



Московский  
педагогический  
государственный  
университет

**А. В. Царев, Г. В. Шеина**

**ЭЛЕМЕНТЫ  
АБСТРАКТНОЙ  
И КОМПЬЮТЕРНОЙ  
АЛГЕБРЫ**

**Москва  
2016**

Министерство образования и науки Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Московский педагогический государственный университет»



А. В. Царев, Г. В. Шеина

# ЭЛЕМЕНТЫ АБСТРАКТНОЙ И КОМПЬЮТЕРНОЙ АЛГЕБРЫ

*Учебное пособие*

МПГУ  
Москва • 2016

УДК 512 (07)  
ББК 22.14я73  
Ц181

**Рецензенты:**

**В. А. Артамонов**, доктор физико-математических наук,  
профессор кафедры высшей алгебры  
Московского государственного университета им. М. В. Ломоносова  
**О. В. Муравьева**, кандидат физико-математических наук, доцент  
кафедры теоретической информатики и дискретной математики  
Московского педагогического государственного университета

**Царев, Андрей Валерьевич.**

Ц181 Элементы абстрактной и компьютерной алгебры : Учебное пособие / А. В. Царев, Г. В. Шеина. – Москва : МПГУ, 2016. – 116 с.

ISBN 978-5-4263-0393-5

Учебное пособие подготовлено на кафедре алгебры МПГУ и адресовано студентам математических факультетов педвузов. В нем рассматриваются не только необходимые теоретические основы курса «Абстрактная и компьютерная алгебра», но и приводится большое количество задач разного уровня сложности, в том числе и задания для самостоятельных и контрольных работ.

УДК 512 (07)  
ББК 22.14я73

ISBN 978-5-4263-0393-5

© МПГУ, 2016  
© Царев А. В., Шеина Г. В., текст, 2016

## Оглавление

<b>ВВЕДЕНИЕ</b> .....	<b>5</b>
<b>ЧТО ТАКОЕ КОМПЬЮТЕРНАЯ АЛГЕБРА?</b> .....	<b>7</b>
<b>§1. НЕОБХОДИМЫЕ СВЕДЕНИЯ ИЗ АБСТРАКТНОЙ АЛГЕБРЫ</b> .....	<b>10</b>
Отношения.....	10
Прямое произведение множеств.....	10
Бинарные отношения.....	11
Виды бинарных отношений.....	12
Отношения эквивалентности. Классы эквивалентности .....	15
<i>Свойства классов эквивалентности</i> .....	16
<i>Фактормножества</i> .....	18
Понятие кольца, поля, области целостности.....	20
Вычисление обратной матрицы.....	23
Решение матричных уравнений.....	25
Варианты для самостоятельных работ.....	26
Теория делимости в коммутативных кольцах.....	29
<b>§2. ПРОБЛЕМА ПРЕДСТАВЛЕНИЯ ДАННЫХ</b> .....	<b>31</b>
Кольцо целых чисел.....	34
Поле рациональных чисел.....	35
Египетские дроби.....	35
Алгоритм Фибоначчи.....	37
Кольца вычетов.....	38
Нахождение остатков от деления .....	39
Конечные поля.....	40
Задания для самостоятельных работ.....	41
Многочлены.....	46
Алгебраические числа.....	48
<b>§3. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ</b> .....	<b>50</b>
Понятие наибольшего общего делителя.....	50
Свойства наибольшего общего делителя целых чисел .....	51
Алгоритмы вычисления НОД для целых чисел .....	52
<i>Алгоритм Евклида</i> .....	52
<i>Расширенный алгоритм Евклида</i> .....	53

<i>Бинарный алгоритм</i> .....	56
<i>Примарный алгоритм</i> .....	57
Наибольший общий делитель многочленов .....	59
ИСПОЛЬЗОВАНИЕ АССОЦИИРОВАННЫХ МНОГОЧЛЕНОВ .....	61
НЕПРИВОДИМОСТЬ НАД ПРОИЗВОЛЬНЫМ ПОЛЕМ И ПОЛЯМИ $\mathbb{R}$ И $\mathbb{C}$ .....	62
МНОГОЧЛЕНЫ НАД ПОЛЕМ $\mathbb{Q}$ .....	65
РЕДУКЦИЯ ЦЕЛОЧИСЛЕННЫХ МНОГОЧЛЕНОВ .....	66
РЕДУКЦИОННЫЙ ПРИЗНАК 1 .....	67
РЕДУКЦИОННЫЙ ПРИЗНАК 2 .....	68
ПРИЗНАК ЭЙЗЕНШТЕЙНА И ЕГО МОДИФИКАЦИИ .....	69
УПРАЖНЕНИЯ .....	71
ЗАДАНИЯ ДЛЯ КОНТРОЛЬНЫХ РАБОТ .....	72
<b>§4. МНОГОЧЛЕНЫ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ .....</b>	<b>75</b>
Степень многочлена .....	76
<i>Свойства степени многочлена</i> .....	76
<i>Лексикографический порядок и его свойства</i> .....	77
<b>§5. РЕШЕНИЕ СИСТЕМ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ .....</b>	<b>80</b>
БАЗИС ИДЕАЛА .....	80
ВСПОМОГАТЕЛЬНЫЕ ПОНЯТИЯ И КОНСТРУКЦИИ .....	84
РЕШЕНИЕ СИСТЕМ УРАВНЕНИЙ С ПОМОЩЬЮ РЕДУКЦИЙ .....	89
ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНЫХ РАБОТ .....	92
БАЗИС ГРЁБНЕРА .....	92
АЛГОРИТМ БУХБЕРГЕРА .....	96
УПРАЖНЕНИЯ .....	99
<b>§6. ОТДЕЛЕНИЕ КОРНЕЙ .....</b>	<b>100</b>
Последовательность многочленов ШТУРМА .....	100
ПРОСТЕЙШИЕ СВОЙСТВА СИСТЕМЫ МНОГОЧЛЕНОВ ШТУРМА .....	102
СЧЕТЧИК ПЕРЕМЕН ЗНАКА И ЕГО СВОЙСТВА .....	103
СЧЕТЧИК ПЕРЕМЕН ЗНАКОВ. ОСНОВНАЯ ЛЕММА .....	104
ФОРМУЛИРОВКА ТЕОРЕМЫ ШТУРМА. ПРИМЕРЫ И УПРАЖНЕНИЯ .....	108
<b>ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ЗАЧЕТА .....</b>	<b>111</b>
<b>ПРИМЕРНЫЕ ВОПРОСЫ К ЭКЗАМЕНУ .....</b>	<b>113</b>
<b>РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА .....</b>	<b>115</b>

## §1. Необходимые сведения из абстрактной алгебры

### Отношения

Элементы двух или нескольких множеств могут быть связаны друг с другом тем или иным образом. Например, две прямые в пространстве могут быть параллельными, перпендикулярными, скрещивающимися. Две прямые могут быть перпендикулярны одной и той же плоскости. Алгебраические выражения могут быть тождественно равными. Для описания подобного рода связей нам понадобятся понятия прямого произведения и отношения.

### Прямое произведение множеств

**Определение.** **Прямым произведением** двух множеств  $A$  и  $B$  называется множество всевозможных упорядоченных пар вида  $(a, b)$ , где  $a \in A$ ,  $b \in B$ . Прямое произведение обозначается так:  $A \times B$ .

**Замечание.** Слова «множество упорядоченных пар» означают, что пары  $(a, b)$  и  $(b, a)$  различны, если  $a \neq b$ .

Отметим, что пары  $(a, b)$  и  $(a_1, b_1)$  мы считаем **равными тогда и только тогда**, когда  $a = a_1$  и  $b = b_1$ .

**Пример 1.** Прямое произведение множества  $\mathbb{R}$  на себя, то есть  $\mathbb{R} \times \mathbb{R}$ , обозначается как  $\mathbb{R}^2$ . Оно обычно отождествляется с множеством координат всех точек плоскости.

Приведем пример множества, не представимого в виде прямого произведения.

**Пример 2.** Рассмотрим множество  $M$  точек на плоскости  $\mathbb{R}^2$ , задаваемое уравнением  $x^2 + y^2 = 1$ . Покажем, что множество  $M$  не может быть представлено в виде прямого произведения множеств  $A \subseteq \mathbb{R}$  и  $B \subseteq \mathbb{R}$ . Предположим, напротив,

что множество  $M$  может быть представлено в виде прямого произведения множеств  $A \subseteq \mathbb{R}$  и  $B \subseteq \mathbb{R}$ , то есть справедливо равенство  $M = A \times B$ .

Точка  $(0; 1)$  удовлетворяет уравнению  $x^2 + y^2 = 1$ . Поэтому  $1 \in B$ . Уравнению  $x^2 + y^2 = 1$  удовлетворяет также точка  $(1; 0)$ , поэтому  $1 \in A$ . Точка  $(1; 1)$ , по определению прямого произведения, также должна принадлежать прямому произведению, и если  $M = A \times B$ , то ее координаты должны удовлетворять уравнению окружности. Но последнее неверно.

Наряду с прямым произведением двух множеств можно рассматривать также прямое произведение  $n$  множеств  $A_1, \dots, A_n$ , которое обычно обозначают

$$A_1 \times \dots \times A_n.$$

По определению,  $A_1 \times \dots \times A_k = \{(a_1, \dots, a_k), a_1 \in A_1, \dots, a_k \in A_k\}$ .

В случае конечных множеств  $A_1$  и  $A_2$  количество элементов в прямом произведении равно  $n(A) \cdot n(B)$ , где  $n(M)$  есть число элементов множества  $M$ .

Индукцией по числу сомножителей можно показать, что

$$n(A_1 \times \dots \times A_k) = n(A_1) \cdot \dots \cdot n(A_k).$$

**Задача.** Пусть  $A = \{a, b\}$ ,  $B = \{c, d, e\}$ . Выпишите все элементы прямых произведений  $A \times A, A \times B, B \times A, B \times B, A \times A \times A$ .

### Бинарные отношения

Элементы двух множеств или одного и того же множества могут находиться в различных отношениях по отношению друг к другу. Например, относительно двух натуральных чисел можно выяснять, какое из них больше, или является ли одно из них делителем другого.

В обычной жизни мы также выясняем, являются ли два человека, например, членами одной семьи, а также является ли один человек старше другого. Дадим определение математического понятия отношения.

**Определение.** Любое подмножество прямого произведения множеств  $A$  и  $B$  называется **бинарным отношением** между элементами множеств  $A$  и  $B$ .

Таким образом, если  $R \subseteq A \times B$ , то  $R$  называется бинарным отношением. При этом говорят, что если  $(x, y) \in R$ , то для элементов  $x, y$  *выполняется отношение*  $R$ . Вместо записи  $(x, y) \in R$  часто используют более простую запись  $xRy$ .

### Примеры

- На множестве всех людей можно рассматривать отношения быть родителем, быть сестрой, быть братом, быть друзьями.
- На множестве всех прямых плоскости можно рассмотреть отношение быть параллельными или перпендикулярными.
- На множестве действительных чисел можно рассмотреть отношения «порядка»: одно число строго меньше другого, одно число не больше другого и т. д.
- Множество  $R$  точек на плоскости  $\mathbb{R}^2$ , задаваемое неравенством  $x^2 + y^2 < 1$  также задает бинарное отношение между действительными числами. Например, числа  $x = 0,5$  и  $y = 1$  не находятся в этом отношении, а числа  $x = 0,5$  и  $y = 0,4$  находятся в этом отношении.

### Виды бинарных отношений

Перейдем теперь к рассмотрению бинарных отношений в случае, когда  $A = B$ . Рассмотрим наиболее распространенные (в математике) виды и примеры таких бинарных отношений.

**1. Рефлексивные** отношения. Так называются отношения  $R$  на множестве  $A$ , обладающие свойством:

для любого элемента  $a \in A$  выполняется условие  $(a, a) \in R$ .

**Примеры.**

- Отношение «число  $x$  делит число  $y$ » на множестве натуральных чисел является рефлексивным, поскольку каждое натуральное число является своим делителем.
- Отношение  $x < y$  на множестве действительных чисел не является рефлексивным, а отношение  $x \leq y$  является рефлексивным.

**2. Симметричные** отношения. Так называются отношения  $R$  на множестве  $A$ , у которых для любых элементов  $a, b \in A$  из того, что  $(a, b) \in R$ , следует, что  $(b, a) \in R$ .

**Примеры.**

- Отношение «число  $x$  делит число  $y$ » на множестве натуральных чисел не является симметричным, поскольку, например, число 2 делит число 4, а 4 не делит число 2.
- Отношение  $x < y$  на множестве действительных чисел не является симметричным; отношение  $x \leq y$  также не является симметричным.

**Замечание.**

Пусть отношение  $R$  задает отношение на множестве действительных чисел, то есть  $R \subseteq \mathbb{R}^2$ . Тогда рефлексивность и симметричность можно «видеть»: для рефлексивных отношений все точки прямой  $y = x$  должны принадлежать множеству  $R$ .

Для симметричных отношений множество  $R$  должно располагаться симметрично относительно прямой  $y = x$ .

**Задача.** Изобразите множество решений неравенства  $y > x$  и неравенства  $y > -x$  и, используя замечание, убедитесь в том, что первое отношение не симметрично, а второе симметрично.

**3. Антисимметричные** отношения. Так называются отношения, у которых для любых элементов  $x, y \in A$  выполняется условие  $\begin{cases} xRy \\ yRx \end{cases} \Rightarrow x = y$ .

#### Примеры

- Отношение «число  $x$  делит число  $y$ » на множестве **натуральных** чисел является антисимметричным, поскольку если натуральное число  $x$  делит число  $y$  и число  $y$  делит число  $x$ , то  $x = y$ .
- Отношение «число  $x$  делит число  $y$ » на множестве **целых** чисел не является антисимметричным, поскольку если целое число  $x$  делит целое число  $y$  и число  $y$  делит число  $x$ , то  $x = \pm y$ .

**4. Транзитивные** отношения. Так называются отношения, у которых для любых элементов  $x, y, z \in A$  выполняется условие  $\begin{cases} xRy \\ yRz \end{cases} \Rightarrow xRz$ .

#### Примеры

- Отношение  $x \leq y$  (или  $x < y$ ) на множестве действительных чисел является транзитивным.
- Отношение делимости на множестве целых чисел является транзитивным.

**5. Отношения порядка.** Все отношения порядка должны обладать свойствами:

- 1) антисимметричность;
- 2) транзитивность;
- 3) отношение **нестрогого** порядка должно, кроме того, быть рефлексивным.

#### Примеры

- Отношение  $\subseteq$  на множестве  $P(M)$  всех подмножеств данного множества  $M$  задает (нестрогий) порядок.
- Отношение  $x \leq y$  также задает нестрогий порядок на множестве действительных чисел.

**Задача 1.** Приведите примеры бинарного отношения, которое

- а) рефлексивно, транзитивно, но не антисимметрично;
- б) транзитивно, симметрично, но не рефлексивно;
- в) рефлексивно, транзитивно, но не симметрично;
- г) рефлексивно, симметрично, но не транзитивно.

**Область определения** отношения  $R \subseteq A \times A$  называется множество таких элементов  $x \in A$ , для которых существует такой элемент  $y \in A$ , что  $(x, y) \in R$ .

Область определения отношения  $R$  будем обозначать  $\delta_R$ .

**Пример.**

Область определения отношения  $x^2 + y^2 = 0$  состоит из одной точки 0, а область определения отношения  $x^2 + y^2 = 1$  состоит из всех точек отрезка  $[-1; 1]$ .

**Задача 2.** Докажите, что если  $R \subseteq A \times A$  – транзитивно и симметрично на множестве  $A$  и область определения  $\delta_R$  совпадает с  $A$ , то  $R$  – рефлексивно.

Среди всех отношений особое место занимают отношения, которые являются рефлексивными, симметричными и транзитивными. К таким отношениям относятся равенства, но не только они. Такие отношения называют **отношениями эквивалентности**.

### Отношения эквивалентности. Классы эквивалентности

**Определение.** Отношение  $R \subseteq A \times A$  называется **отношением эквивалентности** на множестве  $A$ , если оно

- 1) рефлексивно,
- 2) симметрично,
- 3) транзитивно.

Отношение эквивалентности будем символически обозначать знаком  $\sim$  и вместо записи  $aRb$  использовать запись  $a\sim b$ .

### Примеры

- Отношение подобия геометрических фигур является отношением эквивалентности.
- Отношение на множестве комплексных чисел, заданное так:

$$z_1 R z_2 \Leftrightarrow \operatorname{Re} z_1 = \operatorname{Re} z_2.$$

**Задача 1.** Докажите, что приведенные отношения являются отношениями эквивалентности.

**Определение.** Множество элементов, эквивалентных элементу  $a$ , называется **классом эквивалентности** этого элемента. Мы будем обозначать этот класс эквивалентности символом  $C_a$ . Итак,  $C_a = \{a' \mid a' \in A, a' \sim a\}$ .

**Задача 2.** Зададим отношение на множестве комплексных чисел так:

$$z_1 R z_2 \Leftrightarrow \operatorname{Re} z_1 = \operatorname{Re} z_2.$$

Проверьте, что это отношение эквивалентности. Найдите класс эквивалентности числа  $1 + i$ . Изобразите графически все элементы этого класса эквивалентности, то есть изобразите на комплексной плоскости все комплексные числа, которые эквивалентны числу  $1 + i$ .

### *Свойства классов эквивалентности*

1. Любой класс эквивалентности  $C_a$  не пуст.
2. Классы эквивалентности двух элементов совпадают тогда и только тогда, когда элементы эквивалентны:  $C_a = C_{a'} \Leftrightarrow a \sim a'$ .
3. Классы эквивалентности неэквивалентных элементов не пересекаются; точнее,  $a \not\sim a' \Leftrightarrow C_a \cap C_{a'} = \emptyset$ .

*Учебное пособие*

Царев Андрей Валерьевич  
Шеина Галина Валентиновна

ЭЛЕМЕНТЫ АБСТРАКТНОЙ  
И КОМПЬЮТЕРНОЙ АЛГЕБРЫ

Редактор *Дубовец В. В.*  
Оформление обложки *Удовенко В. Г.*  
Компьютерная верстка *Дорожкина О. Н., Потрахов И. А.*

Управление издательской деятельности  
и инновационного проектирования МПГУ  
119571, Москва, Вернадского пр-т, д. 88, оф. 446.  
Тел.: (499) 730-38-61  
E-mail: [izdat@mpgu.edu](mailto:izdat@mpgu.edu)

Подписано в печать 04.07.2016. Формат 60x90/16.  
Бум. офсетная. Печать цифровая. Объем 7,25 п. л.  
Тираж 500 экз. Заказ № 565.

ISBN 978-5-4263-0393-5



9 785426 303935