МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
"ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ"

С.В. Борзунов, Р.Х. Вахитов, Е.В. Вахитова

ФУНДАМЕНТАЛЬНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА

Часть I

Структуры алгебры

Учебно-методическое пособие для вузов

Издательско-полиграфический центр
Воронежского государственного университета
2012

Введение

Содержание данного учебно-методического пособия "Фундаментальная и компьютерная алгебра. Часть 1. Структуры алгебры" составляет материал нескольких тем базовой учебной дисциплины профессионального цикла "Фундаментальная и компьютерная алгебра", изучение которой предусмотрено основной образовательной программой подготовки бакалавра по направлению "Математика и компьютерные науки" для студентов факультета компьютерных наук ФГБОУ ВПО "Воронежский государственный университет". Целью учебной дисциплины является формирование представлений о фундаментальной алгебре: структуры алгебры, линейная алгебра, алгебра многочленов и о компьютерной алгебре. Основными задачами учебной дисциплины являются овладение фундаментальными базовыми знаниями в области фундаментальной и компьютерной алгебры, умением формулировать и доказывать теоремы, самостоятельно решать классические задачи фундаментальной алгебры.

Цель учебно-методического пособия состоит в том, чтобы помочь студентам, изучающим учебную дисциплину "Фундаментальная и компьютерная алгебра", формировать представление о структурах алгебры, приобрести навыки и умения практического использования математических методов при решении задач. В результате изучения учебной дисциплины студент должен знать теоретический материал и уметь формулировать результат, строго доказывать утверждение, грамотно пользоваться языком фундаментальной и компьютерной алгебры.

Учебно-методическое пособие состоит из пяти глав. В конце каждой главы приведены вопросы для самоконтроля и упражнения для самостоятельной работы. Определения, теоремы и их доказательства иллюстрируются численными примерами, цель которых — пояснить общую теорию.

В каждой главе определения, формулы и теоремы имеют независимую нумерацию.

Определение 5. *Элемент a' из непустого множества A с бинарной алгебраической операцией $*$ и нейтральным элементом e называется симметричным элементом для элемента $a \in A$, если* $a * a' = a' * a = e$.

Пример. $\mathbf{Z}$ – множество целых чисел, $\mathbf{Z} \neq \emptyset$, $(+)$ – бинарная алгебраическая операция на $\mathbf{Z}$, так как

$$\Big(\forall\, a,\, b \in \mathbf{Z}\Big)\ \Big(\exists\,!\, c \in \mathbf{Z}\Big)\ \Big(c = a + b\Big).$$

Нейтральный элемент $e = 0$, так как $0 \in \mathbf{Z}$ и

$$\Big(\forall\, a \in \mathbf{Z}\Big)\ \Big(a + 0 = 0 + a = a\Big).$$

Элемент $a' = -a$ является симметричным для элемента $a \in \mathbf{Z}$, так как

$$a + (-a) = (-a) + a = 0.$$

Определение 6. *Полугруппой называется непустое множество G с бинарной алгебраической операцией $*$, если выполнена аксиома:*

бинарная алгебраическая операция $*$ на G ассоциативна, т.е. $\Big(\forall\, a,\, b,\, c \in G\Big)\ \Big(a * (b * c) = (a * b) * c\Big)$.

Определение 7. *Моноидом называется непустое множество G с бинарной алгебраической операцией $*$, если выполнены следующие две аксиомы:*

1. $\Big(\forall\, a,\, b,\, c \in G\Big)\ \Big(a * (b * c) = (a * b) * c\Big)$.

2. *В множестве G имеется нейтральный элемент e относительно операции $*$, т.е.*

$\Big(\exists\, e \in G\Big)\ \Big(\forall\, a \in G\Big)\ \Big(a * e = e * a = a\Big)$.

Определение 8. *Группой называется непустое множество G с бинарной алгебраической операцией $*$, если выполнены следующие три аксиомы:*

1. $\Big(\forall\, a,\, b,\, c \in G\Big)\ \Big(a * (b * c) = (a * b) * c\Big)$.

2. $\Big(\exists\, e \in G\Big)\ \Big(\forall\, a \in G\Big)\ \Big(a * e = e * a = a\Big)$.

3. *Для каждого элемента $a \in G$ имеется симметричный элемент $a' \in G$, то есть*

$\Big(\forall\, a \in G\Big)\ \Big(\exists\, a' \in G\Big)\ \Big(a * a' = a' * a = e\Big)$.

Примеры. 1) $\mathbf{N}$ относительно сложения образует полугруппу, которую называют аддитивной полугруппой натуральных чисел;

2) $\mathbf{N}$ относительно умножения образует моноид, который называют мультипликативным моноидом натуральных чисел;

3) $\mathbf{Z}$ относительно сложения образует группу, которую называют аддитивной группой целых чисел.

Определение 9. *Группа G называется бесконечной (или имеет бесконечный порядок), если множество G бесконечно.*

Группа G имеет порядок n, $n \in \mathrm{N}$, если множество G – конечное множество с числом элементов n.

Определение 10. *Абелевой группой называется группа G с бинарной алгебраической операцией $*$, если выполнена аксиома:*

бинарная алгебраическая операция $*$ коммутативна, то есть

$$\Big(\forall\, a,\, b \in G\Big)\ \Big(a * b = b * a\Big).$$

Если $*$ не является коммутативной, то следует различать левый и правый нейтральные элементы.

Пример. Аддитивная группа целых чисел является абелевой группой, так как $\Big(\forall\, a,\, b \in \mathbf{Z}\Big)\ \Big(a + b = b + a\Big)$.

Приведем пример группы, не являющейся абелевой группой. Для этого изучим группу подстановок.

Пусть $A = \{1,\, 2,\, \ldots, n\}$, $n \in \mathbf{N}$.

Определение 11. *Подстановкой множества A (первых n натуральных чисел, начиная с 1) называется взаимно-однозначное отображение множества A на себя.*

Обозначение:

$$\varphi = \begin{pmatrix} 1 & 2 & ... & n \\ \varphi(1) & \varphi(2) & ... & \varphi(n) \end{pmatrix}.$$

Порядок чисел в первой строке можно как угодно изменить, но надо всегда следить за тем, чтобы для $(\forall\, k \in A)$ число $\varphi(k)$ было записано под k. Заметим, что понятие подстановки можно было бы ввести для произвольного конечного множества натуральных чисел, так как в этом случае можно эти числа занумеровать и работать с их номерами.

Множество всех подстановок множества A обозначим через S_n; элементы множества S_n будем называть еще подстановками степени n.

Если $\varphi \in S_n$, то 1) φ – взаимно-однозначное отображение;

2) $\varphi(A) = A$, то есть $\{\varphi(1), \varphi(2), ..., \varphi(n)\} = \{1, 2, ..., n\}$. Так как A – конечно, то из условия 1) следует 2) и обратно: из условия 2) следует 1).

Произведение $\varphi\psi$ двух подстановок φ и ψ множества A определяется как композиция отображений φ и ψ $(\varphi\psi = \underset{\leftarrow}{\varphi \circ \psi})$.

Таким образом, по определению, $\varphi(\psi(i)) = \varphi\psi(i)$ для $i = 1, 2, ..., n$.

Композиция двух взаимно-однозначных отображений множества A на себя есть взаимно-однозначное отображение множества A на себя, следовательно,

$$\Big(\forall\, \varphi,\, \psi \in S_n\Big)\ \Big(\varphi\psi \in S_n\Big).$$

Обозначим через e тождественное отображение множества A на себя: $e(k) = k$, то есть

$$e = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}.$$