Теория чисел (теория)

Владимир Латыпов
donrumata03@gmail.com

Vladimir Latypov
donrumata03@gmail.com

Содержание

1 Базовые определения

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 **2.1** *(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)

Remark **2.2**
- У любого кольца есть идеалы $0, R$.
- R — поле $\Rightarrow$ есть только эти идеалы

Remark **2.3** Идеалы в кольцах и нормальные подгруппы обозначают «меньше или равно с треугольничком»: $\trianglelefteq$, остальные подструктуры — обычно просто $\leq$

Definition 2.4 *(Операции над идеалами)*
- Сложение
- Пересечение

— определяются поэлементно

- Умножение: натягиваем на произведение множеств по Минковскому

Definition 2.5 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 2.6

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

(линейная комбинация)

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

Definition 2.7 Идеалы, которые можно породить одним элементом — *главные*.

Definition 2.8 *(PID/ОГИ)* Когда все идеалы — главные.

Definition 2.9 *(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 2.10 Понятие идеала пошло из обобщения концепции делимости, «идеальные делители». Простой идеал — обобщение простого числа.

Definition 2.11 *(Простой идеал)* $p \trianglelefteq R$ — простой $\overset{\text{def}}{\iff} ab \in p \Rightarrow a \in p \lor b \in p$.

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

Definition **2.12** *(Нётерово кольцо)* Конечно порождённое кольцо

Theorem **2.13** *(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 стабилизция происходит уже при $I_{\max\{k_i\}}$.

$(2) \to (3)$: Итеративно будем выбирать идеал, содержащий предыдщций, пока таковой имеется.
- Если кончились, мы нашли максимальный
- Если нет, построили последовательность вложенных идеалов. Так как она стабилизирутеся, стабильное значение — наш ответ.

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

Theorem **2.14** *(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 $a(1) \subset a(2) \subset ...$ — вложенная цепочка идеалов $\trianglelefteq R$. Пусть стабилизируется на $a(k)$.

! TODO !

3 Евклидовы кольца

Definition **3.1** *(Евклидово кольцо)* $d : R \setminus \{0\} \to \mathbb{N}_0$, тч

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

Example **3.2** $\mathbb{Z}, F[x]$

Theorem **3.3** Евклидово $\longrightarrow$ ОГИ

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

Definition **3.4** *(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 **3.5** *(Неприводимый элемент)* $a \neq 0, a \notin R^* \quad a = bc \Rightarrow b \in R^* \lor c \in R^*$

Property **3.6** Неприводимость сохраняется при домножении на обратимые ($r \in R^*$)

Definition **3.7** *(Простой элемент)* $a \mid bc \Rightarrow a \mid b \lor a \mid c$ ($\Leftrightarrow aR$ — простой идеал)

Theorem **3.8** Простой $\Rightarrow$ неприводимый

Proof

! TODO !

$\square$

Theorem **3.9** В факториальном кольце: Неприводимый $\Rightarrow$ простой

Proof

! TODO !

$\square$

Corollary **3.10** В факториальном кольце простые идеалы высоты 1 (то есть $0 \leq q \leq p \Rightarrow q = 0 \lor q = p$) являются главными

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

! TODO !

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

Theorem **3.11** Евклидово $\Rightarrow$ ОГИ $\Rightarrow$ Факториальное

Proof *(Евклидово → ОГИ)* ... □

Definition **3.12** R^* — мультипликативная группа кольца (все, для которых есть обратный, с умножением)

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

Lemma **3.13** В ОГИ: неприводимый → 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 !

□

Definition **3.14** нснм — начиная с некоторого места

Remark **3.15** Нётеровость: не можем бесконечно делить, так как при переходе к множителям идеалы расширяются, но в какой-то момент стабилизируются.

Theorem **3.16** R факториально $\Rightarrow R[x]$ — тоже

Example **3.17** 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.

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

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

Theorem **3.18** Над конечным полем существуют неприводимые многочлены любой степени

Example **3.19** $\mathbb{F}_2 \frac{[x]}{(x^2+x+1)}$

Таблица сложения:

	0	1	α	β
0	0	1	3	4

Theorem **3.20** Группа простого порядка — циклическая

3.1 sdafasf

3.1.1 dasasd

3.1.1.1 asdf

4 vdsf

4.1 231

Theorem **4.1** 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

Definition **5.1** *(Подполе)*

Property **5.2** R— поле $\Leftrightarrow$ вR ровно 2 идеала

Property **5.3** Гомоморфизмы полей инъективны, так как ядро — идеал

Definition **5.4** *(F-аглебра (алгебра над F))* кольцо R, тч $F \leq R$

Remark **5.5** Тогда это заодно и векторное пространство

Definition **5.6** *(Гомофморфизм F-алгебр)*
- $f : R \to R'$ — гомоморфизм колец
- $f(\alpha) = \alpha \forall \alpha \in F$ (сохраняет элементы поля)

Remark **5.7** Получается, это автоматически гомоморфизм векторных пространств

Definition **5.8** *(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.

Theorem **5.9** *(Количество элементов конечного поля)* $|F| = \text{char } F^n = p^n, p$ — prime

Theorem **5.10** *(Единственность конечного поля)* Конечные поля равного размера изоморфны.

Definition **5.11** *(Простые поля)* Не содержат подполя

Remark **5.12** *(Бином Ньютона)* В полях характеристики p/в $\mathbb{F}_p$ алгебрах $p \cdot (a = 0) \Rightarrow \quad (a + b)^p = a^p + b^p$.

Definition **5.13** *(эндоморфизм Фробениуса)* $f : \binom{R \to R}{a \mapsto a^p}$.

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

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

.

Definition **5.14** *(Унитарный многочлен)* Старший коэфициент = 1

Theorem **5.15** *(Лемма Гаусса)*

Theorem **5.16** *(Критерий Эйзенштейна)*

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

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

Тогда h — неприводим

Proof

□

Definition **5.17** *(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.

$E \xrightarrow{f} E'$

Example **5.18**

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

Theorem **5.19** $\quad] \ F \leq E \leq L \quad L/F < \infty \Longleftrightarrow E/F < \infty$, при этом

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

Proof

$\Rightarrow$

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

$\Leftarrow$ ...

□

Definition **5.20** *(Подалгебра, порождённая ?)*

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

Lemma **5.21** $\ R$ — конечная F-алг. $\quad R$ — область целостности $\Rightarrow R$ — поле

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

- $f \in$ F-Lin
- $f \in$ Inj

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

Corollary **5.22** $\quad E/F$ — конечное R — подалгебра $E \Rightarrow R$ — поле

Definition **5.23** *(Простое расширение)* $\quad E/F$ — простое $\quad E = F(\alpha), \alpha \in E$

Definition **5.24** *(Композит двух полей)* $\quad F, F' \leq E \quad F(F') = F \cdot F' = F'(F)$

Remark **5.25** 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

5.2 Split fields (of a polynomial)

aka Поле разложения

Theorem **5.26** For any polynomial there exists its splitting field with degree $\leq (\deg f)!$ over F.

Proof … $\square$

Remark **5.27** Многочлены от конечного количества переменных — область целостности, как и от бесконечного, так как для многочлена рассмотрим подкольцо используемых переменных.

Theorem **5.28** lk

Theorem **5.29** lk