Операции, отношения, алгебраические системы и алгебры

Пусть имеется некоторое множество M. Функцию типа $\varphi : M^n \to M$ называют *n – арной* (*n – местной*) *операцией* на множестве M. Число n называется *арностью* (или *местностью*) операции φ. Так как φ функция, она однозначна. При этом, вообще говоря, *не предполагается*, что функция φ определена для всякого элемента множества M. Если операция φ не всюду определена на M, то она называется *n – местной частичной операцией*. Под *нуль-местной* операцией на M понимают *выделение элемента* из M. При $n = 2$ для обозначения результата применения операции φ к элементам $a, b \in M$ часто используют запись $a\varphi b$.

Примеры.

а) Сложение действительных чисел « + » есть двухместная (бинарная) операция на множестве действительных чисел $\mathbb{R}$.

б) Деление « : » действительных чисел двухместная (бинарная) *частичная* операция на множестве $\mathbb{R}$. Деление на 0 запрещено.

в) Выделение какого-либо элемента из $\mathbb{R}$ (например, 1) есть нульмерная операция в $\mathbb{R}$.

Операции, отношения, алгебраические системы и алгебры

Напомним, что на непустом множестве M могут быть введены *m – местные* (*m – мерные*) *отношения* Γ, которые представляют собой подмножества множества M^m, т.е. $\Gamma \subseteq M^m$. В случае двухместного (бинарного) отношения Γ для элементов $a, b \in M$ употребляется запись $a\Gamma b$.

В общем случае на множестве M могут быть одновременно заданы некоторое семейство операций $\Omega = \{\varphi_1, \varphi_2, ..., \varphi_k, ...\}$ различной арности и семейство отношений $R = \{\Gamma_1, \Gamma_2, ..., \Gamma_l, ...\}$ различной мерности.

Алгебраической системой называется совокупность $\mathcal{A} = \langle M, \Omega, R \rangle$, состоящая из непустого множества M, семейства операций Ω и семейства отношений R, заданных на множестве M.

Замечание. Для идентификации единого целого, содержащего объекты, которые имеют *различное* математическое строение, например, множество, операции в нем и отношения на его элементах, используется термин *совокупность*, и это целое обозначается угловыми скобками $\langle\ \rangle$.

Операции, отношения, алгебраические системы и алгебры

Множество M называется *носителем*, или *основным множеством* алгебраической системы $\mathcal{A}$, а его элементы - *элементами* этой системы.

Если в рассматриваемой алгебраической системе множество ее отношений является пустым: $R = \varnothing$, то такая алгебраическая система $\mathcal{A} = \langle M, \Omega \rangle$ называется *алгеброй* или *универсальной алгеброй*. Множество ее операций Ω называется *сигнатурой* алгебры. Вектор арностей операций алгебры называется ее *типом*.

Если в алгебраической системе пусто множество операций: $\Omega = \varnothing$, то такая алгебраическая система $\mathcal{A} = \langle M, R \rangle$ называется *моделью* или *реляционной* системой, R - ее сигнатура.

В дальнейшем мы сосредоточим внимание на алгебрах. В зависимости от характера, числа и типа операций они могут иметь различный вид и описывать разные реальные объекты.

Операции, отношения, алгебраические системы и алгебры

Обычно в полугруппе операция $\circledast$ называется *умножением* и при этом запись $a \circledast b$ называется *мультипликативной*. Если операция $\circledast$ *коммутативна*, т.е.

$$a \circledast b = b \circledast a, \tag{7.2}$$

то полугруппа называется *коммутативной* или *абелевой*.

Если полугруппа содержит такой *нейтральный* элемент e, что для любого $a \in M$ имеет место равенство

$$a \circledast e = e \circledast a = a, \tag{7.3}$$

то e называется *единицей* по отношению к $\circledast$.

Полугруппа с единицей называется *моноидом*.

Единица в полугруппе единственна. Действительно, если есть две единицы $e_1, e_2 \in M$, то, согласно (7.3),

$$e_1 \circledast e_2 = e_1, \quad e_1 \circledast e_2 = e_2.$$

Следовательно, $e_1 = e_2$.

Операции, отношения, алгебраические системы и алгебры

Согласно данным выше определениям, полугруппа и моноид являются алгебрами, сигнатура Ω которых состоит из одной бинарной операции $\Omega = \{\circledast\}$. Поэтому ее тип есть (2).

Полугруппы и моноиды имеют особое значение при обработке строк символов и в теории языков. Покажем это на конкретных примерах.

Символ (или *буква*) – это простой неделимый знак. Множество букв образует *алфавит*.

Например, $A = \{$а, б, в,…,э, ю, я$\}$- алфавит русского языка, $E = \{a, b, c, ..., x, y, z\}$ - алфавит английского языка, $B = \{0,1\}$ - бинарный алфавит, $D = \{0,1,2,3,4,5,6,7,8,9\}$ - десятичный алфавит и т.д.

Алфавиты являются множествами и поэтому к ним можно применять теоретико-множественные обозначения. В частности, если A и B такие алфавиты, что $A \subset B$, то говорят, что A является *подалфавитом* B или что B является *расширением* A.

Операции, отношения, алгебраические системы и алгебры

Строки являются упорядоченными совокупностями букв алфавита (например, алфавита A) и, следовательно, выглядят подобно элементам множества $A^n = A \times A \times \ldots \times A$ (кортежам). Однако, в языке является более естественной запись их в виде $a_1 a_2 .. a_n$, а не $(a_1, a_2, \ldots, a_n)$. Буквы сами по себе также являются строками для случая $n = 1$. Допускается случай, когда строка не имеет букв (*пустая* строка), и эта строка обозначается как Λ. Заметим, что Λ *не является* символом: $\Lambda \notin A$, т.е. Λ не входит ни в один алфавит A.

По аналогии с лингвистикой строки также называются *словами*.

Множество всех строк (слов) над алфавитом A называют *замыканием* A и обозначают A^*, так что

$$A^* = A^0 \cup A^1 \cup A^2 \cup \ldots = \bigcup_{n=0}^{\infty} A^n, \tag{7.4}$$

где $A^0 = \{\Lambda\}$ - множество пустых строк, A^1 - множество слов из одной буквы, A^2 - множество слов из двух букв и т.д.

Для удобства определим также *непустых* строк над A следующим образом:

$$A^+ = A^* \setminus \{\Lambda\} = \bigcup_{n=1}^{\infty} A^n. \tag{7.5}$$

Операции, отношения, алгебраические системы и алгебры

Возьмем в качестве примера трехэлементный алфавит $A = \{x, y, z\}$. Тогда множество A^1 включает в себя однобуквенные строки

$$x, y, z,$$

множество $A^2 = A \times A$ - двухбуквенные строки

$$xx,\ yy,\ zz,\ xy,\ xz,\ yz,\ yx,\ zx,\ zy,$$

множество $A^3 = A \times A \times A$ - трехбуквенные строки

$$xxx,\ xyz,\ xzy, \ldots$$

и т.д. Отсюда следует, что A^* *бесконечно.*

Над строками (т.е. над множеством A^*) можно определить бинарную операцию *конкатенации* $\odot$ следующим образом: если $a, b \in A^*$, то

$$a \odot b = ab, \tag{7.6}$$

т.е. результатом выполнения операции $\odot$ является строка a и сразу же записанная за ней строка b. Следовательно, результатом $a \odot b$ является *слияние* строк a и b. Таким образом, имеем

$$xyz \odot z = xyzz, \quad xz \odot yx = xzyx$$

Операции, отношения, алгебраические системы и алгебры

Операция $\odot$ ассоциативна, но не коммутативна.

Аналогично эта же операция определяется для A^+.

Каждая строка a имеет конечную длину, которая обозначается как $|a|$ и равна числу символов в a (при этом разрешаются повторения). Таким образом,

$$|x| = 1, \quad |xy| = 2, \quad |xxxzy| = 5.$$

Это несколько похоже на обозначение числа элементов (мощности) множества. Однако, полная аналогия отсутствует, так как во множестве два одинаковых элемента принимаются за один. В частности,

$$|x| = 1, \quad |\{x\}| = 1,$$

$$|xy| = 2, \quad |\{x, y\}| = 2,$$

$$|yx| = 2, \quad |\{y, x\}| = 2,$$

$$|xyx| = 3, \quad |\{x, y, x\}| = |\{x, y\}| = 2.$$

Для пустой строки Λ имеем $|\Lambda| = 0$ и

$$\Lambda \odot a = a \odot \Lambda = a$$

для всех строк a. Следовательно, является единицей (нейтральным элементом) по отношению к операции $\odot$.

Операции, отношения, алгебраические системы и алгебры

Пример 7.1. Двухэлементная алгебра $\langle\{0,1\},\wedge\rangle$ с единственной бинарной операцией конъюнкции $\wedge$ является монондом по следующим причинам:

а) выполнено условие замкнутости: $x \wedge y \in \{0,1\}$,

б) операция $\wedge$ ассоциативна: если $x, y, z \in \{0,1\}$, то

$$(x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y \wedge z .$$

Эта операция мультипликативна.

в) В алгебре $\langle\{0,1\},\wedge\rangle$ роль нейтрального элемента играет 1:

$$1 \wedge x = x \wedge 1 = x .$$

Этот моноид абелев.

Операции, отношения, алгебраические системы и алгебры

Не следует думать, что любая алгебра $\langle M, \circledast \rangle$ с одной бинарной операцией $\circledast$ есть полугруппа. Так, полугруппами (а, следовательно, и моноидами) не являются алгебры $\langle \{0,1\}, | \rangle$ и $\langle \{0,1\}, \downarrow \rangle$, где бинарная операция | - штрих Шеффера, а бинарная операция $\downarrow$ - стрелка Пирса. Условие замкнутости здесь выполняется, однако ни штрих Шеффера, ни стрелка Пирса не ассоциативны. Действительно,

$$(x \,|\, y) \,|\, z \neq x \,|\, (y \,|\, z) \text{ или } x \wedge y \vee \overline{z} \neq \overline{x} \vee y \wedge z,$$

а также

$$(x \downarrow y) \downarrow z \neq x \downarrow (y \downarrow z) \text{ или } (x \vee y) \wedge \overline{z} \neq \overline{x} \wedge (y \vee z).$$

В свою очередь, требование ассоциативности операции $\circledast$ лежит в основе понятия полугруппы и моноида.

7.3.2. Группы и подгруппы

Будем обозначать как $\otimes$ бинарную операцию над элементами множества M, если эта операция мультипликативна, и как $\oplus$, если она аддитивна.

Группой называется алгебра $G = \langle M, \otimes \rangle$ или $G = \langle M, \oplus \rangle$, в которой определена *одна* (мультипликативная или аддитивная) операция и выполняются 4 *аксиомы*:

a) В результате применения операции $\otimes$ (или $\oplus$) к любым двум элементам группы образуется элемент этой же группы (требование *замкнутости*), т.е. если $a, b \in M$, то

$$a \otimes b = c \qquad (\text{или } a \oplus b = c), \text{ где } c \in M.$$

b) Для любых трех элементов группы $a, b, c \in M$ удовлетворяется равенство

$$(a \otimes b) \otimes c = a \otimes (b \otimes c),$$

если операция мультипликативна, и равенство

$$(a \oplus b) \oplus c = a \oplus (b \oplus c),$$

если она аддитивна (требование *ассоциативности*).

c) В любой группе G существует однозначно определенный нейтральный элемент e, удовлетворяющий при значениях $a \in M$ условию

$$a \otimes e = e \otimes a = a$$

для мультипликативной операции, либо условию

$$a \oplus e = e \oplus a = a$$

для аддитивной операции. В первом случае элемент e называют *единицей* и часто обозначают символом 1, а во втором – *нулем* и обозначают символом 0.

d) *а*) Всякий элемент a мультипликативной группы обладает элементом a^{-1}, однозначно определенным уравнением

$$a \otimes a^{-1} = a^{-1} \otimes a = e = 1.$$

При этом элемент a^{-1} называется *обратным* элементу a.

б) Всякий элемент a аддитивной группы обладает элементом $-a$, однозначно определенным уравнением

$$a \oplus (-a) = (-a) \oplus a = 0.$$

Такой элемент $-a$ называется *противоположным* элементу a.

Если операция, определенная в группе, коммутативна, то группу называют *коммутативной*, или *абелевой*.

Операции, отношения, алгебраические системы и алгебры

Группу, состоящую из конечного числа элементов, называют *конечной.* Число элементов в группе называют *порядком* группы.

Множество M всех элементов группы G называется *основным множеством* группы и обычно обозначается *той же* буквой G.

Нетрудно видеть, что первые две аксиомы группы определяют полугруппу. Добавление к ним третьей аксиомы приводит к определению моноида. И только четвертая аксиома определяет чисто групповое свойство алгебры: *группа – это моноид с обратным (противоположным) элементом.*

Группа в сравнении с полугруппой и моноидом обладает рядом важных свойств. Например, внутри мультипликативной группы $G = \langle M, \otimes \rangle$ можно решить уравнение

$$a \otimes x = b, \tag{7.7}$$

где a и b известные, а x - неизвестный элемент множества M. Решим его, пользуясь только вышеприведенными аксиомами.

Операции, отношения, алгебраические системы и алгебры

Так как $a \in M$, то в силу аксиомы 4 существует соответствующее ему $a^{-1} \in M$. Умножим обе части (7.7) слева на a^{-1}:

$$a^{-1} \otimes (a \otimes x) = a^{-1} \otimes b.$$

Поскольку операция $\otimes$ ассоциативна (аксиома 2), то отсюда имеем

$$(a^{-1} \otimes a) \otimes x = a^{-1} \otimes b.$$

В силу аксиомы 4*а*) имеем

$$a \otimes a^{-1} = e$$

и предыдущая формула принимает вид

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

Применяя аксиому 3, окончательно найдем

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

Это – решение уравнения (7.7).

Решение уравнения $x \otimes a = b$, очевидно, можно получить таким же способом, но умножая его на a^{-1} справа. Это даст

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

Рассуждая аналогично, решение уравнения

$$a \oplus x = b$$

с аддитивной операцией $\oplus$ получим в виде

$$x = (-a) \oplus b,$$

а решение уравнения

$$x \oplus a = b$$

- в виде

$$x = b \oplus (-a).$$

Для любой группы G справедливо равенство

$$(a \otimes b)^{-1} = b^{-1} \otimes a^{-1}. \tag{7.8}$$

Докажем его. Умножим правую часть этого равенства слева на $a \otimes b$, и преобразуем ее, используя свойства ассоциативности, обратного и нейтрального элементов:

$$(a \otimes b) \otimes (b^{-1} \otimes a^{-1}) = a \otimes (b \otimes b^{-1}) \otimes a^{-1} = a \otimes e \otimes a^{-1} = a \otimes a^{-1} = e,$$

Операции, отношения, алгебраические системы и алгебры

$$(a\otimes b)\otimes(b^{-1}\otimes a^{-1})=e.$$

Согласно аксиоме 4a, это означает, что $b^{-1}\otimes a^{-1}$ является правым обратным элементом к $a\otimes b$. Аналогично можно показать, что он является левым обратным элементом, откуда и следует требуемый результат (7.8). Он может быть распространен на любое количество элементов:

$$(a\otimes b\otimes\ldots\otimes y\otimes z)^{-1}=z^{-1}\otimes y^{-1}\otimes\ldots\otimes b^{-1}\otimes a^{-1}.$$

Для примера рассмотрим алгебру $\langle M,\otimes\rangle$, основное множество (носитель) которой состоит из 6 элементов $M=\{A,B,C,D,F,E\}$, каждый из которых представляет собой квадратную матрицу второго порядка:

$$\begin{gathered}A=\begin{bmatrix}1&0\\0&-1\end{bmatrix},\ B=\begin{bmatrix}-1/2&\sqrt{3}/2\\\sqrt{3}/2&1/2\end{bmatrix},\ C=\begin{bmatrix}-1/2&-\sqrt{3}/2\\-\sqrt{3}/2&1/2\end{bmatrix},\\ D=\begin{bmatrix}-1/2&\sqrt{3}/2\\-\sqrt{3}/2&-1/2\end{bmatrix},\ F=\begin{bmatrix}-1/2&-\sqrt{3}/2\\\sqrt{3}/2&-1/2\end{bmatrix},\ E=\begin{bmatrix}1&0\\0&1\end{bmatrix}.\end{gathered}\qquad(7.9)$$

В качестве бинарной мультипликативной операции выберем операцию обычного умножения матрицы на матрицу. Образуем таблицу из 36 произведений каждой из матриц (7.9) на каждую из них. Получим

$\otimes$	A	B	C	D	F	E
A	E	D	F	B	C	A
B	F	E	D	C	A	B
C	D	F	E	A	B	C
D	C	A	B	F	E	D
F	B	C	A	E	D	F
E	A	B	C	D	F	E

(7.10)

Таблицы такого типа называются *таблицами Кэли* или *групповыми таблицами*. Здесь первый сомножитель берется в столбце, отделенном двойной вертикальной линией, а второй сомножитель – в строке, отделенной двойной горизонтальной линией. Их произведение расположено на пересечении соответствующих строки и столбца в таблице.

Выясним, что представляет собой данная алгебра $\langle M, \otimes \rangle$. Для этого проверим выполнимость в ней аксиом $1-4$.

Операции, отношения, алгебраические системы и алгебры

Таблица (7.10) показывает, что применение операции $\otimes$ к любой паре элементов множества M дает элемент этого же множества, т.е. выполняется требование *замкнутости* (аксиома 1).

Из теории матриц известно, что операция их умножения является ассоциативной. Поэтому в данной алгебре выполняется требование *ассоциативности* (аксиома 2).

Из таблицы (7.10) видно, что умножение любого элемента множества M как слева, так справа на его элемент E, оставляет умножаемый элемент без изменения. Следовательно, матрица E играет роль единичного элемента (аксиома 3). Обычно нейтральный элемент при перечислительной записи множества M записывается последним, даже если это нарушает алфавитный порядок записи элементов. Именно так выполнена запись множества M, где вопреки правилам алфавита, элемент E записан после F.

И, наконец, из таблицы (7.10) следует, что каждый элемент множества M имеет обратный, а именно,

$$A^{-1} = A,\ B^{-1} = B,\ C^{-1} = C,\ D^{-1} = F,\ F^{-1} = D,\ E^{-1} = E,$$

т.е. выполняется аксиома 4.

Итак, из всего изложенного следует, что рассматриваемая алгебра $G = \langle M, \otimes \rangle$ представляет собой конечную группу шестого порядка. Эта группа не коммутативна. Действительно, в частности, $A \otimes B = D \neq F = B \otimes A$.