1 Основные понятия

Определение 1.1:
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 - выражение, составленное из символов сигнатуры и переменных

1. $x \in V$, x - терм
2. c - символ константы, с - 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 - 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

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

Определение 1.5:
$\mathbb{R}$ называется **основным множеством** или носителем алгебры, а I - интерпретацией или интерпретирующей функцией

Определение 1.6:
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 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 $\sigma(t) = I(f)(v_1, ..., v_n)$

2 Изоморфизм

Определение 2.1:
Изоморфизм - Пусть Σ - сигнатура, $\mathbf{A} = (A, I)$, $\mathbf{B} = (B, J)$ - универсальные алгебры сигнатуры Σ, тогда изоморфизм между $\mathbf{A}$ и $\mathbf{B}$ - это $h : \mathbf{A} \to \mathbf{B}$ - 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 2.1:
Пример изоморфизма: пусть $\Sigma = (f^{(2)})$, $\mathbf{A} = (\mathbb{R}, +)$, $\mathbf{B} = (\mathbb{R}, \cdot)$

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 2.1. *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 2.2:
Системы, между которыми существует изоморфизм называют **изоморфными**

$$\mathbf{A} \simeq \mathbf{B}$$

операции в изоморфных системах обладают одними и теми же свойствами

Определение 2.3:
$t(x_1, ..., x_n)$ - терм t не содержит других переменных кроме $x_1, ..., x_n$

Определение 2.4:
Пусть $\mathbf{A}$ - алгебра, $a_1, ..., a_n$ - элементы алгебры $\mathbf{A}$, тогда

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

Теорема 2.2. *h - изоморфизм между $\mathbf{A} = (A, I)$ и $\mathbf{B} = (B, J)$, то для любого терма $t(x_1, ..., x_n)$ и любых $a_1, ..., a_n$ выполняется*

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

Доказательство. Индукция по построению терма t

1. $t = x$
$$t^{\mathbf{A}}(a) = a \Leftrightarrow h(t^{\mathbf{A}}(a)) = h(a) \Leftrightarrow t^{\mathbf{B}}(h(a)) = h(a)$$

2. $t = c$
$$\sigma(c) = I(c) = J(c) \Rightarrow t^{\mathbf{A}} = I(c), t^{\mathbf{B}} = J(c) \Rightarrow h(I(c)) = J(c)$$
по определению гомоморфизма

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

□

Пример 2.2:
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 2.3:
Доказать что $\mathcal{A} = (\mathbb{R}; +) \ncong \mathcal{B} = (\mathbb{R}; \cdot)$

Доказательство. Предположим что существует изоморфизм $h : \mathcal{B} \to \mathcal{A}$, тогда
$h(0) = x, h(1) = y; x, y \in \mathbb{R}$ □

3 Подгруппы и моноиды

Определение 3.1:
Подгруппа - многообразие заданное множеством

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

Теорема 3.1. *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. $1 \leq m \leq n - 1$
$$t = t_1 * t_2 = (a_1 a_2 ... a_m)(a_{m+1} ... a_n) = (a_1 a_2 ... a_m)(a_{m+1} ... a_{n-1}) a_n = (a_1 a_2 ... a_{n-1}) a_n = a_1 a_2 ... a_n$$

□

Определение 3.2:
e_l называется **нейтральным слева** в подгруппе, если $e_l * a = a$ для всех a, e_r называется **нейтральным справа** в подгруппе, если $a * e_r = a$ для всех a, e - нейтральный слева и справа

Пример 3.1:
Примеры нейтрального элемента:

Теорема 3.2. *Если существуют нейтральный слева и нейтральный справа то они равны*

Доказательство.
$$e_l = e_l * e_r = e_r$$

□

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

Определение 3.3:
Моноид - подгруппа с нейтральным элементом

Пример 3.2:
Примеры моноидов:

Определение 3.4:
Свободный моноид - моноид, элементами которого являются конечные последовательности (строки) элементов носителя моноида. Свободный моноид на множестве $A \neq \emptyset$ это $\mathcal{A} = (A^*; \&)$

Теорема 3.3. *Любой моноид, порождённый элементами множества, на котором есть свободный моноид, является гомоморфным образом этого моноида*

Доказательство. Пусть $A \neq \emptyset$, $\mathcal{A} = (A^*; \&)$,
$\mathcal{B} = (\left\{t^{\mathcal{B}}(a_1, ..., a_n) : a_1, ..., a_n \in A\right\}; *)$ 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 $h(u \& v) = h(u) * h(v)$ $\square$

Пример 3.3:
Примеры свободных моноидов и их гомоморфных образов:

Определение 3.5:
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

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

Пример 3.4:
Пример циклическокококого моноида: $< a >= (\{e, a, ...\}; *)$

Таблица умножения $(*)$ -

2.1

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