

Московский физико-технический институт
Физтех-школа прикладной математики и информатики

ТЕОРИЯ КОЛЕЦ И ПОЛЕЙ
IV СЕМЕСТР

Лектор:

h\nu

Автор: *Киселев Николай*
Репозиторий на Github

весна 2025

Содержание

1 Вступление	2
1.1 Примеры колец	2
1.2 Гауссовые целые числа	2
1.3 Делимость	3
1.4 Как доказывать факториальность колец?	4
2 Евклидовы кольца	5
2.1 Примеры	5
2.2 Алгоритм Евклида	6

1 Вступление

Определение 1.1. K — кольцо, если на нем определены две операции $+$, \cdot и

1. $(K, +)$ — абелева группа
2. Дистрибутивность: $a(b + c) = ab + ac, (b + c)a = ba + ca$

В нашем курсе все кольца будут сразу обладать еще двумя свойствами:

3. Ассоциативность: $(ab)c = a(bc)$
4. Существование единицы: $\exists 1 : 1 \cdot a = a \cdot 1 = as$

Таким образом, под *коммутативное кольцо* мы будем понимать кольцо, удовлетворяющее свойствам 1-4, которое является коммутативным (т.е. $ab = ba$)

1.1 Примеры колец

1. \mathbb{Z}
2. $\mathbb{F}[x_1, \dots, x_n]$
3. $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$
4. \mathbb{F} — поле

Определение 1.2. Пусть K, L — кольца, $K \subset L, u \in L$. Тогда:

$$K[u] = f(u) | f \in K[x] = \text{минимальное подкольцо, содержащее } K \cup \{u\}$$

Попробуем решить Великую Теорему Ферма: $x^n + y^n = z^n$. Заметим, что достаточно доказать ее для случая $n = p, 4$, где p — простое. Пусть ξ_p — примитивный корень p -ой степени из 1 в \mathbb{C} . Тогда:

$$x^p + y^p = (x + y)(x + \xi_p y) \dots ((x + \xi_p^{p-1} y)) = z^p$$

Приходим к тому, что если рассмотреть кольцо $\mathbb{Z}[\xi_p]$ и доказать, что в нем работает ОТА (основная теорема арифметики), то тогда получится как-то получить противоречие, используя единственность разложение. Случай $p = 3$ будет доказан далее.

К сожалению, ОТА есть не во всех $\mathbb{Z}[\xi_p]$, а только для $p < 23$. Для "регулярных" p есть некий аналог ОТА, но, к сожалению, регулярных простых чисел на данный момент около 61% против 39% нерегулярных. В общем, надо придумывать что-то другое.

1.2 Гауссовые целые числа

Пример. $\mathbb{Z}[\xi_4] = \mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$

Пример (Числа Эйзенштейна). $\mathbb{Z}[\xi_3] = \mathbb{Z}[w] = \{a + bw, a, b \in \mathbb{Z}\}$, где w — нетривиальный корень $x^3 - 1$.

1.3 Делимость

Определение 1.3. Пусть K — коммутативное кольцо. Будем говорить, что $a \mid b$ или $b \mid a$, если $\exists c \in K : a = bc$

Замечание. $a \mid a, a \mid b, b \mid c \Rightarrow a \mid c$.

Определение 1.4. $a \in K$ — делитель нуля, если $a \neq 0, \exists b \neq 0 \in K : ab = 0$.

Замечание. в \mathbb{Z}_m для любого составного m есть делители нуля.

Определение 1.5. K — область целостности (целостное кольцо), если K — коммутативное кольцо без делителей нуля.

Далее считаем, что кольца — это области целостности

Утверждение 1.1. Пусть K — область целостности, $c \neq 0$. Тогда $ac = bc \Leftrightarrow a = b$

Утверждение 1.2.

$$ac = bc \Leftrightarrow (a - b)c = 0 \Leftrightarrow a - b = 0 \Leftrightarrow a = b$$

Определение 1.6. Пусть K — область целостности. $K^* = \{a \in K | \exists b \in K : ab = ba = 1\}$.

Замечание. K^* образует группу обратимых по умножению элементов

Таким образом, можно рассмотреть действие группы K^* на множестве K .

Определение 1.7. Орбиты данного действия называются классами ассоциированности. Соответственно, пишем $a \sim b$, если $\exists r \in K^* : a = rb$

Замечание. \sim — отношение эквивалентности, это нам известно из курса теории групп.

Утверждение 1.3. Следующие условия эквивалентны:

1. $a \sim b$
2. $a \mid b, b \mid a$
3. $\{c \in K : c \mid a\} = \{c \in K : c \mid b\}$

Доказательство.

$$1 \Rightarrow 2 \quad a \sim b \Rightarrow a = br \Rightarrow b = ar^{-1} \Rightarrow a \mid b, b \mid a$$

$$2 \Rightarrow 1 \quad a \mid b, b \mid a \Rightarrow a = cb, b = da \Rightarrow a = cda \Rightarrow 1 = cd, \text{ т.е. } c, d \in K^* \Rightarrow a \sim b.$$

$$2 \Leftrightarrow 3 \quad a \mid b \Leftrightarrow \{c \in K : c \mid a\} \subset \{c \in K : c \mid b\}. \quad b \mid a \Leftrightarrow \{c \in K : c \mid a\} \supset \{c \in K : c \mid b\}$$

□

Определение 1.8. Пусть K — область целостности. $x \in K$ называется неразложимым, если $x \notin K^* \cup \{0\}$ и из $x = ab \Rightarrow a \in K^*$ или $b \in K^*$.

Определение 1.9. Область целостности K называется факториальным кольцом, если в нем выполнены два свойства:

1. **Существование:** $\forall a \in K, a \neq 0$ представляется в виде $a = up_1 \dots p_s$, где $u \in K^*$, p_1, \dots, p_s — неразложимые
2. **Единственность:** Пусть $a = up_1 \dots p_s = wq_1 \dots q_l$. Тогда $s = l$ и \exists перенумерация, такая, что $p_i \sim q_i$.

Замечание. Кольца \supset Области целостности \supset Факториальные кольца \supset Поля

Пример (Не факториальное кольцо). $\mathbb{Z}[2i]$ не является факториальным. Действительно:

$$4 = 2 \cdot 2 = 2i \cdot (-2i)$$

Но $2 \not\sim 2i, 2 \not\sim -2i$, т.к. $\mathbb{Z}[2i]^* = \{\pm 1\}$.

1.4 Как доказывать факториальность колец?

Для натуральных чисел мы проверяли условие **Леммы Евклида**: $ab:p \Rightarrow a:p$ или $b:p$. Это приводит нас к следующему определению:

Определение 1.10. $p \in K$ называется простым, если p ненулевой, необратимый и $ab:p \Rightarrow a:p$ или $b:p$

Замечание. Таким образом, простые числа в \mathbb{N} можно обобщить двумя способами: как неразложимые и как простые.

Утверждение 1.4. Простой элемент неразложим.

Доказательство. Пусть p — простой. Пусть $p = ab$. Тогда $ab:p \Rightarrow a:p$ или $b:p$. Б.О.О., $a:p$. Тогда $p:a \Rightarrow b \in K^* \Rightarrow p$ неразложим. \square

Теорема 1.1. Пусть K — область целостности, в которой выполнено свойство 1 факториального кольца (т.е. существует разложение на неразложимые) и любой неразложимый прост. Тогда K — факториальное кольцо

Доказательство. Пусть $x = up_1 \dots p_s$, где $u \in K^*$, p_i — неразложимые. Будем вести индукцию по s (хотим доказать единственность разложения, пусть $x = wq_1 \dots q_l$, $w \in K^*$, q_i — неразложимые):

1. **База:** $s = 0 \Rightarrow l = 0$
2. **Переход:** Т.к. $p_i|wq_1 \dots q_l$, то получаем, что $p_i|w$ или $p_i|q_j$. Первое невозможно, т.к. тогда $p_i \in K^*$, поэтому $up_i = q_j$. Т.к. q_j неразложим, то либо $y \in K^*$, либо $p_i \in K^*$. Второе невозможно, поэтому $y \in K^*$, т.е. $q_j \sim p_i$. Сократим обе части на q_j и применим предположение индукции.

\square

2 Евклидовы кольца

Определение 2.1. Область целостности K называется евклидовым кольцом, если \exists функция (называемая нормой) $N : K \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$, такая, что:

1. $\forall a, b \in K \setminus \{0\} N(ab) \geq N(a)$
2. $\forall a, b \in K \setminus \{0\} \exists q, r : a = bq + r$ и $N(r) < N(b)$ или $r = 0$

2.1 Примеры

1. $\mathbb{Z}, N(a) = |a|$
2. $\mathbb{F}[x], N(f) = \deg f$
3. \mathbb{F} — поле, $N(a) = 0$ или $N(a) = 1$

Для некоторых евклидовых колец верна более сильная формулировка первого свойства:

- 1*. $\forall a, b \in K \setminus \{0\} N(ab) = N(a)N(b)$

Это верно, например, для $\mathbb{Z}[i], \mathbb{Z}[\omega]$.

Утверждение 2.1. $\mathbb{Z}[i]$ — евклидово кольцо с нормой $N(a + bi) = a^2 + b^2$

Геометрическое доказательство. Хотим разделить a остатком на b и получить $a = bq + r$. Тогда $\frac{a}{b} = q + \frac{r}{b}$. Рассмотрим целочисленную решетку на комплексной плоскости, и квадрат, куда попадает число $\frac{a}{b}$. Далее выберем ближайшую вершину к $\frac{a}{b}$ и назовем ее q . Т.к. сторона квадрата равна 1, получаем, что максимальная норма $\frac{r}{b} = \frac{a}{b} - q$ не превосходит $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ (т.к. $1/\sqrt{2}$ — максимальное расстояние от точки до ближайшей вершины внутри квадрата). \square

Алгебраическое доказательство. Хотим разделить a остатком на b и получить $a = bq + r$. Пусть $\alpha + \beta i = \frac{a}{b}$. Рассмотрим $q = [\alpha] + [\beta]i$ (здесь $[x]$ — округление). Тогда $\frac{r}{b} = (\alpha - [\alpha]) + (\beta - [\beta])i$ и $N\left(\frac{r}{b}\right) \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$. \square

Утверждение 2.2. $\mathbb{Z}[w]$ — евклидово кольцо с нормой $N(a + bi) = a^2 + b^2$

Геометрическое доказательство. Аналогично рассматриваем сетку из треугольников. \square

Замечание. Аналогично можно доказать, что $\mathbb{Z}[w], \mathbb{Z}[\sqrt{2}i]$ — евклидовы кольца с нормой $N(a + bi) = a^2 + b^2$, а вот $\mathbb{Z}[\sqrt{3}i]$ уже таковым не будет (минимальное расстояние до вершины больше минимальной стороны прямоугольника).

Лемма 2.1. Пусть K — евклидово кольцо, $a, b \in K \setminus \{0\}$. Тогда $N(ab) = N(a) \Leftrightarrow b \in K^*$.

Доказательство.

\Leftarrow Заметим, что $N(a) = N(abb^{-1}) \geq N(ab) \geq N(a) \Rightarrow N(ab) = N(a)$

\Rightarrow Из евклидости: $a = (ab)q + r$, где $r = 0$ или $N(r) < N(ab) = N(a)$. Тогда $a(1 - bq) = r$. Получаем, что либо $1 - bq = 0 \Rightarrow b \in K^*$, либо $N(a(1 - bq)) = N(r) \geq N(a) > N(r)$, чего быть не может, значит $b \in K^*$

\square

2.2 Алгоритм Евклида

Определение 2.2. Пусть $a, b \in K \setminus \{0\}$. d называется наибольшим общим делителем a, b (или $\text{НОД}(a, b)$), если d — общий делитель с наибольшей нормой.

Определение 2.3. Алгоритм Евклида — следующий процесс. Пусть даны $a, b \in K \setminus \{0\}$. Изначально $r_0 = a, r_1 = b$. На каждом шаге мы делим r_{i-1} на r_i с остатком и получаем r_{i+1} . Тогда, при $i \geq 1 : N(r_i) > N(r_{i+1})$. Повторяем операцию, пока r_{i+1} не станет равно 0.

Замечание. $\text{НОД}(r_{i-1}, r_i) = \text{НОД}(r_i, r_{i+1})$

Доказательство. Следует из разложения $r_{i-1} = qr_i + r_{i+1}$ □

Лемма 2.2. Пусть $a, b \in K \setminus \{0\}$, $d = \text{НОД}(a, b)$. Тогда $\exists x, y \in K : ax + by = d$

Доказательство. Заметим, что на каждом шаге алгоритма Евклида, каждый r_i является линейной комбинацией a, b (нетрудно доказать по индукции). Но тогда возьмем предпоследнее r_i в алгоритме Евклида (последний равен 0). Он и будет НОДом. □

Теорема 2.1. Любое евклидово кольцо факториально.

Доказательство. 1. **Существование разложения.** Пусть x — элемент с наименьшей нормой, для которого не существует разложения. Если $x = ab \Leftrightarrow a \in K^*$ или $b \in K^* \Rightarrow x$ — неразложим. Но тогда его разложение $x = x$. Если существует разложение, где $a \notin K^*, b \notin K^*$, то $N(ab) > N(a), N(b)$ (иначе б.о.о $N(ab) = N(a)$ и тогда $b \in K^*$). Но тогда a, b разложимы и $a = up_1 \dots p_s, b = wq_1 \dots q_l$ и $x = (uw)p_1 \dots p_sq_1 \dots q_l$.

2. **Единственность разложения.** Докажем, что любой неразложимый элемент является простым. Пусть p неразложим и $ab:p$. Рассмотрим $\text{НОД}(a, p) = \begin{cases} 1 & p \Rightarrow a:p \\ \dots & \end{cases}$. Для случая $\text{НОД}(a, p) = 1$ имеем: $ax + py = 1$. Тогда: $\underbrace{ab}_{\vdots p} x + pby = b$, левая часть делится на p , поэтому правая — тоже. □

Утверждение 2.3. Первое условие Евклидова кольца не существенно.

Доказательство. Пусть $N : K \setminus \{0\}$ — функция, которая удовлетворяет свойству 2: $\forall a, b \exists q, r : a = bq + r$ причем $r = 0$ или $N(r) < N(b)$. Рассмотрим функцию $\tilde{N}(a) = \min_{c \in K \setminus \{0\}} N(ac)$. Докажем, что это норма на K . Докажем два свойства нормы:

1. $\tilde{N}(ab) = N(abx)$ для некоторого x , получаем, что $\tilde{N}(ab) = N(a(bx)) \geq \min_{c \in K \setminus \{0\}} N(ac)$.
2. Пусть даны $a, b \in K \setminus \{0\}$. При этом, $\tilde{N}(b) = N(bc)$ для некоторого c . Разделим a на bc в норме N : $a = (bc)q + r$. Тогда $a = b(cq) + r$ и $\tilde{N}(r) \leq N(r) < N(bc) = N(b)$ или $r = 0$, что и требовалось.

□