Алгоритмы в математике *(теория чисел)*

Михайлов Максим

29 октября 2021 г.

Оглавление

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

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 $y = z \overset{\text{def}}{=} x^{-1}$ — **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. $\exists \Theta_L, \Theta_R \Rightarrow \Theta_L = \Theta_R \overset{\text{def}}{=} \Theta$

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). $1 \leq k \leq n \Rightarrow T_{i=1}^{n} x_i = \left(T_{i=1}^{k} x_i\right) T \left(T_{i=k+1}^{n} x_i\right)$

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 $g : \Omega \times M \to M$:

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

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. $\lhd z \in \mathbb{Z}$.

$$\underbrace{z + z + z + \dots + z}_{n} = nz$$

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 внешний[1] 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 $\alpha \in \mathbb{R}$

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

Определение.

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

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

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

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

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

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

Определение. Пусть есть множества $\{M, N \ldots \Omega\}$ 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

$\lhd M$, бинарное отношение[2] 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. $\sphericalangle(M, R)$ — 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. $\sphericalangle M = \mathbb{N}$ с операцией сложения, $x, y \in M, \sphericalangle(x, y) \in M \times M$.

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

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

Определение. $x \in M, y \in M$

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

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

Пример.

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

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

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

$$\left.\begin{array}{l} \forall x, x_1 \in M \;\; xRx_1 \\ \forall y, y_1 \in M \;\; yRy_1 \end{array}\right\} \Rightarrow (x \circ y)R(x_1 \circ y_1)$$

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

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

Обозначение.

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

Пример.

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

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

Пример. Пусть S — множество, G — группа. Будем обозначать множество отображений $S \to G$ 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. $G, G, \sigma : G \to G'$.

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

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

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

Доказательство.

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

□

Обозначение.

- $\hom(G\ G')$ — множество всех гомоморфизмов $G \to G'$.
- $\mathrm{End}(G) \coloneqq \hom(G\ G)$.

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

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

Обозначение.

- $\mathrm{Iso}(G\ G')$ — множество всех изоморфизмов
- $\mathrm{Aut}(G) \coloneqq \mathrm{Iso}(G\ G)$ — множество **автоморфизмов**

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

Доказательство.

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

□

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

Определение. G — группа.

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

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

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

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

Определение (ядро гомоморфизма).

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

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

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).

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

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

$$\left.\begin{aligned} &\mathrm{Im}\,\sigma = G' \\ &\mathrm{Ker}\,\sigma = \{e\} \end{aligned}\right\} \Rightarrow \sigma - \text{изоморфизм}$$

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

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

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.

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

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

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

Доказательство.

$$G=\bigcup_i g_iH \quad H=\bigcup_j h_jK$$

$$G=\bigcup_i\bigcup_j g_ih_jK$$

$$g_ih_jK=g_i'h_j'K\Rightarrow\begin{cases}g_iH=g_i'H\\h_jK=h_j'K\end{cases}\Rightarrow\begin{cases}g_i=g_i'\\h_j=h_j'\end{cases}$$

□

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

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

$$\begin{tikzcd}
S_G \arrow[rr, "f"] & & G' \\
& G \arrow[ur, "\tilde f\in\hom(G\ G')"'] &
\end{tikzcd}$$

Доказательство. $\lhd g\in G, g':=\tilde f(g)$

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

□

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

Обозначение. $H\lhd G$

Лемма 14.

- G — группа

- $\sigma \in \hom(G\, G')$

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

Доказательство. $H \coloneqq \operatorname{Ker}\sigma$

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

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

$\lhd G$ — 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 обозначат 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.

$\lhd G/H, H \lhd G, \cdot : [x] \cdot [y] = [x \cdot y]$. 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.

$\lhd \sigma : \operatorname{Ker}\sigma = H$

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

Лекция 5

2 октября

Определение.

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

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

Определение.

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

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

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

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
- $\sigma \in \hom(G\, G')$
- $\chi \in \hom(G'\, G'')$

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

Свойства.

1. Ker $(\chi \circ \sigma) = G$
2. Если σ — сюръекция, то Ker $\chi = G'$
3. Если χ — инъекция, то Ker $\sigma = G$

Пример. $H \lhd G \Rightarrow H \xrightarrow{j} G \xrightarrow{\varphi} G/H$, где j — вложение, φ — канонический гомоморфизм $g \mapsto gH$. Тогда $\forall h \in H$ $(\varphi \circ j)(h) = \varphi(j(h)) = \varphi(h) = hH = 1H = 1_{G/H}$, следовательно эта последовательность точная.

Также рассматриваются последовательности вида $0 \longrightarrow G \xrightarrow{\sigma} G' \xrightarrow{\chi} G'' \longrightarrow 0$, где 0 — группа из одного элемента. Пусть эта последовательность точная. Гомоморфизм $0 \to G$ сопоставляет этому элементу G_e, следовательно Im $(0 \to G) = \{G_e\} \Rightarrow$ Ker $\sigma = \{G_e\} \Rightarrow \sigma$ инъективно. Аналогичными рассуждениями χ сюръективно.

Определение. $\lhd$ $0 \longrightarrow G \xrightarrow{\sigma_1} G' \xrightarrow{\sigma_2} G'' \xrightarrow{\sigma_3} \ldots \xrightarrow{\sigma_{n-1}} G^{(n)} \xrightarrow{\sigma_n} \ldots$. Такая последовательность называется точной, если Ker $\sigma_i =$ Im σ_{i-1}.

$\lhd$ $0 \longrightarrow H \xrightarrow{j} G \xrightarrow{\varphi} G/H \xrightarrow{\tilde{\sigma}} G'$

$\lhd \sigma \in \hom(G\ G'), \sigma = \tilde{\sigma} \circ \varphi$:
$$\begin{tikzcd} G \arrow[rr, "\sigma"] \arrow[dr, "\varphi"'] & & G' \\ & G/H \arrow[ur, "\tilde{\sigma}"'] & \end{tikzcd}$$

Покажем, что $\tilde{\sigma}$ единственно. $\tilde{\sigma} : gH \mapsto \sigma(g)$.

Рассмотрим другую цепочку
$$\begin{tikzcd} G \arrow[r, "\varphi"] & G/H \arrow[r, "\lambda"] \arrow[rr, bend right, "\tilde{\sigma}"'] & \mathrm{Im}\,\sigma \arrow[r, "j"] & G' \end{tikzcd}$$

$\lambda : gH \mapsto \sigma(g)$, Ker $\lambda = \{H\}$, λ — биективно. Таким образом, λ — изоморфизм и $G/H \simeq$ Im σ.

Примечание.

- G — группа
- $H \lhd G, K \lhd G$
- $K \subset H$ — подгруппа

Тогда:

1. $K \lhd H$.

   $\lhd \chi : G/K \to G/H, gK \mapsto gH,$ Ker $\chi = \{hK\}_{h \in H}$, т.к. $hK \mapsto hH = H$.

$$\boxed{(G/K)/(H/K) = G/H}$$

5 Действие группы

Определение.

- G — группа
- S — множество

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

$$T : G \times S \to S$$

, при этом $(g_1 g_2)s = g_1(g_2 s)$

Примечание.

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

G действует на S как группа перестановок.

Определение.

- $s \in S$
- G — группа

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

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

Лемма 15. $G_s \subset G$ — подгруппа

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

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

$\lhd G/G_s$ — 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. $\mathcal{O}_G(S) \coloneqq \{gs : g \in G\}$ — **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 $y, y' \in G$.

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

$$\sigma_x(e) = e$$

Таким образом, σ_x — гомоморфизм.

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

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

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

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

$\triangleleft \sigma : G \to \mathrm{Aut}(G)$.

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

Таким обрзом, $\sigma \in \hom(G, \mathrm{Aut}(G))$

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

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

$$xy = yx$$

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

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

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

$\triangleleft \sigma_x(H) = xHx^{-1} \subset G$ — 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 $x \in G$. $\tau : x \mapsto \tau_x : y \mapsto xy$.

$\tau_x(yy') = xyy'$ — не гомоморфизм.

Пусть $H \subset G$ — подгруппа G. Сопряжение не определяло действие, а трансляция определяет: $\lhd G/H : [g] = gH$, 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 $H = \{mz\}_{m \in \mathbb{Z}}$, $z \coloneqq \min\{t \in \mathbb{Z} \mid t > 0\}$

Лекция 7

16 октября

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

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

Есть два случая:

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

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\varphi"] \arrow[rr, bend right, "\sigma"'] & \mathbb{Z}/H \arrow[r, "\sigma^*"] & G \end{tikzcd}$$

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

Тогда σ^* отображает $\mathbb{Z}/H$ в $a^0, a^1, a^2 \ldots a^{h-1}$, 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 $a^0, a^1 \ldots a^{h-1}$. 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, $\vartriangleleft g \in G, g \neq e$.

Тогда $G = \langle g \rangle$.

Доказательство. $\vartriangleleft g \in G, g \neq e$

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

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

Лемма 22. G — циклическая группа. Тогда

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

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.

   $\vartriangleleft H \subset G$ — подгруппа.

   $|G| \vdots |H| \Rightarrow |H|$ конечна.

   $\vartriangleleft a \in H \Rightarrow a = g^n \Rightarrow a^k = g^{kn} \Rightarrow H = \langle a \rangle$
2. Пусть $G = \langle g \rangle$, тогда $\sigma(g)$ — образующая для $\sigma(G)$ и значит $\sigma(G) = \langle \sigma(g) \rangle$

□

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 **силовской** 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[1], что $n = p_1^{n_1} p_2^{n_2} \ldots$, где p_i — простые. n_i — максимальная степень p_i, которая встречается в n, т.е. $n \not\vdots p_i^{n_i+1}$. 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: $n^k \vdots m \Rightarrow \exists z : n^k = z{\cdot}m = zsp$

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

□

[1] Но докажем потом.

Лемма 26.

- 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. $H \subset G$, $H \lhd G \Rightarrow G/H$. В G/H существует силовская подгруппа p^{n-1} по индукционному предположению, назовём ее 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.

$\square$