# Алгебраические структуры

ЧАСТЬ 3

- Алгебраические методы описания моделей находят самое широкое применение при формализации различных предметных областей.

- Грубо говоря, при построении модели предметной области все начинается с введения подходящих обозначений для операций и отношений с последующим исследованием их свойств.

- Владение алгебраической терминологией, таким образом, входит в арсенал средств, необходимых для абстрактного моделирования, предшествующего практическому программированию задач конкретной предметной области.

# Операции и алгебры

- Всюду определенная (тотальная) функция $f: M^n \to M$ называется *n-арной (n-местной) операцией* на *M.*

- Если операция *f*— бинарная (то есть $f: M \times M \to M$), то будем писать *afb* вместо *f(a, b)* или *a* o *b,* где o — знак операции.

- множество $M$ вместе с набором операций

$\sum = \{f_1, \ldots, f_m\}$, $f_i : M^{ni} \rightarrow M$, где $n_i$ — арность операции $f_i$, называется ***алгебраической структурой***, ***универсальной алгеброй*** или просто ***алгеброй***.

- множество $M$ называется ***основным*** *(несущим)* множеством, или ***основой*** *(носителем);*
- вектор арностей $(n_1,\ldots,n_m)$ называется ***типом;***
- множество операций $\sum$ называется ***сигнатурой;***
- запись: <M; $\sum$>

- Если в качестве $f_i$ допускаются не только функции, но и отношения, то множество *M* вместе с набором операций и отношений называется ***моделью***.
- *В приложениях обычно используется следующее обобщение понятия алгебры.*
- *Пусть* $M = \{M_i, \dots, M_n\}$— множество ***основ***, ∑ = {f1,. . . ,fm},— ***сигнатура***, причем $f_i : M_{i1} \times \dots \times M_{in} \to m_j$. Тогда <*M*; ∑> называется *многоосновной алгеброй*.

## Другими

Многоосновная алгебра имеет несколько носителей, а каждая операция сигнатуры действует из прямого произведения некоторых носителей в некоторый носитель.

# Замыкания и подалгебры

Подмножество $X \subset M$ называется ***замкнутым*** относительно операции $f$, если $\forall\ x_1, \ldots, x_n \in X$, *если* $X$ замкнуто относительно всех $X$ $f \in X$, *то* $\langle X; ?_x \rangle$ называется *подалгеброй* $\langle M;? \rangle$

Приме

Алгебра $\langle R; +, \cdot \rangle$ - *поле действительных чисел.* Тип – (2,2). Все конечные подмножества, кроме {0}, не замкнуты относительно обеих операция. *Поле рациональных чисел* $\langle Q; +, \cdot \rangle$ образует подалгебру.

1. Алгебра $< 2^M; \cup, \cap, \neg >$ - *алгебра подмножеств* над множеством M. Тип –(2, 2, 1). При этом $< 2^x; \cup, \cap, \neg >$ для любого подмножества X множества M образует подалгебру.

2. Алгебра $\{\{f \mid f: R > R\}; \frac{d}{dx}\}$, где ^ - операция дифференцирования. Множество элементарных функций образует подалгебру.

## ТЕОРЕМА

*Непустое пересечение подалгебр образует подалгебру.*

*Замыканием множества* $X \subset M$ относительно сигнатуры $\sum$ (обозначается $[X]_\Sigma$) называется множество всех элементов (включая сами элементы *X),* которые можно получить из *X,* применяя операции из $\sum$. Если сигнатура подразумевается, ее можно не указывать.

## ТЕОРЕМА

*Непустое пересечение подалгебр образует, подалгебру.*

*Замыканием множества X включенного в M* относительно сигнатуры $\sum$ (обозначается $[X]_{\sum}$ ) называется множество всех элементов (включая сами элементы *X),* которые можно получить из *X,* применяя операции из $\sum$. Если сигнатура подразумевается, ее можно не указывать.

## Пример

В алгебре *целых чисел* <Z; +, •> замыканием числа 2 являются четные числа.

## Свойства замыкания:

*I.* $X \subset Y=[X] \subset [Y];$ .

*2.* $X \subset [X];$

*3.* $[[X]] = [X];$

*4.* $[X] \cup [Y] \subset [X \cup Y].$

- Пусть заданы сигнатура $\sum = (\phi_1, \ldots, \phi_m)$ типа $N = (n_1, \ldots, n_m)$ и множество переменных $V = \{x_1, x_2, \ldots\}$. Определим множество *термов* $T$ в сигнатуре $\sum$ следующим образом:
  1. $V \subset T$;
  2. $t_1, \ldots, t_{ni} \in T \;\&\; \phi_i \in \sum \Rightarrow \phi(t_1, \ldots, t_{ni}) \in T$.

- Алгебра $\langle T; \sum \rangle$ называется *свободной алгеброй термов*, или *$\sum$-алгеброй.*
- Носителем $\sum$-алгебры является множество термов, то есть формальных выражений, построенных с помощью знаков операция сигнатуры $\sum$. Таким образом, с $\sum$-алгеброй не связано никакое конкретное множество, являющееся носителем. Поэтому $\sum$-алгебры используются в программировании для определения абстрактных типов данных.

# Свойства операций

Некоторые часто встречающиеся свойства операция имеют специальные названия. Пусть задана алгебра $\langle M;\sum\rangle$ и $a, b, c \in M$; $\circ,\lozenge \in \sum$; $\circ,\lozenge: M \times M \to M$.
Тогда:

1. *Ассоциативность:* $(a\circ b)\circ c = a\circ(b\circ c);$
2. *Коммутативность:* $a\circ b = b\circ a;$
3. *Дистрибутивность* слева: $a\lozenge(b\circ c) = (a\lozenge b)\circ(a\lozenge c);$
4. *Дистрибутивность* справа: $(a\circ b)\lozenge c = (a\lozenge c)\circ(b\lozenge c);$
5. *Поглощение:* $(a\circ b)\lozenge a = a;$
6. *Идемпотентность:* $a\circ a = a.$

## Морфизмы

Понятие изоморфизма, введенное в этом разделе, является одним из ключевых.

## Гомоморфизм

Алгебры с различными типами имеют различное *строение*.

Пусть $A = \langle A; \phi_1, \ldots, \phi_m \rangle$ и $B = \langle B; \psi_1, \ldots, \psi_m \rangle$ - две алгебры одинакового типа. Если существует функция $f$: $A \to B$, такая что $\forall\ i \in 1..m\ f(\phi_i(a_1, \ldots, a_n)) = \psi_I(f(a_1), \ldots, f(a_n))$, то говорят,
что $f$ – *гомоморфизм* из $A$ в $B$.

## Пример

$A = \langle N; + \rangle$, $B = \langle N_{10}; +_{10} \rangle$, где $N_{10} = \{0,1,2,3,4,5,6,7,8,9\}$, а $+_{10}$ сложение по модулю 10.
Тогда $f$: = a mod 10 – гомоморфизм из $A$ в $B$.

**Гомоморфизмы**, обладающие дополнительными свойствами, имеют специальные названия:

- Гомоморфизм, который является **инъекцией**, называется ***мономорфизмом***.
- Гомоморфизм, который является **сюръекцией**, называется ***эпиморфизмом*** *(или* ***эпиоморфизмом****).*
- Гомоморфизм, который является **биекцией**, называется ***изоморфизмом****.*
- Если A=B,
  то гомоморфизм называется ***эндоморфизмом***,
  а изоморфизм называется ***автоморфизмом****.*

# Изоморфизм

Пусть $A = \langle A; \phi_1, \ldots, \phi_m \rangle$ и $B = \langle B; \psi_1, \ldots, \psi_m \rangle$ - две алгебры одинакового типа., и $f$: $A \to B$ – изоморфизм.

**ТЕОРЕМА**

*Если $f$: $A \to B$ – изоморфизм,* то $f^{-1}$: $B \to A$ тоже *изоморфизм.*

*Если $f$: $A \to B$ – изоморфизм, то алгебры $A$ и $B$ называют изоморфными и обозначают так $A \overset{f}{\sim} B$.*

## ТЕОРЕМА

*Отношение изоморфизма на множестве однотипных алгебр является эквивалентностью.*

1. Рефлексивность: $A \overset{f}{\sim} A$, $f := \mathrm{I}$.
2. Симметричность: $A \overset{f}{\sim} B \Rightarrow B \overset{f^{-1}}{\sim} A$.
3. Транзитивность: $A \overset{f}{\sim} B \;\&\; B \overset{g}{\sim} g \Rightarrow A \overset{f \circ g}{\sim} g$.

## Пример

1. Пусть $A = \langle N; + \rangle$, $B = \langle \{n | n = 2k, k \in N\}; + \rangle$ - *четные числа*. Тогда $A \overset{x2}{\simeq} B$.
2. $A = \langle 2^M; \cap, \cup \rangle \overset{f}{\simeq} B = \langle 2^M; \cap, \cup \rangle$, $f(X) = \overline{X}$.
3. $A = \langle R_+; \cdot \rangle \overset{ln}{\simeq} B = \langle R; + \rangle$.

- Понятие изоморфизма является одним из центральных понятий, обеспечивающих применимость алгебраических методов в различных областях.
- Алгебраические структуры принято рассматривать *с точностью до изоморфизма*, то есть рассматривать классы эквивалентности по отношению изоморфизма.

# Алгебры с одной

Естественно начать изучение алгебраических структур с наиболее простых.

Самой простой структурой является алгебра с одной унарной операцией, но этот случай настолько тривиален, что про него нечего сказать.

Следующим по порядку является случай алгебры с одной бинарной операцией

$$\circ : M \times M \longrightarrow M$$

# Полугруппы

*Полугруппа* — это алгебра с одной ассоциативной бинарной операцией:

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

Пример

Множество слов A+ в алфавите A образует полугруппу относительно операции конкатенации.
Всякое множество функций, замкнутое относительно суперпозиции, является полугруппой.

Если в полугруппе существует система образующих, состоящая из одного элемента, то такая полугруппа называется *циклической.*

Пример

(N; +) является циклической полугруппой, поскольку {1} является системой образующих.

# Моноиды

*Моноид* — это полугруппа с *единицей:*

$$\exists\ e\ \forall\ a\ \ a \circ e = e \circ a = a.$$

Пример

1. Множество слов A* в алфавите A вместе с пустым словом Λ образуют моноид.
2. Пусть T – множество термов над множеством переменных V и сигнатурой Σ. *Подстановкой*, или *заменой переменных*, называется множество пар

$$\sigma = \{t_i // v_i\}_{i \in I},$$

где $t_i$ – термы, а $v_i$ – переменные, причем $v_i \notin t_i$. Результатом применения подстановки σ к терму $t$ (обозначается $t\sigma$) называется терм, который получается заменой *всех* вхождений переменных $v_i$ на соответствующие термы $t_i$.

- *Композицией* подстановок $\sigma_1 = \{t_i//v_i\}_{i\in I}$ и $\sigma_2 = \{t_j//v_j\}_{j\in J}$ называется подстановка $\sigma = \sigma_1 \circ \sigma_2 : \{ t_k//v_k \}_{k\in K}$, где $K = I \cup J$, а

$$t_k = \begin{cases} t_i\sigma_2 \text{ , если } k \in I, \\ t_j, \text{если } k \notin I. \end{cases}$$

- Множество подстановок образует моноид относительно композиции, причем тождественная подстановка $\{ v_i//v_i\}$ является единицей.

**ТЕОРЕМА** | *Единица единственна.*

Доказательство

Пусть $\exists\ e_1, e_2\ \forall\ a\ \ a \circ e_1 = e_1 \circ a = a$ & $a \circ e_2 = e_2 \circ a = a$. Тогда $e_1 \circ e_2 = e_1$ & $e_1 \circ e_2 = e_2 \Rightarrow e_1 = e_2$.

# Группы

*Группа* — это моноид, в котором

$$\forall\ a\ \ \exists\ \ a^{-1}\ a \circ a^{-1} = a^{-1} \circ a =$$

Элемент $a^{-1}$ называется *обратным*.

1. Множество невырожденных квадратных матриц порядка $n$ образует группу относительно операции умножения матриц. Единицей группы является единичная матрица. Обратным элементом является обратная матрица.
2. Множество подстановок на множестве $M$, то есть множество взаимно однозначных функций $f: M \to M$ является группой относительно операции суперпозиции. Единицей группы является тождественная функция, а обратным элементом – обратная функция.

**ТЕОРЕМА** | *Обратный элемент единственен.*

Доказательство

Пусть $a \circ a^{-1} = a^{-1} \circ a = e$ & $a \circ b = b \circ a = e$.
Тогда $a^{-1} = a^{-1} \circ e = a^{-1} \circ (a \circ b) = (a^{-1} \circ a) \circ b = e \circ b = b$.

**ТЕОРЕМА** | *В группе выполняются следующие соотношения:*

1. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$;
2. $a \circ b = a \circ c \Rightarrow b = c$;
3. $b \circ a = c \circ a \Rightarrow b = c$;
4. $(a^{-1})^{-1} = a$.

## Доказательство

1. $(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ e \circ a^{-1} = a \circ a^{-1} = e.$
2. $a \circ b = a \circ c \Rightarrow a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) \Rightarrow (a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c \Rightarrow e \circ b = e \circ c \Rightarrow b = c.$
3. $b \circ a = c \circ a \Rightarrow (b \circ a) \circ a^{-1} = (c \circ a) \circ a^{-1} \Rightarrow b \circ (a \circ a^{-1}) = c \circ (a \circ a^{-1}) \Rightarrow b \circ e = c \circ e \Rightarrow b = c.$
4. $(a^{-1}) \circ a = a^{-1} \circ a = e.$

**ТЕОРЕМА** | *В группе можно однозначно решить уравнение $a \circ x = b$ , (решение: $x = a^{-1} \circ b$).*

Доказательство.

$$a \circ x = b \Rightarrow a^{-1} \circ (a \circ x) = a^{-1} \circ b \Rightarrow (a^{-1} \circ a) \circ x = a^{-1} \circ b \Rightarrow e \circ x = a^{-1} \circ b \Rightarrow x = a^{-1} \circ b$$

- *Коммутативная* группа, то есть группа, в которой

  $$a \circ b = b \circ a,$$

  называется *абелевой*. В абелевых группах приняты следующие обозначения: групповая операция обозначается + или $\oplus$, обратный элемент к *a* обозначается *-a*, единица группы обозначается 0 и называется *нулем.*

1. $\langle Z; + \rangle$ - множество целых чисел образует абелеву группу относительно сложения. Нулем группы является число 0. Обратным элементом является число с противоположным знаком: $x^{-1} = -x$.
2. $\langle Q_+; \cdot \rangle$ - множество положительных рациональных чисел образует абелеву группу относительно умножения. Нулем группы является число 1. Обратным элементом является обратное число: $(m/n)^{-1} := n/m$.
3. $\langle 2^M; \Delta \rangle$ - булеан образует абелеву группу относительно симметрической разности. Нулем группы является пустое множество $\varnothing$. Обратным элементом является дополнение: $X^{-1} := M \setminus X$.

# Алгебры с двумя операциями

В этом разделе рассматриваются алгебры с двумя бинарными операциями:

$$\oplus, \otimes : M \times M \to M,$$

которые условно называются «сложением» и «умножением», соответственно.

# Кольца

*Кольцо* – это множество $M$ с двумя бинарными операциями $\oplus$ и $\otimes$, в котором:

1. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ сложение ассоциативно;
2. $\exists\ 0 \in M\ \forall\ a\ a \oplus 0 = 0 \oplus a = a$ существует нуль;
3. $\forall\ a\ \exists\ -a\ a \oplus -a = 0$ существует обратный элемент;
4. $A \oplus b = b \oplus a$ сложение коммутативно, то есть кольцо – абелева группа по сложению;
5. $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ умножение ассоциативно, то есть кольцо – полугруппа по умножению;
6. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ умножение дистрибутивно
   $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$ слева и справа.

Кольцо называется *коммутативным,* если

7. $a \otimes b = b \otimes a$ умножение коммутативно.

Коммутативное кольцо называется кольцом с *единицей*, если

8. $\exists\ 1 \in M\ a \otimes 1 = 1 \otimes a = a$ существует единица, то есть кольцо с единицей – моноид по умножению.

**ТЕОРЕМА** | *В кольце выполняются следующие соотношения:*

1. $0 \otimes a = a \otimes 0 = 0$;
2. $a \otimes (-b) = (-a) \otimes b = -(a \otimes b)$;
3. $(-a) \otimes (-b) = a \otimes b$.

## Доказательство

1. $0 \otimes a = (0 \oplus 0) \otimes a = (0 \otimes a) \oplus (0 \otimes a) \Rightarrow -(0 \otimes a) \oplus (0 \otimes a) = -(0 \otimes a) \oplus ((0 \otimes a) \oplus (0 \otimes a)) = (-(0 \otimes a) \oplus (0 \otimes a)) \oplus (0 \otimes a) \Rightarrow 0 = 0 \oplus (0 \otimes a) = 0 \otimes a$.
2. $(a \otimes (-b)) \oplus (a \otimes b) = a \otimes (-b \oplus b) = a \otimes 0 = 0 \Rightarrow a \otimes (-b) = -(a \otimes b)$, $(a \otimes b) \oplus ((-a) \otimes b) = (a \oplus (-a)) \otimes b = 0 \otimes b = 0 \Rightarrow (-a) \otimes b = -(a \otimes b)$.
3. $(-a) \otimes (-b) = -(a \otimes (-b)) = -(-(a \otimes b)) = a \otimes b$.

## Пример

$\langle Z; +, * \rangle$ - коммутативное кольцо с единицей. Для любого натурального $n$
$\langle Z_n; +, * \rangle$ - коммутативное кольцо с единицей. В частности, машинная арифметика целых чисел $\langle Z_{2^{15}}; +, * \rangle$ - коммутативное кольцо с единицей.

Если в кольце $\exists x \neq 0 \ \exists y \neq 0 \ x \otimes y = 0$, то $x$ называется *левым*, а $y$ *– правым делителем нуля*.

## Пример

В машинной арифметике $\langle Z_{2^{15}}; +, * \rangle$ имеем 256 *128 = 0.
В группе $a \circ b = a \circ c \Rightarrow b = c$, однако в произвольном кольце это не так.

**ТЕОРЕМА** | *Пусть $a \neq 0$. Тогда*

$(a \otimes b = a \otimes c \rightarrow b = c))$

## Доказательство

$\Rightarrow$: От противного. Пусть $x \otimes y = 0$. Тогда $x \neq 0$ & $x \otimes y = 0$ & $x \otimes 0 = 0 \Rightarrow y = 0, y \neq 0$ & $x \otimes y = 0$ & $0 \otimes y = 0 \Rightarrow x = 0$.

$\Leftarrow$: $0 = (a \otimes b) \oplus (-(a \otimes b)) = (a \otimes b) \oplus (-(a \otimes c)) = (a \otimes b) \oplus (a \otimes (-c)) = a \otimes (b \oplus (-c))$, $a \otimes (b \oplus (-c)) = 0$ & $a \neq 0 \Rightarrow b \oplus (-c) = 0 \Rightarrow b = c$.

Коммутативное кольцо с единицей, не имеющее делителей нуля, называется *областью целостности*.

**Пример**

Целые числа $\langle Z; +, * \rangle$ является областью целостности, а машинная арифметика
$\langle Z_{2^{15}}; +, * \rangle$ - не является.

# Поля

*Поле* – это множество $M$ с двумя бинарными операциями $\oplus$ и $\otimes$, такими что:

1. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ сложение ассоциативно;
2. $\exists\ 0 \in M\ \ a \oplus 0 = 0 \oplus a = a$ существует нуль;
3. $\forall\ a\ \exists\ -a\ a \oplus -a = 0$ существует обратный элемент по сложению;
4. $a \oplus b = b \oplus a$ сложение коммутативно, то есть поле – абелева группа по сложению;
5. $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ умножение ассоциативно;
6. $\exists\ 1 \in M\ a \otimes 1 = 1 \otimes a = a$ существует единица;
7. $\forall\ a \neq 0\ \exists\ a^{-1}\ a^{-1} \otimes a = 1$ существует обратный элемент по умножению;
8. $a \otimes b = b \otimes a$ умножение коммутативно, то есть поле – абелева группа по умножению;
9. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ умножение дистрибутивно относительно сложения

## Пример

1. $\langle R; +, \cdot \rangle$ - поле вещественных чисел.
2. $\langle Q; +, \cdot \rangle$ - поле рациональных чисел.
3. Пусть $E_2 := \{0, 1\}$. Определим операции $\oplus$, $\cdot : E_2 \times E_2 \to E_2$ следующим образом: $0 \cdot 0 = 0$, $0 \cdot 1 = 0$, $1 \cdot 0 = 0$, $1 \cdot 1 = 1$, $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$. Тогда $\varepsilon_2 := \langle E_2; \oplus, \cdot \rangle$ является полем и называется *двоичной арифметикой*.

**ТЕОРЕМА** | *В поле выполняются следующие соотношения:*

$(-a) = a \otimes (-1)$;

$-(a \oplus b) = (-a) \oplus (-b)$;

$a \neq 0 \Rightarrow (a^{-1})^{-1} = a$;

$a \otimes b = 0 \Rightarrow a = 0 \vee b = 0$.

## Доказательство

1. $(a \otimes (-1)) \oplus a = (a \otimes (-1)) \oplus (a \otimes 1) = a \otimes (-1 \oplus 1) = a \otimes 0 = 0$.
2. $(a \oplus b) \oplus ((-a) \oplus (-b)) = (a \oplus b) \oplus ((-b) \oplus (-a)) = a \oplus (b \oplus (-b)) \oplus (-a) = a \oplus 0 \oplus (-a) = a \oplus (-a) = 0$.
3. $a^{-1} \otimes a = 1$.
4. $a \otimes b = 0 \,\&\, a \neq 0 \Rightarrow b = 1 \otimes b = (a^{-1} \otimes a) \otimes b = a^{-1} \otimes (a \otimes b) = a^{-1} \otimes 0 = 0$, $a \otimes b = 0 \,\&\, b \neq 0 \Rightarrow a = 1 \otimes a = (b^{-1} \otimes b) \otimes a = b^{-1} \otimes (b \otimes a) = b^{-1} \otimes (a \otimes b) = b^{-1} \otimes 0 = 0$.

**ТЕОРЕМА**

*Если $a \neq 0$, то в поле единственным образом разрешимо уравнение*

$$a \otimes x \oplus b = 0, (x = -(a^{-1}) \otimes b).$$

Доказательство

$a \otimes x \oplus b = 0 \Rightarrow a \otimes x \oplus b \oplus (-b) = 0 \oplus (-b) a \otimes x \oplus (b \oplus (-b))$ $= -b \Rightarrow a \otimes x + 0 = -b \Rightarrow a \otimes x = -b \Rightarrow a^{-1} \otimes (a \otimes x) = a^{-1} \otimes$ $(-b) \Rightarrow (a^{-1} \otimes a) \otimes x = -(a^{-1} \otimes b) \Rightarrow 1 \otimes x = -(a^{-1} \otimes b) \Rightarrow x =$ $-(a^{-1} \otimes b)$.

# Решётки

- Решетки иногда называют «структурами», но слово «структура» перегружено, и мы не будем использовать его в этом значении.
- Решетки сами по себе часто встречаются в разных программистских задачах, но еще важнее то, что понятие решетки непосредственно подводит нас к понятию булевой алгебры, которое имеет множество приложений в программировании и вычислительной технике.

Если в решетке $\exists 0 \in M \ \forall a \ \ 0 \cap a = 0$, то 0 называется *нулем* (или *нижней гранью*) решетки. Если в решетке $\exists 1 \in M \ \forall a \ \ 1 \cup a = 1$, то 1 называется *единицей* (или *верхней гранью*) решетки. Решетка с верхней и нижней гранями называется *ограниченной.*

**ТЕОРЕМА** | *Если нижняя (верхняя) грань существует, то она единственна*

## Доказательство

Пусть 0’ – еще один нуль решетки. Тогда $0 \cap 0' = 0'$ и $0' \cap 0 = 0$. Следовательно $0 = 0'$.

**ТЕОРЕМА** | $a \cap b = b \Leftrightarrow a \cup b = a.$

## Доказательство

$\Rightarrow$: Пусть $a \cap b = b$. Тогда $a \cup b = a \cup (a \cap b) = (a \cap b) \cup a = a$.
$\Leftarrow$: Пусть $a \cup b = a$. Тогда $a \cap b = (a \cap b) \cap b = (b \cup a) \cap b = b$.

В ограниченной решетке элемент $a'$ называется *дополнением* элемента $a$, если $a \cap a' = 0$ и $a \cup a' = 1$. Если $\forall\ a \in M\ \ \exists\ a'\ \in M\ a \cap a' = 0\ \&\ a \cup a' = 1$, то ограниченная решетка называется *решеткой с дополнением.* Вообще говоря, дополнение не обязано существовать и не обязано быть единственным.

## ТЕОРЕМА

(о свойствах дополнения) *В ограниченной дистрибутивной решетке с дополнением выполняется следующее:*

1. *дополнение a' единственно;*
2. *дополнение инволютивно: a" = a;*
3. *грани дополняют друг друга: 1' = 0, 0' = 1;*
4. *выполняются законы де Моргана:* $(a \cup b)' = a' \cap b'$, $(a \cap b)' = a' \cup b'$.

# Частичный порядок в решётке

В любой решетке можно естественным образом ввести нестрогий частичный порядок, а именно: $a \prec b$: $a \cap b = a$.

## ТЕОРЕМА

*Пусть $a \prec b$: $a \cap b = a$. Тогда $\prec$ является отношением частичного порядка.*

## Доказательство

Рефлексивность: $a \cap a = a \Rightarrow a \prec a$.

Антисимметричность: $a \prec b \;\&\; b \prec a \Rightarrow a \cap b = a \;\&\; b \cap a = b$ $\Rightarrow a = a \cap b = b \cap a = b$.

Транзитивность: $a \prec b \;\&\; b \prec c \Rightarrow a \cap b = a \;\&\; b \cap c = b \Rightarrow a \cap c$ $= (a \cap b) \cap c = a \cap (b \cap c) = a \cap b = a \Rightarrow a \prec c$.

- Наличие частичного порядка в решетке не случайно, это ее характеристическое свойство. Более того, обычно решетку определяют, начиная с частичного порядка, следующим образом.

Пусть $M$ – частично упорядоченное множество с частичным порядком $\prec$. Элемент $x$ называется *нижней границей* для $a$ и $b$, если $x \prec a \;\&\; x \prec b$. Аналогично $y$ называется *верхней границей* для $a$ и $b$, если $a \prec y \;\&\; b \prec y$.

- Элемент $x$ называется ***нижней гранью*** (*наибольшей нижней границей*) элементов $a$ и $b$, если $x$ – нижняя граница элементов $a$ и $b$ и для любой другой нижней границы $v$ элементов $a$ и $b$ $v \prec x$. Обозначение: $x = inf(a, b)$. Аналогично, $y$ называется ***верхней*** (*наименьшей верхней границей*) элементов $a$ и $b$, если $y$ - верхняя граница элементов $a$ и $b$ и для любой другой верхней границы $u$ элементов $a$ и $b$ $y \prec u$. Обозначение: $y = \sup(a,b)$.

## ТЕОРЕМА

*Если нижняя(верхняя) грань существует, то она единственна.*

Доказательство

$$x = \inf(a, b) \;\&\; y = \inf(a, b) \Rightarrow y \prec x \;\&\; x \prec y \Rightarrow x = y.$$

## ТЕОРЕМА

*Если в частично упорядоченном множестве для любых двух элементов существуют нижняя и верхняя грани, то это множество образует решетку относительно* inf *и* sup *(то есть* $x \cap y$: $\inf(x, y)$, $x \cup y$: $\sup(x, y)$*)*.

# Булевы алгебры

Дистрибутивная ограниченная решетка, в которой для каждого элемента существует дополнение, называется *булевой алгеброй*.

Пример

1. $\langle 2^M; \cap, \cup, - \rangle$ - булева алгебра, $1 = U$, $0 = \varnothing$, $\prec = \subset$.
2. $\langle E_2; \&, \vee, \neg \rangle$ - булева алгебра, $1 = 1$, $0 = 1$, $\prec = \Rightarrow$.

1. $a \cup a = a$, $a \cap a = a$

по определению решетки;

2. $a \cup b = b \cup a$, $a \cap b = b \cap a$,

по определению решетки;

3. $a \cup (b \cup c) = (a \cup b) \cup c$, $a \cap (b \cap c) = (a \cap b) \cap c$

по определению решетки;

4. $(a \cap b) \cup a = a$, $(a \cup b) \cap a = a$

по определению решетки;

5. $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$, $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$

по свойству дистрибутивности;

6. $a \cup 1 = 1$, $a \cap 0 = 0$

по свойству ограниченности;

7. $a \cup 0 = a$, $a \cap 1 = a$

по следствию из теоремы ограниченности;

8. $a'' = a$

по теореме о свойствах дополнения;

9. $(a \cap b)' = a' \cup b'$, $(a \cup b)' = a' \cap b'$

по теореме о свойствах дополнения;

10. $a \cup a' = 1$, $a \cap a' = 0$

так как дополнение существует.

?