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

Определение 1.3 (Замкнутый терм)**. Замкнутый терм** - терм, не содержащий переменных

Определение 1.4. 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 1.2 (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 1.5 (Носитель алгебры)**.** $\mathbb{R}$ называется **основным множеством** или носителем алгебры, а I - интерпретацией или интерпретирующей функцией

Определение 1.6 (Состояние)**. Состояние** - функция, приписывающая переменной некоторый элемент носителя $\sigma : V \to A$

Пример 1.3. *Пример состояний:* $\sigma = \{(x, 3), (y, -8)\}, \sigma(x) = 3$

Определение 1.7 (Значение терма на состоянии)**.** Значение терма на состоянии - 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 1.8 (Изоморфизм)**. Изоморфизм** - Пусть Σ - сигнатура, $\mathcal{A} = (A, I)$, $\mathcal{B} = (B, J)$ - универсальные алгебры сигнатуры Σ, тогда изоморфизм между $\mathcal{A}$ и $\mathcal{B}$ - это $h : \mathcal{A} \to \mathcal{B}$ - 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 1.4 (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 1.1. 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 $b_1 = h(a_1), ..., b_{n_i} = h(a_{n_i})$,

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

По определению изоморфизма

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

Из этих двух равенств следует то, что надо доказать □

Определение 1.9. Системы, между которыми существует изоморфизм называют **изоморфными**

$$\mathcal{A} \simeq \mathcal{B}$$

операции в изоморфных системах обладают одними и теми же свойствами

Определение 1.10. $t(x_1, ..., x_n)$ - терм t не содержит других переменных кроме $x_1, ..., x_n$

Определение 1.11. Пусть $\mathcal{A}$ - алгебра, $a_1, ..., a_n$ - элементы алгебры $\mathcal{A}$, тогда

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

Теорема 1.2. *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. $t = x$
$$t^{\mathcal{A}}(a) = a \Leftrightarrow h(t^{\mathcal{A}}(a)) = h(a) \Leftrightarrow t^{\mathcal{B}}(h(a)) = h(a)$$

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

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

□

Пример 1.5. *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 1.6. *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) □

1.1

Пример 1.7. *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 1.8. *Доказать что* $\mathcal{A} = (\mathbb{Z}; \min^{(2)}) \ncong \mathcal{B} = (\mathbb{Z}; \max^{(2)})$
Доказательство.

□

Пример 1.9. *Доказать что* $\mathcal{A} = (\omega; +) \ncong \mathcal{B} = (\omega^{+}; \cdot)$
Доказательство.

□

Пример 1.10. *Доказать что* $\mathcal{A} = (\mathbb{Q}; +) \ncong \mathcal{B} = (\mathbb{Q}^{+}; \cdot)$
Доказательство.

□

Пример 1.11. *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 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 2.1 (Пример ограничения операции)**.**

Пример 2.2 (Пример подалгебры)**.** *Пример подалгебры:*

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

Доказательство.

□

Следствие 2.1. *Отношение "является подалгеброй"транзитивно*

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

Доказательство.

□

Теорема 2.1. *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 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 2.3 (Пример на 2.1)**.**

Теорема 2.2.
Доказательство.

□

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: $f(a * b) = f(a) \times f(b)$, $a, b \in G_1$.

Определение 3.2 (Мономорфизм). Инъективный (разнозначный) гомоморфизм

Пример 3.1 (Пример на мономорфизм).

Определение 3.3 (Эпиморфизм). сюръективный гомоморфизм

Пример 3.2 (Пример на Эпиморфизм).

Определение 3.4 (Изоморфизм). взаимно однозначный (биективный) гомоморфизм

Пример 3.3 (Пример на Изоморфизм).

Определение 3.5 (Эндоморфизм). гомоморфизм в само множество

Пример 3.4 (Пример на Эндоморфизм).

Определение 3.6 (Автоморфизм). взаимно однозначный гомоморфизм в само множество

Пример 3.5 (Пример на Автоморфизм).

Определение 3.7 (Гомоморфный образ). Образ гомоморфизма

Пример 3.6 (Пример на гомоморфный образ).

Определение 3.8 (Конгруэнтность). Отношение эквивалентности (рефликсивность, симметричность, транзитивность), сохраняющееся при основных операциях, то есть

$$a_1 \equiv a_2,\, b_1 \equiv b_2 \Rightarrow a_1 \cdot b_1 \equiv a_2 \cdot b_2$$

Определение 3.9 (Фактор-алгебра). Множество классов эквивалентности по отношению к конгруэнтности

4 Декартовы произведения, тождества, многообразия

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

Определение 5.1 (Полугруппа). Полугруппа - многообразие заданное множеством

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

Пример 5.1 (Примеры полугрупп)**.**

Теорема 5.1. *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

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

□

Определение 5.2 (Нейтральный элемент)**.** e_l называется **нейтральным слева** в полугруппе, если $e_l * a = a$ для всех a, e_r называется **нейтральным справа** в полугруппе, если $a * e_r = a$ для всех a, e - нейтральный слева и справа

Пример 5.2 (Примеры нейтрального элемента)**.** $(\omega, +)$ - 0, $(\omega, \cdot)$ - 1, (ω, max) - 0, (ω, min) - *нет нейтрального*

Теорема 5.2. *Если существуют нейтральный слева и нейтральный справа то они равны*

Доказательство.

$$e_l = e_l * e_r = e_r$$

□

Следствие 5.1. *Если нейтральный элемент существует, то он единственный.*

Определение 5.3 (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 5.3 (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 5.4 (Идемпотент)**.** Идемпотент - элемент моноида a, такой что $a^2 = a$

Пример 5.4 (Примеры идемпотентов)**.** $(\omega; +)$ - 0

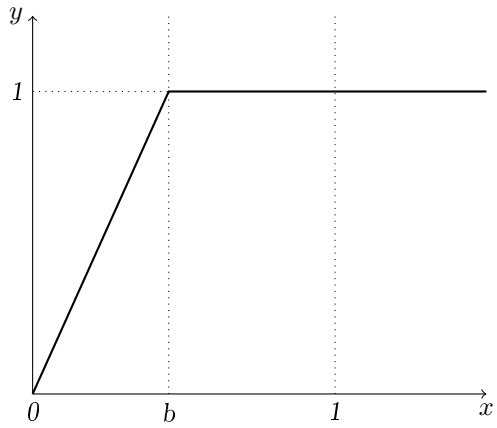
Определение 5.5 (Обратный элемент)**.**

b_l - левый обратный для элемента a, если $b_l * a = e$,
b_r - правый обратный для элемента a, если $a * b_l = e$,
b - обратный для элемента a, если $b * a = a * b = e$

Определение 5.6 (Обратимый элемент)**.** Элемент, для которого существует обратный

Пример 5.5. *Пример чего-то: 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 5.6 (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 5.7 (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 5.8 (Построение моноидов)**.** *Построить все моноиды из двух элементов* $\{e,x\}$

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

Таблица умножения $(*_1)$

	e	x
e	e	x
x	x	e

Таблица умножения $(*_2)$

	e	x
e	e	x
x	x	x

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

1. $a = e$
$$e*(b*c) = b*c = (e*b)*c$$
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 5.3. *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 5.7 (Сократимый элемент)**.** Сократимый слева (справа) - такой элемент моноида, что из $ax = ay$ $(xa = ya)$ следует $x = y$

Пример 5.9 (Пример сократимого элемента)**.** $(\mathbb{Z}, +, 0)$, $x + a = y + a \Rightarrow x = y$

Теорема 5.4. *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 5.5. *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 5.10 (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 6.1. *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 6.1 (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 6.2 (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 6.2 (Пример циклического моноида)**.** $< a >= (\{e, a, ...\}; *)$

Таблица умножения $(*)$ -

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

Теорема 6.2. *Если j - наименьшее число такое что $a^i = a^j$ для какого-то $i < j$, то $< a >$ содержит ровно j элементов*

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

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

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

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

□

Определение 6.3 (Моноид типа $(i, j-i)$)**.** Моноид типа $(i, j-i)$ - моноид с элементами

???

Теорема 6.3. *В моноиде типа $(i, j-i)$, где $i > 0$ существует идемпотент $b \neq e$*
Доказательство.

□

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 7.1. *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 7.3 (Абелева группа)**.** Абелева группа - группа, в которой $xy = yx$

Определение 7.4 (Циклическая группа)**.**

Теорема 7.2 (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:

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

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

$(a, b) \equiv (c, d) \Leftrightarrow ad = bc$ - 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 7.1 (Пример на теорему Гротендика)**.**

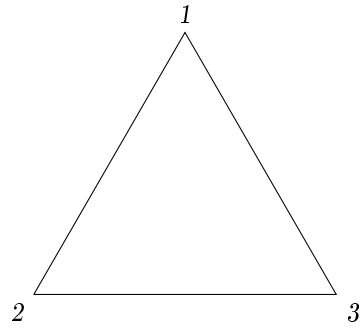
8 Группы перестановок, задание групп определяющими соотношениями.

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

Пример 8.1 (Пример группы перестановок)**.**

Определение 8.2 (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 8.2 (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

Пример 8.3 (задание групп определяющими соотношениями)**.**

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 9.1. *Подгруппа является группой*

Определение 9.2 (Тривиальная подгруппа)**.** Тривиальная подгруппа - подгруппа, состоящая только из одного нейтрального элемента группы или равна самой группе

Пример 9.1 (Пример подгрупп)**.**

Пример 9.2. $(\mathbb{Z}_p; +, 0, -)$, 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 9.1. *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 9.3 (Пример подгрупп)**.** *Возьмём группу из 8.2 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 9.4. *Группа операций над треугольником - подгруппа*

Пример 9.5. *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 $(\mathcal{A}; \dot{-})$, где $\mathcal{A}$ - множество фигур на плоскости.*
Доказательство. Сперва докажем ассоциативность $\dot{-}$: $A \dot{-} (B \dot{-} C) = (A \dot{-} B) \dot{-} C$
$A \dot{-} B = (\overline{A} \cap B) \cup (\overline{B} \cap A)$

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

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

$$A \div (B \div C) = (A \div B) \div C$$

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

Пример 9.6. *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 9.7. *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 9.3 (Рекурсивная перестановка)**.** Рекурсивная перестановка - разнозначная общерекурсивная функция, область значений которой - множество ω

Теорема 9.2. *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 9.3. *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 9.4. *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 9.8. *Построить группу симметричную чему-то там*

Теорема 9.5. *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 9.6. *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 9.4 (Центр группы)**.** Центр группы - $\mathcal{Z} = \{a \in G, ab = ba$ для всех $b \in G\}$

Пример 9.9. $\mathcal{M} = (M_2^*(\mathbb{R}); \cdot)$, *невырожденные матрицы*

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

Теорема 9.7. *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 9.5 (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 9.8. *$\mathcal{G} = \langle a \rangle$, 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 9.9. *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 9.6 (Порядок группы)**.** Порядок группы - количество элементов группы. $ord\mathcal{G}$

Определение 9.7 (Порядок элемента)**.** Порядок элемента - порядок порождённой им циклической подгруппы $orda = ord\langle a\rangle$

Пример 9.10. *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 9.2. $\operatorname{ord} e = 1$, $\langle e\rangle = \{e\}$

Определение 9.8 (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 9.11. *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 9.9 (Нормальная подгруппа)**.** Нормальная подгруппа - подгруппа, у которой любой левый смежный класс совпадает с правым

Пример 9.12. *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 9.10. *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 9.3. *Каждый левый смежный класс является классом эквивалентности*

Следствие 9.4. *Левые смежные классы или совпадают или не пересекаются*

Следствие 9.5. *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 9.10 (Индекс подгруппы)**.** Индекс подгруппы - количество левых смежных классов $\operatorname{ind} H$

Теорема 9.11. *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 9.6. $\operatorname{ind} H = \dfrac{\operatorname{ord} G}{\operatorname{ord} H}$

Следствие 9.7. $\operatorname{ord} H | \operatorname{ord} G$

Следствие 9.8. $\operatorname{ord} a | \operatorname{ord}\mathcal{G}$
Доказательство. $\mathcal{H} = \langle a\rangle$, $\operatorname{ord} a = \operatorname{ord}\mathcal{H}$

□

Теорема 9.12. $a^{\operatorname{ord} a} = e$
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 9.13. $a^n = e \Leftrightarrow \operatorname{ord} a | n$
Доказательство. Пусть $x = \operatorname{ord} a + r = n$, $(0 \le r < \operatorname{ord} a)$, 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 9.14. $a^{\operatorname{ord} G} = e$
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 9.13. *$\mathcal{A}_5$ - группа чётных перестановок из 5 элементов. В $\mathcal{A}_5$ нет нормальных подгрупп*
Доказательство. ДОКАЖИ ДОМА)))))))))))))))) □

Теорема 9.15. *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) $\mathcal{H}a \neq \mathcal{H}$
   $\mathcal{H}a = \mathcal{G}/\mathcal{H}$

□

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 10.1. *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 10.1. *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 10.2 (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 10.2. *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, $a \cdot b \cdot h \cdot h_b \in abH$. □

Теорема 10.3. *Если G и H - группа, $h : G \to H$ и $h(a * b) = h(a) * h(b)$, то h - гомоморфизм*
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 10.3 (Порождённая конгруэнтность)**.** Конгруэнтность порождённая h - если $a \equiv b \Leftrightarrow h(a) = h(b)$ - конгруэнтность, то $h[A] = {}^{A}/_{\equiv}$

Теорема 10.4. *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 10.4 (Ядро подгруппы)**.** Ядро подгруппы - множество элементов эквивалентных e. $\operatorname{Ker} h$

Теорема 10.5. *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 10.5 (щито)**.** $\mathcal{G}$ - группа, $\mathcal{H}$ - нормальная подгруппа, $\equiv$ - отношение конгруэнтности. Тогда $\mathcal{G}/_{\equiv} = \mathcal{G}/_{\mathcal{H}}$

Следствие 10.1. *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 10.2.

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

$\langle r_1 \rangle$ - *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 10.3. $(\mathbb{R}, +) \supseteq (\mathbb{Z}, +)$
$a + \mathbb{Z}$
$ba \in \mathbb{Z}$

$a + \mathbb{Z} = b + \mathbb{Z}$
$a \in [0, 1)$
$(a + \mathbb{Z}) + (b + \mathbb{Z}) = (a + b) = (a + b) \mod 1$
$\mathbb{C}_1 = \{z \in \mathbb{C}, |z| = 1\}$, $(\mathbb{C}_1, \cdot)$
$h(x) = e^{2nix}$
$x \in \mathbb{R} = e^{2nix} \in \mathbb{C}_1$
$h(x + y) = e^{2ni(x+y)} = e^{2nix} e^{2niy} = h(x)h(y)$
$h : (\mathbb{R}, +) \to (\mathbb{C}, \cdot)$
$r \in \operatorname{Ker} h \Leftrightarrow r \equiv e$
$h(r) = h(e)$
$h(r) = h(0)$
$e^{2nix} = e^{2nix} = 1$
$e^{2nix} = 2n \cdot k, k \in \mathbb{Z}$
$r \in \mathbb{Z}$
$\operatorname{Ker} h \in \mathbb{Z}$

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

Определение 11.2. 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 11.2.

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

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

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

$\mathcal{H}$ *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

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

$s_1 ... s_1 r_1 ... r_1$

$s_1^n r_1^m$

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

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

r_1^0	$s_1 r_1^0$
r_1^0	$s_1 r_1^0$
r_1^0	$s_1 r_1^0$

Теорема 11.1. *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 11.3. *Про пирамиду рубика. Конём.*

Пример 11.4. *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 11.5. *Таблица 8x8. Конём.*

Пример 11.6. $Z = 1, -1$

Пример 11.7.

Пример 11.8.

Пример 11.9.

Пример 11.10.

Определение 11.3. Если $X = \emptyset$, то $M/_{\equiv}$ - свободная группа порождённая A

Следствие 11.1. *Любая группа порождённая A - гомоморфный образ свободной группы*

Определение 11.4. $\mathcal{G}$ - 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 11.11. *$\mathcal{G}$ действует на себя правыми умножениями*

Определение 11.5. Сопряжение - действие группы $\mathcal{G}$ на себя или множество подмножеств $P(\mathcal{G}) : h(S, a) = a^{-1}Sa$

Теорема 11.2. *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 11.3. *Любая подгруппа при сопряжении переходит в подгруппу*
Доказательство. Пусть A - подгруппа $\mathcal{G}$ □

Теорема 11.4. *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 11.6 (Стабилизатор)**.** $\mathcal{G}$ действует на S, $s \in S$. Стабилизатор s - $\operatorname{stab} s = \{a \in \mathcal{G}, h(s,a) = s\}$

Теорема 11.5. $\operatorname{stab} s$ - *подгруппа* $\mathcal{G}$
Доказательство. пусть $b, c \in \operatorname{stab} s$, тогда □

Определение 11.7 (Орбита)**.** Пусть G действует на S, $s \in S$. Орбита s - $\operatorname{orb} s = \{sa : a \in G\}$

Теорема 11.6. *Орбиты - классы эквивалентности*

Теорема 11.7. *Количество элементов орбиты равняется индексу стабилизатора*

Теорема 11.8 (Формула орбит)**.** *G действует на множестве S, тогда* $|S| = \sum\limits_{орбиты} \dfrac{\operatorname{ord} G}{\operatorname{ord} q_0}$

Следствие 11.2. *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

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

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 12.1 (Примеры колец)**.**

Теорема 12.1. *Для любых элементов кольца a, b справедливы следующие утверждения:*

1. $a0 = 0a = 0$
2. $(-a)b = a(-b) = -(ab)$

Доказательство.

□

Следствие 12.1. *В кольце с 1 ноль необратим.*

Определение 12.8 (Делитель нуля)**.** Пусть $a \cdot b = 0\, a, b \neq 0$, тогда a - левый делитель нуля, b - правый делитель нуля.

Пример 12.2 (Пример делителей нуля)**.**

Теорема 12.2. *Делители нуля необратимы*
Доказательство.

□

Определение 12.9 (Идемпотент кольца)**.** Такие элементы кольца, для которых выполняется $a = a^2$

Теорема 12.3. *Идемпотенты - делители нуля*
Доказательство.

□

Определение 12.10 (Тело кватернионов)**.**

13 Целостные кольца, вложение кольца в поле

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

Теорема 13.1. *Конечное целое кольцо ?????*
Доказательство.

□

Теорема 13.2. *Каждое целостное кольцо может быть достроено до поля*
Доказательство.

□

14 Гомоморфизмы колец, идеалы, факторкольца

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 14.1. *Ядро кольца - подкольцо*

Определение 14.3 (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)

Пример 14.1 (Пример идеалов)**.**

Теорема 14.2. *R - ассоциативное кольцо с единицей или R - тело или R тогда и только тогда когда в R Нет других идеалов, кроме $\{0\}$ и R*

Определение 14.4 (Булевое кольцо)**.**

Теорема 14.3. *Пусть I - двухсторонний идеал в R, тогда отношение $\equiv$: $x \equiv y \Leftrightarrow x - y \in I$ является конгруэнтностью*
Доказательство.

□

Следствие 14.1. *Существует фактор-алгебра $R/_{\equiv}$, такая что ???*

Следствие 14.2. *$I = \operatorname{Ker} h$, где $h : R \to R/_{\equiv}$*
Доказательство.

□

Определение 14.5 (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 14.6 (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 14.7 (Главный идеал)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда I - главный идеал, если для некоторого $a \in R$ $I = aR$

Пример 14.2 (??????)**.**

Лемма 14.1. *Если I и J - идеалы, то $I + J$ тоже идеал*
Доказательство.

□

Теорема 14.4. *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 15.1. *Каждое евклидово кольцо - кольцо главных идеалов*
Доказательство.

□

Теорема 15.2. *В кольце главных идеалов не существует бесконечно возрастающей цепи идеалов*

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

Доказательство.

□

Определение 15.4 (Простой элемент)**.** Пусть R - ассоциативное, коммутативное кольцо с единицей, тогда a - простой, если из $a = bc$ следует что b или c обратимы

Определение 15.5 (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 $a =$

Теорема 15.3. *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.

□

Теорема 15.4. *пусть R - целостное кольцо главных идеалов, тогда R - факториальное*
Доказательство.

□

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

Определение 16.2 (Корень многочлена)**.**

Теорема 16.2 (Теорема Безу)**.** *Если a - корень многочлена p, то $(x - a)|p(x)$*

Определение 16.3 (Корень кратности)**.** a - корень кратности k многочлена $p(x)$, если $(x - a)^k | p(x)$

Определение 16.4 (Производная)**.** Пусть $p(x)$ - многочлен и $p(x) = \sum_{i=0}^{n} a_i x^i$ тогда его производная равна

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

17 Простые поля, расширения полей, поле разложения многочлена

Определение 17.1 (Простое поле)**.** Поле -простое, если оно не содержит собственных подполей

Определение 17.2 (Собственное подполе)**.**

Теорема 17.1. *F - простое поле, тогда $F \simeq Q$ или $F \simeq \mathcal{Z}_p$*
Доказательство.

□

Следствие 17.1. *Внутри каждого поля есть простое подполе*
Доказательство.

□

Определение 17.3 (Характеристика поля)**.**

Определение 17.4 (Неразложимый многочлен)**.** Неразложимый многочлен - многочлен, который не раскладывается на множители

Следствие 17.2. *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*

Следствие 17.3. *Неразложимый многочлены - простые элементы кольца многочленов*

Теорема 17.2. *R - кольцо главных идеалов, c - простой элемент, тогда cR - простой идеал*

Следствие 17.4. *Если p - неразложимый многочлен, тогда порождёный им мдеал является максимальным*

Следствие 17.5. $F(x) \Big/ \langle p \rangle$ *- поле*

Теорема 17.3. *Для каждого многочлена существует расширение поля, в котором он разложится на линейные множители.*
Доказательство.

□

Следствие 17.6. *Если F - конечное поле, то поле расширений многочлена p тоже конечно*

Следствие 17.7. $degp = n$
Доказательство.

□

18 Конечные поля

Определение 18.1 (Конечное поле)**.**

Следствие 18.1. *Конечные поля имеют конечную характеристику*

Теорема 18.1. *Если F - конечное поле характеристики p, то $|F| = p^k$*
Доказательство.

□

Следствие 18.2. *Если $m \neq p$, ТО поля из m элементов не существует*

Теорема 18.2. *Если F - поле характеристики p, то*

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

Доказательство.

□

Теорема 18.3. *Если F - поле характеристики p, то*

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

Доказательство.

□

Теорема 18.4. *Если F - конечное поле и $|F| = m$, тогда существует корень уравнения типа $x^m - 1$*
Доказательство. Если в один миг Яблочный спас Узнаем всё что есть Засияет тьма □