

# Глава I. Введение

## § 6. Группы, кольца, поля

А. Я. Овсянников

Уральский федеральный университет  
Институт естественных наук и математики  
Департамент математики, механики и компьютерных наук  
Основы алгебры для направлений  
Механика и математическое моделирование и  
Прикладная математика  
(1 семестр)

Пусть на множестве  $G$  определена операция умножения.

## Определение

Множество  $G$  называется *группой*, если

- 1 Операция на множестве  $G$  ассоциативна;
- 2 в множестве  $G$  существует единица;
- 3 для любого элемента из множества  $G$  существует обратный элемент.

Если операция на группе  $G$  коммутативна, то группа  $G$  называется *абелевой*.

Обычно для абелевых групп используется аддитивный способ представления операции.

Абелевыми группами являются множества чисел  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  относительно сложения, множества геометрических векторов относительно сложения, множество из примера 8 на слайде 3 §5.

## Предложение

Пусть  $G$  — группа с операцией умножения,  $x, y, z \in G$ . Тогда

- 1 Если  $xy = xz$  или  $yx = zx$ , то  $y = z$  (закон сокращения).
- 2 Имеет место равенство  $(xy)^{-1} = y^{-1}x^{-1}$ .

↓ Пусть  $xy = xz$ . Умножив обе части этого равенства слева на  $x^{-1}$ , получим  $x^{-1}(xy) = x^{-1}(xz)$ , откуда в силу ассоциативности и определения обратного элемента следует  $(x^{-1}x)y = (x^{-1}x)z$  и  $1y = 1z$ , т.е.  $y = z$ . Аналогично доказывается, что из  $yx = zx$  следует  $y = z$ .

Для доказательства утверждения 2 вычислим

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}(xy)) = y^{-1}((x^{-1}x)y) = y^{-1}(1y) = y^{-1}y = 1.$$

Значит,  $(y^{-1}x^{-1})(xy) = 1$ . Так как  $(xy)^{-1}(xy) = 1$ , из утверждения 1 следует утверждение 2. ↑

## Разность в абелевой группе

Пусть  $(V, +)$  — абелева группа. Тогда  $\forall a, b \in V \exists! x \in V : a + x = b$ .

Указанный элемент  $x$  обозначается через  $b - a$  и называется *разностью* элементов  $a$  и  $b$ .

Положим  $x = b + (-a)$ , тогда ясно, что  $a + x = a + b + (-a) = b$ .

Единственность элемента  $x$  следует из утверждения 1 предложения. ↑

Пусть  $K$  — множество с операциями сложения и умножения.

### Определение

Множество  $K$  называется *кольцом*, если относительно сложения  $K$  является абелевой группой и

$$\forall x, y, z \in K \quad x(y + z) = xy + xz, \quad (x + y)z = xz + yz.$$

Последние условия называются *левой дистрибутивностью* и *правой дистрибутивностью*.

На операцию умножения в кольце никаких ограничений не налагается. Кольцами относительно операций сложения и умножения являются множества чисел  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ , а также множества классов вычетов по модулю  $n$ . Кольцам даются названия по свойствам операции умножения. Если она коммутативна (ассоциативна), то кольцо называется *коммутативным* (*ассоциативным*).

Если для операции умножения существует единица, то кольцо называется *кольцом с единицей*.

Например, кольцо целых чисел  $\mathbb{Z}$  является коммутативным ассоциативным кольцом с единицей.

Пусть  $K$  — кольцо.

## Предложение

Для любого элемента  $x \in K$  имеют место равенства  $0 \cdot x = x \cdot 0 = 0$ .

↓ Умножим равенство  $0 + 0 = 0$  слева на элемент  $x$ , получим  $x \cdot (0 + 0) = x \cdot 0$ . Пользуясь дистрибутивностью, имеем  $x \cdot 0 + x \cdot 0 = x \cdot 0 = x \cdot 0 + 0$ , откуда в силу свойства 1 групп (слайд 3) следует  $x \cdot 0 = 0$ .

Аналогично доказывается, что  $0 \cdot x = 0$ . ↑

## Определение

Элементы  $x, y$  кольца  $K$  называются **делителями нуля**, если  $x, y \neq 0$ , но  $x \cdot y = 0$ .

Делители нуля имеются в кольце вычетов по модулю  $n$ , когда  $n$  — составное число. Если  $n = n_1 n_2$ , где  $n_1 < n$ ,  $n_2 < n$ , то  $\bar{n}_1 \cdot \bar{n}_2 = 0$  в кольце вычетов по модулю  $n$ , но  $\bar{n}_1, \bar{n}_2 \neq 0$ .

## Определения

Коммутативное ассоциативное кольцо с единицей и без делителей нуля называется *областью целостности*.

Говорят, что кольцо  $K$  является *кольцом с законом сокращения*, если для любых  $x, y, z \in K$  при  $x \neq 0$  из  $xy = xz$  или  $yx = zx$  следует  $y = z$ .

Пример области целостности, а также кольца с законом сокращения – кольцо целых чисел  $\mathbb{Z}$ .

## Предложение

Коммутативное ассоциативное кольцо с единицей является областью целостности тогда и только тогда, когда оно является кольцом с законом сокращения.

↓ Пусть  $K$  – область целостности, и  $x, y, z \in K$ , причем  $x \neq 0$ . Из  $xy = xz$  следует  $x(y - z) = 0$ . Значит,  $y - z = 0$  и  $y = z$ . В силу коммутативности  $K$  этого достаточно. Обратно, пусть  $K$  – коммутативное ассоциативное кольцо с единицей и законом сокращения. Предположим, что для  $x, y \in K$  имеет место  $x \neq 0$  и  $x \cdot y = 0$ . По предложению сл.5  $x \cdot 0 = 0$ , значит, в силу закона сокращения из  $x \cdot y = x \cdot 0$  следует  $y = 0$ . Следовательно,  $K$  – кольцо без делителей нуля, т.е. область целостности. ↑

Что такое обратимый элемент кольца?

### Определение

**Полем** называется коммутативное ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим. В поле  $0 \neq 1$ , т.е. поле не может состоять из одного элемента.

Полями относительно операций сложения и умножения являются множества чисел  $\mathbb{Q}$ ,  $\mathbb{R}$ , а также множества классов вычетов по простому модулю  $n$ . В последнем случае для любого натурального  $0 < k < n$  числа  $k$  и  $n$  взаимно просты, поэтому существуют целые  $u, v$  такие что  $uk + vn = 1$ . Обратным к классу вычетов  $\bar{k}$  будет класс вычетов, определенный числом  $u$ .

### Предложение

*Поле не имеет делителей нуля.*

↓ Предположим, что  $x \cdot y = 0$  и  $x \neq 0$ . Тогда в поле существует элемент  $x^{-1}$ . Умножим обе части равенства  $x \cdot y = 0$  слева на  $x^{-1}$ , получим  $x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0$ , откуда  $0 = (x^{-1} \cdot x) \cdot y = 1 \cdot y = y$ , т.е.  $y = 0$ . Следовательно, поле не может содержать делителей нуля. ↑

Пусть  $F$  – поле,  $e$  – единица  $F$ , т.е. нейтральный элемент относительно умножения. Рассмотрим отображение  $\varphi : \mathbb{N} \rightarrow F$ , полагая  $\varphi(n) = e + e + \dots + e$  (сумма  $n$  слагаемых). Если это отображение инъективно, то говорят, что поле  $F$  *имеет характеристику* 0. Если  $\varphi$  не инъективно, то  $\varphi(m) = \varphi(n)$  при некоторых  $m, n \in \mathbb{N}$  таких что  $m < n$ . Тогда  $\varphi(n - m) = 0$  (нуль поля  $F$ ). В этом случае *характеристикой* поля  $F$  называется наименьшее натуральное число  $p$  такое что  $\varphi(p) = 0$ . Характеристику поля обозначим через  $\text{char}(F)$ .

## Предложение

Если характеристика поля не равна нулю, то она является простым числом.

↓ Пусть  $\text{char}(F) \neq 0$ . Так как в поле  $F$  справедливо  $e \neq 0$ , имеем  $\text{char}(F) \neq 1$ . Легко вычислить, что  $\varphi(n \cdot k) = \varphi(n)\varphi(k)$ . Если  $\text{char}(F) = n \cdot k$ , где  $n, k < \text{char}(F)$ , то  $\varphi(n)\varphi(k) = 0$ , в то время как  $\varphi(n) \neq 0$  и  $\varphi(k) \neq 0$ . Так как поле в силу предложения сл.7 не имеет делителей нуля, такая ситуация невозможна. Следовательно,  $\text{char}(F)$  – простое число. ↑

Поля  $\mathbb{Q}$ ,  $\mathbb{R}$  имеют характеристику 0; поле вычетов по простому модулю  $p$  имеет характеристику  $p$ .