Раздел 3 Алгебраические структуры

Сайт:	Электронное обучение ИРНИТУ	Напечатано::	Арбакова Анастасия Вячеславовна
Курс:	Дискретная математика для студентов специальностей АСУ,ЭВМ	Дата:	Понедельник, 7 Июнь 2021, 04:33
Книга:	Раздел 3 Алгебраические структуры		

Оглавление

Алгебраические методы находят самое широкое применение при формализации различных предметных областей. 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, необходимо для абстрактного моделирования, предшествующего практическому программированию задач конкретной предметной области.

§ 1. Операции и алгебры

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

Если операция f— бинарная (то есть f: M × M → M), то будем писать $a\ f\ b$ вместо $f(a, b)$ или $a \circ b$, где о — знак операции.

Определение 1.1. Множество **M** вместе с набором операций $\Sigma = \{f1, . . . ,fm\}$, $f_i : M_{n_i} \to M$, **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 ($n_i,...,n_m$) называется ***типом***;
- Множество операций ∑ называется ***сигнатурой***;
- Запись: **<M; ∑> .**

Определение 1.2. 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**$_i$**}**— множество основ, ∑ = {$f1, . . . ,fm$},— сигнатура, причем $f_i : M_{i1} \times ... \times M_{in} \to M_j$. Тогда <M; ∑> называется ***многоосновной алгеброй***.

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

Loading [MathJax]/jax/output/CommonHTML/jax.js

§ 3. Морфизмы

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

3.1. Гомоморфизм

Алгебры с различными типами имеют различное строение.

Пусть $A = \langle A; \varphi_1, \dots, \varphi_m \rangle$ и $B = \langle B; \psi_1, \dots, \psi_m \rangle$ - две алгебры одинакового типа. Если существует функция $f\colon A \to B$, такая что

$\forall\, i = 1,\dots,m \quad f(\varphi_i\,(a_1, \dots, a_n)) = \psi_I\,(f(a_1), \dots, f(a_n))$, 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***.

3.2. Изоморфизм

Пусть $A = \langle A; \varphi_1, \dots, \varphi_m \rangle$ и $B = \langle B; \psi_1, \dots, \psi_m \rangle$ - две алгебры одинакового типа, и $f\colon A \to B$ – изоморфизм

ТЕОРЕМА 3.1.

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

Если $f\colon A \to B$ – изоморфизм, то алгебры **A** и **B** называют изоморфными и обозначают так **A ~ B**.

ТЕОРЕМА 3.2.

Отношение изоморфизма на множестве однотипных алгебр является эквивалентностью

1. Симметричность: *A~ B* ⇒ *B ~ A*.
2. Транзитивность: *A~ B* & *B ~ g* ⇒ *A ~ g*.
3. Рефлексивность: *A~ A*, *f*: = I.

Пример.

1. $A = \langle 2^M; \cap, \cup \rangle \sim B = \langle 2^M; \cap, \cup \rangle$.
2. $A = \langle R_+; \cdot \rangle \sim B = \langle R; + \rangle$.
3. Пусть $A = \langle N; + \rangle$, $B = \langle \{n \mid n = 2k, k \in N\}; + \rangle$ - *четные*

Loading [MathJax]/jax/output/CommonHTML/jax.js

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.

§ 4. Алгебра с одной операцией

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

$$\bigcirc: \mathbf{M} \times \mathbf{M} \to \mathbf{M}$$

4.1. Полугруппы

Определение 4.1. Полугруппа — это алгебра с одной ассоциативной бинарной операцией:

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

Примеры.

- 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.

4.2. Моноиды

Определение 4.2. Моноид — это полугруппа с ***единицей***:

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

Примеры.

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 S. *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

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

Loading [MathJax]/jax/output/CommonHTML/jax.js

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

ТЕОРЕМА 4.1. ***Единица единственна.***

Доказательство.

Пусть $\exists\ e_1, e_2\ \forall\ a\ \ a \bigcirc e_1 = e_1 \bigcirc a = a\ \&\ a \bigcirc e_2 = e_2 \bigcirc a = a$.

Тогда $e_1 \bigcirc e_2 = e_1\ \&\ e_1 \bigcirc e_2 = e_2 \Rightarrow e_1 = e_2$.

4.3. Группы

Группа — это моноид, в котором $\forall a\ \ \exists\ \ a^{-1}\ \ a \bigcirc a^{-1} = a^{-1} \bigcirc a = e$

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

Примеры.

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 4.2. ***Обратный элемент единственен.***

Доказательство.

Пусть $a \bigcirc a^{-1} = a^{-1} \bigcirc a = e\ \&\ a \bigcirc b = b \bigcirc a = e$.

Тогда $a^{-1} = a^{-1} \bigcirc e = a^{-1} \bigcirc (a \bigcirc b) = (a^{-1} \bigcirc a) \bigcirc b = e \bigcirc b = b$.

ТЕОРЕМА 4.3 ***В группе выполняются следующие соотношения:***

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

Доказательство.

1. $(a \bigcirc b) \bigcirc (b^{-1} \bigcirc a^{-1}) = a \bigcirc (b \bigcirc b^{-1}) \bigcirc a^{-1} = a \bigcirc e \bigcirc a^{-1} = a \bigcirc a^{-1} = e.$

2. *a ○ b = a ○ c* Þ a^{-1}○(*a* ○ *b*) = a^{-1}○(*a* ○ *c*) Þ (a^{-1}○ *a*) ○ *b* = (a^{-1}○ *a*) ○ *c* Þ *e* ○*b* = *e* ○ *c* Þ *b* = *c*.

3. *b* ○ *a* = *c* ○ *a* Þ (*b* ○ *a*) ○ a^{-1} = (*c* ○ *a*) ○ a^{-1} Þ *b* ○ (*a* ○ a^{-1}) = *c* ○ (*a* ○ a^{-1}) Þ *b* ○ *e* = *c* ○ *e* Þ *b* = *c*.

4. (a^{-1}) ○ *a* = a^{-1} ○ *a* =*e*.

ТЕОРЕМА 4.4. ***В группе можно однозначно решить уравнение a ○ x = b ,   (решение: x =*** a^{-1} ***○ b).***

Доказательство.

a ○ *x* = *b* Þ a^{-1} ○ (*a* ○ *x*) = a^{-1} ○ *b* Þ (a^{-1} ○ *a*) ○ *x* = a^{-1} ○ *b* Þ *e* ○ *x* = a^{-1} ○ *b* Þ *x* = a^{-1} ○ *b*

Определение 4.3. *Коммутативная* группа, то есть группа, в которой *a* ○ *b* =*b* ○ *a*, называется ***абелевой.*** В абелевых группах приняты следующие обозначения: групповая операция обозначается + или Å, обратный элемент к *a* обозначается -*a*, единица группы обозначается 0 и называется *нулем*.

Примеры.

1. $< Z, + >$ - множество целых чисел образует абелеву группу относительно сложения. Нулем группы является число 0. Обратным элементом является число с противоположным знаком: x^{-1}= -*x*.

2. $\langle \mathrm{Q}_{+};\ \cdot \rangle$- 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. $\langle 2^{\mathrm{M}};\ \Delta \rangle$ - [булеан] образует абелеву группу относительно симметрической разности. Нулем группы является пустое множество Æ. Обратным элементом является дополнение: X^{-1}: = *M**X*.

Loading [MathJax]/jax/output/CommonHTML/jax.js

§5. 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.

5.1. Кольца

Определение 5.1. Кольцо **– это множество *M* с двумя бинарными операциями $\oplus$, $\otimes$,**

в котором выполняются следующие условия:

1. ***относительно операции сложения множество M— коммутативная группа;***
2. ***кольцо – полугруппа по умножению;***
3. ***$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$***
4. ***$(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$***

Кольцо называется коммутативным, если

$a \otimes b = b \otimes a$

Определение 5.2. Коммутативное кольцо называется кольцом с *единицей*, если существует единица, то есть кольцо с единицей – моноид по умножению.

ТЕОРЕМА 5.1. ***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. $(a \otimes (-b)) \oplus (a \otimes b) = a \otimes (-b \oplus b) = a \otimes 0 = 0 \Rightarrow a \otimes (-b) = -(a \otimes b)$, $(a \otimes b) \oplus((-a) \otimes b) = (a \oplus (-a)) \otimes b = 0 \otimes b = o \Rightarrow (-a) \otimes b = -(a \otimes b)$.
3. $(-a) \otimes (-b) = -(a \otimes (-b)) = -(-(a \otimes b)) = a \otimes b$.

Примеры.

1. $< Z, +, * >$ - коммутативное кольцо с единицей.
2. Для любого натурального n $\langle Z_n, +, * \rangle$ - коммутативное кольцо с единицей.

В частности, машинная арифметика целых чисел - 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*.

Примеры.

В машинной арифметике $\langle Z_{2^{15}};\, +,\, * \rangle$ имеем 256 *128 = 0.

Loading [MathJax]/jax/output/CommonHTML/jax.js нако в произвольном кольце это не так.

ТЕОРЕМА 5.2 ***Пусть a≠ 0. Тогда***

$$\left.\begin{matrix}(a \otimes b \;=\; a \otimes c \Rightarrow b \;=\; c)\\(b \otimes a \;=\; c \otimes a \Rightarrow b \;=\; c)\end{matrix}\right\} \Leftrightarrow (b \neq 0 \;\&c \neq 0 \Rightarrow b \otimes c \neq 0).$$

Доказательство.

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

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

Определение 5.3. Коммутативное кольцо с единицей, не имеющее делителей нуля, называется областью целостности.

Примеры.

1. < z, $+$, $*$ > является областью целостности,

2.а машинная арифметика $\langle Z_{?15}; +, *\rangle$ - не является.

5.2. Поля

Определение 5.4. Поле – это множество M с двумя бинарными операциями $\oplus$, $\otimes$ таким что:

1. ***M – абелева группа по сложению;***
2. ***M – абелева группа по умножению;***
3. ***$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ умножение дистрибутивно относительно сложения***

Примеры.

1. $\langle \mathrm{R}; +, \cdot\rangle$- поле вещественных чисел.
2. $\langle \mathrm{Q}; +, \cdot\rangle$- поле рациональных чисел.
3. Пусть $E_2 := \{0, 1\}$. Определим операции $\oplus$, $\cdot$: $E_2 \times E_2 \rightarrow E_2$ следующим образом: $0\cdot0 = 0$, $0\cdot1 = 0$, $1\cdot0 = 0$, $1\cdot1 = 1$, $0\oplus0 = 0$, $0\oplus1 = 1$, $1\oplus0 = 1$, $1\oplus1=0$. Тогда $\varepsilon_2 := \langle E_2; \oplus, \cdot\rangle$ является полем и называется *двоичной арифметикой*.

ТЕОРЕМА 5.3. ***В поле выполняются следующие соотношения:***

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

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

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

Доказательство.

Loading [MathJax]/jax/output/CommonHTML/jax.js