АЛГЕБРА

Профессор
Мартынов Л.М.

ОмГУПС_ИАТИТ_гр 23п, 23с_
1с_ 2013-14 уч. год

ГЛАВА III. Основные алгебраические структуры

Лит-ра: [1], стр. 31-65.

§ 0. Бинарные алгебраические операции и их свойства
§ 1. Понятие полугруппы и моноида, их простейшие свойства
§ 2. Понятие группы и его простейшие свойства
§ 3. Понятие кольца и его простейшие свойства
§ 4. Понятие поля и его простейшие свойства
§ 5. Подструктуры
§ 6. Изоморфизм алгебраических структур

ЛЕКЦИЯ 5

§ 1. Понятие полугруппы и моноида, их простейшие свойства

§ 1. Понятие полугруппы и моноида, их простейшие свойства

Определение 1. Непустое множество S с определенной на нем (бинарной) операцией $\square$ называется *полугруппой*, если эта операция ассоциативна, т.е

$$(a \square b) \square c = a \square (b \square c)$$

для любых элементов a,b,c *из* S.

Обозначение: $(S, \square)$.

Определение 2. Полугруппа M с нейтральным элементом e, *т.е. таким элементом, что*

$$a \square e = e \square a = a$$

для любого элемента a *из* M называется *моноидом*.

§ 1. Понятие полугруппы и моноида, их простейшие свойства

- Примерами моноидов являются числовые множества **N**, **Z**, **Q**, **R** относительно обычного умножения и **Z**, **Q**, **R** относительно обычного сложения.
- Важнейшими примерами моноидов являются свободные моноиды, которые широко применяются в теориях формальных языков, кодов и криптографии.

Свободные моноиды и полугруппы

- Пусть дано некоторое непустое множество A, которое будем называть ***алфавитом***.
- Элементы множества A условимся называть ***буквами***.
- Под ***словом*** в алфавите A будем понимать любой конечный упорядоченный набор необязательно различных букв.
- Условимся рассматривать и ***пустое слово***, которое будем обозначать буквой e.
- *Длиной слова* называется число $l(w)$ всех букв в его записи, в частности, $l(e)=0$.

Свободные моноиды и полугруппы

- Обозначим через A^* множество всех слов в алфавите A.
- Определим на этом множестве операцию приписывания (контактенации) слов:

$$x_1x_2\ldots x_k \cdot y_1y_2\ldots y_m = x_1x_2\ldots x_ky_1y_2\ldots y_m,$$

- где k, m – любые натуральные числа, а $x_1, x_2, \ldots, x_k$, $y_1, y_2, \ldots, y_m$ – произвольные буквы;
- кроме того, для любого слова w и пустого слова e положим

$$w \cdot e = e \cdot w = w.$$

Свободные моноиды и полугруппы

- Легко понять, что относительно так определенной операции умножения множество A^* является моноидом (его называют *свободным моноидом над алфавитом* A).
- а множество A^+ всех непустых слов - полугруппой (её называют *свободной полугруппой над алфавитом* A).
- Главным свойством, характеризующим свободные моноиды и полугруппы, является *однозначное представление их непустых слов в виде произведения букв алфавита* A.

Свободные моноиды и полугруппы

- Свободные моноиды широко используются в теории алфавитного кодирования. Подмножество C свободного моноида A^* называется *кодом над* A, если любое слово в алфавите C имеет только одно представление в виде произведения элементов из C.
- Например, если $A = \{a,b\}$, то подмножество $C = \{a^2, a^3\}$ моноида A^* не является кодом над A^*, так как

$$a^6 = a^2 \cdot a^3 = a^3 \cdot a^2$$

- и однозначность представления нарушается, а подмножество $C_n = \{ab^k \mid k = 1,2,..,n\}$ при любом натуральном n, как нетрудно понять, является кодом над C.

Свободные моноиды и полугруппы

- Последнее позволяет с помощью двухбуквенного алфавита закодировать любой конечный алфавит, следовательно, и любое сообщение в нем.
- Однозначность представления слов через элементы кода обеспечивают безошибочное восстановление исходной информации, т.е. декодирование.
- Это обстоятельство широко используется при передаче информации по каналам связи. Обычно используется алфавит {0,1}.
- Это объясняется удобством интерпретации этого алфавита при передачи двоичной информации по каналам связи, напр., разной частотой для передачи 1 и 0.

Свободные моноиды и полугруппы

- Для кодирования русского алфавита можно использовать код :
- А – 01, Б – 011, В – 0111, Г – 01111, Д – 011111 и т. д.
- Например, слово ГАД будет закодировано при этом следующим образом: 011110101111 1.
- Для декодирования надо найти цифру 0 и все единицы правее ее до следующего нуля и восстановить соответствующую букву.

Произведение элементов в полугруппе

- Пусть S – мультипликативная полугруппа. Нетрудно понять, что каким бы образом не расставляли скобки при выполнении умножения выбранных n элементов $a_1, a_2, \ldots, a_n$ полугруппы S, ввиду ассоциативности операции умножения всегда будем получать один и тот же элемент полугруппы S.
- Поэтому скобки можно опускать, обозначать этот элемент через $a_1a_2 \ldots a_n$ и называть *произведением элементов* $a_1, a_2, \ldots, a_n$.
- Таким образом, ***произведение элементов в полугруппе не зависит от расстановки скобок***.

Натуральная степень элемента в мультипликативной полугруппе

- В случае, когда все сомножители произведения равны между собой и равны элементу *a* полугруппы *S*, то говорят об *n-й степени* элемента *a* в полугруппе *S*, которую обозначают a^n , т.е.

$$a^n = \underbrace{aa\ldots a}_{n}.$$

- Для моноидов полагают $a^0=e$, где e – единица моноида.

Св-ва натуральной степени элемента в мультипликативной полугруппе

- Легко убедиться в том, что для любого элемента a полугруппы S и любых натуральных чисел k и m справедливы равенства

$$a^k \cdot a^m = a^m \cdot a^k = a^{k+m}, \qquad (1)$$

$$(a^k)^m = a^{km}. \qquad (2)$$

В случае моноидов аналогичные равенства выполняются для любых неотрицательных целых чисел k и m.

Натуральное кратное элемента в аддитивной полугруппе и его св-ва

- Целое кратное в аддитивной полугруппе определяется по аналогии с целой степенью в мультипликативной полугруппе:

$$na = \underbrace{a + a + \ldots + a}_{n}.$$

- Для аддитивных моноидов полагают $0a = 0$, где 0 – нуль моноида.
- В частности, для любого элемента a аддитивной полугруппы S и любых натуральных чисел k и m справедливы равенства

$$ka+ma=(k+m)a, \qquad (1')$$

$$k(ma)=(km)a. \qquad (2')$$

- В случае аддитивных моноидов аналогичные равенства выполняются для любых неотрицательных целых чисел k и m.

§ 2. Понятие группы и его простейшие свойства

§ 2. Понятие группы и его простейшие свойства

- Понятие группы является одним из важнейших понятий современной математики.
- Группы вездесущи: алгебра, геометрия, математический анализ, теоретическая физика, теория линейных кодов, криптография, кристаллография – вот неполный перечень тех областей науки, где применяются группы.
- Термин «группа» введен французским алгебраистом Э.Галуа (**1811–1832**) в 1832 г.

ЭВАРИСТ ГАЛУА
(1811—1832)

§ 2. Понятие группы и его простейшие свойства

- ***Определение* 1.** Непустое множество G с определенной на нем операцией $\square$ называется ***группой***, если в G истинны формулы:
- (G1) $\forall x \forall y \forall z ((x \square y) \square z = x \square (y \square z))$, т.е. операция $\square$ ассоциативна;
- (G2) $\exists e \forall x (x \square e = e \square x = x)$, т.е. относительно операции $\square$ существует нейтральный элемент e;
- (G3) $\forall x \exists x^* (x \square x^* = x^* \square x = e)$, т.е. каждый элемент из G обладает симметричным относительно операции $\square$.

- Можно доказать единственность нейтрального и симметричного элементов в группе.

§ 2. Понятие группы и его простейшие свойства

- Понятие группы можно определить, используя понятие моноида.

- ***Определение 1'.*** Группой называется моноид, в котором каждый элемент обладает симметричным.

Теорема 1. Полугруппа является группой тогда и только тогда, когда для любых элементов a и b из S в ней разрешимы

§ 2. Понятие группы и его простейшие свойства

- ***Определение 1”.*** Группой называется полугруппа S, в которой для любых элементов a *и* b *из* S разрешимы уравнения (*): $a \circ x = b$ и $y \circ a = b$.

- На самом деле, легко видеть, что в любой группе уравнения (*)***однозначно разрешимы:***
  - $x_0 = a^* \circ b$; $y_0 = b \circ a^*$;
- в этом случае говорят, что ***операция в группе обратима***.
- Кроме того, ***операция в группе обладает свойством сократимости, т.е.***
- $a \circ c = b \circ c \Rightarrow a = b$ и $c \circ a = c \circ b \Rightarrow a = b$.

§ 2. Понятие группы и его простейшие свойства

- ***Определение 2.*** Если операция группы *G* коммутативна, т. е. в *G* истинна формула
- (G4) $\forall x \forall y\,(x \circ y = y \circ x)$,
- то группа называется *коммутативной*, или *абелевой*.

НИЛЬС ГЕНРИХ АБЕЛЬ
(1802—1829)

- (В честь норвежского математика **Н.Х.Абеля**, впервые уделившего много внимания таким группам.)

§ 2. Понятие группы и его простейшие свойства

- Если число элементов группы G конечно, то группа G называется *конечной*;
- число элементов конечной группы обозначается символом $|G|$ и называется *порядком группы G.*
- Если число элементов группы G бесконечно, то группа G называется *бесконечной*;
- при этом говорят, что группа G имеет бесконечный порядок и пишут $|G| = \infty$.

§ 1. Понятие полугруппы и моноида, их простейшие свойства

- При изучении групп операцию зачастую называют сложением или умножением и обозначают знаками $+$ или $\cdot$ (иногда, чтобы не путать с арифметическим сложением или умножением, знаками $\oplus$ или $\otimes$);
- в первом случае говорят, что принята *аддитивная терминология*, во втором – *мультипликативная терминология*.
- В общем случае придерживаются мультипликативной терминологии (в теории абелевых групп предпочитают аддитивную терминологию), что мы и будем в дальнейшем делать.
- Для перехода от одной терминологии к другой можно пользоваться следующим словариком.

Словарик перехода от одной терминологии к другой

Термины и обозн. в общем случае	Мультипликативн. термины и обозн.	Аддитивные термины. и обозн.
Операция: □	*Умножение*: ·	*Сложение:* +
Результат: a □ b	*Произведение:* $a \cdot b$	*Сумма:* $a+b$
Комп. опер.: a, b	*Сомножители:* a, b	*Слагаемые:* a, b
Нейтральный : e	*Единица,* e *или* 1	*Нуль:* 0
Симметрич. : a^*	*Обратный:* a^{-1}	*Противополож.:* $-a$
	Степень: a^n	*Кратное*: na

§ 2. Понятие группы и его простейшие свойства

- **Пример 1.** Числовые множества **Z**, **Q**, **R** соответственно целых, рациональных и действительных относительно обычной операции сложения,
- и множества $\mathbf{Q^{-1}= Q\backslash\{0\}}$, $\mathbf{R^{-1} = R\backslash\{0\}}$ относительно умножения являются бесконечными абелевыми группами.
- **Пример 2.** Пример мультипликативной группы порядка 2 доставляет множество $C_2 = \{1,-1\}$ относительно обычного умножения,
- а пример аддитивной группы порядка 2 дает множество $Z_2 = \{0,1\}$ относительно сложения по модулю 2:
- Обе эти группы абелевы.

$\oplus_2$	0	1
0	0	1
1	1	0

§ 2. Понятие группы и его простейшие свойства

- Полезно иметь в виду следующее утверждение.

Т е о р е м а 2. *В мультипликативном моноиде M множество M^{-1} всех обратимых элементов образует группу*.

- ◘ Пусть a, b – произвольные элементы из M . Докажем сначала замкнутость множества M^{-1} относительно операции $\cdot$ умножения моноида M, т.е., что элемент $a \cdot b$ обратим в M.
- Для этого достаточно проверить, что элемент $b^{-1} \cdot a^{-1}$ является обратным для $a \cdot b$:

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

- Аналогично проверяется, что $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$.

§ 2. Понятие группы и его простейшие свойства

- **Т е о р е м а 2.** *В мультипликативном моноиде M множество M^{-1} всех обратимых элементов образует группу*.

- ◘ Далее, ассоциативность операции умножения в M^{-1} следует из ассоциативности ее в моноиде M.
- Единица моноида M обратима ($e \cdot e = e$) и потому $e \in M^{-1}$.
- Наконец, элементы a и a^{-1} взаимно обратные и, следовательно, $a^{-1} \in M^{-1}$.
- Таким образом, M^{-1} – группа. ◙
- Например, $\mathbf{Z}^{-1} = \{-1, 1\}$ – группа ***всех обратимых элементов моноида*** $(\mathbf{Z}, \cdot)$.

§ 2. Понятие группы и его простейшие свойства

- Легко проверяется, что в ***любой группе*** $(G; \square)$ ***истинны следующие свойства:***

$$(x^*)^* = x, \qquad (1)$$

$$(x \square y)^* = y^* \square x^*. \qquad (2)$$

- В случае если принята мультипликативная терминология, свойства (1) и (2) переписываются в более привычной форме

$$(x^{-1})^{-1} = x, \qquad (1')$$

$$(xy)^{-1} = y^{-1}x^{-1}. \qquad (2')$$

- ¬ Обратим внимание на то, что при взятии обратного элемента для произведения порядок сомножителей в правой части равенства (2') меняется на обратный. В абелевых группах это не имеет значения.

$$(xy)^{-1} = y^{-1}x^{-1}. \qquad (2')$$

- Свойство (2’) по индукции распространить на любое конечное число сомножителей:

$$(x_1 x_2 \cdots x_{n-1} x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \cdots x_2^{-1} x_1^{-1} \quad . \qquad (2'')$$

§ 2. Понятие группы и его простейшие свойства

- Поскольку любая группа является моноидом, то в группе можно говорить о любой неотрицательной целой степени любого ее элемента.
- На самом деле, в группе можно определить целую степень любого ее элемента.
- **Определение 4.** Для любого целого числа *n* и любого элемента *a* группы *G* *n*-я степень *a* есть:

$$a^n = \begin{cases} \underbrace{aa\ldots a}_{n}, & если \quad n > 0; \\ e, & если \quad n = 0; \\ \underbrace{a^{-1}a^{-1}\ldots a^{-1}}_{-n} = (a^{-1})^{-n}, & если \quad n < 0. \end{cases}$$

§ 2. Понятие группы и его простейшие свойства

- Можно проверить, что для любого элемента a группы G и любых целых чисел k и m справедливы равенства

$$a^k \cdot a^m = a^m \cdot a^k = a^{k+m}, \quad (3)$$

$$(a^k)^m = a^{km}. \quad (4)$$

- Доказательство этих равенств проводится непосредственным перебором всех возможных случаев, учитывая, что для неотрицательных целых чисел эти свойства справедливы в любом моноиде.

§ 2. Понятие группы и его простейшие свойства

- Целое кратное в аддитивной группе определяется по аналогии с целой степенью в мультипликативной группе:

$$na = \begin{cases} \underbrace{a + a + \ldots + a}_{n}, & \text{если} \quad n > 0; \\ 0, & \text{если} \quad n = 0; \\ \underbrace{(-a) + (-a) + \ldots + (-a)}_{-n} = (-n)(-a), & \text{если} \quad n < 0. \end{cases}$$

- В частности, для любого элемента *a* аддитивной группы *G* и любых целых чисел *k* и *m* справедливы равенства
  - $ka + ma = (k + m)a$, (3’)
  - $k(ma) = (km)a$. (4’)

Симметрическая группа подстановок *n*-й степени

- До сих пор мы приводили примеры абелевых групп. Большой спектр примеров не абелевых конечных групп доставляют группы подстановок, к рассмотрению которых мы и перейдем.
- Напомним, что взаимно-однозначное отображение множества $M = \{1,2,\ldots,n\}$ на себя называется *подстановкой n-й степени*.
- Каноническая запись подстановки:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix},$$

- где $k_1, k_2, \ldots, k_n$ – перестановка множества M.
- Очевидно, что ***число всех подстановок n-множества M*** равно числу перестановок этого множества и, следовательно, ***равно n!***

Симметрическая группа подстановок *n*-й степени

- Пусть S_n обозначает множество всех подстановок *n*-й степени. Рассмотрим на этом множестве операцию умножения преобразований, заключающуюся в их последовательном выполнении (суперпозиции) отображений.
- А именно, для любых подстановок α и β из S_n и любого элемента $x \in M$ имеем
  - $(\alpha \circ \beta)(x) = \alpha(\beta(x))$.
- Обратим внимание на то, что сначала действует вторая подстановка, а затем первая.
- Например, если
- $$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix}$$
- то $$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}.$$

Симметрическая группа подстановок *n*-й степени

- Легко понять, что произведение любых двух подстановок *n*-ой степени будет снова подстановкой *n*-ой степени и умножение подстановкой *n*-й степени ассоциативно.
- Отсюда следует, что
- ***множество S_n относительно умножения подстановок является полугруппой***.
- Легко понять, что роль единицы в полугруппе $(S_n; \square)$ играет тождественная подстановка

$$\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

и поэтому $(S_n; \square)$ - моноид.

Симметрическая группа подстановок *n*-й степени

- Наконец, для любой подстановки

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

существует обратная к ней подстановка

$$\alpha^{-1} = \begin{pmatrix} k_1 & k_2 & \dots & k_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

- Таким образом, ***множество S_n всех подстановок n-й степени относительно умножения подстановок является группой,***
- которая и называется ***симметрической группой подстановок n-ой степени***.

Симметрическая группа подстановок *n*-й степени

- Заметим, что группа S_n конечна, она содержит $n!$ подстановок.
- ***При n > 2 группа S_n некоммутативна.***
- В самом деле, в этом убеждает нас следующий пример.
- Пусть

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix}.$$

- Тогда $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix}$, а $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}$.

Спасибо за внимание!