

Алгоритмы в математике (*теория чисел*)

Михайлов Максим

14 сентября 2021 г.

Оглавление

Лекция 1	4 сентября	2
1	Вводная лекция	2
Лекция 2	11 сентября	3
2	Алгебраические структуры	4
2.1	Структуры с одним законом композиции	4
2.2	Структуры с двумя законами композиции	5
2.3	Основные алгебраические структуры	5

Лекция 1

4 сентября

1 Вводная лекция

Хотя этот курс формально называется “теория чисел”, мы не будем рассматривать только теорию чисел. Теория чисел, разумеется, про числа, делители, простоту, алгоритм Евклида и т.д.. Однако, её можно обобщить на произвольные полугруппы, группы, кольца и поля. Поэтому мы будем рассматривать теорию чисел через призму общей алгебры.

Например, в кольце целых чисел есть понятие “простое число”. А в каких ещё кольцах есть “простые” элементы и каким условиям эти кольца удовлетворяют? Оказывается, кольцо многочленов содержит простые элементы и поэтому там применим алгоритм Евклида.

Мы также затронем теорию категорий (*терминальные объекты*), алгебраическую геометрию (*криптографию на эллиптических кривых*).

Лекция 2

11 сентября

План курса:

- Полугруппа
- Группа
 - Гомоморфизм
 - Фактор-группа
 - Теорема о ядре
 - Произведение групп
- Кольцо
 - \mathbb{Z}
 - Остатки
 - Китайская теорема об остатках
 - Алгоритм Евклида
 - Кольцо многочленов
 - Алгебра многочленов
- Поле
 - Поля Галуа
 - Расширения Галуа
 - Алгебраические кривые
 - Диофантовы уравнения

Начиная с групп мы будем использовать формализм теории категорий.

2 Алгебраические структуры

2.1 Структуры с одним законом композиции

Пусть M — множество с законом композиции $T : \forall x, y \in M \exists xTy \in M$.

Примечание. Такой закон называется **внутренним**, т.к. оба его аргумента $\in M$.

Обозначение. $x \cdot y, x \circ y, x + y, x^y, x * y$

Закон задает структуру на множестве.

Определение. $e_L \in M : \forall x \in M e_L \cdot x = x$ — **левый нейтральный элемент**

$e_R \in M : \forall x \in M x \cdot e_R = x$ — **правый нейтральный элемент**

Лемма 1. $\exists e_L, e_R \in M \Rightarrow e_L = e_R \stackrel{\text{def}}{=} e$

Доказательство. $e_L = e_L \cdot e_R = e_R$ □

Лемма 2. $e, e' — нейтральные элементы \Rightarrow e = e'$.

Доказательство. $e = e \cdot e' = e'$ □

Определение. $p \in M : p \cdot p = p$ — **идемпотент**

Определение. $z \in M : z \cdot x = z \cdot y \Rightarrow x = y$ — **регулярный элемент (левый)**

Определение. $x \in M, \exists e \in M$. Элемент $z \in M : z \cdot x = e$ — **левый обратный элемент к x** .

$y \in M : x \cdot y = e$ — **правый обратный элемент к x** .

Лемма 3. Если $\exists y, z$, то $y = z \stackrel{\text{def}}{=} x^{-1}$ — **обратный элемент**.

Доказательство. $z = z \cdot e = z \cdot (x \cdot y) = (z \cdot x) \cdot y = e \cdot y = y$. Здесь мы воспользовались **ассоциативностью** закона композиции. □

Определение. $\Theta_L : \forall x \in M \Theta_L \cdot x = \Theta_L$ — **поглощающий (слева) элемент**

$\Theta_R : \forall x \in M x \cdot \Theta_R = \Theta_R$ — **поглощающий (справа) элемент**

Лемма 4. $\exists \Theta_L, \Theta_R \Rightarrow \Theta_L = \Theta_R \stackrel{\text{def}}{=} \Theta$

Доказательство. $\Theta_L = \Theta_L \cdot \Theta_R = \Theta_R$ □

$\triangleleft x, y, z \in M, x \cdot y \cdot z = (x \cdot y) \cdot z$ или $x \cdot (y \cdot z)$. Какое выбрать? Без ассоциативности непонятно. Поэтому мы требуем ассоциативность в рамках этого курса.

То же самое можно сказать для семейства элементов.

Теорема 1 (об ассоциативном законе). $1 \leq k \leq n \Rightarrow T_{i=1}^n x_i = (T_{i=1}^k x_i) T (T_{i=k+1}^n x_i)$

Определение. $\triangleleft \forall x, y \in M \ xTy = yTx$. Тогда T называется **коммутативным**.

Определение. $\exists x, y \in M : xTy = yTx$. Тогда x, y называются **перестановочными** относительно закона.

Теорема 2 (об ассоциативном, коммутативном законе). Аргументы ассоциативного, коммутативного закона можно переставлять как угодно.

2.2 Структуры с двумя законами композиции

Пусть M — множество с законами композиции $*$, \circ . Нас интересует случай, когда эти два закона взаимосвязаны.

Как воспринимать $x * y \circ z$? Может иметь место **дистрибутивность** $*$ относительно \circ (слева): $x * (y \circ z) = (x * y) \circ (x * z)$

$\triangleleft e$ — нейтральный элемент по \circ . $\triangleleft x * y = x * (e \circ y) = (x * e) \circ (x * y) \Rightarrow x * e = e$. Поэтому из поля нельзя убрать ноль.

2.3 Основные алгебраические структуры

- **Полугруппа** — множество с ассоциативным законом
- **Моноид** — полугруппа с единицей
- **Группа** — моноид с обратным элементом для любого
- **Абелева группа** — группа с коммутативным законом
- **Кольцо** — два закона, по первому — абелева группа, по второму — полугруппа
- **Поле** — по двум законам группа