

Теория чисел (теория)

Владимир Латыпов
donrumata03@gmail.com

Vladimir Latypov
donrumata03@gmail.com

Содержание

| | |
|-----------------------------|---|
| 1 Базовые определения | 3 |
| 2 Идеалы | 4 |
| 3 Евклидовы кольца | 6 |

1 Базовые определения

Some red text

<https://1>

Определение 1.1 (*definition 1: группа*) $\langle G, \star \rangle$ — группа, если

1. $\forall a, b, c \in G \quad a \star (b \star c) = (a \star b) \star c$ (ассоциативность)
2. $\exists e \in G \quad \forall x \in G \quad x \star e = e \star x = x$ (существование нейтрального элемента)
3. $\forall x \exists y \quad x \star y = y \star x = e$ (существование обратного элемента)

аксиома 1 даёт *полугруппу*, при добавлении аксиомы 4 — получается *абелева группа*

Пример 1.2

- S_n — группа, но не абелева

Определение 1.3 (*definition 3: кольцо*)

1. $\langle R, + \rangle$ — абелева группа
2. $\langle R \setminus \{0\}, \cdot \rangle$ — полугруппа
3. $a \cdot (b + c) = a \cdot b + a \cdot c = (b + c) \cdot a$ (дистрибутивность умножения относительно сложения)

Замечание 1.4 Будем работать с коммутативными кольцами (умножение коммутативно), преимущественно — с областями целостности

Пример 1.5

- \mathbb{Z} — кольцо
- $R[x]$ — кольцо многочленов над R от переменной x .

Определение 1.6 (*definition 6: Гомоморфизм колец*) $f : R_1 \rightarrow R_2$

1. $f(x + y) = f(x) + f(y)$ («дистрибутивность» относительно сложения)
2. $f(ab) = f(a)f(b)$ («дистрибутивность» относительно умножения)
3. $f(1_{R_1}) = 1_{R_2}$ (сохранение единицы)

Пример 1.7 (*example 7: Независимость третьей аксиомы*)

$$f : \begin{pmatrix} R \rightarrow R \times R \\ r \mapsto (r, 0) \end{pmatrix}$$

— 1, 2 выполнены, но не 3

Определение 1.8 (*definition 8: поле*)

- Коммутативное кольцо с единицей
 - $\forall x \neq 0 \exists y \quad x \cdot y = y \cdot x = e$ (существование обратного элемента по умножению)
- (пишут $y = x^{-1}$)

Замечание 1.9 То есть ещё и $R \setminus \{0\}$ — абелева группа.

Пример 1.10

- \mathbb{R}
- \mathbb{C}
- \mathbb{F}_2

Определение 1.11 (*definition 11: область целостности*)

1. $1 \neq 0$
 2. $\forall a, b \in R \quad ab = 0 \Rightarrow a = 0 \vee b = 0$ (отсутствие делителей нуля)
 - 2'. $\forall a \neq 0 \quad ab = ac \Rightarrow b = c$ (можно сокращать на всё, кроме нуля)
- (2 и 2' эквивалентны)

Пример 1.12 \mathbb{Z} , любое поле (действительно, сократим через деление на обратный)

2 Идеалы

Определение 2.13 (*definition 13: идеал*) $I \trianglelefteq R$

- $\forall a, b \in I \quad a - b \in I$ (замкнутость относительно разности)
- $\forall r \in R, a \in I \quad r \cdot a \in I$ (замкнутость относительно умножения на элемент кольца)

Замечание 2.14

- У любого кольца есть идеалы $0, R$.
- R — поле \Rightarrow есть только эти идеалы

Замечание 2.15 Идеалы в кольцах и нормальные подгруппы обозначают «меньше или равно с треугольничком»: \trianglelefteq , остальные подструктуры — обычно просто \leq

Определение 2.16 (*definition 16: Операции над идеалами*)

- Сложение
- Пересечение

— определяются поэлементно

- Умножение: натягиваем на произведение множеств по Минковскому

Определение 2.17 Идеал, порождённый подмножеством $S \subset R$:

$$(S) = \bigcap_{S \subset I \trianglelefteq R} I$$

Он же —

$$\left\{ \sum r_i s_i \mid r_i \in R, s_i \in S \right\}$$

Замечание 2.18

$$(a_1, \dots, a_n) = \left\{ \sum_{i=1}^n r_i a_i \mid r_i \in R \right\}$$

(линейная комбинация)

$$(a) = aR = Ra = \{ra \mid r \in R\}$$

Определение 2.19 Идеалы, которые можно породить одним элементом — *главные*.

Определение 2.20 (*definition 20: PID/ОГИ*) Когда все идеалы — главные.

Определение 2.21 (*definition 21: Факторкольцо по идеалу*) Введём отношение эквивалентности $a \sim b \in I$ и факторизуем по нему. Получим R/I — кольцо с элементами $x + I, \quad x \in R$.

Замечание 2.22 Понятие идеала пошло из обобщения концепции делимости, «идеальные делители». Простой идеал — обобщение простого числа.

Определение 2.23 (*definition 23: Простой идеал*) $p \trianglelefteq R$ — простой $\stackrel{\text{def}}{\iff} ab \in p \Rightarrow a \in p \vee b \in p$.

Эквивалентно: $ab \equiv_p 0 \Rightarrow a \equiv_p 0 \vee b \equiv_p 0$

Определение 2.24 (*definition 24: Нётерово кольцо*) Конечно порождённое кольцо

Теорема 2.25 (*theorem 25: Эквивалентные определения нётеровости*)

1. Все идеалы конечно порождены
2. Вложенная расширяющаяся последовательность идеалов стабилизируется
3. У множества идеалов существует максимальный по включению (но не обязательно — наибольший)

Доказательство

(1) \rightarrow (2): Пусть $I = \bigcup I_k = (a_1, \dots, a_n)$. Каждое a_i лежит в каком-то I_{k_i} . Тогда стабилизация происходит уже при $I_{\max\{k_i\}}$.

(2) \rightarrow (3): Итеративно будем выбирать идеал, содержащий предыдущий, пока таковой имеется.

- Если кончились, мы нашли максимальный
- Если нет, построили последовательность вложенных идеалов. Так как она стабилизируется, стабильное значение — наш ответ.

(3) \rightarrow (1): $I = \max\{J \mid J \subset I, J \text{ — конечно порождён}\}$. □

Теорема 2.26 (*theorem 26: Гильберта о нётеровости кольца многочленов над нётеровым кольцом*) Пусть для $I \subseteq R[x]$ $a(i) = \{r \in R \mid rx^i + * \cdot x^{<i-1} \in I\}$, то есть коэффициенты при x^i , когда это старшая степень.

Тогда $a(1) \subset a(2) \subset \dots$ — вложенная цепочка идеалов $\subseteq R$. Пусть стабилизируется на $a(k)$.

! TODO !

3 Евклидовы кольца

Определение 3.27 (*definition 27: Евклидово кольцо*) $d : R \setminus \{0\} \rightarrow \mathbb{N}_0$, тч

1. $d(ab) \geq d(a)$
2. $\forall a, b, b \neq 0 \exists q, r : a = bq + r, r = 0 \vee d(r) < d(b)$

Пример 3.28 $\mathbb{Z}, F[x]$

Теорема 3.29 Евклидово \rightarrow ОГИ

Доказательство Находим a — минимальный по d , если нашёлся не кратный, делим с остатком на a , получаем меньший, противоречие □

Определение 3.30 (definition 30: Факториальное кольцо (UFD — Unique factorization domain))
Область целостности

- Существует разложение на неприводимые множители
- Единственно с точностью до R^* : если $x = u \cdot a_1 \cdot \dots \cdot a_n = u \cdot b_1 \cdot \dots \cdot b_m \Rightarrow m = n \wedge a_i = b_{\sigma_i} \cdot w_i, w_i \in R^*$

Определение 3.31 (definition 31: Неприводимый элемент)
 $a \neq 0, a \notin R^* \quad a = bc \Rightarrow b \in R^* \vee c \in R^*$

! TODO !
use property not remark

Замечание 3.32 Неприводимость сохраняется при домножении на обратимые ($r \in R^*$)

Определение 3.33 (definition 33: Простой элемент) $a \mid bc \Rightarrow a \mid b \vee a \mid c (\Leftrightarrow aR$ — простой идеал)

Теорема 3.34 Простой \Rightarrow неприводимый

Доказательство

! TODO !

□

Теорема 3.35 В факториальном кольце: Неприводимый \Rightarrow простой

Доказательство

! TODO !

□

Следствие 3.36 В факториальном кольце простые идеалы высоты 1 (то есть $0 \leq q \leq p \Rightarrow q = 0 \vee q = p$) являются главными

Доказательство Элемент идеала раскладывается на множители, а по простоте какой-то $- \in p$, тогда $0 \leq \underbrace{(a_i)}_{\text{прост.}} \leq p \rightarrow (a_i) = p$

□

! TODO !

Помечать разделение не лекции красивыми заголовками (как ornament header в latex)

Теорема 3.37 Евклидово \Rightarrow ОГИ \Rightarrow Факториальное

! TODO !

Перейти на lemmify

Доказательство (proof 38: Евклидово \rightarrow ОГИ) ...

□

Определение 3.38 R^* — мультипликативная группа кольца (все, для которых есть обратный, с умножением)

Доказательство (proof 39: ОГИ \rightarrow факториальное) Схема: следует из двух свойств, докажем оба для ОГИ.

Лемма 3.39 В ОГИ: неприводимый \rightarrow простой

Обобщение ОТА на произвольную ОГА с целых чисел.

Переформулируем: ...

Пусть есть такие элементы, возьмём цепочку максимальной длины, последний — приводим, представим как необратимые, тогда они сами представляются как ..., тогда и он тоже.

! TODO !

□

Определение 3.40 нснм — начиная с некоторого места

Замечание 3.41 Нётеровость: не можем бесконечно делить, так как при переходе к множителям идеалы расширяются, но в какой-то момент стабилизируются.

Теорема 3.42 R факториально $\Rightarrow R[x]$ — тоже

Пример 3.43 F — поле.

$f \in F[x]$ — неприводим.

$\frac{F[x]}{(f)}$ — область целостности, но докажем, что поле.

- $\bar{g} \mid \deg g < \deg f$
- $(f, g) = 1$, то есть $1 = fp_1 + gp_2, \bar{1} = \bar{f}\bar{p}_1 + \bar{g}\bar{p}_2$

$$\dim_F K = \deg f$$

Можем построить все конечные поля.

$$\mathbb{F}_{p[x]} \ni f, \deg f = m$$

$$\mathbb{F}_{p^m}[x] \ll \mathbb{F}_{p^m} \frac{p^m}{(f)}$$

Теорема 3.44 Над конечным полем существуют неприводимые многочлены любой степени

Пример 3.45 $\mathbb{F}_2 \frac{[x]}{(x^2+x+1)}$

Таблица сложения:

| | 0 | 1 | α | β |
|---|---|---|----------|---------|
| 0 | 0 | 1 | 3 | 4 |

Теорема 3.46 Группа простого порядка — циклическая

Тестовое изменение

sdzf

asdf