Федеральное агентство по образованию

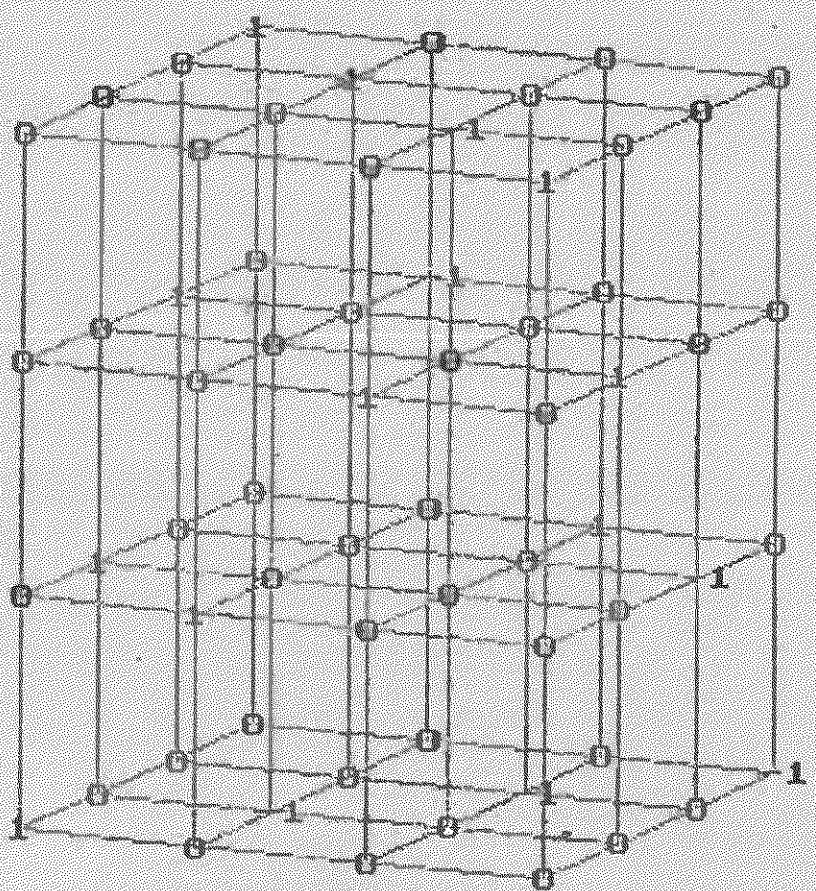
Томский государственный университет систем управления и радиоэлектроники

Кафедра высшей математики (ВМ)

Приходовский М.А.

АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ И АЛГЕБРАИЧЕСКИЕ ОПЕРАЦИИ

Практическое пособие



2006

В данном пособии рассматриваются алгебраические операции, а также алгебраические структуры с одной или несколькими операциями: группы, кольца, поля, модули, конечномерные алгебры. Вводимые понятия иллюстрируются на примерах. Рассматриваются различные задачи с данными алгебраическими структурами.

Может применяться в качестве дополнительного материала при изучении темы «алгебраические структуры» в 1-м семестре.

Содержание.

§1. Множества с одной алгебраической операцией.

На множествах различных объектов вводятся законы, задающие отображение одного или нескольких элементов. Если рассматривается отображение, ставящее в соответствие каждому элементу множества A элемент множества B, то такое отображение называется функцией из A в B, где элементы множества A называются аргументами, а элементы множества B – образами. Возможно также, что $A = B$.

Отображения, при которых двум различным элементам множества ставится в соответствие третий элемент этого множества, называются бинарными алгебраическими операциями.

Определение. Бинарной алгебраической операцией на множестве M называется закон, по которому любой упорядоченной паре элементов из M ставится в соответствие один и только один элемент из M. Множество с введённой бинарной операцией называется группоидом.

Обозначения. Наиболее часто рассматриваются бинарные операции сложение и умножение, операция обозначается $a+b$ или $a \cdot b$. Возможны я другие обозначения, например $a * b$.

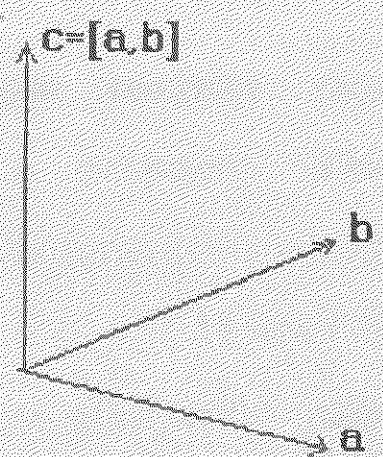
Определение. Бинарная алгебраическая операция называется коммутативной, если $a * b = b * a$ для любых элементов $a, b \in M$. Бинарная алгебраическая операция называется ассоциативной, если $a * (b * c) = (a * b) * c$ для любых элементов $a, b, c \in M$.

Определение. Элемент $e \in M$ называется нейтральным элементом группоида М, если $a * e = e * a = a$ для любого элемента $a \in M$.

Определение. Элемент $b \in M$ называется обратным к элементу $a \in M$, если $a * b = b * a = e$.

Наиболее известные примеры бинарных алгебраических операций - это сложение, умножение, возведение в степень. Сложение и умножение являются коммутативными и ассоциативными операциями. Нейтральный элемент по сложению – число 0, а по умножению – число 1: для любого элемента $a \in A$ выполняется $a \cdot 1 = 1 \cdot a = a$, $a + 0 = 0 + a = a$. Операция возведения в степень не коммутативна и не ассоциативна: например $2^3=8$, но $3^2=9$. $2^{2^3} = 2^8 = 256$, но $(2^2)^3 = 4^3 = 64$. Возведение в степень определено даже не для любых упорядоченных пар чисел для всякого числа $a \neq 0$ верно, что $a^0 = 1$, $0^a = 0$. В то же время выражение 0^0 не определено.

Задача 1.1. Доказать, что на множестве всех векторов трёхмерного пространства с операцией векторного умножения не существует нейтральный элемент.



Решение. Образ векторного произведения $\bar{c} = [\bar{a}, \bar{b}]$ перпендикулярен умножаемым векторам: $\bar{c} \perp \bar{a}$, $\bar{c} \perp \bar{b}$. Предположим, что существует нейтральный элемент относительно данной операции, тогда $\bar{a} = [\bar{a}, \bar{e}]$ для всякого вектора $\bar{a} \in R^3$, откуда

следует $\bar{a} \perp \bar{a}$, что невозможно. Поэтому не существует вектор $\bar{e} \in R^3$, при умножении на который всякий вектор $\bar{a}$ отображался бы в вектор $\bar{a}$.

Задача 1.2. Доказать, что бинарная операция $a * b = \min(a, b)$ на множестве чисел $(-\infty, A]$ является коммутативной и ассоциативной; найти нейтральный элемент.

Решение. Очевидно, что $\min(b, a) = \min(a, b)$. Ассоциативность: $a * (b * c) = (a * b) * c$ выполнена так как при любой расстановке скобок результатом будет минимальное из трёх заданных чисел. Нейтральным элементом является число A, так как для любого $a \in (-\infty, A]$ верно $a \le A$, значит $a * A = a$.

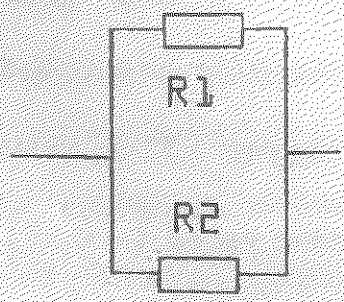
Замечание. Для рассмотренной операции, задаваемой на множестве, неограниченном сверху, а также ограниченном, но не содержащем свою точную верхнюю грань, например $(-\infty, A)$, нейтрального элемента не существует.

Аналогично для множества $[A, +\infty)$ определяется бинарная алгебраическая операция $a * b = \max(a, b)$, причём нейтральным элементом является число A.

Задача 1.3. Доказать, что множество всех сопротивлений (резисторов) образует коммутативный и ассоциативный группоид относительно операции параллельного соединения.

Решение.

Известно, что если сопротивления R_1 и R_2 соединить параллельно, то сопротивление получившегося элемента электрической цепи вычисляется по формуле



$\frac{1}{R} = \frac{1}{R_1} + \frac{1}{R_2}$, т.е. $R = \frac{R_1 R_2}{R_1 + R_2}$.

Можно поставить в соответствие множество сопротивлений и множество неотрицательных чисел. Вводя на множестве неотрицательных действительных чисел $[0, \infty)$ бинарную операцию $a * b = \frac{ab}{a+b}$, докажем, что введённая операция будет коммутативной и ассоциативной. Действительно, $a * b = \frac{ab}{a+b} = \frac{ba}{b+a} = b * a$. Ассоциативность следует из равенств:

$$(a * b) * c = \frac{ab}{a+b} * c = \frac{\frac{ab}{a+b} \cdot c}{\frac{ab}{a+b} + c} = \frac{\frac{abc}{a+b}}{\frac{ab + c(a+b)}{a+b}}$$

$$= \frac{abc}{ab + c(a+b)} = \frac{abc}{ab + ac + bc}.$$

С другой стороны,

$$a * (b * c) = a * \frac{bc}{b+c} = \frac{a \cdot \frac{bc}{b+c}}{a + \frac{bc}{b+c}} = \frac{\frac{abc}{b+c}}{\frac{a(b+c) + bc}{b+c}}$$

$$= \frac{abc}{ab + c(a+b)} = \frac{abc}{ab + ac + bc}.$$

Таким образом, $(a * b) * c = a * (b * c)$.

При этом $a * 0 = 0 * a = 0$, $a * \infty = \infty * a = a$. Последнее следует из того, что $\lim\limits_{b \to \infty} \frac{ab}{a+b} = a$.

Нейтральным элементом относительно операции параллельного соединения будет участок электрической цепи, обладающий нулевой проводимостью, то есть изолятор с бесконечным сопротивлением. Тогда в предельном случае при $R_2 \to \infty$ получаем $\frac{1}{R} = \frac{1}{R_1} + 0$.

Задача 1.4. Доказать, что множество, состоящее из всех интервалов на действительной оси, пустого множества и $(-\infty, +\infty)$, образует коммутативный группоид относительно операции пересечения. Найти нейтральный элемент.

Решение. Пересечением двух интервалов $(a,b) \cap (c,d)$ будет либо интервал, либо пустое множество. Если $(a,b) \subset (c,d)$ (интервал (a,b) содержится в (c,d)) то пересечением будет интервал (a,b), если, напротив, второй интервал является подмножеством первого, то пересечение – интервал (c,d). Если $b \le c$ или $d \le a$, то интервалы не пересекаются, то есть пересечение – пустое множество. Если $a < c$ и $b \in (c,d)$ то $(a,b) \cap (c,d) = (c,b)$.

Нейтральным элементом будет интервал $(-\infty,+\infty)$, так как $(-\infty,+\infty)\cap(a,b)=(a,b)\cap(-\infty,+\infty)=(a,b)$.

Задача 1.5. Доказать, что множество всех интервалов вида (a,∞) (вместе с пустым множеством $\varnothing$) на числовой прямой образует группоид относительно операции объединения и найти нейтральный элемент.

Решение. Очевидно, что объединение - интервал вида:

$(a,\infty)\cup(b,\infty)=\begin{cases}(b,\infty) если a>b\\(a,\infty) если a<b\end{cases}$, поэтому в результате операции пересечения получаем элемент из этого же множества. Нейтральным элементом является пустое множество, так как для любого множества верно $A\cup\varnothing=A$. .

Определение. Непустое множество A, на котором определена бинарная ассоциативная операция, называется группой, если существует нейтральный элемент $e\in A$ и для всякого элемента $a\in A$ существует обратный элемент, то есть такой элемент $b\in A$, что $a*b=b*a=e$.

Докажем свойства:

1. *Если существует нейтральный элемент, то он единственный.*

Допустим, что существует два нейтральных элемента e_1, e_2, при умножении на любой из них всякий элемент сохраняется без изменения. Тогда в произведении e_1e_2 с одной стороны, $e_1e_2=e_1$, поскольку e_2 - нейтральный

элемент, с другой стороны, $e_1 e_2 = e_2$, так как e_1 - нейтральный элемент. Отсюда следует $e_1 = e_2$.

2 *Для каждого элемента в группе существует единственный обратный элемент.*

Допустим, существует два обратных элемента – один по умножению слева, другой по умножению справа. То есть, $ba = e$ и $ac = e$. Тогда в произведении bac в силу ассоциативности: $(ba)c = b(ac)$, откуда следует: $c = ec = (ba)c = b(ac) = be = b$, или $c = b$.

3 $(ab)^{-1} = b^{-1}a^{-1}$.

Для того, чтобы доказать, что обратным элементом к произведению ab является $b^{-1}a^{-1}$, вычислим произведение:

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = (ae)a^{-1} = aa^{-1} = e.$$

Аналогично доказывается, что нейтральный элемент получается в результате умножения в обратном порядке: $(b^{-1}a^{-1})(ab) = e$.

Известные примеры групп. Множество всех действительных чисел R образует группу по сложению (называется также аддитивной группой); множество ненулевых действительных чисел $R \setminus \{0\}$ образует группу по умножению (называется мультипликативной группой).

Группа подстановок. Подстановкой порядка n называется взаимно однозначное отображение множества n натуральных чисел на себя. Для определённости обычно рассматривают первые n чисел. Подстановки представляют в виде матрицы из двух строк и n столбцов, где в первой

строке расположены отображаемые числа, упорядоченные по возрастанию, во второй – соответственно, числа в которые они отображаются.

$$\cdot \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \end{pmatrix}$$

Существует n! различных подстановок порядка n [1]. Рассматривая множество всех подстановок, можем ввести операцию их умножения, определив как композицию. Тождественная подстановка является нейтральным элементом относительно этой операции.

Задача 1.6. Доказать, что группа, состоящая из 3 элементов, является коммутативной.

Решение. Так как A - группа, то она должна содержать единицу относительно операции, действующей в данной группе. Тогда группа состоит из элементов 1, a, b. Рассмотрим всевозможные 9 произведений. Произведение любого элемента на 1 равно исходному элементу. Исследуем произведения a^2, b^2, ab, ba. Для каждого элемента должен существовать обратный, поэтому в каждой строке и каждом столбце должен быть единичный элемент. Таким образом, $a^2=1$ или $ab=1$. Пусть сам элемент a является обратным к a, то есть $a^2=1$. Но тогда $ab \neq 1$, иначе для элемента a существовало бы два различных обратных, а это невозможно. Также при этом не может быть $ab = a$ (тогда элемент b являлся бы нейтральным при умножении на a, но нейтральный элемент единственный, и $b \neq 1$). По этой же причине невозможно $ab = b$. Следовательно, $ab = 1$, это означает, что элемент b - обратный к элементу a относительно операции в этой группе.

Отсюда следует, что $a^2 \neq a$, иначе a также был бы обратным к a, но это невозможно, так как обратный элемент единственный. Остается только одна возможность: $a^2 = b$. Аналогичными рассуждениями доказывается, что $b^2 = a$. Итак, умножение в группе из 3 элементов можно представить следующей таблицей:

	1	a	b
1	1	a	b
a	a	a^2	ab
b	b	ba	b^2

Так как $ab = ba = 1$, группа коммутативна.

Определение. Группы и называются изоморфными, если существует взаимно-однозначное отображение $f : A \to B$, такое, что для любых элементов $a_1, a_2 \in A$ выполняется $f(a_1 * a_2) = f(a_1) * f(a_2)$.

Определение. Пусть A - группа. Подмножество $B \subset A$ называется подгруппой группы A, если B образует группу относительно операции, действующей в группе A. Подгруппа обозначается $B \leq A$.

Критерий подгруппы. Подмножество $B \subset A$ является подгруппой группы A, если для любых элементов $a, b \in B$ выполнено условие $a * b^{-1} \in B$.

(Для групп, где операция – сложение элементов, условие имеет вид $a - b$, а если операция умножение, то $a \cdot b^{-1}$).

Задача 1.7. Доказать, что если $B_1,\ldots,B_k$ являются подгруппами группы A, то их пересечение $B_1 \cap \ldots \cap B_k$ - также подгруппа группы A.

Решение. Пусть элементы a и b принадлежат пересечению подгрупп. Тогда они принадлежат *каждой* из этих подгрупп. Следовательно, по критерию подгруппы, $ab^{-1} \in B_i$ для всякого числа i от 1 до k. То есть, $ab^{-1} \in B_1 \cap \ldots \cap B_k$, откуда по критерию подгруппы следует, что $B_1 \cap \ldots \cap B_k$ - подгруппа группы A.

Задача 1.8. Доказать, что подмножество в Z, состоящее из всех чётных чисел, а также множество всех чисел, кратных какому-либо целому числу α, образует подгруппу по сложению в группе Z всех целых чисел.

Решение. Возьмём любые числа αk и αm, по критерию подгруппы $\alpha k - \alpha m = \alpha(k-m)$, то есть разность также принадлежит рассматриваемому множеству, значит, это подгруппа.

Группы поворотов и симметрий правильных n-угольников. Рассмотрим правильный n-угольник. Поворот на угол кратный 2π/n отображает многоугольник на себя так, что он занимает то же геометрическое место точек на плоскости, что и до отображения.

Например, множество всех поворотов квадрата образует группу, изоморфную подгруппе группы подстановок порядка 4, а именно

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}.$$

В то же время, например, такие подстановки:

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 3 & 4\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 4 & 3\end{pmatrix}$$

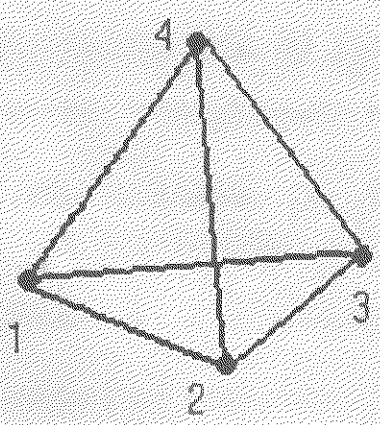
не соответствуют никаким преобразованиям квадрата – ни поворотам, ни отображениям симметрии (здесь меняются местами только две соседние вершины, что невозможно).

Множество всех поворотов плоскости на углы, кратные $\frac{2\pi}{n}$, также образует группу. В группе поворотов плоскости на углы, кратные $\pi/4$, существуют подгруппы, состоящие из всех поворотов на углы, кратные $\pi/2$ и π.

Могут рассматриваться также группы движений и симметрий трёхмерных многогранников.

Задача 1.9. Доказать, что множество всевозможных поворотов и симметрий тетраэдра образует группу, изоморфную группе подстановок 4-го порядка.

Решение. Каждое преобразование симметрии, при котором меняются местами две вершины, соответствует некоторой подстановке, меняющей местами два элемента (такая подстановка называется транспозицией).



Любая подстановка может быть получена из тождественной с помощью конечного числа транспозиций, поэтому любое преобразования тетраэдра может быть получено с помощью последовательного выполнения нескольких отображений симметрии.

Упражнение. Доказать, что множество всех непрерывных взаимно-однозначных отображений отрезка $[a,b] \subset R$ образует группу относительно операции композиции. (Указания: доказать, что композиция непрерывна, рассмотреть тождественное отображение $f(x) = x$ в качестве нейтрального элемента).

Другие известные примеры групп: Группа линейных операторов $L : R^n \to R^n$ относительно операции сложения; группа невырожденных линейных операторов относительно операции умножения (композиции).

Задача 1.10. Доказать, что множество матриц второго порядка:

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, A_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

образует группоид, но не группу относительно операции умножения.

Решение. При умножении любых двух матриц из этого множества получаем матрицу из данного множества. При умножении на единичную матрицу E получаем исходную матрицу, а при умножении любой матрицы на нулевую матрицу A_0 - снова матрицу A_0.

Данное множество не является группой, потому что не для каждого его элемента существует единственный обратный по умножению элемент. Достаточно заметить, что все матрицы A_0, A_1, A_2, A_3, A_4 - вырожденные, то есть ни для одной из них не существует обратная.

Пример. Для любого натурального числа n множество всех невырожденных квадратных матриц порядка n образует группу относительно операции умножения. Эта группа обозначается $GL_n(R)$.

Упражнение. Доказать, что все диагональные невырожденные матрицы образуют группу по умножению, являющуюся подгруппой группы $GL_n(R)$. (Указание: достаточно доказать, что для диагональной матрицы обратная также диагональна).

Упражнение. Доказать, что множество всех невырожденных верхнетреугольных матриц образует подгруппу группы всех квадратных матриц порядка n.

Определение. Пусть B, C - подгруппы группы A, причем $B \cap C = 0$ и всякий элемент группы A может быть единственным образом представлен в виде $a = b + c$, где $b \in B$, $c \in C$. Тогда A называется *прямой суммой* своих подгрупп B и C, и обозначается $A = B \oplus C$.

Пример. Группа всех матриц порядка 2 может быть представлена в виде прямой суммы четырёх подгрупп, состоящих соответственно из матриц вида

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix}.$$

Пример. Множество пар чисел вида $\langle a, b \rangle$, где $a, b \in Z$, образует группу $A = Z \oplus Z$.

Определение. Подгруппа $B \leq A$ называется *нормальной* подгруппой группы A и обозначается $B \lhd A$, если для любого элемента $x \in B$ выполняется равенство $xB = Bx$.

Определение. Элементы $a,b \in A$ называются сопряжёнными, если существует хотя бы один элемент $x \in A$, что выполняется равенство $b = x^{-1}ax$.

Подгруппа $B \leq A$ является нормальной подгруппой тогда и только тогда, когда для каждого её элемента, все элементы, сопряжённые с ним, также принадлежат подгруппе B. Множество всех элементов, сопряжённых с выбранным элементом b, называется смежным классом, соответствующим этому элементу, и обозначается $\bar{b}$. При этом сама подгруппа B совпадает со смежным классом, содержащим нейтральный элемент группы. Можно определить умножение самих смежных классов с помощью умножения их элементов: $\bar{a} \cdot \bar{b} = (aB)(bB) = abB$. Множество смежных классов относительно операции умножения образует группу, называемую *факторгруппой* группы A по подгруппе B. Факторгруппа обозначается A/B.

Пример. Пусть $A = R \oplus R \oplus R$. Элементы вида $<a,0,0>$ образуют подгруппу по сложению. Докажем, что это нормальная подгруппа: $<b,c,d> + <a,0,0> + <-b,-c,-d> = <a,0,0>$. (Данной подгруппе соответствуют все точки на оси $\bar{x}$). Факторгруппа $A/B \cong R \oplus R$, состоит из множества всех прямых параллельных оси $\bar{x}$. Сложение в факторгруппе определяется как сложение в плоскости yz.

§2. Множества с двумя и более алгебраическими операциями.

Определение. Пусть на множестве K заданы две операции, сложение и умножение, взаимосвязанные условиями дистрибутивности: $a(b+c)=ab+ac$ и $(a+b)c=ac+bc$, причём K является абелевой группой относительно сложения. Тогда K называется кольцом.

Обычно рассматривают кольца с операциями сложения и умножения, однако это не единственный способ определить структуру кольца на множестве. Например, закон дистрибутивности выполняется для операций объединения и пересечения множеств: $A\cap(B\cup C)=(A\cap C)\cup(B\cap C)$.

Если рассматривать K как множество только с операцией сложения, то получающаяся абелева группа называется *аддитивной группой* кольца K и обозначается K^+.

Известные примеры числовых колец. Кольцо целых чисел Z, кольцо рациональных чисел Q, кольцо действительных чисел R.

Примеры. Множество всех квадратных матриц порядка n образует кольцо относительно операций сложения и умножения. Также множество всех линейных операторов в пространстве $L: R^n \to R^n$ образует кольцо.

Определение. Подмножество S называется подкольцом кольца K, если S является кольцом относительно тех же алгебраических операций, которые действуют в кольце K (в частности, $r_1, r_2 \in S \Rightarrow r_1 \cdot r_2 \in S$)

При этом S обязательно будет подгруппой по сложению.

Определение. Подмножество I называется идеалом кольца K, если I - подгруппа по сложению и для всякого $a \in I$, $b \in K$ их произведение $a * b \in I$.

Задача 2.1. Доказать, что если $1 \in I$, то $I = K$ (идеал кольца совпадает со всем кольцом).

Решение. Пусть $1 \in I$. По определению, произведение любого элемента кольца на элемент из идеала кольца будет элементом, принадлежащим идеалу кольца. Тогда для всякого $a \in K$ получаем $a \cdot 1 \in I$, откуда следует $a \in I$.

Задача 2.2. Доказать, что все числа, кратные произвольному числу α, образуют идеал кольца Z. (В частности, при $a = 2$ получаем идеал, состоящий из всех чётных чисел).

Решение. Пусть $a = \alpha k$, b - произвольное число. Тогда $ab = \alpha k b \in I$, так как это произведение кратно числу α.

Замечание. Рассмотренные идеалы не являются подкольцами, так как не содержат единицу по умножению.

Пример. Множество всех вырожденных матриц образует идеал кольца всех матриц. Действительно, при умножении любой матрицы на вырожденную снова получим вырожденную матрицу.

Определение. Два элемента $a, b \in K$ называются делителями нуля, если $ab = 0$.

Примеры колец без делителей нуля – числовые кольца: Z, Q, R. Примером кольца с делителями нуля является кольцо всех матриц порядка n.

(Всегда существуют две ненулевые матрицы, при умножении которых получается нулевая матрица).

Определение. Отображение $\varphi : A \to A$ называется эндоморфизмом группы A, если $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(\alpha a) = \alpha\varphi(a)$ для любых элементов $a, b \in A$ и числа $\alpha \in R$.

Отображение, переводящее любой элемент в 0, по определению является эндоморфизмом группы, а также отображение, сохраняющее без изменения каждый элемент, является эндоморфизмом (он называется тождественным, или единичным эндоморфизмом). Эндоморфизмы можно складывать, новое отображение определяется по правилу: $(\varphi + \psi)(a) = \varphi(a) + \psi(a)$. Также композиция двух эндоморфизмов снова является эндоморфизмом. $(\varphi\psi)(a) = \varphi(\psi(a))$. Множество всех эндоморфизмов образует кольцо. Кольцо эндоморфизмов абелевой группы A обозначается $E(A)$.

Определение. Кольцо называется полем, если множество всех его ненулевых элементов образует группу относительно операции умножения.

Примеры. Кольцо рациональных чисел Q и кольцо действительных чисел R являются полями. Кольцо Z полем не является, потому что не для всякого элемента существует обратный по умножению в Z (обратный элемент есть только для чисел 1 и -1).

Поле комплексных чисел C. Рассмотрим важный пример поля, который будет использоваться при дальнейшем изучении курса высшей математики.

Выражение вида $a+bi$ называется комплексным числом, где $i^2=-1$, i - мнимая единица. Произведение комплексных чисел: $(a+bi)(c+di)=(ac-bd)+(bc+ad)i$. Множество $\mathbb{C}$ является полем, так как обратный элемент определён для любого ненулевого комплексного числа: $(a+bi)^{-1}=\dfrac{1}{a+bi}=\dfrac{a-bi}{(a+bi)(a-bi)}=\dfrac{a}{a^2+b^2}-\dfrac{b}{a^2+b^2}i$.

Задача 2.3. Доказать, что множество матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ образует поле относительно операций сложения и умножения; и это поле изоморфно полю комплексных чисел.

Решение. Докажем, что отображение $f: a+bi \to \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ задаёт изоморфизм полей. Для суммы:

$$f(a+bi)+f(c+di)=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}+\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix}=$$

$$f((a+c)+(b+d)i)=f((a+bi)+(c+di)).$$

Для произведения получаем соответствие:

$$f(a+bi)\cdot f(c+di)=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}=$$

$$f((ac-bd)+(ad+bc)i)=f((a+bi)\cdot(c+di)).$$

Кватернионы. Существует обобщение комплексных чисел – система кватернионов. Кватернионом называется число вида

$a+bi+cj+dk$, содержащее действительную часть и мнимую часть из 3 координат. Умножение мнимых единиц определяется таким образом:

$$ij=k, ji=-k, \quad jk=i, kj=-i, \quad ki=j, ik=-j, \quad i^2=j^2=k^2=-1.$$

Умножение элементов может быть представлено в виде таблицы:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Опрделение. Пусть R – ассоциативное кольцо, A - абелева группа. Пусть любым элементам $r \in R$ и $a \in A$ поставлен в соответствие элемент из A, называемый произведением r и a и обозначаемый ra, причём выполняются условия:

1) $(r_1 r_2)a = r_1(r_2 a)$ для всех $r_1, r_2 \in R$ и $a \in A$;

2) $(r_1 + r_2)a = r_1 a + r_2 a$ для всех $r_1, r_2 \in R$ и $a \in A$;

3) $r(a_1 + a_2) = ra_1 + ra_2$ для всех $r \in R$ и $a_1, a_2 \in A$;

Тогда A называется модулем над кольцом R. Если кольцо R не коммутативно, то введённый таким образом модуль называется левым R-модулем, а для определения правого R-модуля нужно вводить умнежение в виле ar. Если кольцо R коммутативно, то нет различия между правыми и левыми R-модулями.

Примеры. Всякая абелева группа - модуль над кольцом целых чисел Z.

Всякое линейное пространство - модуль над полем действительных чисел.

Множества с тремя алгебраическими операциями.

Определение. Если в линейном пространстве A над полем R введена билинейная операция умножения векторов (то есть A является кольцом), то A называется алгеброй над полем R.

Чтобы задать внутреннее умножение, нужно определить n^2 всевозможных произведений базисных элементов пространства. Каждое произведение такого вида – это элемент пространства, то есть задаётся с помощью n координат. Получаем n^2 векторов-столбцов. $e_i e_j = \sum_{k=1}^{n} \alpha_{ijk} e_k$

Таким образом, n^3 чисел полностью определяют внутреннее умножение элементов. Трёхмерная матрица, составленная из них, по строению аналогично матрице линейного оператора, отличие в том, что для линейного оператора нужно задать n векторов: $L(e_1),\ldots,L(e_n)$, поэтому получаем n^2 элементов и, соответственно, плоскую матрицу.

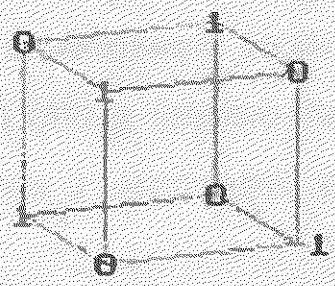
Примеры:

1) Поле комплексных чисел.

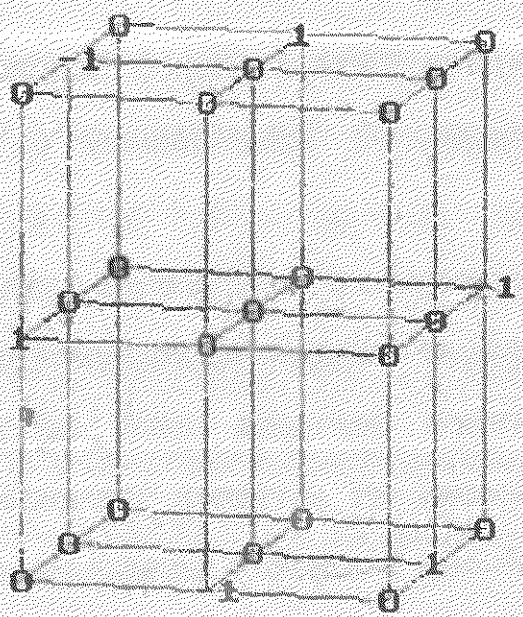
$1\cdot 1 = 1, i\cdot i = -1, 1\cdot i = i\cdot 1 = i$, рассматривая плоскость как 2-мерное пространство с базисом $e_1 = 1, e_2 = i$, умножение перепишем в виде:

$e_1 e_1 = 1e_1 + 0e_2$, $e_2 e_2 = -1e_1 + 0e_2$, $e_1 e_2 = e_2 e_1 = 0e_1 + 1e_2$.

Из этих 8 элементов составляется 3-мерная матрица, задающая умножение:



2) Алгебра векторов в R^3. $e_i^2 = [e_i, e_i] = 0e_1 + 0e_2 + 0e_3$, $[e_1, e_2] = e_3$, остальные векторные произведения базисных элементов находятся аналогично. Матрица, задающая билинейное умножение:



3) Алгебра кватернионов (правила умножения элементов были определены выше, матрица, соответствующая этой системе, изображена на обложке пособия).

Множества с n-арными алгебраическими операциями.

До настоящего момента мы рассматривали только бинарные операции, при которых двум элементам одного и того же или различных множеств ставился

в соответствие новый элемент. Но существуют и n-арные операции, которые ставят в соответствие не двум элементам, а некоторому упорядоченному набору из n элементов новый элемент какого-либо множества. Некоторые из таких операций могут быть определены с помощью композиции бинарных операций.

Пример. 3-арная алгебраическая операция $f(\bar{a},\bar{b},\bar{c}) = [[\bar{a},\bar{b}],\bar{c}]$ - композиция векторных произведений. Данная операция каждой упорядоченной тройке векторов из R^3 ставит в соответствие некоторый вектор в R^3. Очевидно, что если при этом первые два вектора коллинеарны, то результатом операции будет нулевой вектор. То же самое, если третий вектор перпендикулярен плоскости, в которой расположены $\bar{a}$ и $\bar{b}$.

Но существуют операции, не представимые с помощью композиции бинарных операций.

Пример. Обобщённое векторное произведение в 4-мерном пространстве.

Определение. Пусть задана линейно-независимая система из 3 векторов. Векторным произведением векторов этой системы назовём вектор, перпендикулярный каждому из векторов заданной системы, равный по модулю декартовому объёму 3-мерного параллелепипеда в подпространстве размерности 3, порождаемом системой векторов, и направленный таким образом, чтобы определитель системы из 4 векторов, включающей векторное произведение, был положительным.

Таким образом, в четырёхмерном пространстве определяется 3-арная операция над векторами.

$$[a,b,c]=\begin{vmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ i & j & k & l \end{vmatrix}$$

здесь алгебраические дополнения при элементах i,j,k,l будут координатами обобщённого векторного произведения. Введённое таким образом произведение антикоммутативно по любой паре элементов: при перемене мест двух элементов всегда меняется знак. Это происходит из-за смены знака определителя при перемене строк.

Здесь должны вычисляться именно миноры первых 3 строк, в этом случае получается $[e_1,e_2,e_3]=e_4$, иначе было бы $[e_1,e_2,e_3]=-e_4$. Для векторного умножения в трёхмерном пространстве разница несущественна:

$$\begin{vmatrix} i & j & k \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ i & j & k \end{vmatrix}$$

так как один определитель получается из другого с помощью двух последовательных замен соседних строк, его знак не изменяется.

Литература

1. Горбанёв Н.Н., Ельцов А.А., Магазинников Л.И. Линейная алгебра. Аналитическая геометрия. Томск, 2001.
2. Курош А.Г. Теория групп. М, Наука, 1967.
3. Кантор И.Л., Солодовников А.С. Гиперкомплексные числа. М., Наука, 1973.
4. Соколов Н.П. Введение в теорию многомерных матриц. Киев, 1972.
5. Приходовский М.А. Применение многомерных матриц для исследования гиперкомплексных чисел конечномерных алгебр. Вестник ТГУ, №284, декабрь 2004, с.27-29.
6. Фукс Л. Бесконечные абелевы группы т.1. М. Мир, 1974.
7. Хамермеш М. Теория групп и её применение к физическим проблемам. М., Мир, 1966.
8. Чехлов А.Р. Упражнения по теории групп. Томск, Изд-во ТГУ, 2004.