Глава 4. Алгебраические структуры

4.1. Алгебраические операции и их свойства

Бинарные и n-местные алгебраические операции

Пусть A – непустое множество.

Определение 4.1. Отображение множества $A \times A$ в A называется *бинарной алгебраической операцией* на множестве A.

Примерами бинарных алгебраических операций являются обычное сложение и умножение на множестве целых чисел, объединение и пересечение на булеане непустого множества.

Определение 4.2. Отображение множества A^n в A называется *n-арной* (*n-местной*) *алгебраической операцией* на множестве A, а число n ($n \geq 1$) – *рангом операции*. Выделение (фиксация) некоторого элемента множества A называется *нульарной* (*нульместной*) *операцией* на множестве A, число 0 – *рангом нульарной операции*.

Определение 4.3. Частичная функция из множества A^n в A называется *частичной n-арной алгебраической операцией* на множестве A.

Пример 4.1. 1. Пусть $A \neq \varnothing$. Отображение, ставящее в соответствие каждому подмножеству $X \in P(A)$ его дополнение $\overline{X}$, является унарной алгебраической операцией на $P(A)$.

2. Операция деления рациональных чисел является частичной бинарной алгебраической операцией на множестве рациональных чисел.

3. Операция, ставящая в соответствие каждому кортежу натуральных чисел длины n наибольший общий делитель этих чисел, является n-арной алгебраической операцией на множестве N.

Для обозначения n-арной алгебраической операции используется та же форма записи, что и для произвольных отображений. Если f есть n-арная алгебраическая операция на множестве A и $((x_1, x_2, \ldots, x_n), x_{n+1}) \in f$, то пишут $x_{n+1} = f(x_1, x_2, \ldots, x_n)$ и говорят, что x_{n+1} является значением операции f при значениях аргументов $x_1, x_2, \ldots, x_n$.

Свойства бинарных алгебраических операций

Пусть $*$ и $\circ$ – произвольные бинарные алгебраические операции на непустом множестве A.

Определение 4.4. Бинарная алгебраическая операция $*$ называется *коммутативной*, если $(\forall a, b \in A)\ a * b = b * a$.

Определение 4.5. Бинарная алгебраическая операция $*$ называется *ассоциативной*, если $(\forall a, b, c \in A)\ a * (b * c) = (a * b) * c$.

Если операция $*$ ассоциативна, то можно опускать скобки и писать $a * b * c$ вместо $a * (b * c)$ или $(a * b) * c$.

Определение 4.6. Бинарная алгебраическая операция $\circ$ называется *дистрибутивной* относительно бинарной операции $*$, если $(\forall a, b, c \in A)\ (a * b) \circ c = (a \circ c) * (b \circ c)$ и $c \circ (a * b) = (c \circ a) * (c \circ b)$.

Пример 4.2. 1. Сложение и умножение действительных чисел являются коммутативными и ассоциативными бинарными алгебраическими операциями. Умножение действительных чисел дистрибутивно относительно сложения, но сложение не дистрибутивно относительно умножения, так как условие $(\forall a, b, c \in A)\ a + b \cdot c = (a + b) \cdot (a + c)$ не выполняется.

2. Операции объединения и пересечения подмножеств непустого множества A коммутативны, ассоциативны и дистрибутивны относительно друг друга на булеане $P(A)$.

3. Композиция функций есть ассоциативная бинарная алгебраическая операция. Композиция функций не коммутативна, так как условие $(\forall f, g)\ f \circ g = g \circ f$ не выполняется.

Нейтральные элементы

Пусть $*$ – бинарная алгебраическая операция на непустом множестве A.

Определение 4.7. Элемент $e \in A$ называется *нейтральным* относительно операции $*$, если $(\forall a \in A)\ a * e = e * a = a$.

Теорема 4.1. Если нейтральный элемент относительно операции $*$ существует, то он единственен.

Доказательство. Пусть e и e' – нейтральные элементы относительно операции $*$. Тогда $e = e * e' = e'$, то есть $e = e'$.

Пример 4.3. 1. Число 0 есть нейтральный элемент относительно сложения действительных чисел. Число 1 есть нейтральный элемент относительно умножения действительных чисел.

2. На булеане $P(A)$ пустое множество является нейтральным элементом относительно объединения подмножеств непустого множества A, а $P(A)$ – нейтральным элементом относительно пересечения подмножеств.

Симметричные элементы

Пусть $*$ есть бинарная алгебраическая операция на непустом множестве A и элемент $e \in A$ – нейтральный элемент относительно $*$.

Определение 4.8. Элемент $a' \in A$ называется *симметричным* к элементу $a \in A$ относительно операции $*$, если $a * a' = a' * a = e$. В этом случае элемент a называется *симметризуемым*, а элементы a и a' *– взаимно симметричными*.

Пример 4.4. 1. Любое целое число имеет симметричный к нему элемент относительно сложения – то же число, взятое со знаком минус.

2. Любое ненулевое действительное число a имеет симметричный к нему элемент $\frac{1}{a}$, число нуль не имеет симметричного элемента относительно умножения.

Теорема 4.2. Если операция $*$ ассоциативна и элемент a симметризуем, то существует единственный элемент, симметричный к a.

Доказательство. Пусть a', a'' есть элементы, симметричные к элементу a относительно $*$. Следовательно, $a * a' = a' * a = e$ и $a * a'' = a'' * a = e$. Тогда в силу ассоциативности операции $*$ получаем

$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$, то есть $a' = a''$.

Подмножества, замкнутые относительно бинарной алгебраической операции

Пусть $*$ – бинарная алгебраическая операция на непустом множестве A.

Определение 4.9. Подмножество B множества A называется замкнутым относительно операции $*$, если $(\forall\, a, b \in B)\ a * b \in B$.

Пустое множество замкнуто относительно любой операции $*$.

Пример 4.5. Сложение и вычитание являются бинарными алгебраическими операциями на множестве всех действительных чисел. Множество всех положительных действительных чисел замкнуто относительно сложения, но не замкнуто относительно вычитания.

Аддитивная и мультипликативная форма записи бинарной алгебраической операции

Для обозначения бинарной алгебраической операции $*$ наиболее часто используются аддитивная и мультипликативная формы записи. При аддитивной форме записи операцию $*$ называют *сложением*, а ее результат $a * b$ – *суммой* a и b. При этом вместо $a * b$ пишут $a + b$. Нейтральный элемент относительно сложения называют *нулевым элементом* (или *нулем*) и обозначают символом 0.

Элемент, симметричный к элементу a, называют *противоположным* к элементу a и обозначают через $-a$.

При мультипликативной форме записи операцию $*$ называют *умножением*, а ее результат $a * b$ – *произведением* a и b. При этом вместо $a * b$ пишут $a \cdot b$. Нейтральный элемент относительно умножения называют *единичным элементом* (или *единицей*) и обозначают символом 1. Элемент, симметричный к элементу a, называют *обратным* к элементу a и обозначают через a^{-1}.

4.2. Понятие алгебраической структуры

Определение 4.10. *Алгебраической структурой* (*универсальной алгеброй* или просто *алгеброй*) называется упорядоченная пара $\mathcal{A} = < A, \Sigma >$, где A – непустое множество и Σ – множество алгебраических операций на A.

Таким образом, алгебра представляет собой непустое множество A вместе с заданной на нем совокупностью операций $\Sigma = \{f_1, \ldots, f_m, \ldots\}$, где f_i: $A^{n_i} \to A$ и n_i – ранг операции f_i. Множество A называется *основным* (*несущим*) *множеством* или *основой* (*носителем*) алгебры; упорядоченная последовательность рангов $(n_1, \ldots, n_m)$ называется *типом* алгебры; множество операций $\boldsymbol{\Sigma}$ называется *сигнатурой* алгебры.

Если $< A, \Sigma >$ – алгебра, то также говорят, что множество A есть алгебра относительно операций Σ.

Наиболее частым является случай, когда сигнатура конечна. Если $\Sigma = \{f_1, \ldots, f_m\}$, то вместо записи $\mathcal{A} = < A, \{f_1, \ldots, f_m\} >$ обычно употребляется запись $\mathcal{A} = < A, f_1, \ldots, f_m >$.

Замечание 4.1. Для обозначения алгебры везде, где это необходимо, используется рукописная прописная буква латинского алфавита, а для обозначения ее носителя – соответствующая печатная прописная буква.

Определение 4.11. Алгебры $\mathcal{A} = < A, f_1, \ldots, f_m >$ и $\mathcal{B} = < B, f_1', \ldots, f_m' >$ называются *однотипными*, если их типы совпадают, то есть ранг операции f_i совпадает с рангом соответствующей ей операции f_i' для $i = 1,\ldots, m$.

Пример 4.6. 1. Пусть + и · (сложение и умножение) – арифметические операции на множестве действительных чисел. Алгебра $< R, +, \cdot >$ является алгеброй типа (2, 2).

2. Пусть $P(A)$ – булеан непустого множества A и $\cup, \cap, \bar{}$ – операции пересечения, объединения и дополнения над подмножествами множества A. Алгебра $< P(A), \cup, \cap, \bar{} >$ является алгеброй типа (2, 2, 1).

Определение 4.12. Пусть алгебры $\mathcal{A} = < A, f_1, \ldots, f_m >$ и $\mathcal{B} = < B, f_1', \ldots, f_m' >$ – однотипные алгебры. Алгебра $\mathcal{B}$ называется *подалгеброй* алгебры $\mathcal{A}$, если $B \subseteq A$ и любая операция f_i' ($i = 1, \ldots, m$) алгебры $\mathcal{B}$ и соответствующая ей операция f_i алгебры $\mathcal{A}$ удовлетворяют условию:

$(\forall\, b_1, \ldots, b_{n_i} \in B)\ f_i'(b_1, \ldots, b_{n_i}) = f_i(b_1, \ldots, b_{n_i})$, где n_i – ранг операций f_i' и f_i. (12)

Определение 4.13. Пусть $\mathcal{A} = < A, f_1, \ldots, f_m >$ – алгебра и $B \subseteq A$. Подмножество B множества A называется *замкнутым в алгебре* $\mathcal{A}$, если B замкнуто относительно каждой операции f_i ($i = 1, \ldots, m$) алгебры $\mathcal{A}$, то есть выполняется условие: $(\forall\, b_1,\ldots,b_{n_i} \in B)\ f_i(b_1,\ldots,b_{n_i}) \in B$, где n_i – ранг операции f_i. (13)

Если f_i – нульарная операция, которая выделяет элемент $a \in A$, то условие (13) принимает вид $a \in B$.

Из определений 4.12 и 4.13 непосредственно вытекает следующая теорема.

Теорема 4.3. Пусть $\mathcal{A} = < A, f_1, \ldots, f_m >$ – алгебра и B – непустое подмножество множества A, замкнутое в алгебре $\mathcal{A}$. Тогда алгебра $\mathcal{B} = < B, f_1, \ldots, f_m >$ является подалгеброй алгебры $\mathcal{A}$.

Пример 4.7. Рассмотрим алгебру $< N, +, \cdot >$, где + и · – обычные операции сложения и умножения натуральных чисел. Пусть M – множество четных чисел, то есть $M = \{2k \mid k \in N\}$. Множество M замкнуто относительно операций сложения и умножения натуральных чисел. Действительно,

$(\forall\, 2k_1, 2k_2 \in M)\ 2k_1 + 2k_2 = 2(k_1 + k_2) \in M$ и $2k_1 \cdot 2k_2 = 2(2k_1 \cdot k_2) \in M$, так как множество N замкнуто относительно сложения и умножения. Следовательно, по теореме 4.3 алгебра $< M, +, \cdot >$ является подалгеброй алгебры $< N, +, \cdot >$.

4.3. Алгебры с одной бинарной алгебраической операцией

Рассмотрим алгебры, наиболее часто используемые в теории и на практике.

Пусть A – непустое множество.

Определение 4.14. Алгебра $\mathcal{A} = < A, * >$, где $*$ – бинарная алгебраическая операция, называется группоидом.

Таким образом, группоид определяется непустым множеством A и правилом, по которому можно найти значение операции $*$ для любых двух элементов из A.

Если множество A конечно, то эту информацию можно записать в виде таблицы.

Определение 4.15. Пусть на конечном множестве $A = \{a_1, \ldots, a_n\}$ определена бинарная операция $*$. Таблица, состоящая из n строк и n столбцов, в которой на пересечении i-й строки и j-го столбца располагается значение операции $a_i * a_j$, называется *таблицей Кэли*:

$*$	a_1	a_2	…	a_j	…	a_n
a_1	a_1*a_1	a_1*a_2	…	a_1*a_j	…	a_1*a_n
a_2	a_2*a_1	a_2*a_2	…	a_2*a_j	…	a_2*a_n
⋮	⋮	⋮	…	⋮	…	⋮
a_i	a_i*a_1	a_i*a_2	…	a_i*a_j	…	a_i*a_n
⋮	⋮	⋮	…	⋮	…	⋮
a_n	a_n*a_1	a_n*a_2	…	a_n*a_j	…	a_n*a_n

Замечание 4.2. Артур Кэли (1821 – 1895) – английский математик.

Замечание 4.3. 1. Если операция $*$ коммутативна, то таблица Кэли симметрична относительно главной диагонали.

2. Если для некоторого $i \in \{1, 2, \ldots, n\}$ элемент a_i является нейтральным элементом относительно операции $*$, то соответствующие этому элементу i-я строка и i-й столбец таблицы Кэли имеют вид $(a_1, a_2, \ldots, a_n)$.

3. Пусть элемент a_i – нейтральный элемент относительно операции $*$. Для элемента a_j существует симметричный к нему элемент относительно $*$, если в таблице Кэли среди элементов j-й строки и j-го столбца есть элемент a_i.

Определение 4.16. Алгебра $\mathcal{A} = < A, * >$, где $*$ – ассоциативная бинарная алгебраическая операция, называется *полугруппой*.

Пример 4.8. Алгебра $< N, + >$ является полугруппой, так как бинарная операция $+$ (обычная операция сложения натуральных чисел) ассоциативна.

Определение 4.17. Алгебра $\mathcal{A} = < A, * >$, в которой $*$ является ассоциативной бинарной алгебраической операцией и существует нейтральный элемент e относительно $*$, называется *моноидом*.

Другими словами, моноидом является полугруппа с нейтральным элементом.

Пример 4.9. Алгебра $< N, \cdot >$ образует моноид, так как бинарная операция умножения ассоциативна и натуральное число 1 является нейтральным элементом относительно умножения.

Определение 4.18. Алгебра $\mathcal{A} = < A, * >$ называется *группой*, если выполняются условия (аксиомы):

1) $*$ – ассоциативная бинарная операция;
2) существует нейтральный элемент относительно $*$;

3) для каждого элемента $a \in A$ существует симметричный к нему элемент $a' \in A$ относительно операции $*$.

Таким образом, группа – это моноид, в котором каждый элемент симметризуем.

Определение 4.19. Полугруппа, моноид или группа называется *коммутативной* (коммутативным) или *абелевой* (абелевым), если бинарная алгебраическая операция коммутативна.

Замечание 4.4. Нильс Абель (1802 – 1829) – норвежский математик.

Определение 4.20. Если носитель группы имеет конечную мощность, то группа называется *конечной*, а мощность ее носителя – *порядком* группы. В противном случае группа называется *бесконечной*.

Пример 4.10. Полугруппы $< N, + >$ и $< N, \cdot >$ не являются группами, так как в первой из них не существует нейтральный элемент относительно сложения, а во второй для любого элемента, за исключением числа 1, не существует симметричный к нему элемент.

Пример 4.11. Алгебра $< Z, + >$ образует коммутативную аддитивную группу целых чисел. Действительно, бинарная алгебраическая операция сложения ассоциативна, число 0 есть нейтральный (нулевой) элемент, а симметричным (противоположным) к любому $z \in Z$ является число $-z$.

Пример 4.12. Алгебра $< R \setminus \{0\}, \cdot >$ есть коммутативная мультипликативная группа действительных чисел, так как бинарная алгебраическая операция умножения ассоциативна, нейтральным (единичным) элементом является число 1 и для всякого ненулевого действительного числа r существует симметричный (обратный) к нему элемент $\frac{1}{r}$.

Пример 4.13. Доказать, что множество $R \setminus \{1\}$ образует коммутативную группу относительно операции $*$, где $a * b = 2 \cdot (a - 1) \cdot (b - 1) + 1$.

Решение. Покажем, что $R \setminus \{1\}$ замкнуто относительно операции $*$, то есть $(\forall\, a, b \in R \setminus \{1\})\ a * b \in R \setminus \{1\}$.

Действительно, $a * b = 1 \Leftrightarrow 2 \cdot (a - 1) \cdot (b - 1) + 1 = 1 \Leftrightarrow$
$\Leftrightarrow (a - 1) \cdot (b - 1) = 0 \Leftrightarrow a = 1 \vee b = 1$. Отсюда
$(\forall\, a, b \in R)\ a \neq 1 \wedge b \neq 1 \Rightarrow a * b \neq 1$. Далее проверим выполнение аксиом группы.

1. Докажем, что операция $*$ ассоциативна, то есть
$(\forall\, a, b, c \in R \setminus \{1\})\ (a * b) * c = a * (b * c)$.

Рассмотрим левую и правую части этого равенства:
$(a * b) * c = (2 \cdot (a - 1) \cdot (b - 1) + 1) * c = 2 \cdot ((2 \cdot (a - 1) \cdot (b - 1) + 1) - 1) \cdot (c - 1) +$
$+ 1 = 4 \cdot (a - 1) \cdot (b - 1) \cdot (c - 1) + 1,$
$a * (b * c) = a * (2 \cdot (b - 1) \cdot (c - 1) + 1) = 2 \cdot (a - 1) \cdot ((2 \cdot (b - 1) \cdot (c - 1) + 1) - 1) +$
$+ 1 = 4 \cdot (a - 1) * (b - 1) \cdot (c - 1) + 1.$

Итак, первая аксиома группы выполняется. Легко видеть, что операция $*$ коммутативна, то есть $(\forall\, a, b \in R \setminus \{1\})\ a * b = b * a$.

2. Покажем, что существует нейтральный элемент относительно $*$, то есть

$(\forall\, a \in R \setminus \{1\})\ \exists\, e \in R \setminus \{1\}$: $a * e = e * a = a$. Рассмотрим равенство $a * e = a \Leftrightarrow 2\cdot(a-1)\cdot(e-1)+1 = a$. Выразим из этого равенства e:
$2\cdot(a-1)\cdot(e-1)-(a-1)=0 \Leftrightarrow (a-1)\cdot(2e-2-1)=0 \Leftrightarrow (a-1)\cdot(2e-3)=0 \Leftrightarrow$
$\Leftrightarrow 2e-3=0 \Leftrightarrow e=\frac{3}{2} \in R \setminus \{1\}$. Следовательно, $e=\frac{3}{2}$ – нейтральный элемент относительно $*$. Заметим, что $a * e = e * a$, так как $*$ коммутативна.

3. Докажем, что для каждого элемента из $R \setminus \{1\}$ существует симметричный к нему, то есть $(\forall\, a \in R \setminus \{1\})\ \exists\, a' \in R \setminus \{1\}$: $a * a' = a' * a = \frac{3}{2}$. Имеем:

$a * a' = \frac{3}{2} \Leftrightarrow 2\,(a-1)(a'-1)+1 = \frac{3}{2} \Leftrightarrow (a-1)\cdot(a'-1) = \frac{1}{4} \Leftrightarrow a'-1 = \frac{1}{4\cdot(a-1)} \Leftrightarrow$

$\Leftrightarrow a' = \frac{1}{4\cdot(a-1)} + 1 = \frac{1+4a-4}{4\cdot(a-1)} = \frac{4a-3}{4\cdot(a-1)}$. Покажем, что $a' \neq 1$. Действительно, в противном случае получаем

$$\frac{4a-3}{4\cdot(a-1)} = 1 \Leftrightarrow \frac{4a-3}{4\cdot(a-1)} - 1 = 0 \Leftrightarrow \frac{4a-3-4a+4}{4a-4} = 0 \Leftrightarrow 1 = 0.$$

Итак, для любого $a \in R \setminus \{1\}$ существует симметричный к нему элемент $a' = \frac{4a-3}{4\cdot(a-1)} \in R \setminus \{1\}$. Таким образом, алгебра $< R \setminus \{1\}, * >$ есть коммутативная группа.

4.4. Алгебры с двумя бинарными алгебраическими операциями

Среди алгебр с двумя бинарными алгебраическими операциями особо выделяются кольца и поля.

Определение 4.21. Алгебра $\mathcal{A} = < A, +, \cdot >$ называется *ассоциативным кольцом с единицей*, если выполняются следующие условия (аксиомы):

1) алгебра $< A, + >$ есть коммутативная аддитивная группа;
2) алгебра $< A, \cdot >$ есть мультипликативный моноид;
3) умножение дистрибутивно относительно сложения, то есть
$(\forall a, b, c \in A)\,(a+b)\cdot c = a\cdot c + b\cdot c$ и $c\cdot(a+b) = c\cdot a + c\cdot b$.

Замечание 4.5. В дальнейшем под словом «*кольцо*» будем подразумевать ассоциативное кольцо с единицей.

Элементы множества A называются *элементами кольца* $\mathcal{A} = < A, +, \cdot >$.

Определение 4.22. Группа $< A, + >$ называется *аддитивной группой кольца* $\mathcal{A} = < A, +, \cdot >$. Нейтральный элемент относительно сложения называется *нулем кольца* и обозначается через 0 или $0_{\mathcal{A}}$.

Определение 4.23. Моноид $< A, \cdot >$ называется *мультипликативным моноидом кольца* $\mathcal{A} = < A, +, \cdot >$. Нейтральный элемент относительно умножения называется *единицей кольца* $\mathcal{A}$ и обозначается через 1 или $1_{\mathcal{A}}$.

Определение 4.24. Кольцо называется *коммутативным*, если операция умножения коммутативна, т.е. $(\forall a,b\in A)\ \ a\cdot b=b\cdot a$.

Пример 4.14. Алгебра $< Z, +, \cdot >$ образует коммутативное кольцо целых чисел.

Определение 4.25. *Полем* называется коммутативное кольцо, в котором нуль кольца отличен от единицы кольца и для каждого ненулевого элемента существует обратный к нему относительно операции умножения.

Пример 4.15. Кольцо целых чисел $< Z, +, \cdot >$ полем не является, так как ни один ненулевой элемент, кроме 1, не обладает обратным к нему.

Пример 4.16. Множества Q, R и C образуют бесконечные поля относительно обычных операций сложения и умножения, которые соответственно называются полем рациональных чисел, полем действительных чисел и полем комплексных чисел.

Пример 4.17. Выяснить, образует ли алгебра $<\left\{\begin{pmatrix} x & y \\ y & x \end{pmatrix}\middle|\ x,y\in R\right\}, +, \cdot >$ кольцо, поле?

Решение. Докажем сначала, что операции сложения и умножения матриц являются бинарными алгебраическими операциями на множестве $M=\left\{\begin{pmatrix} x & y \\ y & x \end{pmatrix}\middle|\ x,y\in R\right\}$. Для этого достаточно показать замкнутость множества M относительно этих операций.

$$\left(\forall\begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix},\begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix}\in M\right)\ \begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix}+\begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix}=\begin{pmatrix} x_1+x_2 & y_1+y_2 \\ y_1+y_2 & x_1+x_2 \end{pmatrix}\in M,$$

$$\begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix}\cdot\begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix}=\begin{pmatrix} x_1\cdot x_2+y_1\cdot y_2 & x_1\cdot y_2+y_1\cdot x_2 \\ y_1\cdot x_2+x_1\cdot y_2 & y_1\cdot y_2+x_1\cdot x_2 \end{pmatrix}\in M.$$

Следовательно, операции «+» и «·» – бинарные алгебраические операции на M.

Сложение произвольных матриц (если оно определено) коммутативно и ассоциативно. Значит, «+» коммутативно и ассоциативно на M. Очевидно, что матрица $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\in M$ есть нейтральный элемент относительно «+», а $\begin{pmatrix} -x & -y \\ -y & -x \end{pmatrix}\in M$ – противоположный элемент для произвольной матрицы $\begin{pmatrix} x & y \\ y & x \end{pmatrix}$ из множества M. Следовательно, $< M, + >$ – коммутативная группа.

Умножение произвольных матриц (если оно определено), а значит и матриц из множества M, является ассоциативной операцией. Пусть $\begin{pmatrix} x & y \\ y & x \end{pmatrix}$ – произвольная матрица из множества M.

$$\begin{pmatrix} x & y \\ y & x \end{pmatrix}\cdot\begin{pmatrix} a & b \\ b & a \end{pmatrix}=\begin{pmatrix} x & y \\ y & x \end{pmatrix}\Leftrightarrow\begin{pmatrix} xa+yb & xb+ya \\ ya+xb & yb+xa \end{pmatrix}=\begin{pmatrix} x & y \\ y & x \end{pmatrix}\Leftrightarrow\begin{cases} xa+yb=x \\ ya+xb=y \end{cases}\Rightarrow$$

$\Rightarrow b = \frac{y - ya}{x}$ при $x \neq 0$. Отсюда $xa + \frac{y^2 - y^2 a}{x} = x$. Выполним преобразования:

$x^2 a + y^2 - y^2 a = x^2 \Leftrightarrow y^2 (1 - a) = x^2 (1 - a) \Leftrightarrow 1 - a = 0 \Rightarrow a = 1 \Rightarrow b = \frac{y - y}{x} = 0.$

Если $x = 0$, то $\begin{cases} yb = 0 \\ ya = y \end{cases}$. Так как y – произвольное действительное число, то и в этом случае получаем, что $a = 1$ и $b = 0$. Получили, что $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$ – нейтральный элемент относительно «·». Следовательно, $< M, \cdot >$ – моноид.

Известно, что умножение дистрибутивно относительно сложения для произвольных матриц (если операции имеют смысл), в частности, и для матриц из множества M.

Таким образом, алгебра $< M, +, \cdot >$ – кольцо.

$$\left(\forall \begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix}, \begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix} \in M\right) \begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix} \cdot \begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix} = \begin{pmatrix} x_2 \cdot x_1 + y_2 \cdot y_1 & x_2 \cdot y_1 + y_2 \cdot x_1 \\ y_2 \cdot x_1 + x_2 \cdot y_1 & y_2 \cdot y_1 + x_2 \cdot x_1 \end{pmatrix} =$$

$$= \begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix}.$$

Получили, что «·» – коммутативно. Следовательно, кольцо коммутативно. Нуль кольца отличен от единицы кольца: $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Выясним, для каждого ли ненулевого элемента из множества M существует обратный к нему. Легко видеть, что роль обратного элемента к матрице из M играет обратная к ней матрица.

$$\left(\forall \begin{pmatrix} x & y \\ y & x \end{pmatrix} \in M\right) \exists \begin{pmatrix} x & y \\ y & x \end{pmatrix}^{-1} \Leftrightarrow \begin{vmatrix} x & y \\ y & x \end{vmatrix} \neq 0 \Leftrightarrow x^2 - y^2 \neq 0 \Leftrightarrow x^2 \neq y^2 \Leftrightarrow x \neq \pm y.$$

Значит, множество M содержит ненулевые матрицы, например матрицу $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$, для которых не существуют обратные к ним.

Итак, алгебра $< M, +, \cdot >$ образует коммутативное кольцо, но не является полем.

4.5. Конечные поля

Наряду с бесконечными полями, существуют конечные поля, называемые *полями Галуа* в честь французского математика Эвариста Галуá (1811 – 1832), который в возрасте около 20 лет создал основы современной алгебры и, в частности, открыл конечные поля. Конечные поля играют центральную роль в криптографии, в математических моделях микромира и др. Рассмотрим основные построения теории конечных полей Галуа.

Определим сначала бинарное отношение делимости на множестве Z.

Определение 4.26. Целое число x *делится* на целое число y, если существует $z \in Z$ такое, что $x = y \cdot z$. При этом пишут $x \vdots y$ и говорят, что «x делится на y», или «x кратно y», или «y делит x».

Предложение «y делит x» записывают также в виде $y \mid x$.

Далее рассмотрим еще одно бинарное отношение $\equiv$ на множестве Z.

Определение 4.27. Целые числа x и y называются *сравнимыми по модулю* n ($n \in N$), если разность $(x - y)$ делится на n.

Если целое число x сравнимо с целым числом y по модулю n, то пишут $x \equiv y \pmod{n}$.

Покажем, что отношение сравнимости по модулю n обладает свойствами рефлексивности, симметричности и транзитивности, то есть является отношением эквивалентности. Действительно:

1) $(\forall x \in Z)\ x - x = 0 \vdots n \Rightarrow x \equiv x \pmod{n} \Rightarrow \equiv$ – рефлексивное отношение;

2) $(\forall x, y \in Z)\ x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$, так как $(x - y) \vdots n \Rightarrow y - x = -(x - y) \vdots n$. Следовательно, отношение $\equiv$ симметрично.

3) $(\forall x, y, z \in Z)\ x \equiv y \pmod{n} \wedge y \equiv z \pmod{n} \Rightarrow x \equiv z \pmod{n}$, так как если $(x - y) \vdots n \wedge (y - z) \vdots n$, то $(x - y) + (y - z) = x - z \vdots n$. Следовательно, отношение $\equiv$ транзитивно.

По теореме 3.1 отношение эквивалентности $\equiv$ определяет разбиение множества Z на классы эквивалентности, которые называются *классами вычетов по модулю n* и обладают следующими **свойствами**:

1) любые два класса вычетов по модулю n либо совпадают, либо не пересекаются. Объединение всех классов вычетов по модулю n совпадает с множеством Z;

2) пусть A и B – классы вычетов по модулю n, $a \in A$ и $b \in B$. Классы A и B совпадают тогда и только тогда, когда $a \equiv b \pmod{n}$;

3) если A – класс вычетов по модулю n и a – произвольный элемент множества A, то $A = \{a + n \cdot k \mid k \in Z\}$.

Пример 4.18. Пусть A – класс вычетов по модулю 2, и целое число 5 является представителем этого класса. Тогда

$A = \{5 + 2 \cdot k \mid k \in Z\} = \{\ldots, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, \ldots\}$.

Выясним, какова мощность фактор-множества $Z/\equiv$, то есть сколько существует классов вычетов по модулю n.

Утверждение 4.1. Целые числа x и y сравнимы по модулю n тогда и только тогда, когда при делении на n они дают одинаковые остатки.

Существуют n различных остатков при делении целых чисел на n: 0, 1, 2, …, $n - 1$. Согласно утверждению 4.1 получаем, что $|Z/\equiv| = n$.

Итак, множество целых чисел по отношению сравнимости по модулю n разбивается на n классов эквивалентности, которые обозначим следующим образом: $\bar{0}, \bar{1}, \ldots, \overline{n-1}$. Фактор-множество $Z/\equiv$ обозначим через Z_n.

Определение 4.28. Введем на множестве $Z_n = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$ бинарные операции сложения и умножения следующим образом: $\bar{x} + \bar{y} = \overline{x+y}$ и $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$.

Определение операций сложения и умножения на множестве Z_n корректно, так как если $x_1 \equiv x \pmod{n}$ и $y_1 \equiv y \pmod{n}$, то $x_1 + y_1 \equiv (x + y) \pmod{n}$ и $x_1 \cdot y_1 \equiv x \cdot y \pmod{n}$.

Алгебра $\mathcal{Z}_n = < Z_n, +, \cdot >$ является коммутативным кольцом, которое называется *кольцом вычетов по модулю n*.

Пример 4.19. Рассмотрим кольцо $\mathcal{Z}_2 = < Z_2, +, \cdot >$, где $Z_2 = \{\bar{0}; \bar{1}\}$. Приведем таблицы Кэли операций сложения и умножения в кольце $\mathcal{Z}_2$, где для простоты вместо $\bar{0}$ и $\bar{1}$ будем писать 0 и 1 :

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

Кольцо $\mathcal{Z}_2$ коммутативно, нулем кольца является класс вычетов $\bar{0}$, который отличен от единицы кольца – класса вычетов $\bar{1}$. Кроме того, единственный ненулевой элемент $\bar{1}$ кольца $\mathcal{Z}_2$ имеет обратный к нему – этот же класс $\bar{1}$, так как $\bar{1} \cdot \bar{1} = \bar{1}$. Следовательно, $\mathcal{Z}_2 = < Z_2, +, \cdot >$ является полем. Оно имеет большое значение для приложений.

Следующая теорема говорит о том, что существует много конечных полей.

Теорема 4.4. Кольцо $\mathcal{Z}_n$ является полем тогда и только тогда, когда n – простое число.

4.6. Булевы алгебры

Рассмотрим понятие булевой алгебры, имеющее большое число приложений в программировании и вычислительной технике. Оно возникло в трудах ирландского математика и логика Джорджа Буля (1815 – 1864) как аппарат символической логики.

Определение 4.29. Алгебра $\mathcal{A} = < A, \oplus, *, \bar{} >$ типа (2, 2, 1) называется *булевой алгеброй*, если выполняются следующие условия (аксиомы):

A1. Существуют различные элементы $e_1, e_2 \in A$, являющиеся нейтральными относительно бинарных операций $\oplus, *$ соответственно, то есть
$(\forall\, a \in A)\ \exists\, e_1, e_2 \in A$: $a \oplus e_1 = e_1 \oplus a = a \wedge a * e_2 = e_2 * a = a$.

A2. Операции $\oplus, *$ ассоциативны, то есть
$(\forall a, b, c \in A)\ (a \oplus b) \oplus c = a \oplus (b \oplus c) \ \wedge\ (a * b) * c = a * (b * c)$.

A3. Операции $\oplus, *$ коммутативны, то есть
$(\forall a, b \in A)\ a \oplus b = b \oplus a \ \wedge\ a * b = b * a$.

A4. Операции $\oplus, *$ дистрибутивны относительно друг друга, то есть
$(\forall a,b,c\in A)\, a\oplus(b*c)=(a\oplus b)*(a\oplus c)\ \wedge\ a*(b\oplus c)=(a*b)\oplus(a*c)$.
A5. $(\forall a\in A)\,\exists\,\bar{a}\in A: a\oplus\bar{a}=e_2,\ a*\bar{a}=e_1$.

Замечание 4.6. Аксиома A5 может побудить к ошибочному заключению о том, что элемент $\bar{a}$ является симметричным к элементу a, однако это неверно. Если бы $\bar{a}$ был симметричным элементом к a, то $a\oplus\bar{a}=e_1$ и $a*\bar{a}=e_2$. Сравнивая с аксиомой A5, заключаем, что $\bar{a}$ не является симметричным элементом к a ни для одной из бинарных операций.

Бинарную операцию $\oplus$ называют *сложением*, бинарную операцию $*$ – *умножением*, элементы $a\oplus b$ и $a*b$ – *суммой* и *произведением*, соответственно. Унарную операцию « $\bar{}$ » называют *дополнением*, а элемент $\bar{a}$ – *дополнением к элементу a*.

Существует несколько альтернативных способов записи бинарных операций сложения и умножения:

$\oplus$	$*$
$\vee$	$\wedge$
$+$	$\cdot$
$\cup$	$\cap$

Определение 4.30. Для любого выражения булевой алгебры *двойственным выражением* (или *дуализмом*) называется выражение, полученное из исходного, заменой $\oplus$ на $*$, $*$ на $\oplus$, e_1 на e_2, e_2 на e_1.

Заметим, что каждая из аксиом булевой алгебры – это пара аксиом. Внутри каждой пары каждая аксиома является двойственным выражением по отношению к другой.

Пример 4.20. Наиболее простой из булевых алгебр является алгебра $<\{0, 1\}, \vee, \wedge, \bar{}\ >$, в которой две бинарные операции $\vee$ (дизъюнкция), $\wedge$ (конъюнкция) и одна унарная операция $\bar{}$ (отрицание) задаются таблицами Кэли:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

a	$\bar{a}$
0	1
1	0

Эта булева алгебра носит название *двоичной алгебры логики*. В ней роль операции сложения играет дизъюнкция, роль операции умножения – конъюнкция, роль операции дополнения – отрицание. Элемент 0 является нейтральным элементом относительно дизъюнкции, а элемент 1 – нейтральным элементом относительно конъюнкции.

Пример 4.21. Пусть A – непустое множество. Тогда $< P(A), \cup, \cap, \bar{}\ >$ есть булева алгебра, носящая название *алгебры множеств* (или *алгебры Кантора*). Носителем ее является булеан множества A, сигнатурой – операции объ-

единения, пересечения подмножеств множества A, дополнения данного подмножества до множества A, играющих соответственно роли сложения, умножения и дополнения. Пустое множество является нейтральным элементом относительно объединения, а само множество A – нейтральным элементом относительно пересечения.

Свойства булевой алгебры

Утверждение 4.2 (принцип двойственности). Для любой теоремы булевой алгебры двойственная теорема также верна.

Теорема 4.5. Нейтральные элементы e_1 и e_2 относительно $\oplus$ и $*$ соответственно единственны.

Теорема 4.6. $(\forall a \in A)\exists! \bar{a} \in A : a \oplus \bar{a} = e_2$, $a * \bar{a} = e_1$.

Замечание 4.7. Знак «!» означает слово «единственный».

Теорема 4.7 (закон идемпотентности).

$(\forall a \in A)\ a \oplus a = a,\ \ a * a = a$.

Теорема 4.8 (закон идентичности).

$(\forall a \in A)\ a \oplus e_2 = e_2,\ \ a * e_1 = e_1 * a = e_1$.

Теорема 4.9 (закон абсорбции или **поглощения).**

$(\forall a,b \in A) a \oplus (a * b) = a,\ \ a * (a \oplus b) = a$.

Теорема 4.10 (закон инволюции).

$(\forall a \in A)\ \bar{\bar{a}} = a$.

Теорема 4.11 (законы де Моргана).

$(\forall a,b \in A)\ \overline{a \oplus b} = \bar{a} * \bar{b},\ \ \overline{a * b} = \bar{a} \oplus \bar{b}$.

Теорема 4.12. $\bar{e}_1 = e_2,\ \ \bar{e}_2 = e_1$.

Докажем, например, теорему 4.11, в частности, $\overline{a \oplus b} = \bar{a} * \bar{b}$.

Из аксиомы А5 следует, что для этого достаточно показать выполнение равенства $(a \oplus b) \oplus (\bar{a} * \bar{b}) = e_2$. Действительно, $(a \oplus b) \oplus (\bar{a} * \bar{b}) = ((a \oplus b) \oplus \bar{a}) * ((a \oplus b) \oplus \bar{b}) =$ $= (\bar{a} \oplus (a \oplus b)) * ((a \oplus b) \oplus \bar{b}) = ((\bar{a} \oplus a) \oplus b) * (a \oplus (b \oplus \bar{b})) = (e_2 \oplus b) * (a \oplus e_2) = e_2 * e_2 = e_2 \Rightarrow$ $\Rightarrow \overline{a \oplus b} = \bar{a} * \bar{b}$.

Второй закон де Моргана верен по принципу двойственности.

4.7. Гомоморфизмы алгебр

Пусть $\mathcal{A} = < A, f_1, \ldots, f_m >$ и $\mathcal{B} = < B, f_1', \ldots, f_m' >$ – однотипные алгебры, то есть для любого $i \in \{1, \ldots, m\}$ операция f_i алгебры $\mathcal{A}$ и соответствующая ей операция f_i' алгебры $\mathcal{B}$ имеют одинаковые ранги. Говорят, что отображение h носителя A в носитель B *сохраняет операцию* f_i алгебры $\mathcal{A}$, если

$$(\forall\ a_1, \ldots,\ a_{n_i} \in A)\ h\ (f_i(a_1, \ldots, a_{n_i})) = f_i'\ (h(a_1), \ldots, h(a_{n_i})), \qquad (14)$$

где n_i – ранг операции f_i.

Определение 4.31. *Гомоморфизмом* алгебры $\mathcal{A}$ в (на) однотипную алгебру $\mathcal{B}$ называют такое отображение h носителя A в (на) носитель B, которое сохраняет все операции алгебры $\mathcal{A}$, то есть для любой операции f_i ($i = 1, \ldots, m$) алгебры $\mathcal{A}$ выполняется условие (∗).

Определение 4.32. Гомоморфизм h алгебры $\mathcal{A}$ в алгебру $\mathcal{B}$ называется *мономорфизмом* (или *вложением*), если h является инъективным отображением носителя A в носитель B.

Определение 4.33. Гомоморфизм алгебры $\mathcal{A}$ на алгебру $\mathcal{B}$ называется *эпиморфизмом*.

Определение 4.34. Гомоморфизм h алгебры $\mathcal{A}$ на алгебру $\mathcal{B}$ называют *изоморфизмом*, если h есть инъективное отображение носителя A на носитель B.

Определение 4.35. Алгебры $\mathcal{A}$ и $\mathcal{B}$ называются *изоморфными*, если существует изоморфизм алгебры $\mathcal{A}$ на алгебру $\mathcal{B}$. При этом пишут $\mathcal{A} \cong \mathcal{B}$.

Другими словами, отображение h является изоморфизмом алгебры $\mathcal{A}$ на алгебру $\mathcal{B}$, если h – биективное отображение носителя A на носитель B.

Определение 4.36. Гомоморфизм алгебры $\mathcal{A}$ в себя называется *эндоморфизмом*.

Определение 4.37. Изоморфизм алгебры $\mathcal{A}$ на себя называется *автоморфизмом*.

На рис. 4.1 представлена схема определения частного случая гомоморфизма.

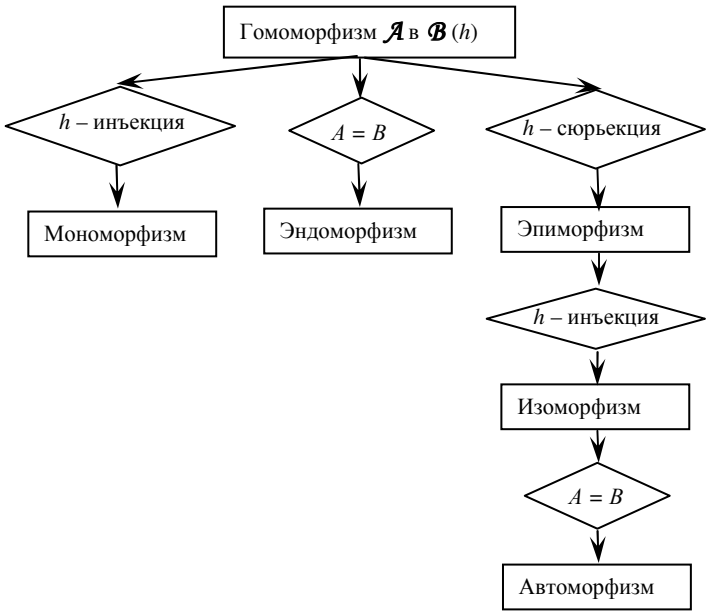

Рис. 4.1

Пример 4.22. Дано отображение

h: $< \{y = ax + b \mid a, b \in R, a \neq 0\}, \circ > \to < R \setminus \{0\}, \cdot >$, где $y = ax + b \mapsto a$.

Выяснить, является ли h гомоморфизмом. Если да, то какой частный случай гомоморфизма имеет место.

Решение. Пусть $A=\{y=ax+b \mid a,b\in R, a\neq 0\}$. Проверим, сохраняет ли h операцию $\circ$, то есть выполняется ли условие:
$(\forall a_1x+b_1, a_2x+b_2\in A)\ h((a_1x+b_1)\circ(a_2x+b_2))= h(a_1x+b_1)\cdot h(a_2x+b_2)$.

Преобразуя левую и правую части равенства, получим:
$h((a_1x+b_1)\circ(a_2x+b_2))=h(a_1(a_2x+b_2)+b_1)=h((a_1a_2)x+(a_1b_2+b_1))=a_1a_2$, (15)
$h(a_1x+b_1)\cdot h(a_2x+b_2)=a_1a_2$. (16)

Из (15) и (16) следует, что h – гомоморфизм алгебры
$<\{y=ax+b \mid a,b\in R, a\neq 0\}, \circ>$ в алгебру $<R\setminus\{0\}, \cdot>$.

Далее выясним, является ли отображение h инъективным или сюръективным.

h – инъекция $\overset{def}{\Leftrightarrow}$ $(\forall a_1x+b_1, a_2x+b_2\in A)\, h(a_1x+b_1)=$
$=h(a_2x+b_2)\Rightarrow a_1x+b_1=a_2x+b_2$.

Это условие не выполняется, так как для любых $b_1\neq b_2$
$h(a_1x+b_1)=h(a_2x+b_2)$. Следовательно, отображение h не является инъективным.

h – сюръекция $\overset{def}{\Leftrightarrow}$ $Im\, h=R\setminus\{0\}$.

Имеем, $(\forall r\in R\setminus\{0\})\, h^{-1}(r)=\{rx+b \mid b\in R\}\neq\varnothing$. Значит, h – сюръекция.

Таким образом, h – эпиморфизм алгебры $<\{y=ax+b \mid a,b\in R, a\neq 0\}, \circ>$ на алгебру $<R\setminus\{0\}, \cdot>$ (см. рис. 4.1).

Пример 4.23. Дано отображение $h:<R, +>\to<R_+, \cdot>$, где $x\mapsto 3^x$ (R_+ – множество положительных действительных чисел).

Решение. Проверим, сохраняет ли h операцию +, то есть выполняется ли условие: $(\forall a,b\in R)\ h(a+b)=h(a)\cdot h(b)$.

Преобразуя левую и правую части равенства, получим:
$h(a+b)=3^{a+b}$, (17)
$h(a)\cdot h(b)=3^a\cdot 3^b=3^{a+b}$. (18)

Из (17) и (18) следует, что h – гомоморфизм алгебры $<R,+>$ в алгебру $<R_+, \cdot>$.

Далее, $(\forall\ a,b\in R\ )\ 3^a=3^b\Rightarrow a=b.$ Следовательно, h – инъекция.

Имеем: $(\forall c\in R_+)\, h^{-1}(c)=\log_3 c$. Следовательно, h – сюръекция.

Значит, h является изоморфизмом алгебры $<R, +>$ на алгебру $<R_+, \cdot>$.

4.8. Алгебраические системы. Решетки

На непустом множестве A, наряду с алгебраическими операциями, можно рассматривать и множество отношений.

Определение 4.38. *Алгебраической системой* называется упорядоченная пара $\mathcal{A} = < A, \Sigma >$, где A – непустое множество и $\Sigma = \Omega \cup \Omega'$, Ω – множество алгебраических операций на A, Ω' – множество отношений на A.

Множество A называется *основным множеством* или *носителем* алгебраической системы, а множество операций и отношений $\mathbf{\Sigma}$ – *сигнатурой* алгебраической системы.

Если множество отношений Ω' пусто, то алгебраическая система $< A, \Sigma > = < A, \Omega >$ является алгеброй. Следовательно, ***алгебры можно считать частным случаем алгебраических систем***. Если множество алгебраических операций Ω пусто, то алгебраическая система $< A, \Sigma > = < A, \Omega' >$ называется *моделью*.

Рассмотрим пример алгебраической системы, который широко используется в математической информатике.

Определение 4.39. *Решеткой* называется алгебраическая система $\mathcal{A} = < A, \leq, \cup, \cap >$, сигнатура которой состоит из одного бинарного отношения $\leq$ частичного порядка и двух бинарных алгебраических операций $\cup$ (объединения) и $\cap$ (пересечения), где бинарные операции определяются следующим образом: $(\forall\, x, y \in A)\ x \cup y = sup\{x, y\}$, $x \cap y = inf\{x, y\}$.

Другими словами, решеткой является частично упорядоченное множество $< A, \leq >$, в котором определены две бинарные алгебраические операции $\cup$ и $\cap$ по вышеуказанным правилам.

Замечание 4.8. Операции $\cup$ и $\cap$ здесь понимаются как абстрактные операции алгебраической системы и отличаются от теоретико-множественных операций объединения и пересечения, определенных в параграфе 1.3, хотя в частных случаях могут с ними совпадать (см. пример 4.24).

Замечание 4.9. Операции $\cup$ и $\cap$ коммутативны и ассоциативны.

Замечание 4.10. Если в алгебраической системе $\mathcal{A}$ ведены операции $\cup$ и $\cap$, то отношение $\leq$ можно по этим операциям восстановить следующим образом: $x \leq y \overset{def}{\Leftrightarrow} x \cup y = y$ или $x \leq y \overset{def}{\Leftrightarrow} x \cap y = x$.

Наименьший элемент решетки (если он существует) называют *нулем* и обозначают через 0. Наибольший элемент решетки (если он существует) называют единицей и обозначают через 1. ***В конечных решетках всегда имеются 0 и 1***.

Пример 4.24. Пусть A – непустое множество, а $P(A)$ – его булеан. Алгебраическая система $< P(A), \subseteq, \cup, \cap >$ является решеткой. Здесь $\cup$ и $\cap$ являются обычными теоретико-множественными операциями объединения и пересечения.

Диаграмма Хассе частично упорядоченного множества $A = \{1, 2, 3\}$ изображена на рис. 4.2. По диаграмме легко видеть, что в этом случае нулем решетки $< P(A), \subseteq, \cup, \cap >$ является $\varnothing$, а единицей – само множество $A = \{1, 2, 3\}$.

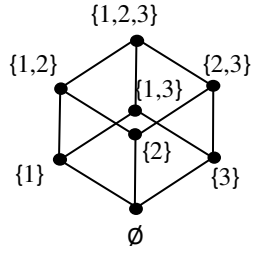

Рис. 4.2

Пример 4.25. Любое линейно упорядоченное мно-

жество $< A, \leq >$, в частности $< R, \leq >$, является решеткой, если в нем определить операции $\cup$ и $\cap$ по правилам:
$(\forall\, x, y \in A)\; x \cup y = max\{x, y\}, x \cap y = min\{x, y\}$.

Определение 4.40. Решетка $\mathcal{A} = < A, \leq >$ называется *дистрибутивной*, если операции объединения и пересечения дистрибутивны относительно друг друга:
$(\forall x, y, z \in A)\; x \cap (y \cup z) = (x \cap y) \cup (x \cap z),\; x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$.

Пример 4.26. Рассмотрим решетку, диаграмма Хассе которой изображена на рис. 4.3. Она не является дистрибутивной, так как $b \cap (d \cup c) = b \cap e = b$, тогда как $(b \cap d) \cup (b \cap c) = a \cup a = a$.

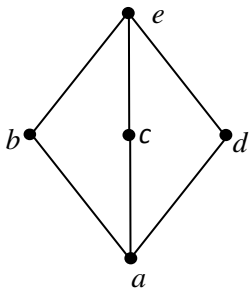

Рис. 4.3

Пример 4.27. Решетка $< P(A), \subseteq, \cup, \cap >$ из примера 4.24 является дистрибутивной, так как обычные теоретико-множественные операции объединения и пересечения дистрибутивны относительно друг друга.

Понятие булевой алгебры является частным случаем понятия решетки.

Определение 4.41. *Булевой алгеброй* называется дистрибутивная решетка $\mathcal{A} = < A, \leq, \cup, \cap >$, в которой имеются различные нуль и единица и $(\forall x \in A)\, \exists\, \bar{x} \in A : x \cup \bar{x} = 1,\; x \cap \bar{x} = 0$. При этом элемент $\bar{x}$ называется дополнением элемента x.

Пример 4.28. Решетка $< P(A), \subseteq, \cup, \cap >$ из примера 4.24 является булевой алгеброй, так как в ней имеются нуль $\varnothing$ и единица A, $\varnothing \neq A$ и
$(\forall\, X \in P(A))\; \exists\; \overline{X} \in P(A)$: $X \cup \overline{X} = A, X \cap \overline{X} = \varnothing$.