Факультет математики и компьютерных наук — 2024 - 2025

Конспект по Алгебре

Фёдоров Павел

1 курс МКН, Санкт-Петербург

04.09.24

Определение кольца

Пусть имеется не пустое множество A и две операции (сложение и умножение). Тогда тройка вида $(A, +, \cdot)$ будет называться кольцом, если выполнены следующие аксиомы.

1. $\forall a, b, c \in \mathbb{R} \quad (a+b)+c = a+(b+c)$ — ассоцитативность по сложению
2. $\exists 0 \in \mathbb{R} \quad \forall a \in \mathbb{R} \quad a+0 = 0+a = a$ — наличие нейтрального элемента по сложению
3. $\forall a \in \mathbb{R} \quad \exists b \in \mathbb{R} \quad a+b = b+a = 0$ — Наличие обратного элемента по сложению

   Утверждение. *Если ноль существует, то он единственный.*

   Доказательство. Пусть существуют два ноля: $0, 0'$. Тогда рассмотрим следующую сумму: $0 = 0 + 0' = 0'$ ∎

4. $\forall a, b \in \mathbb{R} \quad a+b = b+a$ — коммутативность по сложению
5. $\forall a, b, c \in \mathbb{R} \quad (a+b)c = ac+bc$ — дистрибутивность(правая, но есть коммутативность, поэтому и левая)
6. $\forall a, b \in \mathbb{R} \quad ab = ba$ — коммутативность по умножению
7. $\forall a, b, c \in \mathbb{R} \quad (ab)c = a(bc)$ — ассоцитативность по умножению
8. $\exists 1 \in \mathbb{R} \quad \forall a \in \mathbb{R} \quad a \cdot 1 = 1 \cdot a = a$ — Наличие нейтрального элемента по умножению
9. $\forall a \in \mathbb{R} \quad \exists a^{-1} \in \mathbb{R} \quad a(a^{-1}) = 1$ — Наличие обратного элемента по умножению

Если выполнены свойства 1-5, то данная структура называется кольцом. Если выполнена свойтсва 1-8, то структура наывается ассоциативным кольцом с единицей, а если 1-9, то структура называется полем.

Примеры колец

- $(\mathbb{Z}, +, \cdot)$ – кольцо целых чисел
- $(0, +, \cdot)$ – тривиальное кольцо
- Следующий пример слегка интереснее. Пусть $d \in \mathbb{N}$ $\sqrt{d} \notin \mathbb{Z}$
  $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a \in \mathbb{Z}, b \in \mathbb{Z}\}$
  Определим операции следующим образом:
  $(a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{d}$
  $(a_1 + b_1\sqrt{d}) \cdot (a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + b_1a_2)\sqrt{d}$

Эти три примера являются самыми типичными примерами колец. А теперь перейдём к примерам колец, которые являются полями.

- $(\mathbb{Q}, +, \cdot)$ – Поле рациональных чисел
- $(\mathbb{R}, +, \cdot)$ – Поле вещественных чисел
- $(\mathbb{C}, +, \cdot)$ – Поле комплексных чисел

Также, пусть A, B – кольца. Тогда $A \times B$ – Прямое произведение, тоже кольцо.

Предложение. $x_1 \cdot x_2 \cdot ... \cdot x_n$ *– не зависит от расстоновки скобок*

Доказательство. Воспользуемся методом математической инукции.
База: $n = 3$ – простая ассоциативность по умножению
Переход: Будем называть произведение левонормированным, если его можно представить, как $((((x_1x_2)x_3)x_4)x_5...)$.
Рассмотрим число k – это номер, такой что $x_1 \cdot ... \cdot x_k$ левонормированно. Тогда рассмотрим два случая.

1. $k = n - 1$. Тогда всё очевидно
2. $k < n - 1$. Тогда вынесем x_n за всё произведение и сново получим слева левонормированное произведение.

■

Замечание. $(-ab) = (-a)b$

Доказательство. $(-a)b + ab = 0 \cdot b = (0 + 0) \cdot b = 0 \cdot b + 0 \cdot b = 0$(сократим на $0 \cdot b$)
$-(ab) + ab = 0$ ■

Определение Идеала Кольца

Определение 1. *Не пустое* $I \subseteq A$. *Тогда* I *называется идеалом кольца, если*

1. $x, y \in I \Rightarrow x + y \in I$
2. $x \in I \,\&\, a \in A \Rightarrow ax \in I$

Заметим, что если $1 \in I$, то в идеале содержится любой элемент множества A. Тогда $I = A$. Кроме того, по очевидным размышлениям, $0 \in I$.

$(0) = \{0\}$ – нулевой идеал
$I = A$ – единичный идеал

Идеалы целых чисел

Теорема. *Все идеалы множества $\mathbb{Z}$ представимы в виде $k\mathbb{Z}$*

Доказательство. Пусть имеется не нулнвой идеал I, тогда в нём существуют не нулевые и положительные числа. Пусть k - наименьший такой элемент

$\subseteq$: Рассмотрим элемент из идеала I. Тогда $x = kq + r$, где $0 \leqslant r < k$. Заметим, что $r = x - kq \in I \Rightarrow r = 0 \Rightarrow$ любой элемент является элементом $k\mathbb{Z}$

$\supseteq$: Очевидно

■

Ещё примеры идеалов

Пусть $a_1, a_2, a_3, ..., a_n \in A$, тогда обозначим за $(a_1, a_2, a_3, ..., a_n) = \{\sum_{i=1}^{n} a_i x_i | x_i \in A\}$. Это идеал. Проверим

1. $\sum_{i=1}^{n} a_i x_i + \sum_{i=1}^{n} a_i y_i = \sum_{i=1}^{n} a_i (x_i + y_i)$

2. $b \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i b x_i \in (a_1, a_2, a_3, ..., a_n)$

Оба предложения верны, поэтому это действительно идеал.

06.09.24

Определение 2. *Ненулевое кольцо называется* ***областью целостности****, если у него нет делителей нуля. Иными словами, если $ab = 0 \Leftrightarrow a = 0 \vee b = 0$*

Примеры

- $\mathbb{Z}$ - является областью целостности
- Любое поле является областью целостности
- $\mathbb{Z}[\sqrt{d}]$ – является областью целостности
- $A \times B = \{(a, b) | a \in A, b \in B\}, A \neq \varnothing, B \neq \varnothing$ – НЕ является областью целостности.

Определение 3. *Идеал называется **главным**, если он порождён одним элементом.* $I = (a), a \in A$

Определение 4. *Область целостности, в которой любой идеал главный называется **кольцом главных идеалов***

Заметим, что если кольцо является полем, то все идеал либо нулевой, либо единичный, так как есть обратный по умножению.
Вопрос, который из всего этого возникает, а есть ли область целостности, не являющаяся кольцом главных идеалов.
Рассмотрим следующее множество: $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a \in A, b \in B\}$.
Рассмотрим следующее множество: $I = \{a + b\sqrt{-5} | a \in A, b \in B, (b - a) \vdots 2\}$
Простой проверкой в лоб можно понять, что это множество замкнуто относительно сложения и умножения, а также, что оно удовлетворяет обоим свойтсвам идеала. Поэтому I – идеал A. Теперь надо проверить, что он не главный.

Доказательство.

$$2 + 0\sqrt{-5} = (a + b\sqrt{-5})(x + y\sqrt{-5})$$
$$2 - 0\sqrt{-5} = (a - b\sqrt{-5})(x - y\sqrt{-5})$$

Теперь перемножем оба эти равенства и получим

$$4 = (a^2 + 5b^2)(x^2 + 5y^2)$$

Понятно, что если $b \neq 0$, то данное тождество не может иметь решений, поэтому $b = 0$.

$a = \pm 1$: В этом случае в идеале должно лежать число $1 + 0\sqrt{-5}$, что невозможно

$a = \pm 2$: В этом случае идеал содержит число $-2 + 0\sqrt{-5}$, а значит $I = (2)$. Однако число $1 + \sqrt{-5}$, которое лежит в идеале не кратно ему.

Таким образом идеал не главный. ∎

Определение 5. *Классом элемента по идеалу называется такое множество* $x + I = \{x + i | i \in I\}$

Определение 6. *Факторкольцом по идеалу называется такое множество* $A/I = \{x + I | x \in A\}$. *Иными словами это множество всех классов.*

Утверждение. *Два класса либо непересекаются, либо совпадают.*

Доказательство. Пусть это не так, пусть существует $c \in (x + I) \cap (y + I)$.
Тогда $c = x + i_1 = x + i_2 \Rightarrow i_3 = x - y = i_2 - i_1$. Тогда $x + I = y + (i_3 + I)$ Заметим тогда, что $i_3 + I \subset I$, таким образом мы получаем, что классы действительно совпадают. ∎

Так же заметим, что $x_1 + I = x_2 + I \Leftrightarrow x_2 - x_1 \in I$.

Операции над классами

- Пусть $C_1 = x_1 + I, C_2 = x_2 + I$ – два класса. Тогда сумма этих двух классов
$$C_1 + C_2 = x_1 + x_2 + I$$
.

  Утверждение. *Такое определение суммы коректно.*

  Доказательство. Пусть $C_1 + C_2 = x_1 + x_2 + I = y_1 + y_2 + I$.
  Тогда рассмотрим $(y_1 + y_2) - (x_1 + x_2) = (y_1 - x_1) + (y_2 - x_2) \in I$, так как каждое слогаемое тут лежит в I ∎

- Пусть $C_1 = x_1 + I, C_2 = x_2 + I$ – два класса. Тогда произведение этих двух классов
$$C_1 \cdot C_2 = x_1 \cdot x_2 + I$$
.

  Утверждение. *Такое определение произведения коректно.*

  Доказательство. Пусть $C_1 \cdot C_2 = x_1 \cdot x_2 + I = y_1 \cdot y_2 + I$.
  Тогда рассмотрим $(y_1 \cdot y_2) - (x_1 \cdot x_2) = y_1(y_2 - x_2) + x_2(y_1 - x_1) \in I$, так как каждое слогаемое тут лежит в I ∎

Пример Факторкольца

- $\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, ..., n - 1 + n\mathbb{Z}\}$

Морфизмы колец

Определение 7. *Пусть A, B – два кольца, $f : A \to B$.*
Тогда f называется ***гомоморфизмом колец****, если*

1. $\forall a_1, a_2 \in A \quad f(a_1 + a_2) = f(a_1) + f(a_2)$
2. $\forall a_1, a_2 \in A \quad f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$
3. $f(1_A) = 1_B$

Предложение. $f(0_A) = 0_B$

Доказательство. $f(0) = f(0 + 0) = f(0) + f(0) \Rightarrow 0 = f(0)$ ∎

Замечание. Третья акисомы не нужна в поле, но нужна в кольце, так как нет обратног элемента.

Определение 8. ***Мономорфизм*** *это гомоморфизм, для которого верно, что*
$\forall a_1, a_2 \quad f(a_1) = f(a_2) \Rightarrow a_1 = a_2$

Определение 9. ***Эпиморфизм*** *это гомоморфизм, для которого верно, что*
$\forall b \in B \quad \exists a \in A \quad f(a) = b$

Определение 10. ***Изоморфизм*** *это мономорфизм и эпиморфизм одновременно*

11.09.24

Операции над идеалами

1. Пересечение идеалов. Определыется так же как и пересечение множест и очевидно, что пересечение идеалов как множеств является идеалом.

2. Сумма идеалов. $\sum I_i = \{\alpha_1 + \alpha_2 + ... + \alpha_k \mid \alpha_i \in I_i\}$

3. Произведение идеалов. $\prod I_i = \{x_1 x_2 x_3 ... x_n \mid x_i \in I_i\}$

4. Два идеала называются взаимнопростыми, если $I + J = (1)$

Теорема (Китайская теорема об остатках(КТО))**.**

Пусть A - кольцо, $n \geqslant 2$, $I_1, I_2, I_3, ..., I_n$ и $I_i + I_j = (1)$. Тогда

$$\exists \varphi : A/_{\bigcap\limits_{i=1}^{\infty} I_i} \to A/I_1 \times A/I_2 \times ... \times A/I_n$$

Доказательство.
Рассмотрим отображение $\overline{a}(mod\ I_1 \cap I_2 \cap ... \cap I_n) \longmapsto (\overline{a}(mod\ I_1) \cdot \overline{a}(mod\ I_2) \cdot ... \cdot \overline{a}(mod\ I_n))$

- Докажем, что отображение корректно.
  Для этого пусть $a + I_1 \cap I_2 \cap ... \cap I_n = a' + I_1 \cap I_2 \cap ... \cap I_n \ \Rightarrow\ a' - a \in I_1 \cap I_2 \cap ... \cap I_n \subset I_i\ \forall i$

- Докажем, что данное отображение является гомоморфизмом. Для этого проверим свойства.

  - Нужно доказать, что $f(\overline{a} + \overline{b}) = f(\overline{a}) + f(\overline{b})$. Разложим левую и правую часть.
    $f(\overline{a}+\overline{b}) = ((\overline{a}+\overline{b})(mod\ I_1) + (\overline{a}+\overline{b})(mod\ I_2) + (\overline{a}+\overline{b})(mod\ I_3) + ... + (\overline{a}+\overline{b})(mod\ I_n))$
    $f(\overline{a}) + f(\overline{b}) = ((\overline{a}(mod\ I_1) + ... + \overline{a}(mod\ I_n)) + (\overline{b}(mod\ I_1) + ... + \overline{b}(mod\ I_n))) =$
    $= ((\overline{a} + \overline{b})(mod\ I_1) + ... + (\overline{a} + \overline{b})(mod\ I_n))$
  - Тоже самое, но про умножение доказывается абсолютно аналогично.

- Докажем, что это Мономорфизм.
  Пусть $\overline{a}(mod\ I_1) \cdot ... \cdot \overline{a}(mod\ I_n) = \overline{b}(mod\ I_1) \cdot ... \cdot \overline{b}(mod\ I_n)$
  Тогда $(a-b) \in I_1,\ (a-b) \in I_2, ..., (a-b) \in I_n \ \Rightarrow\ (a-b) \in \cap I_i \ \Rightarrow\ \overline{a}(mod\ \cap I_i) = \overline{b}(mod\ \cap I_i)$

- Теперь докажем, что это эпиморфизм. Для этого сначала докажем две леммы.

  Лемма. $I_1 + I_2 = (1) \ \Rightarrow\ A/_{I_1 \cap I_2} \simeq A/I_1 \times A/I_2$

  Доказательство. Нужно найти $a \in A \quad a - b \in I_1,\ a - c \in I_2$
  $a = b + i_1 = c + i_2 \ \Leftrightarrow\ b - c = i_2 - i_1$ тогда $i_1 = (c-b)x_1, \quad i_2 = (c-b)x_2$
  $I_1 + I_2 = (1) \ \Rightarrow\ x_1 + x_2 = 1\ \ x_1 \in I_1,\ x_2 \in I_2 \ \Rightarrow\ (b-c)x_1 + (b-c)x_2 = (b-c)$ ■

  Лемма. *Пусть $I_1, I_2, ..., I_n$ – Идеалы, $I_1 + I_i = (1)\ \forall i \geqslant 2$, то $I_1 + \bigcap\limits_{i \geqslant 2} I_j = (1)$*

Доказательство. $x_2, x_3, x_4, ..., x_n \in I_1 \quad y_2 \in I_2,\ y_3 \in I_3, ..., y_n \in I_n,\ x_i + y_i = 1.$

Тогда возьмём и перемножим все эти равентва. Получиться следующее:

$$(x_2 + y_2)(x_3 + y_3) + ... + (x_n + y_n) \ = \ 1$$

.

Тогда если раскрыть все скобки, то получится $y_1 \cdot y_2 \cdot y_3 \cdot ... \cdot y_n + A$, где все слагаемые из A лежат в идеале, а Также

$$y_2 \cdot y_3 \cdot ... \cdot y_n \in I_1 \cdot I_2 \cdot ... \cdot I_n \subset I_1 \cap I_2 \cap ... \cap I_n$$

∎

Теперь соберём все вместе. По первой лемме ясно, что существует изоморфизм

$$\varphi : A/_{I_1 \cap I_2 \cap ... \cap I_n} \to A/I_1 \times A/I_2 \times ... \times A/I_n$$

Ну а тогда по индукции существует и искомый изоморфизм. Что и требовалось доказать.

∎

Простые и максимальные идеалы

Определение 11. *Идеал называется **простым**, если*

1. $I \neq (1)$
2. $\forall x, y \notin I \quad xy \notin I$

Определение 12. *Идеал называется **максимальным**, если*

1. $I \neq (1)$
2. $I \subsetneqq J \ \Rightarrow \ J = (1)$

Теорема. *Любой максимальный идеал простой.*

Доказательство. Пусть $\forall x, y \notin I \ \&\ xy \in I$.

$$\begin{cases} I \subseteq I + (x) \\ I \subseteq I + (y) \end{cases} \quad \Rightarrow \quad \begin{cases} i_1 + ax = 1 \\ i_2 + by = 1 \end{cases} \quad = \quad i_1 i_2 + i_1 by + i_2 ax + abxy = 1 \ \Rightarrow \ 1 \in A$$

∎

Примеры

Утверждение. *В $A = \mathbb{Z}$ все максимальные идеалы совпадают – идеалы заделанные простыми числами.*

Доказательство.

1. $a = 0:$ Не годится, идеал нулевой, содержится во всех
2. $a = 1:$ Не годится, идеал единичный
3. $a \geqslant 2:$
   - 3.1. $a = bc, \;\; b \neq 1 \neq c \;\; \Rightarrow \;\; (a) \subseteq (b)$
   - 3.2. a - простое $= p$. $(p) \subseteq (p) + (x) \subseteq Z \quad \Rightarrow \quad p \vdots b \;\; \Rightarrow \;\; b = 1 \vee b = p \;\Rightarrow$ противоречие в обоих случаях

■

Утверждение. *$I \subseteq A$ - идеал.*

- *I - простой $\Leftrightarrow A/I$ - область целостности*
- *I - максимальный $\Leftrightarrow A/I$ - поле*

Доказательство.

$\Rightarrow: \;\; x \in I, y \in I, xy \notin I \quad \Rightarrow \quad xy + I \neq 0 + I$

$\Leftarrow: \;\; xy + I \neq I \quad \Rightarrow \quad xy \notin I$

■

13.09.24

Евклидовы кольца

Определение 13. *Область целостности A называется* ***Евклидовым кольцом****, если существует норма $(\| \,\| : A \smallsetminus \{0\} \to \mathbb{N} \cup \{0\})$, такая что*

$$\forall a, b \in A, b \neq 0: \;\; \exists q, r \in A \quad a = bq + r, \quad r = 0 \vee \|r\| < \|b\|$$

Пример. Если $A = \mathbb{Z}$, то $\|b\| = |b|$

Теорема.
Любое евклидово кольцо является кольцом главных идеалов.

Доказательство. Пусть I – ненулевой идеал, рассмотрим $a \in I$, такой что $\|a\| = \min\limits_{i \in I \setminus \{0\}} \|i\|$
$i \in I \Rightarrow i = aq + r, r \neq 0 \Rightarrow r = i - aq \in I \Rightarrow \|r\| < \|a\| \Rightarrow I \subset (a) \Rightarrow I = (a)$

■

Утверждение. *Обратное неверно.*

Доказательство. Рассмотрим множество $A = \left\{\frac{a+b\sqrt{-19}}{2} \mid a, b \in \mathbb{Z},\ a \equiv b (mod\, 2)\right\}$. Данное кольцо является кольцом главных идеалов, но не является евклидовым. Доказательство выходит за рамки курса.

■

Обратимые и неразложимые элементы

Определение 14. *Пусть A – область целостности. Тогда $a \in A$ называется **обратимым**, если $\exists b \in A \quad ab = 1$*

Определение 15. *Пусть A – область целостности. Тогда $a \in A$ называется **неразложимым**, если*

1. *a не обратимый*
2. *$a = bc \Leftrightarrow b$ – обратимый или c – обратимый*

Утверждение. *(a) – простой $\Rightarrow$ a – неразложимый*

Доказательство. $a = bc \in (a) \Rightarrow b \in (a) \vee c \in (a) \Rightarrow b = ad \Rightarrow a = adc \Rightarrow bc = 1 \Rightarrow$ c – обратимый $\Rightarrow a$ – обратимый

■

Утверждение. *a – неразложимый $\Rightarrow (a)$ – простой неверно.*

Доказательство. В качестве контрпримера возьмём $\mathbb{Z}[\sqrt{-5}]$ ■

Определение 16. *Область целостности A называется **факториальным кольцом**, если $\forall 0 \neq a \in A$:*

1. *$a = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n$, где u – обратим, p_i – неразложимый*
2. *$a = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n = v \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_m \Rightarrow m = n$ и существует отображение $q_i = p_{\pi(i)} \cdot u_i$, где u_i – обратимы.*

Теорема. *Кольцо главных идеалов явлется факториальным кольцом*

Доказательство.

1. **Существование:** $a = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n$, где u – обратим, p_i – неразложимый.
   Пусть существует такое ненулевое a, у которого нет такого разложения. Тогда построим цепочку вложенных главных идеалов.

$$(a) \subset (a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset \ldots,\ \ a_i \in A$$

Лемма. *Докажем, что такая цепочка главных идеалов стабилизируется.*

Доказательство. Рассмотрим обьединение всех идеалов из этой цепочки $\bigcup\limits_{k=1}^{\infty}(a_n) = (b)$, так как объединения идеалов тоже идеал в этом же кольце, а у нас кольцо главных идеалов, значит любой идела главный.

$x, y \in \bigcup\limits_{k=1}^{\infty}(a_n) \quad x \in (a_k),\ y \in (a_s) \Rightarrow xy \in (a_s) \Rightarrow x + y \in (a_s)$

Заметим, что так как идеал (b) это идеал равный обьединению других идеалов, то $\exists n\ \ b \in (a_n)$. Но тогда он лежит и в каждом следующем.

Тогда $b \in (a_n) \Rightarrow (b) \subset (a_n) \subset (b) \Rightarrow (b) = (a_n)$. По аналогии $(b) = (a_i),\ \ i \geqslant n$

∎

Вернёмся к доказательству теоремы. Рассмотрим $a \in A$ и пусть он не неразложимый. Тогда $a = bc$, b, c оба необратимые и либо одно, либо второн не разлагается в произведение неразложимых. Пусть b.

$$(a) \subset (b) \Rightarrow b = a \cdot d \Rightarrow a = adc \Rightarrow c \text{ — обратимый (противоречие)}$$

2. **Единственность:** Рассмотрим два разложения $a = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n = v \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_m$
   Проведём индукцию по m.

   - **База:** $m = 0$ — очевидно.
   - **Переход:** $m > 0$. Тогда $u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n \in (q_m)$ и q_m – простой.
     Тогда $p_n \in (q_m) \Rightarrow p_n = q_m \cdot u_m$. В этом случае равенство

     $$a = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n = v \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_m$$

     Примет вид

     $$a = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot q_m \cdot u_m = v \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_m$$

     И перейдёт

     $$a = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} \cdot u_m = v \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_{m-1}$$

     А дальше по индукции. Тогда действительно $n = m$ и существует биекция.

∎

18.09.24

Вспомним, что любое евклидово кольцо является областью главных идеалов, а любая область главных идеалов является факториальным кольцом.

Цель на этой лекции понять, для каких простых чисел существует разложение в сумму целых квадратов. Для начала рассмотрим частные случаи.

- $2 = 1^2 + 1^2$

- $p = 4k + 3 \Rightarrow a = 2m,\ b = 2n + 1 \Rightarrow a^2 + b^2 = 4l + 1$ противоречие
- $p = 4k+1$. В этом случае на маленьких числах легко проверить наличие разложения. А на больших?

Утверждение. *Кольцо $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ евклидово по норме $\|u + vi\| = u^2 + v^2$*

Доказательство. Рассмотрим $a + bi, c + di \in \mathbb{Z}$, $c + di \neq 0$, $a + bi$ не кратно $c + di$ в этом кольце.
Тогда поделим эти два числа просто в поле $\mathbb{C}$: $\frac{a+bi}{c+di} = \alpha + \beta i$, где $\alpha, \beta \in \mathbb{Q}$. Понятно, что найдутся такие u, v, для которых

1. $|u - \alpha| \leqslant \frac{1}{2}$
2. $|v - \beta| \leqslant \frac{1}{2}$

Тогда распишем через них α и β.

$$a + bi = (c + di)(\alpha + \beta i) = (c + di)(u + vi) + (c + di)((\alpha - u) + (\beta - v)i)$$

$a + bi$ – делимое, $c + di$ – делитель, $u + vi$ – частное и $(c + di)((\alpha - u) + (\beta - v)i)$ – остаток. Нам нужно доказать, что норма отстатка меньше нормы делителя.

$$\|(c + di)((\alpha - u) + (\beta - v)i)\| = (c^2 + d^2)((\alpha - u)^2 + (\beta - v)^2) \leqslant (c^2 + b^2)(\frac{1}{4} + \frac{1}{4}) = \frac{1}{2}(c^2 + d^2)$$

■

Теперь мы хотим понять, а сколько сущесвтует обратимых элементов в кольце $\mathbb{Z}[i]$. Ну, пусть нашёлся элемент $a + bi$ такой, что для него существует обратный $c + di$

$$\left.\begin{matrix}(a + bi)(c + di) = 1\\(a - bi)(c - di) = 1\end{matrix}\right\} \Rightarrow (a^2 + b^2)(c^2 + b^2) = 1 \Rightarrow a^2 + b^2 = 1 \Rightarrow \begin{cases}a = \pm 1, b = 0\\ a = 0, b = \pm 1\end{cases}$$

Таким образом у нас только четыре обратимых элементов в $\mathbb{Z}[i]$, а именно $1, -1, i, -i$.

Теорема. *Если p – простое, то $\mathbb{Z}/p\mathbb{Z}$ – поле.*

Доказательство. Нужно доказать, что любой элемент имеет обратный по умножению. Для этого рассмотрим множество всех не нулевых классов в $\mathbb{Z}/p\mathbb{Z}$ и домножим его на ненулевой класс от туда же. Так вот утверждается, что эта операция эквивалентна перестановке. Ну-с, рассмотрим $\{\overline{1}, \overline{2}, ..., \overline{p-1}\} \to \{\overline{1} \cdot \overline{a}, \overline{2} \cdot \overline{a}, ..., \overline{p-1} \cdot \overline{a}\}$. Что бы доказать, что это действительно перестановка нужно доказать, что ничто не обратится в ноль и два класса не совпадут.

1. Ну пусть нашлось такое k, что $\overline{k} \cdot \overline{a} = \overline{0} \Rightarrow ka \vdots p$ противоречие
2. Пусть $\overline{k_1} \cdot \overline{a} = \overline{k_2} \cdot \overline{a} \Rightarrow (k_1 - k_2) \cdot a \vdots p \Rightarrow k_1 = k_2$

Таким образом, так как это перестановка, то какой-то элемент перейдёт в $\overline{1}$. Тогда $\overline{a}$ является его обратным по умножению. А так как перестановки всегда отличаются, то и для любого элемента найдётся обратный.

■

Теорема (Вильсона)**.** *Пусть p – простое, тогда* $(p-1)!+1 \vdots p$

Доказательство. Рассмотрим $p \geqslant 5$. Тогда рассмотрим множетво $W = \left\{\overline{2}, \overline{3}, ..., \overline{p-2}\right\}$. Понятно, что для любого $\overline{a} \in W$ найдётся $\overline{b} \in W$ такой что $\overline{a} \cdot \overline{b} = \overline{1}$. Тогда данное множество можно представить следующим образом.

$$W = \left\{\overline{2}, \overline{3}, ..., \overline{p-2}\right\} = \left\{\overline{a_1}, \overline{b_1}\right\} \cup \left\{\overline{a_2}, \overline{b_2}\right\} \cup ... \cup \left\{\overline{a_{\frac{p-3}{2}}}, \overline{b_{\frac{p-3}{2}}}\right\}$$

В каждой получившейся паре будут взаимнообратные элементы. Тогда

$$\overline{2} \cdot \overline{3} \cdot ... \cdot \overline{p-2} = \overline{1}$$

А тогда

$$\overline{1} \cdot \overline{2} \cdot \overline{3} \cdot ... \cdot \overline{p-1} = \overline{p-1} = \overline{-1}$$

Ну а это и означает, что $(p-1)!+1 \vdots p$

■

Пусть $p = 4k+1$ простое. Тогда расположим остатки от деления следующим образом.

$$\overline{-\frac{p-1}{2}}, ..., \overline{-2}, \overline{-1}, \overline{1}, \overline{2}, ..., \overline{\frac{p-1}{2}}$$

Так как $p = 4k+1$, то $\frac{p-1}{2} = 2k$, то бишь чётное, то если их перемножить получится $\overline{1}$
Тогда по Теореме Вильсона $(\frac{p-1}{2})!^2 + 1 \vdots p$.
Рассмотрим $x = (\frac{p-1}{2})!$. Тогда $x^2+1 \vdots p \Rightarrow (x+i)(x-i) \vdots p$ в $\mathbb{Z}[i]$. В этом случае p не может быть неразложимым. Тогда в $\mathbb{Z}[i]$

$$\left.\begin{aligned} p &= (a+bi)(c+di) \\ p &= (a-bi)(c-di) \end{aligned}\right\} \Rightarrow p = (a^2+b^2)(c^2+b^2) \Rightarrow a^2+b^2 = p \text{ и } c^2+d^2 = p$$

Последний переход верен, потому что ни один из множителей не равен 1. Если бы это было так, то p был бы обратим. Собственно мы и получили что хотели.

Теперь докажем единственность такого представления. Ну пусть $p = a^2+b^2 = a_1^2+b_1^2$, тогда $p = (a+bi)(c+di) = (a_1+b_1 i)(c_1+d_1 i)$. Ну, тогда пусть

$$\left.\begin{aligned} a+bi &= (r+si)(\tilde{r}+\tilde{s}i) \\ a-bi &= (r-si)(\tilde{r}-\tilde{s}i) \end{aligned}\right\} \Rightarrow p = (r^2+s^2)(\tilde{r}^2+\tilde{s}^2) \text{ противоречие}$$

Тогда $a+bi = (a_1 \pm b_1 i) \cdot u$, где $u \in \{-1, 1, -i, i\}$. При выполнении полного перебора станет ясно, что разложение единственно. Таким образом разложение единственно.

Дальше стоит заметить, что

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$$

То есть произведение сумм квадратов снова сумма квадратов. Тогда, так как любое число в факториальном кольце раскладывается на произведение простых, то если эти все простые вида $4k+1$, то и само число раскладывается в сумму квадратов.

20.09.24

Теорема (КТО для $\mathbb{Z}$)**.** *Пусть* $m_1, m_2, ..., m_n \in \mathbb{Z}$ *и* $(m_i, m_j) = (1)$. *Тогда*

$$\mathbb{Z}/_{m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_n \mathbb{Z}} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z}$$

Доказательство ничем не отличается от доказательство самой КТО.

Обозначение. Будем обозначать за A^* множество обратимых элементов кольца A.

Заметим, что

$$(\overline{a_1}, \overline{a_2}, ..., \overline{a_n}) \in (\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z})^* \Leftrightarrow \overline{a_1} \in (\mathbb{Z}/m_1\mathbb{Z})^*, \ldots, \overline{a_n} \in (\mathbb{Z}/m_n\mathbb{Z})^*$$

Поэтому возникает достаточно логичный вопрос. А как узнать количество обратимых элементов у того или иного множества. Для это была придумана функция Эйлера.

Определение 17. *Функция* $\varphi : \mathbb{N} \to \mathbb{N}$, $\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^*\right|$ *называется* ***функцией Эйлера***

Заметим, что по КТО $\varphi(m_1 \cdot m_2 \cdot \ldots \cdot m_n) = \varphi(m_1) \cdot \varphi(m_2) \cdot \ldots \cdot \varphi(m_n)$.
Кроме того данное определение можно дать ещё одним способом, а именно:

- $\varphi(1) = 1$
- $\varphi(n) = \left|\{m \mid 1 \leqslant m \leqslant n-1,\ (m,n) = (1)\}\right|$

Задача. Вычислить значение функции Эйлера в явном виде.

1. $n = p$ – простое. В этом случае $\varphi(n) = \varphi(p) = p - 1$
2. n – составное. Тогда $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s} \Rightarrow \varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot \ldots \cdot \varphi(p_s^{k_s}) =$
   $= p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s} \cdot (1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots(1 - \frac{1}{p_s}) = n \cdot (1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots(1 - \frac{1}{p_s})$

Теорема (Эйлера)**.** *Пусть* $n \in \mathbb{N}, a \in Z, (a,n) = (1)$. *Тогда* $a^{\varphi(n)} - 1 \vdots n$

Доказательство. Рассмотрим $\overline{b_1}, \overline{b_2}, ..., \overline{b_{\varphi(n)}} \in (\mathbb{Z}/n\mathbb{Z})^*$ – попарно различные обратимые элементы. Будем действовать аналогично доказательству того, что $\mathbb{Z}/p\mathbb{Z}$, а именно домножим каждый класс на какой-то обратимый $\overline{a}$. Ровно так же доказывается, что это снова перестановка. Заметим, что

$$\overline{b_1} \cdot \overline{b_2} \cdot \overline{b_3} \cdot \ldots \cdot \overline{b_n} = (\overline{a} \cdot \overline{b_1})(\overline{a} \cdot \overline{b_2})\ldots(\overline{a} \cdot \overline{b_n})$$

А тогда

$$\overline{b_1} \cdot \overline{b_2} \cdot \overline{b_3} \cdot \ldots \cdot \overline{b_n} \cdot (\overline{a}^{\varphi(n)} - 1) = \overline{0} \Rightarrow (\overline{a}^{\varphi(n)} - 1) = \overline{0} \Leftrightarrow (\overline{a}^{\varphi(n)} - 1) \vdots n$$

∎

Следствие (Малая теорема Ферма)**.** *Пусть* p *- простое* $\Rightarrow a \in \mathbb{Z}\ a \not\vdots\, p \Rightarrow (a^{p-1} - 1) \vdots p$

Следствие (Переформулировка малой теоремы Ферма)**.** $\forall a \in Z\ \ a^p - a \vdots p$

Доказательство. 1. $a = 1 \quad 1^p - 1 = 0 \,\vdots\, p$

2. $a \rightsquigarrow a+1: \quad a^p - a \,\vdots\, p \Rightarrow (a+1)^p - (a+1) \,\vdots\, p$
   $(a+1)^p - (a+1) = a^p + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \ldots + C_p^{p-1} a + \cancel{1} - a - \cancel{1}$
   Вспомним, что
   $$C_p^k = \frac{p!}{k!(p-k!)} \,\vdots\, p$$
   Тогда по предположеию индукции они вся большая сумма кратна p.

■

Теорема. *Пусть* $n \geqslant 2, n \in nat$. *Тогда* 1) $\Leftrightarrow$ 2)

- $\exists a, b \in \mathbb{Z},\ n = a^2 + b^2$
- *В разложении на простые множители каждый простой множитель* p *сравним с* $3(\mod 4)$ *стоит в чётной степени.*

Доказательство.

- 1) $\Rightarrow$ 2) : Пусть нет и n - наименьший такой элемент, что $n = a^2 + b^2 = \ldots\ldots\ldots p^{2k+1}\ldots\ldots.$ $p \equiv 3(\mod 1)$
  1. $\overline{b} = \overline{0} \Rightarrow \left(\frac{\overline{a}}{\overline{b}}\right) + \overline{1} = \overline{0} \Rightarrow \left(\frac{\overline{a}}{\overline{b}}\right)^2 = \overline{-1}$
  2. $\overline{b} = \overline{0} \Rightarrow \overline{a} = \overline{0} \Rightarrow a, b \,\vdots\, p \Rightarrow a = pa_1,\ b = pb_1 \Rightarrow p^2 \cdot (a_1^2 + b_1^2) = \ldots\ldots p^{2k+1}\ldots\ldots. \Rightarrow$ $a_1^2 + b_1^2 = \ldots\ldots p^{2k-1}\ldots\ldots.$ – противоречие
- 2) $\Rightarrow$ 1) : Уже было в курсе

■

Теорема Дирихле о простых числах

Теорема. *Пусть* $a \in \mathbb{Z}$ $d \in \mathbb{N}$ $\quad (a, d) = (1) \Rightarrow$ *в последовательности* $a, a + d, a + 2d, \ldots$ *имеется беконечное число простых чисел.*

Данная теорема очевидна для случая, когда $a = 1 = d$, ведь тогда пусть p - наибольшее простое, тогда $p! + 1$ тоже простое.

НОД

Определение 18. *Пусть* A *– область целостности.* $a, b \in A$ $\ d \in A$ *называется НОДом* a *и* b*, если*

- $a \,\vdots\, b \,\&\, b \,\vdots\, d$
- $a \,\vdots\, c \,\&\, b \,\vdots\, c \Rightarrow d \,\vdots\, c$

Понятно, что если $a = b = 0 \Rightarrow d = 0$

Утверждение. *НОД единственный*

Доказательство. Пусть нет, пусть существует два НОДа d и d'

$$\left.\begin{aligned} d \,\vdots\, d' \;\Rightarrow\; d = d' \cdot q \\ d' \,\vdots\, d \;\Rightarrow\; d' = d \cdot v \end{aligned}\right\} \;\Rightarrow\; d = duv \;\Rightarrow\; d(1 - uv) = 0 \;\Rightarrow\; 1 - uv = 0 \;\Rightarrow\; uv = 1 \;\Rightarrow\; d = d'$$

■