

Дискретная математика

Операции и алгебры

- ***N*-арная операция** на множестве M – это функция типа

$$\varphi: M^n \rightarrow M ,$$

- где ***n* – арность** операции. Операция замкнута относительно множества M по определению, т. е. операция над элементами множества M , и результат тоже элемент M .

- **Алгеброй** называется множество, вместе с заданной на нем совокупностью операций, т. е. система $\Omega = \{ \varphi_1, \varphi_2, \dots, \varphi_n \}$

$$A = (M; \varphi_1, \varphi_2, \dots, \varphi_n)$$

- ***M*** – ***основное (несущее)***
множество (носитель алгебры)
алгебры *A*.
- ***Тип алгебры*** – вектор арностей
операций.
- ***Сигнатура*** – совокупность
операций Ω .

● Множество $M' \subset M$ называется *замкнутым* относительно

n -арной операции на M , если

$$\varphi(M'^n) \subseteq M',$$

т. е. если значения на аргументе из

M' принадлежат M' .

- Если M' замкнуто относительно всех операций $\varphi_1, \varphi_2, \dots, \varphi_n$ алгебры A с носителем M , то система

$$A' = (M'; \varphi_1, \varphi_2, \dots, \varphi_n)$$

называется *подалгеброй* алгебры A

Примеры:

- Алгебра $(R, +, \cdot)$ – называется *полем действительных чисел*.
- Обе операции бинарные, поэтому тип этой алгебры $(2,2)$.
- Сигнатура $\Omega = (+, \cdot)$.
- Подалгеброй этой алгебры является, например, *поле рациональных чисел*.

Примеры:

● Пусть $N_p = \{0, 1, 2, \dots, p-1\}$.

Определим на N_p операции:

\oplus – «сложение по модулю p »,

\otimes – «умножение по модулю p »,

следующим образом:

$$a \oplus b = c \quad \text{и} \quad a \otimes b = d ,$$

где c и d – остатки от деления на p чисел

$a + b$ и $a \cdot b$ соответственно.

Примеры:

- Пусть, например, $p = 7$, тогда

$$N_p = \{ 0, 1, 2, 3, 4, 5, 6 \} \quad \text{и}$$

$$3 \oplus 4 = 0, \quad 3 \otimes 4 = 5,$$

$$4 \oplus 6 = 3 \quad .$$

- Часто обозначают: $a + b = c \pmod{p}$ и $a \cdot b = d \pmod{p}$.

Примеры:

- *Конечным полем характеристики p называется алгебра*

$\{N_p, \oplus, \otimes\}$
если p – простое число.

Пример:

- **Булеаном U** называется множество всех подмножеств множества U (обозначается $B(U)$).
- **Булева алгебра множеств над U или алгебра Кантора** – алгебра $B = (B(U), \cup, \cap, \neg)$. Ее тип $(2, 2, 1)$, сигнатура $\Omega = (\cup, \cap, \neg)$.
- Элементами основного множества булевой алгебры являются множества (подмножества U).

Пример:

- Для любого $U' \boxtimes U$

$$B' = (B(U'), \boxtimes, \boxtimes, \neg)$$

– является подалгеброй B .

Пример:

- Множество $U = \{a, b, c, d\}$

тогда основное множество

алгебры B содержит 16

элементов.

$$B' = (B(\{a, b\}), \boxtimes, \boxtimes, \neg)$$

является подалгеброй B .

Свойства бинарных алгебраических операций

- Операция φ называется *ассоциативной*, если для любых элементов a, b, c

$$(a \varphi b) \varphi c = a \varphi (b \varphi c) = a \varphi b \varphi c$$

Пример:

1. Сложение и умножение чисел ассоциативны, что позволяет не ставить скобки в выражениях

и $a + b + c$ $a \cdot b \cdot c$

2. Возведение в степень $a^b = a \varphi b$

– не ассоциативна, так как $(a \varphi b) \varphi c = (a^b)^c = a^{bc}$

не равно $a \varphi (b \varphi c) = a^{b^c}$

Свойства бинарных алгебраических операций

- Операция φ называется *коммутативной*, если для любых элементов a, b

$$a \varphi b = b \varphi a$$

Пример:

1 Сложение чисел коммутативно («от перемены мест слагаемых сумма не меняется»):

$$a + b = b + a$$

2. Умножение чисел коммутативно («от перемены мест множителей произведение не меняется»):

$$a \cdot b = b \cdot a$$

Пример:

3 Вычитание и деление – некоммутативные операции.

$$a - b \neq b - a$$

$$a / b \neq b / a$$

2. Умножение матриц – некоммутативная операция, например:

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 0 & 1 \end{pmatrix}$$

Свойства бинарных алгебраических операций

- Операция φ называется *дистрибутивной слева* относительно операции ψ , если для любых a, b, c

$$a \varphi (b \psi c) = (a \varphi b) \psi (a \varphi c)$$

Свойства бинарных алгебраических операций

- Операция φ называется *дистрибутивной справа* относительно операции ψ , если для любых a, b, c

$$(a \psi b) \varphi c = (a \varphi c) \psi (b \varphi c)$$

Пример:

1 Умножение дистрибутивно относительно сложения
слева и справа

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

Пример:

2 Возведение в степень дистрибутивно относительно умножения справа.

$$(a \psi b) \varphi c = (a \cdot b)^c = a^c \cdot b^c = (a \varphi c) \psi (b \varphi c)$$

Пример:

НО НЕ СЛЕВА, ТАК КАК

$$a \varphi (b \psi c) = a^{b \cdot c}$$

$$(a \varphi b) \psi (a \varphi c) = a^b \cdot a^c = a^{b+c}$$

Пример:

- 3. Сложение не дистрибутивно относительно умножения

$$a + (b \cdot c) \neq (a + b) \cdot (a + c)$$

$$(a \cdot b) + c \neq (a + c) \cdot (b + c)$$