Алгоритмы в математике *(теория чисел)*

Михайлов Максим

21 октября 2022 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. $\exists e_L, e_R \in M \Rightarrow e_L = e_R \stackrel{\text{def}}{=} e$

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

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

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

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 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 $\alpha \in \mathbb{R}$

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

Определение.

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

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

$$\begin{aligned}(\alpha * \beta)(x \circ y) &\doteq (\alpha * \beta)(x) \circ (\alpha * \beta)(y) \\ &\doteq \alpha(\beta(x)) \circ \alpha(\beta(y)) = \alpha(\beta(x \circ y))\end{aligned}$$

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

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

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

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

$\lessdot M$, 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. $\triangleleft(M, R)$ — 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, $x, y \in M, \triangleleft(x, y) \in M \times M$.

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

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:

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

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.

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

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.

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

$\square$

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).

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

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

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

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

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

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

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

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

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

□

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

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 $\ker \sigma$ — 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, $g^{-1}Hg \subset H$. Заменим 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 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.

$\triangleleft G/H, H \triangleleft G, \cdot : [x] \cdot [y] = [x \cdot y]$. 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 $\sigma : G \to G/H, g \mapsto [g]$.

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

Свойства.

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

Пример. $H \lhd G \Rightarrow \quad H \xrightarrow{j} G \xrightarrow{\varphi} G/H$, 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 $\operatorname{Im}(0 \to G) = \{G_e\} \Rightarrow \ker \sigma = \{G_e\} \Rightarrow \sigma$ инъективно. Аналогичными рассуждениями χ сюръективно.

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

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

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

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

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

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

Примечание.

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

Тогда:

1. $K \lhd H$.

   $\lessdot \chi : G/K \to G/H, gK \mapsto gH, \ker \chi = \{hK\}_{h \in H}$, 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. $\square$

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.

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

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

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

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

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

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

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

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

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

$$xy = yx$$

Таким образом, $\ker \sigma = Z_G$

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

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

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

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

Пусть $x \in G$.

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

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

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

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

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

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

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

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: $\triangleleft G/H : [g] = gH$, 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 $H = \{mz\}_{m \in \mathbb{Z}}, z \coloneqq \min\{t \in \mathbb{Z} \mid t > 0\}$

Лекция 7

16 октября

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

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

Есть два случая:

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

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

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

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

Утверждение. Все элементы различны, т.е. $\lessdot s, r : a^s = a^r$. 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 $g^d = e$.

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

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

□

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

Тогда $G = \langle g \rangle$.

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

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

   $\lessdot H \subset G$ — подгруппа.

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

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

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

$\lessdot |G/H|$

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.

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

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.

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

   $\triangleleft \varphi : HK \to HK/K$ — 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 силовской p-подгруппе.

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

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

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

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

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

Примечание. $|H| = p^k \Rightarrow \forall \tilde{H} \subset H \;\; |\tilde{H}| \,\vdots\, p$

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

Т.к. H — p-подгруппа, остатки от деления $(H : \tilde{H}_x)$ либо $\vdots\, p$, либо $= 1$. Т.к. $|S_0| \not\vdots\, p$, 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 $O_H(\mathcal{P}') = \mathcal{P}', \forall h \in H \;\; h\mathcal{P}'h^{-1} = \mathcal{P}' \Rightarrow h\mathcal{P}' = \mathcal{P}'h$, а следовательно $H \subset N_{\mathcal{P}'}$.

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

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

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

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 $\mathrm{Obj}(\mathcal{C}) : A, B, C \ldots X, Y$
2. Множество морфизмов $\mathrm{Arr}(\mathcal{C}) : f, g, h, \varphi, \chi, \psi$

   $\lhd A, B \in \mathrm{Obj}(\mathcal{C}), A \xrightarrow{f} B, f \in \mathrm{Mor}(A, B)$
3. $\mathrm{Mor}(B, C) \times \mathrm{Mor}(A, B) = \mathrm{Mor}(A, C)$

Аксиомы категории:

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

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

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

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

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

Лемма 26. $\mathrm{End}(A)$ — моноид

Лемма 27. $\mathrm{Aut}(A)$ — группа

Категории, которые мы будем рассматривать:

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

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

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

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\varphi"] & B \arrow[d, "\psi"] \\ A' \arrow[r, "g"] & B' \end{tikzcd}$$

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

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

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

$$\begin{tikzcd} X \arrow[rr, "\varphi"] \arrow[dr, "f"'] & & X' \arrow[dl, "g"] \\ & A & \end{tikzcd}$$

9.3 Функтор

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

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

со следующими аксиомами:

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

Пример. $\mathcal{C} \coloneqq \mathrm{Grp}, \mathrm{Obj}(\mathcal{C})$ — группы, $\mathrm{Arr}(\mathcal{C})$ — 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 $A \in \mathrm{Obj}(\mathcal{A})$ сопоставляет $F'(A) \in \mathrm{Obj}(\mathcal{B})$.
- Каждому $f \in \mathrm{Mor}(A, B)$[2] сопоставляет $F'(f) \in \mathrm{Mor}(F'(B), F'(A))$

со следующими аксиомами:

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

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

$\lhd \mathcal{A}, A \in \mathrm{Obj}(\mathcal{A}), F_A : \mathcal{A} \to \mathrm{Set}$

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

$$\forall f \in \mathrm{Mor}(X, X')\ \ F_A(f) = \mathrm{Mor}(A, X) \to \mathrm{Mor}(A, X'), \varphi \mapsto f \circ \varphi$$

$$\begin{tikzcd}
X \arrow[rr, "f"] & & X' \\
& A \arrow[ul, "\varphi"] \arrow[ur, "f \circ \varphi"'] &
\end{tikzcd}$$

$F_A^c : \mathcal{A} \to \mathrm{Set}$

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

[1] $A \in \mathrm{Obj}(\mathcal{A}), B \in \mathrm{Obj}(\mathcal{B})$
[2] $A \in \mathrm{Obj}(\mathcal{A}), B \in \mathrm{Obj}(\mathcal{B})$

$$\forall g \in \mathrm{Mor}(Y', Y) \;\; F_A^c(g) : \mathrm{Mor}(Y', A) \to \mathrm{Mor}(Y, A)$$

$$\begin{tikzcd} Y \arrow[dr, "\psi"'] & & Y' \arrow[ll, "g"'] \arrow[dl, "g \circ \psi"] \\ & A & \end{tikzcd}$$

Построенные функторы — **представляющие**[3].

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

Лекция 10

6 ноября

9.4 Произведения и копроизведения

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

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

, такая что если $\varphi : A \to C, \psi : B \to C$, тогда $\exists$ морфизм h, такой что $\varphi = f \circ h, \psi = g \circ h$, т.е. следующая диаграмма[1] коммутирует:

$$\begin{tikzcd} & C \arrow[dl, "\varphi"'] \arrow[d, "h"] \arrow[dr, "\psi"] & \\ A & P \arrow[l, "f"] \arrow[r, "g"'] & B \end{tikzcd}$$

Пример. $\mathcal{A} = \mathrm{Set}$

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

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

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

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

Определение. Копроизведение $A \in \mathrm{Obj}(\mathcal{A})$ и $B \in \mathrm{Obj}(\mathcal{A})$ — 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.

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

, такая что

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

, т.е. следующая диаграмма коммутирует:

$$\begin{tikzcd}
& C & \\
A \arrow[ur, "\varphi"] \arrow[r, "f"'] & P' \arrow[u, "h"] & B \arrow[ul, "\psi"'] \arrow[l, "g"]
\end{tikzcd}$$

Пример. Пусть $\mathcal{A} = \mathrm{Set}, S_1 \in \mathrm{Obj}(\mathcal{A}), S_2 \in \mathrm{Obj}(\mathcal{A})$. 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:

$$\forall C' \in \mathrm{Obj}(\mathcal{A}) : g_i : A_i \to C \;\; \exists h : g_i = h \circ f_i$$

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

$$\forall A \in \mathrm{Obj}(\mathcal{A}) \;\; \exists! \varphi : I \to A$$

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

$$\forall B \in \mathrm{Obj}(\mathcal{A}) \;\; \exists! \varphi : B \to T$$

Примечание. Терминальный и инициальный объект универсальны.

$$\begin{tikzcd}
I \arrow[r, bend left, "\varphi"] & I' \arrow[l, bend left, "\varphi'"]
\end{tikzcd}$$

По определению:

$$\varphi \circ \varphi' : I' \to I'!$$

$$\varphi' \circ \varphi : I \to I!$$

[3] Это дизъюнктное объединение.

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

$$\begin{tikzcd}
 & P \arrow[dddl, bend right, "h'"'] \arrow[dddr, bend left, "h"] & \\
 & A_1 \arrow[u, "g_1"] \arrow[ddl, "f'_1"'] \arrow[ddr, "f_1"] & \\
 & A_2 \arrow[uu, "g_2"] \arrow[dl, "f'_2"] \arrow[dr, "f_2"] & \\
B' & \vdots & B \arrow[ll, bend left=60, "\varphi"] \\
 & A_n \arrow[uuuu, "g_n"] \arrow[ul, "f'_n"] \arrow[ur, "f_n"'] &
\end{tikzcd}$$

$\varphi : B \to B'$ — 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 $\{g_i : A_i \to P\}$ 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. □

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

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

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

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

$g_i(y) = (y)_i$, 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.

$$\begin{tikzcd}
 & & \tilde{G} \arrow[dll, "g_1"'] \arrow[dl, "g_2"] \arrow[d] \arrow[dr, "g_n"] \arrow[drr] \arrow[dd, bend right, "h"'] & & \\
G_1 & G_2 & \dots & G_n & \dots \\
 & & \prod_i G_i \arrow[ull, "f_1"] \arrow[ul, "f_2"'] \arrow[u] \arrow[ur, "f_n"'] \arrow[urr] & &
\end{tikzcd}$$

$\square$

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. $\lessdot \psi : (x, y) \mapsto xy, \psi \in \hom(H \times K, G)$

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. $\square$

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.

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

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

Определение. S — **множество образующих**[1] 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 $f : S \to F, g : S \to G$, где $f(S)$ порождает F и $g(S)$ порождает G.

$$\begin{tikzcd} & F \arrow[dd, "g_*"] \\ S \arrow[ur, "f"] \arrow[dr, "g"'] & \\ & G \end{tikzcd}$$

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

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

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.

$\lhd T$ — 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 $\varphi : S \to T_{\gamma,\varphi}$. $T_{\gamma,\varphi} \in \mathrm{Obj}(\zeta)$, а $T_\gamma \in \mathrm{Grp}$.

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

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

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

[1] Также называется множеством порождающих.

[2] $M_\gamma = \mathrm{Arr}(-, T_\gamma)$

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

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

$$\begin{tikzcd} & F_0 \arrow[dd, "g_*"] \\ S \arrow[ur, "f_0"] \arrow[dr, "g"'] & \\ & G \end{tikzcd}$$

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

Рассмотрим $\overline{G} = G \times \mathbb{Z}$. 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 $\lambda : G \times \mathbb{Z} \to T_\gamma$.

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

$$\psi \coloneqq \lambda \circ h \circ g \in M_\gamma \qquad S \xrightarrow{\ \psi\ } T_{\gamma,\psi}$$

$$\psi_* \coloneqq \operatorname{proj}_G \circ \lambda^{-1} \circ \operatorname{proj}_{\gamma,\psi}$$

$$\begin{tikzcd} F_0 \arrow[r, "\operatorname{proj}_{\gamma,\psi}"] \arrow[d, "\psi_*"] & T_{\gamma,\psi} \arrow[d, "\lambda^{-1}"] \\ G & G \times \mathbb{Z} \arrow[l, "\operatorname{proj}_G"] \end{tikzcd}$$

$$\begin{tikzcd} & F_0 \arrow[d, "\operatorname{proj}_{\gamma,\psi}"] \arrow[ddd, bend left, "\psi_*"] \\ S \arrow[ur, "f_0"] \arrow[ddr, "g"'] & T_{\gamma,\psi} \arrow[d, "\lambda^{-1}"] \\ & G \times \mathbb{Z} \arrow[d, "\operatorname{proj}_G"] \\ & G \end{tikzcd}$$

Рассмотрим $f : S \to F, f(S) = F$. Для единственности g_* мы сужаем его на $g_*\big|_F$. 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 инъектвиное.

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:

$$a \cdot (b + c) = ab + ac$$
$$(a + b) \cdot c = ac + bc$$

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****)*:

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

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:

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

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

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

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

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

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

□

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:

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

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

Доказательство. $\vartriangleleft a \in R$

$$\sum_{k=1}^{n} x_k y_k \in J_1 J_2$$

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

□

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

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

$$J_1 \cap J_2 \coloneqq \{x \mid x \in J_1, x \in J_2\}$$

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

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

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

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

$$J_2 \ni ax \in J_1$$

□

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. $J^+ \lhd R^+$

Определение. ${}^{R}\!/_{J}$ — **фактор–кольцо**:

$$ {}^{R}\!/_{J} \coloneqq \{[x] \mid x \in R\} = \{x + J \mid x \in R\} $$

Теорема 15. ${}^{R}\!/_{J}$ — кольцо.

Доказательство. $\lhd x + J, y + J \in {}^{R}\!/_{J}$

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

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

□

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 $\operatorname{mod} J$.

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

$$ x \equiv y \mod J \overset{\text{def}}{\Leftrightarrow} x - y \in J $$

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

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

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

$$ (a_1 \ldots a_n) = a_1 R + \cdots + a_n R $$

Примечание.

- $\langle \ldots \rangle$ — кольцо
- $(\ldots)$ — идеал

Пример. $\lhd R = \mathbb{Z}$

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

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. $f : R \to R'$ — 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.

$$\ker f \coloneqq \{x \in R \mid f(x) = 0\}$$
$$\operatorname{Im} f \coloneqq f(R) = \{y \in R' \mid \exists x \;\; f(x) = y\}$$

Лемма 32. $\ker f \in \mathcal{I}(R)$

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

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

$$ax \in \ker f \Leftrightarrow f(ax) = 0$$
$$f(ax) = f(a)f(x) = f(a) \cdot 0 = 0$$

□

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

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

$\lhd x + \ker f \in R/_{\ker f}$

$$\sigma(x + \ker f) \coloneqq f(x)$$

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 кольца[1] 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.

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

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

$\lhd 1 - ba = 0 \Rightarrow ba = 1 \Rightarrow$ и a, и b — 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. $\lhd \mathcal{P}$: ${}^{R}\!/\!_{\mathcal{P}}$ — целостное

"$\Rightarrow$" $\lhd [x], [y] \in {}^{R}\!/\!_{\mathcal{P}} \Rightarrow [x] = x + \mathcal{P}, [y] = y + \mathcal{P}$.

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

"$\Leftarrow$" $\lhd x, y \in \mathcal{P} \Rightarrow x \in \mathcal{P}$ или $y \in \mathcal{P}$

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

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

□

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

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

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

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

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

Противоречие. □

Определение. Спектром кольца называется множество его простых идеалов.

Обозначение. $\operatorname{spec}(R)$

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. $\lhd \mathcal{M}$ — максимальный идеал.

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

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

$$rx + m = 1$$
$$r \underbrace{xy}_{\overset{(??)}{\in \mathcal{M}}} + \underbrace{my}_{\overset{(??)}{\in \mathcal{M}}} = y$$

Тогда $y \in \mathcal{M}$. □

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

Доказательство. $\lhd I_1 \subset I_2 \subset \cdots \subset I_m \subset R$

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

Лемма 38.

- $\sigma : R \to R'$ — 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. $\lhd [x] \neq [0] \in {}^{R}\!/\!_{\mathcal{M}}$. Мы хотим показать, что $\exists [x]^{-1} : [x][x]^{-1} = [1]$

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

$$rx + m = 1$$
$$[rx + m] = [1]$$
$$[rx] = [1]$$
$$[r][x] = [1]$$

□

??: по условию $xy \in \mathcal{M}$
??: 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. $\square$