p \mid ab \implies p \mid a$ или $p \mid b$.

Предложение. $\exists a \neq \pm 1$, 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. Составное число — это число отличное от 0, и не являющееся простым.