Теория чисел (теория)

Владимир Латыпов
donrumata03@gmail.com

Vladimir Latypov
donrumata03@gmail.com

Содержание

1 Базовые определения

Some red text

https://1

Definition 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*

Example 1.2

- S_n — группа, но не абелева

Definition 1.3 *(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)

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

Example 1.5

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

Definition 1.6 *(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)

Example 1.7 *(Независимость третей аксиомы)*

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

— 1, 2 выполнены, но не 3

Definition 1.8 *(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 $y = x^{-1}$)

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

Example 1.10

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

Definition 1.11 *(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)

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

2 Идеалы

Definition 2.13 *(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)

Remark 2.14

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

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

Definition 2.16 *(Операции над идеалами)*

- Сложение
- Пересечение

— определяются поэлементно

- Умножение: натягиваем на произведение множеств по Минковскому

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

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

Он же —

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

Remark 2.18

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

(линейная комбинация)

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

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

Definition 2.20 *(PID/ОГИ)* Когда все идеалы — главные.

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

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

Definition 2.23 *(Простой идеал)* $p \trianglelefteq R$ — простой $\overset{\text{def}}{\Longleftrightarrow} ab \in p \Rightarrow a \in p \lor b \in p$.

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

Definition 2.24 *(Нётерово кольцо)* Конечно порождённое кольцо

Theorem 2.25 *(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*)

Proof

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

$(2) \to (3)$: Итеративно будем выбирать идеал, содержащий предыдцщий, пока таковой имеется.

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

$(3) \to (1)$: $I = \max\{J \mid J \subset I, J - \text{конечно порождён}\}$. $\square$

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

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

! TODO !

3 Евклидовы кольца

Definition 3.27 *(Евклидово кольцо)* $\quad d : R \setminus \{0\} \to \mathbb{N}_0$, тч

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

Example 3.28 $\mathbb{Z}, F[x]$

Theorem 3.29 Евклидово $\longrightarrow$ ОГИ

Proof Находим a — минимальный по d, если нашёлся не кратный, делим с остатком на a, получаем меньший, противоречие $\square$

Definition 3.30 *(Факториальное кольцо (UFD — Unique factorization domain))* Область целостности

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

Definition 3.31 *(Неприводимый элемент)* $\quad a \neq 0, a \notin R^* \quad a = bc \Rightarrow b \in R^* \lor c \in R^*$

! TODO !
use propertym not remark

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

Definition 3.33 *(Простой элемент)* $a \mid bc \Rightarrow a \mid b \vee a \mid c$ ($\Leftrightarrow aR$ — простой идеал)

Theorem 3.34 Простой $\Rightarrow$ неприводимый

Proof

! TODO !

$\square$

Theorem 3.35 В факториальном кольце: Неприводимый $\Rightarrow$ простой

Proof

! TODO !

$\square$

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

Proof 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)

Theorem 3.37 Евклидово $\Rightarrow$ ОГИ $\Rightarrow$ Факториальное

! TODO !

Перейти на lemmify

Proof *(Евклидово $\longrightarrow$ ОГИ)* ... $\square$

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

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

Lemma 3.39 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 !

$\square$

Definition 3.40 нснм — начиная с некоторого места

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

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

Example 3.43 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 $1 = fp_1 + gp_2$, $\overline{1} = \overline{fp_1} + \overline{gp_2}$

$\dim_F K = \deg f$

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.