Теория чисел (теория)

Владимир Латыпов
donrumata03@gmail.com

Vladimir Latypov
donrumata03@gmail.com

Содержание

1 Базовые определения

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: 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 1.7 *(example 7: Независимость третей аксиомы)*

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

— 1, 2 выполнены, но не 3

Определение 1.8 *(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. $\forall a, b \in R \quad ab = 0 \Rightarrow a = 0 \lor b = 0$ (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

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

(линейная комбинация)

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

Определение 2.19 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 $a - b \in I$ 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 $\overset{\text{def}}{\iff}$ $ab \in p \Rightarrow a \in p \lor b \in p$.

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

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

$(1) \to (2)$: 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 предыдщций, пока такой имеется.
- Если кончились, мы нашли максимальный
- Если нет, построили последовательность вложенных идеалов. Так как она стабилизирутеся, стабильное значение — наш ответ.

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

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

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

! TODO !

3 Евклидовы кольца

Определение 3.27 *(definition 27: 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 3.28 $\mathbb{Z}, F[x]$

Теорема 3.29 Евклидово $\longrightarrow$ 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 $x = u \cdot a_1 \cdot \ldots \cdot a_n = u \cdot b_1 \cdot \ldots \cdot b_m \Rightarrow m = n \wedge a_i = b_{\sigma_i} \cdot w_i, w_i \in R^*$

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

Свойство 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 !

$\square$

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

Доказательство

! TODO !

$\square$

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

! TODO !

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

Теорема 3.37 Евклидово $\Rightarrow$ ОГИ $\Rightarrow$ Факториальное

Доказательство *(proof 38: Евклидово $\to$ ОГИ)* ... □

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

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

Лемма 3.39 В ОГИ: неприводимый $\to$ 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.

- $\overline{g}\quad \deg g < \deg f$
- $(f, g) = 1$, 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.

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

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

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

3.1 sdafasf

3.1.1 dasasd

3.1.1.1 asdf

4 vdsf

4.1 231

Теорема 4.1.47 sdfs

! TODO !

Why isn't the theorem counter reset?

OMG, I'm lecture 1

Ahh, im lecture-2!

Could not find `theory/lecture-3.typ`

Could not find `theory/lecture-4.typ`

Could not find `theory/lecture-5.typ`

Could not find `theory/lecture-6.typ`

Could not find `theory/lecture-7.typ`

Could not find `theory/lecture-8.typ`

Could not find `theory/lecture-9.typ`

Could not find `theory/lecture-10.typ`

Could not find `theory/lecture-11.typ`

Could not find `theory/lecture-12.typ`

Could not find `theory/lecture-13.typ`

Could not find `theory/lecture-14.typ`

Лекция 3

5 Поля

Определение 5.48 *(definition 48: Подполе)*

Свойство 5.49 R— поле $\Leftrightarrow$ вR ровно 2 идеала

Свойство 5.50 Гомоморфизмы полей инъективны, так как ядро — идеал

Определение 5.51 *(definition 51: F-аглебра (алгебра над F))* кольцо R, тч $F \leq R$

Замечание 5.52 Тогда это заодно и векторное пространство

Определение 5.53 *(definition 53: Гомофморфизм F-алгебр)*
- $f : R \to R'$ — гомоморфизм колец
- $f(\alpha) = \alpha \forall \alpha \in F$ (сохраняет элементы поля)

Замечание 5.54 Получается, это автоматически гомоморфизм векторных пространств

Определение 5.55 *(definition 55: Характеристика)*

$$\begin{aligned} &\mathbb{Z} \xrightarrow{f} F \\ &n \mapsto \underbrace{1_F + 1_F + ...1_F}_{n \text{ раз}} \end{aligned}.$$

1. $\ker f = 0$

$$\begin{tikzcd} \mathbb{Z} \arrow[rr, "f"] \arrow[dr] & & F \\ & \mathbb{Q} \arrow[ur, dashed] & \end{tikzcd}$$

1. $\ker f = (p)$

Итого: минимальное количество раз, которое нужно сложить единицу с собой, чтобы стала нулём.

Определение 5.56 *(definition 56: Простые поля)* Не содержат подполя

Замечание 5.57 *(remark 57: Бином Ньютона)* В полях характеристики p/в $\mathbb{F}_p$ алгебрах $p \cdot (a = 0) \Rightarrow \quad (a+b)^p = a^p + b^p$.

Определение 5.58 *(definition 58: эндоморфизм Фробениуса)* $f : \begin{pmatrix} R \to R \\ a \mapsto a^p \end{pmatrix}$.

- Если поле, то инъективен ($\ker f = 0$) и $\operatorname{Im} f$ — подполе
- $R = \mathbb{F}_p$ — конечное поле $\Rightarrow$ назвают «автоморфизм Фробениуса»

$$\mathbb{F}_{p(x)} \xrightarrow{f} \mathbb{F}_{p(x)} \quad \mathfrak{I} f = \mathbb{F}_{p(X^p)} = \left\{ \frac{g(x^p)}{h(x^p)} \mid g, h \in \mathbb{F}_{p[x]}, h \neq 0 \right\}$$

.

Определение 5.59 *(definition 59: Унитарный многочлен)* Старший коэфициент = 1

Теорема 5.60 *(theorem 60: Лемма Гаусса)*

Теорема 5.61 *(theorem 61: Критерий Эйзенштейна)*

$$h = a_n x^n + \ldots + a_1 x + a_0, \quad a_i \in \mathbb{Z}, \quad p \text{ — простой}$$

1. $p \nmid a_n$
2. $p \mid a_{n-1}, \ldots a_0$
3. $p^2 \nmid a_0$

Тогда h — неприводим

Доказательство

□

Определение 5.62 *(definition 62: Расширение поля)* E — расширение F, если $F \leq E$. «E/F» — E расширяет F.

E/F называется конечным, если $\infty > \dim_F E := [E :: F]$ — степень E над F.

$E \xrightarrow{f} E'$

Пример 5.63

- $\mathbb{C}/\mathbb{R}$
- $\mathbb{R}/\mathbb{Q}$
- $\mathbb{Q}[i]/\mathbb{Q}$
- $F(x)/F$

Теорема 5.64 $\rceil F \leq E \leq L \quad L/F < \infty \Longleftrightarrow E/F < \infty$, при этом

$$[L : F] = [L : E] \cdot [E : F]$$

Доказательство

$\Rightarrow$

- E — подпространство $F \Rightarrow \dim_F E < \infty$
- $\{e\}_1^n$ — базис L над $F \Rightarrow \{e\}_1^n$ порождает L над E

$\Leftarrow$ …

□

Определение 5.65 *(definition 65: Подалгебра, порождённая ?)*

$$E/F \quad S \leq E \quad F[S] = \left\{\sum a_I \alpha^I \mid a_I \in F, \alpha_I \in S\right\}$$

Лемма 5.66 R — конечная F-алг. $\quad R$ — область целостности $\Rightarrow R$ — поле

Доказательство $\quad a \neq 0 \quad f : R \to R \quad f(r) = ar$

- $f \in$ F-Lin
- $f \in \mathrm{Inj}$

$\Rightarrow f \in \mathrm{Surj}$, а тогда $\exists b$, тч $ab = 1$, значит любой $a \neq 0$ обратим, значит, это поле. □

Следствие 5.67 E/F — конечное R — подалгебра $E \Rightarrow R$ — поле

Определение 5.68 *(definition 68: Простое расширение)*
E/F — простое $\quad E = F(\alpha), \alpha \in E$

Определение 5.69 *(definition 69: Композит двух полей)*
$F, F' \leq E \quad F(F') = F \cdot F' = F'(F)$

Замечание 5.70 Поля разных характеристик не могут содержаться в одном поле, так как единица должна лежать и там, и там

$F[x] \ni f$ — непрерывны, унитарны.

5.1 Построение циркулем и линейкой

Удалить