Ткачев С.Б.
каф. Математического моделирования
МГТУ им. Н.Э. Баумана

ДИСКРЕТНАЯ МАТЕМАТИКА

ИУ5 — 4 семестр, 2015 г.

Лекция 8. ЭЛЕМЕНТЫ ОБЩЕЙ АЛГЕБРЫ. ПОЛУГРУППЫ И ГРУППЫ

Предметом рассмотрения в абстрактной алгебре являются произвольные множества с заданными на них операциями.

Природа множеств и операций может существенно отличаться от привычных числовых множеств и известных операций над числами.

8.1. Операции. Понятие алгебраической структуры

Определение 8.1. Пусть A — произвольное непустое множество и n — натуральное число. Любое отображение

$$\omega\colon A^n \to A$$

называют **n -арной** (или **n -местной**) **операцией** на множестве A.

n -арная операция ω каждому *кортежу* $(a_1, \ldots, a_n) \in A^n$ однозначно сопоставляет элемент $b \in A$.

Компоненты кортежа называют **аргументами операции** ω, а b — **результатом применения операции** ω к аргументам $a_1, \ldots, a_n$.

Для n -арной операции используют обозначение

$$b = \omega(a_1, \ldots, a_n)$$

или

$$b = a_1 \ldots a_n \omega.$$

Обычно, если $n = 2$, пишут $a_1 \, \omega \, a_2$.

При $n = 1$ говорят об **унарной операции**.

При $n = 2$ — о **бинарной операции**.

Пример унарной операции — *дополнение* заданного *множества* до *универсального множества*.

Примеры бинарных операций:
— сложение и умножение чисел,

— сложение и умножение матриц квадратных матриц типа $n \times n$,

— сложение векторов линейного пространства.

Специально вводят понятие **нульарной операции** (т.е. при $n = 0$).

Под нульарной операцией на множестве A понимают произвольный фиксированный элемент множества A .

Нульарные операции позволяют фиксировать элементы множества A , обладающие некоторыми специальными свойствами.

Пример нульарной операции — фиксирование нуля в множестве целых чисел с операцией сложения.

Рассмотрим бинарную операцию на множестве A, обозначив ее звездочкой $(*)$.
Эту операцию называют:

1) **ассоциативной**, если $(x*y)*z = x*(y*z)$ для любых x, y, $z \in A$;

2) **коммутативной**, если $x*y = y*x$ для любых x, $y \in A$;

3) **идемпотентной**, если $x*x = x$ для любого $x \in A$.

Ассоциативность операции $*$ позволяет для любых элементов a_1, a_2, $\ldots$, $a_n \in A$ однозначно трактовать результат выражения $a_1 * a_2 * \ldots * a_n$, так как

$$a_1 * a_2 * \ldots * a_n = a_1 * (a_2 * \ldots * a_n) =$$
$$= (a_1 * a_2) * (a_3 * \ldots * a_n) = (a_1 * a_2 * \ldots * a_{n-1}) * a_n.$$

Операция сложения, заданная на множестве натуральных чисел, является ассоциативной и коммутативной.

Операция умножения матриц ассоциативна, но не коммутативна.

Идемпотентными являются операции объединения и пересечения множеств.

Определение 8.2. Элемент $\mathbf{1}$ множества A называют **левым нейтральным элементом** относительно операции $*$, если $\mathbf{1} * x = x$ для любого элемента $x \in A$.

Определение 8.3. Элемент $\mathbf{1}$ множества A называют **правым нейтральным элементом** относительно операции $*$, если $x * \mathbf{1} = x$ для любого элемента $x \in A$.

Если существуют левый ($\mathbf{1}'$) и правый ($\mathbf{1}''$) нейтральные элементы, то они совпадают. $\mathbf{1}' = \mathbf{1}' * \mathbf{1}'' = \mathbf{1}''$.

В этом случае элемент $\mathbf{1}$ единственный, и его называют просто **нейтральным элементом**.

Нейтральным элементом относительно операции умножения на множестве натуральных чисел является число 1.

На множестве целых чисел нейтральным элементом относительно операции сложения будет число 0.

Пример 8.1.

На множестве квадратных матриц вида $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$, где элементы a и b — действительные числа, любая матрица вида $\begin{pmatrix} 1 & 0 \\ d & 0 \end{pmatrix}$ будет правым нейтральным элементом по операции умножения.

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}.$$

Правых нейтральных элементов бесконечно много.

Левого нейтрального элемента по этой операции нет (иначе существовал бы единственный нейтральный элемент). #

Определение 8.4. Алгебра (универсальная алгебра, Ω-алгебра) считается заданной, если заданы некоторое множество A, называемое **носителем** данной **алгебры**, и некоторое множество операций Ω на A, называемое **сигнатурой** данной **алгебры**.

Алгебра — упорядоченная пара множеств $\mathcal{A} = (A, \Omega)$, первая компонента этой пары есть носитель, а вторая — сигнатура.

Результат применения любой операции обязательно должен принадлежать тому же множеству, что и ее аргументы.

Рассмотрим множество V_3 всех свободных векторов в пространстве и операцию скалярного умножения векторов. Это **не алгебра**, т.к. скалярное произведение двух векторов не есть вектор.

Множество V_3 всех свободных векторов в пространстве и операция векторного умножения векторов **является** алгеброй.

Пара $(\mathbb{R} \setminus \{0\},\ \{:\})$ есть алгебра.

Пример 8.2.
Для любого множества M можно определить алгебру

$$\mathcal{A}_2 = \left(2^{M\times M},\ \{\cup,\ \circ,\ ^{-1}\}\right),$$

носителем которой является множество всех подмножеств множества упорядоченных пар на M, т.е. множество всех *бинарных отношений на множестве* M.
Сигнатура состоит из операций объединения, композиции бинарных отношений и взятия обратного отношения. #

8.2. Группоиды, полугруппы, группы

Рассмотрим алгебры, сигнатуры которых состоят из одной бинарной операции. Эту операцию будем обозначать точкой $(\cdot)$ и условно называть в этом случае умножением.

Группоидом называют любую алгебру $\mathcal{G} = (G, \cdot)$, сигнатура которой состоит из одной бинарной операции. В группоиде на бинарную операцию нет никаких ограничений.

Группоид $(G, \cdot)$ называют **полугруппой**, если его операция **ассоциативна**, т.е. для любых элементов a, b, c *носителя* G выполняется равенство $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Группоид $\mathcal{G} = (G, \cdot)$ называют **моноидом**, если его операция **ассоциативна** и относительно операции существует **нейтральный элемент**.
Его называют **нейтральным элементом моноида** $\mathcal{G}$ или **единицей моноида** и обозначают $\mathbf{1}$.

Моноид $\mathcal{G} = (G, \cdot)$ есть полугруппа, в которой для любого a имеют место равенства $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$, где $\mathbf{1}$ — нейтральный элемент (единица) моноида.

При задании моноида можно в сигнатуре указать только бинарную операцию, описав ее свойства дополнительно, а можно включить в сигнатуру нульарную операцию — нейтральный элемент моноида. На практике используют оба способа.

Пример 8.3. а. $(2^{A\times A},\ \circ,\ \mathrm{id}_A)$ Множество всех бинарных отношений на произвольном множестве A с операцией композиции отношений будет моноидом.
Для любых бинарных отношений ρ, τ и σ на множестве A имеют место равенства $\rho \circ (\tau \circ \sigma) = (\rho \circ \tau) \circ \sigma$ — операция ассоциативна.

Нейтральным элементом будет диагональ множества $A \times A$, поскольку $\mathrm{id}_A \circ \rho = \rho \circ \mathrm{id}_A = \rho$.

Группоид $\mathcal{G} = (G, \cdot)$ называют **группой**, если

1) операция $\cdot$ ассоциативна,
2) существует нейтральный элемент (единица) $\mathbf{1}$ относительно умножения,
3) для каждого $a \in G$ существует такой элемент $a' \in G$, называемый **обратным** к a, что $a \cdot a' = a' \cdot a = \mathbf{1}$.

Группа — это моноид, в котором для **каждого** элемента существует обратный элемент.

Теорема 1. В любой группе $\mathcal{G} = (G, \cdot)$ для каждого $a \in G$ элемент, обратный к a, единственный.

◄ Пусть в группе $(G, \cdot)$ с единицей $\mathbf{1}$ для некоторого a существуют два элемента a' и a'', обратных к a.
Тогда $a' = a' \cdot \mathbf{1}$ в силу свойства единицы.
Так как $\mathbf{1} = a \cdot a''$, то $a' = a' \cdot (a \cdot a'')$.
Используя ассоциативность и учитывая, что a' — элемент, обратный к a, получим

$$a' \cdot (a \cdot a'') = (a' \cdot a) \cdot a'' = \mathbf{1} \cdot a'' = a''. \qquad \blacktriangleright$$

Полугруппа, операция которой коммутативна, называется **коммутативной полугруппой**.

Моноид, операция которого коммутативна, называется **коммутативный моноид.**

Среди групп также выделяют те, бинарная операция в которых коммутативна, — **коммутативные (абелевы) группы**.

В коммутативных полугруппах и группах бинарную операцию часто обозначают знаком $+$ и называют **сложением**. Нейтральный элемент (если он существует) обозначают знаком $\mathbf{0}$ и называют нулем.

Свойства операции вычисления обратного элемента.

Теорема 2. Пусть $\mathcal{G} = (G, \cdot)$ — группа. Для любых элементов $a, b \in G$ верны тожества

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}; \quad (1)$$
$$(a^{-1})^{-1} = a. \quad (2)$$

◀ Покажем

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

В силу ассоциативности умножения группы имеем

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

Используя еще раз ассоциативность, определение элемента, обратного к данному, и свойства единицы, получим

$$((a \cdot b) \cdot b^{-1}) \cdot a^{-1} = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot a^{-1} = \mathbf{1}.$$

Итак, $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = \mathbf{1}$ — для $a \cdot b$ найден правый обратный.

Точно так же доказывается, что $(b^{-1} \cdot a^{-1})(a \cdot b) = \mathbf{1}$, т.е. найден левый обратный.

Поэтому элемент $b^{-1} \cdot a^{-1}$ является обратным к элементу $a \cdot b$.

Обратный элемент единственный в силу теоремы о единственности обратного элемента в группе, и поэтому

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

Равенство $(a^{-1})^{-1} = a$ следует непосредственно из определения элемента, обратного к данному.

Действительно, определение элемента a^{-1}, обратного к a, равенством $a^{-1} \cdot a = a \cdot a^{-1} = \mathbf{1}$ можно рассматривать как определение $(a^{-1})^{-1}$ — обратного элемента к a^{-1}, которым является, согласно этим равенствам, элемент a. Обратный элемент единственный в силу теоремы о единственности обратного элемента в группе, т.е. $a = (a^{-1})^{-1}$. ▶

Теорема 3. В любой группе $\mathcal{G} = (G, \cdot, \mathbf{1})$ справедливы **левый** и **правый законы сокращения**:
если $a \cdot x = a \cdot y$, то $x = y$,
если $x \cdot a = y \cdot a$, то $x = y$.

◀ Пусть $a \cdot x = a \cdot y$.
Умножим обе части этого равенства слева на элемент a^{-1}.
Получим

$a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (a \cdot y)$
в силу ассоциативности $(a^{-1} \cdot a) \cdot x = (a^{-1} \cdot a) \cdot y.$
поскольку $a^{-1} \cdot a = \mathbf{1} \;\Rightarrow\; \mathbf{1} \cdot x = \mathbf{1} \cdot y \;\Rightarrow\; x = y$

Доказан левый закон сокращения. Аналогично доказывается и правый закон. ▶

8.3. Решение уравнений в группе

Пусть $\mathcal{G} = (G, \cdot, \mathbf{1})$ — группа, a, b — фиксированные элементы G.
Рассмотрим задачу решения уравнений

$$a \cdot x = b, \tag{8.1}$$

$$x \cdot a = b \tag{8.2}$$

в группе $\mathcal{G}$.
т.е. поиска всех таких элементов $x \in G$, для которых уравнение (8.1) (или (8.2)) превращается в тождество.

Теорема 4. В любой группе $\mathcal{G}$ уравнения вида $a \cdot x = b$ (8.1)
и $x \cdot a = b$ (8.2)
имеют решения, и притом единственные.

◀ Покажем, что $x = a^{-1} \cdot b$ есть решение (8.1).

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

Докажем единственность решения.
Пусть для фиксированных a и b и некоторого x выполнено равенство $a \cdot x = b$.
В группе для любого a существует и однозначно определен элемент a^{-1}, обратный к a.

Умножим на a^{-1} обе части равенства и преобразуем, используя ассоциативность операции в группе.

$$\begin{gathered} a^{-1} \cdot (a \cdot x) = a^{-1} \cdot b \ \Rightarrow \\ \Rightarrow \ (a^{-1} \cdot a) \cdot x = a^{-1} \cdot b \ \Rightarrow \\ \Rightarrow \ \mathbf{1} \cdot x = a^{-1} \cdot b \ \Rightarrow \\ \Rightarrow x = a^{-1} \cdot b. \end{gathered}$$

Это решение единственное в силу единственности обратного элемента.

Аналогично из $x \cdot a = b$ получаем $x = b \cdot a^{-1}$, и это решение также единственное. ▶

ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ.

Нуль относительно операции

Элемент $\mathbf{0}$ множества A называют **левым** (**правым**) **нулем** относительно данной операции $*$, если $\mathbf{0} * x = \mathbf{0}$ ($x * \mathbf{0} = \mathbf{0}$) для любого $x \in A$.

Если $\mathbf{0}'$ — левый нуль, а $\mathbf{0}''$ — правый нуль, то они совпадают.

Если $\mathbf{0}'$ и $\mathbf{0}''$ существуют, то они совпадают, так как $\mathbf{0}' = \mathbf{0}' * \mathbf{0}'' = \mathbf{0}''$, и в этом случае говорят просто о **нуле относительно операции**.

Нуль единственный и для него одновременно выполнены оба равенства $\mathbf{0} * x = \mathbf{0}$ и $x * \mathbf{0} = \mathbf{0}$.

Пример 8.4. **а.** На множестве целых чисел нулем относительно операции умножения будет число 0.

б. На множестве квадратных матриц вида $\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}$, где элементы a и b — действительные числа, любая матрица вида $\begin{pmatrix} 0 & 0 \\ d & 1 \end{pmatrix}$ будет правым нулем относительно операции умножения.

$$\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ d & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ d & 1 \end{pmatrix}.$$

Левого нуля в этом множестве нет .

Правых нулей имеется больше одного. #

Примеры алгебр.

Пример 8.5. Алгебра $(\mathbb{Z}^+, +)$, где носитель — множество $\mathbb{Z}$ неотрицательных целых чисел, а сигнатура состоит из одной операции сложения, есть коммутативный моноид, в котором нейтральный элемент — это число 0.
Сумма двух неотрицательных целых чисел есть целое неотрицательное число, операция сложения ассоциативна, коммутативна и для любого целого числа n имеет место равенство $n + 0 = n$.

Пример 8.6. Алгебра $(\mathbb{Z}, \cdot)$, у которой носителем является множество целых чисел, а сигнатура состоит из одной операции умножения, есть коммутативный моноид. Нейтральным элементом этого моноида является число 1.

Пример 8.7. Пусть A — конечное множество, а A^n — множество кортежей длины n. На множестве всех кортежей $A^+ = \bigcup\limits_{n\geq 1} A^n$ определим операцию **соединения (конкатенации) кортежей** следующим образом:

$$(a_1, \ldots, a_m) \cdot (b_1, \ldots, b_k) = (a_1, \ldots, a_m, b_1, \ldots, b_k).$$

Введенная операция ассоциативна, но не имеет нейтрального элемента. Таким образом, построена полугруппа, но не моноид.

Чтобы превратить эту полугруппу в моноид, расширим носитель полугруппы, введя понятие **нулевой декартовой степени** A^0 произвольного множества A.
Под A^0 понимают одноэлементное множество $\{\lambda\}$, единственный элемент которого называют **пустым кортежем**
Обозначив $A^* = A^0 \cup A^+$, по определению для любого $x \in A^*$ полагаем $x \cdot \lambda = \lambda \cdot x = x$.

В результате получим алгебру $(A^*, \cdot)$.
Это моноид, с нейтральным элементом λ.
Этот моноид называют **свободным моноидом**, порожденным множеством A.

Алгебры однотипные

Для алгебры $\mathcal{A} = (A, \Omega)$ обозначим через $\Omega^{(n)}$ подмножество сигнатур Ω, состоящее из всех n-арных операций. Тогда $\Omega = \bigcup\limits_{n \geq 0} \Omega^{(n)}$.

Рассмотрим алгебру

$$\mathcal{A}_1 = \left(2^M, \left\{\cup, \cap, \setminus, \Delta, \overline{\ }, \varnothing, M\right\}\right).$$

Носителем является множество всех подмножеств произвольно фиксированного множества M. Сигнатура состоит из следующих операций над множествами: объединения, пересечения, разности, симметрической разности, дополнения, пустого множества и множества M. Пустое множество и множество M определяют нульарные операции.

Имеем:

$$\Omega^{(0)} = \{\varnothing,\ M\},$$
$$\Omega^{(1)} = \left\{\overline{\ }\right\},$$
$$\Omega^{(2)} = \{\cup,\ \cap,\ \setminus,\ \Delta\},$$
$$\Omega^{(n)} = \varnothing \text{ при } n > 2.$$

Определение 8.5. Две алгебры $\mathcal{A}_1 = (A_1,\ \Omega_1)$ и $\mathcal{A}_2 = (A_2,\ \Omega_2)$ называют **однотипными**, если существует такая *биекция* Ω_1 на Ω_2, при которой n-арная операция из Ω_1 для любого n переходит в n-арную из Ω_2.

Нередко сигнатуры однотипных алгебр и элементы этих сигнатур — операции — обозначают одинаково. Так, мы пишем $(\mathbb{R},\ +,\ \cdot,\ 0,\ 1)$ и $(\mathbb{Q},\ +,\ \cdot,\ 0,\ 1)$, хотя первая алгебра задана на множестве всех действительных чисел, а вторая — на множестве рациональных чисел, и, например, сложение в первой алгебре, строго говоря, не есть та же самая операция, что сложение во второй алгебре. В общем случае мы часто будем говорить о различных (но однотипных) Ω-алгебрах, заданных на разных носителях, понимая, что Ω есть общее для всех этих алгебр обозначение их сигнатур.

Пример 8.8. Алгебра $(2^M,\ \cup,\ \cap,\ \varnothing,\ M)$, заданная на множестве всех подмножеств множества M, и алгебра $\mathcal{A}_3 = (\mathbb{R},\ +,\ \cdot,\ 0,\ 1)$, заданная на множестве действительных чисел, однотипны.

Биекцию (*взаимно однозначное соответствие*) между их сигнатурами, которая сохраняла бы арность операций, можно определить и так:

$\cup \mapsto +$, $\cap \mapsto \cdot$, $\varnothing \mapsto 0$, $M \mapsto 1$.

Указанный способ задания биекции не единственный. Например, ее можно определить так:

$\cup \mapsto \cdot$, $\cap \mapsto +$, $\varnothing \mapsto 1$, $M \mapsto 0$.

Не являются однотипными и алгебры $\left(2^M, \overline{\ }\right)$ и $(\mathbb{N}, +)$, ибо в первой алгебре единственная операция ее сигнатуры является унарной, а во второй — бинарной. #