

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

**А. В. Звягин**

## **ЭЛЕМЕНТЫ АБСТРАКТНОЙ АЛГЕБРЫ**

Учебно-методическое пособие

Воронеж  
Издательский дом ВГУ  
2016

## Оглавление

<b>Предисловие</b> . . . . .	<b>5</b>
<b>Глава 1. Элементы теории множеств</b> . . . . .	<b>5</b>
1.1. Понятие множества . . . . .	5
1.2. Операции над множествами . . . . .	7
1.3. Фактор-множество . . . . .	9
<b>Глава 2. Определения основных алгебраических структур</b>	<b>13</b>
2.1. Определение алгебраической структуры . . . . .	13
2.2. Полугруппа. Моноид . . . . .	14
<b>Глава 3. Группы</b> . . . . .	<b>16</b>
3.1. Определение группы . . . . .	16
3.2. Подгруппа . . . . .	17
3.3. Циклические группы . . . . .	17
3.4. Изоморфизмы групп . . . . .	19
3.5. Смежные классы . . . . .	20
3.6. Фактор-группа . . . . .	22
3.7. Группа вычетов по модулю $p$ . . . . .	23
<b>Глава 4. Кольцо</b> . . . . .	<b>24</b>
4.1. Определение кольца . . . . .	24
4.2. Подкольцо . . . . .	27
4.3. Идеалы кольца . . . . .	28
4.4. Простые и максимальные идеалы . . . . .	30
4.5. Гомоморфизмы и изоморфизмы колец . . . . .	31

ляется элементом множества  $A$ , а запись  $a \notin A$  или  $a \bar{\in} A$  означает, что элемент  $a$  не принадлежит множеству  $A$ .

Возможны различные способы задания множества. Один из способов состоит в простом перечислении его элементов. Так, например, запись  $A = \{a, b, c\}$  указывает, что множество  $A$  состоит из элементов  $a, b, c$ . Другой способ состоит в определении множества с помощью некоторого характеристического свойства, которым обладают те и только те элементы, которые принадлежат данному множеству. Обозначая символом  $P(a)$  характеристическое свойство элементов множества  $A$ , множество  $A$  в данном случае задают записью  $A = \{a : P(a)\}$ . Например, множество целых чисел, принадлежащих отрезку  $[0, 5]$  можно задать следующим образом:  $A = \{a \in \mathbb{Z} : 0 \leq a \leq 5\}$ .

Не всегда заранее известно, что рассматриваемое множество содержит хотя бы один элемент, поэтому для правомочности рассуждений целесообразно ввести понятие множества, не содержащего ни одного элемента. Такое множество называется *пустым* и обозначается  $\emptyset$ .

**Определение 1.1.** *Всякое множество, число элементов которого равно одному из чисел  $0, 1, 2, \dots$ , называется конечным. Множества, не являющиеся конечными, называются бесконечными.*

**Определение 1.2.** *Множества  $A$  и  $B$ , состоящие из одних и тех же элементов, называют равными и пишут  $A = B$ .*

На практике для доказательства равенства двух множеств показывают, что всякий элемент одного множества принадлежит другому, и наоборот.

Если множество  $A$  состоит из элементов, принадлежащих множеству  $X$ , то говорят, что  $A$  является *подмножеством* множества  $X$  (или  $A$  включено в  $X$ ), и в этом случае пишут  $A \subset X$  (или  $A \subseteq X$ ). Например,  $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ . Используют также обозначение  $X \supset A$ , которое читается так:  $X$  содержит  $A$ .

Для всякого множества  $A$  имеют место вложения  $\emptyset \subset A$ ,  $A \subseteq A$ . Подмножества множества  $A$ , отличные от  $\emptyset$  и  $A$ , называются *собственными подмножествами* множества  $A$ .

## 1.2. Операции над множествами

Из данных множеств можно конструировать другие множества. Приведем наиболее важные и необходимые в дальнейшем способы конструирования.

**Определение 1.3.** Объединением двух множеств  $A$  и  $B$  называется множество, состоящее из всех элементов, принадлежащих хотя бы одному из множеств  $A$  и  $B$ , т.е.

$$A \cup B = \{a : a \in A \text{ или } a \in B\}.$$

**Определение 1.4.** Пересечением двух множеств  $A$  и  $B$  называется множество, состоящее из всех элементов, принадлежащих как  $A$ , так и  $B$ , т.е.

$$A \cap B = \{a : a \in A \text{ и } a \in B\}.$$

Если  $A \cap B = \emptyset$ , то множества  $A$ ,  $B$  называются *непересекающимися*.

Аналогично определяется объединение и пересечение любого (конечного или бесконечного) числа множеств  $A_\alpha$ ,  $\alpha \in I$ , где  $I$  – произвольное множество индексов. А именно, положим

$$\bigcup_{\alpha \in I} A_\alpha = \{a : a \in A_\alpha \text{ хотя бы для одного } \alpha \in I\};$$

$$\bigcap_{\alpha \in I} A_\alpha = \{a : a \in A_\alpha \text{ для всех } \alpha \in I\}.$$

**Определение 1.5.** Разностью двух множеств  $A$  и  $B$  называется множество, состоящее из всех элементов, принадлежащих  $A$  и не принадлежащих  $B$ , т.е.

$$A \setminus B = \{a : a \in A \text{ и } a \notin B\}.$$

Если  $A$  – подмножество множества  $X$ , то множество  $X \setminus A$  называют *дополнением* множества  $A$  до множества  $X$  и обозначают  $CA$  или  $\bar{A}$ .

**Определение 1.6.** Симметрической разностью двух множеств  $A$  и  $B$  называется множество

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

Отметим следующие свойства введенных операций над множествами:

- 1)  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ;
- 2)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;
- 3)  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ;
- 4)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;
- 5)  $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ ;
- 6)  $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$ ;
- 7)  $A \Delta B = (A \cup B) \setminus (A \cap B)$ ;
- 8)  $(A \Delta B) \Delta C = A \Delta (B \Delta C)$ ;
- 9)  $(A \Delta B) \Delta C = (A \cup B \cup C) \setminus (A \cap B \cap C)$ .

Заметим также, если  $A_\alpha$  система подмножеств множества  $X$ , то

$$X \setminus \left( \bigcup_{\alpha} A_{\alpha} \right) = \bigcap_{\alpha} (X \setminus A_{\alpha}); \quad X \setminus \left( \bigcap_{\alpha} A_{\alpha} \right) = \bigcup_{\alpha} (X \setminus A_{\alpha}).$$

**Определение 1.7.** *Декартовым произведением (или просто произведением)  $A \times B$  множеств  $A$  и  $B$  называется множество всех упорядоченных пар вида  $(a, b)$ , у которых на первом месте стоит элемент из множества  $A$ , а на втором – из  $B$ , т.е.*

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Аналогичным образом дается определение произведения  $A_1 \times \dots \times A_n$  любого конечного набора множеств  $A_1, \dots, A_n$  как множество всех упорядоченных наборов из  $n$  элементов.

**Пример 1.2.** Если множества  $A$  и  $B$  состоят из вещественных чисел, то пару  $(a, b)$ , где  $a \in A, b \in B$ , можно рассмотреть как точку плоскости с абсциссой  $a$  и ординатой  $b$ . Заметим также, что произведение  $\mathbb{R} \times \mathbb{R}$  образует множество всех точек плоскости.

### 1.3. Фактор-множество

Рассмотрим произвольное множество  $A$ . По данному множеству можно строить новые множества, рассматривая множество некоторых подмножеств множества  $A$ . Среди таких множеств важную роль играют так называемые *покрытия* и *разбиения*.

**Определение 1.8.** *Всякое семейство  $S = \{B_\alpha\}$ ,  $\alpha \in I$  непустых подмножеств множества  $A$  называется покрытием множества  $A$ , если каждый элемент множества  $A$  принадлежит хотя бы одному из множеств  $B_\alpha$  семейства  $S$ .*

**Определение 1.9.** *Покрытие  $S = \{B_\alpha\}$ ,  $\alpha \in I$  множества  $A$  называется разбиением множества  $A$ , если каждый элемент множества  $A$  принадлежит только одному из множеств  $B_\alpha$  покрытия  $S$ .*

Иными словами, всякое семейство  $S = \{B_\alpha\}$ ,  $\alpha \in I$  непустых подмножеств множества  $A$  называется *разбиением* множества  $A$ , если его множества попарно не пересекаются, а объединение всех множеств семейства есть множество  $A$ .

**Определение 1.10.** *Подмножество  $B_\alpha$  разбиения  $S$  называют классом данного разбиения, а само разбиение  $S$  называют также фактор-множеством множества  $A$ .*

Таким образом, задание фактор-множества сводится к заданию классов разбиения. Основным инструментом для описания классов разбиения является понятие отношения эквивалентности.

**Определение 1.11.** *Бинарным отношением называется любое множество упорядоченных пар.*

Из определения следует, что бинарным отношением является любое подмножество прямого произведения двух множеств.

Если  $R$  – бинарное отношение и  $(a, b) \in R$ , то говорят, что  $a$  и  $b$  связаны отношением  $R$ , или что для  $a$  и  $b$  выполняется отношение  $R$ . Вместо записи  $(a, b) \in R$  часто используют более простую  $aRb$ .

**Замечание 1.1.** *Если  $R \in A \times A$ , то говорят, что  $R$  есть бинарное отношение на множестве  $A$ .*

**Определение 1.12.** *Бинарное отношение  $R$  на множестве  $A$  называется рефлексивным на  $A$ , если для каждого  $a$  из  $A$  выполнено  $aRa$ .*

В качестве примеров рефлексивных отношений можно указать отношение параллельности на множестве прямых плоскости, отношение равенства на каком-либо множестве чисел и отношение делимости на какой-либо совокупности целых чисел.

**Определение 1.13.** *Бинарное отношение  $R$  (на  $A$ ) называется транзитивным (на  $A$ ), если для любых  $a, b, c$  из области отношения  $R$  (на  $A$ ) из  $aRb$  и  $bRc$  следует  $aRc$ .*

Например, отношение делимости на множестве целых чисел является транзитивным.

**Определение 1.14.** *Бинарное отношение  $R$  (на  $A$ ) называется симметричным (на  $A$ ), если для любых  $a, b$  из области отношения  $R$  (на  $A$ ) из  $aRb$  следует  $bRa$ .*

Например, симметричными являются отношение параллельности прямых, отношение перпендикулярности прямых и отношение равенства.

Важным видом бинарного отношения является отношение эквивалентности.

**Определение 1.15.** *Бинарное отношение  $R$  на  $A$  называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.*

Отношение эквивалентности часто обозначают символом  $a \sim b$ . Элементы  $a$  и  $b$  будем называть эквивалентными.

**Пример 1.3.** Пусть  $A$  – множество прямых на плоскости и  $R = \{(a, b) : a, b \in R \text{ и } a \text{ параллельно } b\}$  – отношение параллельности. Отношение параллельности на  $A$  есть отношение эквивалентности.

**Пример 1.4.** Пусть  $\mathbb{Z}$  – множество всех целых чисел и  $n$  – целое число, отличное от нуля. Отношение  $R = \{(a, b) : a, b \in \mathbb{Z} \text{ и } (a - b) \text{ делится на } n\}$  называется отношением сравнения по модулю  $n$ . Это отношение является отношением эквивалентности на  $\mathbb{Z}$ .