

Алгоритмы в математике (*теория чисел*)

Михайлов Максим

17 декабря 2021 г.

Оглавление

Лекция 1	4 сентября	4
1	Вводная лекция	4
Лекция 2	11 сентября	5
2	Алгебраические структуры	6
2.1	Структуры с одним законом композиции	6
2.2	Структуры с двумя законами композиции	7
2.3	Основные алгебраические структуры	7
Лекция 3	18 сентября	8
3	Внешний закон композиции	8
3.1	Фактор-структуры	9
Лекция 4	25 сентября	12
4	Структура групп	12
4.1	Смежные классы	14
Лекция 5	2 октября	17
4.2	Цепочки гомоморфизмов	17
5	Действие группы	19
5.1	Орбиты	20
Лекция 6	9 октября	21
6	Действие группы на себя	21
6.1	Сопряжение	21
6.2	Левая трансляция	23
7	Циклические группы	23
Лекция 7	16 октября	24
8	Силовские группы	25
Лекция 8	23 октября	28
8.1	Теоремы Силова	28
Лекция 9	30 октября	30
9	Элементы теории категорий	30
9.1	Определения	30
9.2	Коммутативные диаграммы	31
9.3	Функтор	32
Лекция 10	6 ноября	34
9.4	Произведения и копроизведения	34
Лекция 11	13 ноября	37

10 Свободные группы	38
Лекция 12 4 декабря	41
11 Кольца	41
Лекция 13 11 декабря	46
11.1 Делимость в кольце	46

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

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:

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

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

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

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).

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

Лемма 8. Если $\ker \sigma = \{e\}$, 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.

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

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 $\ker \sigma$ — 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 $\ker \sigma$ — нормальная подгруппа G .

Доказательство. $H := \ker \sigma$

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

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.

$$\triangleleft \sigma : \ker \sigma = H$$

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 $\ker \chi = \text{Im } \sigma$.

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

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

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

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

$$xy = yx$$

Таким образом, $\ker \sigma = Z_G$

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, $\langle \sigma : \mathbb{Z} \rightarrow G, \sigma : z \mapsto a^z$

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

Есть два случая:

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

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

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

Тогда σ^* 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. $\langle s, r : a^s = a^r \rangle$. 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 $g^d = e$.

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

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

□

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

Тогда $G = \langle g \rangle$.

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

$\triangleleft H = \langle g \rangle \Rightarrow |H| \neq 1$, 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.

$\triangleleft H \subset G$ — подгруппа.

$|G| : |H| \Rightarrow |H|$ конечна.

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

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 знаем¹, 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: $n^k \vdots m \Rightarrow \exists z : n^k = z \cdot m = zsp$

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

□

¹ 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 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.

□

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

$\ker \varphi = K$, 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 ? $(G : \mathcal{P}) \not\equiv p \Rightarrow |S_0| \not\equiv p$

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

Примечание. $|H| = p^k \Rightarrow \forall \tilde{H} \subset H \quad |\tilde{H}| \not\equiv p$

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

Т.к. H — p -подгруппа, остатки от деления $(H : \tilde{H}_x)$ либо $\equiv p$, либо $= 1$. Т.к. $|S_0| \not\equiv p$, 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

Лекция 9

30 октября

9 Элементы теории категорий

Теория категорий позволит нам обобщить уже известные нам утверждения и позволит их применять в других алгебраических структурах, например кольцах.

9.1 Определения

Определение. \mathcal{C} — категория:

1. Коллекция объектов $\text{Obj}(\mathcal{C}) : A, B, C \dots X, Y$
2. Множество морфизмов $\text{Arr}(\mathcal{C}) : f, g, h, \varphi, \chi, \psi$
 $\triangleleft A, B \in \text{Obj}(\mathcal{C}), A \xrightarrow{f} B, f \in \text{Mor}(A, B)$
3. $\text{Mor}(B, C) \times \text{Mor}(A, B) = \text{Mor}(A, C)$

Аксиомы категории:

1. Множества морфизмов не пересекаются: $f \in \text{Mor}(A, B), f \in \text{Mor}(A', B') \Leftrightarrow A = A', B = B'$
2. $f \in \text{Mor}(A, B), g \in \text{Mor}(B, C), h \in \text{Mor}(C, D) \Rightarrow (h \circ g) \circ f = h \circ (g \circ f)$
3. $\forall A \in \text{Obj}(\mathcal{C}) \exists \text{id}_A \in \text{Mor}(A, A) : \begin{cases} \forall f \in \text{Mor}(A, B) & f \circ \text{id}_A = f \\ \forall g \in \text{Mor}(B, A) & \text{id}_A \circ g = g \end{cases}$

Определение. $f \in \text{Mor}(A, B)$ — **изоморфизм**, если $\exists g \in \text{Mor}(B, A)$:

$$\begin{cases} g \circ f = \text{id}_A \\ f \circ g = \text{id}_B \end{cases}$$

Определение. Автоморфизм — изоморфизм из объекта в него же, т.е. $f \in \text{Mor}(A, A)$, f — изоморфизм $\Rightarrow f \in \text{Aut}(A)$

Определение. Эндоморфизм — морфизм из объекта в него же, $\text{End}(A) = \text{Mor}(A, A)$

Лемма 26. $\text{End}(A)$ — моноид

Лемма 27. $\text{Aut}(A)$ — группа

Категории, которые мы будем рассматривать:

- Set — категория множеств.
- Mon — категория моноидов.
- Grp — категория групп.
- Set_G — категория множеств, на которые действует группа.

$\triangleleft \text{Set}_G = \mathcal{C}, G$ — группа.

Пусть $A, B \in \text{Obj}(\mathcal{C}), A = A_G, B = B_G$

$\text{Mor}(A, B)$ — отображения множеств.

Действие группы это $\sigma : x \mapsto \sigma_x$, где $x \in G, \sigma_x$ — перестановка множества A .

9.2 Коммутативные диаграммы

Пусть \mathcal{C} — категория. Рассмотрим категорию $\zeta : \text{Obj}(\zeta) = \text{Arr}(\mathcal{C})$. Пусть $f \in \text{Mor}(A, B), g \in \text{Mor}(A', B')$. Рассмотрим $(\varphi, \psi) \in \text{Mor}(f, g)$, такие что $\varphi, \psi \in \text{Arr}(\mathcal{C})$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \varphi & & \downarrow \psi \\ A' & \xrightarrow{g} & B' \end{array}$$

Если свойство $g \circ \varphi = \psi \circ f$ выполнено, то эта диаграмма называется **коммутативной**.

Рассмотри категорию $\mathcal{C}, A \in \text{Obj}(\mathcal{C})$, рассмотрим $\mathcal{C}_A : f \in \text{Obj}(\mathcal{C}_A) \quad f : X \rightarrow A \quad \forall X \in \text{Obj}(\mathcal{C})$, то есть категорию стрелок в некоторый отмеченный элемент A .

$\triangleleft f : X \rightarrow A, g : X' \rightarrow A, \varphi \in \text{Arr}(\mathcal{C}_A), \varphi \in \text{Mor}(f, g), \varphi : X \rightarrow X'$, тогда $g \circ \varphi = f$, т.е. следующая диаграмма коммутативна:

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & X' \\ & \searrow f & \swarrow g \\ & A & \end{array}$$

9.3 Функтор

Определение. Рассмотрим категории \mathcal{A}, \mathcal{B} . **Ковариантный функтор** — отображение, которое:

- Каждому $A \in \text{Obj}(\mathcal{A})$ сопоставляет $F(A) \in \text{Obj}(\mathcal{B})$.
- Каждому $f \in \text{Mor}(A, B)$ ¹ сопоставляет $F(f) \in \text{Mor}(F(A), F(B))$

со следующими аксиомами:

1. $\forall A \in \text{Obj}(\mathcal{A}) \quad F(\text{id}_A) = \text{id}_{F(A)}$
2. $\forall f \in \text{Mor}(A, B), g \in \text{Mor}(B, C) \quad F(g \circ f) = F(g) \circ F(f)$

Пример. $\mathcal{C} := \text{Grp}$, $\text{Obj}(\mathcal{C})$ — группы, $\text{Arr}(\mathcal{C})$ — гомоморфизмы групп.

Рассмотрим стирающий функтор F , который группам сопоставляет множества, а гомоморфизмам — отображения.

Лемма 28. Функтор переводит изоморфизм в изоморфизм.

Определение. Рассмотрим категории \mathcal{A}, \mathcal{B} . **Контравариантный функтор** — отображение, которое:

- Каждому $A \in \text{Obj}(\mathcal{A})$ сопоставляет $F'(A) \in \text{Obj}(\mathcal{B})$.
- Каждому $f \in \text{Mor}(A, B)$ ² сопоставляет $F'(f) \in \text{Mor}(F'(B), F'(A))$

со следующими аксиомами:

1. $\forall A \in \text{Obj}(\mathcal{A}) \quad F'(\text{id}_A) = \text{id}_{F'(A)}$
2. $\forall f \in \text{Mor}(A, B), g \in \text{Mor}(B, C) \quad F'(g \circ f) = F'(f) \circ F'(g)$

Обозначение. F — ковариантный функтор, F' — контравариантный функтор.

$\triangleleft \mathcal{A}, A \in \text{Obj}(\mathcal{A}), F_A : \mathcal{A} \rightarrow \text{Set}$

$$\forall X \in \text{Obj}(\mathcal{A}) \quad F_A(X) = \text{Mor}(A, X)$$

$$\forall f \in \text{Mor}(X, X') \quad F_A(f) = \text{Mor}(A, X) \rightarrow \text{Mor}(A, X'), \varphi \mapsto f \circ \varphi$$

$$\begin{array}{ccc} X & \xrightarrow{f} & X' \\ & \nwarrow \varphi & \nearrow f \circ \varphi \\ & A & \end{array}$$

$$F_A^c : \mathcal{A} \rightarrow \text{Set}$$

$$\forall Y \in \text{Obj}(\mathcal{A}) \quad F_A^c(Y) = \text{Mor}(Y, A)$$

¹ $A \in \text{Obj}(\mathcal{A}), B \in \text{Obj}(\mathcal{B})$

² $A \in \text{Obj}(\mathcal{A}), B \in \text{Obj}(\mathcal{B})$

$$\forall g \in \text{Mor}(Y', Y) \quad F_A^c(g) : \text{Mor}(Y', A) \rightarrow \text{Mor}(Y, A)$$

$$\begin{array}{ccc} Y & \xleftarrow{g} & Y' \\ & \searrow \psi & \swarrow g \circ \psi \\ & A & \end{array}$$

Построенные функторы — представляющие³.

³ Кажется, у АС ошибка — такие функторы называются представимыми.

Лекция 10

6 ноября

9.4 Произведения и копроизведения

Определение. Произведением $A \in \text{Obj}(\mathcal{A})$ и $B \in \text{Obj}(\mathcal{A})$ называется тройка $\{P, f, g\}$, где:

- $P \in \text{Obj}(\mathcal{A})$
- $f, g \in \text{Arr}(\mathcal{A})$

, такая что если $\varphi : A \rightarrow C, \psi : B \rightarrow C$, тогда \exists морфизм h , такой что $\varphi = f \circ h, \psi = g \circ h$, т.е. следующая диаграмма¹ коммутует:

$$\begin{array}{ccccc} & & C & & \\ & \swarrow \varphi & \downarrow h & \searrow \psi & \\ A & \xleftarrow{f} & P & \xrightarrow{g} & B \end{array}$$

Пример. $\mathcal{A} = \text{Set}$

Тогда категориальное произведение $S_1 \in \text{Obj}(\mathcal{A}), S_2 \in \text{Obj}(\mathcal{A})$ есть $\{S_1 \times S_2, \text{proj}_1, \text{proj}_2\}$.

Обобщение: (прямое)² произведение $\{A_i\}_{i \in I}$ это $(P, \{f_i\}_{i \in I})$, удовлетворяющее условию:

$$\forall C \in \text{Obj}(\mathcal{A}) : g_i : C \rightarrow A_i \quad \exists h : g_i = f_i \circ h$$

Примечание. Произведение двух объектов обозначается как $A \times B$, произведение нескольких как $\prod_{i \in I} A_i$

Определение. Копроизведение $A \in \text{Obj}(\mathcal{A})$ и $B \in \text{Obj}(\mathcal{A})$ — тройка $\{P', f, g\}$, где:

¹ На лекции диаграмма была представлена в другом виде, но категорист во мне взвыл в этот момент.

² Иногда говорят “прямое”, обычно — нет.

- $P' \in \text{Obj}(\mathcal{A})$
- $f, g \in \text{Arr}(\mathcal{A})$

, такая что

$$\forall C \in \text{Obj}(\mathcal{A}), \varphi : A \rightarrow C, \psi : B \rightarrow C \quad \exists h : P' \rightarrow C : \varphi = h \circ f, \psi = h \circ g$$

, т.е. следующая диаграмма коммутует:

$$\begin{array}{ccccc} & & C & & \\ & \nearrow \varphi & \uparrow h & \nwarrow \psi & \\ A & \xrightarrow{f} & P' & \xleftarrow{g} & B \end{array}$$

Пример. Пусть $\mathcal{A} = \text{Set}$, $S_1 \in \text{Obj}(\mathcal{A})$, $S_2 \in \text{Obj}(\mathcal{A})$. Пусть U — копроизведение S_1 и S_2 . Тогда $U = (\{1\} \times S_1) \cup (\{2\} \times S_2)$ ³.

Обобщение: копроизведение $\{A_i\}_{i \in I}$ это $(P', \{f_i\}_{i \in I})$, удовлетворяющее условию:

$$\forall C' \in \text{Obj}(\mathcal{A}) : g_i : A_i \rightarrow C' \quad \exists h : P' \rightarrow C' : g_i = h \circ f_i$$

Определение. Инициальным объектом в \mathcal{A} называется $I \in \text{Obj}(\mathcal{A})$, такой что:

$$\forall A \in \text{Obj}(\mathcal{A}) \quad \exists! \varphi : I \rightarrow A$$

Определение. Терминальным объектом в \mathcal{A} называется $T \in \text{Obj}(\mathcal{A})$, такой что:

$$\forall B \in \text{Obj}(\mathcal{A}) \quad \exists! \varphi : B \rightarrow T$$

Примечание. Терминальный и инициальный объект универсальны.

$$\begin{array}{ccc} I & \xrightarrow{\varphi} & I' \\ & \xleftarrow{\varphi'} & \end{array}$$

По определению:

$$\varphi \circ \varphi' : I' \rightarrow I'$$

$$\varphi' \circ \varphi : I \rightarrow I$$

³ Это дизъюнктивное объединение.

Рассмотрим категорию \mathcal{A} , $\{A_i\}, B, B' \in \text{Obj}(\mathcal{A})$ и категорию ζ , где $\{f_i : A_i \rightarrow B\} \in \text{Obj}(\zeta)$ и $\{f'_i : A_i \rightarrow B'\} \in \text{Obj}(\zeta)$.



$\varphi : B \rightarrow B'$ — морфизм в \mathcal{A} , но с другой стороны это и морфизм в ζ , т.к. $f'_i = \varphi \circ f_i$.

P — копроизведение.

В ζ $\{g_i : A_i \rightarrow P\}$ является универсальным объектом.

Лекция 11

13 ноября

Пусть $\{G_i\}$ — группы. Рассмотрим объект $\prod_i G_i$ — декартово произведение этих групп как множеств.

Пусть $G_i = \{x'_i, x''_i \dots\}$, $\prod_i G_i = \{(x_i, x_j \dots)\} = \{(x_i)\}$

Лемма 29. $\prod_i G_i$ может быть наделено структурой группы.

$\triangleleft (x_i), (y_i) \in \prod_i G_i$ и $(x_1, x_2 \dots x_n \dots) * (y_1, y_2 \dots y_n \dots) = (x_1 y_1, x_2 y_2 \dots x_n y_n \dots)$

Доказательство. Проверим аксиомы группы. Они все очевидны из аксиом групп G_i . \square

$\triangleleft \lambda_j : G_j \rightarrow \prod_i G_i$ $\lambda_j(x) = (e_1, e_2 \dots x \dots e_n \dots)$ и обратное к нему отображение proj_j

Лемма 30. $(\prod_i G_i, \{\text{proj}_k\})$ — произведение в Grp .

Доказательство. Рассмотрим $\tilde{G} \in \text{Obj}(\text{Grp})$, $\{g_i : \tilde{G} \rightarrow G_i\}$. Нужно показать, что $\exists! h : \tilde{G} \rightarrow \prod_i G_i$ такое, что $f_i \circ h = g_i$.

$\triangleleft y \in \tilde{G}, y \xrightarrow{h} (y_i) \xrightarrow{\text{proj}_i} y_i$

$g_i(y) = (y)_i$, поэтому $f_i \circ \underbrace{h(y)}_{x_1 \dots x_i \dots} = \underbrace{g_i(y)}_{x_i}$. Тогда $h(y)$ существует, и это может быть только $(g_1(y), g_2(y) \dots g_n(y) \dots)$, из этого следует единственность.



□

Лемма 31 (критерий прямого произведения).

- G — группа
- H, K — подгруппы G
- $H \cap K = \{e\}$
- $\forall x \in H \ y \in K \ xy = yx$
- $HK = G$

Тогда и только тогда $H \times K \cong G$

Доказательство. $\triangleleft \psi : (x, y) \mapsto xy, \psi \in \text{hom}(H \times K, G)$

Сюръективность очевидна, т.к. $HK = G$.

Рассмотрим (x, y) , такие что $\psi((x, y)) = e$. Тогда $xy = e \Rightarrow x = y^{-1}$. $y \in K \Rightarrow y^{-1} \in K \Rightarrow x \in K$, но кроме того $x \in H \Rightarrow x \in H \cap K$, следовательно, $x = e$. Аналогично $y = e$.

Т.к. ψ — биективный гомоморфизм, ψ — изоморфизм.

□

Обобщение:

$$H_1 \times H_2 \times \dots \times H_n \cong G \Leftrightarrow \begin{cases} H_{j+1} \cap (H_1 H_2 \dots H_j) = \{e\} \\ H_i H_j = H_j H_i \ \forall i, j \end{cases}$$

10 Свободные группы

Рассмотрим S — множество.

$\triangleleft g : S \rightarrow g(S) \subset G$, где $g(S)$ — множество образующих группы G .

Определение. Отображение $g : S \rightarrow G$ порождает группу G , если образ g порождает G .

Определение. S — множество образующих¹ группы G , если $\forall y \in G \ y = \prod_i x_i$, где $x_i \in S$ или $x_i^{-1} \in S$

Рассмотрим два отображения $f : S \rightarrow F, g : S \rightarrow G$, где $f(S)$ порождает F и $g(S)$ порождает G .



По доказанной ранее лемме 13 существует не более одного гомоморфизма g_* .

Рассмотрим категорию ζ , объекты которой являются парами вида (F, f) . Рассмотрим гомоморфизм $\varphi : F \rightarrow G$, тогда $\varphi \in \text{Arr}(\zeta)$: $(F, f) \xrightarrow{\varphi} (G, g)$.

Определение. Свободная группа, определяемая множеством S — инициальный объект в категории ζ .

Теорема 9. Для всякого множества S существует определяемая им свободная группа (F, f) , при этом:

1. f инъективен.
2. f порождает F .

Доказательство. Рассмотрим случай, когда S конечно.

$\triangleleft T$ — счётное множество. Пусть на нём мы можем заводить групповые структуры, множество всех таких структур назовём Γ . Пусть тогда T_γ , где $\gamma \in \Gamma$ — реализация группы на T .

Рассмотрим отображение φ между S и T_γ . Т.к. множество образующих можно по-разному вкладывать в T_γ . Чтобы это фиксировать, скажем, что $\varphi : S \rightarrow T_{\gamma, \varphi}$. $T_{\gamma, \varphi} \in \text{Obj}(\zeta)$, а $T_\gamma \in \text{Grp}$.

Рассмотрим также множество $M_\gamma = \{\varphi\}$ — множество отображений S в T_γ .²

$$F_0 := \prod_{g \in \Gamma} \prod_{\varphi \in M_\gamma} T_{\gamma, \varphi}$$

$F_0 \in \text{Grp}$ ³, поскольку это произведение элементов $\text{Obj}(\text{Grp})$. Рассмотрим $f_0 : S \rightarrow F_0$: $S \mapsto (\varphi_1(S)_{\gamma_1}, \varphi_2(S)_{\gamma_1} \dots \varphi'_1(S)_{\gamma_2}, \varphi'_2(S)_{\gamma_2} \dots)$.

¹ Также называется множеством порождающих.

² $M_\gamma = \text{Arr}(-, T_\gamma)$

³ Мы игнорируем тот факт, что произведение это тройка из объекта и двух морфизмов, нас интересует только объект.

Покажем, что $\forall g : S \rightarrow G \exists! g_* : F_0 \rightarrow G$, такой что следующая диаграмма коммутативна:

$$\begin{array}{ccc} & F_0 & \\ f_0 \nearrow & & \downarrow g_* \\ S & & G \\ g \searrow & & \end{array}$$

Пусть $g(S)$ порождает G . Т.к. S конечно, $|G| \leq |T|$, т.к. T счётно.

Рассмотрим $\bar{G} = G \times \mathbb{Z}$. Надо, чтобы $|G \times \mathbb{Z}| = |T|$ и тогда будет существовать биекция между $G \times \mathbb{Z}$ и T , тогда $\exists \gamma \in \Gamma : G \times \mathbb{Z} \cong T_\gamma$ с изоморфизмом $\lambda : G \times \mathbb{Z} \rightarrow T_\gamma$.

$$S \xrightarrow{g} G \xrightarrow{h} G \times \mathbb{Z} \xrightarrow{\lambda} T_\gamma$$

$$\psi := \lambda \circ h \circ g \in M_\gamma \quad S \xrightarrow{\psi} T_{\gamma, \psi}$$

$$\psi_* := \text{proj}_G \circ \lambda^{-1} \circ \text{proj}_{\gamma, \psi}$$

$$\begin{array}{ccc} F_0 & \xrightarrow{\text{proj}_{\gamma, \psi}} & T_{\gamma, \psi} \\ \downarrow \psi_* & & \downarrow \lambda^{-1} \\ G & \xleftarrow{\text{proj}_G} & G \times \mathbb{Z} \end{array}$$

$$\begin{array}{ccc} & F_0 & \\ f_0 \nearrow & \downarrow \text{proj}_{\gamma, \psi} & \\ S & T_{\gamma, \psi} & \\ & \downarrow \lambda^{-1} & \\ & G \times \mathbb{Z} & \\ g \searrow & \downarrow \text{proj}_G & \\ & G & \end{array} \quad \begin{array}{c} \psi_* \\ \curvearrowright \end{array}$$

Рассмотрим $f : S \rightarrow F$, $f(S) = F$. Для единственности g_* мы сужаем его на $g_*|_F$. Весь трюк заключается в том, что в F_0 много лишнего, т.к. там много одинаковых элементов.

f инъективно, т.к. всех $\varphi \in M_\gamma$ найдётся инъективное.

Если S несчётно, ты мы не знаем что делать.

Если S счётно, то все то же самое, но за T возьмём S и тогда $G \times \mathbb{Z} \cong T \underbrace{\times \mathbb{Z} \times \mathbb{Z} \times \dots}_{\text{нужное количество } \mathbb{Z}}$ \square

Лекция 12

4 декабря

11 Кольца

Определение. Множество R с бинарными операциями $+$ и \cdot называется **кольцом**, если:

1. $(R, +)$ — коммутативная группа
2. (R, \cdot) — моноид
3. Дистрибутивность справа и слева:

$$\begin{aligned}a \cdot (b + c) &= ab + ac \\(a + b) \cdot c &= ac + bc\end{aligned}$$

Пример.

- $R = \mathbb{Z}$
- $R = \mathbb{R}_{n \times n}$

Определение. Кольцо R **коммутативно**, если $ab = ba$.

Примечание. Мы будем рассматривать в основном коммутативные кольца. Если не сказано иначе, то кольцо коммутативно.

Примечание. $0, 1 \in R$, где:

- 0 — нейтральный по $+$
- 1 — из моноида (R, \cdot)

Примечание. Если $0 = 1$, то $R = \{0\}$

Определение. $a \in R$ называется **обратимым**, если $\exists b : ab = 1$.

Определение. R^* называется группой обратимых элементов (или группой единиц):

$$R^* := \{a \in R \mid \exists b \ ab = 1\}$$

Теорема 10. (R^*, \cdot) — группа.

Примечание.

- $0 \cdot a = 0$
- $(-1) \cdot a = -a$
- $(-a)(-b) = a \cdot b$

Определение. $S \subset R$ называется подкольцом, если S — кольцо с индуцированными операциями.

Примечание. $S \subset R$ — подкольцо, если $+$ и \cdot замкнуты в S .

Пример. $S = 2\mathbb{Z}$ — подкольцо

Вообще говоря, можно рассматривать кольцо без 1.

Определение. $J \subset R$ называется идеалом, если J — подкольцо и $\forall a \in R \ \forall x \in J \ ax \in J$

Пример. $J = 2\mathbb{Z}$ — идеал

Определение. $\mathcal{I}(R)$ — множество идеалов.¹

Определение. Если $J_1, J_2 \in \mathcal{I}(R)$, то:

$$J_1 + J_2 := \langle J_1 + J_2 \rangle := \{x + y \mid x \in J_1, y \in J_2\}$$

Теорема 11. $J_1 + J_2 \in \mathcal{I}(R)$

Доказательство. $\triangleleft x_1 + y_1, x_2 + y_2 \in J_1 + J_2$

$$(x_1 + y_1) + (x_2 + y_2) = (x_1 + x_2) + (y_1 + y_2) \in J_1 + J_2$$

$$\triangleleft a \in R, x + y \in J_1 + J_2$$

$$a \cdot (x + y) = \underbrace{ax}_{J_1} + \underbrace{ay}_{J_2} \in J_1 + J_2$$

□

Примечание. Если S — подкольцо, то $0 \in S$

Теорема 12. $J_1 \in \mathcal{I}(J_1 + J_2)$

¹ На лекции обозначено I , но это чаще используется для дробных идеалов.

Определение. Если $J_1, J_2 \in \mathcal{I}(R)$, то:

$$\underbrace{J_1 \cdot J_2}_{\text{умножение идеалов}} := \overbrace{\langle J_1 \cdot J_2 \rangle}^{\text{поэлементное умножение}} := \left\{ \sum_{k=1}^n x_k y_k \mid x_k \in J_1, y_k \in J_2, n \in \mathbb{N} \right\}$$

Теорема 13. $J_1 \cdot J_2 \in \mathcal{I}(R)$

Доказательство. $\triangleleft a \in R$

$$\begin{aligned} \sum_{k=1}^n x_k y_k &\in J_1 J_2 \\ a \sum_{k=1}^n x_k y_k &= \sum_{k=1}^n \underbrace{a x_k}_{\in J_1} y_k \in J_1 \cdot J_2 \end{aligned}$$

□

Примечание. Вообще говоря, $\mathcal{I}(R)$ — не кольцо, только полукольцо.

Определение. Если $J_1, J_2 \in \mathcal{I}(R)$, то:

$$J_1 \cap J_2 := \{x \mid x \in J_1, x \in J_2\}$$

Теорема 14. $J_1 \cap J_2 \in \mathcal{I}(R)$

Доказательство. $\triangleleft x_1, x_2 \in J_1 \cap J_2$

$$J_2 \ni x_1 + x_2 \in J_1$$

$$\triangleleft a \in R, x \in J_1 \cap J_2$$

$$J_2 \ni ax \in J_1$$

□

Определение. $J_1 \leq J_2$, если $J_1 \subset J_2$.

Примечание. Это частичный порядок.

Определение.

- $\{0\}$ — тривиальный идеал
- $J = R$ — несобственный идеал

Определение. $J \in \mathcal{I}(R)$, тогда $x \sim y$, если $x - y \in J \Leftrightarrow x + J = y + J$

Примечание. $J^+ \triangleleft R^+$

Определение. R/J – фактор-кольцо:

$$R/J := \{[x] \mid x \in R\} = \{x + J \mid x \in R\}$$

Теорема 15. R/J – кольцо.

Доказательство. $\triangleleft x + J, y + J \in R/J$

$$x + J + y + J = x + y + J + J = x + y + J$$

$$(x + J)(y + J) = xy + xJ + Jy + JJ = xy + J$$

□

Пример. $R = \mathbb{Z}, J = 5\mathbb{Z}$

$$R/J = \{0 + J, 1 + J, 2 + J, 3 + J, 4 + J\}$$

$$R/J \cong \mathbb{Z}_5$$

Примечание. R/J называют кольцом вычетов $\text{mod } J$.

Определение. Если $x, y \in R, J \in \mathcal{I}(R)$, то:

$$x \equiv y \pmod{J} \stackrel{\text{def}}{\Leftrightarrow} x - y \in J$$

x и y называются сравнимыми $\text{mod } J$.

Примечание. $x \in R, J = x \cdot R \in \mathcal{I}(R)$

Определение. $a_k \in R$, тогда $(a_1 \dots a_n)$ называется идеалом, порожденным элементами $a_1 \dots a_n$:

$$(a_1 \dots a_n) = a_1 R + \dots + a_n R$$

Примечание.

- $\langle \dots \rangle$ – кольцо
- (\dots) – идеал

Пример. $\triangleleft R = \mathbb{Z}$

$$(12, 18) = \{12x + 18y \mid x, y \in \mathbb{Z}\} = 6\mathbb{Z}$$

Определение. $J \in \mathcal{I}(R)$ называется главным идеалом, если:

$$\exists a \in R \quad J = (a) = aR$$

Определение. R называется **кольцом главных идеалов**, если в нём любой идеал — главный.

Определение. $f : R \rightarrow R'$ — гомоморфизм, если:

- $f(x + y) = f(x) + f(y)$
- $f(xy) = f(x)f(y)$
- $f(0) = 0$
- $f(1) = 1$, если $1 \in R$

Примечание. Пунктов 1 и 2 достаточно.

Определение.

$$\ker f := \{x \in R \mid f(x) = 0\}$$

$$\operatorname{Im} f := f(R) = \{y \in R' \mid \exists x \ f(x) = y\}$$

Лемма 32. $\ker f \in \mathcal{I}(R)$

Доказательство. Замкнутость по сложению следует из того что f есть гомоморфизм абелевых групп.

$$\triangleleft a \in R, x \in \ker f$$

$$ax \in \ker f \Leftrightarrow f(ax) = 0$$

$$f(ax) = f(a)f(x) = f(a) \cdot 0 = 0$$

□

Теорема 16. Если $f : R \rightarrow R'$ — гомоморфизм, то $R/\ker f \cong \operatorname{Im} f$.

Доказательство. Построим $\sigma : R/\ker f \rightarrow \operatorname{Im} f \subset R'$.

$$\triangleleft x + \ker f \in R/\ker f$$

$$\sigma(x + \ker f) := f(x)$$

Тогда σ — изоморфизм.

□

Лекция 13

11 декабря

11.1 Делимость в кольце

Пусть R — кольцо.

Определение. Делителями нуля в кольце R называются такие элементы, что $x \cdot y = 0$, при этом $x \neq 0, y \neq 0$.

Примечание. Если в R нет делителей нуля, то R называется **кольцом целостности**.

Пример. \mathbb{Z}, \mathbb{Z}_p — кольца целостности.

Определение. Единицей кольца¹ называется любой элемент $u \in R$, такой что $\exists v : u \cdot v = 1$. $\{u\}$ — группа обратимых элементов кольца, обозначим R^* .

Лемма 33. R — целостное, тогда

$$Rx = Ry \Leftrightarrow \exists u \in R^* : y = ux$$

Доказательство.

“ \Rightarrow ” $\triangleleft y \in Rx \Rightarrow y = bx, \triangleleft x \in Ry \Rightarrow x = ay, y = bay \Rightarrow (1 - ba)y = 0 \Rightarrow$ или $y = 0$, или $1 - ba = 0$.

$$\triangleleft y = 0 \Rightarrow x = 0 \Rightarrow 0 = 1 \cdot 0$$

$$\triangleleft 1 - ba = 0 \Rightarrow ba = 1 \Rightarrow \text{и } a, \text{ и } b \text{ — единицы } R.$$

“ \Leftarrow ”

$$Ry = R(ux) \subseteq Rx = R(u^{-1}y) \subseteq Ry$$

□

¹ С единицей.

Определение (1). Пусть \mathcal{P} — идеал в R и R/\mathcal{P} — целостное кольцо. Тогда \mathcal{P} называется **простым идеалом**.

Определение (2). \mathcal{P} — **простой идеал**, если $x \cdot y \in \mathcal{P} \Rightarrow x \in \mathcal{P}$ или $y \in \mathcal{P}$.

Лемма 34. $1 \Leftrightarrow 2$

Доказательство. $\triangleleft \mathcal{P} : R/\mathcal{P}$ — целостное

“ \Rightarrow ” $\triangleleft [x], [y] \in R/\mathcal{P} \Rightarrow [x] = x + \mathcal{P}, [y] = y + \mathcal{P}$.

$$\begin{aligned} [x][y] = [0] &\Leftrightarrow [x] = [0] \text{ или } [y] = [0] \\ [xy] = xy + \mathcal{P} = \mathcal{P} &\Rightarrow x \in \mathcal{P} \text{ или } y \in \mathcal{P} \end{aligned}$$

“ \Leftarrow ” $\triangleleft x, y \in \mathcal{P} \Rightarrow x \in \mathcal{P}$ или $y \in \mathcal{P}$

$$\triangleleft [x] = x + \mathcal{P}, [y] = y + \mathcal{P}$$

$$[x] \cdot [y] = \underbrace{x \cdot y}_{\in \mathcal{P}} + \mathcal{P} = \mathcal{P} = [0]$$

□

Лемма 35. $\triangleleft \sigma : R \rightarrow R'$ — гомоморфизм колец, $\mathcal{P}' \subset R'$ — простой идеал в R' .

Тогда $\sigma^{-1}(\mathcal{P}')$ — простой идеал в R .

Доказательство. $\mathcal{P} := \sigma^{-1}(\mathcal{P}')$. Докажем от противного: пусть \mathcal{P} — не простой.

$\triangleleft x, y \in R : xy \in \mathcal{P}, x \notin \mathcal{P}, y \notin \mathcal{P}$

$$\sigma(xy) = \underbrace{\sigma(x)}_{\notin \mathcal{P}'} \underbrace{\sigma(y)}_{\notin \mathcal{P}'} \in \mathcal{P}'$$

Противоречие.

□

Определение. **Спектром** кольца называется множество его простых идеалов.

Обозначение. $\text{spec}(R)$

Определение. Идеал \mathcal{M} называется **максимальным** в R , если \mathcal{M} — идеал в R и \mathcal{M} не содержится ни в каком другом идеале.

Примечание. R — целостное, если $\{0\}$ — простой идеал.

Лемма 36. Всякий максимальный идеал — простой.

Доказательство. $\triangleleft \mathcal{M}$ — максимальный идеал.

$$\triangleleft x, y \in R : x \cdot y \in \mathcal{M}, x \notin \mathcal{M}$$

По максимальнойности идеала $Rx + \mathcal{M} = R$, тогда $\exists r \in R, m \in \mathcal{M} : rx + m = 1$

$$\begin{aligned} rx + m &= 1 \\ r \underbrace{xy}_{\substack{(1) \\ \in \mathcal{M}}} + \underbrace{my}_{\substack{(2) \\ \in \mathcal{M}}} &= y \end{aligned}$$

Тогда $y \in \mathcal{M}$. □

Лемма 37. Всякий идеал I кольца R содержится в некотором максимальном идеале \mathcal{M} .

Доказательство. $\triangleleft I_1 \subset I_2 \subset \dots \subset I_m \subset R$

В любой такой цепочке есть максимальный элемент $I = \bigcup_{j=1}^m I_j$ □

Лемма 38.

- $\sigma : R \rightarrow R'$ — сюръективный
- \mathcal{M}' — максимальный идеал в R'

Тогда $\sigma^{-1}(\mathcal{M}') = \mathcal{M}$ — максимальный идеал.

Доказательство. Очевидно. □

Определение. Полем K называется кольцо R , множество ненулевых элементов которого образует мультипликативную абелеву группу.

Лемма 39. R/\mathcal{M} — поле.

Доказательство. $\triangleleft [x] \neq [0] \in R/\mathcal{M}$. Мы хотим показать, что $\exists [x]^{-1} : [x][x]^{-1} = [1]$

$\triangleleft x \in R, x \notin \mathcal{M} \Rightarrow Rx + \mathcal{M} = R \Rightarrow \exists r \in R, m \in \mathcal{M} : rx + m = 1$

$$\begin{aligned} rx + m &= 1 \\ [rx + m] &= [1] \\ [rx] &= [1] \\ [r][x] &= [1] \end{aligned}$$

□

1: по условию $xy \in \mathcal{M}$

2: т.к. $m \in \mathcal{M}$ и \mathcal{M} — идеал

Лемма 40.

- $\mathcal{M} \subset R$
- R/\mathcal{M} — поле

Тогда \mathcal{M} — максимальный.

Доказательство. Самостоятельно.

