

Теория чисел (теория)

Владимир Латыпов
donrumata03@gmail.com

Vladimir Latypov
donrumata03@gmail.com

Содержание

1 Базовые определения	3
2 Идеалы	4
3 Евклидовы кольца	6
3.1 sdfasf	9
3.1.1 dasasd	9
4 vdsf	9
4.1 231	9
5 Поля	11
5.1 Построение циркулем и линейкой	14
5.2 Split fields (of a polynomial)	14

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 1.2

• S_n — группа, но не абелева

ОПРЕДЕЛЕНИЕ 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)

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 (Гомоморфизм колец) $f : R_1 \rightarrow R_2$

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

ПРИМЕР 1.7 (Независимость третьей аксиомы)

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

— 1, 2 выполнены, но не 3

ОПРЕДЕЛЕНИЕ 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 $y = x^{-1}$)

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 (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 1.12 \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 2.2

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

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

ОПРЕДЕЛЕНИЕ 2.4 (Операции над идеалами)

- Сложение
- Пересечение
- определяются поэлементно
- Умножение: натягиваем на произведение множеств по Минковскому

ОПРЕДЕЛЕНИЕ 2.5 Идеал, порождённый подмножеством $S \subset R$:

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

Он же —

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

ЗАМЕЧАНИЕ 2.6

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

(линейная комбинация)

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

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

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

ОПРЕДЕЛЕНИЕ 2.9 (Факторкольцо по идеалу) Введём отношение эквивалентности $a - b \in I$ и факторизуем по нему. Получим R/I — кольцо с элементами $x + I$, $x \in R$.

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

ОПРЕДЕЛЕНИЕ 2.11 (Простой идеал) $p \leq R$ — простой $\stackrel{\text{def}}{\iff} ab \in p \Rightarrow a \in p \vee b \in p$.

Эквивалентно: $ab \equiv_p 0 \Rightarrow a \equiv_p 0 \vee b \equiv_p 0$

ОПРЕДЕЛЕНИЕ 2.12 (Нётерово кольцо) Конечно порождённое кольцо

ТЕОРЕМА 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)

Доказательство

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

(2) \rightarrow (3): Итеративно будем выбирать идеал, содержащий предыдущий, пока таковой имеется.

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

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

ТЕОРЕМА 2.14 (Гильберта о нётеровости кольца многочленов над нётеровым кольцом)

Пусть для $I \trianglelefteq R[x]$ $a(i) = \{r \in R \mid rx^i + \dots \in I\}$, то есть коэффициенты при x^i , когда это старшая степень.

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

! TODO !

3 Евклидовы кольца

ОПРЕДЕЛЕНИЕ 3.1 (Евклидово кольцо) $d : R \setminus \{0\} \rightarrow \mathbb{N}_0$, 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 3.2 $\mathbb{Z}, F[x]$

ТЕОРЕМА 3.3 Евклидово \rightarrow ОГИ

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

ОПРЕДЕЛЕНИЕ 3.4 (Факториальное кольцо (UFD — Unique factorization domain)) Область целостности

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

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

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

ОПРЕДЕЛЕНИЕ 3.7 (Простой элемент) $a \mid bc \Rightarrow a \mid b \vee a \mid c (\Leftrightarrow aR — \text{простой идеал})$

ТЕОРЕМА 3.8 Простой \Rightarrow неприводимый

Доказательство

! TODO !

□

ТЕОРЕМА 3.9 В факториальном кольце: Неприводимый \Rightarrow простой

Доказательство

! TODO !

□

СЛЕДСТВИЕ 3.10 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 $0 \leq \underbrace{(a_i)}_{\text{прост.}} \leq p \rightarrow (a_i) = p$

□

! TODO !

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

ТЕОРЕМА 3.11 Евклидово \Rightarrow ОГИ \Rightarrow Факториальное

Доказательство (Евклидово \rightarrow ОГИ) ...

□

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

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

ЛЕММА 3.13 В ОГИ: неприводимый \rightarrow 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 3.14 нснм — начиная с некоторого места

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

ТЕОРЕМА 3.16 R факториально $\Rightarrow R[x]$ — тоже

ПРИМЕР 3.17 F — поле.

$f \in F[x]$ — неприводим.

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

• $\bar{g} \mid \deg g < \deg f$

• $(f, g) = 1$, то есть $1 = fp_1 + gp_2$, $\bar{1} = \bar{f}\bar{p}_1 + \bar{g}\bar{p}_2$

$\dim_F K = \deg f$

Можем построить все конечные поля.

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

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

ТЕОРЕМА 3.18 Над конечным полем существуют неприводимые многочлены любой степени

ПРИМЕР 3.19 $\mathbb{F}_2[x]/(x^2+x+1)$

Таблица сложения:

	0	1	α	β
0	0	1	3	4

ТЕОРЕМА 3.20 Группа простого порядка — циклическая

3.1 sdfasf

3.1.1 dasasd

3.1.1.1 asdf

4 vdsf

4.1 231

ТЕОРЕМА 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

ОПРЕДЕЛЕНИЕ 5.1 (Подполе)

Property 5.2 R — поле \Leftrightarrow в R ровно 2 идеала

Property 5.3 Гомоморфизмы полей инъективны, так как ядро — идеал

ОПРЕДЕЛЕНИЕ 5.4 (F -алгебра (алгебра над F)) кольцо R , тч $F \leq R$

ЗАМЕЧАНИЕ 5.5 Тогда это заодно и векторное пространство

ОПРЕДЕЛЕНИЕ 5.6 (Гомоморфизм F -алгебр)

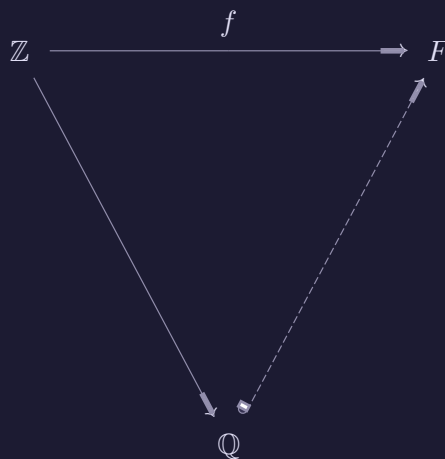
- $f : R \rightarrow R'$ — гомоморфизм колец
- $f(\alpha) = \alpha \forall \alpha \in F$ (сохраняет элементы поля)

ЗАМЕЧАНИЕ 5.7 Получается, это автоматически гомоморфизм векторных пространств

ОПРЕДЕЛЕНИЕ 5.8 (Характеристика)

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

1. $\ker f = 0$



1. $\ker f = (p)$

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

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

ТЕОРЕМА 5.10 (Единственность конечного поля) Конечные поля равного размера изоморфны.

ОПРЕДЕЛЕНИЕ 5.11 (Простые поля) Не содержат подполя

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

ОПРЕДЕЛЕНИЕ 5.13 (эндоморфизм Фробениуса) $f : \begin{pmatrix} R \rightarrow R \\ a \mapsto a^p \end{pmatrix}$.

- Если поле, то инъективен ($\ker f = 0$) и $\text{Im } f$ — подполе
- $R = \mathbb{F}_p$ — конечное поле \Rightarrow называют «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 5.14 (Унитарный многочлен) Старший коэффициент = 1

ТЕОРЕМА 5.15 (Лемма Гаусса)

ТЕОРЕМА 5.16 (Критерий Эйзенштейна)

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

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

Тогда h — неприводим

Доказательство

□

ОПРЕДЕЛЕНИЕ 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 .

$$E \xrightarrow{f} E'$$

ПРИМЕР 5.18

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

ТЕОРЕМА 5.19] $F \leq E \leq L$ $L/F < \infty \iff E/F < \infty$, при этом

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

Доказательство



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



□

ОПРЕДЕЛЕНИЕ 5.20 (Подалгебра, порождённая ?)

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

ЛЕММА 5.21 R — конечная F -алг. R — область целостности $\Rightarrow R$ — поле

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

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

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

СЛЕДСТВИЕ 5.22 E/F — конечное R — подалгебра $E \Rightarrow R$ — поле

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

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

ЗАМЕЧАНИЕ 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

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

Доказательство ...

□

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

ТЕОРЕМА 5.28 l_k

ТЕОРЕМА 5.29 l_k

ТЕОРЕМА 5.30 Корни многочлена переводятся автоморфизмом в корни многочлена

Существуют поле \mathbb{F}^n (поле разложения $x^{pn} - x$) Показываем, что оно размера p^n , показали что оно единственно Множественных корней нет по критерию $\gcd(f, f') = 1$