

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

Конспект лекций
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 2. ОСНОВНЫЕ АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

Санкт-Петербург 2023

Лекция 1.

Множества, подмножества. Операции над множествами. Определение полугруппы, группы, кольца и поля. Основные примеры групп и колец.

АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ.

Определение 1. Операцией на множестве X называется функция $f : X \times X \rightarrow X$, которая сопоставляет паре элементов (x_1, x_2) множества X элемент того же множества, т.е. $f(x_1, x_2) \in X$.

Обозначение для произвольной операции: $f(x_1, x_2) = x_1 * x_2$.

Таким образом, сложение (+) и умножение ($\cdot$) являются операциями.

Определение 2. Множество G называется группой, если на нем задана операция $*$ со следующими свойствами:

1. $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ — ассоциативность;
2. $\exists e \in G : \forall g \in G \quad e * g = g * e = g$ — наличие единичного элемента;
3. $\forall g \in G \quad \exists g^{-1} \in G : g * g^{-1} = g^{-1} * g = e$ — наличие обратного элемента.

Определение 3. Группа G называется коммутативной или абелевой, если операция $*$ в ней коммутативна, т.е. $g_1 * g_2 = g_2 * g_1$.

В качестве примера можно рассмотреть множество целых чисел $\mathbb{Z}$. Относительно операции сложения множество $\mathbb{Z}$ будет являться группой (единичным элементом будет 0, а обратным — элемент с обратным знаком), кроме того, эта группа будет абелевой. С другой стороны, множество $\mathbb{Z}$ относительно операции умножения не будет группой (не все элементы имеют обратный).

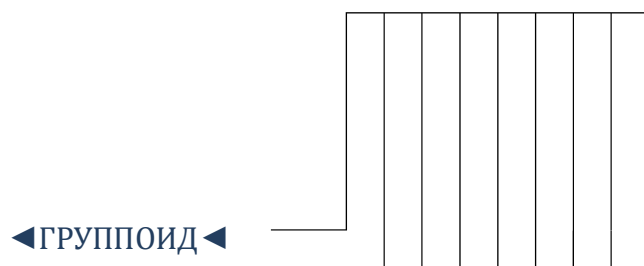
Определение 4. Множество K называется кольцом, если в нем определены две операции: сложения и умножения. Относительно операции сложения множество K является абелевой группой, а относительно умножения множество $K \setminus \{0\}$ является полугруппой. Умножение и сложение связаны между собой законом дистрибутивности:

1. $(a + b) \cdot c = a \cdot c + b \cdot c$;
2. $a \cdot (b + c) = a \cdot b + a \cdot c$.

Определение 5. Кольцо K называется коммутативным, если операция умножения коммутативна. Если полугруппа $K \setminus \{0\}$ относительно умножения имеет единицу, то кольцо называется кольцом с единицей.

Примерами колец могут служить множества рациональных $\mathbb{Q}$ и комплексных чисел $\mathbb{C}$. Причем оба эти кольца будут коммутативными и иметь единицу (т.к. операция умножения коммутативна, а единицей будет служить 1).

Под алгебраической структурой (иногда говорят об универсальных алгебрах) понимается множество A , на котором определена некоторая система внутренних операций и отношений, подчиняющихся тем или иным законам — аксиомам



2. Ассоциативность сложения:

$$(a + b) + c = a + (b + c)$$

◀ПОЛУГРУППА◀

3. Существует «нуль» - нейтральный элемент по сложению:

$$\exists 0 : a + 0 = 0 + a = a$$

◀МОНОИД◀

4. Для $\forall a$ существует противоположный элемент $-a$ - симметричный a по сложению:

$$\forall a \exists -a : a + (-a) = 0$$

◀ГРУППА◀

5. Коммутативность сложения:

$$a + b = b + a$$

◀АБЕЛЕВА ГРУППА◀

6. На $\mathcal{E}$ определено «умножение»

$$\bullet : \mathcal{E} \times \mathcal{E} \rightarrow \mathcal{E} \text{ (алгебраичность}$$

умножения):

$$a \cdot b = p$$

7. Ассоциативность умножения:

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

8. Правая дистрибутивность умножения:

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

9. Левая дистрибутивность умножения:

$$c \cdot (a + b) = c \cdot a + c \cdot b$$

◀КОЛЬЦО◀

10. Существует «единица» - нейтральный элемент по умножению:

$$\exists 1 : 1 \cdot a = a$$

◀КОЛЬЦО С 1◀

11. Для $\forall a \neq 0$ существует обратный к a элемент a^{-1} - симметричный a по умножению:

$$\forall a \neq 0 \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1$$

◀ТЕЛО, если $1 \neq 0$ ◀

12. Коммутативность умножения:

$$a \cdot b = b \cdot a$$

◀ПОЛЕ◀