Содержание

1 Универсальные алгебры, сигнатуры, термы, изоморфизмы

Определение 1.1 (Сигнатура)**. Сигнатура** - множество имён операций с указанием их местности.

$$(f^{(2)}, g^{(3)}, h^{(0)}), (+^{(2)}, \cdot^{(3)})$$

$h^{(0)}$ - символ константы, V - имена переменных

Определение 1.2 (Терм)**. Терм** - выражение, составленное из символов сигнатуры и переменных

1. $x \in V$, x - терм
2. c - символ константы, c - терм
3. если $t_1, ..., t_n$ - термы и f - символ n-местной операции, то $f(t_1, ..., t_n)$ - терм

Пример 1.3. *Примеры термов:* $-(x), -(0), +(x, y), 2 + 3 + a$

Определение 1.4 (Замкнутый терм)**. Замкнутый терм** - терм, не содержащий переменных

Определение 1.5. Универсальная алгебра - пусть Σ - сигнатура, тогда *универсальная алгебра* сигнатуры Σ - это пара вида (A, I), где A - произвольное непустое множество, а I - некоторое отображение, которое для всякого $p^{(m)} \in \Sigma$, $I(p^{(m)})$ - n-местной операции на множестве

Пример 1.6 (Пример универсальной алгебры)**.** *Пусть*

$$\Sigma = (+^{(2)}, \cdot^{(2)}, -^{(1)}, 0^{(0)}, 1^{(0)})$$

тогда

$$\begin{aligned} R = (\mathbb{R}, I) : & I(+) - \textit{сложение} \\ & I(\cdot) - \textit{умножение} \\ & I(-) - \textit{вычитание} \\ & I(0) - 0 \\ & I(1) - 1 \end{aligned}$$

Определение 1.7 (Носитель алгебры)**.** $\mathbb{R}$ называется **основным множеством** или носителем алгебры, а I - интерпретацией или интерпретирующей функцией

Определение 1.8 (Состояние)**. Состояние** - функция, приписывающая переменной некоторый элемент носителя $\sigma : V \to A$

Пример 1.9. *Пример состояний:* $\sigma = \{(x, 3), (y, -8)\}, \sigma(x) = 3$

Определение 1.10 (Значение терма на состоянии)**.** Значение терма t на состоянии σ - значение того выражения, в котором переменные заменены их значениями

1. t - переменная, $\sigma(t)$ - по определению состояния
2. t - символ константы, $I(t) = \sigma(t_1) = v_1$
3. если $t_1, ..., t_n$ - термы и $\sigma(t_1) = v_1, ..., \sigma(t_n) = v_n$, то $\sigma(t) = I(f)(v_1, ..., v_n)$

Определение 1.11 (Изоморфизм)**. Изоморфизм** - Пусть $\Sigma = \{f_i^{(n_i)} : i \in I\}$ - сигнатура, $\mathcal{A} = (A, I)$, $\mathcal{B} = (B, J)$ - универсальные алгебры сигнатуры Σ, тогда изоморфизм между $\mathcal{A}$ и $\mathcal{B}$ - это $h : \mathcal{A} \leftrightarrow \mathcal{B}$ - биективная функция, которая удовлетворяет следующему условию:

$$h(I(f_i)(a_1, ..., a_n)) = J(f_i)(h(a_1), ..., h(a_n))$$

для любых $a_1, ..., a_n$ и $f_i \in \Sigma$

Пример 1.12 (Пример изоморфизма)**.** *пусть* $\Sigma = (f^{(2)})$, $\mathcal{A} = (\mathbb{R}, +)$, $\mathcal{B} = (\mathbb{R}, \cdot)$

Надо доказать:

$$h(a_1 + a_2) = h(a_1) \cdot h(a_2)$$

$a_1, a_2 \in \mathbb{R}$

Пусть $h(x) = e^x$, *тогда*

$$h(a_1 + a_2) = e^{a_1 + a_2} = e^{a_1} \cdot e^{a_2} = h(a_1) \cdot h(a_2) \blacksquare$$

Теорема 1.13. h - *изоморфизм между* A *и* B, *то* h^{-1} - *изоморфизм между* B *и* A

Доказательство. пусть $b_1, ..., b_{n_i} \in B$, тогда надо доказать

$$h^{-1}(J(f_i)(b_1, ..., b_{n_i})) = I(f_i)(h^{-1}(b_1), ..., h^{-1}(b_{n_i}))$$

Так как $b_1 = h(a_1), ..., b_{n_i} = h(a_{n_i})$,

$$\begin{aligned} I(f_i)(h^{-1}(b_1), ..., h^{-1}(b_{n_i})) &= I(f_i)(h^{-1}(h(a_1)), ..., h^{-1}(h(a_{n_i}))) \\ &= I(f_i)(a_1, ..., a_{n_i}) \end{aligned}$$

$$\begin{aligned} h^{-1}(J(f_i)(b_1, ..., b_{n_i})) &= h^{-1}(J(f_i)(h(a_1), ..., h(a_{n_i}))) \\ &= h^{-1}(h(I(f_i)(a_1, ..., a_{n_1}))) \\ &= I(f_i)(a_1, ..., a_{n_1}) \end{aligned}$$

Из этих двух равенств следует то, что надо доказать □

Определение 1.14. Системы, между которыми существует изоморфизм называют **изоморфными**

$$(\mathbf{R}, +) \simeq (\mathbf{R}^+, \cdot)$$

операции в изоморфных системах обладают одними и теми же свойствами

Определение 1.15 (Терм, содержащий переменные)**.** Пусть t - терм, $x_1, ..., x_n$ - переменные, $t(x_1, ..., x_n)$ - терм t не содержит других переменных кроме $x_1, ..., x_n$

Определение 1.16. Пусть $\mathcal{A}$ - алгебра, $a_1, ..., a_n$ - элементы алгебры $\mathcal{A}$, тогда

$$t(a_1, ..., a_n) = \sigma(t), \sigma(x_1) = a_1, ..., \sigma(x_n) = a_n$$

Пример: В алгебре $(\mathbf{R}, +)$:

$$t(x, y) = x + y \quad t(4, 8) = 4 + 8 = 12$$

Теорема 1.17. *h - изоморфизм между $\mathcal{A} = (A, I)$ и $\mathcal{B} = (B, J)$, то для любого терма $t(x_1, ..., x_n)$ и любых $a_1, ..., a_n$ выполняется*

$$h(t^{\mathcal{A}}(a_1, ..., a_n)) = t^{\mathcal{B}}(h(a_1), ..., h(a_n))$$

Доказательство. Индукция по построению терма t

1. $t = x$

$$t^{\mathcal{A}}(a) = a = t^{\mathcal{B}}(a) \Rightarrow h(t^{\mathcal{A}}(a)) = h(a),\ t^{\mathcal{B}}(h(a)) = h(a)$$

2. $t = c$

$$\sigma(c) = I(c) = J(c) \Rightarrow t^{\mathcal{A}} = I(c), t^{\mathcal{B}} = J(c) \Rightarrow h(I(c)) = J(c)$$

по определению гомоморфизма

3. $t = f(t_1, ..., t_k)$

$$\begin{aligned} h(t^{\mathcal{A}}(a_1, ..., a_n)) = \\ h(I(f)(t_1^{\mathcal{A}}(a_1, ..., a_n), ..., t_k^{\mathcal{A}}(a_1, ..., a_n))) = \\ J(f)(h(t_1^{\mathcal{A}}(a_1, ..., a_n)), ..., h(t_k^{\mathcal{A}}(a_1, ..., a_n))) = \\ J(f)(t_1^{\mathcal{B}}(h(a_1), ..., h(a_n)), ..., t_k^{\mathcal{B}}(h(a_1), ..., h(a_n)) = \\ t^{\mathcal{B}}(h(a_1), ..., h(a_n)) \end{aligned}$$

□

Пример 1.18. *Доказать что* $\mathcal{A} = (\mathbb{R}; \cdot) \ncong \mathcal{B} = (\mathbb{R}^+; \cdot)$

Доказательство. Предположим что существует изоморфизм $h : \mathcal{A} \to \mathcal{B}$, тогда

$h(0) = x, x \in \mathbb{R}^+$

$$x = h(0) = h(0 \cdot 0) = h(0) \cdot h(0) = x^2$$

$$x = x^2 \Rightarrow x = 1$$

$h(1) = y, y \in \mathbb{R}^+$

$$y = h(1) = h(1 \cdot 1) = h(1) \cdot h(1) = y^2$$

$$y = y^2 \Rightarrow y = 1$$

$h(0) = 1 = h(1)$ - противоречие (h не биективна). Утверждение не верно. □

Пример 1.19. *Доказать что* $\mathcal{A} = (\mathbb{R}; +) \ncong \mathcal{B} = (\mathbb{R}; \cdot)$

Доказательство. Предположим что существует изоморфизм $h : \mathcal{B} \to \mathcal{A}$, тогда

$h(0) = x, h(1) = y; x, y \in \mathbb{R}$

$$x = h(0) = h(0 \cdot 0) = h(0) + h(0) = 2x \Rightarrow x = 2x = 0$$

$$y = h(1) = h(1 \cdot 1) = h(1) + h(1) = 2y \Rightarrow y = 2y = 0$$

Противоречие (h должно быть биекцией) □

1.13

Пример 1.20. *Доказать что* $\mathcal{A} = (\mathbb{R}; \cdot) \cong \mathcal{B} = (\mathbb{C}; \cdot)$

Доказательство. Предположим что существует изоморфизм $h : \mathcal{B} \to \mathcal{A}$, тогда

$h(x) = -1; x \in \mathbb{C}, -1 \in \mathbb{R}$

□

Пример 1.21. *Доказать что* $\mathcal{A} = (\mathbb{Z}; \min^{(2)}) \ncong \mathcal{B} = (\mathbb{Z}; \max^{(2)})$

Доказательство. □

Пример 1.22. *Доказать что* $\mathcal{A} = (\omega; +) \ncong \mathcal{B} = (\omega^{+}; \cdot)$

Доказательство. □

Пример 1.23. *Доказать что* $\mathcal{A} = (\mathbb{Q}; +) \ncong \mathcal{B} = (\mathbb{Q}^{+}; \cdot)$

Доказательство. □

Пример 1.24. *Доказать что* $\mathcal{A} = (\mathbb{Z}; \cdot) \ncong \mathcal{B} = (\mathbb{G}; \cdot)$

Доказательство. □

2 Подалгебры, порождающие элементы, вложения

Определение 2.1 (Подалгебра)**.** Подалгебра - алгебра $\mathcal{B} = (B, J)$ является подалдгеброй $\mathcal{A} = (A, I)$, если $B \subseteq A$ и $J(f)$ - ограничение $I(f)$ на B для всякого f

Определение 2.2 (Ограничение операции)**.** Ограничение операции - n-местная операция g на B является ограничением операции f множеством B если

$$g(b_1, ..., b_n) = f(b_1, ..., b_n)$$

для любых $b_1, ..., b_n$ из B

Пример 2.3 (Пример ограничения операции)**.**

Пример 2.4 (Пример подалгебры)**.** *Пример подалгебры:*

$$(\mathbb{C}, +, \cdot) \supseteq (\mathbb{R}, +, \cdot) \supseteq (\mathbb{Q}, +, \cdot)$$

Доказательство. □

Следствие 2.5. *Отношение "является подалгеброй"транзитивно*

$$A \subseteq B, B \subseteq C \Rightarrow A \subseteq C$$

Доказательство. □

Теорема 2.6. *Если $\mathcal{A} = (A, I)$ - алгебра, то B $(B \subseteq A; B \neq \emptyset)$ является носителем некоторой подалгебры тогда и только тогда, когда B замкнута относительно сигнатурной операции в алгебре $\mathcal{A}$*

Доказательство. 1. $\Rightarrow$

B - носитель некоторой подалгебры $\mathcal{B} = (B, J)$ и $B \subseteq A$, тогда

$$f^{\mathcal{A}}(b_1, ..., b_n) = f^{\mathcal{B}}(b_1, ..., b_n) \in B$$

B замкнута относительно сигнатурной операции в алгебре $\mathcal{A}$

2. $\Leftarrow$ B замкнута относительно сигнатурной операции в алгебре $\mathcal{A}$, тогда

$J(f)$ - функция на B

$J(f)(b_1, ..., b_n) = f^{\mathcal{A}}(b_1, ..., b_n) \in B$

$J(f)$ - ограниение $f^{\mathcal{A}}$ на B

следовательно $\mathcal{B} = (B, J)$ - подалгебра и B - её носитель

□

Пример 2.7 (Пример на 2.6)**.**

Теорема 2.8. *Пусть $\mathcal{A} = (A, I)$ - алгебра, $\mathcal{B}_k$ - подалгебры, такие что $\bigcap\limits_k \mathcal{B}_k \neq \emptyset$, тогда $\bigcap\limits_k \mathcal{B}_k$ - носитель подалгебры*

Доказательство. Пусть $f^{(n)} \in \Sigma$, $b_1, ..., b_n \in \bigcap\limits_k \mathcal{B}_k$, тогда

$\Rightarrow$ по определению пересечения	$b_1, ..., b_n \in \mathcal{B}$	для всех k
$\Rightarrow$ по 2.6	$f^{\mathcal{A}}(b_1, ..., b_n) \in \mathcal{B}$	для всех k
$\Rightarrow$ по определению пересечения	$f^{\mathcal{A}}(b_1, ..., b_n) \in \bigcap\limits_k \mathcal{B}_k$	

□

Определение 2.9 (Порождённая подалгебра)**.** Пусть $\mathcal{A} = (A, I)$, $x \subseteq A$, $X \neq \emptyset$, $\mathcal{B}_k$ - всевозможные подалгебры, включающие X, тогда $\bigcap \mathcal{B}_k$ - подалгебра, порождённвя X.

Теорема 2.10. *$\mathcal{A}$ - алгебра, $X \subseteq A$, $X \neq \emptyset$, $\mathcal{B}$ - подалгебра, порождённвя X тогда и только тогда, когда $\mathcal{B}$ состоит из всевозможных $t^{\mathcal{A}}(x_1, ..., x_n)$ для $x_1, ..., x_n \in X$*

Доказательство. Достаточность($\Leftarrow$). Пусть $\mathcal{B}$ состоит из всевозможных $t^{\mathcal{A}}(x_1, ..., x_n)$ для $x_1, ..., x_n \in X$. Пусть $B_k \in \mathcal{A}$ - подалгебры такие что $X \subseteq B_k$, тогда

$$\begin{aligned} x_1, ..., x_n &\in B_k \\ t^{\mathcal{A}}(x_1, ..., x_n) &\in B_k \\ t^{\mathcal{A}}(x_1, ..., x_n) &\in \bigcap_X B_k \\ t^{\mathcal{A}}(x_1, ..., x_n) &\in \mathcal{B} \end{aligned}$$

Необходимость($\Rightarrow$). Предположим, что найдётся $b \in \mathcal{B}$, что $b \neq t^{\mathcal{A}}(x_1, ..., x_n)$ для любых t и $x_1, ..., x_n \in X$, Пусть $C = \{t^{\mathcal{A}}(x_1, ..., x_n) : t - \text{терм}, x_1, ..., x_n \in X\}$, следовательно $b \notin C$, $x_i \in C$ и $X \subseteq C$.

C является подалгеброй: пусть $c_1, ..., c_m \in C$ и

$$c_1 = t_1^{\mathcal{A}}(x_1, ..., x_n) \qquad \vdots c_m = t_m^{\mathcal{A}}(x_1, ..., x_n)$$

$$f^{\mathcal{A}}(c_1, ..., c_m) = f^{\mathcal{A}}(t_1^{\mathcal{A}}(x_1, ..., x_n), ..., t_m^{\mathcal{A}}(x_1, ..., x_n))$$

По определению терма $f^{\mathcal{A}}(t_1^{\mathcal{A}}(x_1, ..., x_n), ..., t_m^{\mathcal{A}}(x_1, ..., x_n))$ тоже является термом, содержащий переменные $x_1, ..., x_n$, следовательно C замкнуто по сигнатурной операции A и по 2.6 является подалгеброй.

$C = \mathcal{B}_k$ ждя некоторого k, $\mathcal{B} = \bigcap_k \mathcal{B}_k$. Так как $b \notin C$, то $b \notin \mathcal{B}$, что является противоречием. □

Определение 2.11 (Разнозначное отображение)**.** f - разнозначное, если $f(x) \neq f(y)$ при $x \neq y$

Определение 2.12 (Вложение)**.** $h : \mathcal{A} \to \mathcal{B}$ - вложение $\mathcal{A}$ в $\mathcal{B}$, если h - разнозначное отображение и

$$h(f^{\mathcal{A}}(a_1, ..., a_n)) = f^{\mathcal{B}}(h(a_1), ..., h(a_n))$$

говорят "$\mathcal{A}$ вкладывается в $\mathcal{B}$"

Теорема 2.13. $h : \mathcal{A} \to \mathcal{B}$ - *вложение* $\mathcal{A}$ *в* $\mathcal{B}$, *тогда*

1. *образ* h - $\mathcal{C}$, *подалгебра в* $\mathcal{B}$
2. $h : \mathcal{A} \simeq \mathcal{C}$

Доказательство. 1. Пусть $c_1, ..., c_n \in \operatorname{rng} h$, тогда $c_1 = h(a_1), ..., c_n = h(a_n)$ и

$$h(f^{\mathcal{A}}(a_1, ..., a_n)) = f^{\mathcal{B}}(h(a_1), ..., h(a_n)) = f^{\mathcal{B}}(c_1, ..., c_n) \in \operatorname{rng} h$$

Элементы образа h замкнуты относительно сигнатурных операций $\mathcal{B}$

2. $\mathcal{C} = \operatorname{rng} h$, $h : A \leftrightarrow C$, $\Rightarrow h$ - изоморфизм

□

3 Гомоморфизмы, гомоморфные образы, конгруэнтности, фактор-алгебры

Определение 3.1 (Гомоморфизм)**.** Отображение $f\colon G_1 \to G_2$ называется гомоморфизмом групп $(G_1, *)$, $(G_2, \times)$, если оно одну групповую операцию переводит в другую: $f(a * b) = f(a) \times f(b)$, $a, b \in G_1$.

Следствие 3.2. *Изоморфизм и вложение - частный случай изоморфизма*

Определение 3.3 (Единичаня алгебра)**.** Единичная алгебра - алгебра, содержащая всего один элемент. Σ - сигнатура, e - единственный элемент, $f^{(n)}(e, ..., e) = e$

Пример 3.4 (Пример единичной алгебры)**.** $(\{0\}; +, \cdot)$, $(\{1\}; \cdot)$

Следствие 3.5. *Все единичные алгебры одной сигнатуры изоморфны между собой*

Доказательство. Пусть $\varepsilon_1 = (\{e_1\}; I)$, $\varepsilon_2 = (\{e_2\}; J)$, тогда

$$h(f^{\varepsilon_1}(e_1, ..., e_1)) = h(e_1) = e_2$$

$$f^{\varepsilon_2}(h(e_1), ..., h(e_1)) = f^{\varepsilon_2}(e_2, ..., e_2) = e_2$$

следовательно

$$h(f^{\varepsilon_1}(e_1, ..., e_1)) = f^{\varepsilon_2}(h(e_1), ..., h(e_1))$$

□

Теорема 3.6. *Из любой алгебры существует изоморфизм в единичную алгебру и только один*

Доказательство. Пусть $\mathcal{A} = (A, I)$, $\varepsilon = (\{e\}, J)$ и $h : \mathcal{A} \to \varepsilon$ определено так: $h(a) = e$, для всех $a \in A$. Тогда

$$h(f^{\mathcal{A}}(a_1, ..., a_n)) = e$$

$$f^{\varepsilon}(h(a_1), ..., h(a_n)) = f^{\varepsilon}(e, ..., e) = e$$

следовательно

$$h(f^{\mathcal{A}}(a_1, ..., a_n)) = f^{\varepsilon}(h(a_1), ..., h(a_n))$$

□

Теорема 3.7. *Пусть $h : \mathcal{A} \to \mathcal{B}$ - гомоморфизм, $t(x_1, ..., x_n)$ - терм, $a_1, ..., a_n \in \mathcal{A}$, тогда $h(t^{\mathcal{A}}(a_1, ..., a_n)) = t^{\mathcal{B}}(h(a_1), ..., h(a_n))$*

Доказательство. Так же как для изоморфизма □

Теорема 3.8. *Пусть $h : \mathcal{A} \to \mathcal{B}$ - гомоморфизм, тогда образ множества A при отображении h образует подалгебру в $\mathcal{B}$*

Доказательство. Так же как для вложения □

Определение 3.9 (Эпиморфизм)**.** сюръективный гомоморфизм

Пример 3.10 (Пример на Эпиморфизм)**.**

Определение 3.11 (Эндоморфизм)**.** гомоморфизм в само множество

Пример 3.12 (Пример на Эндоморфизм)**.**

Определение 3.13 (Автоморфизм)**.** взаимно однозначный гомоморфизм в само множество

Пример 3.14 (Пример на Автоморфизм)**.**

Определение 3.15 (Отношение эквивалентности)**.** пока нет

Определение 3.16 (Класс эквивалентности)**.** пока нет

Теорема 3.17. *Любое отношение эквивалентности получается из функции*

Доказательство. Пусть $\equiv$ - отношение эквивалентности на $A \neq \emptyset$. $B = A| \equiv$ - множество классов эквивалентности. Для $a \in A$, $h(a) = \{b \in A : a \equiv b\}$. Пусть $R(a,b) \Leftrightarrow h(a) = h(b)$, тогда

$$R(a,b) \Leftrightarrow h(a) = h(b) \Leftrightarrow \{c \in A : a \equiv c\} = \{c \in A : b \equiv c\}$$

Из этого следует

$$b \in \{c \in A : a \equiv c\} \Rightarrow b \equiv a$$

Следовательно

$$a \equiv b \Rightarrow h(a) = h(b) \Rightarrow R(a,b)$$

Любое отношение эквивалентности можно получить таким образом $\square$

Теорема 3.18. *$h : A \to B$ - гомоморфизм, тогда $x \equiv y \Leftrightarrow h(x) = h(y)$ - отношение эквивалентности.*

Доказательство. Пусть $f^{(n)}$ - сигнаутрная операция, $x_1, ..., x_n, y_1, ..., y_n \in A$ и $x_1 \equiv y_1, ..., x_n \equiv y_n$, тогда

$$h(f^A(x_1, ..., x_n)) = f^B(h(x_1), ..., h(x_n))$$

$$h(f^A(y_1, ..., y_n)) = f^B(h(y_1), ..., h(y_n))$$

Так как $x_i \equiv y_i \Leftrightarrow h(x_i) = h(y_i)$, то

$$h(f^A(x_1, ..., x_n)) = h(f^A(y_1, ..., y_n)) \Leftrightarrow f^A(x_1, ..., x_n) \equiv f^A(y_1, ..., y_n)$$

$\square$

Определение 3.19 (Конгруэнтность)**.** $\mathcal{A}$ - алгебра с сигнатурой Σ, Отношение $\equiv$ - конгруэнтность в $\mathcal{A}$, если

1. $\equiv$ - эквивалентность
2. если $x_1, ..., x_n, y_1, ..., y_n \in \mathcal{A}$, $f^{(n)} \in \Sigma$, $x_1 \equiv y_1, ..., x_n \equiv y_n$, то

$$f^A(x_1, ..., x_n) \equiv f^A(y_1, ..., y_n)$$

Следствие 3.20. *Пусть $h : A \to B$ - гомоморфизм, то $x \equiv y \Leftrightarrow h(a) = h(b)$ - отношение конгруэнтности на A*

Определение 3.21 (Фактор-алгебра)**.** Пусть $\mathcal{A}$ - алгебра с сигнатурой Σ, Отношение $\equiv$ - конгруэнтность в $\mathcal{A}$, тогда фактор-алгебра - $B = \mathcal{A}/_{\equiv}$ - множество классов эквивалентности по отношению к конгруэнтности

Теорема 3.22. *Для каждого отношения конгруэнтности существует порождающий его гомоморфизм*

Доказательство. Пусть $\mathcal{A}$ - алгебра с сигнатурой Σ, Отношение $\equiv$ - конгруэнтность в $\mathcal{A}$, $\mathcal{B} = \mathcal{A}/_{\equiv}$ - множество классов эквивалентности.

$f^{\mathcal{B}}(b_1, ..., b_n) = b \Leftrightarrow f^{\mathcal{A}}(a_1, ..., a_n) = a$ для некоторых $a_1 \in b_1, ..., a_n \in b_n, a \in b$. Докажем что от выбора $a_1, ..., a_n$ значение $f^{\mathcal{B}}(b_1, ..., b_n)$ не зависит.

Предположим что зависит, выберем значения $a'_1, ..., a'_n$, такие что $a'_1 \in b_1, ..., a'_n \in b_n$, тогда $f^{\mathcal{A}}(a'_1, ..., a'_n) = a' \notin b$, но так как $a_1 \equiv a'_1, ..., a_n \equiv a'_n$ и $\equiv$ - конгруэнтность, то $a \equiv a'$, но при этом $a' \notin b$. Противоречие.

Возьмём $h : \mathcal{A} \to \mathcal{B}$, $h(a)$ =класс эквивалентности a

$$h(a) = h(f^{\mathcal{A}}(a_1, ..., a_n)) = f^{\mathcal{B}}(h(a_1), ..., h(a_n)) = h(a)$$

$f^{\mathcal{A}}(a_1, ..., a_n) = a$, $h(a) = b$, к чему всё это □

Теорема 3.23. *Пусть $h : \mathcal{A} \to \mathcal{B}$ - эпиморфизм, $\equiv$ - отношение конгруэнтности для h, тогда $\mathcal{A}/_{\equiv} \simeq \mathcal{B}$*

Доказательство. не уверен что вообще нужно □

Следствие 3.24. *$h : \mathcal{A} \to \mathcal{B}_1$ и $h : \mathcal{A} \to \mathcal{B}_2$ - эпиморфзмы, если $\equiv_1$ и $\equiv_2$ совпадают, то $\mathcal{B}_1 \simeq \mathcal{B}_2$*

Доказательство. не уверен что вообще нужно □

4 Декартовы произведения, тождества, многообразия

Определение 4.1 (Декартово произведение)**.** Пусть $\mathcal{A} = (A, I)$, $\mathcal{B} = (B, J)$ - алгебры одной сигнатуры Σ, декартово произведение $\mathcal{C} = \mathcal{A} \times \mathcal{B}$ - это

$$\mathcal{C} = (C, K), C = A \times B = \{(a, b) : a \in A, b \in B\}$$

где определены операции $f^{(n)} \in \Sigma$

$$f^{\mathcal{C}}((a_1, b_1), ..., (a_n, b_n)) = (f^{\mathcal{A}}(a_1, ..., a_n), f^{\mathcal{B}}(b_1, ..., b_n))$$

Пример 4.2 (Пример декартова произведения)**.**

Теорема 4.3. *Пусть $\mathcal{C} = \mathcal{A} \times \mathcal{B}$, $h_1(a, b) = a$, $h_2(a, b) = b$, тогда $h_1 : C \to A$ и $h_2 : C \to B$ - гомоморфизмы.*

Доказательство.

$$\begin{aligned} h_1(f^{\varepsilon}((a_1,b_1),...,(a_n,b_n))) &= h_1(f^{\mathcal{A}}(a_1,...,a_n), f^{\mathcal{B}}(b_1,...,b_n)) \\ &= f^{\mathcal{A}}(a_1,...,a_n) \\ &= f^{\mathcal{A}}(h_1(a_1,b_1),...,h_1(a_n,b_n)) \end{aligned}$$

□

Определение 4.4 (Тождество)**.** Пусть Σ - сигнатура, t_1, t_2 - термы в Σ, тогда тождество - формула вида $t_1 = t_2$.

В $\mathcal{A}$ выполнено $t_1 = t_2$, если оно выполнено для любых значений переменных.

Определение 4.5 (Многообразие)**.** Пусть T - множество тождеств, многообразие задаваемое(определяемое) T - это класс всех алгебр, в котором выполнены все тождества из T.

$\mathcal{A} \in M \Leftrightarrow$ в $\mathcal{A}$ выполнены $t_1 = t_2 \in T$

Пример 4.6 (Пример многообразия)**.**

Лемма 4.7. *Пусть $\mathcal{C} = \mathcal{A} \times \mathcal{B}$. Тогда для любого терма $t(x_1,...,x_n)$:*

$$t^{\mathcal{C}}((a_1,b_1),...,(a_n,b_n)) = (t^{\mathcal{A}}(a_1,...,a_n), t^{\mathcal{B}}(b_1,...,b_n))$$

Доказательство. Индукция по построению t

1. $t = x$, $t^{\mathcal{C}}((a_1,b_1),...,(a_n,b_n)) = (a_i,b_i)$, $(a_i,b_i) = (t^{\mathcal{A}}(a_1,...,a_n), t^{\mathcal{B}}(b_1,...,b_n))$
2. $t = d$ - константа, $t^{\mathcal{C}}((a_1,b_1),...,(a_n,b_n)) = (d^{\mathcal{A}}, d^{\mathcal{B}})$, $(t^{\mathcal{A}}(a_1,...,a_n), t^{\mathcal{B}}(b_1,...,b_n)) = (d^{\mathcal{A}}, d^{\mathcal{B}})$
3. пусть $s_1,...,s_k$ - термы, $t = f(s_1,...,s_k) = (s_i^{\mathcal{A}}(a_1,...,a_n), s_i^{\mathcal{B}}(b_1,...,b_n))$, тогда

$$\begin{aligned} &t^{\mathcal{C}}((a_1,b_1),...,(a_n,b_n)) = \\ &\quad f^{\mathcal{C}}(s_1^{\mathcal{C}}((a_1,b_1),...,(a_n,b_n)),...,s_n^{\mathcal{C}}((a_1,b_1),...,(a_n,b_n))) = \\ &f^{\mathcal{C}}((s_i^{\mathcal{A}}(a_1,...,a_n), s_i^{\mathcal{B}}(b_1,...,b_n)),...,(s_k^{\mathcal{A}}(a_1,...,a_n), s_k^{\mathcal{B}}(b_1,...,b_n))) = \\ &(f^{\mathcal{A}}(s_i^{\mathcal{A}}(a_1,...,a_n),...,s_k^{\mathcal{A}}(a_1,...,a_n)), f^{\mathcal{B}}(s_i^{\mathcal{B}}(b_1,...,b_n),...,s_k^{\mathcal{B}}(b_1,...,b_n))) = \\ &\qquad (t^{\mathcal{A}}(a_1,...,a_n), t^{\mathcal{B}}(b_1,...,b_n)) \end{aligned}$$

□

Теорема 4.8 (Теорема Бишопа)**.** *Пусть M - многообразие, $\mathcal{A}, \mathcal{B} \in M$, тогда*

1. *$\mathcal{C} \subseteq \mathcal{A} \Rightarrow \mathcal{C} \in M$ (замкнутость относительно подалгебры)*
2. *$\mathcal{C}$ - гомоморфный образ $\mathcal{A} \Rightarrow \mathcal{C} \in M$ (замкнутость относительно гомоморфизма)*
3. *$\mathcal{C} = \mathcal{A} \times \mathcal{B} \Rightarrow \mathcal{C} \in M$ (замкнутость относительно декартовых произведений)*

Доказательство. Пусть $T = \{t_1(x_1, ..., x_n) = t_2(x_1, ..., x_n)\}$ - множество тождеств

1. пусть $c_1, ..., c_n \in \mathcal{C}$ и $\mathcal{C} \subseteq \mathcal{A}$, тогда $c_1, ..., c_n \in \mathcal{A}$ и

$$\begin{aligned} t_1^{\mathcal{C}}(c_1, ..., c_n) &= t_1^{\mathcal{A}}(c_1, ..., c_n) \\ &= t_2^{\mathcal{A}}(c_1, ..., c_n) \\ &= t_2^{\mathcal{C}}(c_1, ..., c_n) \end{aligned}$$

   это и значит что $\mathcal{C} \in M$

2. пусть $c_1, ..., c_n \in \mathcal{C}$ и $h : \mathcal{A} \to \mathcal{C}$, тогда $c_1 = h(a_1), ..., c_n = h(a_n)$, $a_1, ..., a_n \in \mathcal{A}$ и

$$\begin{aligned} t_1^{\mathcal{C}}(c_1, ..., c_n) &= t_1^{\mathcal{C}}(h(a_1), ..., h(a_n)) \\ &= h(t_1^{\mathcal{A}}(a_1, ..., a_n)) \\ &= h(t_2^{\mathcal{A}}(a_1, ..., a_n)) \\ &= t_2^{\mathcal{C}}(h(a_1), ..., h(a_n)) \\ &= t_2^{\mathcal{C}}(c_1, ..., c_n) \end{aligned}$$

3. пусть $c_1, ..., c_n \in \mathcal{C}$ и $\mathcal{C} = \mathcal{A} \times \mathcal{B}$, тогда $(a_1, b_1), ..., (a_n, b_n) \in \mathcal{C}$ и

$$\begin{aligned} t_1^{\mathcal{C}}((a_1, b_1), ..., (a_n, b_n)) &= (t_1^{\mathcal{A}}(a_1, ..., a_n), t_1^{\mathcal{B}}(b_1, ..., b_n)) \\ &= (t_2^{\mathcal{A}}(a_1, ..., a_n), t_2^{\mathcal{B}}(b_1, ..., b_n)) \\ &= t_2^{\mathcal{C}}((a_1, b_1), ..., (a_n, b_n)) \end{aligned}$$

□

5 Полугруппы и моноиды. Идемпотенты, сократимые и обратимые элементы.

Определение 5.1 (Полугруппа)**.** Полугруппа - многообразие заданное множеством

$$(x * y) * z = x * (y * z)$$

Пример 5.2 (Примеры полугрупп)**.**

Теорема 5.3. *Значение терма не зависит от расстановки скобок (Ассоциативный закон)*

$$t = t_1 * t_2 = (a_1 a_2 ... a_m)(a_{m+1} ... a_n) = a_1 a_2 ... a_n$$

Доказательство. Индукция по длине t

Базис: $n = 1$, нет скобок

Шаг: для $n - 1$ верно, тогда

1. $m = n - 1$

$$t = t_1 * a_n = (a_1 a_2 ... a_m) * a_n = a_1 a_2 ... a_n$$

2. $1 \leq m \leq n - 1$

$$t = t_1 * t_2 = (a_1 a_2 ... a_m)(a_{m+1} ... a_n) = (a_1 a_2 ... a_m)(a_{m+1} ... a_{n-1}) a_n$$

Так как длина $(a_1 a_2 ... a_m)(a_{m+1} ... a_{n-1})$ равна $n - 1$ то выполняется индукционное предположение и

$$(a_1 a_2 ... a_m)(a_{m+1} ... a_{n-1}) = (a_1 a_2 ... a_{n-1})$$

соотвественно

$$(a_1 a_2 ... a_m)(a_{m+1} ... a_{n-1}) a_n = (a_1 a_2 ... a_{n-1}) a_n = a_1 a_2 ... a_n$$

по-моему он не так доказывал □

Теорема 5.4 (как он доказывал)**.** $\mathcal{A}$ *- полугруппа, тогда значение любого терма не зависит от расстановки скобок*

Доказательство. Индукция по длине терма (по количеству умножений)

Базис: ≤ 1, скобок нет

Индукционный шаг: $t = t_1 * t_2$, в t_1, t_2 меньше умножений

$t_1(a_1, ..., a_n)$
$t_1(a_1, ..., a_n) = (...((a_1 * a_2) * a_3)...) * a_m$
$t_2(a_1, ..., a_n)$
Индукция по $n - m$
Базис: $t_2 = a_n$

$$t = t_1 * a_n = (...((a_1 * a_2) * a_3)...) * a_m) * a_n$$

Индукционный шаг: $< n - m$

$$\begin{aligned} t = t_1 * t_2 = \\ (...((a_1 * a_2) * a_3)...) * a_m) * (a_{m+1} * (a_{m+1} * (... * a_n))) = \\ ((...((a_1 * a_2) * a_3)...) * a_m) * a_{m+1}) * (a_{m+1} * (... * a_n)) = \\ (...((a_1 * a_2) * a_3)...) * a_n \end{aligned}$$

□

Теорема 5.5. $a^{n+m} = a^n a^m$

Доказательство. $a^{n+m} = \underbrace{a...a}_{n+m} = \underbrace{a...a}_{n}\underbrace{a...a}_{m} = a^n a^m$ □

Теорема 5.6. *Если операция коммутативна, то* $(ab)^n = a^n b^n$

Доказательство. $(ab)^n = \underbrace{ab...ab}_{n} = \underbrace{a...a}_{n}\underbrace{b...b}_{n} = a^n b^n$ □

Определение 5.7 (Нейтральный слева)**.** e_l называется нейтральным слева в полугруппе, если $e_l * a = a$ для всех a,

Определение 5.8 (Нейтральный справа)**.** e_r называется нейтральным справа в полугруппе, если $a * e_r = a$ для всех a,

Определение 5.9 (Нейтральный элемент)**.** e - нейтральный слева и справа

Пример 5.10 (Примеры нейтрального элемента)**.** $(\omega, +)$ - 0, $(\omega, \cdot)$ - 1, (ω, max) - 0, (ω, min) - *нет нейтрального*

Теорема 5.11. *Если существуют нейтральный слева и нейтральный справа то они равны*

Доказательство.

$$e_l = e_l * e_r = e_r$$

□

Следствие 5.12. *Если нейтральный элемент существует, то он единственный.*

Определение 5.13 (Моноид)**.** Моноид - полугруппа с нейтральным элементом ИЛИ

Моноид - это элементы многообразия, которые определяются равенствами

$$\begin{cases} x * (y * z) = (x * y) * z \\ x * e = x \\ e * x = x \end{cases}$$

Пример 5.14 (Примеры моноидов)**.** $(\omega, +, 0)$, $(\omega, \cdot, 1)$, $(\omega, max, 0)$

A^A - *множество одноместных функций из* A *в* A $h = f \circ g$, *если* $h(a) = g(f(a))$ *для любого* $a \in A$

Доказать что $(A^A, \circ)$ - *моноид*

Доказательство. $e(a) = a$ для всех a, тогда

$$\left.\begin{array}{ll} (e \circ f)(a) & = f(e(a)) = f(a) \\ (f \circ e)(a) & = e(f(a)) = f(a) \end{array}\right\} e \circ f = f \circ e = f$$

e - нейтральный элемент

$$((f \circ g)h)(a) = h(f \circ g)(a) = h(g(f(a)))$$
$$(f(g \circ h))(a) = (g \circ h)(f(a)) = h(g(f(a)))$$
$$((f \circ g)h)(a) = (f(g \circ h))(a)$$

Выполняется ассоциативность, соответственно $(A^A, \circ, e)$ - моноид

□

Определение 5.15 (Идемпотент)**.** Идемпотент - элемент моноида a, такой что $a^2 = a$

Пример 5.16 (Примеры идемпотентов)**.** $(\omega; +)$ - 0

Определение 5.17 (Левый обратный элемент)**.** b_l - левый обратный для элемента a, если $b_l * a = e$

Определение 5.18 (Правый обратный элемент)**.** b_r - правый обратный для элемента a, если $a * b_l = e$

Определение 5.19 (Обратный элемент)**.** b - обратный для элемента a, если $b * a = a * b = e$

Определение 5.20 (Обратимый элемент)**.** Элемент, для которого существует обратный

Теорема 5.21. *Если a обратим слева и справа, то он обратим и обратный элемент является единственным.*

Доказательство.

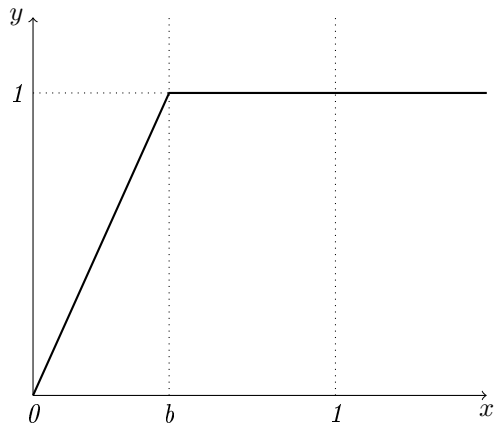
$$b_l a = e, \quad a b_r = e$$

$$b_l = b_l e = b_l(a b_r) = (b_l a) b_r = e b_r = b_r$$

□

Пример 5.22. *Доказать что множество функций этого вида замкнуты относительно композиции:*

$$f(x) = \begin{cases} ax & \text{при } x < b \\ ab & \text{при } x \geq b \end{cases}$$



Доказательство. □

Пример 5.23 (Пример изоморфизма)**.** *Доказать*

$$(P(A \cup B); \cup, \cap) \cong (P(A); \cup, \cap) \times (P(B); \cup, \cap)$$

где $P(A)$ *- множество всех подмножеств множества* A

Доказательство. Надо доказать

$$h(x_1 \cup x_2) = h(x_1) \cup h(x_2)$$

$$h(x_1 \cap x_2) = h(x_1) \cap h(x_2)$$

и h - биекция

По сути функция h должна выдавать пару, первая часть которой состоит из элементов A, вторая из B □

Пример 5.24 (Пример полугруппы)**.** *Является ли* $(\omega, \text{НОД}())$ *полугруппой*

Доказательство. Предположим что является, надо доказать

$$\text{НОД}(\text{НОД}(x, y), z) = \text{НОД}(x, \text{НОД}(y, z))$$

1. $\Rightarrow$ Пусть $d : d|\,\text{НОД}(x, y), d|z$
   Надо доказать $d|\,\text{НОД}(y, z)$, $d|x$

$$d|\,\text{НОД}(x, y) \Rightarrow d|x$$
$$d|\,\text{НОД}(x, y) \Rightarrow d|y$$
$$d|x, d|y \Rightarrow d|\,\text{НОД}(y, z)$$

2. $\Leftarrow$ также

□

Пример 5.25 (Построение моноидов)**.** *Построить все моноиды из двух элементов* $\{e, x\}$

$$A_1 = (\{e, x\}; *_1), A_2 = (\{e, x\}; *_2)$$

Доказать их ассоциативность: $a * (b * c) = (a * b) * c$

1. $a = e$

$$e * (b * c) = b * c = (e * b) * c$$

Таблица умножения ($*_1$)

	e	x
e	e	x
x	x	e

Таблица умножения ($*_2$)

	e	x
e	e	x
x	x	x

2. $b = e$ *также*
3. $c = e$ *также*
4. $a = b = c = x$

$$x * (x * x) = x * e = e * x = (x * x) * x$$

Все остальные моноиды или изоморфны или тривиальны

Теорема 5.26. *Если в конечном моноиде каждый элемент имеет левый обратный, то существует правый обратный*

Доказательство. Предположим обратное: Если в конечном моноиде каждый элемент имеет левый обратный, то хотя бы для одного не существует правый обратный: $ab_r \neq e$ для всех b_r

НЕ ДОКАЗАНО □

Определение 5.27 (Сократимый элемент)**.** Сократимый слева (справа) - такой элемент моноида, что из $ax = ay$ ($xa = ya$) следует $x = y$

Пример 5.28 (Пример сократимого элемента)**.** $(\mathbb{Z}, +, 0)$, $x + a = y + a \Rightarrow x = y$

Теорема 5.29. *Неединичные идемпотенты несократимы*

Доказательство. $a \cdot a = a = e \cdot a$ но $a \neq e$, соответственно a несократим справа, $a \cdot a = a = a \cdot e$ но $a \neq e$, соответственно a несократим слева

a несократим □

Теорема 5.30. *Все обратимые слева(справа) элементы сократимы слева(справа)*

Доказательство. Пусть a - обратимый слева, тогда $ax = ay \Rightarrow b_l ax = b_l ay \Rightarrow ex = ey \Rightarrow x = y$, следовательно a - сократимый слева □

Пример 5.31 (Пример обратимого элемента)**.** $(\mathbb{Z}^+, \cdot, 1)$, *обратимый только* 1, *сократимы все. (Какой к половым органам это пример?)*

6 Циклические моноиды, свободные моноиды .

Определение 6.1 (Свободный моноид)**.** Свободный моноид - моноид, элементами которого являются конечные последовательности (строки) элементов носителя моноида. Свободный моноид на множестве $A \neq \emptyset$ это $\mathcal{A} = (A^*; \&, \varepsilon)$, A^* - множество всех слов в алфавите A, & - конкатенация, ε - пустое слово.

Теорема 6.2. *Любой моноид, порождённый элементами множества, на котором есть свободный моноид, является гомоморфным образом этого моноида*

Доказательство. Пусть $A \neq \emptyset$, $\mathcal{A} = (A^*; \&)$,
$\mathcal{B} = (\{t^{\mathcal{B}}(a_1, ..., a_n) : a_1, ..., a_n \in A\}; *)$ и $h : \mathcal{A} \to \mathcal{B}$ - Гомоморфизм

$$h(a_1...a_n) = (a_1, ..., a_n)^{\mathcal{B}}$$

$$h(\varepsilon) = e^{\mathcal{B}}$$

Надо доказать свойство гомоморфизма:

$$h(u\&v) = h(u) * h(v)$$

Пусть $u = a_1...a_n$, $v = {a'}_1...{a'}_n$, тогда

$$h(u\&v) = h(uv) = h(a_1...a_n{a'}_1...{a'}_n) = (a_1...a_n{a'}_1...{a'}_n)^{\mathcal{B}}$$

$$h(u) * h(v) = h(a_1...a_n) * h({a'}_1...{a'}_n) = (a_1...a_n)^{\mathcal{B}} * ({a'}_1...{a'}_n)^{\mathcal{B}} = (a_1...a_n{a'}_1...{a'}_n)^{\mathcal{B}}$$

Из этого следует что $h(u\&v) = h(u) * h(v)$ □

Пример 6.3 (Примеры свободных моноидов и их гомоморфных образов)**.** *Пусть дан алфавит* $A = \{1\}$*, который образует множество слов* $A^* = \{\varepsilon, 1, 11, ...\}$ *и моноид* $\mathcal{A} = (A^*; \&, \varepsilon)$*, тогда*

1. $\mathcal{B} = (\{1\}; \cdot, 1)$*, порождённый элементами* A *является гомоморфным образом* $\mathcal{A}$*,* $h : A \to B$*,* $h(1...1) = 1$
2. $\mathcal{C} = (\omega; +, 0)$*, порождённый элементами* A*(натуральные числа можно получить сложением единицы) является гомоморфным образом* $\mathcal{A}$*,* $h : A \to B$*,* $h(\underbrace{1...1}_{n}) = n$

Определение 6.4 (Циклический моноид)**.** Циклический моноид - моноид порождённый одним элементом. $< a >$ - циклический моноид, порождённый элементом a.

$e, a, a^1, a^2, a^3, ...$ - элементы моноида $< a >$

1. $a^i \neq a^j$ при $i \neq j$

   $h :< a > \to (\{a\}^*; \&)$, $h(a^i) = i$ - изоморфизм.

2. $a^i = a^j$ при $i \neq j$

$$k = i + (k - i) = i + y(j - i) + r$$

$$r = (k - i) mod (j - i)$$

$$r < j - i$$

тогда

$$a^k = a^i \underbrace{a^{j-i}...a^{j-i}}_{y} a^r =$$

$$(a^i a^{j-i}) \underbrace{a^{j-i}...a^{j-i}}_{y-1} a^r \overset{(a^i a^{j-i} = a^{i+j-i} = a^j = a^i)}{=} a^i \underbrace{a^{j-i}...a^{j-i}}_{y-1} a^r =$$

$$a^i a^r = a^{i+r} (r < j - i; i + r < j)$$

к чему весь этот список?

Пример 6.5 (Пример циклического моноида)**.** $< a >= (\{e, a, ...\}; *)$

Таблица умножения $(*)$ -

Теорема 6.6. *Если* j *- наименьшее число такое что* $a^i = a^j$ *для какого-то* $i < j$*, то* $< a >$ *содержит ровно* j *элементов*

	e	a	a^2
e	a	a	a^2
a	a	a^2	a
a^2	a^2	a	a^2

Доказательство.

$$\underbrace{e, a^1, ..., a^{j-1}}_{\text{нет равных}}, \underbrace{a^j = a^i, a^{j+1} = a^{i+1}, ...}_{\text{повторяющиеся}}$$

если j - номер наименьшего повтора, тогда

$$a^x * a^y = \begin{cases} a^{x+y}, & \text{если } x+y < j \\ a^{i+(x+y-i)mod(j-i)}, & \text{если } x+y \geq i \end{cases}$$

$$x + y = k, \qquad k = i + (k - i \cdot z + r$$
$$r = (k-i)mod(j-i)$$
$$a^k = a^{i+z}$$

$$a^{x+y} = a^k = a^{i+(x+y-i)mod(j-i)}$$

□

Определение 6.7 (Моноид типа $(i, j-i)$)**.** Вначале идут i элементов без повтора, потом идёт цикл $j - i$

Теорема 6.8. *В моноиде типа $(i, j-i)$, где $i > 0$ существует идемпотент $b \neq e$*

Доказательство. Пусть $j - i = m$, проверим элемент $a^{i+(m-i) \bmod m}$

$$(a^{i+(m-i) \bmod m})^2 = a^{2i+2(m-i) \bmod m} = a^{i+(2i+2(m-i)) \bmod m-i) \bmod m}$$

$$\begin{aligned} i + (2i + 2(m-i) - i) \bmod m - i) \bmod m &= i + (2i + 2m - 2i - i) \bmod m \\ &= i + (2m - i) \bmod m \\ &= i + (m - i) \bmod m \end{aligned}$$

Следовательно $a^{i+(m-i) \bmod m}$ - идемпотент □

7 Группы, абелевы группы, циклические группы. Вложение моноида в группу

Определение 7.1 (Группа)**.** Группа - моноид, в котором все элементы обратимы

Определение 7.2 (Тривиальная группа)**.** Тривиальная группа - группа, состоящая из одного элемента

Теорема 7.3. *Если M - моноид и $G \subseteq M$ - подмножество обратимых элементов, то G - группа*

Доказательство. $G \subseteq M$ следовательно G ассоциативна, e - обратимый следовательно G имеет нейтральный элемент. Надо доказать замкнутость: $x * y \in G$

x', y' - обратные к x и y элементы, тогда

$$(x * y) * (y' * x') = x * (y * y') * x' = x * e * x' = x * x' = e$$

$$(y' * x') * (x * y) = y' * (x' * x) * y = y * e * y' = y * y' = e$$

$x * y$ обратим $\Rightarrow xy \in G$

если $x \in G$, то $x' * x = x * x' = e$, тогда x' имеет обратный элемент, тогда $x' \in G$. Любой элемент G имеет обратный.

G - группа. Теорема доказана.

□

Определение 7.4 (Абелева группа)**.** Абелева группа - группа, в которой $xy = yx$

Определение 7.5 (Циклическая группа)**.** Циклическая группа - группа, порождённая одним элементов a. $\langle a \rangle$ - циклическая группа, порождённая a.

Теорема 7.6. *Пусть $\mathcal{G} = \langle a \rangle$, тогда $\mathcal{G}$ изоморфна $(\mathbb{Z}, +)$ или $(\mathbb{Z}_n, +)$ для некоторого n*

Доказательство. Пусть M - подмоноид, порождённый a, M - циклический.

$M \overset{\text{h}}{\simeq} (\omega, +, 0)$

□

Теорема 7.7 (Теорема Гротендика)**.** *Каждый коммутативный моноид, в котором все элементы сократимы можно вложить в группу*

Доказательство. Пусть M - коммутативный моноид, $G' = M \times M = (a, b)$, где $a, b \in M$, $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$, (e_1, e_2) - нейтральный элемент.

Пусть $(a, b) \equiv (c, d) \Leftrightarrow ad = bc$. Является ли $\equiv$ конгруэнтностью?

1. $(a, b) \equiv (a, b)$, $ab = ba$
2. $(a, b) \equiv (c, d)$, $ad = bc \Rightarrow cb = da \Rightarrow (c, d) \equiv (a, b)$
3. $(a, b) \equiv (c, d) \equiv (u, v) \Rightarrow (a, b) \equiv (u, v)$

Надо доказать:

$$(a_1, b_1) \equiv (a_2, b_2), (c_1, d_1) \equiv (c_2, d_2) \Rightarrow (a_1c_1, b_1d_1) \equiv (a_2c_2, b_2d_2)$$

$$(a_1, b_1) \equiv (a_2, b_2), (c_1, d_1) \equiv (c_2, d_2) \Rightarrow$$
$$a_1b_2 = b_1a_2, c_1d_2 = d_1c_2 \Rightarrow a_1b_2c_1d_2 = b_1a_2d_1c_2 \Rightarrow$$
$$(a_1c_1)(b_2d_2) = (b_1d_1)(a_2c_2) \Rightarrow$$
$$(a_1c_1, b_1d_1) \equiv (a_2c_2, b_2d_2)$$

$(a, b) \equiv (c, d) \Leftrightarrow ad = bc$ - конгруэнтность

Пусть $G = {}^{G'}/_{\equiv}$ надо доказать что G - группа и M вкладывается в G

$$ab = ba \Rightarrow abe = ab = ba = bae \Rightarrow (ab, ba) \equiv (e, e)$$
$$\widehat{(a, b)} * \widehat{(b, a)} = \widehat{(ab, ba)} = \widehat{(e, e)}$$

$\Rightarrow$ каждый элемент G имеет обратный $\Rightarrow$ G - группа

Пусть $h : M \to G$ и $h(a) = \widehat{(a, e)}$, тогда

$$h(ab) = \widehat{(ab, e)} = \widehat{(a, e)}\widehat{(b, e)} = h(a)h(b)$$

$$h(e) = \widehat{(e, e)}$$

h - гомоморфизм

Пусть $h(a) = h(b)$

$$\widehat{(a,e)} = \widehat{(b,e)} \Rightarrow (a,e) \equiv (b,e) \Rightarrow ae = eb \Rightarrow a = b$$

следовательно h - инъекция, следовательно h - вложение

□

Пример 7.8 (Пример на теорему Гротендика)**.**

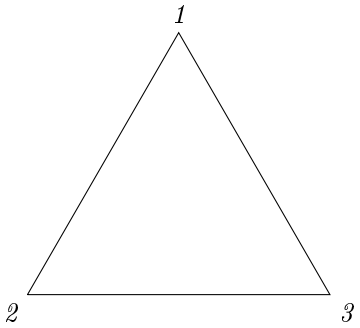
8 Группы перестановок, задание групп определяющими соотношениями.

Определение 8.1 (Группа перестановок)**.** Группа перестановок - группа перестановок множества S называется группа всех биекций $f : S \to S$. $(F, \circ, e, ^{-1})$

Пример 8.2 (Пример группы перестановок)**.**

Определение 8.3 (Симметрическая группа порядка)**.** Симметрическая группа порядка n: S - конечно и состоит из n элементов. $(A, \circ, e, ^{-1})$, A - множество автоморфизмов $h : S \to S$

Пример 8.4 (Пример симметрической группы)**.** *Пример симметрической группы:*



$A = \{e, r_1, r_2, s_1, s_2, s_3\}$

- e - *тождественное преобразование*
- r_1, r_2 - *поворот на* $120°$ *и* $240°$ *соответственно*
- s_1, s_2, s_3 - *оборот вокруг высоты, идущей из первой, второй и третьей вершины соответственно*

$$\mathbf{D}_3 = (A, \circ)$$

Таблица умножения $\circ$

	e	r_1	r_2	s_1	s_2	s_3
e	e	x	e	x	e	x
r_1	e	x	e	x	e	x
r_2	e	x	e	x	e	x
s_1	e	x	e	x	e	x
s_2	e	x	e	x	e	x
s_3	x	x	e	x	e	x

Определение 8.5 (Определяющее соотношение)**.** ???

Пример 8.6 (задание групп определяющими соотношениями)**.** *Нужно кинуть какой-нибудь пример*

9 Подгруппы, смежные классы, порядок и индекс подгруппы

Определение 9.1 (Подгруппа)**.** Подгруппа - подмножество H группы G, само являющееся группой относительно операции, определяющей G Подгруппа - подалгебра в группе

Следствие 9.2. *Подгруппа является группой*

Определение 9.3 (Тривиальная подгруппа)**.** Тривиальная подгруппа - подгруппа, состоящая только из одного нейтрального элемента группы или равна самой группе

Пример 9.4 (Пример подгрупп)**.**

Пример 9.5. $(\mathbb{Z}_p; +, 0, -)$, p - *простое число*
В этой группе нет нетривиальных подгрупп

Доказательство. $A \subseteq \mathbb{Z}_p$, $x \in A$, x $x, 2x, 3x, ..., px$ - все разные
предположим, что $ix = jx (i < j)$, тогда $jx - ix = 0 \Rightarrow (j - i)x = 0$
$(j - i)xmodp = 0$
$(j - i)modp = 0$
$j - i = 0$ ПОЧЕМУ
$j = i$
$A = \mathbb{Z}_p$

□

Теорема 9.6. *Любая бесконечная группа имеет нетривиальную подгруппу*

Доказательство. Пусть $a \in G$, $a \neq e$, тогда
$A = \{a^0 = e, a^1, a^2, ..., a^{-1}, a^{-2}, ...\}$

1. $A \neq G$ A - нетривиальная подгруппа
2. $A = G$ $A' = \{a^0, a^2, a^4, ..., a^{-2}, a^{-4}, ...\}$

□

Пример 9.7 (Пример подгрупп)**.** *Возьмём группу из 8.4 и выпишем подгруппы:*

1. $\{e\}$ - *тривиальная подгруппа*
2. $\{e, r_1, r_2, s_1, s_2, s_3\}$ - *тривиальная подгруппа*
3. $\{e, r_1, r_2\}$
4. $\{e, s_1\}$, $\{e, s_2\}$, $\{e, s_3\}$

Пример 9.8. *Группа операций над треугольником - подгруппа*

Пример 9.9. *Является ли группой моноид* $(\mathcal{A}; \cap, e)$*, где* $\mathcal{A}$ *- множество фигур на плоскости,* e *- вся плоскость.*

Доказательство. $A \cap A^{-1} = e$, этого не может быть, $(\mathcal{A}; \cap, e)$ - не группа
□

Является ли группой алгебра $(\mathcal{A}; \div)$*, где* $\mathcal{A}$ *- множество фигур на плоскости.*

Доказательство. Сперва докажем ассоциативность $\dot{-}$: $A \dot{-} (B \dot{-} C) = (A \dot{-} B) \dot{-} C$

$A \dot{-} B = (\overline{A} \cap B) \cup (\overline{B} \cap A)$

$$A \dot{-} (B \dot{-} C) = (\overline{A} \cap (B \dot{-} C)) \cup (A \cap (\overline{B \dot{-} C})) =$$
$$(\overline{A} \cap ((\overline{B} \cap C) \cup (\overline{C} \cap B)) \cup (A \cap (\overline{(\overline{B} \cap C) \cup (\overline{C} \cap B)})) =$$
$$(\overline{A} \cap ((\overline{B} \cap C) \cup (\overline{C} \cap B)) \cup (A \cap (\overline{(\overline{B} \cap C)} \cap \overline{(\overline{C} \cap B)})) =$$
$$(\overline{A} \cap ((\overline{B} \cap C) \cup (\overline{C} \cap B)) \cup (A \cap ((B \cup \overline{C}) \cap (C \cup \overline{B})) =$$
$$(\overline{A} \cap \overline{B} \cap C) \cup (\overline{A} \cap B \cap \overline{C}) \cup (A \cap ((B \cup \overline{C}) \cap (C \cup \overline{B})) =$$
$$(\overline{A} \cap \overline{B} \cap C) \cup (\overline{A} \cap B \cap \overline{C}) \cup (A \cap B \cap \overline{C}) \cup (A \cap B \cap C) \cup (A \cap \overline{B} \cap \overline{C}) \cup (A \cap \overline{C} \cap C) =$$
$$(\overline{A} \cap \overline{B} \cap C) \cup (\overline{A} \cap B \cap \overline{C}) \cup (A \cap B \cap C) \cup (A \cap \overline{B} \cap \overline{C})$$

$$(A \dot{-} B) \dot{-} C = C \dot{-} (A \dot{-} B) = ... =$$
$$(\overline{C} \cap \overline{B} \cap A) \cup (\overline{C} \cap B \cap \overline{A}) \cup (C \cap B \cap A) \cup (C \cap \overline{B} \cap \overline{A})$$

$$A \dot{-} (B \dot{-} C) = (A \dot{-} B) \dot{-} C$$

теперь доказать существование обратного
Пусть $e = \emptyset$, Тогда $A \dot{-} \emptyset = A$
$A \dot{-} A^{-1} = \emptyset \Rightarrow (\overline{A} \cap A^{-1}) \cup (\overline{A^{-1}} \cap A) = \emptyset \Rightarrow A^{-1} = A$
$(\mathcal{A}; \dot{-})$ - группа □

Пример 9.10. *Конечные группы*

1. $\mathcal{G}_1 = (\{e\}; *)$

Таблица умножения $*$

	e
e	e

2. $\mathcal{G}_2 = (\{e, a\}; *)$

Таблица умножения $*$

	e	a
e	e	a
a	a	e

3. $\mathcal{G}_3 = (\{e, a, b\}; *)$

Таблица умножения $*$

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

4. $\mathcal{A} = (\{e, a, b, c\}, *)$

Таблица умножения $*$

	e	a	b	c
e	e	a	b	c
a	a	e	b	c
b	b	c	e	a
c	c	b	a	e

Пример 9.11. *Построить группу симметрии правильного n-угольника (Диэдрическая группа)*

$\mathcal{D}_n = (r_0, ..., r_{n-1}, s_1, ..., s_n; \circ, e, ^{-1})$, *где* $r_0, ..., r_{n-1}$ *- повороты,* $s_1, ..., s_n$ *- отражения, эти элементы множсетва являются автоморфизмами, композиция задана следующей таблицей умножения:*

Таблица умножения $\circ$

	r_i	s_i
r_j	$r_{(i+j)\mathrm{mod}n}$	$s_{(i+j)\mathrm{mod}n}$
s_j	$s_{(j-i)\mathrm{mod}n}$	$r_{(i-j)\mathrm{mod}n}$

нейтральным элементом является r_0, обратным к любому отражению s_i само отражение s_i, обратным к повороту r_i поворот r_{n-i}

Определение 9.12 (Рекурсивная перестановка)**.** Рекурсивная перестановка - разнозначная общерекурсивная функция, область значений которой - множество ω

Теорема 9.13. *Рекурсивные перестановки с операцией композиции образуют группу*

Доказательство. Надо доказать ассоциативность $\circ$, существование нейтрального и обратных

1. $a \in \omega$, $a = g(b)$, $b = f(c)$, $a = g(f(c)) = (f \circ g)(c)$, $\circ$ ассоциативна
2. $e = \mathrm{Id}_1^1$, $(f \circ e)(a) = e(f(a)) = f(a)$
3. $f^{-1} =$

□

Теорема 9.14. *Любая группа вкладывается в группу перестановок*

Доказательство. Пусть $\mathcal{G} = (G, *)$, S - множество перестановок G, надо доказать

$$h(x * y) = h(x) \circ h(y)$$

Пусть $h(x) = f_x$, такой что $f_x(y) = y * x$ (А существует ли f_x для каждого x?). h разнозначна, так как $f_x(e) = f_y(e) \Rightarrow ex = ey \Rightarrow x = y$,

$$h(x * y)(a) = f_{x*y}(a) = a * (x * y) = (a * x) * y = f_x(a) * y = f_y(f_x(a)) = (f_x \circ f_y)(a) = (h(x) \circ h(y))(a)$$

□

Теорема 9.15. *Любой конечный моноид, в котором нет неединичных идемпотентов является группой*

Доказательство. Пусть M - конечный моноид, $a \in M$, $a * a^{-}1 = e$
Индукция по количеству элементов
Базис: $n = 1$, $a = e$, $M = \{e\}$
Шаг индукции: пусть для моноидов с $k < n$ верно. Тогда для $k = n$
Пусть $a \in M$, A - циклический моноид, порождённый a

1. $A \neq M$, $|A| < n$, по индукционному предположению
2. $A = M$, так как M не содержит неединичных идемпотентов, то A - это моноид типа $(0, n)$

$$a^x a^y = \begin{cases} a^{x+y} & \text{, если } x + y < n, y < n - 1 \\ a^{j+(x+y-i)} & \text{, если } x + y \geq n \end{cases}$$

следовательно $a^x a^y = a^{(x+y) \bmod n}$ и $a^{-1} = a^{n-1}$

□

Пример 9.16. *Построить группу симметричную чему-то там*

Теорема 9.17. *Любая чётная перестановка является произведением циклов длины 3*

Доказательство. Любую чётную перестановку можно разложить в произведение циклов длины 2. Таких циклов будет чётное число, соответственно будет n произведений циклов вида $(ab)(cd)$

1. $b = c$, тогда $(ab)(cd) = (abd)$
2. $b \neq c$, тогда $(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$

□

Теорема 9.18. *Если $\mathcal{G}$ - группа, $\mathcal{H} \subseteq \mathcal{G}$, $\mathcal{H} \neq \emptyset$, $a, b \in \mathcal{H} \to ab^{-1} \in \mathcal{H}$, тогда $\mathcal{H}$ является подгруппой*

Доказательство. Пусть $a, b \in H$

1. $H \neq \emptyset$, $a \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$ есть нейтральный элемент
2. $a \in H \Rightarrow ea^{-1} \in H \Rightarrow a^{-1} \in H$, есть обратные
3. $a, b \in H$, $b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$, замкнуто по операции группы $\mathcal{G}$

   $\mathcal{H}$ - подгруппа

□

Определение 9.19 (Центр группы)**.** Центр группы - $\mathcal{Z} = \{a \in G, ab = ba$ для всех $b \in G\}$

Пример 9.20. $\mathcal{M} = (M_2^*(\mathbb{R}); \cdot)$, *невырожденные матрицы*

$$\mathcal{Z} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in R \right\}$$

Теорема 9.21. *Центр группы - подгруппа*

Доказательство. $a, b \in \mathcal{Z}$, $ab^{-1} \in \mathcal{Z}$

Надо доказать: $x \in \mathcal{G}$, $(ab^{-1})x = x(ab^{-1})$

$$(ab^{-1})x = ab^{-1}xe = ab^{-1}xbb^{-1} = ab^{-1}bxb^{-1} = axb^{-1} = x(ab)^{-1}$$

следует что $x \in \mathcal{Z}$ (что это вообще доказывает) □

Определение 9.22 (Циклическая группа)**.** Циклическая группа - группа, порождённая одним элементом. $< a >$ - циклическая группа порождённая a.

$(\omega, +, 0)$ изоморфно бесконечной циклической группе

моноид типа (i, j) изоморфен конечной циклической группе

Теорема 9.23. $\mathcal{G} = \langle a \rangle$, *тогда* $\mathcal{G} \cong (\mathbb{Z}, +)$ *или* $\mathcal{G} \cong (\mathbb{Z}_n, +)$ *для некоторого* n

Доказательство. Пусть $\mathcal{M}$ - подмоноид, порождённый a. M - циклический

1. $\mathcal{M} \cong (\omega, +, 0)$

   $x \in \mathcal{M}$ x^{-1} $xx^{-1} = e$

   $x \in \mathcal{M}$ $x \neq e$ $x^{-1} \neq \mathcal{M}$

   $$0 = h(x) + h(x^{-1}) = h(xx^{-1}) = h(e) = 0$$

   Доказать что изоморфизм

2. $\mathcal{M}$ - конечный (i, j) моноид, если $i > 0$, то в $\mathcal{M}$ есть нееденичный идемпотент, следовательно он необратимый, следовательно в группе должно быть $i = 0$

   $$a^x a^y = \begin{cases} a^{x+y} & \text{, если } x + y < j \\ a^{(x+y) \pmod j} & \text{, если } x + y \geq j \end{cases}$$

$\mathcal{M}$ - группа

$$a^x = a^{j-x} = a^j \pmod{j} = e$$

$\mathcal{M}$ - группа порождённая a, $\mathcal{M} = \mathcal{G}$

$h : a^x \to x$

□

Теорема 9.24. *В циклической группе существуют нетривиальные группы тогда и только тогда когда она бесконечна или n в $(\mathbb{Z}_n, +)$ составное*

Доказательство. 1. $\Rightarrow$ пусть имеется $(\mathbb{Z}_n, +)$, n - простое, $a \neq 0$, $a < n$, a и n взаимно простые, следовательно $xa + yn = 1$. пусть $b \in \mathbb{Z}$, тогда

$$b = b \cdot 1 = b(ax + yn) = (bx)a + (by)n$$

$$(\underbrace{a + a + ... + a}_{bx}) \mod n = (b - (by)n) \mod n = b \mod n = b$$

Таким (КАКИМ) образом любые подгруппы, содержащие не только 0 содержат $\mathbb{Z}_n$

2. $\Leftarrow$

   (a) бесконечная циклическая группа имеет нетривиальную подгруппу

   (b) пусть $n = xy$, тогда $(\mathbb{Z}_{xy}, +) \supseteq \{0, x, 2x, ..., (y-1)x\}$

□

Определение 9.25 (Порядок группы)**.** Порядок группы - количество элементов группы. $ord\mathcal{G}$

Определение 9.26 (Порядок элемента)**.** Порядок элемента - порядок порождённой им циклической подгруппы $orda = ord\langle a \rangle$

Пример 9.27. *Пример на порядок через группу треугольника*

$$\mathcal{D}_3 = \{e, r_1, r_2, s_1, s_2, s_3\}$$
$$\operatorname{ord} \mathcal{D}_3 = 6$$

$$\begin{aligned}
\langle r_0\rangle &= \{r_0\} & \operatorname{ord} r_0 &= 1\\
\langle r_1\rangle &= \{r_0, r_1, r_2\} & \operatorname{ord} r_1 &= 3\\
\langle r_2\rangle &= \{r_0, r_1, r_2\} & \operatorname{ord} r_2 &= 3\\
\langle s_1\rangle &= \{r_0, s_1\} & \operatorname{ord} s_1 &= 2\\
\langle s_2\rangle &= \{r_0, s_2\} & \operatorname{ord} s_2 &= 2\\
\langle s_3\rangle &= \{r_0, s_3\} & \operatorname{ord} s_3 &= 2
\end{aligned}$$

Следствие 9.28. $\operatorname{ord} e = 1$, $\langle e\rangle = \{e\}$

Определение 9.29 (Смежный класс)**.** Пусть $\mathcal{G}$ - группа, $\mathcal{H} \subseteq \mathcal{G}$, $a \in \mathcal{G}$
Левый смежный класс a по $\mathcal{H}$ - $a\mathcal{H} = \{ab : b \in \mathcal{H}\}$
Правый смежный класс a по $\mathcal{H}$ - $\mathcal{H}a = \{ba : b \in \mathcal{H}\}$

Пример 9.30. *Пример смежных классов:*
$\langle s_1\rangle \subseteq \mathcal{D}_3$, $r_1 \in \mathcal{D}_3$

$$r_1\langle s_1\rangle = r_1\{r_0, s_1\} = \{r_1, s_2\}$$
$$\langle s_1\rangle r_1 = \{r_0, s_1\}r_1 = \{r_1, s_3\}$$
$$r_1\langle s_1\rangle \neq \langle s_1\rangle r_1$$

Определение 9.31 (Нормальная подгруппа)**.** Нормальная подгруппа - подгруппа, у которой любой левый смежный класс совпадает с правым

Пример 9.32. *Пример нормальных групп*

$$\langle r_1\rangle = \{r_0, r_1, r_2\} \subseteq \mathcal{D}_3$$

$$r_i\langle r_1\rangle = r_i\{r_0, r_1, r_2\} = \{r_{0+i}, r_{1+i}, r_{2+i}\} = \langle r_1\rangle$$
$$\langle r_1\rangle r_i = \{r_0, r_1, r_2\}r_i = \{r_{0+i}, r_{1+i}, r_{2+i}\} = \langle r_1\rangle$$
$$r_i\langle r_1\rangle = \langle r_1\rangle r_i$$
$$s_i\langle r_1\rangle = \{s_i r_0, s_i r_1, s_i r_2\} = \{s_i, s_{i-1}, s_{i+1}\}$$
$$\langle r_1\rangle s_i = \{r_0 s_i, r_1 s_i, r_2 s_i\} = \{s_i, s_{i+1}, s_{i-1}\}$$
$$s_i\langle r_1\rangle = \langle r_1\rangle s_i$$

$\langle r_1\rangle$ - *нормальная подгруппа*

Теорема 9.33. *Если $\mathcal{G}$ - группа, $\mathcal{H} \subseteq \mathcal{G}$, и $\equiv$ - отношение принадлежности к одному левому смежному классу, то $\equiv$ - отношение эквивалентности*

Доказательство. 1. Рефлексивность $a \in a\mathcal{H} \Rightarrow a \equiv a$

2. Симметричность $a \equiv b \Rightarrow a \in x\mathcal{H}, b \in x\mathcal{H} \Rightarrow b \equiv a$

3. Транзитивность $a \equiv b$, $b \equiv c \Rightarrow$

$$\begin{array}{lll} a, b \in x\mathcal{H} & a = xh_a & b = xh_b \\ b, c \in y\mathcal{H} & b = yh'_b & c = yh_c \end{array}$$

$$xh_b = yh'_b \Rightarrow x = yh'_b h_b^{-1} \Rightarrow a = y\underbrace{h'_b h_b^{-1} h_a}_{\mathcal{H}}$$

$$\left.\begin{array}{l} c \in y\mathcal{H} \\ a \in y\mathcal{H} \end{array}\right\} a \equiv c$$

□

Следствие 9.34. *Каждый левый смежный класс является классом эквивалентности*

Следствие 9.35. *Левые смежные классы или совпадают или не пересекаются*

Следствие 9.36. *Количество элементов в левом смежном классе совпадает с* $\operatorname{ord}\mathcal{H}$

Доказательство. Пусть $f : \mathcal{H} \to a\mathcal{H}$, $f(x) = ax$, тогда

$$f(x) = f(y) \Rightarrow ax = ay \Rightarrow = a^{-1}ax = a^{-1}ay \Rightarrow x = y$$

f - взаимоодназначная функция, соответственно $\operatorname{ord} a\mathcal{H} = \operatorname{ord}\mathcal{H}$ □

Определение 9.37 (Индекс подгруппы)**.** Индекс подгруппы - количество левых смежных классов $\operatorname{ind} H$

Теорема 9.38. *Если H - подгруппа G, то* $\operatorname{ord} G = \operatorname{ord} H \cdot \operatorname{ind} H$

Доказательство. Разобьём группу G на левые смежные классы. Их количество - $\operatorname{ind} H$, каждый содержит $\operatorname{ord} H$ элементов. Общее количество этих элементов - $\operatorname{ind} H \cdot \operatorname{ord} H$

□

Следствие 9.39. $\operatorname{ind} H = \dfrac{\operatorname{ord} G}{\operatorname{ord} H}$

Следствие 9.40. $\operatorname{ord} H | \operatorname{ord} G$

Следствие 9.41. $\operatorname{ord} a | \operatorname{ord} \mathcal{G}$

Доказательство. $\mathcal{H} = \langle a \rangle$, $\operatorname{ord} a = \operatorname{ord} \mathcal{H}$

□

Теорема 9.42. $a^{\operatorname{ord} a} = e$

Доказательство. $\langle a \rangle = \{\underbrace{a^0, a^1, ..., a^{\operatorname{ord} a - 1}}_{\operatorname{ord} a}\}$, $a^{\operatorname{ord} a} = a^0 = e$

□

Теорема 9.43. $a^n = e \Leftrightarrow \operatorname{ord} a | n$

Доказательство. Пусть $x = \operatorname{ord} a + r = n$, $(0 \leq r < \operatorname{ord} a)$, тогда

$$e = a^n = a^{x \operatorname{ord} a} \cdot a^r = (a^{\operatorname{ord} a})^x \cdot a^r = e^x \cdot a^r = a^r$$

$a^r = e \Rightarrow r = 0 \Rightarrow n = x \cdot \operatorname{ord} a \Rightarrow \operatorname{ord} a | n$

□

Теорема 9.44. $a^{\operatorname{ord} G} = e$

Доказательство. $\operatorname{ord} a | \operatorname{ord} \mathcal{G} \Rightarrow \operatorname{ord} \mathcal{G} = x \cdot \operatorname{ord} a \Rightarrow a^{\operatorname{ord} \mathcal{G}} = (a^{\operatorname{ord} a})^x = e$

□

Пример 9.45. *$\mathcal{A}_5$ - группа чётных перестановок из 5 элементов. В $\mathcal{A}_5$ нет нормальных подгрупп*

Доказательство. ДОКАЖИ ДОМА)))))))))))))))) □

Теорема 9.46. *Любая подгруппа индекса 2 является нормальной*

Доказательство.
1. (a) $e\mathcal{H} = \mathcal{H}$
   (b) $a\mathcal{H} \neq \mathcal{H}$
   $a\mathcal{H} = \mathcal{G}/\mathcal{H}$
2. (a) $\mathcal{H}e = \mathcal{H}$
   (b) $\mathcal{H}a \neq \mathcal{H}$
   $\mathcal{H}a = \mathcal{G}/\mathcal{H}$

Что и зачем □

10 Гомоморфизмы групп, нормальные подгруппы, фактор-группа

Определение 10.1 (Нормальная подгруппа)**.** Нормальная подгруппа - подгруппа, у которой любой левый смежный класс совпадает с правым

Пример 10.2. *Пример нормальных групп*

$$\langle r_1\rangle = \{r_0, r_1, r_2\} \subseteq \mathcal{D}_3$$

$$r_i\langle r_1\rangle = r_i\{r_0, r_1, r_2\} = \{r_{0+i}, r_{1+i}, r_{2+i}\} = \langle r_1\rangle$$

$$\langle r_1\rangle r_i = \{r_0, r_1, r_2\}r_i = \{r_{0+i}, r_{1+i}, r_{2+i}\} = \langle r_1\rangle$$

$$r_i\langle r_1\rangle = \langle r_1\rangle r_i$$

$$s_i\langle r_1\rangle = \{s_i r_0, s_i r_1, s_i r_2\} = \{s_i, s_{i-1}, s_{i+1}\}$$

$$\langle r_1\rangle s_i = \{r_0 s_i, r_1 s_i, r_2 s_i\} = \{s_i, s_{i+1}, s_{i-1}\}$$

$$s_i\langle r_1\rangle = \langle r_1\rangle s_i$$

$\langle r_1\rangle$ - *нормальная подгруппа*

Теорема 10.3. *Если $\mathcal{G}$ - группа, $\mathcal{H} \subseteq \mathcal{G}$, и $\equiv$ - отношение принадлежности к одному левому смежному классу, то $\equiv$ - отношение эквивалентности*

Доказательство. 1. Рефлексивность $a \in a\mathcal{H} \Rightarrow a \equiv a$

2. Симметричность $a \equiv b \Rightarrow a \in x\mathcal{H}, b \in x\mathcal{H} \Rightarrow b \equiv a$

3. Транзитивность $a \equiv b$, $b \equiv c \Rightarrow$

$$\begin{array}{lll} a, b \in x\mathcal{H} & a = xh_a & b = xh_b \\ b, c \in y\mathcal{H} & b = yh'_b & c = yh_c \end{array}$$

$$xh_b = yh'_b \Rightarrow x = yh'_b h_b^{-1} \Rightarrow a = y\underbrace{h'_b h_b^{-1} h_a}_{\mathcal{H}}$$

$$\left.\begin{array}{l} c \in y\mathcal{H} \\ a \in y\mathcal{H} \end{array}\right\} a \equiv c$$

□

Определение 10.4 (Факторгруппа)**.** Рассмотрим группу G и ее нормальную подгруппу H. Пусть G/H — множество смежных классов G по H. Определим в G/H операцию умножения по следующему правилу: $aH \cdot bH = (ab)H$

Теорема 10.5. *Определение произведения смежных классов корректно. То есть произведение смежных классов не зависит от выбранных представителей a и b*

Доказательство. Пусть $aH, bH \in G/H$, $a_1 = a \cdot h_a \in aH$, $b_1 = b \cdot h_b \in bH$. Докажем, что $abH = a_1 b_1 H$. Достаточно показать, что $a_1 \cdot b_1 \in abH$.

В самом деле, $a_1 \cdot b_1 = a \cdot h_a \cdot b \cdot h_b = a \cdot b \cdot (b^{-1} \cdot h_a \cdot b) \cdot h_b$. Элемент $h = (b^{-1} \cdot h_a \cdot b)$ лежит в H по свойству нормальности H. Следовательно, $a \cdot b \cdot h \cdot h_b \in abH$. □

Определение 10.6 (Гомоморфизм групп)**.** Если G и H - группа, $h : G \to H$ и $h(a * b) = h(a) * h(b)$, то h - гомоморфизм

Следствие 10.7. *Гомоморфизм групп обладает следующими свойствами:*

1. $h(e) = e$
2. $h(a^{-1}) = h(a)^{-1}$

Доказательство. $h(e) = h(e * e) = h(e) * h(e)$
$h(e)$ - идемпотент в $\mathcal{H}$, следовательно $h(e) = e$

$$h(a^{-1}) = h(a^{-1}) * e = h(a^{-1}) * h(a) * (h(a))^{-1} =$$
$$h(a^{-1} * a) * (h(a))^{-1} = h(e) * (h(a))^{-1} = e * (h(a))^{-1} = (h(a))^{-1}$$

□

Определение 10.8 (Порождённая конгруэнтность)**.** Конгруэнтность порождённая h - если $a \equiv b \Leftrightarrow h(a) = h(b)$ - конгруэнтность, то $h[A] = {}^{A}/_{\equiv}$

Теорема 10.9. *Если $h : G \to H$ - гомоморфизм, $\equiv$ - конгруэнтность порождённая h, то классы эквивалентные e в G являются нормальными подгруппами*

Доказательство. Пусть $a, b \in f \Rightarrow ab^{-1} \in f$, $a \equiv e$, $b \equiv e$, $b^{-1} \equiv e^{-1} \equiv e$, $ab^{-1} \equiv ee \equiv e$

$$a\{b \in \mathcal{G} : b \equiv e\} \ni c$$

$$aba^{-1} \in \{b \in \mathcal{G} : b \equiv e\}a \ni c$$

$$c = ab = abe = aba^{-1}a$$
$$b \equiv e \quad a \equiv a \quad a^{-1} \equiv a^{-1}$$
$$aba^{-1} \equiv aea^{-1} = e$$
$$aba^{-1} \equiv e$$
$$aba^{-1}a = abe = ab = c$$

□

"И в обратную сторону". Хотя я в душе не знаю как в эту получилось.

Определение 10.10 (Ядро подгруппы)**.** Ядро подгруппы - множество элементов эквивалентных e. $\operatorname{Ker} h$

Теорема 10.11. *G - группа, H - нормальная подгруппа, $a \equiv b \Leftrightarrow a$ и b принадлежат одному левому классу, то $\equiv$ - конгруэнтность*

Доказательство. Пусть $a \equiv b$, $c \equiv d$, надо доказать

1. $ac \equiv bd$
2. $a^{-1} \equiv b^{-1}$ (зачем)

1.

$$a, b \in x\mathcal{H} \qquad a = xh_a, b = xh_b$$
$$c, d \in y\mathcal{H} \qquad c = yh_c, d = yh_d$$

$ac = xh_a \cdot yh_c$, $h_a y = yh'$, $h_a y \in \mathcal{H}y = y\mathcal{H}$

$$\left.\begin{aligned} ac = xh_a yh_c = xy\underbrace{h'h_c}_{\in\mathcal{H}} \in xy\mathcal{H} \\ bd = xh_b yh_d = xy\underbrace{h''h_d}_{\in\mathcal{H}} \in xy\mathcal{H} \end{aligned}\right\} \text{эквивалентные}$$

$h_b y = yh''$, $h_b y \in \mathcal{H}y = y\mathcal{H}$

2.

h_a h_b
h_a^{-1} h_b^{-1}
$\mathcal{H}x^{-1}$ $\mathcal{H}x^{-1}$

$a^{-1}, b^{-1} \in x^{-1}\mathcal{H}$

□

Определение 10.12 (щито)**.** $\mathcal{G}$ - группа, $\mathcal{H}$ - нормальная подгруппа, $\equiv$ - отношение конгруэнтности. Тогда $\mathcal{G}/_{\equiv} = \mathcal{G}/_{\mathcal{H}}$

Следствие 10.13. *Если $h : \mathcal{G} \to \mathcal{H}$ - гомоморфизм, тогда $h[\mathcal{G}] = \mathcal{G}/_{\operatorname{Ker} h}$*

Доказательство. $h[\mathcal{G}] = \mathcal{G}/_{\equiv} = \mathcal{G}/_{\operatorname{Ker} h}$ □

Пример 10.14.

$$\mathcal{D}_3 = \{e, r_1, r_2, s_1, s_2, s_3\}$$

$\langle r_1 \rangle$ - *подгруппа вращений*
$\langle r_1 \rangle$
$S_1\langle r_1 \rangle$

Таблица умножения (ЧЕГО???)

	$\langle r_1 \rangle$	$S_1\langle r_1 \rangle$
$\langle r_1 \rangle$	$\langle r_1 \rangle$	$S_1\langle r_1 \rangle$
$S_1\langle r_1 \rangle$	$S_1\langle r_1 \rangle$	$\langle r_1 \rangle$

Пример 10.15. $(\mathbb{R}, +) \supseteq (\mathbb{Z}, +)$
$a + \mathbb{Z}$
$ba \in \mathbb{Z}$
$a + \mathbb{Z} = b + \mathbb{Z}$
$a \in [0, 1)$
$(a + \mathbb{Z}) + (b + \mathbb{Z}) = (a + b) = (a + b) \mod 1$
$\mathbb{C}_1 = \{z \in \mathbb{C}, |z| = 1\}$, $(\mathbb{C}_1, \cdot)$
$h(x) = e^{2nix}$
$x \in \mathbb{R} = e^{2nix} \in \mathbb{C}_1$
$h(x + y) = e^{2ni(x+y)} = e^{2nix}e^{2niy} = h(x)h(y)$

$h : (\mathbb{R}, +) \to (\mathbb{C}, \cdot)$
$r \in \operatorname{Ker} h \Leftrightarrow r \equiv e$
$h(r) = h(e)$
$h(r) = h(0)$
$e^{2nix} = e^{2nix} = 1$
$e^{2nix} = 2n \cdot k, k \in \mathbb{Z}$
$r \in \mathbb{Z}$
$\operatorname{Ker} h \in \mathbb{Z}$

11 Действие группы на множестве , орбиты

Определение 11.1. $\mathcal{G}$ - группа, A - множество, образующее группу, тогда определяющим соотношением называют равенство вида $t(a) = s(a)$, где t, s - термы, $a \in A$

Пример 11.2. $A = \{a, b\}$, $a^2 = b^2$, $a^3 b = ba$

Определение 11.3. A - множество элементов, X - множество определяющих соотношений. Группа, порождённая A и X - $\mathcal{G}$ такая, что

1. образована при помощи A
2. в $\mathcal{G}$ выполняются все определяющие соотношения из X
3. любая группа $\mathcal{H}$, удовлетворяющая условиям 1 и 2 является гомоморфным множеством $\mathcal{G}$

Пример 11.4.

$$\mathcal{D}_3 = \{e, r_1, r_2, s_1, s_2, s_3\}$$

$A = \{r_1, s_1\}$, $\langle A \rangle = \mathcal{D}_3$

$$\begin{cases} r_1^3 = e \\ r_1 s_1 = s_1 r_1^2 \\ s_1^2 = e \end{cases}$$

$\mathcal{H}$ порождена A

$*$ - одноместная операция

$\mathcal{H}$?????? ??? слова, состоящие из $r_1, s_1, r_1^{-1}, s_1^{-1}$, пусть в $\mathcal{H}$ выполнены определяющие соотношения X

$$r_1^3 = e \qquad r_1^{-1} = r_1^2 \qquad r_1^{-1} = r_1 r_1$$
$$s_1^2 = e \qquad s_1^{-1} = s_1 \qquad s_1^{-1} = s_1$$

$s_1...s_1r_1...r_1$

$s_1^n r_1^m$

$s_1^n = s_1^n \mod 2$

$r_1^m = r^m \mod 3$

r_1^0	$s_1r_1^0$
r_1^0	$s_1r_1^0$
r_1^0	$s_1r_1^0$

Теорема 11.5. *Для любого множества A и множества определяющих соотношений X существует группа, образованная A и X*

Доказательство. Пусть $A' = A \cup \{a{-}1 : a \in A^{\}}$. Нужно проверить три свойства

1. Если M - свободный моноид образованный A'(M - множество слов алфавита A' с конкатенацией), M' - моноид, порождённый A', то M' - гомоморфный образ M. $u, v \in M$, $u \equiv v \Leftrightarrow h(u) = h(v)$ для любого гомоморфизма $h : M \to \mathcal{G}$. $\mathcal{G}$ - группа, порождённая A в которой ??? X.

   Надо доказать что $\equiv$ является конгруэнтностью

   (a) $a \equiv a$

   (b) $a \equiv b \Rightarrow b \equiv a$

   (c) $a \equiv b, b \equiv c \Rightarrow a \equiv c$

   Пусть $a \equiv b$, $c \equiv d$, то есть $h(a) = h(b)$, $h(c) = h(d)$, тогда, так как h является гомоморфизмом

   $$h(ac) = h(a)h(c) = h(b)h(d) = h(bd)$$

   следовательно $ac \equiv bd$ и $\equiv$ - конгруэнтность

   Пусть группа $F = {}^{M}/_{\equiv}$, $\widehat{a} \in F$, $a = u_1...u_n$, $b = u_n^{-1}...u_1^{-1}$, $a, b \in M$

   $h(a) = h(u_1)...h(u_n)$

   $h(b) = h(u_n^{-1})...h(u_1^{-1})$

   $h(ab) = h(u_1)...h(u_n)h(u_n^{-1})...h(u_1^{-1}) = e$

   $\widehat{a}\widehat{b} = \widehat{e}$

   F порождается A

2. Доказать $t(\overline{a}) = s(\overline{a}) \in X$

$$h(t(a_1, ..., a_n)) = t(h(a_1), ..., h(a_n)) = s(h(a_1), ..., h(a_n)) = h(s(a_1, ..., a_n))$$

$$t(\overline{a}) \equiv s(\overline{a}) \Rightarrow \widehat{t(\overline{a})} = widehats(\overline{a}) \Rightarrow t(\widehat{a_1}, ..., \widehat{a_n}) = s(\widehat{a_1}, ..., \widehat{a_n}$$

3. Из чего следует?

и WTF в общем □

Пример 11.6. *Про пирамиду рубика. Конём.*

Пример 11.7. *Дана "головоломка"*

1	2
3	4

Построить группу $\mathcal{G}$
a *- перестановка двух столбцов*
b *- перестановка строк*

e: | 1 | 2 | / | 3 | 4 | a: | 2 | 3 | / | 4 | 1 | b: | 3 | 4 | / | 1 | 2 | ab: | 4 | 1 | / | 2 | 3 |

$a^2 = e$, $b^2 = e$, $ab = ba$

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ba	e	a
ab	ab	b	a	e

$\mathcal{G} = (\{e, a, b, ab\}, \circ)$

Пример 11.8. *Таблица 8x8. Конём.*

Пример 11.9. $Z = 1, -1$

Пример 11.10.

Пример 11.11.

Пример 11.12.

Пример 11.13.

Определение 11.14. Если $X = \emptyset$, то ${}^{M}/_{\equiv}$ - свободная группа порождённая A

Следствие 11.15. *Любая группа порождённая A - гомоморфный образ свободной группы*

Определение 11.16. $\mathcal{G}$ - группа, $S \neq \emptyset$. Действие группы $\mathcal{G}$ на S - это отображение $h : S \times \mathcal{G} \to S$ и

1. $h(S, e) = S$
2. $h(h(S, a), b) = h(S, ab)$

Эти два условия по другому:

1. $Se = S$
2. $(Sa)b = S(ab)$

Пример 11.17. *$\mathcal{G}$ действует на себя правыми умножениями*

Определение 11.18. Сопряжение - действие группы $\mathcal{G}$ на себя или множество подмножеств $P(\mathcal{G}) : h(S, a) = a^{-1}Sa$

Теорема 11.19. *Сопряжение - действие*

Доказательство. Проверим условия сопряжения

1. $e^{-1}Se = eSe = S$
2. $h(h(S, a)b) = h(a^{-1}Sa, b) = b^{-1}a^{-1}Sab = (ab)^{-1}Sab = h(S, ab)$
   $a^{-1}Aa = A \subseteq \mathcal{G}$

□

Теорема 11.20. *Любая подгруппа при сопряжении переходит в подгруппу*

Доказательство. Пусть A - подгруппа $\mathcal{G}$ □

Теорема 11.21. *Пусть A - подгруппа, то A неподвижна при всех сопряжениях тогда и только тогда когда A - нормальная подгруппа*

Доказательство. • $\Rightarrow a^{-1}Aa = a \Rightarrow aa^{-1}Aa = aA \Rightarrow Aa = aA$

• $\Leftarrow Aa = aA \Rightarrow a^{-1}Aa = a^{-1}aA \Rightarrow a^{-1}Aa = A$

□

Определение 11.22 (Стабилизатор)**.** $\mathcal{G}$ действует на S, $s \in S$. Стабилизатор s - $\operatorname{stab} s = \{a \in \mathcal{G}, h(s,a) = s\}$

Теорема 11.23. $\operatorname{stab} s$ - *подгруппа* $\mathcal{G}$

Доказательство. пусть $b, c \in \operatorname{stab} s$, тогда □

Определение 11.24 (Орбита)**.** Пусть G действует на S, $s \in S$. Орбита s - $\operatorname{orb} s = \{sa : a \in G\}$

Теорема 11.25. *Орбиты - классы эквивалентности*

Теорема 11.26. *Количество элементов орбиты равняется индексу стабилизатора*

Теорема 11.27 (Формула орбит)**.** *G действует на множестве S, тогда* $|S| = \sum\limits_{орбиты} \dfrac{\operatorname{ord} G}{\operatorname{ord} q_0}$

Следствие 11.28. *Если* $\operatorname{ord} G = p^k$, *$p$ - простое, то $Z \neq \{e\}$*

12 Кольца, тела, поля. Делители нуля. Тело кватернионов

Определение 12.1 (Кольцо)**.** Кольцо - алгебра сигнатуры

$$(+^{(2)}, 0^{(0)}, {}^{-(1)}, \cdot^{(2)})$$

обладающее свойствами:

1. $(a + b) + c = a + (b + c)$
2. $a + 0 = a$
3. $a + (-a) = 0$

4. $a + b = b + a$

5. $a(b + c) = ab + ac$

Определение 12.2 (Ассоциативное кольцо)**.** Кольцо с ассоциативностью умножения $(ab)c = a(bc)$

Определение 12.3 (Кольцо с единицей)**.** Кольцо, в котором существует элемент 1, такой что $a \cdot 1 = 1 \cdot a = a$

Определение 12.4 (Коммутативное кольцо)**.** Кольцо с коммутативностью умножения $ab = ba$

Определение 12.5 (Кольцо с делением)**.** Если для любого элемента кольца $a\,(a \neq 0))$ существует $b : ab = 1$, то такое кольцо называется кольцом с делением

Определение 12.6 (Тело)**.** Тело - ассоциативное, коммутативное кольцо с делением

Определение 12.7 (Поле)**.** Поле - ассоциативное, коммутативное кольцо с делением и единицей

Пример 12.8 (Примеры колец)**.**

Теорема 12.9. *Для любых элементов кольца a, b справедливы следующие утверждения:*

1. $a0 = 0a = 0$

2. $(-a)b = a(-b) = -(ab)$

Доказательство. a □

Следствие 12.10. *В кольце с* 1 *ноль необратим.*

Определение 12.11 (Делитель нуля)**.** Пусть $a \cdot b = 0\, a, b \neq 0$, тогда a - левый делитель нуля, b - правый делитель нуля.

Пример 12.12 (Пример делителей нуля)**.**

Теорема 12.13. *Делители нуля необратимы*

Доказательство. □

Определение 12.14 (Идемпотент кольца)**.** Такие элементы кольца, для которых выполняется $a = a^2$

Теорема 12.15. *Идемпотенты - делители нуля*

Доказательство. □

Определение 12.16 (Тело кватернионов)**.**

Определение 12.17 (Подкольцо)**.**

Теорема 12.18. *Пусть S - подмножество кольца $(R, +, \circ)$, тогда $(S, +, \circ)$ - подкольцо $(R, +, \circ)$ тогда и только тогда когда*

1. $S \neq \emptyset$
2. $\forall x, y \in S : x + (-y) \in S$
3. $\forall x, y \in S : x \circ y \in S$

Доказательство. Необходимое условие выполняется по определению кольца.

Достаточное условие:

По 9.18 и условиям 1 и 2 $(S, +)$ является группой, то есть замкнута по сложению, ассоциативна, имеет нейтральный по сложению и обратный по сложению. По условию 3 $(S, \circ)$ замкнута. Так как $S \subset R$, то на S выполняются дистрибутивность и коммутативность.

Следовательно $(S, +, \circ)$ - кольцо. □

13 Целостные кольца, вложение кольца в поле

Определение 13.1 (Целостное кольцо)**.** Ассоциативное, коммутативное кольцо с единицей без делителей нуля

Теорема 13.2. *Конечное целое кольцо ?????*

Доказательство. □

Теорема 13.3. *Каждое целостное кольцо может быть достроено до поля*

Доказательство. □

14 Гомоморфизмы колец, идеалы, фактор-кольца

Определение 14.1 (Гомоморфизм колец)**.** $h : R \to S$ - гомоморфизм, определённый так: $a \equiv b \Leftrightarrow h(a) = h(b)$

Определение 14.2 (Ядро кольца)**.** $h : R \to S$ - гомоморфизм, тогда ядро кольца $\operatorname{Ker} h = \{a \in R : h(a) = 0\}$

Теорема 14.3. *Ядро кольца - подкольцо*

Доказательство. Пусть $\operatorname{Ker} h$ - ядро кольца R по гомоморфизму $R \to S$, тогда

1. $\operatorname{Ker} h \neq \emptyset$
2. $\forall x, y \in \operatorname{Ker} h : h(x + (-y)) = h(x) + h(-y) \overset{10.7}{=} h(x) - h(y) \overset{14.2}{=} 0 \Rightarrow x + (-y) \in \operatorname{Ker} h$
3. $\forall x, y \in \operatorname{Ker} h : h(x \circ y) = h(x) \circ h(y) = 0 \circ 0 = 0 \Rightarrow x \circ y \in \operatorname{Ker} h$

По 12.18 ядро $\operatorname{Ker} h$ является группой □

Определение 14.4 (Идеал)**.** R - кольцо, $\mathcal{I} \subseteq R$ - идеал (левый, правый, двусторонний), если

1. $\mathcal{I}$ - подкольцо
2. для любого $x \in R$ $x\mathcal{I} \subseteq \mathcal{I}$ (левый идеал), $\mathcal{I}x \subseteq \mathcal{I}$ (правый идеал)

Теорема 14.5. *Ядро кольца - идеал*

Доказательство. Пусть $\operatorname{Ker} h$ - ядро кольца R по гомоморфизму $R \to S$, тогда

1. по теореме 14.3
2. (a) $\forall x \in R, y \in \operatorname{Ker} h : h(xy) = h(x)h(y) = h(x) * 0 = 0 \Rightarrow xy \in \operatorname{Ker} h \Rightarrow x \operatorname{Ker} h \subseteq \operatorname{Ker} h$

   (b) $\forall x \in R, y \in \operatorname{Ker} h : h(yx) = h(y)h(x) = 0 * h(x) = 0 \Rightarrow yx \in \operatorname{Ker} h \Rightarrow \operatorname{Ker} h * x \subseteq \operatorname{Ker} h$

По определению идеала ядро $\operatorname{Ker} h$ является идеалом □

Пример 14.6 (Пример идеалов)**.**

Теорема 14.7. *Пусть R, S - кольца, $h : R \to S$ - гомоморфизм. Если* $\operatorname{Ker} h = \{0\}$, *то h - вложение*

Доказательство. Пусть $\operatorname{Ker} h = \{0\}$, $x, y \in A$. Пусть $h(x) = h(y) = b$, тогда

$$\begin{aligned} & h(x) - h(y) = b - b \\ & = 0 \\ \Rightarrow \quad & h(x - y) = 0 && 3.1 \\ \Rightarrow \quad & (x - y) \in \operatorname{Ker} h && 14.2 \\ \Rightarrow \quad & x - y = 0h \\ \Rightarrow \quad & x = y \end{aligned}$$

Так как x, y были произвольными, то h - вложение □

Лемма 14.8. *Если R - кольцо, $a \neq 0$, $a \in R$ и $1 \in aR$, то $aR = R$*

Доказательство. Так как $1 \in aR$, то a обратим, то есть существует $a^{-1} \in R$,следовательно

$$aR \supseteq aa^{-1}R = R$$

Так как $R \subseteq aR$ и $aR \subseteq R$, то $aR = R$ □

Теорема 14.9. *R - ассоциативное кольцо с единицей или R - тело или R тогда и только тогда когда в R Нет других идеалов, кроме* $\{0\}$ *и R*

Доказательство. Так как R - ассоциативное кольцо с единицей или или тело, то для каждого a существует обратное a^{-1}. По лемме 14.8 для всех $a \neq 0$ $aR = R$. Остаётся только $a = 0$, который образует идеал $\{0\}$ □

Определение 14.10 (Булевое кольцо)**.**

Теорема 14.11. *Пусть I - двухсторонний идеал в R, тогда отношение $\equiv$: $x \equiv y \Leftrightarrow x - y \in I$ является конгруэнтностью*

Доказательство. □

Следствие 14.12. *Существует фактор-алгебра $R/_{\equiv}$, такая что ???*

Следствие 14.13. *$I = \operatorname{Ker} h$, где $h : R \to R/_{\equiv}$*

Доказательство. □

Определение 14.14 (Простой идеал)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда I - простой идеал, если $ab \in I \Leftrightarrow a \in I$ или $b \in I$

Определение 14.15 (Максимальный идеал)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда I - максимальный идеал, если для любого идеала $J : I \subseteq J, I \neq J$ выполняется $J = R$

Определение 14.16 (Главный идеал)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда I - главный идеал, если для некоторого $a \in R$ $I = aR$

Пример 14.17 (??????)**.**

Лемма 14.18. *Если I и J - идеалы, то $I + J$ тоже идеал*

Доказательство. □

Теорема 14.19. *Пусть R - ассоциативное, коммутативное кольцо с единицей, I - идеал, тогда*

1. *I - простой идеал $\Leftrightarrow {}^{R}/_{I}$ - целостное*
2. *I - максимальный идеал $\Leftrightarrow {}^{R}/_{I}$ - поле*

Доказательство. □

15 Евклидовы кольца, кольца главных идеалов, факториальные кольца

Определение 15.1 (Евклидово кольцо)**.** R - ассоциативное, коммутативное кольцо с единицей, R - евклидово, если для каждого элемента a этого кольца существует его норма $\|a\|$.

Определение 15.2 (Евклидова норма)**.** Это некоторая функция элемента кольца, такая что

1. $\|a\| \in \omega$
2. если $a, b \neq 0$, то $\|ab\| \geq \max(\|a\|, \|b\|)$
3. если $a \neq 0$, то для любого b существуют d и r такие что $b = da + r$ и $\|r\| < \|a\|$ или $r = 0$

Определение 15.3 (Кольцо главных идеалов)**.** Кольцо главных идеалов - кольцо, в котором все идеалы главные

Теорема 15.4. *Каждое евклидово кольцо - кольцо главных идеалов*

Доказательство. □

Теорема 15.5. *В кольце главных идеалов R не существует бесконечно возрастающей цепи идеалов*

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq ...$$

Доказательство. Пусть $I_0 \subseteq I_1 \subseteq I_2 \subseteq ...$ - возрастающая цепь идеалов и $I = \cup_{i=0}^{\infty} I_i$, докажем что I - идеал

1. докажем что I - подкольцо по теореме 12.18

   (a) I замкнут по сложению и умножению, покажем на элементах $a, b \in I$. В таком случае в цепи есть идеалы I_j и I_k, такие что $a \in I_j$ и $b \in I_k$. Если $m \geq \max(j, k)$ то оба элемента a и b принадлежат I_m, поэтому принадлежат и $a + b$ и ab. Поэтому $a + b \in I$ и $ab \in I$

   (b) $0 \in I$ потому что $0 \in I_i$ для всякого i

   (c) Пусть $a \in I$. Тогда $a \in I_j$ Для какого-то j, в этом случае $-a \in I_j$, следовательно $-a \in I$

   следовательно I - подкольцо

2. Пусть $a \in I$. Тогда $a \in I_j$ Для какого-то j. Пусть r - любой элемент R, тогда $ra \in I_j$, следовательно $ra \in I$. Следовательно $rI \subseteq I$

по определению 14.4 I - идеал.

Так как R - КГИ и I - идеал, то существует $a \in R$, такое что $I = aR$. Так как $a \in I$ существует n такой что $a \in I_n$. Следовательно $aR \subseteq I_n$. По определению I $I_n \subset I = aR$. I_n и I входят друг в друга следовательно $I = I_n$. Если брать любое $m \geq n$ то должно выполнятся условие $I \subseteq I_m$. Это возможно только если $I_m = I$.

Следовательно после некоторого конечного элемента n цепь идеалов перестаёт возрастать □

Определение 15.6 (Простой элемент)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда a - простой, если из $a = bc$ следует что b или c обратимы

Определение 15.7 (Факториальное кольцо)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда R - факториальное кольцо, если для каждого элемента $a \in R$

1. существует простые $b_1, ..., b_n$, такие что $a = b_1...b_n$
2. если $a = c_1...c_m$, где $c_1, ..., c_m$ - простые, то $m = n$, существует перестановка σ, Такая что $c_i = e_i b_{\sigma(i)}$ Для обратимого e_i

Теорема 15.8. *Существует нефакториальное кольцо*

Теорема 15.9. *R - целостное кольцо и $a \neq 0$, Тогда следующие условия эквивалентны*

1. *a - необратимый*
2. *$aR \neq R$*
3. *Для любого $b \neq 0$ $abr \neq bR$*
4. *для некоторого $b \neq 0$ $abr \neq bR$*

Доказательство. $1 \Rightarrow 2$

$ab \neq 1$ для любого b, соответственно $aR \not\ni 1$, следовательно $aR \neq R$

$2 \Rightarrow 3$

Пусть $b \neq 0$. Допустим $abR = br \ni b$. Пусть для некоторого $r \in R$ верно $abr = b$, следовательно

$$arb - b = 0 \Rightarrow (ar - 1)b = 0 \Rightarrow ar - 1 = 0 \Rightarrow ar = 1$$

то есть $1 \in aR$, следовательно $aR = R$, Противоречие.

$3 \Rightarrow 4$

Если для любого $b \neq 0$ верно $abr \neq bR$, то верно и для некоторого

$4 \Rightarrow 1$

Допустим a - обратимый, то есть существует $r \in R$, такой что $ar = 1$, получается

$$abR = baR \subseteq bR$$

и

$$bR = 1 \cdot bR = arbR = abrR \subseteq abR$$

следовательно $bR = abR$, что противоречит 4, следовательно a необратим □

Теорема 15.10. *Если R - КГИ, то каждый необратимый элемент отличный от нуля раскладывается в конечное произведение простых элементов*

Доказательство. Пусть $a \in R$, $a \neq 0$, и a - необратимый

1. Сначала покажем что a имеет в разложении простой множитель. Если a простой, то разложение завершено. Если нет, то $a = a_1 b_1$, где ни a_1 ни b_1 необратимые. Тогда $a \in a_1 R$ и $aR \subset a_1 R$. Включение строгое, потому что если $aR = a_1 R$, то для некоторого $r \in R$ было бы $a_1 = ar$ и $a = arb_1$. Так как R - целостное и $rb_1 = 1$, то b_1 - обратимый, что противоречит разложению $a = a_1 b_1$, где ни a_1 ни b_1 необратимые.

   Если a_1 не простой, то можно сказать $a_1 = a_2 b_2$, где ни a_2 ни b_2 необратимые. Получается

   $$aR \subset a_1 R \subset a_2 R$$

   где каждое включение строгое. Если a_2 не простое то можно продолжить цепь, но по теореме 15.5 цепь нельзя продолжать бесконечно и после конечного числа шагов она закончится идеалом $a_r R$, где a_r - простое число. Следовательно в разложении a есть некоторый простой элемент a_r

2. Теперь покажем что a раскладывается в произведение простых элементов R. Если a не простое, то по пункту 1 можно сказать $a = p_1 c_1$, где p_1 - простое число и c_1 необратимое. Поэтому aR строго вкладывается в $c_1 R$. Если c_1 не простой, то $c_1 = p_2 c_2$ где p_2 - простое число и c_2 необратимое. Можно построить строго возрастающую цепь идеалов

   $$aR \subset c_1 R \subset c_2 R$$

   Эта цепь должна остановиться после конечного числа шагов на идеале $c_r R$, где c_r - простой. Тогда

   $$a = p_1 p_2 ... p_r c_r$$

   разложение на конечное число простых множителей

□

Лемма 15.11. *Пусть I - идеал КГИ R. Тогда I является максимальным тогда и только тогда когда $I = pR$, где p - простой*

Доказательство. Необходимость. Пусть I - максимальный идеал и $I = pR$ для некоторого $p \in R$. Если p - не простой, тогда $p = ab$, где a, b - необратимые и $pR \subseteq aR$. Более того $pR \neq aR$, так как $a \in pR$ подразумевало

бы $a = pc$ и $p = pcb$, что означало бы что b - обратимый. Также $aR \neq R$ так как a необратим (15.9). Непростота p противоречит максимольности идеала I: нашёлся идеал I' такой что $I \subseteq I'$ и $I' \neq R$ (14.15).

Достаточность. Пусть p - простой элемент и I_1 - идеал в R, содержащий $I = pR$. Тогда $I_1 = qR$ для некоторого $q \in R$ и $p \in I_1$ означает что $p = rq$ для некоторого $r \in R$. Тогда или q или r обратим. В первом случае $I_1 = qR = R$ а во втором случае $q = r^{-1}p$ и $q \in pR$, что подразумевает $qR = pR$ и $I_1 = I$. Поэтому I - максимальный идеал в R □

Теорема 15.12. *пусть R - целостное кольцо главных идеалов, тогда R - факториальное*

Доказательство. Для того чтобы показать что R - факториальное, надо показать что оно удовлетворяет условиям из 15.7:

1. по теореме 15.10
2. Надо показать что если $a = c_1...c_m = b_1, ..., b_n$, где $c_1, ..., c_m, b_1, ..., b_n$ - простые, то $m = n$, существует перестановка σ, Такая что $c_i = e_i b_{\sigma(i)}$ Для обратимого e_i

   Предположим что $n \geq m$. Так как $c_1|a$, то $c_1|b_1, ..., b_n$, то есть $c_1|b_j$ для какого-то j. Можно переставить местами так что $c_1|b_1$. Тогда $b_1 = c_1 e_1$ для какого-то обратимого $e_1 \in R$. Следовательно

   $$c_1 c_2 ... c_m = e_1 c_1 b_2 ... b_n$$

   и

   $$c_2 ... c_m = e_1 b_2 ... b_n$$

   Продолжая процесс получается

   $$1 = e_1 e_1 ... e_m b_{m+1} b_n$$

   Так как ни один из b_i необратим, получается $m = n$ и $c_i = e_i b_{\sigma(i)}$. Покажем что существует такая $\sigma : \{1, ..., m\} \to \{1, ..., m\}$ что σ - биекция. Определим $\sigma(i) =$ минимальный j, такой что $b_j|c_i$ и $j \notin \{\sigma(1), ..., \sigma(i-1)\}$. Нужно доказать что такой j всегда найдётся, что σ инъективна и сюръективна.

□

16 Поля. Кольца многочленов над полями. Корни многочлена, производная

Определение 16.1 (Многочлен над полем)**.** Пусть P - поле, многочлен над полем P это выражение

$$a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$$

где $a_i \in P$

Теорема 16.2. *Множество многочелнов над полем P $P[x]$ - евклидово кольцо, где норма $\|p\|, p \in P[x]$ - степень многочлена*

Доказательство. Чтобы $P[x]$ было евклидовым по определению 15.1 оно должно быть ассоциативным, коммутативным кольцом с единицей, что доказывается тривиально. К тому же оно является целостным.

Теперь нужно доказать что степень многочлена является нормой, воспользуемся определением евклидово нормы 15.2:

1. Степень многочлена - натуральные числа, поэтому $\|p\| = \deg p \in \omega$
2. Пусть $p(x), q(x) \in P[x]$, где $p(x), q(x) \neq 0$ и $\deg p = n, \deg q = m$. Тогда $\deg pq = n + m$, то есть $\|pq\| \geq \max(\|p\|, \|q\|)$
3. если $p(x) \neq 0$, то для любого $q(x)$ существуют $d(x)$ и $r(x)$ такие что $p(x) = d(x)q(x) + r(x)$ и $\|r\| < \|q\|$ или $r(x) = 0$. Доказательство индукцией по степени $p(x)$:

   Базис: $\deg p < \deg q$. $p(x) = 0 \cdot q(x) + p(x)$

   Индукционный шаг: для всех $\deg p : m = \deg q < \deg p < n$ верно. Показать что верно для $\deg p = n$. Пусть

   $$p(x) = a_0 + a_1 + ...a_n x^n$$

   $$q(x) = b_0 + b_1 + ...b_m x^m$$

   Мы можем отнять от $p(x)$ подходящий многочлен, после которого не останется слагаемого степени n

   $$\begin{aligned} p(x) - q(x) \cdot \frac{a_n}{b_m} x^{n-m} &= a_n x^n + p'(x) - (a_n x^n + \frac{a_n}{b_m} x^{n-m} q'(x)) \\ &= p'(x) - \frac{a_n}{b_m} x^{n-m} q'(x) \end{aligned}$$

Где $p'(x)$ и $q'(x)$ - не производные, это просто обозначение. По индукционному предположению

$$\underbrace{\underbrace{\underbrace{p'(x)}_{<n} - \frac{a_n}{b_m}x^{n-m}\underbrace{q'(x)}_{<m}}_{<n} = d'(x)\cdot q(x) + r(x)}_{<n} \quad \|r\| < \|q\|$$

Так как

$$p(x) - q(x)\cdot\frac{a_n}{b_m}x^{n-m} = d'(x)\cdot q(x) + r(x)$$

то

$$p(x) = q(x)\left(d'(x) + \frac{a_n}{b_m}x^{n-m}\right) + r(x) = q(x)\cdot d(x) + r(x) \quad \|r\| < \|q\|$$

□

Определение 16.3 (Корень многочлена)**.** Корень многочлена $p(x)$ над полем P это такой Элемент поля $a \in P$ что $p(a) = 0$

Теорема 16.4 (Теорема Безу)**.** *Если a - корень многочлена p, то $(x - a)|p(x)$*

Доказательство. Предположим обратное, тогда деление $p(x)$ на $(x-a)$ будет давать остаток

$$p(x) = d(x)(x - a) + r(x)$$

По теореме 16.2 $\|r\| < \|(x - a)\|$, и так как $\|(x - a)\| = 1$, то $\|r\| = 0$, то есть r - константа, следовательно

$$\begin{aligned} p(x) &= d(x)(x - a) + C \\ p(a) &= d(a)(a - a) + C \\ 0 &= 0 + C \end{aligned}$$

Следовательно $C = 0$, $p(x) = d(x)(x-a)$, а это и значит что $(x-a)|p(x)$ □

Определение 16.5 (Корень кратности)**.** a - корень кратности k многочлена $p(x)$, если $(x - a)^k|p(x)$

Определение 16.6 (Производная)**.** Пусть $p(x)$ - многочлен и $p(x) = \sum_{i=0}^{n} a_i x^i$ тогда его производная равна

$$p'(x) = \sum_{i=0}^{n} a_i \underbrace{1 + 1 + ... + 1}_{i} x^{i-1}$$

Теорема 16.7 (Свойства производных)**.** *Пусть $p(x), q(x) \in P[x]$, тогда*

1. $(p + q)' = p' + q'$
2. $(pq)' = p'q + pq'$

Теорема 16.8. *Пусть $p(x) \in P[x]$, $p(a) = 0$, $k - 1 \neq 0$, тогда a является корнем кратности степени k тогда и только тогда, когда является корнем кратности степени $k - 1$ производной этого многочлена.*

Доказательство. 1. Необходимость. Пусть a является корнем кратности степени k, тогда

$$p(x) = (x - a)^k q(x) \quad q(a) \neq 0$$

Найдём производную

$$\begin{aligned} p'(x) &= k(x - a)^{k-1} q(x) + (x - a)^k q'(x) \\ &= (x - a)^{k-1}(kq(x) + (x - a)q'(x)) \\ &= (x - a)^{k-1} S(x) \end{aligned}$$

подставляя в $S(x)$ вместо x a получаем

$$\begin{aligned} S(a) &= kq(a) + (a - a)q'(a) \\ &= kq(a) \\ &= \underbrace{q(a) + ...q(a)}_{k} \\ &= \underbrace{(1 + ... + 1)}_{k} q(a) \end{aligned}$$

Если $k \cdot 1 \neq 0$, то $k \cdot q(a) \neq 0$, следовательно a является корнем произаодной многочлена

$$p'(x) = (x - a)^{k-1} S(x)$$

2. Достаточность. Пусть $p(x) \in P[x]$ и a - корень кратности $k-1$ производной многочлена $p(x)$:

$$p'(x) = (x-a)^{k-1}s(x)$$

тогда

$$p(x) = (x-a)^m q(x) \quad q(a) \neq 0,\ m \geq 1$$

очевидно a является корнем кратности m. Найдём производную

$$\begin{aligned} p'(x) &= m(x-a)^{m-1} + (x-a)^m q'(x) = (x-a)^{k-1}s(x) \\ &= (x-a)^{m-1}(m \cdot q(x) + (x-a)q'(x)) \\ &= (x-a)^{k-1}s(x) \end{aligned}$$

Из этого следует что $m = k$, то есть a является корнем кратности k □

17 Простые поля, расширения полей, поле разложения многочлена

Определение 17.1 (Простое поле)**.** Поле - простое, если его подалгебры не являются полями

Определение 17.2 (Собственное подполе)**.**

Теорема 17.3. *Любое просто поле изоморфно либо рациональным числам или полю вычетов по простому числу, то есть F - простое поле, тогда $F \simeq Q$ или $F \simeq \mathbb{Z}_p$, где $p \in \mathbb{Z}$ - простое*

Доказательство. В поле есть 1, поэтому можно строить кратные суммы единиц $(1 + .. + 1)$. Строя такие суммы мы или никогда не получим 0 или получим

1. Никогда не получится 0, то есть $k \cdot 1 \neq 0\,(-(k \cdot 1) \neq 0)$ при $k > 0$.

   В поле для любого элемента есть обратный: $(k \cdot 1)^{-1}$ и $-(k \cdot 1)^{-1}$. В поле можно умножать: $(m \cdot 1)(k \cdot 1)^{-1}$. Так можно заметить что все элементы имеют вид

$$\begin{aligned} m \cdot 1 &= (m \cdot 1)(1 \cdot 1)^{-1} \\ k \cdot 1 &= (1 \cdot 1)(k \cdot 1)^{-1} \end{aligned}$$

Если $m \neq 0, k \neq 0$, то $(m \cdot 1)(k \cdot 1)^{-1} \neq 0$. Так как $\{(m \cdot 1)(k \cdot 1)^{-1}\}$ образует поле и F - простое, то $\{(m \cdot 1)(k \cdot 1)^{-1}\}$ образует всё поле.

Можно построить изоморфизм где $(m \cdot 1)(k \cdot 1)^{-1} \xrightarrow{\text{h}} \frac{m}{k}$. Покажем что это так. Сначала нужно доказать что это гомоморфизм:

Да, это гомоморфизм

Так как поле - это кольцо, для h существует $\operatorname{Ker} h$ и по 14.5 $\operatorname{Ker} h$ - идеал. Так как поле - тело, то по 14.9 существует только два идеала: F и $\{0\}$. Ядро гомоморфизма является одним из этих идеалов, и так как оно не может быть равно всему полю F оно равно $\{0\}$ Для того чтобы показать что h - изоморфизм, нужно показать что это инъекция и сюръекция

(a) Так как $\operatorname{Ker} h = \{0\}$ то по 14.7 h разнозначно
(b) для каждого образа $\frac{m}{k} \in \mathbb{Q}$ есть прообраз $(m \cdot 1)(k \cdot 1)^{-1} \in F$

Следовательно $F \simeq \mathbb{Q}$

2. $k \cdot 1 = 0$ для некоторого $k > 0$

Выберем наименьшее $k > 0$ для которого $k \cdot 1 = 0$. Мы можем получить элементы $0, 1, 2 \cdot 1, 3 \cdot 1, ..., (k-1) \cdot 1$. Докажем от противного что k должно быть простым:

Так как k не простое, то оно раскладывается $k = pq$, где $p, q > 1$, $p, q < k$.

$$0 = k \cdot 1 = (p \cdot 1)(q \cdot 1)$$

поскольку $p, q < k$, то

$$(p \cdot 1) \neq 0 \neq (q \cdot 1)$$

делители нуля. Противоречие, число не составное.

Возьмём $p = k$, $\mathbb{Z}_p = \{0, ..., p-1\}$ - это кольцо (ассоциативное, коммутативное, с единицей), остаётся проверить наличие обратного. Пусть $x \neq 0$ и $x \in \mathbb{Z}_p$, тогда $\text{НОД}(x, p) = 1$. Из этого следует что $nx + mp = 1$ для некоторых $n, m \in \mathbb{Z}_p$

$$\begin{aligned} nx + mp &= 1 \\ (nx + mp) \bmod p &= 1 \bmod p \\ nx \bmod p + mp \bmod p &= 1 \\ nx \bmod p &= 1 \\ n \bmod p \cdot x \bmod p &= 1 \\ n \bmod p \cdot x &= 1 \end{aligned}$$

$n \bmod p$ - обратный для произвольного x, соответственно $\mathbb{Z}_p$ - поле.

□

Следствие 17.4. *Внутри каждого поля есть простое подполе*

Доказательство. □

Определение 17.5 (Характеристика поля)**.** Для некоторого поля F его характеристика это

1. если $k \cdot 1 \neq 0$ для всех $k > 0$, то 0 - характеристика поля F
2. если $k \cdot 1 = 0$ для некоторого $k > 0$, то k - характеристика поля F (F - поле конечной характеристики)

Определение 17.6 (Неразложимый многочлен)**.** Неразложимый многочлен - многочлен, который не раскладывается на множители, ни один из которых не является многочленом нулевой степени.

Пример 17.7 (Пример неразложимого многочлена)**.**

Следствие 17.8. 1. *Многочлен 1 степени всегда неразложим*

2. *Многочлен 2 или 3 степени неразложим $\Leftrightarrow$ не имеет корней*
3. *Если многочлен степени большей 3 не разложим, то он не имеет корней*

Доказательство. □

Следствие 17.9. *Неразложимый многочлены - простые элементы кольца многочленов*

Доказательство. □

Теорема 17.10. *R - кольцо главных идеалов, c - простой элемент, тогда cR - простой идеал*

Доказательство. Пусть c - простой элемент, допустим что cR - не простой идеал, тогда найдутся $a, b \notin cR$ такие что $ab \in cR$. Сумма идеалов $dR = aR + cR$ - тоже идеал. Потом я не пойму ПОЧЕМУ. □

Теорема 17.11. *R - кольцо главных идеалов, I - простой идеал, тогда I - максимальный идеал*

Доказательство. Пусть дан простой идеал $I = cR$, дальше магия $\square$

Следствие 17.12. *Если p - неразложимый многочлен, тогда порождённый им идеал является максимальным*

Доказательство. Следует из двух предыдущих и 17.9 или из 15.11 и 17.9 $\square$

Следствие 17.13. $F[x] \Big/ \langle p \rangle$ *- поле*

Доказательство. Следует из того что факторкольцо по протому элементу - это поле, но здесь такой теоремы (пока) нет $\square$

Теорема 17.14. *Для каждого многочлена существует расширение поля, в котором он разложится на линейные множители.*

Доказательство. Пусть $p(x) \in P[x]$. Индукция по степени многочлена p:

Базис. $\deg p = 1$. $p(x) = ax + b$ - линейный, то есть уже разложен

Индукционный шаг. Предположим p раскладывается на два многочлена $p = q \cdot s$, тогда по индукционному предположению для этих многочленов существует поле где они разложатся.

Теперь предположим что p не раскладывается. Построим $F[y] \Big/ \langle p(y) \rangle = F'$ - расширение F. Это будет расширением потому что можно построить изоморфизм $h : F \to F'$, $h(y) = y + \langle p(y) \rangle$

Пусть $\alpha = y + \langle p(y) \rangle$ - корень многочлена p в F', тогда

$$\begin{aligned} p(y + \langle p(y) \rangle) &= \sum_{i=0}^{n} p_i (y + \langle p(y) \rangle)^i \\ &= \sum_{i=0}^{n} p_i (y^i + \langle p(y) \rangle) \\ &= (\sum_{i=0}^{n} p_i y^i) + \langle p(y) \rangle \\ &= p(y) + \langle p(y) \rangle \\ &= 0 \end{aligned}$$

действительно, $\alpha = y + \langle p(y) \rangle$ - корень многочлена p в F' $\square$

Пример 17.15 (Пример расширения поля)**.**

Следствие 17.16. *Если F - конечное поле, то поле расширений многочлена p тоже конечно*

Доказательство. По индукции □

Следствие 17.17. *Пусть $p \in P[x]$ и $\deg p = n$, тогда количество корней p с учётом кратности будет $\leq n$ и существует поле где оно равно n*

Доказательство. Пусть F' - расширение F, в над которым многочлен раскладывается на линейные множители. Тогда $p(x) = a_0(x-a_1)^{n_1}...(x-a_k)^{n_k}$. Если $\deg p = n$, то $n_1 + ...n_k = n$ □

18 Конечные поля

Определение 18.1 (Конечное поле)**.**

Следствие 18.2. *Конечные поля имеют конечную характеристику*

Доказательство.

$$\underbrace{1+...+1}_{n} = \underbrace{1+...+1}_{m} \qquad n = m$$

$$\underbrace{1+...+1}_{n} = 0$$

Что это вообще такое □

Теорема 18.3. *Если F - конечное поле характеристики p, то $|F| = p^k$*

Доказательство. Так как F - конечное поле $\mathbb{Z}_p \subseteq F$, тогда F - линейное пространство (почему это линейное пространство) над $\mathbb{Z}_p$, в таком случае имеется базис $e_1, ..., e_k$. Пусть $a \in F$б тогда

$$a = a_1e_1 + ... + a_ke_k \quad a_1, ..., a_k \in \mathbb{Z}_p$$

И так как $|\mathbb{Z}_p| = p$, то $|F| = p^k$ - количество комбинаций $a_1, ..., a_k$ □

Следствие 18.4. *Если $m \neq p$, то поля из m элементов не существует*

Доказательство. ??? □

Теорема 18.5 (Мечта школьника)**.** *Если F - поле характеристики p, то*

$$(x+y)^p = x^p + y^p$$

Доказательство. Пусть $x, y \in F$, тогда по формуле бинома ньютона

$$(x+y)^p = \sum_{i=0}^{p} C_p^i x^i y^{p-i}$$

Рассмотрим первый и последний элемент этой суммы. По формуле сочетания

$$C_p^0 = \frac{p!}{0!(p-0)!} = 1$$

$$C_p^p = \frac{p!}{p!(p-p)!} = 1$$

поэтому

$$\begin{aligned}(x+y)^p &= \sum_{i=0}^{p} C_p^i x^i y^{p-i} \\ &= C_p^0 x^0 y^p + \sum_{i=1}^{p-1} C_p^i x^i y^{p-i} + C_p^p x^p y^0 \\ &= y^p + \sum_{i=1}^{p-1} C_p^i x^i y^{p-i} + x^p\end{aligned}$$

Рассмотрим оставшуюся часть суммы, то есть для $i \neq 0 \neq p$. По формуле сочетания

$$C_p^i = \frac{p!}{i!(p-i)!} = p \cdot c_i \quad i \neq 0 \neq p$$

где c_i - некоторое число, зависимое от i. Подставляя C_p^i получаем

$$\sum_{i=1}^{p-1} C_p^i x^i y^{p-i} = \sum_{i=1}^{p-1} p c_i x^i y^{p-i} = \sum_{i=1}^{p-1} \underbrace{(1+\ldots+1)}_{p} c_i x^i y^{p-i} = 0$$

так как элемент $p \in F$ равен нулю. Таким образом

$$(x+y)^p = y^p + \sum_{i=1}^{p-1} C_p^i x^i y^{p-i} + x^p = x^p + y^p$$

□

Теорема 18.6. *Если F - поле характеристики p, то*

$$((x+y)^p)^k = (x^p)^k + (y^p)^k$$

Доказательство.

$$\begin{aligned}(x+y)^{p^k} &= ((x+y)^p)^{p^{k-1}} \\ &= (x^p + y^p)^{p^{k-1}} \\ &= ((x^p + y^p)^p)^{p^{k-2}} \\ &= ... \\ &= (x^{p^{k-1}} + y^{p^{k-1}})^{p^1} \\ &= x^{p^k} + y^{p^k}\end{aligned}$$

□

Теорема 18.7. *Если F - конечное поле и $|F| = m$, тогда существует корень уравнения типа $x^{m-1} - x$*

Доказательство. Пусть $F' = \{F \setminus \{0\}, \cdot, 1, -1\}$, F' является группой и $|F'| = m - 1$. Пусть $a \in F'$, тогда по 9.44

$$a^{m-1} = 1$$

То есть все ненулевые элементы группы удовлетворяют $x^{m-1} = 0$.

Так как $x^m - x = x(x^{m-1} - 1)$, то и нулевой элемент и ненулевые элементы являются корнями этого уравнения. □

Теорема 18.8. *Если существует поле F, такое что $|F| = p^k$, то существует поле F', такое что $|F'| = p^{k'}$, при любом $k' \leq k$*

Доказательство. Если $a|b$, то $(x^a - 1)|(x^b - 1)$ (как так). Предположим $b = ac$, то есть

$$x^b = (x^a)^c - 1 = (x^a - 1)((x^a)^{c-1} + (x^a)^{c-2} + ... + x^a + 1)$$

F - корни многочлена $x^{p^k} - x = x(x^{p^{k-1}} - 1)$

Что дальше в этой теореме? □

Что дальше в этой главе?