Теория чисел (теория)

Владимир Латыпов

donrumata03@gmail.com

Vladimir Latypov

donrumata03@gmail.com

Содержание

1 Базовые определения

Определение 1.1 (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:

- S_n — группа, но не абелева

Определение 1.2 (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: Будем работать с коммутативными кольцами (умножение коммутативно), преимущественно — с областями целостности

Пример:

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

Определение 1.3 (Гомофморфизм колец): $f : R_1 \to R_2$

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

Пример (Независимость третей аксиомы):

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

— 1, 2 выполнены, но не 3

Определение 1.4 (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: То есть ещё и $R \setminus \{0\}$ — абелева группа.

Пример:
- $\mathbb{R}$
- $\mathbb{C}$
- $\mathbb{F}_2$

Определение 1.5 (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: $\mathbb{Z}$, любое поле (действительно, сократим через деление на обратный)

2 Идеалы

Определение 2.1 (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:

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

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

Определение 2.2 (Операции над идеалами):
- Сложение
- Пересечение

— определяются поэлементно

- Умножение: натягиваем на произведение множество по Минковскому

Определение 2.3: 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:

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

(линейная комбинация)

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

Определение 2.4: Идеалы, которые можно породить одним элементом — *главные*.

Определение 2.5 (PID/ОГИ): Когда все идеалы — главные.

Определение 2.6 (Факторкольцо по идеалу): Введём отношение эквивалентности $a - b \in I$ и факторизуем по нему. Получим R/I — кольцо с элементами $x + I, \quad x \in R$.

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

Определение 2.7 (Простой идеал): $p \trianglelefteq R$ — простой $\overset{\text{def}}{\iff} ab \in p \Rightarrow a \in p \vee b \in p$.

Эквивалентно: $ab \underset{p}{\equiv} 0 \Rightarrow a \underset{p}{\equiv} 0 \vee b \underset{p}{\equiv} 0$

Определение 2.8 (нётерово кольцо): …

Теорема 1 (Гаусса о нётеровости кольца многочленов над Гауссовым полем): …

3 Евклидовы кольца

Определение 3.1 (Евклидово кольцо): $d : R \setminus \{0\} \to \mathbb{N}_0$, 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: $\mathbb{Z}, F[x]$

Теорема 1: Евклидово $\longrightarrow$ ОГИ

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

Определение 3.2 (Факториальное кольцо (UFD — Unique factorization domain)): Область целостности

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

Определение 3.3 (Неприводимый элемент): $a \neq 0, a \notin R^* \quad a = bc \Rightarrow b \in R^* \vee c \in R^*$

Свойство 3.3.1: Неприводимость сохраняется при домножении на обратимые ($r \in R^*$)

Определение 3.4 (Простой элемент): $a \mid bc \Rightarrow a \mid b \vee a \mid c$ ($\Leftrightarrow aR$ — простой идеал)

Теорема 2: Простой $\Rightarrow$ неприводимый

Доказательство:

! TODO !

$\square$

Теорема 3: В факториальном кольце: Неприводимый $\Rightarrow$ простой

Доказательство:

! TODO !

$\square$

Следствие 3.1: 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 $0 \leq \underbrace{(a_i)}_{\text{прост.}} \leq p \longrightarrow (a_i) = p$ $\square$

! TODO !

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

Теорема 4: Евклидово $\Rightarrow$ ОГИ $\Rightarrow$ Факториальное

! TODO !

Перейти на lemmify

Доказательство (Евклидово $\longrightarrow$ ОГИ): ... $\square$

Определение 3.5: R^* — мультипликативная группа кольца (все, для которых есть обратный, с умножением)

Доказательство (ОГИ $\longrightarrow$ факториальное): Схема: следует из двух свойств, докажем оба для ОГИ.

Лемма 3.5: В ОГИ: неприводимый $\longrightarrow$ 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 !

$\square$

Определение 3.6: нснм — начиная с некоторого места

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

Теорема 6: R факториально $\Rightarrow R[x]$ — тоже

Пример: F — поле.

$f \in F[x]$ — неприводим.

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

. $\overline{g} \quad \deg g < \deg f$

- $(f, g) = 1$, то есть $1 = fp_1 + gp_2$, $\overline{1} = \overline{f}\overline{p_1} + \overline{gp_2}$

  $\dim_F K = \deg f$

Можем построить все конечные поля.

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

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

Над конечным полем существуют неприводимые многочлены любой степени.

...