

Алгоритмы в математике (*теория чисел*)

Михайлов Максим

28 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 3	18 сентября	6
3	Внешний закон композиции	6
3.1	Фактор-структуры	7
Лекция 4	25 сентября	10
4	Структура групп	10
4.1	Смежные классы	12

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. $e, e' — \text{нейтральные элементы} \Rightarrow e = e'$.

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

Лекция 3

18 сентября

3 Внешний закон композиции

Пусть Ω — множество.

Определение. Внешний закон композиции — бинарная операция $g : \Omega \times M \rightarrow M$:

$$\forall \alpha \in \Omega, x \in M \quad g : (\alpha, x) \mapsto \alpha \perp x \in M$$

Пример. X — линейное пространство над \mathbb{R} . Тогда $g(\alpha, x) = \alpha \cdot x$.

Обозначение. $g(\alpha, x)$ обозначается как:

- $\alpha(x)$
- αx
- x^α

Пример. $M = \mathbb{Z}$ — абелева группа по сложению. $\triangleleft z \in \mathbb{Z}$.

$$\underbrace{z + z + z + \cdots + z}_n = nz$$

Слева написано применение внутреннего закона $n-1$ раз, а справа — применение внешнего закона. Не всегда внешний закон можно представить в виде внутреннего, иначе внешний закон был бы не содержательным.

Пусть M имеет внутренний закон композиции \top , множество Ω имеет внешний¹ закон \perp .

Обозначение.

¹ Относительно M .

- $\top = \circ$
- $\perp(\alpha, x) = \alpha x$

Определение. Внешний закон согласован с внутренним законом, если:

$$\alpha(x \circ y) = \alpha(x) \circ \alpha(y)$$

Пример. $\alpha(x + y) = \alpha x + \alpha y$, где $\alpha \in \mathbb{R}$

\triangleleft алгебраические структуры (M, \circ) , $(\Omega, *)$ и \perp — внешний закон Ω по M .

Определение.

$$\triangleleft \alpha, \beta \in \Omega, x \in M \quad (\alpha * \beta)x = \alpha(\beta(x))$$

Такой способ согласования мы называем **действием** Ω на M .

$$\begin{aligned} (\alpha * \beta)(x \circ y) &\stackrel{\text{согл.}}{=} (\alpha * \beta)(x) \circ (\alpha * \beta)(y) \\ &\stackrel{\text{действ.}}{=} \alpha(\beta(x)) \circ \alpha(\beta(y)) = \alpha(\beta(x \circ y)) \end{aligned}$$

Пример. $(\mathbb{Z}, +)$, (\mathbb{N}, \cdot)

$$\triangleleft n(z_1 + z_2) = nz_1 + nz_2$$

$$(n \cdot m)(z_1 + z_2)$$

Определение. Пусть есть множества $\{M, N \dots \Omega\}$ со своими внутренними законами композиции. Кроме того, некоторые из них могут являться носителями внешнего закона для других множеств. Этот набор множеств, внутренних и внешних законов есть алгебраическая структура.

3.1 Фактор-структуры

$\triangleleft M$, бинарное отношение² R

Свойства бинарного отношения:

- $\forall x \exists y : xRy$ — полнота
- $\forall x, y \ xRy \ \& \ xRz \Rightarrow yRz$ — евклидовость

Определение. R — отношение эквивалентности, если оно:

- Рефлексивно
- Симметрично

² Над M .

- Транзитивно

Определение. $\triangleleft(M, R)$ — множество с отношением эквивалентности. Тогда M/R — фактор-множество, состоящее из классов эквивалентности M по R . Каждому $x \in M$ сопоставляется класс эквивалентности $[x] \in M/R$

Пример. $\triangleleft M = \mathbb{N}$ с операцией сложения, $x, y \in M, \triangleleft(x, y) \in M \times M$.

$$(a_1, b_1) \sim (a_2, b_2) \stackrel{\text{def}}{\Leftrightarrow} a_1 + b_2 = a_2 + b_1$$

Несложно заметить, что фактор-множество $(M \times M)/\sim$ соответствует \mathbb{Z} :

Определение. $x \in M, y \in M$

$$[x \circ y] \stackrel{?}{=} [x] * [y]$$

Здесь $*$ — фактор-закон закона \circ .

Пример.

$$(a_1, b_1) \tilde{+} (a_2, b_2) \stackrel{\text{def}}{=} (a_1 + a_2, b_1 + b_2)$$

Чтобы рассмотреть $\hat{+}$ — фактор-закон операции $\tilde{+}$, нужно показать, что для $z = [(a_1 + a_2, b_1 + b_2)]$ верно $z = z_1 \hat{+} z_2$

Определение. Закон \circ согласован с отношением R , если:

$$\left. \begin{array}{l} \forall x, x_1 \in M \quad x R x_1 \\ \forall y, y_1 \in M \quad y R y_1 \end{array} \right\} \Rightarrow (x \circ y) R (x_1 \circ y_1)$$

Теорема 3. Если закон композиции согласован с отношением эквивалентности, то он совпадает со своим фактор-законом.

$$[x] * [y] \stackrel{\text{def}}{=} [x \circ y] = [x] \circ [y]$$

Обозначение.

$$M \cdot N := \{m \cdot n \mid m \in M, n \in N\}$$

Пример.

- $(a_1, b_1), (a_2, b_2) \in M \times M$
- $(c_1, d_1) \sim (a_1, b_1) \Leftrightarrow c_1 + b_1 = d_1 + a_1$
- $(a_1, b_1) \rightarrow [(a_1, b_1)] = z_1 \ni (c_1, d_1)$
- $(a_2, b_2) \rightarrow [(a_2, b_2)] = z_2 \ni (c_2, d_2)$
- $(a_1, b_1) \tilde{+} (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \rightarrow [(a_1 + a_2, b_1 + b_2)] = z$

Выполнено ли $(c_1 + c_2, d_1 + d_2) \in z$?

$$c_1 + c_2 + (b_1 + b_2) = d_1 + d_2 + (a_1 + a_2)$$

$$a_1 + d_1 = b_1 + c_1$$

$$a_2 + d_2 = b_2 + c_2$$

Таким образом, наша операция согласована.

Лекция 4

25 сентября

4 Структура групп

Определение (группа). G — множество с внутренним законом \cdot , таким что:

1. $\forall x, y, z \in G \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\exists e \in G : \forall x \in G \quad e \cdot x = x \cdot e = x$
3. $\forall x \in G \quad \exists x^{-1} \in G : xx^{-1} = x^{-1}x = e$

Пример. Пусть S — множество, G — группа. Будем обозначать множество отображений $S \rightarrow G$ как $M(SG)$. Наделим его структурой группы:

$$f, g \in M(SG) \Rightarrow \begin{cases} (f \cdot g)(x) = f(x) \cdot g(x) \\ f(x^{-1}) = f(x)^{-1} \\ f_e(x) = e_G \end{cases}$$

Определение. $G, G, \sigma : G \rightarrow G'$.

σ — гомоморфизм группы G в группу G' , если:

$$\forall x, y \in G \quad \sigma(xy) = \sigma(x)\sigma(y), \sigma(e_G) = e_{G'}$$

Лемма 5. $\sigma(x^{-1}) = \sigma(x)^{-1}$

Доказательство.

$$\begin{aligned} e_{G'} &= \sigma(e_G) = \sigma(xx^{-1}) = \sigma(x)\sigma(x^{-1}) \\ \sigma(x)^{-1}e_{G'} &= \sigma(x)^{-1}\sigma(x)\sigma(x^{-1}) \\ \sigma(x)^{-1} &= \sigma(x^{-1}) \end{aligned}$$

□

Обозначение.

- $\text{hom}(G \rightarrow G')$ — множество всех гомоморфизмов $G \rightarrow G'$.
- $\text{End}(G) := \text{hom}(G \rightarrow G)$.

Определение. $\sigma \in \text{hom}(G \rightarrow G')$ называется **изоморфизмом**, если:

$$\chi \in \text{hom}(G' \rightarrow G) : \sigma \circ \chi = \text{id}_{G'}, \chi \circ \sigma = \text{id}_G$$

Обозначение.

- $\text{Iso}(G \rightarrow G')$ — множество всех изоморфизмов
- $\text{Aut}(G) := \text{Iso}(G \rightarrow G)$ — множество **автоморфизмов**

Лемма 6. $\sigma \in \text{hom}(G \rightarrow G'), \chi \in \text{hom}(G' \rightarrow G'') \Rightarrow \zeta = \chi \circ \sigma \in \text{hom}(G \rightarrow G'')$

Доказательство.

$$\begin{aligned} \forall x, y \in G \quad \zeta(x \cdot y) &= (\chi \circ \sigma)(x \cdot y) \\ &= \chi(\sigma(x \cdot y)) \\ &= \chi(\sigma(x) \cdot \sigma(y)) \\ &= (\chi \circ \sigma)(x) \cdot (\chi \circ \sigma)(y) \\ &= \zeta(x) \cdot \zeta(y) \end{aligned}$$

□

Примечание. $\text{Aut}(G)$ — группа относительно \circ .

Определение. G — группа.

$\triangleleft S_G = \{S_i\}_{i \in I}$:

$$\forall g \in G \quad a = \prod_{j \in J \subseteq I} S_j$$

S_G тогда называется **множеством образующих группы G** .

Лемма 7. Мы проиграли, вернемся к этой лемме позже.

Определение (ядро гомоморфизма).

$$\text{Ker } \sigma := \{g \in G : \sigma(g) = e\}$$

Лемма 8. Если $\text{Ker } \sigma = \{e\}$, то $\sigma(x) = \sigma(y) \Rightarrow x = y$, т.е. σ инъективно.

Доказательство.

$$\sigma(x)\sigma(y^{-1}) = \sigma(y)\sigma(y^{-1}) = e_{G'}$$

Таким образом, x есть обратный к y^{-1} , т.е. $x = y$. □

Определение (образ гомоморфизма).

$$\text{Im } \sigma = \{g' \in G' : \exists g \in G : \sigma(g) = g'\}$$

Лемма 9. $\text{Im } \sigma = G' \Rightarrow \sigma$ сюръективно.

$$\left. \begin{array}{l} \text{Im } \sigma = G' \\ \text{Ker } \sigma = \{e\} \end{array} \right\} \Rightarrow \sigma - \text{изоморфизм}$$

Определение. Подгруппой H группы G называется подмножество элементов G , на котором групповой закон G индуцирует структуру группы.

Определение. Несобственные подгруппы: $\{e_G\}, G$.

Иначе подгруппа **собственная**.

Пример. $\sigma \in \text{hom}(G, G')$. Тогда $\text{Ker } \sigma$ — подгруппа G , $\text{Im } \sigma$ — подгруппа G' .

4.1 Смежные классы

Пусть G — группа, H — подгруппа G .

Определение. $gH, g \in G$ — левый смежный класс группы G по подгруппе H .

Лемма 10. Пусть $\exists z : z \in gH, z \in g'H$. Тогда $gH = g'H$

Доказательство. $z = gh, z = g'h' \Rightarrow gh = g'h' \Rightarrow g = g'h'h^{-1}$

$$gH = (g'h'h^{-1})H = g'h'h^{-1}H$$

□

Лемма 11.

$$\forall g, g' \in G \quad |gH| = |g'H|$$

Доказательство. Отображение $h \mapsto gg^{-1}h$ есть биекция между gH и $g'H$ □

Обозначение. $(G : H)$ — индекс группы G по H — количество смежных классов.

Примечание. В общем случае это кардинальное число, но мы будем рассматривать только конечные индексы.

$(G : 1)$ — количество элементов G (порядок группы).

Лемма 12.

$$(G : 1) \cdot (G : H)$$

Теорема 4. H — подгруппа G , K — подгруппа H .

$$(G : H)(H : K) = (G : K)$$

Доказательство.

$$G = \bigcup_i g_i H \quad H = \bigcup_j h_j K$$

$$G = \bigcup_i \bigcup_j g_i h_j K$$

$$g_i h_j K = g'_i h'_j K \Rightarrow \begin{cases} g_i H = g'_i H \\ h_j K = h'_j K \end{cases} \Rightarrow \begin{cases} g_i = g'_i \\ h_j = h'_j \end{cases}$$

□

Лемма 13 (проигранная). Дано: G, G' — группы, S_G — множество производящих G , $f : S_G \rightarrow G'$.

Если $\exists \tilde{f} \in \text{hom}(G, G')$, то $\tilde{f}|_{S_G} = f \Rightarrow \tilde{f}$ единственно.

$$\begin{array}{ccc} S_G & \xrightarrow{f} & G' \\ & \nearrow \tilde{f} \in \text{hom}(G, G') & \\ G & & \end{array}$$

Доказательство. $\triangleleft g \in G, g' := \tilde{f}(g)$

$$g = \prod_{i \in I} S_i \quad \tilde{f}(g) = \tilde{f}\left(\prod_{i \in I} S_i\right) = \prod_{i \in I} \tilde{f}(S_i) = \prod_{i \in I} f(S_i)$$

□

Определение. Подгруппа H группы G называется **нормальной** или **инвариантной**, если $\forall g \in G \quad gH = Hg$. Аналогично можно определить через $H = g^{-1}Hg$

Обозначение. $H \triangleleft G$

Лемма 14.

- G — группа

$$\bullet \sigma \in \text{hom}(G, G')$$

Тогда $\text{Ker } \sigma$ — нормальная подгруппа G .

Доказательство. $H := \text{Ker } \sigma$

$$\sigma(e) = \sigma(g^{-1}g) = \sigma(g^{-1})\sigma(g) = \sigma(g^{-1})e\sigma(g) = \sigma(g^{-1})\sigma(H)\sigma(g) = \sigma(g^{-1}Hg) = e_{G'}$$

Таким образом, $g^{-1}Hg \subset H$. Заменяем g на g^{-1} : $H \subset g^{-1}Hg \Rightarrow H = g^{-1}Hg$. \square

$\triangleleft G$ — группа, H — подгруппа G .

Рассмотрим отношение \sim : $g_1 \sim g_2 \Leftrightarrow g_1g_2^{-1} \in H$. Это отношение эквивалентности:

1. $g_1g_1^{-1} = e \in H$
2. $g_1g_2^{-1} \in H \Rightarrow (g_1g_2^{-1})^{-1} \in H \Rightarrow g_1^{-1}g_2 \in H$
3. $g_1g_2^{-1} \in H, g_2g_3^{-1} \in H \Rightarrow g_1g_3^{-1} \in H$

Кроме того, $g_1 \sim g_2 \Leftrightarrow g_1H = g_2H$, поэтому \sim это отношение эквивалентности на смежных классах, будем обозначать фактор-множество как G/H .

Для каких H выполняется следующее: если $x_1 \sim y_1$ и $x_2 \sim y_2$, тогда $(x_1x_2) \sim (y_1y_2)$? $x_1H = y_1H, x_2H = y_2H$. Тогда H — нормальная подгруппа.

$\triangleleft G/H, H \triangleleft G, \cdot : [x] \cdot [y] = [x \cdot y]$. Свойства “ \cdot ”:

1. $[x] \cdot ([y] \cdot [z]) = ([x] \cdot [y]) \cdot [z]$
2. $\exists [e] : [x][e] = [e][x] = [x], [e] = H$
3. $[x]^{-1} = [x^{-1}]$

Примечание. G/H — фактор-группа.

$$\triangleleft \sigma : \text{Ker } \sigma = H$$

Тогда пусть $\sigma : G \rightarrow G/H, g \mapsto [g]$.