ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное
учреждение высшего образования
“ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ ИМПЕРАТОРА АЛЕКСАНДРА I”

Кафедра «Высшая математика»

Е.А. Благовещенская

Методические указания
по выполнению практических заданий

по дисциплине

«АЛГЕБРА И ГЕОМЕТРИЯ» (Б1.Б.13)

для специальности
10.05.03 «Информационная безопасность автоматизированных систем»

по специализации
«*Безопасность автоматизированных систем на железнодорожном транспорте*»

Форма обучения – очная

РАЗДЕЛ 1. ОСНОВНЫЕ АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

Санкт-Петербург 2023

Практическое занятие 1. Операции над множествами.

Задача 1. Установить, является ли группой множество $A = \{x \mid x \in \& \;\; x > 0\}$ относительно операции f:

$$a\, f\, b = \frac{a+b}{2}.$$

Решение. Для того, чтобы установить наличие на A структуры группы, проверим выполнимость аксиом группы:

1) алгебраичность операции f $(\forall\, x, y \in A : x\, f\, y \in A)$.

$$\left.\begin{array}{l} x \in A \Rightarrow x \in \cdot\,,\ x > 0 \\ y \in A \Rightarrow x \in \cdot\,,\ y > 0 \end{array}\right. \Rightarrow x + y \in \cdot\,,\ x + y > 0,\ \frac{x+y}{2} \in \& \ \frac{x+y}{2} > 0 \Rightarrow x\, f\, y \in A,$$

т. е. операция f алгебраическая на множестве A;

2) ассоциативность операции f $\left((x\, f\, y)\, f\, z = x\, f\, (y\, f\, z)\right.$ для $\forall\, x, y, z \in A)$

$$x\, f\, y = \frac{x+y}{2}, \quad (x\, f\, y)\, f\, z = \frac{\left(\dfrac{x+y}{2}\right) + z}{2} = \frac{x + y + 2z}{4},$$

$$y\, f\, z = \frac{y+z}{2}, \quad x\, f\, (y\, f\, z) = \frac{x + \dfrac{y+z}{2}}{2} = \frac{2x + y + z}{4}.$$

Операция f не является ассоциативной, т. к. тождество ассоциативности нарушается, например, при $x = 1$, $y = 2$, $z = 3$

$$\frac{1+2+6}{4} \neq \frac{2+2+3}{4}.$$

Следовательно, $A(f)$ группой не является.

Задача 2. Определить, является ли группой множество подстановок $M = \{a_1, a_2, a_3, a_4, a_5, a_6\}$ относительно обычного умножения подстановок, где

$$a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad a_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad a_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$a_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad a_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad a_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Решение *1 способ*. Составим таблицу Кэли для умножения на M:

$\bullet$	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_1	a_6	a_5	a_4	a_3
a_3	a_3	a_5	a_1	a_6	a_2	a_4

a_4	a_4	a_6	a_5	a_1	a_3	a_2
a_5	a_5	a_3	a_4	a_2	a_6	a_1
a_6	a_6	a_4	a_2	a_3	a_1	a_5

1) Алгебраичность операции. Все клеточки внутри таблицы заполнены элементами из M, причем однозначно. Следовательно операция $(\cdot)$ – алгебраична.
2) Существует нейтральный элемент $e = a_1$, т. к. $a_1 X = X$ и $X a_1 = X$ при любом значении X из M.
3) Операция $(\cdot)$ обратима, т. к. для любого значения x из M в M существует x^{-1}:

   $a_1^{-1} = a_1, \quad a_2^{-1} = a_2, \quad a_3^{-1} = a_3, \quad a_4^{-1} = a_4, \quad a_5^{-1} = a_5, \quad a_6^{-1} = a_6.$

   Действительно, $a_1 \cdot a_1 = a_1$, $a_2 \cdot a_2 = a_1$, $a_3 \cdot a_3 = a_1$, $a_3 \cdot a_3 = a_1$, $a_4 \cdot a_4 = a_1$, $a_5 \cdot a_6 = a_6 \cdot a_5 = a_1$ $(a_1 = e)$.
4) Операция $(\cdot)$ ассоциативна, т. к. тождество ассоциативности

$$\big((X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)\big)$$

выполняется при всех значениях X, Y, Z из M. Действительно, пусть X принял значение $x = \begin{pmatrix} a \\ b \end{pmatrix}$, Y принимает значение $y = \begin{pmatrix} b \\ c \end{pmatrix}$, Z принимает значение $z = \begin{pmatrix} c \\ d \end{pmatrix}$, где a, b, c, d, независимо друг от друга пробегает множество $\{1, 2, 3\}$. Тогда

$$\left.\begin{aligned} xy &= \begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} b \\ c \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}, \; (xy)z = \begin{pmatrix} a \\ c \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \\ d \end{pmatrix} \\ yz &= \begin{pmatrix} b \\ c \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} b \\ d \end{pmatrix}, \; x(yz) = \begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} a \\ d \end{pmatrix} \end{aligned}\right\}, \text{ следовательно, } (xy)z = x(yz), \text{ т. е.}$$

умножение на M ассоциативно.

Следовательно, $M(\cdot)$ – группа.

2 способ. Из комбинаторики известно, что для множества состоящего из трех элементов имеется в точности $3! = 1 \cdot 2 \cdot 3 = 6$ различных подстановок и они образуют мультипликативную симметрическую группу. Множество M состоит из шести различных подстановок трех элементов. Следовательно, $M(\cdot)$ – симметрическая группа.

Задача 3.

Является ли кольцом (полем) множество $K = \{\alpha \mid \alpha = a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$ кольцом относительно обычных операций сложения и умножения вещественных чисел?

Решение.

$K = \{\alpha \mid \alpha = a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$, $\quad \alpha_1 = a_1 + b_1\sqrt{2}$, $a_1, b_1 \in \mathbb{Z}$,

$\alpha_2 = a_2 + b_2\sqrt{2}$, $a_2, b_2 \in \mathbb{Z}$; $\quad \alpha_1 = \alpha_2 \overset{def}{\Leftrightarrow} \begin{cases} a_1 = a_2 \\ b_1 = b_2 \end{cases}$,

$\alpha_1 + \alpha_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$, $\quad \alpha_1 \cdot \alpha_2 = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$

Проверим выполнение аксиом кольца.

1. Алгебраичность сложения:

$$\left.\begin{array}{l} \alpha_1 \in K,\ \text{т.е. } \alpha_1 = a_1 + b_1\sqrt{2},\ a_1, b_1 \in \mathbb{Z} \\ \alpha_2 \in K,\ \text{т.е. } \alpha_2 = a_2 + b_2\sqrt{2},\ a_2, b_2 \in \mathbb{Z} \end{array}\right\}$$

следовательно, $\left.\begin{array}{l} \alpha_1 + \alpha_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \\ a_1 + a_2 \text{ и } b_1 + b_2 \in \mathbb{Z} \end{array}\right\}$ т. е. $\alpha_1 + \alpha_2 \in K$.

2. Коммутативность сложения:

$\begin{cases} \alpha_1 \in K,\ \text{т.е. } \alpha_1 \in \mathbb{R} \\ \alpha_2 \in K,\ \text{т.е. } \alpha_2 \in \mathbb{R} \end{cases}$, т. е. $\alpha_1 + \alpha_2 = \alpha_2 + \alpha_1 \in \mathbb{R}$, т. е. $\alpha_1 + \alpha_2 = \alpha_2 + \alpha_1$ в K, так как $K \subset \mathbb{R}$, т. е. сложение в K коммутативно.

3. Ассоциативность сложения:

$\left.\begin{array}{l} \alpha_1 \in K,\ \text{следовательно, } \alpha_1 \in \mathbb{R} \\ \alpha_2 \in K,\ \text{следовательно, } \alpha_2 \in \mathbb{R} \\ \alpha_3 \in K,\ \text{следовательно, } \alpha_3 \in \mathbb{R} \end{array}\right\}$, т. е. $(\alpha_1 + \alpha_2) + \alpha_3 = \alpha_1 + (\alpha_2 + \alpha_3)$ в $\mathbb{R}$, т. е. $(\alpha_1 + \alpha_2) + \alpha_3 = \alpha_1 + (\alpha_2 + \alpha_3)$ в K, так как $K \subset \mathbb{R}$, т. е. в K ассоциативно.

4. Наличие нейтрального элемента по сложению (ноль $\bar{0}$).

Если ноль $\bar{0}$ существует, то это элемент множества K, т. е. имеет вид $\bar{0} = x + y\sqrt{2}$, $x, y \in \mathbb{Z}$, и удовлетворяет условию $\bar{0} + \alpha = \alpha$ для $\forall\, \alpha \in K$, т. е. $(x + y\sqrt{2}) + (a + b\sqrt{2}) = (a + b\sqrt{2})$. Тогда $(x + a) + (y + b)\sqrt{2} = a + b\sqrt{2}$, т. е. $\begin{cases} x + a = a \\ y + b = b \end{cases}$, т. е. $\begin{cases} x = 0 \\ y = 0 \end{cases}$, т. е. $\bar{0} = 0 + 0\sqrt{2}$, где $0 \in \mathbb{Z}$, т. е. $\bar{0} = 0 + 0\sqrt{2} \in K$.

5. Симметризуемость операции сложения.

Для каждого элемента $\alpha \in K$ существует в K элемент $(-\alpha)$, удовлетворяющий условию $\alpha + (-\alpha) = \bar{0}$. Действительно, если $\alpha = a + b\sqrt{2}$, то $-\alpha = (-a) + (-b)\sqrt{2}$. Так как $a, b \in \mathbb{Z}$, то $(-a)$ и $(-b) \in \mathbb{Z}$, то есть $-\alpha \in K$.

6. Алгебраичность умножения.

$$\left.\begin{array}{l} \alpha_1 = a_1 + b_1\sqrt{2},\ a_1, b_1 \in \mathbb{Z} \\ \alpha_2 = a_2 + b_2\sqrt{2},\ a_2, b_2 \in \mathbb{Z} \end{array}\right. \Rightarrow \alpha_1 \cdot \alpha_2 = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in K$$

т. к. $(a_1a_2 + 2b_1b_2)$ и $(a_1b_2 + a_2b_1) \in \mathbb{Z}$.

7. Ассоциативность умножения.

$$\left.\begin{array}{l}\alpha_1 \in K \Rightarrow \alpha_1 \in \mathbb{R}\\ \alpha_2 \in K \Rightarrow \alpha_2 \in \mathbb{R}\\ \alpha_3 \in K \Rightarrow \alpha_3 \in \mathbb{R}\end{array}\right\}$$ т. е. $(\alpha_1 \cdot \alpha_2)\alpha_3 = \alpha_1(\alpha_2 \cdot \alpha_3)$ в $\mathbb{R}$, т. е. $(\alpha_1 \cdot \alpha_2)\alpha_3 =$
$= \alpha_1(\alpha_2 \cdot \alpha_3) \in K$, так как $K \subset \mathbb{R}$. То есть в K ассоциативно.

8. Умножение двоякодистрибутивно относительно сложения.

$$\left.\begin{array}{l}\alpha_1 \in K, \text{ следовательно, } \alpha_1 \in \mathbb{R}\\ \alpha_2 \in K, \text{ следовательно, } \alpha_2 \in \mathbb{R}\\ \alpha_3 \in K, \text{ следовательно, } \alpha_3 \in \mathbb{R}\end{array}\right\} \text{ т. е. } \begin{array}{l}(1)\ (\alpha_2 + \alpha_3)\alpha_1 = \alpha_1\alpha_2 + \alpha_1\alpha_3 \text{ в } \mathbb{R}\\ (2)\ \alpha_1(\alpha_2 + \alpha_3) = \alpha_2\alpha_1 + \alpha_3\alpha_1 \text{ в } \mathbb{R}\end{array}, \text{ т. е.}$$

$$\left.\begin{array}{l}(1) \text{ выполняется в } K\\ (2) \text{ выполняется в } K\end{array}\right\},$$ т. е. умножение двоякодистрибутивно относительно сложения в K.

Следовательно, $K(+, \cdot)$ – кольцо.

9. Проверим, является ли это кольцо коммутативным.

$$\left.\begin{array}{l}\alpha_1 \in K, \text{ то есть, } \alpha_1 \in \mathbb{R}\\ \alpha_2 \in K, \text{ то есть, } \alpha_2 \in \mathbb{R}\end{array}\right\},$$ т. е. $\alpha_1 \cdot \alpha_2 = \alpha_2 \cdot \alpha_1$ в $\mathbb{R}$, т. е. $\alpha_1 \cdot \alpha_2 = \alpha_2 \cdot \alpha_1$ в K, т. к. $K \subset \mathbb{R}$, т. е. умножение в K коммутативно.

10. Проверим, имеет ли кольцо K единицу e.

Если e из K, то $e = x + y\sqrt{2}$, $x, y \in \mathbb{Q}$, причем, $e \cdot \alpha = \alpha \cdot e = \alpha$ для $\forall\, \alpha \in K$, т. е. $(x + y\sqrt{2})(a + b\sqrt{2}) = a + b\sqrt{2}$. Тогда

$$(xa + 2yb)(xb + ya) = a + b\sqrt{2}, \text{ т. е. } \begin{cases} ax + 2by = a\\ bx + ay = b\end{cases}.$$

Решим линейную систему относительно неизвестных x и y методом Крамера:

$$\Delta = \begin{vmatrix} a & 2b\\ b & a\end{vmatrix} = a^2 - 2b^2, \qquad \Delta_1 = \begin{vmatrix} a & 2b\\ b & a\end{vmatrix} = a^2 - 2b^2, \qquad \Delta_2 = \begin{vmatrix} a & a\\ b & b\end{vmatrix} = 0.$$

$\Delta \neq 0$, т. к. если бы $a^2 - 2b^2 = 0$, то $a^2 = 2b^2$ и a должно быть иррациональным числом, что противоречит условию $(a \in \mathbb{Q})$. Значит, система имеет только одно решение, которое можно найти по формулам Крамера: $x = \dfrac{\Delta_1}{\Delta} = 1$, $y = \dfrac{\Delta_2}{\Delta} = 0$, т. е. $e = 1 + 0\sqrt{2}$. Следовательно, $e \in K$, т. к. $1, 0 \in \mathbb{Q}$. Так как умножение в K коммутативно, то с выполнением $e \cdot \alpha = \alpha$ следует выполнение $\alpha \cdot e = \alpha$.

11. Выясним, обратим ли каждый, отличный от $\bar{0}$ элемент в K.

Возьмем $\alpha \in K$, $\alpha \neq \bar{0}$, т. е. $\alpha = a + b\sqrt{2}$, где a и b удовлетворяют

$$\left[\begin{array}{l} 1)\ a = 0, b \neq 0\\ 2)\ a \neq 0, b = 0, \qquad a, b \in \mathbb{Q}.\\ 3)\ a \neq 0, b \neq 0\end{array}\right.$$

Если α^{-1} существует в K, то $\alpha^{-1} = x + y\sqrt{2}$, $x, y \in \mathbb{Q}$ и $\alpha^{-1} \cdot \alpha = = \alpha \cdot \alpha^{-1} = e$, т. е. $\left(x + y\sqrt{2}\right)\left(a + b\sqrt{2}\right) = 1 + 0\sqrt{2}$.

Значит $(xa + 2yb) + (xb + ya)\sqrt{2} = 1 + 0\sqrt{2}$, т. е.

$$\begin{cases} ax + 2by = 1 \\ bx + ay = 0 \end{cases}.$$

Решим систему методом Крамера относительно неизвестных x и y.

$$\Delta = \begin{vmatrix} a & 2b \\ b & a \end{vmatrix} = a^2 - 2b^2, \qquad \Delta_1 = \begin{vmatrix} 1 & 2b \\ 0 & a \end{vmatrix} = a, \qquad \Delta_2 = \begin{vmatrix} a & 1 \\ b & 0 \end{vmatrix} = -b.$$

Для указанных ограничений на a и b следует, что $\Delta \neq 0$ и тогда $x = \frac{\Delta_1}{\Delta} = \frac{a}{a^2 - 2b^2}$, $y = -\frac{b}{a^2 - 2b^2}$. Значения x и y существуют в $\mathbb{R}$, то в $\mathbb{Q}$ не обязательно. Например, при $a = 5$, $b = 1$ имеем $x = \frac{5}{25 - 2} = \frac{5}{23} \notin \mathbb{Q}$, $y = -\frac{1}{25 - 2} = -\frac{1}{23} \notin \mathbb{Q}$, т. е. α^{-1} не обязан существовать в K для $\alpha \in K$ $\left(\alpha \neq \bar{0}\right)$.

Вывод: $K(+, \cdot)$ – коммутативное кольцо с единицей, но не поле.