9. Двоичные алгебры

9.1. Понятие двоичной (бинарной) операции

Пусть A — непустое множество. *Двоичной операцией* на A называется отображение

$$* : A \times A \longrightarrow A, \quad (x, y) \mapsto x * y.$$

Интуиция: берём два элемента из A, «складываем» их по правилу $*$ и получаем снова элемент из A.

9.2. Свойства двоичной операции

Пусть $*$ — двоичная операция на A. Говорят, что $*$ обладает свойствами:

- **Замкнутость**: по определению $x * y \in A$ для любых $x, y \in A$.
- **Ассоциативность**:

  $$(x * y) * z = x * (y * z), \quad \forall x, y, z \in A.$$

  Позволяет не ставить скобок при многократном применении.
- **Коммутативность**:

  $$x * y = y * x, \quad \forall x, y \in A.$$

- **Нейтральный (единичный) элемент**: существует $e \in A$ такое, что

  $$e * x = x * e = x, \quad \forall x \in A.$$

  Его часто обозначают 0 или 1 в зависимости от контекста.
- **Обратимые элементы**: элемент $x \in A$ называется обратимым, если существует $y \in A$ такой, что

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

  Тогда y называют *обратным* к x и обозначают x^{-1}.

9.3. Классификация двоичных алгебр

1) **Магма**: $(A, *)$ — любое множество с двоичной операцией (требуется лишь замкнутость).

2) **Полугруппа**: магма с ассоциативной операцией.

3) **Моноид**: полугруппа, в которой есть единица e.

4) **Группа**: моноид, в котором каждый элемент обратим.

5) **Абелева (коммутативная) группа**: группа с коммутативным $*$.

9.4. Примеры

1) $(\mathbb{Z}, +)$ — абелева группа, где единица 0, обратный к x есть $-x$.

2) $(\mathbb{N}, +)$ — моноид (нет обратных элементов, кроме 0).

3) $(\{0,1\}, \wedge)$ — коммутативная монода, где $0 \wedge 1 = 0$, единица 1.

4) $(\{0,1\}, \oplus)$ (сумма по модулю 2) — абелева группа:

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 1 = 0; \quad e = 0,\ x^{-1} = x.$$

5) $(M_n(\mathbb{R}), \cdot)$ — полугруппа матриц; моноид при наличии единичной матрицы.

9.5. Таблица Кэли

Для конечных алгебр удобно задавать операцию таблицей. *Пример:* группа $(\{0,1\}, \oplus)$:

$\oplus$	0	1
0	0	1
1	1	0

9.6. Связь с булевыми алгебрами

Булева алгебра — это *расширенная* коммутативная группа с дополнительными операциями «и», «или» и «не» на множестве $\{0,1\}$. В частности, структура $(\{0,1\}, \wedge, \vee, \neg)$ удовлетворяет ряду аксиом идемпотентности и дистрибутивности.

9.7. Зачем нужны двоичные алгебры?

- Моделирование и анализ абстрактных операций (сложение, умножение, логические связки).
- Основа теории групп и её приложений: симметрии, криптография, теории кодирования.
- В информатике: операции над битами, булевы функции, конечные автоматы.

Источники

- С. Ланг, *Алгебра*.
- Д. С. Джонсонбауг, *Дискретная математика*, Pearson.
- Википедия: Бинарная операция.