

УДК 512:511(075.8)  
ББК 22.14я73+22.13я73  
С 35

Рецензент - кандидат физико-математических наук В.В.Носов

**Сикорская, Г.А.**  
**С 35** Алгебра и теория чисел: учебное пособие / Г.А. Сикорская;  
Оренбургский гос. ун-т. – Оренбург : ОГУ, 2017. – 303с.  
"  
УДР ; 9: /7/9632/3; 65/8

Пособие подготовлено в соответствии с содержанием курса «Алгебра и теория чисел», входящего в дисциплину «Математика», определяемую стандартом высшего образования. Пособие способствует приобретению обучающимися знаний в области основ алгебры и теории чисел, как теоретической базы для изучения последующих дисциплин профессионального цикла.

Пособие состоит из двух частей, 18 глав. Каждая глава включает в себя относительно самостоятельную теоретическую часть курса, обычно разделяемую преподавателем на 2 – 4 лекции.

Излагаемые теоретические вопросы курса алгебры и теории чисел снабжены задачами практического характера, способствующими лучшему пониманию теории.

В заключении пособия предлагаются теоретические вопросы для самоконтроля по каждой из глав, а также тесты практического содержания.

Учебное пособие предназначено для подготовки бакалавров по направлению 02.03.02 «Фундаментальная информатика и информационные технологии» с общим профилем подготовки.

"

УДК 512:511(075.8)  
ББК 22.14я73+22.13я73

© Сикорская Г.А., 2017  
© ОГУ, 2017

## Содержание

Предисловие .....	8
Введение.....	9
Часть 1 Алгебра .....	15
Глава 1 Основные алгебраические структуры .....	15
1.1 Множества. Основные понятия .....	15
1.2 Операции над множествами и их свойства .....	16
1.3 Алгебраическая операция.....	20
1.4 Алгебраические структуры .....	22
1.5 Группа.....	23
1.6 Кольцо .....	25
1.7 Поле .....	25
Глава 2 Поле комплексных чисел.....	26
2.1 Комплексные числа алгебраической формы.....	26
2.2 Операции над комплексными числами алгебраической формы .....	28
2.3 Тригонометрическая форма комплексных чисел .....	32
2.4 Операции над комплексными числами тригонометрической формы .....	35
2.5 Корни из единицы .....	38
Глава 3 Кольцо многочленов .....	41
3.1 Сложение многочленов. Умножение многочлена на число .....	41
3.2 Деление многочленов .....	42
3.3 Метод Горнера.....	44
3.4 Деление многочленов нацело .....	46
3.5 Корни многочлена. Теорема Безу.....	47
3.6 Основная теорема алгебры.....	49
3.7 Формулы Вьета .....	51
3.8 Разложение многочлена на множители .....	51
3.9 Наибольший общий делитель многочленов. Алгоритм Евклида .....	52
Глава 4 Матрицы и определители .....	57
4.1 Матрицы. Основные понятия и определения.....	57
4.2 Умножение матрицы на число. Сумма матриц.....	58
4.3 Произведение матриц .....	59

4.4 Многочлен от матрицы.....	61
4.5 Транспонирование матриц .....	61
4.6 Обратная матрица.....	63
4.7 Ортогональная матрица.....	64
4.8 Определитель матрицы.....	65
4.9 Свойства определителей.....	72
4.10 Методы вычисления определителей n-го порядка .....	74
4.11 Обратная матрица.....	79
4.12 Методы нахождения обратных матриц .....	81
4.13 Простейшие матричные уравнения.....	83
4.14 Ранг матрицы .....	84
4.15 Методы вычисления ранга матрицы .....	85
4.16 Базисный минор матрицы .....	88
Глава 5 Системы линейных уравнений.....	90
5.1 Методы решения СЛУ .....	91
5.2 Критерий совместности системы линейных уравнений .....	99
5.3 Метод решения неопределенной системы .....	100
5.4 Системы линейных однородных уравнений. Фундаментальная система решений.....	101
5.5 Взаимосвязь между решениями неоднородных и однородных систем ..	105
Глава 6 Линейное пространство. Подпространство линейного пространства .....	106
6.1 Понятие линейного пространства .....	106
6.2 Линейная зависимость векторов.....	110
6.3 Размерность и базис линейного пространства .....	112
6.4 Ранг системы векторов линейного пространства .....	115
6.5 Матрица перехода от базиса к базису. Преобразование координат вектора .....	116
6.6 Изоморфизм линейных пространств.....	119
6.7 Подпространство линейного пространства .....	120
Глава 7 Евклидово пространство.....	121
7.1 Евклидово пространство. Основные понятия и определения .....	121
7.2 Ортогональные векторы. Система ортогональных векторов .....	124
7.3 Норма вектора евклидова пространства .....	125
7.4 Угол между двумя векторами евклидова пространства.....	126

7.5 Ортонормированный базис .....	127
Глава 8 Линейный оператор.....	129
8.1 Оператор. Основные понятия и определения .....	129
8.2 Линейный оператор.....	130
8.3 Матрица линейного оператора .....	134
8.4 Связь между координатами вектора и его образа.....	136
8.5 Преобразование матрицы линейного оператора при переходе к новому базису.....	137
8.6 Ядро и область значений линейного оператора.....	140
8.7 Характеристический многочлен, характеристическое уравнение линейного оператора.....	141
8.8 Собственные векторы линейного оператора.....	142
8.9 Собственные значения и собственные векторы симметрической матрицы .....	145
8.10 Диагонализируемость линейного оператора.....	147
8.11 Действия над линейными операторами .....	149
8.12 Оператор, обратный данному линейному оператору.....	153
8.13 Ортогональные операторы .....	154
Глава 9 Квадратичные формы .....	156
9.1 Квадратичные формы. Основные понятия и определения .....	156
9.2 Матричный вид квадратичной формы .....	157
9.3 Преобразование квадратичной формы линейным однородным оператором .....	158
9.4 Канонический вид квадратичной формы.....	160
9.5 Методы приведения квадратичной формы к каноническому виду .....	162
9.6 Нормальный вид квадратичной формы .....	167
Часть 2 Теория чисел .....	171
Глава 10 Теория делимости.....	171
10.1 Целые числа. Свойства .....	171
10.2 Наибольший общий делитель .....	173
10.3 Алгоритм Евклида.....	175
10.4 Алгоритм нахождения НОД более чем двух чисел .....	177
10.5 Представление наибольшего общего делителя в линейной форме .....	178
10.6 Наименьшее общее кратное .....	179
10.7 Алгоритм нахождения НОК более чем двух чисел .....	180

10.8 Таблица простых чисел .....	180
10.9 Основная теорема арифметики .....	181
10.10 Признаки делимости целых чисел.....	183
10.11 Разложение чисел на простые множители .....	186
10.12 Связь НОД (a, b) и НОК (a, b). Задачи на теорию делимости целых чисел .....	190
Глава 11 Важнейшие функции в теории чисел .....	191
11.1 Целая часть числа, дробная часть числа.....	191
11.2 Мультипликативные функции .....	193
11.3 Число делителей данного числа .....	195
11.4 Сумма делителей данного числа .....	195
11.6 Функция Эйлера .....	197
Глава 12 Цепные дроби. Подходящие дроби .....	199
12.1 Конечные цепные дроби.....	199
12.2 Подходящие дроби.....	201
Глава 13 Сравнение по модулю .....	206
13.1 Сравнение по модулю. Основные понятия и определения.....	206
13.2 Действия над сравнениями.....	207
13.3 Свойства сравнений .....	208
13.5 Операции над вычетами .....	213
13.6 Взаимнообратные по модулю m.....	217
Глава 14 Сравнения первой степени с одним неизвестным .....	219
14.1 Сравнения. Основные понятия и определения .....	219
14.2 Сравнение первой степени .....	220
14.3 Методы решений линейных сравнений .....	221
14.4 Системы линейных сравнений.....	224
Глава 15 Диофантовы уравнения.....	227
15.1 Диофантовы уравнения. Историческая справка .....	227
15.2 Диофантовы уравнения 1-й степени и методы их решения .....	227
15.3 Линейное однородное диофантово уравнение с двумя переменными.	232
15.4 Линейное диофантово уравнение с двумя неизвестными .....	232
Глава 16 Сравнения высших степеней.....	240
16.1 Сравнение второй степени по простому модулю .....	240

16.2 Квадратичный вычет по модулю $p$ .....	241
16.3 Символ Лежандра и его свойства .....	241
16.4 Символ Якоби .....	243
16.5 Сравнения высших степеней по простому модулю .....	243
16.6 Сравнение любой степени по составному модулю .....	245
Глава 17 Первообразные корни и индексы .....	247
17.1 Порядок числа по данному модулю .....	247
17.2 Первообразный корень по модулю $m$ .....	247
17.3 Алгоритм поиска попарно не сравнимых первообразных корней по простому модулю $p > 2$ .....	250
17.4 Индекс числа по основанию. Дискретный логарифм .....	251
Глава 18 Приложение теории чисел к криптографии .....	254
18.1 Криптография как прикладная наука .....	254
18.2 Теория чисел и метод ассиметричного шифрования RSA .....	255
Список использованных источников .....	259
Приложение А .....	261
Вопросы для самопроверки теоретических знаний по дисциплине «Алгебра и теория чисел» .....	261
Приложение Б .....	275
Тестовые задания по дисциплине «Алгебра и теория чисел» .....	275