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

Определение 1.1 (Полугруппа)**.** Полугруппа - многообразие заданное множеством

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

Пример 1.2 (Примеры полугрупп)**.**

Теорема 1.3. *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 1.4 (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 1.5. $a^{n+m} = a^n a^m$

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

Теорема 1.6. *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 1.7 (Нейтральный слева)**.** e_l называется нейтральным слева в полугруппе, если $e_l * a = a$ для всех a,

Определение 1.8 (Нейтральный справа)**.** e_r называется нейтральным справа в полугруппе, если $a * e_r = a$ для всех a,

Определение 1.9 (Нейтральный элемент)**.** e - нейтральный слева и справа

Пример 1.10 (Примеры нейтрального элемента)**.** $(\omega, +)$ - 0, $(\omega, \cdot)$ - 1, (ω, max) - 0, (ω, min) - *нет нейтрального*

Теорема 1.11. *Если существуют нейтральный слева и нейтральный справа то они равны*

Доказательство.

$$e_l = e_l * e_r = e_r$$

□

Следствие 1.12. *Если нейтральный элемент существует, то он единственный.*

Определение 1.13 (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 1.14 (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

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

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

Пример 1.16 (Примеры идемпотентов)**.** $(\omega; +)$ - 0

Определение 1.17 (Левый обратный элемент)**.** b_l - левый обратный для элемента a, если $b_l * a = e$

Определение 1.18 (Правый обратный элемент)**.** b_r - правый обратный для элемента a, если $a * b_l = e$

Определение 1.19 (Обратный элемент)**.** b - обратный для элемента a, если $b * a = a * b = e$

Определение 1.20 (Обратимый элемент)**.** Элемент, для которого существует обратный

Теорема 1.21. *Если a обратим слева и справа, то он обратим и обратный элемент является единственным.*

Доказательство.

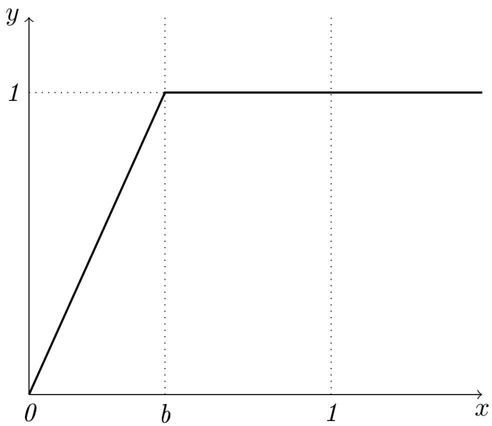
$$b_l a = e, \quad ab_r = e$$

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

□

Пример 1.22. *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 1.23 (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 1.24 (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 1.25 (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 1.26. *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 1.27 (Сократимый элемент)**.** Сократимый слева (справа) - такой элемент моноида, что из $ax = ay$ ($xa = ya$) следует $x = y$

Пример 1.28 (Пример сократимого элемента)**.** $(\mathbb{Z}, +, 0)$, $x + a = y + a \Rightarrow x = y$

Теорема 1.29. *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 1.30. *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 $\square$

Пример 1.31 (Пример обратимого элемента)**.** $(\mathbb{Z}^+, \cdot, 1)$, *обратимый только* 1, *сократимы все. (Какой к половым органам это пример?)*