

# Алгоритмы в математике (*теория чисел*)

Михайлов Максим

18 ноября 2021 г.

# Оглавление

Лекция 1	4 сентября	3
1	Вводная лекция . . . . .	3
Лекция 2	11 сентября	4
2	Алгебраические структуры . . . . .	5
2.1	Структуры с одним законом композиции . . . . .	5
2.2	Структуры с двумя законами композиции . . . . .	6
2.3	Основные алгебраические структуры . . . . .	6
Лекция 3	18 сентября	7
3	Внешний закон композиции . . . . .	7
3.1	Фактор-структуры . . . . .	8
Лекция 4	25 сентября	11
4	Структура групп . . . . .	11
4.1	Смежные классы . . . . .	13
Лекция 5	2 октября	16
4.2	Цепочки гомоморфизмов . . . . .	16
5	Действие группы . . . . .	18
5.1	Орбиты . . . . .	19
Лекция 6	9 октября	20
6	Действие группы на себя . . . . .	20
6.1	Сопряжение . . . . .	20
6.2	Левая трансляция . . . . .	22
7	Циклические группы . . . . .	22
Лекция 7	16 октября	23
8	Силовские группы . . . . .	24
Лекция 8	23 октября	27
8.1	Теоремы Силова . . . . .	27

# 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  $\Omega$  — 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:

- $\alpha(x)$
- $\alpha x$
- $x^\alpha$

*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  $\Omega$  имеет внешний<sup>1</sup> закон  $\perp$ .

*Обозначение.*

---

<sup>1</sup> 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  $\Omega$  по  $M$ .

**Определение.**

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

Такой способ согласования мы называем **действием**  $\Omega$  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 отношение<sup>2</sup>  $R$

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

---

<sup>2</sup> 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,  $x, y \in M$ ,  $\triangleleft(x, y) \in M \times M$ .

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

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

$\sigma$  — 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.

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

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

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

Обозначение.

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

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

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.  $\sigma$  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

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

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  $g^{-1}$ :  $H \subset g^{-1}Hg \Rightarrow H = g^{-1}Hg$ . □

$\triangleleft G$  — 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  $\sigma : G \rightarrow G/H, g \mapsto [g]$ .

# Лекция 5

## 2 октября

**Определение.**

- $G$  — группа
- $S \subset G$  — подмножество элементов  $G$

**Нормализатор  $S$ :**  $N_S := \{g \in G : gS = Sg\}$

**Определение.**

- $G$  — группа
- $x \in G$
- $S \subset G$

**Централизатор  $x$ :**  $Z_x := \{g \in G : gx = xg\}$

$Z_S := \{g \in G : \forall y \in S \quad gy = yg\}$

$Z_G$  — центр группы  $G$ .

*Пример.* В группе  $GL(n, \mathbb{R})$  инвертируемых матриц  $n \times n$  центр — единичная матрица.

### 4.2 Цепочки гомоморфизмов

**Определение.**

- $G, G', G''$  — группы
- $\sigma \in \text{hom}(G, G')$
- $\chi \in \text{hom}(G', G'')$

Рассмотрим цепочку  $G \xrightarrow{\sigma} G' \xrightarrow{\chi} G''$ . Такая последовательность называется **точной**, если  $\text{Ker } \chi = \text{Im } \sigma$ .





$$(G/K)/(H/K) = G/H$$

## 5 Действие группы

**Определение.**

- $G$  — группа
- $S$  — множество

$G$  действует на  $S$ , если существует отображение

$$T : G \times S \rightarrow S$$

, при этом  $(g_1 g_2)s = g_1(g_2 s)$

*Примечание.*

$$T_{g_1} T_{g_2} = T_{g_1 g_2} \quad T_e = \text{id} \quad T_{g^{-1}} = T_g^{-1}$$

$G$  действует на  $S$  как группа перестановок.

**Определение.**

- $s \in S$
- $G$  — группа

$G_s := \{g \in G : gs = s\}$  — **стабилизатор** элемента  $s$ .

*Пример.*  $\mathbb{Q}$  действует на  $\mathbb{R}^3$  через  $T$ .

**Лемма 15.**  $G_s \subset G$  — подгруппа

*Доказательство.*  $g_1, g_2 \in G_s \Rightarrow g_1 s = s, g_2 s = s$

$$(g_1 g_2) \cdot s = g_1(g_2 s) = g_1 s = s$$

□

$G/G_s$  — фактор-множество.

**Лемма 16.**  $s, s' \in S, s' = xs, x \in G$ . Тогда  $G_{s'} = xG_s x^{-1}$  и  $G_{s'}$  вместе с  $G_s$  называются **сопряженными**

*Доказательство.*

$$g' s' = s' = xs = xgs = xgx^{-1} s'$$

$$g' = xgx^{-1}$$

□

**Определение.** Преобразование вида  $xAx^{-1}$ , где  $A \subset G$  — подгруппа  $G$ , называется сопряжением.

**Лемма 17.**  $gG_s, g'G_s \in G/G_s$

$$gs = g's \Leftrightarrow gG_s = g'G_s$$

## 5.1 Орбиты

**Определение.**  $\mathcal{O}_G(S) := \{gs : g \in G\}$  — орбита

**Лемма 18.**  $|\mathcal{O}_G(S)| = (G : G_S)$

*Доказательство.* Из предыдущей леммы. □

Остаётся на следующую лекцию:

1.  $S = \bigsqcup_{S \in C} \mathcal{O}_G(S)$ , где  $C$  — непересекающиеся орбиты
2. Действия группы на себя

## Лекция 6

### 9 октября

**Лемма 19.** Орбиты элементов  $\mathcal{O}_G(s)$  и  $\mathcal{O}_G(s')$  или непересекаются или совпадают.

*Доказательство.* Пусть орбиты пересекаются, т.е.  $\exists s_0 : s_0 \in \mathcal{O}_G(s)$  и  $s_0 \in \mathcal{O}_G(s')$ . Тогда  $\exists g \in G : s_0 = gs, \exists g' \in G : s_0 = g's'$

$$\mathcal{O}_G(s') = \mathcal{O}_G(g's') = \mathcal{O}_G(s_0) = \mathcal{O}_G(gs) = \mathcal{O}_G(s)$$

Таким образом,  $\mathcal{O}_G(s') = \mathcal{O}_G(s)$ . □

*Примечание.*

$$S = \bigsqcup_{i \in I} \mathcal{O}_G(S_i)$$

*Примечание.* Если  $S$  — конечно, то

$$|S| = \sum_{i \in I} |\mathcal{O}_G(s_i)|$$

## 6 Действие группы на себя

Пусть  $S_G = G$ , т.е. группа действует сама на себя.

### 6.1 Сопряжение

Пусть  $x \in G$ .  $\sigma : x \mapsto \sigma_x : \sigma_x(y) = xyx^{-1}$

Пусть  $y, y' \in G$ .

$$\sigma_x(y \cdot y') = xy'y^{-1} = xyx^{-1}xy'x^{-1} = \sigma_x(y)\sigma_x(y')$$

$$\sigma_x(e) = e$$

Таким образом,  $\sigma_x$  — гомоморфизм.

$$\sigma_x^{-1} = \sigma_{x^{-1}}$$

$$\sigma_x^{-1} \circ \sigma_x = \text{id}_G$$

$$\sigma_x^{-1} \circ \sigma_x(y) = G_x^{-1}(xyx^{-1}) = x^{-1}xyx^{-1}x = y \quad \forall y$$

$$\sigma_x \in \text{Aut}(G) \quad \forall x$$

$$\triangleleft \sigma : G \rightarrow \text{Aut}(G).$$

$$\sigma_x \sigma_y = \sigma_{xy} \quad \sigma_e = \text{id}_G$$

Таким образом,  $\sigma \in \text{hom}(G, \text{Aut}(G))$

$$\text{Ker } \sigma = \{x \in G : \forall y \quad \sigma_x y = y\}$$

$$xyx^{-1} = y$$

$$xy = yx$$

Таким образом,  $\text{Ker } \sigma = Z_G$

Рассмотрим  $G$  как множество.  $A \subset G$  — подмножество  $G$ .

$$\triangleleft \sigma_x(A) = xAx^{-1} \subset G$$

$$\triangleleft \sigma_x(H) = xHx^{-1} \subset G \text{ — подгруппа } G.$$

Пусть  $S$  — множество подгрупп группы  $G$ ,  $H$  — подгруппа  $G$ , рассмотрим  $G/H$ .

Пусть  $x \in G$ .

$$G_x := \{g \in G : \sigma_g(x) = x\} = Z_x$$

$$\mathcal{O}_G(x) = \{\sigma_g(x), g \in G\}$$

$$|\mathcal{O}_G(x)| = (G : Z_x)$$

$$G = \bigsqcup_{i \in I} \mathcal{O}_G(x_i)$$

$$\boxed{|G| = \sum_{i \in I} (G : Z_{x_i})}$$

$$G_H = \{g \in G : \sigma_g H = H\} \stackrel{\text{def}}{=} N_H$$

$$G = \bigsqcup_{i \in I} \mathcal{O}_G(H_i) \quad |G| = \sum_{i \in I} (G : N_i)$$

## 6.2 Левая трансляция

Пусть  $x \in G$ .  $\tau : x \mapsto \tau_x : y \mapsto xy$ .

$\tau_x(yu') = xyu'$  — не гомоморфизм.

Пусть  $H \subset G$  — подгруппа  $G$ . Сопряжение не определяло действие, а трансляция определяет:  $\triangleleft G/H : [g] = gH$ , тогда  $\tau_x(gH) = xgH = g'H \in G/H$ .

## 7 Циклические группы

**Определение.** Группа  $G$  называется **циклической**, если  $\exists g : \forall h \in G \ h = g^m = \underbrace{g \cdot g \cdots}_m$ .

*Обозначение.*  $G = \langle g \rangle$

**Определение.** Показатель элемента  $g$  в  $G = \langle g \rangle$  это число  $m > 0$ , такое что  $g^m = e$ .

**Определение.** Показатель группы  $\langle g \rangle$  — число  $k > 0$ , такое что  $\forall x \in G \ x^k = e$ .

*Пример.*  $(\mathbb{Z}, +)$  — бесконечная циклическая группа.

Если  $H$  — подгруппа  $\mathbb{Z}$ , то  $H = \{mz\}_{m \in \mathbb{Z}}$ ,  $z := \min\{t \in \mathbb{Z} \mid t > 0\}$

# Лекция 7

## 16 октября

Пусть  $G$  — произвольная группа,  $\triangleleft \sigma : \mathbb{Z} \rightarrow G, \sigma : z \mapsto a^z$

$\text{Im } \sigma = \langle a \rangle \subset G$

Есть два случая:

1.  $\text{Ker } \sigma = \{0\} \Rightarrow \text{Im } \sigma \cong \mathbb{Z}$  и  $G$  содержит бесконечную циклическую подгруппу.
2.  $\text{Ker } \sigma \neq \{0\} \Rightarrow \text{Ker } \sigma = H \subset \mathbb{Z} \Rightarrow H = \{nh\}_{n \in \mathbb{Z}} \Rightarrow \mathbb{Z}/H = \{[0], [1], [2] \dots [h-1]\}$

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/H \xrightarrow{\sigma^*} G \\ & \searrow \sigma & \nearrow \end{array}$$

Разложили  $\sigma = \sigma^* \circ \varphi$ , где  $\varphi$  — канонический гомоморфизм.

Тогда  $\sigma^*$  отображает  $\mathbb{Z}/H$  в  $a^0, a^1, a^2 \dots a^{h-1}$ , где  $a^h = a^0 = e$ .

*Утверждение.* Все элементы различны, т.е.  $\triangleleft s, r : a^s = a^r$ . Тогда  $s = r$ .

*Доказательство.*  $a^{s-r} = e \Rightarrow s - r = kh = 0 \Rightarrow s = r$ . □

**Определение.** Пусть  $G$  — циклическая группа  $a^0, a^1 \dots a^{h-1}$ . Тогда  $h$  — **период** элемента  $a$ . Это не то же самое, что показатель: показатель имеет вид  $qh$ .

**Лемма 20.**  $G$  — конечная  $\Rightarrow$  период  $\forall g \in G$  делит порядок группы.

*Доказательство.* Пусть  $d$  — период  $g \in G$ , тогда  $g^d = e$ .

$\triangleleft H = \langle g \rangle$  — подгруппа  $G$  и  $|H| = d$

$$|G| = (G : 1) = (G : H)(H : 1) = (G : H)|H|$$

□

**Лемма 21.** Пусть  $|G| = p$  — простое число,  $\langle g \in G, g \neq e$ .

Тогда  $G = \langle g \rangle$ .

*Доказательство.*  $\langle g \in G, g \neq e$

$\langle H = \langle g \rangle \Rightarrow |H| \neq 1$ , т.к.  $e \in H, g \in H$ .

$p = (G : 1) = (G : H)(H : 1)$ . Но тогда  $(G : H) = 1$  по простоте  $p$ , следовательно  $G = \langle g \rangle$   $\square$

**Лемма 22.**  $G$  — циклическая группа. Тогда

1.  $H \subset G$  — циклическая
2.  $\sigma(G)$  — циклическая, если  $\sigma \in \text{Hom}(G)$

*Доказательство.*  $G$  — циклическая группа

1. (a)  $G$  — бесконечная циклическая группа.

Тогда  $G \cong \mathbb{Z}$  — знаем все подгруппы (они циклические).

- (b)  $G$  — конечная циклическая группа.

$\langle H \subset G$  — подгруппа.

$|G| : |H| \Rightarrow |H|$  конечна.

$\langle a \in H \Rightarrow a = g^n \Rightarrow a^k = g^{kn} \Rightarrow H = \langle a \rangle$

2. Пусть  $G = \langle g \rangle$ , тогда  $\sigma(g)$  — образующая для  $\sigma(G)$  и значит  $\sigma(G) = \langle \sigma(g) \rangle$

$\square$

**Лемма 23.**  $G$  — бесконечная циклическая группа. Тогда у  $G$  есть две образующие:  $g$  и  $g^{-1}$ .

## 8 Силовские группы

**Определение.** Группа называется  $p$ -группой, если ее порядок является степенью простого числа  $p$ .

**Определение.** Подгруппа  $H$  называется  $p$ -подгруппой группы  $G$ , если  $H \subset G$ ,  $H$  —  $p$ -группа.

**Определение.**  $H$  называется силовой подгруппой  $G$ , если  $H$  —  $p$ -подгруппа  $G$  и  $|H| = p^n$ , где  $p^n$  — максимальный порядок в группе.



Пусть  $n$  — порядок группы  $G$ . Мы знаем<sup>1</sup>, что  $n = p_1^{n_1} p_2^{n_2} \dots$ , где  $p_i$  — простые.  $n_i$  — максимальная степень  $p_i$ , которая встречается в  $n$ , т.е.  $n \not\equiv p_i^{n_i+1}$ . Т.к. порядок подгруппы делит порядок группы, то найдутся подгруппы, порядки которых соответствуют этому разложению.

**Лемма 24.**

- $|G| = m$
- Показатель  $G = n$
- $G$  — коммутативная группа

Тогда порядок  $G$  делит некоторую степень показателя:

$$\exists k : n^k \vdots m$$

*Доказательство.* По индукции (по порядку группы)

$\triangleleft H \triangleleft G, H = \langle b \rangle$ . Т.к. показатель  $G = n, b^n = e$ .

$\triangleleft |G/H|$

Так как  $n \vdots (H : 1)$  и по индукции  $n^k \vdots (G : H)$ , то  $n^{k+1} \vdots (G : 1) = (G : H)(H : 1)$  □

**Лемма 25.**

- $G$  — конечная абелева группа
- $|G| \vdots p$  ( $p$  — простое)

Тогда  $\exists H \subset G : |H| = p$ .

*Доказательство.*  $|G| \vdots p$  по условию.

$\triangleleft H = \langle x \rangle, x^n = e$

Пусть показатель группы  $G$  есть  $n, m$  — порядок группы.

$$m \vdots p \Rightarrow \exists s : m = sp$$

Некоторая степень показателя делится на порядок группы:  $n^k \vdots m \Rightarrow \exists z : n^k = z \cdot m = zsp$

$$x^{zs} =: y, y^p = e \Rightarrow H' = \langle y \rangle \text{ — искомая группа}$$

□

---

<sup>1</sup> Но докажем потом.

**Теорема 5.**

- $G$  — конечная группа
- $|G| \vdots p$  ( $p$  — простое)

Тогда в  $G$   $\exists$  силовская подгруппа.

*Доказательство.* По индукции.

Если  $|G| = p$ , искомое очевидно.

Пусть искомое доказано для всех порядков меньших  $G$ .

Пусть  $H \subset G \Rightarrow (G : 1) = (G : H)(H : 1)$

1. Если  $|H| \vdots p$ , то силовская подгруппа для  $G$  будет силовской подгруппой для  $H$ , которая существует по индукционному предположению.
2. Если  $(G : H) \vdots p$

Пусть  $G$  действует на себя.

$$(G : 1) = |Z_G| + \sum_x (G : G_x)$$

Так как  $(G : 1) \vdots p$  и  $\forall x : (G : G_x) \vdots p \Rightarrow |Z_G| \vdots p$ , т.е. центр нетривиальный. Кроме того, центр абелев, следовательно по лемме 25  $\exists H \subset Z_G$  - абелева подгруппа, такая что  $|H| = p$ .

Т.к.  $H \subset G$ ,  $H \triangleleft G \Rightarrow G/H$ . В  $G/H$  существует силовская подгруппа  $p^{n-1}$  по индукционному предположению, назовём её  $K'$ .

$|K'| = p^{n-1}$ ,  $|K'H| = p^{n-1} \cdot p = p^n$ , при этом  $K'H$  — подгруппа, т.к.  $H$  — нормальная подгруппа.  $K'H$  — искомая подгруппа.

□

# Лекция 8

## 23 октября

### 8.1 Теоремы Силова

*Примечание.*

- $G$  — произвольная группа
- $H, K$  — подгруппы  $G$
- $H \subset N_K = \{g \in G : gKg^{-1} = K\}$

Тогда:

1.  $HK$  — подгруппа  $G$

*Доказательство.*  $\triangleleft h_1k_1, h_2k_2 \in HK$

$$(h_1k_1)(h_2k_2) = h_1k_1h_2k_2 = \underbrace{h_1h_2}_h \underbrace{k_1k_2}_k$$

□

2.  $K \triangleleft HK \Rightarrow \exists HK/K$

$\triangleleft \varphi : HK \rightarrow HK/K$  — канонический гомоморфизм

$\text{Ker } \varphi = K$ , т.к.  $1 \cdot K \cdot K = K^2 = K$ , что есть нейтральный элемент фактор-группы.

Мы запутались, но каким-то образом  $HK/K \cong H/H \cap K$ .

Не дописано

**Теорема 6** (первая теорема Силова). Каждая  $p$ -подгруппа содержится в силовой  $p$ -подгруппе.

*Доказательство.* Пусть  $G$  — группа,  $S$  — множество силовских  $p$ -подгрупп и  $G$  действует на  $S$  сопряжением.

$$\langle \mathcal{P} \in S, S = S_G$$

$$S_0 := O_G(\mathcal{P}) \stackrel{\text{def}}{=} \{g\mathcal{P}g^{-1}\}_{g \in G} = \{\tilde{\mathcal{P}}_1, \tilde{\mathcal{P}}_2 \dots \tilde{\mathcal{P}}_m\}$$

Сколько элементов в  $S_0$ ?  $(G : \mathcal{P}) \not\vdash p \Rightarrow |S_0| \not\vdash p$

Пусть  $H$  —  $p$ -подгруппа  $G$ , действующая на  $S_0$  сопряжением.

*Примечание.*  $|H| = p^k \Rightarrow \forall \tilde{H} \subset H \quad |\tilde{H}| \vdash p$

$$|S_0| = \sum_C (H : \tilde{H}_x)$$

Т.к.  $H$  —  $p$ -подгруппа, остатки от деления  $(H : \tilde{H}_x)$  либо  $\vdash p$ , либо  $= 1$ . Т.к.  $|S_0| \not\vdash p$ , существуют слагаемые, не делящиеся на  $p$  и по предыдущему утверждению они равны единице. Рассмотрим одну из таких групп,  $\tilde{H}'$ . Ей соответствует  $\mathcal{P}'$ , причём  $O_H(\mathcal{P}') = \mathcal{P}'$ ,  $\forall h \in H \quad h\mathcal{P}'h^{-1} = \mathcal{P}' \Rightarrow h\mathcal{P}' = \mathcal{P}'h$ , а следовательно  $H \subset N_{\mathcal{P}'}$ .

Так как  $HK/K \cong H/H \cap K$ ,  $H\mathcal{P}'/\mathcal{P}' \cong H/(H \cap \mathcal{P}') \Rightarrow \mathcal{P}'H \cong \mathcal{P}' \Rightarrow H \subset \mathcal{P}' \quad \square$

**Теорема 7** (вторая теорема Силова). Силоские  $p$ -подгруппы сопряжены.

**Теорема 8** (третья теорема Силова). Число силоских  $p$ -подгрупп  $\equiv 1 \pmod p$ .

Не дописано