Теория чисел (теория)

Владимир Латыпов
donrumata03@gmail.com

Vladimir Latypov
donrumata03@gmail.com

Содержание

1 Базовые определения

Определение 1.1 (группа): ...

Определение 1.2 (кольцо): ...

Замечание: Будем работать с коммутативными кольцами, преимущественно — с областями целостности

Пример (многочлены):

Определение 1.3 (поле): ...

Определение 1.4 (область целостности): ...

2 Идеалы

Определение 2.1 (идеал): ...

Замечание: Пошло из обобщения понятия делимости, «идеальные делители».

Простой идеал — обобщение простого числа.

Определение 2.2 (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 2.3 (факторкольцо по идеалу): ...

Определение 2.4 (ОГИ): ...

Определение 2.5 (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 !

□

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

Доказательство:

! TODO !

□

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 $0 \leq \underbrace{(a_i)}_{\text{прост.}} \leq p \longrightarrow (a_i) = p$ □

! 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): ... □

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.