Содержание

1. Основные алгебраические структуры

1.1. Бинарные операции и их свойства

Определение 1.1. *Пусть A - множество. Бинарной операцией на множестве A называется отображение:*

$$f : A^2 \to A \quad (f : A \times A \to A) \tag{1}$$

Замечание 1.2. *Если f - бинарная операция на A и пара $(a, b) \in A^2$, то образ пары (a, b) при отображении f называется значением операции f на элементах a и b (результатом применения операции f к элементам a и b) и обозначается $f(a, b)$ или afb.*

Пример 1.3. Примеры бинарных операций

1) Сложение и усножение на множествах $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

2) Вычитание на $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ - определеноб $\mathbb{N}, \mathbb{N}_0$ - не определено.

3) Пусть f_1, f_2 такие, что $f_1 : (1, n)^2 \to (\overline{1, n})$, $f_2 : (\overline{1, n})^2 \to (1, n)$ при этом
$$f_1(a, b) = \max\{a, b\}, \quad f_2(a, b) = \min\{a, b\} \tag{2}$$

   Так как $\forall a, b \in \overline{1, n}$ max и min однозначно определены и содержатся во множестве от $\overline{1, n}$, то отображения f_1, f_2 являются бинарными операциями на множестве $\overline{1, n}$.

4) M - множество, $P(M)$ - множество всех подмножеств, тогда пересечение и объединение $\forall A, B \in P(M)$ является бинарными операциями на множестве $P(M)$.

Определение 1.4. *Бинарная операция $*$ на множестве M называется ассоциативной, если $\forall a, b \in M$ выполняется условие $(a*b)*c = a*(b*c)$. Примерами ассоциативных операций могут служить бинарные операции из примера 1.3.*

Определение 1.5. *Бинарная операция $*$ на множестве M называется коммутативной, если $\forall a, b \in M$ выполняется условие*

$$a * b = b * a \tag{3}$$

Пример 1.6. Примеры коммутативных и некоммутативных операций:

1) Коммутативные - пункты $1, 3, 4$ из 1.3.

2) Некоммутативная - пункт 2 из 1.3, декартово произведение, композиция.

Замечание 1.7. *Для отдельных элементов $a, b \in M$ равенство $a * b = b * a$ может выполняться в том случае, если операция $*$ не коммутативна. Такие элементы называются перестановочными (коммутирующими) друг с другом*

Пример 1.8. $a = 0, b = 0: \quad a - b = b - a$

Замечание 1.9. *Свойства ассоциативности и коммутативности операции независимы. пример коммутативной но не ассоциативной операции:*

$$a * b = \frac{a + b}{2} \tag{4}$$

Определение 1.10. *Бинарная операция $*$ на множестве M называется леводистрибутивной(праводистрибутивной) относительно операции o если $\forall\ a, b, c \in M$ выполнено условие:*

$$a * (b \circ c) = (a * b) \circ (a * c) \quad \text{- леводистрибутивная} \tag{5}$$

$$(b \circ c) * a = (b * a) \circ (c * a) \quad \text{- праводистрибутивная} \tag{6}$$

если выполняются оба этих равенства, то говорят, что $*$ дистрибутивна относительно операции $\circ$. Например умножение дистрибутивна к сложению.

1.2. Алгебраические структуры с одной бинарной операцией

Определение 1.11. *Алгебраической структурой (алгеброй) называется множество с системой операций.*

Определение 1.12. *Множество G с одной бинарной операцией называют группоидом, обозначают $(G, *)$.*

Замечание 1.13. *Из определения группоида следует, что если множество G - конечно, то правило по которому можно найти значение операции $*$. $\forall a, b \in G$, можно записать в таблицу $G = \{a_1, \ldots, a_n\}$ - т.к. G - конечно.*

$$\begin{pmatrix} * & a_1 & \ldots & a_j & \ldots & a_n \\ a_1 & a_1 * a_1 & \ldots & a_1 * a_j & \ldots & a_1 * a_n \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_i & a_i * a_1 & \ldots & a_i * a_j & \ldots & a_i * a_n \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_n & a_n * a_1 & \ldots & a_n * a_j & \ldots & a_n * a_n \end{pmatrix}$$

Определение 1.14. *Пусть $G_1 \subset G$, $\exists(G, *)$, G_1 называют замкнутым относительно операции $*$, если выполнены условия $\forall a, b \in G : ab \in G_1$. В этом случае группоид $(G_1, *)$ называют подгруппоидом группоида $(G, *)$.*

Определение 1.15. *Элемент Λ группоида $(G, *)$ называют нейтральным, если $\forall a \in G$ выполнено:*

$$\Lambda * a = a \tag{7}$$

Пример 1.16. []

1) $(\mathbb{N}_0, +)(\mathbb{Q}, +)$ 0-нейтральные
2) $(\mathbb{N}_0, \bullet)(\mathbb{Q}, \bullet)$ 1-нейтральные
3) $(\mathbb{N}, +)(\mathbb{Z}, +)$ не имеют нейтрального элемента

Утверждение 1.17. *Если в группоиде $(G, *)$ существует нейтральный элемент, то он единственный.*

Доказательство. пусть это не так, тогда Λ_1, Λ_2 - нейтральные элементы группоида $(G, *)$. Т.к. Λ_1 - нейтральный, то $\Lambda_1 * \Lambda_2 = \Lambda_2$, а т.к. Λ_2 - нейтральный, то $\Lambda_1 * \Lambda_2 = \Lambda_1$.
Тогда $\Lambda_1 = \Lambda_2$. □

Определение 1.18. *Пусть есть $(G, *)$, Λ - нейтральный элемент. Элемент $a' \in G$ Называется симметричным элементом элемента $a \in G$, если выполнено условие:*

$$a' * a = a * a' = \Lambda \tag{8}$$

Замечание 1.19. *В общем случае в группоиде с нейтральным элементом Λ элемент α может не иметь симметричных элементов, а может иметь 1 или несколько симметричных элементов.*

Определение 1.20. *Группоид $(G, *)$ с ассоциативной операцией называют полугруппой.*

Утверждение 1.21. *Если в полугруппе $(G, *)$ с нейтральным элементом Λ для элемента α существует симметричный элемент, то он единственный.*

Доказательство. Пусть есть α' и α'' - симметричные элементы для α, тогда получается:

$$\alpha' = \alpha' * \Lambda = \alpha' * (\alpha * \alpha'') = (\alpha' * \alpha) * \alpha'' = \Lambda * \alpha'' = \alpha'' \Rightarrow \alpha' = \alpha'' \quad (9)$$

□

Определение 1.22. *Группоид $(G, *)$ называется группой, если выполнены условия:*

1) $*$ *- ассоциативна*

2) в $(G, *)$ *существует нейтральный элемент* Λ

3) $\forall \alpha \in G \qquad \exists \alpha' \in G$
если кроме того выполнено:

4) $*$ *- коммутативна,*
то такую группу будут называть абалевой группой

Пример 1.23. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ - группы (абелева группа)
$(\mathbb{Q}, \bullet), (\mathbb{R}, \bullet)$ - коммутативные полугруппы с нейтральным элементом $\Lambda = 1$, но они не являются группами.
$(\mathbb{Q}\backslash\{0\}, \bullet), (\mathbb{R}\backslash\{0\}, \bullet)$ - группы
$(\{1\}, \bullet)$ - группа
$(\{1, -1\}, \bullet)$ - группа

Теорема 1.24. *В любой группе* $(G, *) \qquad \forall a, b \in G$ *однозначно разрешимы уравнения:*

$$a * x = b \qquad y * a = b \quad (10)$$

Доказательство. С помощью непосредственной проверки, можно убедиться, что решением уравнения:
$a * x = b$ является $x = a' * b \to a * (a' * b) = b$,
и решением уравнения:
$y * a = b$ является $y = b * a' \to (a * a') * b = b$

Теперь необходимо доказать единственность этих решений. Допустим первое уравнение имеет 2 решения x_1, x_2, тогда:
$a * x_1 = a * x_2$ - умножим на a'
$a' * (a * x_1) = a' * (a * x_2) \Rightarrow (a' * a) * x_1 = (a' * a) * x_2$
$\Lambda * x_1 = \Lambda * x_2 \Rightarrow x_1 = x_2$ - противоречие, $\Rightarrow$ существует только одно решение. Аналогично с y. □

Определение 1.25. *Пусть есть* $(G, *)$ - *полугруппа* $(a_1, ..., a_n) \in G$, *если* $a_1 = a_2 = .. = a_n$. *Тогда*

1) $a_1 * a_2 * ... * a_n = a^n$, *если* $*$ - *умножение.*

2) $a_1 * a_2 * ... * a_n = na$, *если* $*$ - *сложение.*

В таком случае элемент a^n *называется* n-*степенью элемента* a, *элемент* na *называется* n-*кратным элементом* a.

Утверждение 1.26. *Если* $(G, \bullet)$ *и* $(G, +)$ - *полугруппы, то для* $\forall a \in G, \forall n_1, n_2 \in \mathbb{N}$ *выполнены условия:*

1) $a^{n_1} * a^{n_2} = a^{n_1+n_2}$

2) $(a^{n_1})^{n_2} = a^{n_1*n_2}$

3) $n_1 a + n_2 a = (n_1 + n_2)a$

4) $n_1(n_2 a) = (n_1 n_2)a$

Замечание 1.27. *Если группоид* $(G, \bullet)(G, +)$ *являктся группой, то понятия* n-*ой степени и* n-*кратного элемента можно распространить на любое* $n \in \mathbb{Z}$ *для этого введем следующие обозначения:*

1) 0 - *нейтральный элемент относительно* $+$

2) e - *нейтральный элемент относительно* $\bullet$

3) $-a$ *- противоположный элемент к* a *относительно* $+$

4) a^{-1} *- обратный к* a *относительно* $\bullet$

5) $a^0 = e$

6) $0 * a = 0$

7) $(a^n)^{-1} = a^{-n}$

8) $(-n)a = -(na)$

1.3. Кольца и поля

Определение 1.28. *Кольцом называется множество* R *с бинарными операциями* $+, \bullet$ *если выполены условия:*

1) $(R, +)$ *- абелева группа*

2) $(R, \bullet)$ *- полугруппа*

3) умножение дистрибутивно относительно $+$

при этом группа $(R, +)$ *называется аддитивной группой кольца* R*.*

Определение 1.29. *Кольцо* $(R, +, \bullet)$ *называется коммутативным, если умножение коммутативно и кольцом с единицей, если* $(R, \bullet)$ *- полугруппа с единицей.*

Пример 1.30. []

1) $(\mathbb{Z}, +, \bullet), (\mathbb{Q}, +, \bullet), (\mathbb{R}, +, \bullet)$ - коммутативные кольца с единицей

2) $(2\mathbb{Z}, +, \bullet)$, где $2\mathbb{Z}$ - множество всех четных чисел

3) $R^2 = \{(a, b) | a, b \in \mathbb{R}\}$ - множество упорядоченных пар (кольцо не коммутативно)

Введем на множестве R^2 операции сложения и умножения:

$$\forall (c, d) \in R^2 : (a, b) + (c, d) = (a + c, b + d) \qquad (a, b) \bullet (c, d) = (ac, bd) \quad (11)$$

Так как операции над парами производятся покомпонентно, то из свойств целых чисел получаем:

1) $+, \bullet$ в R^2 - коммутативны и ассоциативны

2) $\bullet$ - дистрибутивна относительно $+$

3) $(0,0)$ - нулевой элемент

4) $(1,1)$ - единичный элемент

5) $(-a,-b)$ - противоположный элемент для (a,b)

$(R^2,+,\bullet)$ - коммутативное кольцо с единицей

Теорема 1.31. $\forall a,b,c \in R^2$, *где* R^2 - *произвольное кольцо с нулем, справедливы следующие выражения:*

1) $a*0=0*a=0$

2) $-(-a)=a$

3) $(-a)b=-(ab)$

4) $(-a)(-b)=ab$

5) $a(b-c)=ab-ac$

6) $m(ab)=(ma)b, \quad m \in \mathbb{Z}$

7) $(m_1a)(m_2b)=(m_1m_2)(ab), \quad m_1,m_2 \in \mathbb{Z}$

Доказательство. Пункт 1: $a*0=0*a=0, \quad 0-\Lambda, \quad 0+0=0$
$a*0=a(0+0)=a*0+a*0$ прибавим к обеим частям противоположный элемент $(-a*0)$
$(a*0)-(a*0)=-a*0+a*0+a*0 \Rightarrow 0=0_a*0 \Rightarrow a*0=0$

Пункт 2: $-(-a)=a$
$(-a)$ противоположный для (a), (a) - противоположный для $(-a)$

Пункт 3: $(-a)(b)=-(ab)$
т.к. $-(ab)$ противоположный к (ab), то для доказательства достаточно показать, что $-(a)b$ противоположен (ab):

$ab + (-a)b = (a + (-a))b = 0 * b = 0$
$a * (-b) = -(ab)$ - аналогично

Пункт 4: $(-a)(-b) = ab$
$(-a)(-b) = -(a(-b)) = -(-ab) = ab$

Пункт 5: $a(b - c) = ab - ac$
$a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac$

Пункт 6: $m(ab) = (ma)b = a(mb)$
Для доказательства достаточно воспользоваться определением n-кратного элемента. Свойствами ассоциативности умножения пользоваться нельзя.

1) $m \in \mathbb{N} \quad m(ab) = ab + ab + ... + ab = (a + ... + a)b = (ma)b$

2) $m = 0 \quad m(ab) = (ma)b \Rightarrow$ из свойства 1

3) $m \in \mathbb{Z} \backslash \mathbb{N}_0 \Rightarrow m = -n, \quad$ где $n \in \mathbb{N}$
$-n(ab) = (-na)b \qquad (-n)a = -(na) \quad$ - по определению n-кратного элемента
$-n(ab) = (-na)b, \quad$ так как $(-a)b = a(-b) = -ab$

Пункт 7: $(m_1 a)(m_2 b) = (m_1 m_2)(ab)$
$(m_1 a)(m_2 b) = (a + a + ... + a)(b + b + ... + b) = ab + ab + ... + ab = m_1(m_2 ab)$
□