Раздел 2

Алгебраические структуры

Лекция 4-5
Группы

- 1. Алгебраические операции. Понятие алгебры.
- 2. Полугруппа. Моноид. Группа.
- 3. Теоремы о свойствах группы.

Литература

1. Белоусов А.И. Дискретная математика. М., 2002.
2. Бухштаб А.А. Теория чисел: учебное пособие. СПб., 2015.
3. Нестеренко Ю.В. Теория чисел. М., 2008.

В широком смысле алгебра – раздел математики, изучающий операции над элементами множеств произвольной природы.

Алгебраические структуры определяются множеством элементов и конечным набором заданных на этом множестве алгебраических операций.

1. Алгебраические операции. Понятие алгебры

$X \neq \varnothing, \ n \in \boldsymbol{N}.$

Определение 1

Любое *отображение*

$$f: \ X^n \to X$$

называется n-арной (n-местной) алгебраической операцией на X.

Операция f называется:

- при n=0 – нульарной (это произвольный фиксированный элемент множества X);
- при n=1 – унарной;
- при n=2 – бинарной.

Обозначение: $y = f(x_1, x_2, \ldots, x_n)$

$x_1, x_2, \ldots, x_n$ – аргументы операции f ,
$y \in X$ – результат применения операции f к аргументам.

Определение 2

Пусть на множестве X заданы несколько операций:

$$f_k : \ X^{n_k} \to X,$$

где $\kappa = 1, 2, \ldots, m$,

n_k – натуральное число, зависящее от κ.

Множество X с такой структурой называется алгеброй.

Обозначение: $A = < X, f_1, f_2, \ldots f_m >$

Множество X называется **носителем алгебры**;

множество операций $f_1, f_2, \ldots, f_m$ – **сигнатурой** алгебры.

Алгебра называется **конечной**, если X – конечное множество.

Определение 3

Множество $M \subseteq X$ называется системой образующих (порождающих) или базисом алгебры A, если любой элемент X можно получить из элементов M при помощи операций алгебры A.

Пусть $A = < X, * >$, $*$ – бинарная операция на X.

Определение 4

Операция $*$ называется:

- ассоциативной, если

$$\forall x, y, z \in X \quad (x * y) * z = x * (y * z);$$

- коммутативной, если

$$\forall x, y \in X \;\; x * y = y * x;$$

- идемпотентной, если

$$\forall x \in X \;\; x * x = x.$$

Ассоциативность операции $*$ позволяет для любых элементов $x_1, x_2, \ldots, x_n \in X$ однозначно понимать результат выражения $x_1 * x_2 * \ldots * x_n$:

$$x_1 * x_2 * \ldots * x_n = x_1 * (x_2 * \ldots * x_n) =$$
$$=(x_1 * x_2) * (x_3 * \ldots * x_n) = \ldots =$$
$$= (x_1 * x_2 * \ldots * x_{n-1}) * x_n$$

Определение 5

Элемент $e \in X$ называется **нейтральным** по операции $*$, если

$$\forall x \in X \quad x * e = e * x = x.$$

Теорема 1

Если нейтральный элемент по операции $*$ существует, то он *единственный.*

Если нейтральный элемент существует, то его можно задать как нульарную операцию и включить в сигнатуру.

Доказательство:

Пусть $e_1, e_2 \in X$ – нейтральные элементы по операции $*$.

Тогда $\forall x \in X \;\; x * e_2 = x$, в частности,

$$e_1 * e_2 = e_1$$

и $e_1 * x = x$, в частности,

$$e_1 * e_2 = e_2$$

$\Rightarrow e_1 = e_2$

Ч.т.д.

$X=\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ где $a,b\in \mathbf{R}$

$A = < X, \cdot >$

Любая матрица $\begin{pmatrix} 1 & 0 \\ d & 0 \end{pmatrix}$ где $d\in \mathbf{R}$ –

правый нейтральный элемент:

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix};$$

левый нейтральный элемент ? **СР**

$< X, *, e >$ – алгебра, причем существует нейтральный элемент относительно $*$; $x \in X$.

Определение 6

Элемент $y \in X$ называется обратным к элементу x по операции $*$, если

$$x * y = y * x = e.$$

Элемент x, для которого существует обратный элемент, называется обратимым.

Для *ассоциативной бинарной операции* $*$ существует две формы записи:

1) аддитивная запись:

$$x * x * \ldots * x = x + x + \ldots + x = nx,$$

здесь нейтральный элемент называют *нулем* и обозначают символом $\mathbf{0}$, т.е.

$$x + \mathbf{0} = \mathbf{0} + x = x;$$

обратный элемент к x называют *противоположным* и обозначают $-x$, т.е.

$$x + (-x) = (-x) + x = \mathbf{0};$$

операция + называется *сложением алгебры*;

2) мультипликативная запись:

$$x * x * \ldots * x = x \cdot x \cdot \ldots \cdot x = x^n,$$

здесь нейтральный элемент называют *единицей* и обозначают символом **1**, т.е.

$$x \cdot \mathbf{1} = \mathbf{1} \cdot x = x,$$

обратный элемент к x обозначают x^{-1}, т.е.

$$x \cdot x^{-1} = x^{-1} \cdot x = \mathbf{1},$$

операция $\cdot$ называется *умножением алгебры*.

Пусть $< X, *, \ldots >, < Y, \circ, \ldots >$

– две алгебры с одинаковым числом соответствующих n-арных алгебраических операций.

Определение 7

Отображение $f: X \to Y$ называется **изоморфизмом алгебр**, если:

- f – биекция,
- все операции первой алгебры поставлены в биективное соответствие всем операциям второй алгебры,
- при этом для соответствующих операций выполняется

$$f(x*y) = f(x) \circ f(y),$$

где $x,y \in X;\quad f(x), f(y) \in Y.$

$f:\ \boldsymbol{R} \to \boldsymbol{R}^+$, где $\boldsymbol{R}^+ = \{x \in \boldsymbol{R}:\ x > 0\}$

$f(x) = 10^x,\ \ x \in \boldsymbol{R}$

$f(x+y) = 10^{x+y} = 10^x \cdot 10^y$

- f – биекция,
- бинарной операции (+) поставлена в биективное соответствие бинарная операция (·)
- $f(x+y) = f(x) \cdot f(y)$

Вывод: f – изоморфизм алгебры $<\boldsymbol{R},+>$ на алгебру $<\boldsymbol{R}^+,\cdot>$

2. Полугруппа. Моноид. Группа

$A = < X, * >$ – алгебра.

Определение 8

Алгебра, сигнатура которой состоит из одной *ассоциативной* бинарной операции называется полугруппой.

Определение 9

Если заданная бинарная операция коммутативна, то полугруппа называется коммутативной (абелевой).

Полугруппу, операция которой

- коммутативна,
- идемпотентна

называют полурешеткой.

Нильс Хенрик Абель
(1802 – 1829)

Определение 10

Полугруппа с нейтральным элементом называется моноидом или полугруппой с единицей.

Определение 11

Алгебра называется группой, если она моноид, в котором каждый элемент обратим.

Обозначение: $G = < X, * >$

Порядком конечной группы называется число элементов этой группы.

Аксиомы группы:

(1) $*$ *ассоциативная* бинарная операция

(2) $\exists$ *нейтральный* элемент по операции $*$

(3) $\forall x \in X$ $\exists$ *обратный* элемент по операции $*$

Определение 12

Если алгебра $G_1 = < X, * >$ – группа,

$Y \subseteq X$ и алгебра $G_2 = < Y, * >$ – группа

с той же операцией, что и в G_1,

то G_2 называется подгруппой группы G_1.

3. Теоремы о свойствах группы

$G = < X, * >$ – группа.

Теорема 2

В любой группе $\forall x \in X$ элемент,

обратный к x, *единственный*.

Теорема 3

Пусть $G = < X, \cdot\ , \mathbf{1} >$ – группа.
$\forall x,y \in X$ верны тождества:

$$(x{\cdot}y)^{-1} = y^{-1}{\cdot}\, x^{-1},$$

СР $$(x^{-1})^{-1} = x.$$

СР Запишите теорему 3 в аддитивной форме записи.

$G = < X, \cdot, \mathbf{1} >$ – группа, $a, b \in X$.

Теорема 4

В любой группе справедливы:

1) левый закон сокращения:

$$a \cdot x = a \cdot y \;\Rightarrow x = y$$

2) правый закон сокращения:

$$x \cdot a = y \cdot a \;\Rightarrow x = y$$

Рассмотрим уравнения:

$$a \cdot x = b \qquad (1)$$

$$x \cdot a = b \qquad (2)$$

- **Теорема 5**

В любой группе каждое из уравнений (1), (2) имеет решение, и притом *единственное*:

$$x = a^{-1} \cdot b$$

$$x = b \cdot a^{-1}$$

В мультипликативной форме записи *коммутативной группы* решение обоих уравнений (1), (2):

$$x = b \cdot a^{-1}.$$

Выражение вида $b \cdot a^{-1}$ называется *частным от деления* b на a и обозначается $\dfrac{b}{a}$; сама операция – операцией *деления*.

Решение уравнений записывают в виде:

$$x = \frac{b}{a}.$$

В аддитивной форме записи *коммутативной группы* $G = <X, +, \mathbf{0}>$ оба уравнения (1), (2) имеют вид:

$$a + x = b, \qquad (3)$$

которое имеет единственное решение

$$x = b + (-a),$$

где правая часть называется *разностью* элементов b и a и обозначается $b - a$.

Решение уравнения (3) записывают в виде:

$$x = b - a.$$

Лекция 4-5
Группы

- 4. Степень элемента группы.
- 5. Циклическая группа.

4. Степень элемента группы

$A = < X, \cdot >, \quad x_0 \in X.$

В *полугруппе* элемент вида

$$\underbrace{x_0 \cdot x_0 \cdot \ldots \cdot x_0}_{n \text{ раз}}$$

называется n–й степенью элемента x_0 и обозначается x_0^n.

$$x_0^1 = x_0\ ; \qquad x_0^n = x_0 \cdot x_0^{n-1}, \ \ n = 2, 3, \ldots$$

В *моноиде* $<X, \cdot, \mathbf{1}>$ вводят нулевую степень элемента x_0:

$$x_0^{\,0} = \mathbf{1}.$$

Если $< X, \cdot\, , \mathbf{1} >$ – *группа*, то вводят отрицательную степень элемента x_0 согласно равенству:

$$x_0^{-n} = (x_0^{-1})^n\,, \ n = 1, 2, 3, \ldots$$

Теорема 6

Для любой *группы* выполняется:

$$x_0^m \cdot x_0^n = x_0^{m+n}$$

$$(x_0^m)^n = x_0^{m \cdot n}$$

$$x_0^{-n} = (x_0^n)^{-1}$$

где $m, n \in \mathbf{Z}$.

При аддитивной форме записи бинарной операции возведения элемента x_0 в степень $k>0$, x_0^{κ} понимают как сумму k элементов x_0 и записывают как $k \cdot x_0$.

СР Запишите теорему 6 в аддитивной форме записи.

5. Циклическая группа

$< X, \cdot\ , \mathbf{1} >$ – группа.

- **Определение 13**

Группа называется циклической, если существует такой элемент x_0, что любой элемент группы является некоторой целой степенью элемента x_0 :

- в мультипликативной форме

$$\exists x_0 \in X: \ \forall x \in X \quad x = x_0^k, \ k \in \mathbf{Z}$$

- в аддитивной форме

$$\exists x_0 \in X: \ \forall x \in X \quad x = kx_0, \ k \in \mathbf{Z}$$

x_0 – *образующий элемент* группы.

Пример

$A = < N_0, + >$, где $N_0 = N \cup \{0\}$

$x_0 = 1$ – образующий элемент:

$x = k \cdot 1,\ k \geq 0,$

$< N_0, + >$ – циклическая *полугруппа*

Пример

$A = \langle \mathbf{Z}, +, 0 \rangle$

$x_0 = 1$ – образующий элемент:

$x = k \cdot 1,\ k \in \mathbf{Z}$

$$0 \cdot 1 = 0, \quad k \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{k \text{ раз}} = k \ \ (k > 0)$$

$$(-1) \cdot 1 = -1,$$

$$(-k) \cdot 1 = k \cdot (-1) = \underbrace{(-1) + (-1) + \cdots + (-1)}_{k \text{ раз}} = -k \ \ (k > 0)$$

$x_0 = -1$ – образующий элемент:

$x = k\cdot(-1)$

$0\cdot(-1) = 0$

$$k\cdot(-1) = \underbrace{(-1) + (-1) + \cdots + (-1)}_{k \text{ раз}} = -k \quad (k > 0)$$

$(-1)\cdot(-1) = 1$

$$(-k)\cdot(-1) = k\cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{k \text{ раз}} = k \quad (k > 0)$$

$< Z, +, 0 >$ – циклическая группа.

$A = \langle \boldsymbol{Z}_{[3]}, \oplus, [0] \rangle$ – циклическая группа

$< X, \cdot, \mathbf{1} >$ – циклическая группа.

Порядок образующего элемента циклической группы – это наименьшее число $k > 0$, такое, что

$$x_0^k = \mathbf{1}.$$

Теорема 7

Порядок образующего элемента *конечной* циклической группы равен порядку самой группы.

Следствие:

в *бесконечной* циклической группе $\nexists k>0$ такого, что для образующего элемента x_0 группы выполняется равенство $x_0^k=\mathbf{1}$.

Группа подстановок

$X \neq \varnothing$

$f : X \to X$ – биекция X на себя

f_X – множество всех биекций X на себя

$\circ$ – композиция биекций:

$$\forall x \in X \ \ (g \circ f)(x) = g(f(x)) \in f_X$$

$$A = < f_X, \circ >$$

(1) $\forall\, g, f, h \in f_X$ выполняется $(g \circ f) \circ h = g \circ (f \circ h)$

$\Rightarrow \circ$ – ассоциативная

(2) $\forall x \in X \quad e_X(x) = x$ – тождественное отображение на X:

$e_X \in f_X$ и $\forall f \in f_X \quad f \circ e_X = e_X \circ f = f$

$\Rightarrow e_X$ – нейтральный элемент по $\circ$

(3) $\forall\, f \in f_X$ определено отображение $f^{-1} \in f_X$:

$$f \circ f^{-1} = f^{-1} \circ f = e$$

$\Rightarrow f^{-1}$ – элемент, обратный биекции f по $\circ$

$G = < f_X, \circ >$ – *симметрическая* группа множества X.

- **Определение 14**

Если X *конечно,* то группа всех биекций X на себя с операцией композиции биекций называется группой подстановок множества X.

- **Определение 15**

  Группа подстановок множества X с числом элементов n называется симметрической группой степени n.

  Обозначение: S_n

- **Теорема Кэли** (о представлении групп)

Всякая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.