Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования
«Рязанский государственный университет имени С.А.Есенина»

Согласовано:
Декан
физико-математического факультета
___________________________________Кирьяков Б.С.
«_____»____________________________2009 г.

Утверждено на заседании кафедры
математики и МОМД
Протокол № 6 от «18» ноября 2009 г.
Зав. кафедрой доктор пед. н., канд. физ-мат. н.,
профессор ____________________ Назиев А.Х.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО ДИСЦИПЛИНАМ

Алгебра и теория чисел,

Избранные вопросы алгебры

Для специальности 351500 – Математическое обеспечение и администрирование информационных систем
Факультет: физико-математический.

Курс «Алгебра и теория чисел»: курсы 1, 2, семестры 1, 2, 3.
Всего часов (включая самостоятельную работу) – 358.

Курс «Избранные вопросы алгебры»: курс 2, семестр 4.
Всего часов (включая самостоятельную работу) – 144.

Составитель: **С.А. Моисеев**, кандидат педагогических наук, доцент

Рязань, 2009

ПРОГРАММЫ КУРСОВ

Пояснительная записка

Данные курсы посвящены изучению основных числовых и алгебраических структур. Изложение идет от рассмотрения более простых понятий к более трудным и абстрактным. Оба этих курса составляют неразрывное единое целое: материал первого курса доставляет примеры, иллюстрирующие более абстрактный материал второго курса, со своей стороны, материал второго курса позволяет унифицировать изучаемые понятия первого курса, посмотреть на них с единой точки зрения (например, параллелизм в свойствах делимости целых чисел и многочленов отражает то обстоятельство, что оба эти кольца являются евклидовыми кольцами).

Первый семестр начинается с изложения элементов теории множеств, математической логики и сведений о важнейших числовых множествах. Далее рассматриваются основные алгебраические структуры, системы линейных уравнений, арифметические векторы, матрицы и определители.

Во втором семестре рассматриваются элементы теории векторных пространств, пространств с метрикой и линейные отображения векторных пространств.

Третий семестр посвящён изучению чисел и многочленов: вначале изучается теория делимости целых чисел, затем – она же, только на языке теории сравнений, далее изучаются комплексные числа. Далее подробно изучается кольцо многочленов от одной переменной, в том числе и над важнейшими числовыми полями, более бегло – кольцо многочленов от нескольких переменных, его подкольцо симметрических многочленов. Завершает курс раздел, в котором рассматриваются элементы теории расширения полей.

В четвёртом семестре изучение алгебраического материала продолжается в рамках курса «Избранные вопросы алгебры». Он посвящён более подробному изучению важнейших алгебраических структур: групп, колец и полей. Рассматриваются подалгебры и морфизмы этих структур, а также взаимосвязь основных операций с некоторыми отношениями на этих алгебрах: отношением порядка и отношением делимости.

Тематическое планирование является примерным. Преподаватель имеет право изменять последовательность прохождения отдельных разделов, соотношение количества часов на лекции и практические занятия.

Настоящая программа разработана в соответствии с требованиями государственного образовательного стандарта к подготовке специалистов по специальности 351500 «Математическое обеспечение и администрирование информационных систем».

Содержание учебной дисциплины

«Алгебра и теория чисел»

1. Элементы теории множеств, математической логики, числовых систем.
Множества и операции над ними. Бинарные отношения. Отношение эквивалентности и отношение порядка Отображения, композиция отображений, обратимые отображения. Высказывания и предикаты. Отношения следования и равносильности. Системы действительных, рациональных, целых и натуральных чисел.

2. Основные алгебраические структуры.
Алгебраические операции. Группа, кольцо, поле. Простейшие свойства групп, колец, полей. Подгруппа. Подкольцо. Подполе. Изоморфизм алгебраических структур.

3. Системы линейных уравнений. Арифметическое *n*-мерное векторное пространство.
Решение систем линейных уравнений методом Гаусса. Арифметическое *n*-мерное векторное пространство. Линейная зависимость векторов. Базис и ранг системы векторов. Ранг матрицы. Теорема Кронекера-Капелли.
Связь между решениями неоднородной и соответствующей однородной систем. Свойства решений однородной системы уравнений.

4. Матрицы и определители.
Операции над матрицами и их свойства. Обратная матрица. Условие обратимости матрицы. Перестановки и подстановки. Определение определителя. Свойства определителя. Миноры и алгебраические дополнения. Разложение определителя по строке или столбцу. Определитель произведения матриц. Теорема о ранге матрицы.

5. Векторные пространства.
Определение, примеры, простейшие свойства векторных пространств. Линейная зависимость векторов. Базис и ранг системы векторов. Конечномерные векторные пространства. Базис и размерность конечномерного векторного пространства. Координаты вектора относительно данного базиса. Подпространство. Пересечение, сумма и прямая сумма подпространств.
Связь между координатами векторов относительно различных базисов. Изоморфизм векторных пространств.

6. Евклидовы пространства.
Скалярное произведение, евклидовы и унитарные пространства. Длина вектора и угол между векторами. Ортогональность. Процесс ортогонализации. Ортонормированный базис, его существование. Ортогональное дополнение к подпространству, свойства ортогонального дополнения. Изоморфизм евклидовых пространств.

7. Линейные отображения и линейные операторы.
Понятия линейного отображения и оператора. Операции над линейными отображениями. Ранг, дефект, ядро и образ линейного отображения. Обратимые операторы. Изоморфизм алгебры операторов и полной матричной алгебры. Собственные числа и собственные векторы оператора, связь с матричными понятиями. Характеристический многочлен оператора. Теорема Гамильтона-Кэли для операторов.

8. Теория делимости целых чисел.
Отношение делимости. Теорема о делении с остатком для целых чисел. Систематическая запись натуральных чисел. НОД и НОК чисел. Взаимно простые числа. Простые числа и основная теорема арифметики. Бесконечность множества простых чисел. Каноническое разложение.

9. Теория сравнений.
Числовые сравнения и их свойства. Классы вычетов. Полная и приведенная системы вычетов. Функция Эйлера. Теорема Эйлера. Сравнений первой степени. Диофантовы уравнения. Признаки делимости

10. Комплексные числа.
Определение поля комплексных чисел. Алгебраическая и тригонометрическая формы комплексного числа. Действия с комплексными числами в тригонометрической форме. Извлечение корней из комплексных чисел. Комплексно сопряженные числа

11. Многочлены от одной переменной.
Кольцо многочленов от одной переменной над коммутативным кольцом. Теорема Безу. Схема Горнера. Корни многочлена. Алгебраическое и функциональное равенство многочленов. Теорема о делении с остатком для многочленов над полем. Приводимые и неприводимые многочлены. Каноническое разложение многочлена над полем. Формальная производная. Формула Тейлора.
Кольцо многочленов над факториальным кольцом.
12. Многочлены от нескольких переменных.
Понятие многочлена от нескольких переменных. Степень многочлена. Лексикографическое упорядочение членов многочлена. Симметрические многочлены. Основная теорема теории симметрических многочленов.
13. Многочлены над числовыми полями.
Алгебраическая замкнутость поля комплексных чисел. Разложение многочлена над полем комплексных чисел в произведение неприводимых множителей.
Сопряженность мнимых корней многочлена с действительными коэффициентами. Разложение многочлена над полем действительных чисел в произведение неприводимых множителей.
Рациональные корни многочлена с целыми коэффициентами. Критерий Эйзенштейна.
14. Расширения полей.
Простое алгебраическое расширение поля и его строение. Конечное расширение поля. Алгебраическое расширение поля. Составное алгебраическое расширение поля. Поле алгебраических чисел и его алгебраическая замкнутость. Простота конечного расширения.

Содержание учебной дисциплины
«Избранные вопросы алгебры»
(мы продолжаем нумерацию глав)
15. Элементы теории групп.
Теорема о факторизации. Алгебры и алгебраические системы. Изоморфизм алгебр. Примеры и простейшие свойства групп. Целые степени элемента группы. Порядок элемента. Циклические группы. Подгруппы. Теорема Кэли. Разложение группы по подгруппе. Теорема Лагранжа. Нормальные подгруппы. Фактор-группы. Гомоморфизмы и эпиморфизмы групп. Теорема об эпимоморфизмах.
16. Кольца и поля.

Примеры и простейшие свойства колец и полей. Разность и частное, их свойства. Изоморфизм колец и полей. Подкольцо. Подполе. Характеристика кольца.

Упорядоченные кольца и поля. Модуль элемента. Свойства порядка натуральных, целых и рациональных чисел: дискретность $\boldsymbol{N}$ и $\boldsymbol{Z}$, неограниченность $\boldsymbol{N}$, $\boldsymbol{Z}$ и $\boldsymbol{Q}$ в $\boldsymbol{R}$, принцип Архимеда.

Идеалы колец. Сравнение по идеалу. Фактор-кольца. Кольца классов вычетов. Гомоморфизмы и эпиморфизмы колец. Теорема об эпиморфизмах.

17. Элементы теории делимости в целостных кольцах.

Отношение делимости в целостных кольцах. Ассоциированность элементов. Разложение на простые множители. Факториальные кольца (кольца с однозначным разложением), кольца с неоднозначным разложением, кольца без разложения. Кольца главных идеалов. Евклидовы кольца.

18. Поле частных целостного кольца.

Определение и строение поля частных. Изоморфизм полей частных. Теорема о существовании поля частных целостного кольца.

Тематический план курса «Алгебра и теория чисел»

№	Наименование разделов и тем	Всего часов	В т. ч. аудиторных			СР
			Всего	Лек-ции	Пр. зан.	
1.	Элементы теории множеств, математической логики, числовых систем Множества и операции над ними. Бинарные отношения. Отношение эквивалентности и отношение порядка Отображения, композиция отображений, обратимые отображения. Высказывания и предикаты. Отношения следования и равносильности. Системы действительных, рациональных, целых и натуральных чисел.	36	20	10	10	16
2.	Основные алгебраические структуры Алгебраические операции. Группа, кольцо, поле. Простейшие свойства групп, колец, полей. Подгруппа. Подкольцо. Подполе. Изоморфизм алгебраических структур.	22	12	6	6	10
3.	Системы линейных уравнений. Арифметическое n-мерное векторное пространство Решение систем линейных уравнений методом Гаусса. Арифметическое n-	36	20	10	10	16

	мерное векторное пространство. Линейная зависимость векторов. Базис и ранг системы векторов. Ранг матрицы. Теорема Кронекера-Капелли. Связь между решениями неоднородной и соответствующей однородной систем. Свойства решений однородной системы уравнений.					
4.	Матрицы и определители Операции над матрицами и их свойства. Обратная матрица. Условие обратимости матрицы. Перестановки и подстановки. Определение определителя. Свойства определителя. Миноры и алгебраические дополнения. Разложение определителя по строке или столбцу. Определитель произведения матриц. Теорема о ранге матрицы.	36	20	10	10	16
5.	Векторные пространства Определение, примеры, простейшие свойства векторных пространств. Линейная зависимость векторов. Базис и ранг системы векторов. Конечномерные векторные пространства. Базис и размерность конечномерного пространства. Координаты вектора относительно данного базиса. Подпространство. Пересечение, сумма и прямая сумма подпространств. Связь между координатами векторов относительно различных базисов. Изоморфизм векторных пространств.	22	12	6	6	10
6.	Евклидовы пространства Скалярное произведение, евклидовы и унитарные пространства. Длина вектора и угол между векторами. Ортогональность. Процесс ортогонализации. Ортонормированный базис, его существование. Ортогональное дополнение к подпространству, свойства ортогонального дополнения. Изоморфизм евклидовых пространств.	22	12	6	6	10
7.	Линейные отображения и линейные операторы Понятия линейного отображения и оператора. Операции над линейными отображениями. Ранг, дефект, ядро и образ линейного отображения. Обратимые операторы. Изоморфизм	22	12	6	6	10

	алгебры операторов и полной матричной алгебры. Собственные числа и собственные векторы оператора, связь с матричными понятиями. Характеристический многочлен оператора. Теорема Гамильтона-Кэли для операторов.					
8.	Теория делимости целых чисел Отношение делимости. Теорема о делении с остатком. Систематическая запись натуральных чисел. НОД и НОК чисел. Взаимно простые числа. Простые числа и основная теорема арифметики. Бесконечность множества простых чисел. Каноническое разложение.	32	20	12	8	12
9.	Теория сравнений Числовые сравнения и их свойства. Классы вычетов. Полная и приведенная системы вычетов. Функция Эйлера. Теорема Эйлера. Сравнений первой степени. Диофантовы уравнения. Признаки делимости.	24	14	8	6	10
10.	Комплексные числа Определение поля комплексных чисел. Алгебраическая и тригонометрическая формы комплексного числа. Действия с комплексными числами в тригонометрической форме. Извлечение корней из комплексных чисел. Комплексно сопряженные числа.	26	14	8	6	12
11.	Многочлены от одной переменной Кольцо многочленов от одной переменной над коммутативным кольцом. Теорема Безу. Схема Горнера. Корни многочлена. Алгебраическое и функциональное равенство многочленов. Теорема о делении с остатком для многочленов над полем. Приводимые и неприводимые многочлены. Каноническое разложение многочлена над полем. Формальная производная. Формула Тейлора. Кольцо многочленов над факториальным кольцом.	28	16	10	6	12

12.	Многочлены от нескольких переменных Понятие многочлена от нескольких переменных. Степень многочлена. Лексикографическое упорядочение одночленов. Симметрические многочлены. Основная теорема теории симметрических многочленов.	19	9	6	3	10
13.	Многочлены над числовыми полями Алгебраическая замкнутость поля комплексных чисел. Разложение многочлена над полем комплексных чисел в произведение неприводимых множителей. Сопряженность мнимых корней многочлена с действительными коэффициентами. Разложение многочлена над полем действительных чисел в произведение неприводимых множителей. Рациональные корни многочлена с целыми коэффициентами. Критерий Эйзенштейна.	15	7	4	3	8
14.	Расширения полей Простое алгебраическое расширение поля и его строение. Конечное расширение поля. Алгебраическое расширение поля. Составное алгебраическое расширение поля. Поле алгебраических чисел и его алгебраическая замкнутость.	18	10	6	4	8
	ИТОГО	358	198	108	90	160

Тематический план курса «Избранные вопросы алгебры»

№	Наименование разделов и тем	Всего часов	В том числе аудиторных			СР
			Всего	Лек-ции	Пр. зан.	
15.	Элементы теории групп Теорема о факторизации. Алгебры и алгебраические системы. Изоморфизм алгебр. Примеры и простейшие свойства групп. Целые степени элемента группы. Порядок элемента. Циклические группы. Подгруппы. Теорема Кэли. Разложение группы по подгруппе. Теорема Лагранжа. Нормальные подгруппы. Фактор-группы. Гомоморфизмы и эпиморфизмы групп. Теорема об эпимоморфизмах.	40	22	10	12	18

16.	Кольца и поля Примеры и простейшие свойства колец и полей. Разность и частное, их свойства. Изоморфизм колец и полей. Подкольцо. Подполе. Характеристика кольца. Упорядоченные кольца и поля. Модуль элемента. Свойства порядка натуральных, целых и рациональных чисел: дискретность $\boldsymbol{N}$ и $\boldsymbol{Z}$, неограниченность $\boldsymbol{N}$, $\boldsymbol{Z}$ и $\boldsymbol{Q}$ в $\boldsymbol{R}$. принцип Архимеда. Идеалы колец. Сравнение по идеалу. Фактор-кольца. Кольца классов вычетов. Гомоморфизмы и эпиморфизмы колец. Теорема об эпиморфизмах.	66	34	16	18	32
17.	Элементы теории делимости в целостных кольцах Отношение делимости в целостных кольцах. Ассоциированность элементов. Разложение на простые множители. Факториальные кольца (кольца с однозначным разложением), кольца с неоднозначным разложением, кольца без разложения. Кольца главных идеалов. Евклидовы кольца.	29	13	7	6	16
18.	Поле частных целостного кольца Определение и строение поля частных. Изоморфизм полей частных. Теорема о существовании поля частных целостного кольца.	9	3	3	0	6
	Итого	144	72	36	36	72

Перечень практических занятий

Перечень заданий, как правило, избыточен, поэтому преподавателю предоставляется право выбирать задания.

1 семестр

Занятие 1. Операции над множествами. Свойства включения.
[5]: 1.3.1, 1.3.2, 1.3.5, 1.3.9, 1.4.8 – 1.4.10, 1.4.17 – 1.4.20.
[8]: ИЗ 1.

Занятие 2. Высказывания и предикаты.
[5]: 1.1.1, 1.1.6 – 1.1.9, 1.1.12, 1.1.18 – 1.1.21.
[8]: ИЗ 2 – ИЗ 5.

Занятие 3. Бинарные отношения. Отношения эквивалентности и порядка.
[5]: 1.5.17 – 1.5.19, 1.5.26; 1.7.1, 1.7.9, 1.7.14, 1.7.15; 1.8.1 – 1.8.3, 1.8.8.
[8]: ИЗ 8 – ИЗ 10, ГЗ 2.

Занятие 4. Функции и отображения.

[5]: 1.6.1, 1.6.3, 1.6.6, 1.6.7, 1.6.19 – 1.6.21, 1.6.23.
[8]: ГЗ 3.

Занятие 5. Метод математической индукции. Делимость целых чисел, деление с остатком.
[5]: 2.5.16, 2.5.20, 2.5.24 – 2.5.27; 8.8.16.
[8]: ИЗ 12, ИЗ 47.

Занятие 6. Определение и свойства групп.
[5]: 2.1.1, 2.1.2 а) – б), 2.1.6, 2.1.7, 2.1.13.
[8]: ИЗ 23.

Занятие 7. Определение и свойства колец и полей.
[5]: 2.4.1, 2.4.34, 2.4.38 а) – в), 2.4.55.
[8]: ИЗ 28.

Занятие 8. Подалгебры и изоморфизм алгебр.
[5]: 2.2.3, 2.2.4, 2.4.39, 2.4.41, .4.43, 2.4.45; 2.2.6–2.2.7, 2.3.70, 2.4.69.
[8]: ИЗ 27.

Занятие 9. Решение систем линейных уравнений.
[6]: 693, 699, 692, 703, 704, 709.
[8]: ИЗ 13.

Занятие 10. Исследование систем линейных уравнений.
[6]: 712, 714 – 717.
[8]: ИЗ 14.

Занятие 11. Линейно зависимые и линейно независимые системы векторов.
[5]: 4.1.7, 4.1.8.
[6]: 642 – 644.
[8]: ИЗ 16.

Занятие 12. Базис и ранг системы векторов.
[5]: 4.2.6, 4.2.10 – 4.2.14.
[6]: 673 – 676, 679 – 681.
[8]: ИЗ 17.

Занятие 13. Фундаментальная система решений однородной системы линейных уравнений. Многообразие решений системы линейных уравнений.
[6]: 737 – 741, 724 – 727.
[8]: ИЗ 15.

Занятие 14. Операции над матрицами.
[6]: 790 – 792, 804, 809, 827, 828, 815, 824.
[8]: ИЗ 18.

Занятие 15. Обратная матрица. Матричные уравнения.
[6]: 840 – 843, 876, 865 – 867, 869.

[8]: ИЗ 19.

Занятие 16. Определение и свойства определителя.
[6]: 188, 198, 200, 204, 205, 212.
[8]: ИЗ 20 – ИЗ 21, ГЗ 5.

Занятие 17. Вычисление определителей.
[6]: 44 – 47, 236, 260 – 263.
[8]: ИЗ 20, ГЗ 6.

Занятие 18. Теорема Крамера. Определитель произведения матриц.
[6]: 554 – 558.
[7]: 374, 375.
[8]: ИЗ 22.

2 семестр

Занятие 1. Примеры векторных пространств. Линейно зависимые и линейно независимые системы векторов. Размерность конечномерных векторных пространств.
[5]: 6.1.6, 6.1.10 – 6.1.12.
[6]: 1289 – 1293, 1297 – 1300, 1308, 1310, 1311.
[8]: ИЗ 36 – ИЗ 37.

Занятие 2. Подпространства. Пересечение и сумма подпространств.
[6]: 1317, 1318, 1320 – 1322.
[7]: 235.
[8]: ИЗ 39.

Занятие 3. Координаты вектора в разных базисах.
[5]: 6.5.1, 6.5.4, 6.5.6, 6.5.7.
[6]: 1277 – 1281.
[8]: ИЗ 38.

Занятие 4. Определение, примеры, свойства евклидовых пространств.
[5]: 6.6.4, 6.6.5, 6.6.10 – 6.6.12.
[8]: ИЗ 40.

Занятие 5. Длина вектора, угол между векторами. Ортогональная проекция вектора на подпространство.
[6]: 1366 – 1368, 1370 – 1372, 1385.
[7]: 1077 – 1079.
[8]: ИЗ 42.

Занятие 6. Процесс ортогонализации системы векторов.
[6]: 1361 – 1363, 1357, 1358.
[8]: ИЗ 41.

Занятие 7. Примеры линейных отображений. Матрица линейного отображения в разных базисах.

[6]: 1441 – 1444, 1448 – 1450, 1445, 1453, 1457, 1458.
[8]: ИЗ 43 – ИЗ 44.

Занятие 8. Ранг, дефект, ядро и образ линейного отображения.
[5]: 7.1.2, 7.1.11.
[7]: 966.
[8]: ИЗ 45.
На примере $V = \boldsymbol{R}[x]$, $\varphi: f \mapsto f'$, $\psi: f \mapsto xf$ убедиться, что для бесконечномерных векторных пространств теорема 7.4.1 неверна.

Занятие 9. Собственные векторы и собственные значения линейного оператора. Приведение матрицы к диагональному виду.
[6]: 1479 – 1481.
[8]: ИЗ 46, ГЗ 18.

3 семестр

Занятие 1. Систематические числа. Перевод из одной системы счисления в другую.
[12]: С.49, №№ 20 – 25.
[8]: ИЗ 48 – ИЗ 49.

Занятие 2. Делимость целых чисел. НОД и НОК.
[8]: ИЗ 47, ИЗ 51, ГЗ 27 – ГЗ 28АБ.

Занятие 3. Взаимно простые числа.
[8]: ГЗ 28 Б, ИЗ 50, ИЗ 54.

Занятие 4. Простые числа. Основная теорема арифметики. Применения числовых сравнений в арифметике.
[12]: С.27, №№ 19, 20, 22.
[8]: ГЗ 28ВГД – ГЗ 30.

Занятия 5 – 6. Функция Эйлера. Числовые сравнения.
[12]: С.122, №№ 16 – 19, 24 – 26, 30 – 32.
[8]: ИЗ 56, ИЗ 57.

Занятие 7. Сравнения первой степени и неопределённые уравнения первой степени.
[12]: С.138, №№ 18, 20, 24, 25, 17, 27.
[8]: ИЗ 58, ИЗ 61.

Занятие 8. Операции над комплексными числами в алгебраической форме.
[7]: 107 с), 108 а), 113.
[17]: 443, 454, 461, 462, 469.
[8]: ИЗ 34.

Занятие 9. Геометрическое изображение комплексных чисел. Тригонометрическая форма комплексного числа.
[7]: 124, 125, 135, 137, 141.

[17]: 501 – 503, 515, 517.
[8]: ИЗ 32 – ИЗ 33.

Занятие 10. Корни из комплексных чисел. Комплексно сопряжённые числа.
[7]: 143.
[17]: 529, 532.
[8]: ИЗ 35.

Занятие 11. Определение многочлена. Схема Горнера. Корни многочлена.
[7]: 599 – 605, 51, 555, 586.
[17]: 560 – 564, 572 – 579, 582, 588.
См. Приложение 2.1°.
[8]: ИЗ 69, ИЗ 71.

Занятие 12. Деление многочленов с остатком. НОД и НОК многочленов.
[7]: 580.
[17]: 601, 605 – 607, 611.
[8]: ИЗ

Занятие 13. Разложение многочлена над полем на неприводимые множители.
[17]: 675, 678.
[8]: ГЗ 37.

Занятие 14. Симметрические многочлены.
[7]: 693, 695, 697.
[17]: 756, 757.
[8]: ИЗ 76.

Занятие 15. Рациональные корни многочлена. Многочлены над ***C*** и ***R***.
[7]: 650, 592.
[17]: 675, 678.
[8]: ИЗ 72, ИЗ 74, ИЗ 75.

Занятие 16. Формулы Виета. Применения симметрических многочленов.
[7]: 614 – 617, 700 – 702.
[17]: 763 – 765.
[8]: ИЗ

Занятие 17. Освобождение от алгебраической иррациональности в знаменателе дроби.
[7]: 684.
[17]: 773.
[8]: ИЗ 78.

Занятие 18. Алгебраические числа.
[8]: ИЗ 79 – ИЗ 82.

4 семестр

Занятие 1. Примеры групп. Группы подстановок.

[5]: 8.1.17, 8.1.18.
[6]: 1634 16), 1634 21), 1634 26), 1635, 1636, 1651
[8]: ГЗ 7 А.

Занятие 2. Подгруппы. Операции над подгруппами.
[5]: 8.1.19, 8.1.20.
[6]: 1650, 1652.
[8]: ГЗ 7 В, ГЗ 8.

Занятие 3. Порядок элемента группы. Циклические группы.
[5]: 8.2.1, 8.2.2; 8.2.5, 8.2.6, 8.2.8, 8.2.10; 8.2.27, 8.2.28, 8.2.33, 8.2.46.
[6]: 1646, 1656.
[8]: ГЗ 7 Б, ИЗ 25.

Занятие 4. Теорема Кэли. Теорема Лагранжа.
[6]: 1637, 1645.
[8]: ГЗ 7 Д.

Занятие 5. Разложение группы по подгруппе. Фактор-группы.
[5]: 8.3.24, 8.3.25, 8.3.31, 8.3.32.
[6]: 1659, 1660, 1663; 1670; 1685.
[8]: ГЗ 10 АБВГ, ИЗ 24.

Занятие 6. Изоморфизм групп. Теорема об эпиморфизмах.
[5]: 8.2.45; 8.2.55 – 8.2.57; 8.2.61, 8.3.37, 8.3.38; 8.3.42, 8.3.43.
[6]: 1642, 1653; 1681, 1682; 1687; 1688, 1689.
[8]: ГЗ 7 Г, ГЗ 9, ГЗ 10 Д, ИЗ 26, ИЗ 27.

Занятие 7. Примеры и свойства колец и полей.
[5]: 8.4.6, 8.4.7, 8.4.10; 8.4.4.
[6]: 1732, 1733, 1738.
[8]: ГЗ 20.

Занятие 8. Свойства разностей и частных.
План-конспект курса, Т. 16.1.3 и Т. 16.1.7.
[8]: ИЗ 28

Занятие 9. Подкольца. Подполя.
[5]: 8.4.3.
[8]: ИЗ

Занятие 10. Свойства упорядоченных колец и полей.
План-конспект курса, Т. 16.4.3 – 16.4.5.
[8]: ГЗ 25, ИЗ 28.

Занятие 11. Доказательство числовых неравенств.
См. Приложение 2.2°.

Занятие 12. <u>Свойства дискретности ***N*** и ***Z***</u>.
См. приложение 2.3°.

Занятие 13. <u>Идеалы. Операции над идеалами</u>.
[5]: 8.5.1, 8.5.3, 8.5.6, 8.5.8.
[6]: 1781; 1794 – 1796.
[8]: ИЗ 55.

Занятие 14. <u>Фактор-кольца. Кольца классов вычетов</u>.
[5]: 8.5.35, 8.5.36, 8.5.40, 8.5.41, 8.5.54.
[6]: 1792, 1793.

Занятие 15. <u>Изоморфизм и эпиморфизм колец</u>.
[5]: 8.5.55, 8.5.56.
[6]: 1745, 1746, 1749, 1751 – 1753, 1790.
[8]: ГЗ 22, ГЗ 23.

Занятие 16. <u>Делимость в кольцах</u>.
[6]: 1774.
[12]: С.72, №№ 4, 5, 7, 15, 17.
[8]: ГЗ 20.

Занятие 17. <u>Кольца главных идеалов</u>.
[5]: 8.8.10 – 8.8.13.
[12]: С. 85, №№ 3; 8, 10, 19, 21.
[8]: ИЗ 55.

Занятие 18. <u>Евклидовы кольца</u>.
[5]: 8.8.17, 8.8.18; 8.8.20, 8.8.22.
[8]: ГЗ 31, ИЗ 52, ИЗ 53.

Тематика контрольных работ

Мы являемся сторонниками “непрерывных” контрольных работ, когда каждое практическое занятие сопровождается домашним заданием, в котором каждый студент получает индивидуальное задание на отработку стандартного материала, изучаемого на данном занятии: отработку определения или решение задачи алгоритмического характера. Эти задания мы берём из сборника индивидуальных заданий (далее – ИЗ) задачника [8].

Для приверженцев традиционных форм контроль укажем перечень заданий контрольных работ, материал для которых также берётся из [8].

Контрольные работы по курсу алгебры и теории чисел

Контрольная работа № 1

1. Выяснить, являются ли формулы логически истинными – ИЗ 4–5.
2. Указать свойства бинарных отношений – ИЗ 8.
3. Выяснить, является ли группой алгебра – ИЗ 24.
4. Доказать утверждение, используя метод математической индукции – ИЗ 12.
5. Поделить с остатком в $\boldsymbol{Z}$ – ИЗ 47.

Контрольная работа № 2

1. Решить систему линейных уравнений – ИЗ 13.
2. Выяснить линейную зависимость системы векторов – ИЗ 16.
3. Выполнить умножение матриц – ИЗ 18.
4. Вычислить матрицу, обратную для данной – ИЗ 19.
5. Вычислить значение определителя – ИЗ 20.

Контрольная работа № 3

1. Выяснить, является ли векторным пространством данное множество – ИЗ 36.
2. Выяснить, образуют ли векторы a_1, a_2, a_3 базис векторного пространства. Если образуют, то найти координаты вектора x в этом базисе – ИЗ 38.
3. Найти базисы и размерности подпространств U_1+U_2 и U_1 U_2, если $U_1 = L(a_1, a_2, a_3)$, $U_2 = L(b_1, b_2, b_3)$ – ИЗ 39.
4. Выяснить, задаёт ли правило a b = ... скалярное произведение на $\boldsymbol{R}^3$, если $a = (\alpha_1, \alpha_2, \alpha_3)$, $b = (\beta_1, \beta_2, \beta_3)$ – ИЗ 40.
5. Построить ортогональный базис подпространства $L(a_1, a_2, a_3)$ – ИЗ 41.

Контрольная работа № 4

1. Выяснить, является ли линейным отображением заданная функция. Если является, то найти её матрицу в стандартном базисе – ИЗ 43.
2. Найти матрицу линейного отображения в новом базисе – ИЗ 44.
3. Найти ранг, дефект, ядро и образ линейного оператора – ИЗ 45.
4. Существует ли базис, в котором данный линейный оператор имеет диагональную матрицу? Если существует, то найти этот базис и вид диагональной матрицы.

Контрольная работа № 5

1. Найти НОД и НОК чисел и представить НОД в виде линейной комбинации данных чисел – ИЗ 51.
2. Записать данное число в новой системе счисления – ИЗ 49.
3. С помощью сравнений найти остаток от деления – ИЗ 56.
4. Решить сравнение первой степени – ИЗ 58.
5. Выполнить действия над комплексными числами – ИЗ 35.

Контрольная работа № 6

1. Разложить многочлен по степеням $x–\alpha$ – ИЗ 71.
2. Разложить на неприводимые множители над $\boldsymbol{Q}$, $\boldsymbol{R}$ и $\boldsymbol{C}$ – ИЗ 74.
3. Известно, что α является корнем данного многочлена. Найти все остальные корни многочлена и разложить его на неприводимые множители над $\boldsymbol{Q}$, $\boldsymbol{R}$ и $\boldsymbol{C}$ – ИЗ 75.
4. Выразить симметрический многочлен через элементарные симметрические – ИЗ 76.
5. Освободиться от иррациональности в знаменателе дроби – ИЗ 78.

Контрольные работы по курсу «Избранные вопросы алгебры»

Контрольная работа № 1

1. Доказать, что подмножество H является подгруппой данной группы. Описать строение смежных классов группы по подгруппе H – ИЗ 24.
2. Составить таблицу Кэли для циклической группы данного порядка n. Существуют ли в группе подгруппы порядка n_1, n_2? Если существует, то составить таблицу Кэли для неё и для её фактор-группы – ИЗ 25.
3. Функция f отображает одну группу в другую. Является ли эта функция гомоморфизмом? Если является, то найти её ядро – ИЗ 26.
4. Доказать, что данные алгебры не изоморфны – ИЗ 27.
5. Доказать свойства колец и упорядоченных колец – ИЗ 28–29.

Контрольная работа № 2

1. Составить таблицы сложения и умножения в данном $\boldsymbol{Z}_m$. Используя таблицы, выяснить, является ли данное кольцо классов вычетов полем.
2. Сократима ли дробь? Если сократима, то на какое число – ИЗ 54.
3. Найти порождающие элементы идеалов $(a)+(b)$ и (a) (b) и провести подробное доказательство – ИЗ 55.
4. Поделить с остатком a на b в кольце $\boldsymbol{Z}[i]$ – ИЗ 52.
5. Простым или составным является данный элемент кольца $\boldsymbol{Z}[i]$ – ИЗ 53.

Критерии оценок знаний

Оценка «отлично» ставится при условии выполнения аудиторных контрольных работ, всех индивидуальных заданий и отчетностей, полном ответе на экзамене по билету.

Оценка «хорошо» ставится при тех же условиях и ответе на экзаменационный билет с 1–2 замечаниями непринципиального характера.

Оценка «удовлетворительно» ставится, если промежуточные отчетности и индивидуальные задания в течение семестра были выполнены с некоторыми замечаниями, а ответ на экзамене имеет существенные недостатки, при этом одна из двух задач решена правильно и основные определения теории усвоены.

Перечень основных знаний, умений и навыков

В результате изучения дисциплины студент должен

– *знать* основные понятия алгебры и теории чисел, приводить примеры, иллюстрирующие эти понятия, уметь доказывать основные теоремы данного курса;

– *знать* определения основных алгебраических структур: группы, кольца, поля, векторного пространства, линейной алгебры (в узком смысле), упорядоченного кольца и поля, определения соответствующих подструктур и морфизмов данных структур;

– *знать* основные факты теории многочленов, в том числе – многочленов над основными числовыми полями;

– *уметь* свободно решать системы линейных уравнений методом последовательного исключения неизвестных и с помощью теоремы Крамера; *уметь* исследовать систему векторов на линейную зависимость, находить базис и ранг системы векторов, базис и размерность векторных пространств и их подпространств, осуществлять процесс ортогонализации системы векторов;

– *уметь* выполнять операции над матрицами и находить различными способами матрицу, обратную данной, применять полученные умения для решения прикладных задач, в частности, для решения матричных уравнений и систем линейных уравнений, уметь вычислять определители матриц;

– *уметь* находить матрицы перехода от одного базиса к другому и решать задачи по нахождению координат вектора относительно данного базиса, определять, является ли данное отображение линейным, находить его матрицу относительно различных базисов, а также его собственные векторы и собственные значения, приводить матрицу линейного оператора к диагональному виду;

– *уметь* разлагать натуральные числа на простые множители, вычислять НОД и НОК чисел, владеть навыками использования важнейших методов теории делимости, в том числе – и на языке теории сравнений;

– *уметь* применять аппарат комплексных чисел к решению разнообразных задач алгебры;

– *уметь* использовать результаты теории многочленов для решения прикладных задач, в частности, при отыскании интерполяционных многочленов или при разложении выражений на множители (теорема о числе корней многочлена) и т.п.

Рекомендации по организации самостоятельной работы студентов

При изучении данного курса можно пользоваться любым учебным пособием по алгебре для студентов математических факультетов университетов и педагогических вузов. В списке литературы указаны некоторые из них, наиболее соответствующие содержанию курса и уровню математической подготовки аудитории.

Учебник Л.Я. Куликова [3] полностью соответствует программе, но написан довольно сложным языком. Учебное пособие Д.К. Фаддеева [4] написано менее формально. Одним из его достоинств является удобный для первого знакомства порядок следования разделов, при котором происходит плавный переход от рассмотрения конкретных объектов к более абстрактным понятиям. Не потерял своей актуальности и классический учебник А.Г. Куроша [14]. Более современное изложение алгебры, содержащее материал, выходящий за рамки данного курса, можно найти у А.И. Кострикина [2]. При изучении теории делимости и сравнений целых чисел рекомендуем использовать лаконичный классический учебник И.М. Виноградова [1].

Для первоначального знакомства мы рекомендуем также использовать серию пособий [9]–[12], где стиль изложения менее формальный. Изложение сопровождается большим количеством пояснений, отступлений, иллюстрирующих примеров.

Перечислим по разделам привязку материала к учебникам.

1. Элементы теории множеств, математической логики, числовых систем – [3], [9].
2. Основные алгебраические структуры – [3], [9], [10].
3. Системы линейных уравнений. Арифметическое n-мерное векторное пространство – [3], [9].
4. Матрицы и определители – [3], [9].
5. Векторные пространства – [3], [10].
6. Евклидовы пространства – [3], [10].
7. Линейные отображения и линейные операторы – [3], [10].
8. Теория делимости целых чисел – [1], [12].
9. Теория сравнений – [1], [12].
10. Комплексные числа – [3], [4], [14].
11. Многочлены от одной переменной – [3], [11].
12. Многочлены от нескольких переменных – [3], [11], [14].
13. Многочлены над числовыми полями – [3], [11], [14].
14. Расширения полей – [3], [11].
15. Элементы теории групп – [3], [10].
16. Кольца и поля – [3], [14], [12].
17. Элементы теории делимости в целостных кольцах – [3], [12].
18. Поле частных целостного кольца – [3], [12].

Рекомендуемая литература

Основная литература

1. *Виноградов И.М.* Основы теории чисел. М.: Наука, 1974.
2. *Кострикин А.И.* Введение в алгебру. М.: Наука, 1977.
3. *Куликов Л.Я.* Алгебра и теория чисел. М.: Высшая школа, 1979.
4. *Фаддеев Д.К.* Лекции по алгебре. М.: Наука, 1984.
5. *Куликов Л.Я.*, *Москаленко А.И.*, *Фомин А.А.* Сборник задач по алгебре и теории чисел. М.: Просвещение, 1993.
6. *Проскуряков И.В.* Сборник задач по линейной алгебре. М.: Наука, 1984.
7. *Фаддеев Д.К.*, *Соминский И.С.* Сборник задач по высшей алгебре. М.: Наука, 1977.
8. *Моисеев С.А.*, *Суворов Н.М.* Задачник-практикум по алгебре и теории чисел. Рязань: Изд-во РГУ, 2006.

Дополнительная литература

9. *Варпаховский Ф.Л.*, *Солодовников А.С.* Алгебра. Элементы теории множеств. Линейные уравнения и неравенства. Матрицы и определители. М.: Просвещение, 1974.
10. *Варпаховский Ф.Л.*, *Солодовников А.С.*, *Стеллецкий И.В.* Алгебра. Группы, кольца, поля. Векторные и евклидовы пространства. Линейные отображения. М.: Просвещение, 1978.
11. *Винберг Э.Б.* Алгебра многочленов. М.: Просвещение, 1980.
12. *Казачек Н.А.*, *Перлатов Г.Н.*, *Виленкин Н.Я.*, *Бородин А.И.* Алгебра и теория чисел. М.: Просвещение, 1984.
13. *Кострикин А.И.*, *Манин Ю.И.* Линейная алгебра и геометрия. М.: Наука, 1986.
14. *Курош А.Г.* Лекции по общей алгебре. М.: Наука, 1973.
15. *Мальцев А.И.* Основы линейной алгебры. М.: Наука, 1970.
16. *Постников М.М.* Теория Галуа. М.: Физматгиз, 1963.
17. *Окунев Л.Я.* Сборник задач по высшей алгебре. М.: Просвещение, 1964.
17\. Сборник задач по алгебре: Учебное пособие /Под ред. *А.И.Кострикина.* М.: Факториал, 1995.

План-конспект

курсов «Алгебра и теория чисел» и «Избранные вопросы алгебры»

План-конспект курса предназначен для создания целостного представления обо всём курсе, в нём наряду с подробным изложением содержания курса (здесь приведены формулировки всех утверждений, которые требуется доказать), сделаны указания по поводу их доказательства, часто указаны планы и идеи проведения доказательства.

ГЛАВА 1. Множества, логика, числа

§ 1. Множества, элементы, подмножества

Множества и элементы. $a \quad A$. Конечные и бесконечные множества. Способы задания множества. $\{a_1, a_2, ..., a_n\}$, $\{x \quad \varphi(x)\}$. $\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$, $\boldsymbol{R}_+$, $\boldsymbol{R}^*$.

Равенство и неравенство множеств. Подмножества. $A \quad B$. Пустое и универсальное множества. , U.

Теорема. Свойства включения.

1°. $A \quad A$.

2°. $A \quad B \; B \quad C \quad A \quad C$.

3°. $\quad A$, $A \quad$ U.

4°. $A \quad B \; B \quad A \quad A = B$.

5°. Пустое множество единственное.

§ 2. Операции над множествами

Пересечение, объединение, разность симметрическая разность двух множеств. Дополнение множества. , , \, ¯. Диаграммы Эйлера-Венна.

Теорема. Свойства операций.

1°. $A \quad A = A$;

2°. $A \quad B = B \quad A$;

1 . $A \quad A = A$;

2 . $A \quad B = B \quad A$;

3°. $(A \quad B) \quad C = A \quad (B \quad C)$;

4°. $A \quad (B \quad C) = (A \quad B) \quad (A \quad C)$;

5°. $A\backslash(B \quad C) = (A\backslash B) \quad (A\backslash C)$;

6°. $\overline{A \cap B} = \overline{A} \cup \overline{B}$;

7°. $A \quad (A \quad B) = A$;

8°. $A \quad \overline{A} = \quad$;

9°. $A \quad = \quad$, $A \quad \mathrm{U} = A$;

3 . $(A \quad B) \quad C = A \quad (B \quad C)$;

4 . $A \quad (B \quad C) = (A \quad B) \quad (A \quad C)$;

5 . $A\setminus(B \quad C) = (A\setminus B) \quad (A\setminus C)$;

6 . $\overline{A \cup B} = \overline{A} \cap \overline{B}$;

7 . $A \quad (A \quad B) = A$;

8 . $A \quad \overline{A} = \mathrm{U}$;

9 . $A \quad \mathrm{U} = \mathrm{U}, A \qquad = A$;

10°. $\overline{\overline{A}} = A$;

11°. $A \qquad B \qquad A \quad B = A \qquad A \quad B = B$;

§ 3. Декартово (прямое) произведение множеств. Бинарные отношения

Упорядоченная пара элементов. (a, b).

Основное свойство: $(a, b) = (c, d) \qquad a = c \quad b = d$.

Декартово произведение двух множеств. $A_1 \quad A_2$.

Упорядоченная n-ка элементов (кортеж длины n). $(a_1, a_2, ..., a_n)$. Декартово произведение n множеств. Декартов квадрат A^2 и декартова степень A^n.

Бинарные отношения. Проекции, график, граф бинарного отношения. Обратное бинарное отношение. $^{-1}$. Частные виды бинарных отношений. Всюду определённые, сюръективные, функциональные, инъективные, биективные бинарные отношения.

Рефлексивные, антирефлексивные, симметричные, асимметричные, антисимметричные, транзитивные, линейные (= связные) бинарные отношения. Диагональное и универсальное отношения.

§ 4. Отношения эквивалентности. Отношения порядка

Отношения эквивалентности. Разбиения. Класс эквивалентности, порождённый элементом a. K_a или $\overline{a}$.

<u>Теорема об эквивалентности</u>.

1°. Всякое отношение эквивалентности на множестве A порождает разбиение этого множества классами эквивалентности.

2°. Всякое разбиение $\{A_i\}$ множества A порождает отношение эквивалентности на этом множестве: отношение $\rho = \{(x, y) | x, y \quad A_i$ для некоторого A_i из разбиения$\}$ является отношением эквивалентности, причём классы эквивалентности по ρ совпадают с подмножествами A_i разбиения.

Граф отношения эквивалентности. Фактор-множество A/ρ.

Отношения порядка. Отношения строгого порядка. Отношения нестрогого порядка. Отношения линейного (строгого или нестрогого) порядка. Упорядоченные множества. Важнейшие примеры упорядоченных множеств: числовые множества, булеан с отношением включения, множество натуральных чисел с отношением делимости.

*→ Наибольший и наименьший элементы. Максимальный и минимальный

элементы. Верхняя и нижняя границы подмножества, верхняя и нижняя грани (sup и inf) подмножества.←*

§ 5. Функции

Функции как упорядоченные тройки. Равенство двух функций. Область отправления, область прибытия, график функции. Область определения и множество значений функции. $f\colon A \to B$. $f\colon a \mapsto b$. D(f). E(f). Функция = всюду определённая функция. Инъекция, сюръекция, биекция. Тождественное отображение. ε_A.

Теорема 1. Критерий обратимости функции.

Если f – функция, то отношение f^{-1} является функцией тогда и только тогда, когда f – биекция.

Композиция функций. $g\circ f$.

Теорема 2. Свойства композиции функций.

1°. Композиция не коммутативна.

2°. Композиция ассоциативна.

3°. Если $f\colon A \to B$, то $f\circ\varepsilon_A = \varepsilon_B\circ f = f$.

4°. Если $f\colon A \to B$ – биекция, то $f^{-1}\circ f = \varepsilon_A$, $f\circ f^{-1} = \varepsilon_B$.

5°. Если $f\colon A \to B$, $g\colon B \to A$ и $g\circ f = \varepsilon_A$, $f\circ g = \varepsilon_B$, то f – биекция и $f^{-1} = g$.

6°. Если f – биекция, то f^{-1} – также биекция, причём $(f^{-1})^{-1} = f$.

7°. Если $f\colon A \to B$ и $g\colon B \to C$ – биекции, то $g\circ f$ – биекция и $(g\circ f)^{-1} = f^{-1}\circ g^{-1}$.

Образ и полный прообраз множества.

§ 6. Высказывания и предикаты. Логические операции. Формулы

Высказывания. Предикаты. Область истинности предиката. Связь между n-местными отношениями и n-местными предикатами. Логические операции: отрицание, конъюнкция, дизъюнкция, импликация, эквиваленция. Истинностные значения сложных высказываний и предикатов. Кванторы всеобщности и существования. Геометрическая интерпретация для операций навешивания кванторов. Связь с операциями над множествами. Формулы логики высказываний. Формулы логики предикатов. Порядок выполнения операций. Тождественно истинные высказывания (= тавтологии) и тождественно истинные (= общезначимые) формулы логики предикатов.

§ 7. Отношения следования и равносильности

Отношения следования и равносильности. . .

Теорема 1. Первые свойства отношений следования и равносильности.

1°. Отношение следования рефлексивно и транзитивно.

2°. Отношение равносильности является отношением эквивалентности.

3°. φ ψ тогда и только тогда, когда формула $\varphi \to \psi$ является общезначимой (тавтологией в случае высказываний).

4°. $\varphi \quad \psi$ тогда и только тогда, когда формула $\varphi \leftrightarrow \psi$ является общезначимой (тавтологией в случае высказываний).

Теорема 2. Основные равносильности логики высказываний.

1°. $\overline{\overline{\varphi}} \quad \varphi$.

2°. $\varphi \ \varphi \quad \varphi$.

3°. $\varphi \ \psi \quad \psi \ \varphi$.

4°. $(\varphi \ \psi) \ \chi \quad \varphi \ (\psi \ \chi)$.

5°. $\varphi \ (\psi \ \chi) \quad (\varphi \ \psi) \ (\varphi \ \chi)$.

6°. $\overline{\varphi \wedge \psi} \quad \overline{\varphi} \vee \overline{\psi}$.

7°. $\varphi \ (\varphi \ \psi) \quad \varphi$.

8°. $\varphi \ \overline{\varphi} \quad \mathbf{0}$.

9°. $\mathbf{0} \ \varphi \quad \mathbf{0}$, $\mathbf{1} \ \varphi \quad \varphi$.

2 . $\varphi \ \varphi \quad \varphi$.

3 . $\varphi \ \psi \quad \psi \ \varphi$.

4 . $(\varphi \ \psi) \ \chi \quad \varphi \ (\psi \ \chi)$.

5 . $\varphi \ (\psi \ \chi) \quad (\varphi \ \psi) \ (\varphi \ \chi)$.

6 . $\overline{\varphi \vee \psi} \quad \overline{\varphi} \wedge \overline{\psi}$.

7 . $\varphi \ (\varphi \ \psi) \quad \varphi$.

8 . $\varphi \ \overline{\varphi} \quad \mathbf{1}$.

9 . $\mathbf{1} \ \varphi \quad \mathbf{1}$, $\mathbf{0} \ \varphi \quad \varphi$.

10°. $\varphi \to \psi \quad \overline{\varphi} \ \psi$.

11°. $\overline{\varphi \to \psi} \quad \varphi \wedge \overline{\psi}$.

12°. $\varphi \leftrightarrow \psi \quad (\varphi \to \psi) \ (\psi \to \varphi)$.

13°. $\varphi \to \psi \quad \overline{\psi} \to \overline{\varphi} \quad \varphi \ \overline{\psi} \to \mathbf{0}$.

Теорема 3. Основные следствия и равносильности логики предикатов.

1°. $(\forall\alpha)\varphi \quad \varphi, \quad \varphi \quad (\exists\alpha)\varphi$.

2°. $\overline{(\exists\alpha)\varphi} \quad (\forall\alpha)\overline{\varphi}$.

3°. $\overline{(\forall\alpha)\varphi} \quad (\exists\alpha)\overline{\varphi}$.

4°. $(\forall\alpha)(\forall\beta)\varphi \quad (\forall\beta)(\forall\alpha)\varphi$.

5°. $(\exists\alpha)(\exists\beta)\varphi \quad (\exists\beta)(\exists\alpha)\varphi$.

6°. $(\exists\alpha)(\forall\beta)\varphi \quad (\forall\beta)(\exists\alpha)\varphi$.

$(\exists\alpha)\varphi \quad (\forall\alpha)\psi$

7°. $(\forall\alpha)\varphi \quad (\forall\alpha)\psi \qquad (\forall\alpha)(\varphi \quad \psi) \qquad\qquad (\exists\alpha)(\varphi \quad \psi) \qquad (\exists\alpha)\varphi \quad (\exists\alpha)\psi$.

$(\forall\alpha)\varphi \quad (\exists\alpha)\psi$

$(\exists\alpha)\varphi \quad (\forall\alpha)\psi$

8°. $(\forall\alpha)(\varphi \quad \psi) \qquad (\forall\alpha)\varphi \quad (\forall\alpha)\psi \qquad\qquad (\exists\alpha)(\varphi \quad \psi) \qquad (\exists\alpha)\varphi \quad (\exists\alpha)\psi$.

$(\forall\alpha)\varphi \quad (\exists\alpha)\psi$

$(\forall\alpha)\varphi\to(\forall\alpha)\psi$

9°. $(\exists\alpha)\varphi\to(\forall\alpha)\psi \qquad (\forall\alpha)(\varphi\to\psi) \qquad\qquad (\forall\alpha)\varphi\to(\exists\alpha)\psi \qquad (\exists\alpha)(\varphi\to\psi)$.

$(\exists\alpha)\varphi\to(\exists\alpha)\psi$

$(\forall\alpha)\varphi\leftrightarrow(\forall\alpha)\psi \qquad\qquad (\exists\alpha)\varphi\leftrightarrow(\forall\alpha)\psi$

10°. $(\forall\alpha)(\varphi\leftrightarrow\psi) \qquad\qquad (\exists\alpha)(\varphi\leftrightarrow\psi)$.

$(\exists\alpha)\varphi\leftrightarrow(\exists\alpha)\psi \qquad\qquad (\forall\alpha)\varphi\leftrightarrow(\exists\alpha)\psi$

Прямое, обратное, противоположное, обратное противоположному (= противоположное обратному) утверждения. Необходимое и достаточное условия.

§ 8. Определение системы действительных чисел

Аксиомы системы действительных чисел. ***R***. Группы аксиом A, M, AM, O, OA, OM, C.

Важнейшие свойства операций. Разность и частное.

Важнейшие свойства порядка. Свойство трихотомии. Неотрицательность квадрата.

§ 9. Система натуральных чисел. Принцип математической индукции

Индуктивные множества. ***N***.

Теорема 1. Первые свойства ***N***.

1°. $1 \quad \boldsymbol{N}$.

2°. $(\forall n)(n \quad \boldsymbol{N} \to n+1 \quad \boldsymbol{N})$/

3°. (ПМИ) $(M \quad \boldsymbol{N}) \quad (1 \quad \boldsymbol{N}) \quad (\forall n)(n \quad \boldsymbol{N} \to n+1 \quad \boldsymbol{N}) \qquad M \quad \boldsymbol{N}$.

Метод математической индукции. Обоснование ММИ. База индукции. Шаг индукции.

Разновидности метода математической индукции. Возвратная индукция. Примеры доказательства методом математической индукции.

Теорема 2. Свойства операций в ***N***.

1°. Сумма любых двух натуральных чисел является натуральным числом.

2°. Произведение любых двух натуральных чисел является натуральным числом.

Дискретность ***N***. Принцип наименьшего числа. Неограниченность ***N*** в ***R***.

§ 10. Системы целых и рациональных чисел

Определения целого и рационального чисел. $\boldsymbol{Z}$. $\boldsymbol{Q}$.

Теорема 1. Свойства операций в $\boldsymbol{Z}$.

Множество целых чисел замкнуто относительно операций сложения, вычитания и умножения.

Дискретность $\boldsymbol{Z}$. Неограниченность $\boldsymbol{Z}$ в $\boldsymbol{R}$. Целая часть числа.

Теорема 2. Свойства операций в $\boldsymbol{Q}$.

Множество рациональных чисел замкнуто относительно операций сложения, вычитания, умножения и деления на ненулевое число.

Свойство плотности $\boldsymbol{Q}$. Плотность $\boldsymbol{Q}$ в $\boldsymbol{R}$.

ГЛАВА 2. Основные алгебраические структуры

§ 1. Алгебраические операции. Алгебры. Алгебраические системы. Группы

Понятия бинарной и n-местной алгебраической операции. Алгебры. Алгебраические системы.

Некоторые свойства бинарных операций: коммутативность, ассоциативность, нейтральные элементы, аннулирующие элементы, обратные элементы, обратимость операции; дистрибутивности. Полугруппы. Квазигруппы. Лупы.

Два определения группы.

Теорема 1. Определения группы эквивалентны.

Примеры групп.

1. Группы чисел по сложению: $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$, $2\boldsymbol{Z}$.
2. Группы чисел по умножению: $\boldsymbol{Q}^*$, $\boldsymbol{R}^*$, $\boldsymbol{R}^*_+$.
3. Группа $P(M)$ всех биективных преобразований некоторого множества M.

Теорема 2. Простейшие свойства групп.

1°. В группе нейтральный элемент единственный.

2°. В группе обратный для данного элемент единственный.

3°. $(a^{-1})^{-1} = a$.

4°. $(ab)^{-1} = b^{-1}a^{-1}$.

Мультипликативная и аддитивная записи и терминология.

Изоморфизмы групп.

Теорема 3. Свойства изоморфизма групп.

1°. Тождественное отображение группы является изоморфизмом.

2°. Отображение, обратное изоморфизму, является изоморфизмом групп.

3°. Композиция двух изоморфизмов является изоморфизмом.

Отношение изоморфизма. ≅.

<u>Теорема 4</u>. Отношение изоморфизма в классе групп является отношением эквивалентности.

§ 2. Подгруппы

Определение и примеры подгрупп.

<u>Теорема 1</u>. Первый критерий подгруппы.

Пусть G; – группа, H G. Тогда H является подгруппой группы H, если и только если одновременно выполняются следующие три условия:

1) H ; 2) h_1, h_2 H h_1 h_2 H; 3) h H h^{-1} H.

<u>Теорема 2</u>. Второй критерий подгруппы.

Пусть G; – группа, H G. Тогда H является подгруппой группы H, если и только если одновременно выполняются следующие два условия:

1) H ; 2) h_1, h_2 H h_1 h_2^{-1} H.

§ 3. Кольца и поля

Примеры колец: $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{R}[x]$,

Нулевой и единичный элементы, противоположный и обратный элементы.

<u>Теорема 1</u>. Свойства противоположных и обратных.

1°. В кольце нуль и единица единственные.

2°. В кольце каждый элемент имеет единственный противоположный; в поле каждый ненулевой элемент имеет единственный обратный.

3°. В кольце: $-0 = 0$; в поле: $1^{-1} = 1$.

4°. $-(a+b) = (-a)+(-b)$; $(ab)^{-1} = a^{-1}b^{-1}$.

5°. $-(-a) = a$; $(a^{-1})^{-1} = a$.

<u>Теорема 2</u>. О расщеплении.

1°. В кольце $(\forall a)(\forall b)(\exists! c)(b+c = a)$.

2°. В поле $(\forall a)(\forall b$ $0)(\exists! c)(b$ $c = a)$.

Разность и частное: $a-b$, $\dfrac{a}{b}$.

Изоморфизм колец и полей. Отношение изоморфизма ≅.

Теорема 3. Свойства изоморфизма колец и полей.

1°. Тождественное отображение является изоморфизмом.

2°. Отображение, обратное изоморфизму, является изоморфизмом.

3°. Композиция двух изоморфизмов является изоморфизмом.

4°. Отношение изоморфизма является отношением эквивалентности.

§ 4. Подкольца и подполя

Определение и примеры подколец и подполей.

Теорема 1. Первый критерий подкольца.

Пусть A; +, – кольцо, B A. Тогда B является подкольцом кольца A, если и только если одновременно выполняются следующие четыре условия:

1) B ; 2) a_1, a_2 B a_1+a_2 B; 3) a B $-a$ B; 4) a_1, a_2 B $a_1 a_2$ B.

Теорема 2. Второй критерий подкольца.

Пусть A; +, – кольцо, B A. Тогда B является подкольцом кольца A, если и только если одновременно выполняются следующие три условия:

1) B ; 2) a_1, a_2 B a_1-a_2 B; 3) a_1, a_2 B $a_1 a_2$ B.

Теорема 3. Критерий подполя.

Пусть A; +, – поле, B A. Тогда B является подполем поля A, если и только если одновременно выполняются следующие три условия:

1) B^* ; 2) a_1, a_2 B a_1-a_2 B; 3) a_1, a_2 B^* $a_1 a_2^{-1}$ B^*.

ГЛАВА 3. Системы линейных уравнений. Арифметическое *n*-мерное векторное пространство

§ 1. Решение систем линейных уравнений методом Гаусса

Запись системы линейных уравнений. Решение системы линейных уравнений. Совместные и несовместные системы линейных уравнений. Определённые и неопределённые системы линейных уравнений. Следствия системы линейных уравнений. Равносильные системы линейных уравнений. Однородные системы линейных уравнений. Совместность однородной системы линейных уравнений. Элементарные преобразования системы линейных уравнений.

Теорема 1. Свойства элементарных преобразований.

1°. Элементарные преобразования обратимы, причём обратные им преобразования являются преобразованиями того же вида.

2°. Элементарное преобразование третьего вида может быть получено цепочкой преобразований двух первых видов.

3°. Всякая система линейных уравнений, получающаяся из исходной системы линейных уравнений с помощью цепочки элементарных преобразований, равносильна исходной.

Ступенчатые системы линейных уравнений. Треугольные и трапециевидные ступенчатые системы. Противоречивые уравнения. Вид противоречивых уравнений.

Теорема 2. Теорема Гаусса.

Всякая система линейных уравнений может быть приведена к ступенчатому виду или к системе, содержащей противоречивое уравнение с помощью элементарных преобразований и, возможно, перенумерации переменных. В первом случае система совместна и определённа или неопределённа, в зависимости от того, выполняется ли равенство $r = n$ или неравенство $r < n$, где r – число уравнений ступенчатой системы, n – число переменных. Во втором случае система несовместна.

Главные и свободные неизвестные. Матрица и расширенная матрица системы линейных уравнений. Обозначения при преобразованиях.

Теорема 3. Однородная система линейных уравнений, в которой число уравнений меньше числа неизвестных, имеет ненулевые решения.

§ 2. Арифметическое n-мерное векторное пространство P^n

Векторы. Скаляры. Сумма двух векторов. Произведение вектора на число.

Теорема 1. Простейшие свойства операций над векторами.

1°. $(\forall a)(\forall b)(a+b = b+a)$.
2°. $(\forall a)(\forall b)(\forall c)(a+(b+c) = (a+b)+c)$.
3°. $(\exists\theta)(\forall a)(a+\theta = a)$.
4°. $(\forall a)(\exists \bar{a})(a+\bar{a} = \theta)$.
5°. $(\forall\alpha)(\forall\beta)(\forall a)(\alpha(\beta a) = (\alpha\beta)a)$.
6°. $(\forall\alpha)(\forall\beta)(\forall a)((\alpha+\beta)a = \alpha a+\beta a)$.
7°. $(\forall\alpha)(\forall a)(\forall b)(\alpha(a+b)) = \alpha a+\alpha b)$.
8°. $(\forall a)(1\, a = a)$.

Разность векторов.

Теорема 2. Дальнейшие свойства векторов.

1°. Нуль единственный.
2°. Для каждого вектора противоположный ему единственный.

3°. $(\forall a)(-(-a) = a)$.
4°. $(\forall a)(\forall b)(-(a+b) = (-a)+(-b))$.

5°. Уравнение $a + x = b$ разрешимо при всех a и b, причём единственным образом.

6°. $(\forall a)(\forall b)(a-b = a+(-b))$.
7°. $(\forall a)(0\, a = \theta)$.

8°. $(\forall\alpha)(\alpha\,\theta = \theta)$.
9°. $(\forall\alpha)(\forall a)(\alpha a = \theta \rightarrow \alpha = 0 \;\; a = \theta)$.
10°. $(\forall\alpha)(\forall a)((-\alpha)a = \alpha(-a) = -\alpha a)$.
11°. $(\forall\alpha)(\forall a)(\forall b)(\alpha(a-b)) = \alpha a - \alpha b)$.
12°. $(\forall\alpha)(\forall\beta)(\forall a)((\alpha-\beta)a = \alpha a - \beta a)$.

§ 3. Линейная зависимость и линейная независимость систем векторов

Два определения линейной зависимости и линейной независимости системы векторов.

Теорема 1. О равносильности определений линейной зависимости.

Два определения линейной зависимости системы векторов равносильны.

Теорема 2. Свойства линейной зависимости и линейной независимости.

1°. Система, содержащая нуль-вектор или равные векторы, или коллинеарные векторы, линейно зависимая.

2°. Если часть системы векторов линейно зависимая, то и вся система линейно зависимая.

3°. Если система векторов S линейно независимая, но при добавлении к ней вектора b становится линейно зависимой, то вектор b является линейной комбинацией векторов системы S.

4°. Ступенчатая система векторов линейно независимая.

5°. В P^n существует линейно независимая система, состоящая из n векторов, через которую линейно выражается любой вектор из P^n (система единичных векторов).

Теорема 3. Если даны две системы векторов, содержащие соответственно r и s векторов, причём $r < s$, и векторы второй системы являются линейными комбинациями векторов первой системы, то вторая система линейно зависимая (Если бóльшая система выражается через меньшую, то она линейно зависимая).

Теорема 4. В P^n любая система векторов, содержащая более чем n векторов, линейно зависимая.

§ 4. Базис и ранг системы векторов

Два определения базиса системы векторов.

Теорема 1. Два определения базиса равносильны.

Теорема 2. Свойства базиса и ранга.

1°. Любая ненулевая система векторов из P^n обладает базисом.

2°. Любые два базиса системы векторов содержат одинаковое количество векторов.

3°. Линейно независимая система векторов $a_1, a_2, \ldots, a_k$ является базисом P^n тогда и только тогда, когда $k = n$.

4°. Ранг любой системы векторов из P^n не превышает n.

5°. При добавлении (удалении) к системе векторов вектора, являющегося линейной комбинацией векторов системы, ранг не изменяется.

6°. Элементарные преобразования не изменяют ранга системы векторов.

7°. Любая линейно независимая система векторов может быть дополнена до базиса P^n.

§ 5. Ранг матрицы

Запись векторного равенства в виде системы числовых равенств. Строчечный и столбцовый ранги матрицы.

Теорема о ранге матрицы.

Строчечный и столбцовый ранги матрицы равны.

Лемма 1. Элементарные преобразования строк и перестановка столбцов не меняют строчечного ранга матрицы. Лемма 2. Элементарные преобразования строк и перестановка столбцов не меняют столбцового ранга матрицы.	а) сохранение линейной зависимости (той же самой); б) сохранение линейной независимости; в) сохранение базиса

Лемма 3. Столбцовый и строчечный ранги ступенчатой матрицы равны.

§ 6. Исследование системы линейных уравнений

Теорема 1. Теорема Кронекера-Капелли.

Система линейных уравнений совместно тогда и только тогда, когда ранг матрицы этой системы равен рангу расширенной матрицы.

Теорема 2. Если система линейных уравнений с n неизвестными совместна и ранг этой системы равен r, то при любом способе решения этой системы методом Гаусса число уравнений в ступенчатой системе равно r, а число свободных неизвестных равно $n–r$.

Теорема 3. Связь решений системы линейных уравнений и сопутствующей однородной системы линейных уравнений.

Пусть X – множество решений совместной системы линейных уравнений, a – некоторое фиксированное решение этой системы (a X), X_0 – множество решений сопутствующей однородной системы линейных уравнений. Тогда множество всех решений системы линейных уравнений может быть получено путём сложения данного фиксированного решения со всеми решениями сопутствующей однородной системы: $X = a+X_0$.

Лемма 1. Сумма любого решения данной системы с любым решением сопутствующей однородной системы является решением данной системы.

Лемма 2. Разность любых двух решений данной системы является решением сопутствующей однородной системы.

§ 7. Однородные системы линейных уравнений

Теорема 1. Критерий существования ненулевых решений.

Однородная система линейных уравнений имеет ненулевые решения тогда и только тогда, когда ранг матрицы системы меньше числа неизвестных.

Теорема 2. Свойства решений однородной системы линейных уравнений.

1°. Сумма любых двух решений однородной системы линейных уравнений также является решением этой однородной системы линейных уравнений.

2°. Произведение решения однородной системы линейных уравнений на скаляр также является решением этой однородной системы линейных уравнений.

3°. Любая линейная комбинация решений однородной системы линейных уравнений также является решением этой однородной системы линейных уравнений.

Фундаментальная система решений однородной системы линейных уравнений.

Теорема 3. Если однородная система линейных уравнений с n неизвестными имеет ранг r, то любая фундаментальная система решений этой системы состоит из $n–r$ векторов.

План доказательства

1. Решение методом Гаусса.

2. Построение решения $a_1, a_2, ..., a_{n-r}$.

3. Доказательство линейной независимости этой системы векторов.

4. Выражение произвольного решения b через $a_1, a_2, ..., a_{n-r}$: построение вектора b_1 – линейной комбинации системы $a_1, a_2, ..., a_{n-r}$, доказательство равенства $b-b_1 = \theta$.

ГЛАВА 4. Матрицы и определители

§ 1. Операции над матрицами

Равенство двух матриц. Сумма двух матриц. Произведение матрицы на число. Матрица как особым образом записанный вектор. Свойства сложения и умножения на число (см. теоремы 2.3.1 и 2.3.2).

Произведение матриц.

$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$; “скалярное произведение” строки и столбца:

$$C = \begin{bmatrix} A_1B^1 & A_1B^2 & ... & A_1B^p \\ A_2B^1 & A_2B^2 & ... & A_2B^p \\ ... & ... & ... & ... \\ A_mB^1 & A_mB^2 & ... & A_mB^p \end{bmatrix}.$$

Теорема 1. Свойства умножения матриц.

1°. Умножение не коммутативно.

2°. Умножение ассоциативно.

3°. Умножение связано со сложением законами дистрибутивности.

4°. Существует единичная матрица.

5°. $(\exists A)(\exists B)(A \quad \theta \ \ B \quad \theta \ \ AB = \theta)$.

Квадратные матрицы. Значение многочлена от матрицы.

Матричные единицы E_{ij} – стандартный базис P^{mn}.

Умножение матричных единиц. Перестановочность матриц.

Элементарные матрицы (= матрицы элементарных преобразований). Результат умножения элементарных матриц слева и справа на данную.

Транспонирование матриц. Свойства транспонирования. Симметрические и кососимметрические матрицы.

Сравнение ранга произведения матриц с рангами множителей.

$C^k = A^1b_{1k}+ A^2b_{2k}+ \ldots + A^nb_{nk}, \quad C_k = a_{k1}B_1+a_{k2}B_2+ \ldots +a_{kn}B_n.$

§ 2. Обратная матрица. Условие обратимости матрицы

Матрица, обратная для данной.

Не всякая матрица имеет обратную.

Теорема 1. Простейшие свойства обратной матрицы.

1°. Всякая матрица может иметь не более одной обратной.

2°. $E^{-1} = E$.

3°. $(A^{-1})^{-1} = A$.

4°. $(AB)^{-1} = B^{-1}A^{-1}$.

Вырожденные и невырожденные квадратные матрицы.

Теорема 2. Критерий обратимости матрицы.

Матрица обратима тогда и только тогда, когда она невырожденная.

Лемма 1. Всякое строчечное (столбцовое) элементарное преобразование матрицы можно реализовать путём умножения этой матрицы слева (справа) на соответствующую элементарную матрицу.

Лемма 2. Для того чтобы матрица была невырожденной, необходимо и достаточно, чтобы её можно было привести к единичной матрице с помощью только строчечных элементарных преобразований.

Лемма 3. Если строки (столбцы) матрицы A (B) линейно зависимы и $C = AB$, то точно такая же линейная зависимость выполняется для строк (столбцов) матрицы C.

Практический способ вычисления обратной матрицы:

$A|E \xrightarrow{\varphi_1} \ \ldots \ \xrightarrow{\varphi_e} E|A^{-1}$.

Матричные уравнения.

Запись СЛУ в виде одного матричного уравнения специального вида. Терема Крамера в матричной форме.

§ 3. Перестановки и подстановки

Перестановки. Запись перестановки. Число перестановок n элементов. Инверсии. Чётные и нечётные перестановки. Транспозиции.

Теорема. Свойства транспозиций.

1°. От любой перестановки можно перейти к любой другой перестановке с помощью нескольких транспозиций.

2°. Всякая транспозиция изменяет чётность перестановки.

Подстановки. S_n. Запись подстановок. Чётность подстановки. Корректность определения чётности подстановки. Знак подстановки. $(-1)^{\sigma(\pi)}$.

§ 4. Определение определителя

Определение определителя.

Примеры вычисления определителей матриц второго и третьего порядков, определителя верхней (нижней) треугольной матрицы, определителя матрицы, у которой все элементы ниже (выше) побочной диагонали равны нулю.

§ 5. Свойства определителя

Теорема. Свойства определителя.

1°. $\det {}^tA = \det A$.

2°. $\det\begin{bmatrix} A_1 \\ A_2 \\ \ldots \\ A_k = B + C \\ \ldots \\ A_n \end{bmatrix} = \det\begin{bmatrix} A_1 \\ A_2 \\ \ldots \\ B \\ \ldots \\ A_n \end{bmatrix} + \det\begin{bmatrix} A_1 \\ A_2 \\ \ldots \\ C \\ \ldots \\ A_n \end{bmatrix}.$

3°. $\det\begin{bmatrix} A_1 \\ A_2 \\ \ldots \\ A_k = \lambda B \\ \ldots \\ A_n \end{bmatrix} = \lambda \det\begin{bmatrix} A_1 \\ A_2 \\ \ldots \\ B \\ \ldots \\ A_n \end{bmatrix}.$

4°. $\det\begin{bmatrix} A_1 \\ A_2 \\ \dots \\ A_i \\ \dots \\ A_j \\ \dots \\ A_n \end{bmatrix} = -\det\begin{bmatrix} A_1 \\ A_2 \\ \dots \\ A_j \\ \dots \\ A_i \\ \dots \\ A_n \end{bmatrix}$.

5°. Если одна из строк матрицы нулевая, то определитель матрицы равен нулю.

6°. Если какие-либо две строки матрицы равны, то определитель матрицы равен нулю.

7°. Если какие-либо две строки матрицы пропорциональны, то определитель матрицы равен нулю.

8°. Если одну из строк матрицы умножить на число и прибавить к другой строке, то определитель не изменится.

9°. Определитель вырожденной матрицы равен нулю.

10°. Определитель невырожденной матрицы отличен от нуля.

Примечание. Свойства 1°–4° доказываются по определению, остальные свойства выводятся с помощью свойств 1°–4°.

Следствие 1. Критерий невырожденности матрицы.

Квадратная матрица является невырожденной тогда и только тогда, когда её определитель отличен от нуля.

Следствие 2. Однородная система линейных уравнений, состоящая из n уравнений с n неизвестными, имеет ненулевые решения тогда и только тогда, когда определитель матрицы системы равен нулю.

§ 6. Миноры и алгебраические дополнения. Разложение определителя по строке и по столбцу

Минор M_{ij} квадратной матрицы. Алгебраическое дополнение A_{ij} элемента a_{ij} квадратной матрицы.

Теорема о разложении.

$\det A = a_{k1}A_{k1}+a_{k2}A_{k2}+ \dots +a_{kn}A_{kn}$, $\det A = a_{1k}A_{1k}+a_{2k}A_{2k}+ \dots +a_{nk}A_{nk}$

для любых $k = \overline{1,n}$.

Этапы доказательства

1. Для матрицы, в которой $A_n = e_n$, по определению det.

2. Для матрицы, в которой $A_i = e_j$, путём сведения к случаю 1, учётом знака A_i и неизменности M_{ij}.

3. Общий случай путём представления A_i в виде суммы n векторов и сведения к случаю 2.

Ещё одно свойство определителя

11°. $a_{k1}A_{p1}+a_{k2}A_{p2}+ \ldots +a_{kn}A_{pn}$, $a_{1k}A_{1p}+a_{2k}A_{2p}+ \ldots +a_{nk}A_{np}$, если $k \quad p$.

§ 7. Формула для обратной матрицы. Теорема Крамера

Теорема 1. Формула для вычисления обратной матрицы.

Если квадратная матрица A невырожденная, то

$$A^{-1} = \frac{1}{\det \mathrm{A}}\begin{bmatrix} A_{11} & A_{12} & \ldots & A_{1n} \\ A_{21} & A_{22} & \ldots & A_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ A_{n1} & A_{n1} & \ldots & A_{nn} \end{bmatrix}.$$

Теорема 2. Теорема Крамера.

Если в системе n линейных уравнений с n неизвестными матрица коэффициентов невырожденная, то система имеет единственное решение, которое задаётся формулами $x_k = \frac{\det A_k}{\det A}$, где матрица A_k получается из матрицы A заменой k-го столбца столбцом свободных членов.

§ 8. Определитель произведения матриц

Теорема.

Если A и B – квадратные матрицы одного формата, то $\det(AB) = \det A \det B$.

Лемма. Если E_φ – матрица элементарного преобразования φ, то $\det(E_\varphi B) = \det E_\varphi \det B$.

§ 9. Теорема о ранге матрицы

Обобщение понятия минора. $M\begin{pmatrix} i_1 & i_2 & \ldots & i_k \\ j_1 & j_2 & \ldots & j_k \end{pmatrix}$.

Теорема. Ранг матрицы равен наибольшему из порядков её ненулевых миноров.

План доказательства

1. Если $A_{k_1}, A_{k_2}, \ldots, A_{k_r}$ – базис системы вектор-строк, то существуют столбцы с номерам $p_1, p_2, \ldots, p_r$ такие, что $M\begin{pmatrix} i_1 & i_2 & \ldots & i_k \\ p_1 & p_2 & \ldots & p_k \end{pmatrix} \quad 0$.

2. $M = 0$ для любого $k \;\; k$- минора, если $k > r$.

ГЛАВА 5. Векторные пространства

§ 1. Определение, примеры, простейшие свойства векторных пространств

Определение векторного пространства.

Важнейшие примеры.

1. $\boldsymbol{R}^{2,3}$. **2**. P^n. **3**. $M_{m\times n}$. **4**. $F_{\boldsymbol{R}}$. **5**. $\boldsymbol{R}[x]$. **6**. $\boldsymbol{R}_n[x]$. **7**. Поле над любым своим подполем. **8**. R_+^* над $\boldsymbol{R}$.

Теорема. Простейшие свойства векторных пространств.

Совпадает с теоремой 3.2.2.

§ 2. Линейная зависимость и линейная независимость систем векторов. Базис и ранг системы векторов

Содержание этого параграфа полностью повторяет содержание параграфов 3.3. и 3.4.

§ 3. Конечномерные векторные пространства. Изоморфизм векторных пространств. Координаты вектора в некотором базисе

Примеры конечномерных и бесконечномерных векторных пространств. Размерности этих конечномерных векторных пространств.

Теорема 1. Любая ненулевая система векторов конечномерного векторного пространства обладает базисом. Количество векторов этого базиса не превосходит размерности пространства.

Координаты вектора в базисе E. Столбец координат $[a]_E$. Равенство $a = E\,[a]_E$.

Теорема 2. Свойства координат.

1°. $[a+b] = [a]+[b]$.

2°. $[\alpha a] = \alpha[a]$.

Изоморфизм векторных пространств. Отношение изоморфизма.

Пример.

Если V – n-мерное векторное пространство над полем P и E – базис V, то отображение φ: $a \mapsto [a]_E$ является изоморфизмом V на P^n.

Теорема 3. Свойства изоморфизма векторных пространств.

Содержание этой теоремы и его доказательство полностью повторяет содержание теоремы 2.3.3.

Теорема 4. Свойства векторов и их систем, сохраняемые при изоморфизмах.

1°. При изоморфизме нуль-вектор переходит в нуль-вектор.

2°. При изоморфизме противоположный вектор переходит в противоположный вектор.

3°. Изоморфизм сохраняет линейную комбинацию.

4°. Изоморфизм сохраняет линейную зависимость.

5°. Изоморфизм сохраняет линейную независимость.

6°. Изоморфизм сохраняет базисы.

Теорема 5. Критерий изоморфизма конечномерных векторных пространств.

Два конечномерных векторных пространства над одним и тем же полем изоморфны тогда и только тогда, когда равны их размерности.

§ 4. Связь между различными базисами конечномерных векторных пространств. Координаты вектора в разных базисах

Матрица перехода от одного базиса к другому $M = M_E(E\ )$: $E\ \ = E\ M$.

Теорема 1. Критерий матрицы перехода.

n n-матрица A служит матрицей перехода от одного базиса n-мерного пространства к другому тогда и только тогда, когда A невырожденная матрица.

Координаты вектора в разных базисах.

Теорема 2. Связь между координатами вектора в разных базисах.

$[a]_E\ = M_E^{-1}(E\ )\ [a]_E$.

§ 5. Подпространства векторного пространства

Определение подпространства.

Теорема 1. Критерий подпространства.

Подмножество U векторного пространства V над полем P является подпространством этого пространства тогда и только тогда, когда одновременно выполняются следующие условия:

1) U ; 2) a_1, a_2 U a_1+a_2 U; 3) λ P, a U λa U.

Примеры подпространств.

1. θ и V.

2. Множества симметрических, кососимметрических, верхних треугольных матриц в пространстве квадратных матриц.

3. Линейная оболочка системы векторов $L(a_1, a_2, ..., a_k)$.

Теорема 2. Размерность линейной оболочки.

$\dim L(S) = r(S)$.

Теорема 3. Всякое подпространство U конечномерного векторного пространства V является линейной оболочкой некоторой конечной системы векторов:
$U = L(a_1, a_2, ..., a_k)$. При этом $\dim U$ $\dim V$.

Пересечение и сумма подпространств.

Теорема 4. Тождество Грассмана.

Для любых конечномерных подпространств U_1 и U_2 произвольного векторного пространства выполняется равенство

$$\dim(U_1+U_2) = \dim U_1 + \dim U_2 - \dim (U_1\ \ U_2).$$

План доказательства

Дополнить базис A подпространства U_1 U_2 до базисов (A, B) и (A, C) подпространств U_1 и U_2 соответственно и проверить, что система векторов (A, B, C) составляет базис U_1+U_2.

§ 6. Прямая сумма подпространств

Определение и примеры прямой суммы и не прямой суммы подпространств.

Теорема 1. Следующие условия равносильны.

1. Сумма U_1+U_2 подпространств U_1 и U_2 является прямой суммой.
2. Существует вектор a подпространства U_1+U_2, который единственным образом представляется в виде $a = a_1+a_2$, где a_1 U_1, a_2 U_2.
3. U_1 $U_2 = \theta$.
4. $\dim(U_1+U_2) = \dim U_1 + \dim U_2$.

План доказательства: 1 2 3 1. 3 4.

Теорема 2. Если U произвольное подпространство конечномерного векторного пространства V, то V можно представить в виде прямой суммы подпространства U и некоторого другого подпространства W.

§ 7. Линейные многообразия

Примеры линейных многообразий.

1. Прямые в $\boldsymbol{R}^2$ и $\boldsymbol{R}^3$.
2. Плоскости в $\boldsymbol{R}^3$.
3. Множество решений совместной системы линейных уравнений.

Теорема 1. Если U подпространство пространства V, то $U+a = U+b$ тогда и только тогда, когда $a-b$ U.

→ Теорема 2. Если $K_1 = U_1+a_1$, $K_2 = U_2+a_2$, то K_1 K_2 тогда и только тогда, когда U_1 U_2 и a_1-a_2 U_2.←

ГЛАВА 6. Евклидовы пространства

§ 1. Скалярное произведение. Определение, примеры, простейшие свойства евклидовых пространств. Длина вектора. Угол между векторами

Определение скалярного произведения. Определение евклидова пространства.
Примеры евклидовых пространств.
1. $\boldsymbol{R}^2$. **2**. $\boldsymbol{R}^3$. **3**. $\boldsymbol{R}^n$. **4**. C[α; β]. **5**. $\boldsymbol{R}[x][\alpha; \beta]$.

Теорема 1. Свойства скалярного произведения.

1°. $(\alpha a, b) = \alpha(a, b)$.
2°. $(a+b, c) = (a, c)+(b, c)$.
3°. $(\Sigma a_k, \Sigma b_p) = \Sigma(a_k, b_p)$.
4°. $(\Sigma\alpha_k a_k, \Sigma\beta_p b_p) = \alpha_k\beta_p\Sigma(a_k, b_p)$.

Длина вектора. Угол между векторами.

Теорема 2. Свойства длины вектора и угла между векторами.

1°. $|\alpha a| = |\alpha| |a|$.

2°. $|a| = 0 \quad a = \theta$.

3°. Неравенство Коши-Буняковского: $|(a, b)| \le |a| \cdot |b|$.

4°. Определения угла между векторами корректно.

Расстояние между векторами. $\rho(a, b)$.

Теорема 3. Свойства расстояния между векторами.

1°. $\rho(a, b) = 0 \quad a = b$.

2°. $\rho(a, b) = \rho(b, a)$.

3°. $\rho(a, c) \quad \rho(a, b)+\rho(b, c)$. Условие равенства.

§ 2. Ортогональность. Ортонормированная система векторов. Изоморфизм евклидовых пространств

Ортогональные системы векторов. Ортонормированные системы векторов.

Теорема 1. Свойства ортогональности и ортонормированности.

1°. $a \perp \theta$.

2°. $a \perp b \quad b \perp a$.

3°. $b \perp a_1, a_2, \ldots, a_k \quad b \perp L(a_1, a_2, \ldots, a_k)$.

4°. Ортогональная система ненулевых векторов линейно независима.

5°. Для любой системы векторов $a_1, a_2, \ldots, a_k$, где $k < \dim E_n$, найдётся ненулевой вектор, ортогональный им всем.

6°. В E_n существует ортогональный базис.

7°. В E_n существует ортонормированный базис.

Теорема 2. Критерий ортонормированного базиса.

Система из n линейно независимых векторов $a_1, a_2, \ldots, a_n$ n-мерного евклидова пространства E_n является ортонормированным базисом тогда и только тогда, когда для любых $x, y \quad E_n$, если $x = \alpha_1 a_1+\alpha_2 a_2+ \ldots +\alpha_n a_n$, $y = \beta_1 b_1+\beta_2 b_2+ \ldots +\beta_n b_n$, то $(x, y) = \alpha_1\beta_1+\alpha_2\beta_2+ \ldots +\alpha_n\beta_n$.

Изоморфизм евклидовых пространств и отношение изоморфизма.

Теорема 3. Свойства изоморфизма евклидовых пространств.

Содержание этой теоремы и его доказательство полностью повторяет содержание теоремы 5.3.3.

Теорема 4. Свойства векторов и их систем, сохраняемые при евклидовых изоморфизмах.

Свойства 1°–6° такие же, как свойства изоморфизма векторных пространств (Т. 6.3.4.).

7°. Евклидов изоморфизм сохраняет длину вектора.

8°. Евклидов изоморфизм сохраняет величину угла.

9°. Евклидов изоморфизм сохраняет ортогональность.

10°. Евклидов изоморфизм сохраняет расстояние между векторами.

Теорема 5. Критерий изоморфизма конечномерных евклидовых пространств.

Два конечномерных евклидовых пространства изоморфны тогда и только тогда, когда равны их размерности.

§ 3. Ортогональное дополнение к подпространству. Ортогональная проекция вектора на подпространство. Процесс ортогонализации системы векторов

Ортогональное дополнение $U^\perp$ к подмножеству $U \quad E_n$.

Теорема 1. Свойства ортогонального дополнения.

1°. $U^\perp$ – векторное подпространство пространства E_n.

2°. Пространство E_n есть прямая сумма любого своего подпространства U и его ортогонального дополнения $U^\perp$.

3°. Если U – подпространство E_n , то $\dim U^\perp = n - \dim U$.

4°. $(U^\perp)^\perp = U$ для любого подпространства U пространства E_n.

→5°. $E_n^\perp = \theta$; $\theta^\perp = E_n$; $U \quad W \quad W^\perp \quad U^\perp$; $(U_1+U_2)^\perp = U_1^\perp \quad U_2^\perp$; $(U_1 \quad U_2)^\perp = U_1^\perp + U_2^\perp$.←

Проекция вектора b на подпространство U. $\mathrm{pr}_U b$.

Теорема 2. Если $a_1, a_2, \ldots, a_k$ – ортогональный базис подпространства U, то

$$\mathrm{pr}_U b = \frac{(b, a_1)}{(a_1, a_1)} a_1 + \frac{(b, a_2)}{(a_2, a_2)} a_2 + \ldots + \frac{(b, a_k)}{(a_k, a_k)} a_k .$$

Процесс ортогонализации.

Имеется система векторов $b_1, b_2, \ldots, b_k$.

Ищется система векторов $a_1, a_2, \ldots, a_k$, удовлетворяющая следующим условиям:

если $U_p = L(b_1, b_2, \ldots, b_p)$, то $a_1 \quad U_1$; $a_2 \quad U_2$, $a_2 \perp U_1$; $a_3 \quad U_3$, $a_3 \perp U_2$; ...; $a_p \quad U_p$, $a_p \perp U_{p-1}$.

Для этого полагают $a_1 = b_1$, $a_2 = b_2 - \mathrm{pr}_{U_1} b_2$, $a_3 = b_3 - \mathrm{pr}_{U_2} b_3$, $a_p = b_p - \mathrm{pr}_{U_{p-1}} b_p$.

ГЛАВА 7. Линейные отображения и линейные операторы

§ 1. Линейные отображения. Матрица линейного отображения

Определение, примеры, простейшие свойства (свойства 1°–4° изоморфизма векторных пространств в Т. 5.3.4.) линейных отображений.

Теорема 1. Структурная теорема.

Пусть V_1 и V_2 – векторные пространства над одним полем, $\dim V_1 = n$,

$a_1, a_1, ..., a_n$ – базис пространства V_1, $b_1, b_1, ..., b_n$ – произвольная система векторов из пространства V_2. Тогда существует, и только одно, линейное отображение

$\varphi: V_1 \to V_2$, обладающее свойством $\varphi(a_k) = b_k$, $k = \overline{1, n}$.

Матрица линейного отображения $A = M_\varphi(E_1, E_2)$: $\varphi(E_1) = E_2 A$.

Координаты образа вектора.

<u>Теорема 2</u>. Связь координат вектора и его образа.

$[\varphi(a)]^{E_2} = M_\varphi(E_1, E_2)\, [a]^{E_1}$.

<u>Теорема 3</u>. Если V_1 и V_2 – конечномерные векторные пространства над одним и тем же полем, размерности которых равны n и m соответственно, E_1 и E_2 – их базисы, то отображение
$\Phi: \varphi \mapsto M_\varphi(E_1, E_2)$ является биекцией множества всех линейных отображений пространства V_1 в пространство V_2 на множество всех m n-матриц над тем же полем.

§ 2. Операции над линейными отображениями

Сумма и произведение (композиция) линейных отображений. Произведение линейного отображения на элемент поля.

<u>Теорема 1</u>. Свойства операций над линейными отображениями.

1°. Сумма и произведение линейных отображений, а также произведение линейного отображения на скаляр, являются линейными отображениями.

2°. Множество всех линейных отображений векторного пространства V_1 в векторное пространство V_2 является векторным пространством над тем же полем относительно операций сложения линейных отображений и умножения на скаляр.

3°. Множество всех линейных преобразований (линейных функционалов) векторного пространства в себя является кольцом относительно операций сложения и умножения.

<u>Теорема 2</u>. Связь линейных отображений и их матриц.

Если V_1, V_2 и V_3 – конечномерные векторные пространства над одним и тем же полем, E_1, E_2 и E_3 – их базисы, соответственно, то:

а) $\varphi: V_1 \to V_2$ – изоморфизм $\quad M_\varphi(E_1, E_2)$ – невырожденная;

б) $M_{\lambda\varphi}(E_1, E_2) = \lambda\, M_\varphi(E_1, E_2)$;

в) $M_{\varphi+\psi}(E_1, E_2) = M_\varphi(E_1, E_2)+M_\psi(E_1, E_2)$;

г) $M_{\varphi \circ \psi}(E_1, E_2) = M_\varphi(E_1, E_2)\, M_\psi(E_2, E_3)$.

§ 3. Ранг, дефект, ядро и образ линейного отображения

Ядро и образ линейного отображения φ. Ker φ. Im φ. Ранг и дефект линейного отображения. $r(\varphi)$. $d(\varphi)$.

Теорема 1. Ядро и образ линейного отображения $\varphi: V_1 \to V_2$ являются подпространствами векторных пространств V_1 и V_2, соответственно.

Теорема 2. Ранг линейного отображения конечномерного векторного пространства равен рангу матрицы линейного отображения.

Теорема 3. Если $\varphi: V_1 \to V_2$ – линейное отображение конечномерного векторного пространства, то сумма ранга и дефекта этого отображения равна размерности пространства V_1: $\dim V_1 = r(\varphi)+d(\varphi)$.

§ 4. Линейные операторы

Теорема 1. Всякий инъективный линейный оператор конечномерного векторного пространства сюръективен и наоборот.

Подобие матриц.

Теорема 2. Две квадратные матрицы подобны тогда и только тогда, когда они являются матрицами одного и того же линейного оператора, но в разных базисах.

§ 5. Линейные алгебры

Определение линейной алгебры.
Важнейшие примеры.

1. $M_{n\times n}$. **2**. *End V*. **3**. $\boldsymbol{R}[x]$. **4**. $F_{\boldsymbol{R}}$.

Изоморфизм линейных алгебр. Стандартные свойства изоморфизма линейных алгебр (см. теоремы 5.3.3 и 5.3.4).

Теорема. Алгебра всех линейных операторов n-мерного векторного пространства над полем P изоморфна алгебре n n-матриц над этим же полем.

§ 6. Собственные векторы и собственные значения линейного оператора

Инвариантные подпространства линейного оператора. Примеры. Собственные векторы и собственные значения линейного оператора. Геометрическая интерпретация.

Корневое (собственное) подпространство $K(\lambda)$.

Теорема 1. Свойства собственных векторов.

1°. $K(\lambda)$ является подпространством векторного пространства.

2°. Собственные векторы, принадлежащие различным собственным значениям, ЛНЗ.

3°. Для любого линейного оператора конечномерного векторного пространства сумма размерностей всех его корневых подпространств не превышает размерности всего пространства.

4°. Линейный оператор имеет диагональную матрицу в некотором базисе тогда и только тогда, когда этот базис состоит из собственных векторов линейного оператора.

Характеристический многочлен матрицы. Характеристический многочлен линейного оператора.

<u>Теорема 2</u>. Корректность определения характеристического многочлена линейного оператора.

1°. Подобные матрицы имеют одинаковые характеристические многочлены.

2°. Определения характеристического многочлена линейного оператора корректно.

<u>Теорема 3</u>. Правила отыскания собственных векторов и собственных значений линейного оператора.

1°. Множество собственных значений линейного оператора совпадает с множеством корней характеристического многочлена.

2°. Собственное подпространство $K(\lambda)$ совпадает с множеством решений однородной системы линейных уравнений $(A–\lambda E)\,X = \theta$.

ГЛАВА 8. Теория делимости целых чисел

§ 1. Отношение делимости. Деление с остатком

Определение делимости целых чисел. $a \vdots b$, $b|a$.

<u>Теорема 1</u>. Свойства делимости.

Для любых целых чисел имеют место следующие соотношения

1°. $a \vdots a$.

2°. $a \vdots 1$.

3°. $a \vdots b \quad \pm a \vdots \pm b$.

4°. $0 \vdots a$;

5°. $a \vdots b \;\; b \vdots c \quad a \vdots c$.

6°. $a \vdots b \;\; b \vdots c \quad ua+vb \vdots c$.

7°. $a \quad 0 \;\; a \vdots b \quad |a| \quad |b|$.

8° $a \quad 0 \;\; b \quad 0 \;\; a \vdots b \;\; b \vdots a \quad a = \pm b$.

Определение деления с остатком.

<u>Теорема 2</u>. О делении с остатком.

Любое целое число a можно разделить с остатком на любое целое число $b \quad 0$. Это деление осуществляется единственным образом.

Определение систематического представления натурального числа.

Теорема 3. Любое целое неотрицательное число a может быть представлено, причем единственным образом, в виде

$$a = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0,$$

где g $\boldsymbol{N}$, g 1, 0 a_k $g-1$ при всех 0 k n.

Запись: $\overline{a_n a_{n-1} \ldots a_1 a_0}\ _g$.

Таблицы сложения и умножения в g-ичной системе счисления.

Перевод из одной системы счисления в другую: правила деления и умножения.

§ 2. **НОД чисел. Алгоритм Евклида**

ОД и НОД системы чисел.

Теорема 1. Единственность НОД.

Любые два НОД системы чисел совпадают, с точностью до знака, если они существуют.

$(a_1, a_2, \ldots, a_n)$.

Алгоритм Евклида: описание алгоритма, конечность алгоритма.

Теорема 2. Существование НОД двух чисел.

Для любых двух целых чисел, не равных нулю одновременно, их НОД существует. Он равен последнему, отличному от нуля, остатку алгоритма Евклида для этих двух чисел.

Следствие 1. Свойства НОД.

1°. С точностью до знака, $(ac, bc) = (a, b)c$.

2°. Если t – ОД(a, b), то, с точностью до знака, $\left(\frac{a}{t}, \frac{b}{t}\right) = \frac{(a, b)}{t}$.

3°. Если $d = (a, b)$, то $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

4°. Если $d = (a, b)$, то существуют числа u, v такие, что $ua+vb = d$.

5°. Наибольший по модулю общий делитель чисел a и b является их НОД.

Теорема 3. Цепное правило.

НОД нескольких чисел $a_1, a_2, \ldots, a_n$ существует. Он вычисляется по правилу $((\ldots ((a_1, a_2), a_3), \ldots, a_{n-1}), a_n)$.

Следствие 2. Свойства НОД 1°–5° двух чисел справедливы для любого конечного количества чисел.

§ 3. **Взаимно простые числа**

Теорема 1. Критерий взаимной простоты чисел.

Числа a и b взаимно простые тогда и только тогда, когда существуют целые числа u и v такие, что $ua+vb = 1$.

Теорема 2. Свойства взаимно простых чисел.

1°. $(a, c) = (b, c) = 1 \quad (ab, c) = 1$.
2°. $ab \,\vdots\, c \;\; (a, c) = 1 \quad b \,\vdots\, c$.
3°. $a \,\vdots\, b \;\; a \,\vdots\, c \;\; (b, c) = 1 \quad a \,\vdots\, bc$.

Обобщение результатов теорем 1 и 2 на случай n чисел.

§ 4. **НОК чисел**

ОК и НОК системы чисел.

Теорема 1. Единственность НОК.

Любые два НОК системы чисел совпадают, с точностью до знака, если они существуют.

$[a_1, a_2, ..., a_n]$.

Теорема 2. Существование НОК двух чисел.

Для любых двух целых чисел a и b, не равных нулю одновременно, их НОК существует. Он равен $\dfrac{ab}{(a, b)}$.

Следствие 1. Свойства НОК двух чисел.

1°. С точностью до знака, $[ac, bc] = [a, b]c$.
2°. Если t – ОД(a, b), то, с точностью до знака, $\left[\dfrac{a}{t}, \dfrac{b}{t}\right] = \dfrac{[a, b]}{t}$;
3°. Наименьшее по модулю общее кратное чисел a и b является их НОК.

Теорема 3. Цепное правило.

НОК нескольких чисел $a_1, a_2, ..., a_n$ существует. Оно вычисляется по правилу $[[\ ...\ [[a_1, a_2], a_3], ..., a_{n-1}], a_n]$.

Следствие 2. Свойства НОК 1°–3° двух чисел справедливы для любого конечного количества чисел.

§ 5. **Простые числа. Основная теорема арифметики**

Простые и составные числа.

Теорема 1. Свойства простых чисел.

1°. p – простое $p \vdots a$ $a = 1$ $a = p$.

2°. Если p_1, p_2 – различные простые числа, то ни одно из них не делится на другое.

3°. p – простое $(\forall a)(a \vdots p$ $(a, p) = 1)$.

4°. $a_1 a_2 \ldots a_n \vdots p$ $a_1 \vdots p$ $a_2 \vdots p$ ... $a_n \vdots p$.

5°. $(\forall a$ $1)(\exists p)(p$ – простое $a \vdots p)$.

6°. Если a 1 и a не делится ни на одно простое число p $\sqrt{a}$, то a – простое число.

Теорема 2. Основная Теорема Арифметики.

Всякое натуральное число, отличное от единицы, либо является простым числом, либо представляется в виде произведения простых чисел, причем такое представление единственное, с точностью до порядка следования множителей.

Каноническое разложение (факторизация) натурального числа.

Следствие 1. Всякое натуральное составное число имеет единственное каноническое разложение.

Следствие 2. Если a имеет каноническое разложение $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, то $b|a$ $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$, где 0 β_i α_i для всех $i = \overline{1, s}$.

Следствие 3. Правила отыскания НОД и НОК.

Пусть $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ – почти канонические разложения чисел a и b, то есть для всех $i = \overline{1, s}$ 0 α_i, 0 β_i причем одно из них 0. Тогда

1°. $(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}$, где $(\forall i = \overline{1, s})(\gamma_i = \min\{\alpha_i, \beta_i\}$.

2°. $[a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_s^{\delta_s}$, где $(\forall i = \overline{1, s})(\delta_i = \max\{\alpha_i, \beta_i\}$.

Теорема 3. Множество простых чисел бесконечно.

Доказательство Евклида.

ГЛАВА 9. Теория сравнений целых чисел

§ 1. **Числовые сравнения**

$a \quad b$ (mod m).

Теорема 1. Следующие утверждения равносильны.

1°. $a \quad b$ (mod m).
2°. $a = b+mt,\ t \quad \boldsymbol{Z}$.
3°. a и b равноостаточны при делении на m.

Теорема 2. Свойства числовых сравнений.

1°. Отношение сравнения является отношением эквивалентности.
2°. Отношение сравнения согласовано со сложением.
3°. Отношение сравнения согласовано с умножением.
4°. Сравнения можно почленно складывать.
5°. Сравнения можно почленно умножать.
6°. $a \quad b$ (mod m) $d|m \quad d > 0 \qquad a \quad b$ (mod d).
7°. Если $c > 0$, то $a \quad b$ (mod m) $\qquad ac \quad bc$ (mod mc).
8°. $ac \quad bc$ (mod m) $d = (m, c) \qquad a \quad b$ (mod $\frac{m}{c}$).
9°. $ac \quad bc$ (mod mc) $(m, c) = 1 \qquad a \quad b$ (mod m).
10°. $a \quad b$ (mod m) $\qquad (a, m) = (b, m)$.
11°. $a \quad b$ (mod m) $f(x) \quad \boldsymbol{Z}[x] \qquad f(a) \quad f(b)$ (mod m).
12°. $a = mq+r \qquad a \quad r$ (mod m).

Признаки делимости. Общий признак делимости Паскаля. Признаки делимости на 2, 2^k, 5, 5^k, 3, 9, 11.

§ 2. **Функция Эйлера.**

Определение функции Эйлера. $\varphi(m)$.

Теорема 1. Свойства функции Эйлера.

1°. Если p – простое число, то $\varphi(p) = p-1$.
2°. Если p – простое число, то $\varphi(p^k) = p^{k-1}(p-1)$.
3°. Функция φ мультипликативная.
4°. Формулы для вычисления $\varphi(m)$.
5°. Тождество Гаусса: $\sum_{m:d} \varphi(d) = m$.

§ 3. Полная и приведенная системы вычетов. Теоремы Эйлера и Ферма

Полная система вычетов. Приведённая система вычетов. Наиболее употребительные системы вычетов: наименьшая положительная, наименьшая неотрицательная, абсолютно наименьшая и т.д.

Теорема 1. Свойства полной и приведённой система вычетов.

1°. Критерий полной системы вычетов. Любая совокупность из m целых чисел, попарно не сравнимых по модулю m, образует полную систему вычетов по модулю m.

2°. Если числа x_1, x_2, ..., x_m – полная система вычетов по модулю m, $(a, m) = 1$, b – произвольное целое число, то числа ax_1+b, ax_2+b, ..., ax_m+b также составляют полную систему вычетов по модулю m.

3°. Критерий Приведённой системы вычетов. Любая совокупность, состоящая из $\varphi(m)$ целых чисел, попарно не сравнимых по модулю m и взаимно простых с модулем, образует приведённую систему вычетов по модулю m.

4°. Если числа x_1, x_2, ..., $x_{\varphi(m)}$ – приведённая система вычетов по модулю m, $(a, m) = 1$, то числа ax_1, ax_2, ..., $a\ x_{\varphi(m)}$ также составляют приведённую систему вычетов по модулю m.

Теорема 2. Теорема Эйлера.

Если числа a и m взаимно простые, то $a^{\varphi(m)}\quad 1(\mathrm{mod}\ m)$.

Следствие.

1°. Теорема Ферма. Если p – простое число и a не делится на p, то $a^{p-1}\quad 1(\mathrm{mod}\ p)$.

2°. Обобщенная теорема Ферма. Если p – простое число, то $a^p\quad a\ (\mathrm{mod}\ p)$ для любых $a\quad \boldsymbol{Z}$.

§ 4. **Решение сравнений с переменной**

Решение сравнений. Равносильность. Степень сравнения.

Теорема. Свойства решений сравнений.

1°. Решениями сравнений являются целые классы вычетов.

2°. $(\forall k)(a_k\quad b_k(\mathrm{mod}\ m))$ $k = \overline{0, n}$ сравнения $\sum_k a_k x^k\quad 0\ (\mathrm{mod}\ m)$ и $\sum_k b_k x^k\quad 0\ (\mathrm{mod}\ m)$ равносильны.

3°. Если обе части сравнения умножить на число, взаимно простое с модулем, то получится сравнение, равносильное исходному.

4°. Всякое сравнение по простому модулю p равносильно сравнению, степень которого не превосходит p–1.

5°. Сравнение $\sum_{k=0}^{n} a_k x^k\quad 0\ (\mathrm{mod}\ p)$, где p – простое число, имеет не более n различных решений.

6°. Теорема Вильсона. $(n-1)!\quad -1\ (\mathrm{mod}\ n)\quad n$ простое число.

§ 5. **Решение сравнений первой степени**

$ax \quad b \pmod{m}$.

Теорема. 1°. Если $(a, m) = 1$, то сравнение имеет решение, причем единственное.

2°. Если $(a, m) = d$ и b не делится на d, то сравнение не имеет решений.

3°. Если $(a, m) = d$ и b делится на d, то сравнение имеет d различных решений, которые составляют один класс вычетов по модулю $\frac{m}{d}$.

Способы решения сравнений $ax \quad b \pmod{m}$ в случае, когда $(a, m) = 1$:

1) подбор (перебор элементов полной системы вычетов);
2) использование теоремы Эйлера;
3) использование алгоритма Евклида;
4) вариация коэффициентов (использование свойства 2° полной системы вычетов из Теоремы 2.2);

§ 6. Неопределенные уравнения первой степени

$ax+by = c$.

Теорема. Уравнение $ax+by = c$ разрешимо тогда и только тогда, когда $c \,\vdots\, (a, b)$.

В случае $(a, b) = 1$ все решения уравнения задаются формулами

$$\begin{cases} x = x_0 + bt, \\ y = y_0 - at, \end{cases} \quad t \quad \boldsymbol{Z},$$ где x_0 является каким-либо решением сравнения

$ax \quad c \pmod{b}$, $y_0 = \dfrac{c - ax_0}{b}$.

Диофантовы уравнения.

ГЛАВА 10. Комплексные числа

§ 1. Определение системы комплексных чисел. Существование системы комплексных чисел

Определение системы комплексных чисел.

Теорема. Система комплексных чисел существует.

Модель: $\boldsymbol{R}^2$ с операциями

$(a, b)+(c, d) = (a+c, b+d)$, $(a, b)\,(c, d) = (ac-bd, bc+ad)$,

$i = (0, 1)$ и отождествлением $a = (a, 0)$.

§ 2. Алгебраическая форма комплексного числа

Представление комплексного числа в виде $z = a+bi$, где $a, b \quad \boldsymbol{R}$, $i^2 = -1$. Единственность такого представления. Re z, Im z.

Правила выполнения арифметических действий над комплексными числами в алгебраической форме.

Арифметическое n-мерное векторное пространство $\boldsymbol{C}^n$. Системы линейных уравнений, матрицы и определители над $\boldsymbol{C}$.

Извлечение квадратных корней из комплексных чисел в алгебраической форме.

§ 3. Геометрическое изображение комплексных чисел

Действительная и мнимая части, модуль и аргумент комплексного числа. Связь между ними.

Тригонометрическая форма комплексного числа.

Теорема. Всякое комплексное число единственным образом представляется в тригонометрической форме.

Свойства модуля комплексного числа, связанные со сложением и вычитанием.

§ 4. Тригонометрическая форма комплексного числа

Теорема 1. Если $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$, $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$, то

а) $z_1 z_2 = r_1 r_2 (\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2))$; б) $\frac{z_1}{z_2} = \frac{r_1}{r_2}(\cos(\varphi_1-\varphi_2) + i\sin(\varphi_1-\varphi_2))$.

Следствие.

$|z_1 z_2| = |z_1||z_2|$, $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$; $\arg(z_1 z_2) = \arg z_1 + \arg z_2$, $\arg\frac{z_1}{z_2} = \arg z_1 - \arg z_2$.

Теорема 2. Формулы Муавра.

1°. Если $z = r(\cos\varphi + i\sin\varphi)$, n $\boldsymbol{N}$, то $z^n = r^n(\cos n\varphi + i\sin n\varphi)$.

2°. Если $z = r(\cos\varphi + i\sin\varphi)$, n $\boldsymbol{Z}$, то $z^n = r^n(\cos n\varphi + i\sin n\varphi)$.

§ 5. Комплексно сопряжённые числа

Теорема. Свойства комплексно сопряжённых чисел.

1°. $\mathrm{Re}\,\bar{z} = \mathrm{Re}\,z$, $\mathrm{Im}\,\bar{z} = -\mathrm{Im}\,z$.

2°. $|\bar{z}| = |z|$, $\arg\bar{z} = -\arg z$.

3°. $\bar{\bar{z}} = z$.

4°. z $\boldsymbol{R}$ $\bar{z} = z$.

5°. $\bar{z} + z$ $\boldsymbol{R}$, $\bar{z}$ z $\boldsymbol{R}$.

6°. z_1+z_2 $\boldsymbol{R}$ $z_1 z_2$ $\boldsymbol{R}$ z_1, z_2 $\boldsymbol{R}$ $z_1 =$.

7°. $\overline{z_1 * z_2} = \overline{z_1} * \overline{z_2}$ для любой арифметической операции $*$.

8°. Если комплексное число w получено из комплексных чисел z_1, z_2, ..., z_n с помощью четырёх арифметических операций: $w = f(z_1, z_2, ..., z_n)$, то, заменив числа z_1, z_2, ..., z_n на числа, комплексно сопряжённые им, и проделав те же операции, и в том же порядке, получим число, комплексно сопряжённое w: $\overline{w} = f(\overline{z_1}, \overline{z_2}, ..., \overline{z_n})$.

§ 6. Корни из комплексных чисел

Теорема. Пусть z $\boldsymbol{C}$, z 0, n $\boldsymbol{N}$, $n > 1$. Тогда существует в точности n корней степени n из числа z. Если $z = r(\cos\varphi + i\sin\varphi)$ – тригонометрическая форма z, то все корни могут быть найдены по формуле

$$\sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right),\ k = \overline{0, n-1}. \qquad (1)$$

Этапы доказательства:

1) очерчивание круга поиска; 2)числа вида (1) различны;

3) любой корень степени n из z совпадает с одним из чисел (1).

Корни из единицы. $\sqrt[n]{1}$. Первообразные корни.

Теорема. Свойства корней из единицы.

1°. Произведение и частное корней степени n из единицы также являются корнями степени n из единицы.

2°. Если w – один из корней степени n из числа z, то множество всех корней степени n из числа z может быть получено умножением w на значения корней степени n из единицы: $\sqrt[n]{z} = w \cdot \sqrt[n]{1}$.

3°. Для любого n $\boldsymbol{N}$ существует первообразный корень степени n из единицы: $\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

4°. Число ε $\sqrt[n]{1}$ является первообразным корнем из единицы тогда и только тогда, когда все числа $\varepsilon^0 = 1$, ε^1, ε^2, ..., ε^{n-1} различны.

5°. Сумма всех корней степени n из ненулевого числа равна нулю.

ГЛАВА 11. Кольцо многочленов от одной переменной

§ 1. Определение многочлена

Многочлен как бесконечная последовательность элементов кольца A, в которой только конечное число элементов отлично от нуля. M_A. Операции сложения и умножения многочленов. Степень многочлена. $\deg f$.

Теорема 1. Наследование свойств кольца.

1°. Сумма и произведение двух многочленов над кольцом также являются многочленами.

2°. Алгебра многочленов $M_A; +,$ над кольцом также является кольцом.

3°. Если кольцо A коммутативно или ассоциативно, или кольцо с единицей, или целостное кольцо, то этим же свойством обладает кольцо $M_A; +,$.

<u>Теорема 2</u>. Свойства степени многочлена.

1°. deg $(f \pm g)$ max $\{\deg f, \deg g\}$.

2°. deg $(f \;\; g)$ $\deg f + \deg g$.

3°. Если кольцо A целостное, то deg $(f \;\; g) = \deg f + \deg g$.

Многочлен x. Натуральные степени многочлена x. Стандартная форма многочлена: $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$. Условие равенства двух многочленов, записанных в стандартной форме. $A[x]$.

§ 2. Многочленные функции

Многочленная функция $\overline{f} : A \to A$, соответствующая многочлену f.

<u>Теорема</u>. Свойства кольца многочленных функций.

1°. Множество $\overline{A[x]}$ всех многочленных функций является подкольцом в кольце всех функций F_A, отображающих A в A.

2°. Соответствие Φ: $f \mapsto \overline{f}$ является эпиморфизмом кольца многочленов $A[x]$ на кольцо многочленных функций $\overline{A[x]}$.

3°. Для конечного кольца A соответствие Φ изоморфизмом не является.

§ 3. Деление многочлена на двучлен $x-\alpha$. Схема Горнера

<u>Теорема 1</u>. Если $f \;\; A[x]$, $\alpha \;\; A$, то многочлен $f(x)$ можно, причём единственным образом, представить в виде

$$f = (x-\alpha)g(x)+r,$$

где $g \;\; A[x]$, $r \;\; A$. При этом $r = \overline{f}(\alpha)$.

Схема Горнера.

Разложение многочлена по степеням двучлена $x-\alpha$.

<u>Теорема 2</u>. Если $f \;\; A[x]$, $\alpha \;\; A$, то многочлен f можно, причём единственным образом, разложить по степеням двучлена $x-\alpha$.

§ 4. Корни многочлена. Число корней многочлена. Интерполяционные многочлены. Функциональное и алгебраическое равенство многочленов

В этом параграфе кольцо коэффициентов полагается целостным кольцом.

Теорема 1. Многочлен f делится на $x–\alpha$ тогда и только тогда, когда α является корнем f.

Теорема 2. Число корней ненулевого многочлена не превосходит степени этого многочлена.

Следствие. Многочлен степени не выше n однозначно определяется значениями своей многочленной функции в n+1 точках.

Интерполяционные многочлены Лагранжа. Интерполяционные многочлены Ньютона.

Теорема 3. Функциональное и алгебраическое равенство многочленов

Если кольцо A бесконечно, то $\Phi: f \mapsto \overline{f}$ – изоморфизм.

§ 5. Кратные корни многочлена

Понятие корня кратности k.

Теорема. Число корней многочлена с учётом их кратностей.

Сумма кратностей всех корней ненулевого многочлена не превосходит его степени, при этом равенство выполняется тогда и только тогда, когда многочлен разлагается на линейные множители.

Лемма 1. Всякий многочлен $f \quad A[x]$ может быть представлен в виде

$$f = (x–\alpha_1)^{k_1} (x–\alpha_2)^{k_2} \; ... \; (x–\alpha_s)^{k_s} g, \tag{1}$$

где α_1, α_2, ..., α_s – различные элементы кольца A, а g – многочлен, не имеющий корней в A.

Лемма 2. Если многочлен представлен в виде (1), то α_1, α_2, ..., α_s – это все его корни, причём кратность корня α_i равна k_i, $i = \overline{1, s}$.

Формулы Виета.

§ 6. Кольцо многочленов над полем

Теорема 1. Группа обратимых элементов кольца $P[x]$ есть P^*.

Теорема 2. Для любых двух многочленов f и $g \quad 0$ существует, причём единственная, пара многочленов h и r, удовлетворяющая условиям:

1) $f = g\ h+r$;
2) $r = 0 \quad \deg r < \deg g$.

НОД многочленов.

Теорема 3. Единственность НОД.

Любые два НОД системы многочленов совпадают, с точностью до скаляра, если они существуют.

(f, g).

Алгоритм Евклида.

Теорема 4. Существование НОД двух многочленов.

Для любых двух многочленов, не равных нулю одновременно, их НОД существует. Он равен последнему, отличному от нуля, остатку алгоритма Евклида для этих двух многочленов.

Следствие 1. Свойства НОД.

1°. С точностью до скаляра, $(f\,h, g\,h) = (f, g)h$.

2°. Если t – ОД (f, g), то, с точностью до скаляра, $\left(\frac{f}{t}, \frac{g}{t}\right) = \frac{(f, g)}{t}$.

3°. Если $d = (f, g)$, то $\left(\frac{f}{d}, \frac{g}{d}\right) = 1$.

4°. Если $d = (f, g)$, то существуют многочлены u, v такие, что $uf+vg = d$.

5°. Наибольший по степени общий делитель многочленов f и g является их НОД.

Теорема 5. Если многочлен h, кратный $d = (f, g)$, удовлетворяет условию

$$\deg h < \deg f + \deg g,$$

то существуют такие многочлены u, v, что

$$h = uf+vg,$$

причём

$$\deg u < \deg g,\ \deg v < \deg f.$$

Метод неопределённых коэффициентов для выражения НОД.

Теорема 6. Цепное правило.

НОД нескольких многочленов $f_1, f_2, \ldots, f_n$ существует. Он вычисляется по правилу $((\ldots((f_1, f_2), f_3), \ldots, f_{n-1}), f_n)$.

Следствие 2. Свойства НОД 1°–5° двух многочленов справедливы для любого конечного количества многочленов.

Взаимно простые многочлены

Теорема 7. Критерий взаимной простоты.

Многочлены f и g взаимно простые тогда и только тогда, когда существуют многочлены u и v такие, что $uf+vg = 1$.

Теорема 8. Свойства взаимно простых многочленов.

1°. $(f, h) = (g, h) = 1 \quad (fg, h) = 1$.
2°. $fg \,\vdots\, h \quad (f, h) = 1 \quad g \,\vdots\, h$.
3°. $f \,\vdots\, g \quad f \,\vdots\, h \quad (g, h) = 1 \quad f \,\vdots\, gh$.

Обобщение результатов теорем 1 и 2 на случай n многочленов.

НОК многочленов

ОК и НОК системы многочленов.

Теорема 9. Единственность НОК.

Любые два НОК системы многочленов совпадают, с точностью до скаляра, если они существуют.

$[f_1, f_2, \ldots, f_n]$.

Теорема 10. Существование НОК двух многочленов.

Для любых двух многочленов f и g, не равных нулю одновременно, их НОК существует. Он равен $\dfrac{fg}{(f, g)}$.

Следствие 3. Свойства НОК двух многочленов.

1°. С точностью до скаляра, $[fh, gh] = [f, g]h$.
2°. Если t – ОД(f, g), то, с точностью до скаляра, $\left[\dfrac{f}{t}, \dfrac{g}{t}\right] = \dfrac{[f, g]}{t}$.
3°. Наименьшее по степени общее кратное многочленов f и g является их НОК.

Теорема 11. Цепное правило.

НОК нескольких многочленов $f_1, f_2, \ldots, f_n$ существует. Оно вычисляется по правилу $[[\ldots[[f_1, f_2], f_3], \ldots, f_{n-1}], f_n]$.

Следствие 4. Свойства НОК 1°–3° двух многочленов справедливы для любого конечного количества многочленов.

§ 7. **Неприводимые многочлены. Факториальность кольца многочленов над полем**

Приводимые и неприводимые многочлены.

Теорема 1. Свойства неприводимых (простых) многочленов.

1°. p – простой $p \vdots f$ f P $f = cp$, где c P.

2°. Если p_1, p_2 – не асоциированные простые многочлены, то они не делятся друг на друга.

3°. p – простой $(\forall f)(f \vdots p$ $(f, p) = 1)$.

4°. $f_1 f_2 \dots f_n \vdots p$ p – простой $f_1 \vdots p$ $f_2 \vdots p$ $\dots$ $f_n \vdots p$.

Теорема 2. Теорема о факторизации.

Всякий многочлен ненулевой степени либо является простым многочленом, либо представляется в виде произведения простых многочленов, причем такое представление единственное, с точностью до скаляра и порядка следования множителей.

Каноническое разложение (факторизация) многочлена.

Следствие 1. Всякий составной многочлен имеет единственное каноническое разложение.

Следствие 2. Если f имеет каноническое разложение $f = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, то $g|f$ $g = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$, где 0 β_i α_i для всех $i = \overline{1, s}$.

Следствие 3. Правила отыскания НОД и НОК.

Пусть $f = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, $g = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ – почти канонические разложения многочленов f и g, то есть для всех $i = \overline{1, s}$ 0 α_i, 0 β_i причем одно из них 0. Тогда

1°. $(f, g) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}$, где $(\forall i = \overline{1, s})(\gamma_i = \min\{\alpha_i, \beta_i\}$.

2°. $[f, g] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_s^{\delta_s}$, где $(\forall i = \overline{1, s})(\delta_i = \max\{\alpha_i, \beta_i\}$.

§ 8. Производная многочлена

Теорема 1. Свойства производной.

1°. $(cf) = cf$, если c P.

2°. $(f+g) = f + g$.

3°. $(f\ g) = f\ g+f\ g$.

4°. $(f_1\ f_2\ \dots f_n) = f_1\ f_2\ \dots f_n + f_1\ f_2\ \dots f_n + \dots + f_1\ f_2\ \dots f_n$.

5°. $(f^n) = n f^{n-1} f$.

Теорема 2. Если p – неприводимый делитель кратности k 1 многочлена f, то p является делителем кратности k–1 производной f .

Следствие 1. Неприводимый делитель p многочлена f имеет кратность k 1 тогда и только тогда, когда p делит многочлен f и все его производные, до (k–1)-й, и не является делителем k-й производной.

Следствие 2. Элемент α поля является корнем многочлена кратности k тогда и только тогда, когда α является корнем многочлен f и всех его производных, до (k–1)-й, и не является корнем k-й производной.

Следствие 3. Неприводимый над полем P многочлен не имеет кратных корней над любым расширением этого поля.

Схема выделения кратных множителей.

§ 9. Кольцо многочленов над факториальным кольцом

Теорема 1. Группа обратимых элементов кольца $A[x]$ совпадает с группой обратимых элементов кольца A.

Теорема 2. Если кольцо A факториально, то кольцо $A[x]$ также факториально.

Примитивные многочлены. Содержание многочлена.

Лемма 1. Всякий многочлен $f \quad A[x]$ представляется в виде $f = d\varphi$, где $d \quad A$, φ – примитивный многочлен. Такое представление единственное, с точностью до ассоциированности над A.

Лемма 2. Всякий многочлен $g \quad P[x]$, где P – поле частных кольца A, представляется в виде $f = \frac{m}{n}\varphi$, где $m, n \quad A$, φ – примитивный многочлен.

Лемма 3. Всякий простой в $A[x]$ многочлен является примитивным многочленом. Наоборот, всякий примитивный многочлен является либо простым многочленом, либо представляется в виде произведения примитивных многочленов меньшей степени.

Лемма 4. Лемма Гаусса. Произведение примитивных многочленов также является примитивным многочленом.

Лемма 5. Если два примитивных многочлена ассоциированы над полем частных факториального кольца, то они ассоциированы и над самим этим кольцом.

Лемма 6. Если многочлен $f \quad A[x]$ приводим над полем частных P кольца A, то многочлен приводим и над A.

ГЛАВА 12. Кольцо многочленов от нескольких переменных

§ 1. Кольцо многочленов от *n* переменных

$A[x_1\, x_2, \ldots, x_{n-1}, x_n] = A[x_1\, x_2, \ldots, x_{n-1}][x_n]$.

Теорема 1. Наследование свойств кольца.

Если кольцо A коммутативно или ассоциативно, или содержит единицу, или является целостным кольцом, или факториальное кольцо, то этим же свойством обладает кольцо многочленов $A[x_1\ x_2, \ldots, x_{n-1}, x_n]$.

Степень многочлена относительно переменной x_i, степень многочлена относительно совокупности переменных. $\deg^{x_i} f$, $\deg^{\Sigma} f$. Однородные многочлены (формы) степени n.

Теорема 2. Свойства степени.

1°. $\deg^{x_i}(f \pm g) \quad \max\{\deg^{x_i} f, \deg^{x_i} g\}$; $\deg^{\Sigma}(f \pm g) \quad \max\{\deg^{\Sigma} f, \deg^{\Sigma} g\}$.

2°. $\deg^{x_i}(f \quad g) \quad \deg^{x_i} f + \deg^{x_i} g$; $\deg^{\Sigma}(f \quad g) \quad \deg^{\Sigma} f + \deg^{\Sigma} g$.

3°. Если кольцо A целостное, то

$\deg^{x_i}(f \quad g) = \deg^{x_i} f + \deg^{x_i} g$; $\deg^{\Sigma}(f \quad g) = \deg^{\Sigma} f + \deg^{\Sigma} g$.

Многочленная функция $\overline{f} : A^n \to A$, соответствующая многочлену $f = f(x_1\ x_2, \ldots, x_n)$.

Теорема 3. Свойства кольца многочленных функций.

1°. Множество $\overline{A[x_1, x_2, \ldots, x_n]}$ всех многочленных функций является подкольцом в кольце всех функций, отображающих A^n в A.

2°. Соответствие $\Phi : f \mapsto \overline{f}$ является эпиморфизмом кольца многочленов $A[x_1\ x_2, \ldots, x_n]$ на кольцо многочленных функций $\overline{A[x_1, x_2, \ldots, x_n]}$.

3°. Если кольцо A бесконечное, то Φ является изоморфизмом.

§ 2. Лексикографическое (алфавитное) упорядочение многочлена от *n* переменных

Лексикографический порядок на множестве (неподобных) одночленов многочлена. $\succ$.

Теорема. Свойства лексикографического порядка $\succ$.

1°. Отношение $\succ$ транзитивно.

2°. Отношение $\succ$ линейно.

3°. Отношение $\succ$ стабильно относительно умножения на одночлен.

Следствие. Лемма о высшем члене произведения.

Высший член произведения многочленов равен произведению высших членов множителей.

§ 3. Симметрические многочлены

Действие подстановки π на многочлен f. Симметрические многочлены. Элементарные симметрические многочлены. Степенные суммы.

Теорема 1. Множество $SA[x_1\, x_2, \dots, x_n]$ симметрических многочленов от n переменных образует подкольцо в кольце $A[x_1\, x_2, \dots, x_n]$ многочленов от n переменных.

Лемма 1. Если $ax_1^{\alpha_1} x_2^{\alpha_2} \ \dots \ x_n^{\alpha_n}$ – высший член симметрического многочлена в лексикографическом упорядочении, то последовательность его показателей степени составляет нестрого убывающую последовательность: $\alpha_1 \quad \alpha_2 \quad \dots \quad \alpha_n$.

Лемма 2. Для любого одночлена $ax_1^{\alpha_1} x_2^{\alpha_2} \ \dots \ x_n^{\alpha_n}$, показатели степени которого образуют нестрого убывающую последовательность: $\alpha_1 \quad \alpha_2 \quad \dots \quad \alpha_n$, существует, и, причём только один, одночлен от элементарных симметрических многочленов $a\sigma_1^{\beta_1}\sigma_2^{\beta_2} \dots \sigma_n^{\beta_n}$, старший член которого совпадает с этим одночленом.

Теорема 2. Основная теорема теории симметрических многочленов.

Всякий симметрический многочлен может быть представлен в виде многочлена от элементарных симметрических многочленов.

Теорема 3. Всякий симметрический многочлен единственным образом представляется в виде многочлена от элементарных симметрических многочленов.

Метод неопределённых коэффициентов для выражения однородного симметрического многочлена через элементарные симметрические многочлены.

Связь с формулами Виета.

Решение симметрических систем уравнений.

ГЛАВА 13. Многочлены над основными числовыми полями

§ 1. Кольцо многочленов над полем комплексных чисел

Теорема. Основная Теорема Алгебры.

Всякий многочлен ненулевой степени с комплексными коэффициентами имеет хотя бы один комплексный корень.

Следствие 1. Число корней многочлена с комплексными коэффициентами равна степени этого многочлена, если каждый корень считать столько раз, какова его кратность.

Следствие 2. Над полем комплексных чисел неприводимы только многочлены первой степени. Каноническое разложение многочлена над $\boldsymbol{C}$ имеет вид

$$a_n(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2} \dots (x-\alpha_s)^{k_s}\ .$$

Следствие 3. Над $\boldsymbol{C}$ $f \,\vdots\, g$ все корни g являются корнями f, при этом их кратности для g не превосходят кратностей для f.

§ 2. Кольцо многочленов над полем действительных чисел

Теорема 1. Если комплексное число α является корнем многочлена с действительными коэффициентами, то комплексно сопряжённое число $\overline{\alpha}$ также является корнем этого многочлена. При этом кратности α и $\overline{\alpha}$ совпадают.

Теорема 2. Над полем действительных чисел неприводимы только многочлены первой степени и многочлены второй степени с отрицательным дискриминантом. Каноническое разложение многочлена над $\boldsymbol{R}$ имеет вид

$$a_n(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\ \dots (x-\alpha_s)^{k_s}\ (x^2+p_1x+q_1)^{l_1}\ )(x^2+p_2x+q_2)^{l_2}\ \dots (x^2+p_tx+q_t)^{l_t}\ ,$$

где $p_i^2-4q_i<0$ для $i=\overline{1,t}$.

§ 3. Многочлены над полем рациональных чисел

Сведение вопросов отыскания рациональных корней и разложения на множители многочленов над $\boldsymbol{Q}$ к многочленам над $\boldsymbol{Z}$.

Теорема 1. Если $f(x) = a_nx^n+a_{n-1}x^{n-1}+ \dots +a_1x+a_0$ $\boldsymbol{Z}[x]$ и рациональное число $\alpha = \dfrac{p}{q}$, где p и q – взаимно простые числа, является корнем f , то $a_0 \vdots p$, $a_n \vdots q$.

Теорема 2. Если $f(x)$ $\boldsymbol{Z}[x]$ и рациональное число $\alpha = \dfrac{p}{q}$, где p и q – взаимно простые числа, является корнем f , то $(\forall m$ $\boldsymbol{Z})(\overline{f(m)} \vdots (p-mq))$.

Теорема 3. Критерий неприводимости Эйзенштейна.

Если $f(x) = a_nx^n+a_{n-1}x^{n-1}+ \dots +a_1x+a_0$ $\boldsymbol{Z}[x]$ и существует такое простое число p, что a_n не делится на p, все остальные коэффициенты делятся на p и a_0 не делится на p^2, то многочлен f неприводим над $\boldsymbol{Z}$, а, следовательно, и над $\boldsymbol{Q}$.

ГЛАВА 14. Расширения числовых полей. Алгебраические числа

§ 1. Простое расширение $P(\alpha)$ поля P

Теорема 1. Строение $P(\alpha)$.

Всякий элемент простого расширения поля P с помощью элемента α представляется в виде отношения значений от α многочленных функций над P:

$$P(\alpha) = \{\beta : (\exists \overline{f})(\exists \overline{g})(\beta = \frac{\overline{f}(\alpha)}{\overline{g}(\alpha)} \quad \overline{f} \in \overline{P[x]} \quad \overline{g} \in \overline{P[x]})\}.$$

Алгебраические и трансцендентные над полем P элементы.

Теорема 2. Строение простого трансцендентного расширения.

Если α – трансцендентный над полем P элемент, то каждый элемент из $P(\alpha)$ единственным образом представляется в виде $\beta = \dfrac{\overline{f}(\alpha)}{\overline{g}(\alpha)}$, где f и g – взаимно простые многочлены и g – нормированный многочлен.

Примитивный многочлен алгебраического элемента.

Теорема 3. Строение простого алгебраического расширения.

Пусть α – алгебраический над полем P элемент. Тогда

1°. Минимальный многочлен φ элемента α неприводим над P.

2°. Если $\deg \varphi = n$, то всякий элемент β $P(\alpha)$ представляется в виде $\beta = \overline{f}(\alpha)$, где f $P[x]$ и $\deg f < n$.

3°. Представление 2° единственно.

Освобождение от алгебраической иррациональности в знаменателе дроби.

§ 2. Последовательное (цепное) расширение поля. Расширение поля конечной совокупностью элементов

$P(\alpha_1)(\alpha_2) \ldots (\alpha_n)$. $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Теорема 1. $P(\alpha_1)(\alpha_2) \ldots (\alpha_n) = P(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Теорема 2. Строение $P(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Всякий элемент расширения поля P с помощью элементов $\alpha_1, \alpha_2, \ldots, \alpha_n$ представляется в виде отношения значений от $\alpha_1, \alpha_2, \ldots, \alpha_n$ многочленных функций над P: $P(\alpha_1, \alpha_2, \ldots, \alpha_n) =$

$$= \left\{ \beta \,\middle|\, (\exists f)(\exists g)(\beta = \frac{\overline{f}(\alpha_1, \alpha_2, \ldots, \alpha_n)}{\overline{g}(\alpha_1, \alpha_2, \ldots, \alpha_n)} \wedge f \in P[x_1, x_2, \ldots, x_n] \wedge g \in P[x_1, x_2, \ldots, x_n] \right\}.$$

§ 3. Конечное расширение поля

Расширение поля как векторное пространство над этим полем. $\dfrac{K}{P}$.

Теорема 1. Критерий конечности простого расширения.

Поле $P(\alpha)$ является конечным расширением тогда и только тогда, когда элемент α является алгебраическим над полем P.

Теорема 2. Свойства конечных расширений.

1°. Если кольцо A, являющееся расширением поля P, является конечномерным векторным пространством над P, то всякий элемент из A является алгебраическим над полем P.

2°. Всякое кольцо, являющееся конечномерным векторным пространством над полем P, является полем.

3°. Транзитивность конечного расширения. Если K – конечное расширение поля P, а L – конечное расширение поля K, то L является конечным расширением поля P, причём выполняется равенство $\frac{L}{P} = \frac{L}{K}\,\frac{K}{P}$.

§ 4. Алгебраические над полем *P* элементы

<u>Теорема 1</u>. Множество алгебраических над полем P элементов является полем.

<u>Теорема 2</u>. Поле алгебраических над полем P элементов алгебраически замкнуто.

§ 5. Простота конечных расширений

<u>Теорема</u>. Всякое конечное расширение числового поля является простым алгебраическим расширением этого поля.

<u>Лемма</u>. Если α и β – алгебраические над полем P элементы, то существует элемент γ, также алгебраический над P, для которого выполняется равенство $P(\alpha)(\beta) = P(\gamma)$.

Идея доказательства.

Если φ_α и φ_β минимальные многочлены чисел α и β, имеющие корни $\alpha_1 = \alpha$, α_2, ..., α_n и $\beta_1 = \beta$, β_2, ..., β_m, соответственно, то ищут γ в виде $\gamma = \alpha + c\beta$, где c $\boldsymbol{Q}$, c $\{\frac{\alpha_i - \alpha}{\beta - \beta_j} : i = \overline{1,n}, j = \overline{2,m}\}$ и доказывают, что $\psi(x) = \varphi_\alpha(\gamma - cx)$ имеет с φ_β НОД, равный $x - \beta$.

ГЛАВА 15. Группы

§ 1. Теорема о факторизации

Отношение равнóбразности. ρ_f. Естественная сюръекция множества A на фактор-множество A/ρ.

<u>Теорема о факторизации</u>. Пусть f: $A \to B$ – сюръекция, $\rho = \rho_f$ – соответствующее f отношение равнóбразности, $C = A/\rho$ – соответствующее ρ фактор-множество, φ –

естественная сюръекция A на фактор-множество A/ρ. Тогда существует, причём единственная, биекция $\theta\colon C \to B$, обладающая свойством $f = \theta\circ\varphi$.

§ 2. Алгебраические операции. Алгебры. Алгебраические системы. Изоморфизмы. Гомоморфизмы

Понятия бинарной и n-местной алгебраической операции. Алгебры. Алгебраические системы. Сигнатура. Подалгебры. Подсистемы. Прямое (декартово) произведение алгебр. Отображения алгебр и алгебраических систем. Изоморфизмы. Эпиморфизмы. Гомоморфизмы.

Теорема 1. Свойства изоморфизма.

1°. Тождественное отображение алгебры является изоморфизмом.

2°. Отображение, обратное изоморфизму, является изоморфизмом.

3°. Композиция двух изоморфизмов является изоморфизмом.

Отношение изоморфизма. $\cong$.

Теорема 2. Отношение изоморфизма в классе алгебр данной сигнатуры является отношением эквивалентности.

Некоторые свойства бинарных операций: коммутативность, ассоциативность, нейтральные элементы, аннулирующие элементы, обратные элементы, обратимость операции; дистрибутивности. Полугруппы. Квазигруппы. Лупы.

Теорема 3. Эпиморфизмы сохраняют перечисленные свойства бинарных операций.

§ 3. Определения, примеры, простейшие свойства групп

Включает всё содержание § 2.1. Два определения группы.

Примеры групп.

1. Группы чисел по сложению из § 2.1.
2. Группы чисел по умножению из § 2.1, $\boldsymbol{C}^*$, $\sqrt[n]{1}$.
3. $\boldsymbol{R}^n; +$, $M_{m\times n}; +$.
4. $GL(n, \boldsymbol{R})$.
5. S_n.
6. Группа $P(M)$ из § 2.1.
7. Группы движений, подобий, аффинных и проективных преобразований в геометрии.
8. Группы биекций некоторого множества, преобразующих некоторое подмножество этого множества в себя.

Теорема. Некоторые конструкции.

1°. Прямое (декартово) произведение групп также является группой.

2°. Эпиморфный образ группы также является группой.

3°. Алгебра, изоморфная группе, сама является группой.

§ 4. Целые степени элемента группы. Порядок элемента группы. Циклические группы

Определение целой степени элемента группы.

<u>Теорема 1</u>. Свойства целой степени элемента группы.

1°. $(a^{-1})^n = (a^n)^{-1}$ для любого n $\boldsymbol{N}$.

2°. $a^m a^n = a^{m+n}$ для любых m, n $\boldsymbol{Z}$.

3°. $(a^m)^n = a^{m\,n}$ для любых m, n $\boldsymbol{Z}$.

Порядок элемента группы. ord a.

<u>Теорема 2</u>. Свойства порядка.

Пусть ord $a = n$. Тогда

1°. Элементы $a^0 = e$, a, a^2, ..., a^{n-1} различны и любая целая степень элемента a совпадает с одним из этих элементов.

2°. $a^k = a^l$ тогда и только тогда, когда $k{-}l \,\vdots\, n$.

3°. $a^k = e$ тогда и только тогда, когда $k \,\vdots\, n$.

4°. При 0 k, $l < n$ $a^k\,a^l = \begin{cases} a^{k+l}, \text{ если } k + l < n, \\ a^{k+l-n}, \text{ если } k + l \geq n. \end{cases}$

Определение циклической группы. a .

Примеры циклических групп: $\boldsymbol{Z}$; + , $\sqrt[n]{1}$; .

<u>Теорема 3</u>. Изоморфизм циклических групп.

1°. Любые две циклические группы порядка n изоморфны.

2°. Любые две циклические группы бесконечного порядка изоморфны.

§ 5. Подгруппы

Повторяет содержание § 2.2.

<u>Теорема 3</u>. О подгруппах циклической группы.

Любая подгруппа циклической группы также является циклической группой.

Пересечение и объединение групп. Объединение возрастающей цепочки подгрупп.

§ 6. Теорема Кэли

Теорема. Любая группа G изоморфна некоторой подгруппе группы биекций некоторого множества. В частности, любая конечная группа порядка n изоморфна некоторой подгруппе группы S_n.

Этапы доказательства

1. $\lambda_a: x \mapsto ax$ – биекция G в G. 2. $\overline{G} = \{\lambda_a: a \quad G\}$ – подгруппа в $P(G)$.

3. $\Phi: a \mapsto \lambda_a$ – изоморфизм G на $\overline{G}$.

§ 7. Разбиение группы по подгруппе. Теорема Лагранжа

Умножение подмножеств группы. H_1H_2. Ha. aH.

Теорема 1. Свойства умножения подмножеств.

1°. Умножение подмножеств ассоциативно.

2°. Если H – подгруппа группы G, то $Ha = H$ тогда и только тогда, когда $a \quad H$.

3°. Если H – подгруппа группы G, то отображение $\rho_a: H \to Ha$ по правилу $h \mapsto ha$ является биекцией. В частности, если H – конечная подгруппа, то $|H| = |Ha|$.

Отношение ρ_H правой смежности: $a\rho_H b \qquad Ha = Hb$.

Теорема 2. Свойства отношения правой смежности.

1°. Отношение ρ_H является отношением эквивалентности.

2°. Если K_a – класс эквивалентности, порождённый элементом a, то $K_a = Ha$.

Теорема 3. Теорема Лагранжа.

Порядок конечной группы делится на порядок любой её подгруппы.

Теорема 4. Если G – конечная циклическая группа порядка n и d произвольный делитель числа n , то существует подгруппа H группы G порядка d.

§ 8. Нормальные подгруппы. Фактор-группы. Естественный эпиморфизм

Примеры и контрпримеры нормальных подгрупп.

Теорема 1. Критерий нормальной подгруппы.

Подгруппа H группы G является нормальной подгруппой тогда и только тогда, когда выполняется условие: $x \quad G \ h \quad H \qquad x^{-1}hx \quad H$.

Теорема-определение 2. Множество правых (= левых) смежных классов группы G по нормальной подгруппе H является группой относительно операции $\circ$, определённой правилом $Ha \circ Hb = Hab$. Эта группа называется фактор-группой группы G по нормальной подгруппе H: $G/H; \circ$.

Теорема-определение 3. Отображение $\varphi: a \qquad Ha$ группы G на фактор-группу G/H является эпиморфизмом. Этот эпиморфизм называется естественным эпиморфизмом группы G на фактор-группу G/H.

§ 9. Гомоморфизмы и эпиморфизмы групп. Теорема об эпиморфизмах

Определение, примеры и простейшие свойства гомоморфизма групп. Ядро гомоморфизма. Ker f.

Теорема 1. Критерий нормальной подгруппы.

Подгруппа H группы G является нормальной подгруппой тогда и только тогда, когда существует гомоморфизм группы G, ядром которого является H.

Теорема 2. Если f: $G \to G_1$ – гомоморфизм групп и H = Ker f – ядро гомоморфизма, то для любого a_1 G_1 его полный прообраз $f^{-1}(a_1)$ является либо пустым множеством, либо представляет собой смежный класс группы G по подгруппе H.

Теорема 3. Теорема об эпиморфизмах.

Если f: $G \to G_1$ – эпимоморфизм групп, H = Ker f, φ: $G \to G/H$ – естественный эпиморфизм, то существует, и причём единственный, изоморфизм θ: $G/H \to G_1$, обладающий свойством $f = \theta \circ \varphi$.

ГЛАВА 16. Кольца и поля

§ 1. Кольца и поля

Примеры колец: $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}[x]$, $M_{n\times n}$, R^3; +, . Особенности этих примеров.

Нулевой и единичный элементы, противоположный и обратный элементы.

Теорема 1. Свойства противоположных и обратных.

Совпадает с теоремой 2.3.1.

Теорема 2. О расщеплении.

Совпадает с теоремой 2.3.2.

Разность и частное: $a–b$, $\frac{a}{b}$.

Теорема 3. Свойства разности.

1°. $(a–b)+b = a$.
2°. $a–b = a+(–b)$.
3°. $0–a = –a$.
4°. $a+(b–c) = (a+b)–c$.
5°. $a–b = c–d \leftrightarrow a+d = b+c$.

6°. $a-b = a \leftrightarrow b = 0$.
7°. $a-b = 0 \leftrightarrow a = b$.
8°. $a-(-b) = a+b$.
9°. $a-(b+c) = (a-b)-c$.
10°. $a-(b-c) = (a-b)+c$.
11°. $(a-b)+(c-d) = (a+c)-(b+d)$.
12°. $(a-b)-(c-d) = (a+d)-(b+c)$.

<u>Теорема 4</u>. Законы сокращения.

1°. В кольце $a+b = a+c \to b = c$.
2°. В поле $a\ b = a\ c \to a = 0 \quad b = c$.

<u>Теорема 5</u>. Следствия аксиомы дистрибутивности.

1°. $a\ 0 = 0\ a = 0$.
2°. $(a-b)c = ac-bc$.
3°. $(-a)b = a(-b) = -ab$.
4°. $(-a)(-b) = ab$.
5°. $a-b = c-d \leftrightarrow a+d = b+c$.
6°. $a-b = a \leftrightarrow b = 0$.
7°. $(a-b)\,(c-d) = (ac+bd)-(bc+ad)$.

<u>Теорема 6</u>. Условия обратимости и равенства нулю в поле.

1°. $a\ b = 0 \leftrightarrow a = 0 \quad b = 0$.
2°. $\frac{a}{b} = 0 \leftrightarrow a = 0 \quad b \quad 0$.
3°. 0 не обратим; a обратим $\leftrightarrow a \quad 0$.
4°. Если a обратим, то $-a$ тоже обратим, причем $(-a)^{-1} = -a^{-1}$.

<u>Теорема 7</u>. Свойства частного в поле.

Пусть $b \quad 0$ и $d \quad 0$. Тогда

1°. $\frac{a}{b}\ b = a$.
2°. $\frac{a}{b} = a\ b^{-1}$.
3°. $\frac{1}{b} = b^{-1}$.
4°. $a\ \frac{c}{b} = \frac{ac}{b}$.
5°. $\frac{a}{b} = \frac{c}{d} \leftrightarrow ad = bc \quad b \quad 0 \quad d \quad 0$.

6°. $\frac{a}{b} = a \leftrightarrow b = 1 \quad a = 0$.

7°. $\frac{a}{b} = 1 \leftrightarrow a = b \quad b \quad 0$.

8°. $\frac{a}{b^{-1}} = a\ b$.

9°. $\left(\frac{b}{d}\right)^{-1} = \frac{d}{b}$.

10°. $\frac{ad}{bd} = \frac{a}{b}$.

11°. $\frac{a}{bd} = \frac{a}{b} : d$.

12°. $a : \frac{b}{d} = \frac{ad}{b}$.

13°. $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$.

14°. $\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$.

15°. $\frac{a}{b}\ \frac{c}{d} = \frac{ac}{bd}$.

16°. Если $c \quad 0$, то $\frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}$.

Изоморфизм колец и полей. Отношение изоморфизма $\cong$.

Теорема 8. Свойства изоморфизма колец и полей.
Совпадает с теоремой 2.3.3.

Гомоморфизмы и эпиморфизмы колец. Примеры. Простейшие свойства гомоморфизмов.

Теорема 9. Некоторые конструкции.

1°. Прямое (декартово) произведение колец также является кольцом.
2°. Эпиморфный образ кольца также является кольцом.
3°. Алгебра, изоморфная кольцу (полю), сама является кольцом (полем).

§ 2. Подкольца и подполя

Включает всё содержание § 2.4.

Теорема 4. Особенности числовых подколец и подполей.

1°. Кольцо целых чисел является наименьшим числовым кольцом с единицей.
2°. Поле рациональных чисел является наименьшим числовым полем.
3°. Всякий изоморфизм числовых полей действует тождественно на множестве рациональных чисел.

§ 3. Характеристика кольца с единицей

Понятие характеристики кольца с единицей.

Теорема. Пусть n – ненулевая характеристика кольца A. Тогда

1°. $(\forall a)(na = 0)$.
2°. Если A – поле, то n – простое число.

§ 4. Упорядоченные кольца и поля

Определение упорядоченного кольца и упорядоченного поля. (OA), (OM). Линейно упорядоченные кольца и поля.

Теорема 1. Свойства упорядоченных колец и полей.

1°. $a \quad b \leftrightarrow b-a \quad 0 \leftrightarrow -b \quad -a$.
2°. $a+b \quad c \leftrightarrow a \quad c-b$; $a-b \quad c \leftrightarrow a \quad c+b$.
3°. а) $a \quad b \quad c \quad d \rightarrow a+c \quad b+d$; б) $a \quad b \quad c < d \rightarrow a+c < b+d$;
в) $a < b \quad c \quad d \rightarrow a+c < b+d$
4°. $0 \quad a \quad b \quad 0 \quad c \quad d \rightarrow a\,c \quad b\,d$.

Теорема 2. Свойства линейно упорядоченных колец и полей.

1°. В линейно упорядоченном кольце
а) $a^2 \quad 0$; $a \quad 0 \rightarrow a^2 > 0$;
б) $-1 < 0 < 1$;
в) нет ни наибольшего, ни наименьшего элементов;
г) если $c > 0$, то $a < b \leftrightarrow ac < bc$;
д) если $c < 0$, то $a < b \leftrightarrow ac > bc$;
е) если $a > 0$, $b > 0$, то $a < b \leftrightarrow a^2 < b^2$.
2°. В линейно упорядоченном поле
а) $\frac{a}{b} > 0 \leftrightarrow ab > 0 \leftrightarrow a > 0 \quad b > 0 \quad a < 0 \quad b < 0$;
б) $a > 0 \leftrightarrow a^{-1} > 0$;
в) если $ab > 0$, то $a < b \leftrightarrow a^{-1} > b^{-1}$;
г) если $a < b$, то $a < \frac{a+b}{2} < b$.

Модуль элемента линейно упорядоченного кольца. $|a|$.

Теорема 3. Простейшие свойства модуля.

1°. $|a| \geq 0$.

2°. $|a| = 0 \leftrightarrow a = 0$.

3°. $|a| = \max\{a, -a\}$.

4°. $|a| = |-a|$.

5°. $-|a| \leq a \leq |a|$.

6°. $|a|^2 = a^2$; $|a| < |b| \leftrightarrow a^2 < b^2$.

Теорема 4. Освобождение от модуля в равенстве и неравенствах.

1°. $|a| = b \leftrightarrow b \geq 0 \quad (a = b \quad a = -b)$.

2°. $|a| < b \leftrightarrow -b < a < b$.

3°. $|a| > b \leftrightarrow a > b \quad a < -b$.

Теорема 5. Связь модуля с операциями.

1°. $|a \cdot b| = |a| \cdot |b|$.

2°. В поле если $b \neq 0$, то $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$.

3°. $|a+b| \leq |a| + |b|$.

4°. $\big||a| - |b|\big| \leq |a-b|$.

5°. $\big||a| - |b|\big| \leq |a \pm b| \leq |a| + |b|$.

§ 5. Свойства порядка натуральных, целых и рациональных чисел

Теорема 1. Дискретность $\boldsymbol{N}$.

Пусть m, n – произвольные натуральные числа. Тогда

1°. $n \quad 1$.

2°. $n > 1 \leftrightarrow n-1 \quad \boldsymbol{N}$.

3°. $m > n \leftrightarrow m-n \quad \boldsymbol{N}$.

4°. $m > n \leftrightarrow m \quad n-1$.

5°. $m+1 > n \leftrightarrow m \quad n$.

6°. $\quad (m < n < m+1)$.

Теорема 2.

1°. Принцип наименьшего числа. Любое непустое подмножество в $\boldsymbol{N}$ имеет наименьший элемент.

2°. Множество $\boldsymbol{N}$ не ограничено сверху в $\boldsymbol{R}$.

Теорема 3. Первые свойства порядка на $\boldsymbol{Z}$.

Пусть m, n – произвольные целые числа. Тогда

1°. $n > 0 \leftrightarrow n \quad \boldsymbol{N}$.

2°. $n = 0 \quad n \quad \boldsymbol{N} \quad -n \quad \boldsymbol{N}$.

3°. Дискретность $\boldsymbol{Z}$: а) $m > n \leftrightarrow m \quad n-1$;

б) $m+1 > n \leftrightarrow m \quad n$;

в) $\quad (m < n < m+1)$.

Теорема 4.

1°. Всякое непустое ограниченное снизу подмножество из $\boldsymbol{Z}$ имеет наименьший элемент.

2°. Всякое непустое ограниченное сверху подмножество из $\boldsymbol{Z}$ имеет наибольший элемент.

3°. Множество $\boldsymbol{Z}$ не ограничено сверху и снизу в $\boldsymbol{R}$.

Целая и дробная части числа. $[a]$. $\{a\}$.

Теорема 5. Всякое действительное число обладает целой частью.

Теорема 6. Свойства порядка на $\boldsymbol{Q}$.

1°. Порядок на $\boldsymbol{Q}$ плотный.

2°. $\boldsymbol{Q}$ не ограничено сверху и снизу в $\boldsymbol{R}$.

3°. $\boldsymbol{Q}$ плотно в $\boldsymbol{R}$.

Теорема 7. Принцип Архимеда.

1°. $(\forall a)(\forall b>0)(\exists n \quad \boldsymbol{N})(nb > a)$.

2°. $(\forall a)(\forall b>1)(\exists n \quad \boldsymbol{N})(a < b^n)$.

3°. $(\forall a)(\forall b>0)(\exists n \quad \boldsymbol{Z})(nb \quad a < (n+1)b)$.

4°. $(\forall a)(\forall b>1)(\exists n \quad \boldsymbol{Z})(b^n \quad a < b^{n+1})$.

Теорема 8. Поле $\boldsymbol{C}$ невозможно превратить в линейно упорядоченное поле.

Теорема 9. Кольцо $\boldsymbol{Z}$ и поле $\boldsymbol{Q}$ допускают только единственное линейное упорядочение.

§ 5. Идеалы коммутативных колец

Определение идеала.

Примеры идеалов.

1. 0 и A.

2. Главные идеалы. (a).

Пересечение, сумма, объединение возрастающей цепочки идеалов. Идеал, порождённый множеством M: (M).

Теорема. Свойства операций над идеалами.

1°. Пересечение, сумма, объединение возрастающей цепочки идеалов также являются идеалами.

2°. Объединение идеалов, вообще говоря, не является идеалом.

3°. Наименьший идеал $I(M)$ кольца A, содержащий подмножество M кольца, совпадает с идеалом (M) порождённым множеством M.

§ 6. Сравнение по идеалу. Фактор-кольца

Сравнение по идеалу. $a \quad b$ (mod I).

Теорема 1. Свойства сравнения по идеалу.

1°. Сравнение по идеалу является отношением эквивалентности.

2°. Сравнение по идеалу согласуется со сложением.

3°. Сравнение по идеалу согласуется с умножением.

4°. Классы эквивалентности отношения сравнения по идеалу имеют вид $K_a = I+a$.

Теорема-определение 2. Множество A/I классов эквивалентности является кольцом относительно операций и , которые определяются следующим образом: $(I+a) \quad (I+b) = I+(a+b)$, $(I+a) \quad (I+b) = I+(a\ b)$.

Это кольцо называется фактор-кольцом кольца A по идеалу I: A/I; , .

Кольца классов вычетов. $\boldsymbol{Z}_m = \boldsymbol{Z}/(m)$

Теорема 3. Строение колец классов вычетов.

1°. Если m – число простое, то $\boldsymbol{Z}_m$ – поле.

2°. Если m – число составное, то $\boldsymbol{Z}_m$ содержит делители нуля.

3°. Всякий ненулевой элемент кольца $\boldsymbol{Z}_m$ является либо делителем нуля, либо делителем единицы (обратимым элементом).

4°. $\boldsymbol{G}^{\mathbf{Z}_m} = \{\bar{a} : (a, m) = 1\}$.

§ 6. Гомоморфизмы и эпиморфизмы колец. Теорема об эпиморфизмах

Определение, примеры, простейшие (групповые) свойства гомоморфизма колец. Ядро гомоморфизма. $\mathrm{Ker}\, f$.

Теорема 1. Ядро гомоморфизма является идеалом кольца.

Теорема-определение 2. Отображение φ: $A \to A/I$ по правилу $\varphi(a) = I+a$ является эпиморфизмом колец. Этот эпиморфизм называется естественным эпиморфизмом кольца A на фактор-кольцо A/I.

Теорема 5. Теорема об эпиморфизмах.

Если f: $A \to A_1$ – эпимоморфизм колец, I = Ker f, φ: $A \to A/I$ – естественный эпиморфизм, то существует, и причём единственный, изоморфизм θ: $A/I \to A_1$, обладающий свойством $f = \theta\circ\varphi$.

ГЛАВА 17. Элементы теории делимости в целостных кольцах

§ 1. Отношение делимости в целостных кольцах.

Стандартные свойства отношения делимости.

Обратимые элементы (делители единицы) кольца.

Теорема 1. Множество G обратимых элементов кольца образует коммутативную группу относительно операции умножения.

Отношение ассоциированности. ~.

Простые и составные элементы кольца.

Теорема 2. Свойства отношения ассоциированности.

1°. Критерий ассоциированности: $a \sim b$ $a \vdots b$ $b \vdots a$.
2°. Отношение ассоциированности является отношением эквивалентности.
3°. Классы эквивалентности по отношению ассоциированности имеют вид $K_a = aG$.
4°. $a \sim a_1$ $b \sim b_1$ $a \vdots b$ $a_1 \vdots b_1$.
5°. $p \sim a$ p – простой элемент a – простой элемент.
6°. $a \sim b$ a – составной элемент b – составной элемент.

Теорема 3. Связь главных идеалов с теорией делимости.

1°. $a \vdots b$ (a) (b).
2°. $a \sim b$ $(a) = (b)$.

Делимость идеалов. НОД и НОК идеалов.

Теорема 4. Существование НОД и НОК идеалов.

1°. Любые два идеала кольца имеют НОД. Им является сумма этих идеалов.
2°. Любые два идеала кольца имеют НОК. Им является пересечение этих идеалов.

§ 2. Разложение на простые множители в кольцах

Разложение на простые множители: по существу, одинаковые; существенно различные. Кольца с однозначным разложением (= факториальные кольца). Кольца с неоднозначным разложением. Кольца без разложения. КОР. КНОР. КБР.

Примеры.

1. $\boldsymbol{Z}$ – кольцо с однозначным разложением (ММИ по модулю числа).

2. $\boldsymbol{Z}[\sqrt{-3}\,]$ – кольцо с неоднозначным разложением.

Разложимость доказывается ММИ по величине нормы, неоднозначность следует из того, что $4 = 2\ 2 = (1+\sqrt{-3}\,)(1-\sqrt{-3}\,)$, при этом числа 2, $1+\sqrt{-3}$ и $1-\sqrt{-3}$ – простые неассоциированные элементы.

3. $\{\boldsymbol{Z}[\sqrt[2^k]{2}\,]: k\ \ \boldsymbol{N}\}$ – кольцо без разложения: элемент 2 не имеет конечного разложения на простые множители.

§ 3. Кольца главных идеалов

Примеры.

1. $\boldsymbol{Z}$ является кольцом главных идеалов.

2. $\boldsymbol{R}[x, y]$ не является кольцом главных идеалов: $(x)+(y)$ не является главным идеалом.

Теорема 1. В кольце главных идеалов

1°. Любые два элемента имеют НОД и имеют НОК.

2°. Любые два НОД и НОК элементов ассоциированные.

3°. Если d – НОД элементов a и b, то найдутся u, v такие, что выполняется равенство $d = ua+vb$.

Взаимно простые элементы.

Теорема 2. Свойства взаимно простых элементов.

1°. Критерий взаимной простоты. Элементы a и b кольца главных идеалов взаимно просты тогда и только тогда, когда существуют u, v, такие, что выполняется равенство $1 = ua+vb$.

2°. Если элементы a и c, а также b и с – взаимно простые, то элементы $a\ b$ и c – также взаимно простые.

3°. Если $a\ b \vdots c$ и a и c – взаимно простые элементы, то $b \vdots c$.

4°. Если $c \vdots a$, $c \vdots b$ и a и b – взаимно простые элементы, то $c \vdots a\ b$.

Обобщение свойств 1°–4° на любое конечное число элементов.

Контрпримеры к свойствам 3° и 4° для не взаимно простых элементов.

Простые элементы.

Теорема 3. Свойства простых элементов.

1°. $p \,\vdots\, a$ p – простой элемент a G $a \sim p$.

2°. Если p_1 и p_2 – простые элементы и они не ассоциированные, то ни один из них не делится на другой.

3°. $(\forall a)(\forall p)$(p – простой элемент $\to$ $a \,\vdots\, p$ a и p – взаимно простые элементы).

4°. $a_1 a_2 \ldots a_n \,\vdots\, p$ p – простой элемент $a_1 \,\vdots\, p$ $a_2 \,\vdots\, p$ … $a_n \,\vdots\, p$.

Теорема 4. В кольце главных идеалов последовательность элементов $a_1, a_2, \ldots, a_n, \ldots$, в которой каждый элемент является делителем предыдущего и не ассоциирован с ним, содержит конечное число элементов.

Теорема 5. Всякое кольцо главных идеалов является факториальным кольцом.

Лемма. В кольце главных идеалов всякий необратимый элемент, отличный от нуля, обладает простым делителем.

§ 4. Евклидовы кольца

Определение евклидова кольца. Норма.
Примеры евклидовых колец.
1. $\boldsymbol{Z}$. **2**. $\boldsymbol{R}[x]$. **3**. $\boldsymbol{Z}[i]$.

Теорема 1. Всякое евклидово кольцо является кольцом главных идеалов.

Теорема 2. В евклидовом кольце последний ненулевой остаток обобщённого алгоритма Евклида двух элементов является НОД этих элементов.

ГЛАВА 4. Поле частных целостного кольца

§ 1. Определение и строение поля частных целостного кольца

Определение поля частных. Поле частных кольца $\boldsymbol{Z}$. Поле частных кольца $\boldsymbol{R}$.

Теорема 1. Строение поля частных.

Любой элемент поля частных целостного кольца A представляется в виде частного элементов этого кольца.

Теорема 2. Изоморфизм полей частных.

Если целостные кольца A_1 и A_2 изоморфны, то поля частных этих колец также изоморфны, если они существуют.

§ 2. Существование поля частных целостного кольца

Теорема. Любое целостное кольцо имеет поле частных.

Этапы построения поля частных.

1. Алгебра пар $A \quad A^*$; $+$, : коммутативность и ассоциативность операций; не дистрибутивность; наличие нейтральных элементов; необратимость каждой из операций.

2. Отношение сравнения ~ между парами: ~ – отношение эквивалентности, стабильное относительно операций.

3. Фактор-кольцо $A \quad A^*/\sim$; , : фактор-кольцо является полем.

4. Подкольцо фактор-кольца $\overline{A} = \{\overline{(a, 1)} : a \quad A\}$: $\overline{A} \cong A$.

5. Фактор-кольцо $A \quad A^*/\sim$; , является полем частных кольца $\overline{A}$.

Приложение

1°. <u>Использование теоремы о числе корней ненулевого многочлена</u>

1. Доказать тождество:

а) $(x-y)(xz+1)(yz+1)+(y-z)(yx+1)(zx+1)+(z-x)(zy+1)(xy+1) = (x-y)(y-z)(z-x)$;

б) $\dfrac{a(x-b)(x-c)}{(a-b)(a-c)}+\dfrac{b(x-a)(x-c)}{(b-a)(b-c)}+\dfrac{c(x-a)(x-b)}{(c-a)(c-b)}=x.$

2. Разложить на множители выражение:

а) $a^3(b-c)(c-d)(d-b)-b^3(c-d)(d-a)(a-c)+c^3(d-a)(a-b)(b-d)-d^3(a-b)(b-c)(c-a)$;

б) $(a-b)^3+(b-c)^3+(c-a)^3$;

в) $4(a^2c+c^2b+b^2a)-2(a^2b+b^2c+c^2a)-7abc$;

г) $(a+b+c)(ab+bc+ca)-abc$;

д) $ab(a-b)-ac(a+c)+bc(2a-b+c)$;

е) $a^2(b-c)+b^2(c-a)+c^2(a-b)$;

ж) $a^3(b-c)+b^3(c-a)+c^3(a-b)$;

з) $ab(a^2-b^2)+bc(b^2-c^2)+ca(c^2-a^2)$.

3. Доказать, что функция sin не является многочленом.
4. Пусть a, b, c–различные числа. Легко проверить, что эти числа являются корнями многочлена $\dfrac{(x-b)(x-c)}{(a-b)(a-c)}+\dfrac{(x-a)(x-c)}{(b-a)(b-c)}+\dfrac{(x-a)(x-b)}{(c-a)(c-b)}-1.$

Нет ли здесь противоречия с теоремой о числе корней многочлена?

2°. <u>Доказательство неравенств</u>

А. Выделение полного квадрата

1. Доказать, что для любых чисел a , b , c справедливо неравенство $a^2+b^2+c^2 \geq ab+bc+ca$, причем равенство выполняется, если только $a = b = c$.
2. Доказать, что для любых a справедливо неравенство $a^4-a+0,5 > 0$.
3. Известно, что уравнение $x^4+ax^3+2x^2+bx+1 = 0$ имеет хотя бы один корень. Доказать, что справедливо неравенство $a^2+b^2 \geq 8$.
4. $a^2+b^2-2ab+2a-2b+1 \geq 0$.
5. $a^2+4b^2+4b-4a+5 \geq 0$.

Б. Использование свойств квадратичной функции

1. Доказать, что при всех $a \geq 0$ справедливо неравенство $10a^3-9a^2+9a+\frac{1}{10} > 0$.
2. Доказать, что при любых значениях a и b имеет место неравенство $a^2+2ab+3b^2+2a+6b+4 \geq 1$.
3. Доказать, что если $(a+c)(a+b+c) < 0$ и $a \neq 0$, то справедливо неравенство $(b-c)^2 > 4a(a+b+c)$.
4. Про положительные числа a_1, b_1, c_1, a_2, b_2, c_2 известно, что $b_1^2 \leq a_1c_1$, $b_2^2 \leq a_2c_2$. Доказать, что $(a_1+a_2+5)(c_1+c_2+2) > (b_1+b_2+3)^2$.
5. Доказать, что при любых значениях a справедливо неравенство $(a^3-a+2)^2 > > 4a^2(a^2+1)(a-2)$.
6. Доказать, что если ненулевые действительные числа a, b, c удовлетворяют

равенствам $a+b+c = abc$, $a^2 = bc$, то $a^2 \geq 3$.

7. Уравнение $ax^2+bx+c = 0$ не имеет действительных корней, $a+b+c < 0$. Какой знак имеет число c?
8. Доказать, что если a, b и c–стороны треугольника, то уравнение $b^2x^2+(b^2+c^2-a^2)x+c^2 = 0$ не имеет действительных корней.
9. Доказать, что выражение $3\left(\frac{x^2}{y^2}+\frac{y^2}{x^2}\right)-8\left(\frac{x}{y}+\frac{y}{x}\right)+10$ неотрицательно при любых ненулевых x и y.
10. Доказать, что если числа a, b, c удовлетворяют условиям $a+b+c = 5$, $ab+bc+ca = 8$, то $1 \leq a \leq \frac{7}{3}$, $1 \leq b \leq \frac{7}{3}$, $1 \leq c \leq \frac{7}{3}$.
11. Доказать, что если $a+b+c > 0$, $ab+bc+ca > 0$, $abc > 0$, то числа a, b, c положительные.

3°. <u>Дискретность порядка на множестве натуральных и целых чисел</u>

1. Доказать, что не существует строго возрастающей последовательности (a_n) целых неотрицательных чисел, для которой при любых m и n выполняется соотношение $a_{mn} = a_m+a_n$.
2. Решить в $\boldsymbol{Z}$ систему $x+y \geq 25$, $y \leq 2x+18$, $y \geq x^2+4x$.
3. Доказать, что при любом натуральном n число $n^4+2n^3+2n^2+2n+1$ не является полным квадратом.
4. При каких значениях n $\boldsymbol{N}$ выражение n^3+7n^2+6n+1 является кубом натурального числа?
5. Сколько пар целых чисел $(x; y)$ удовлетворяет системе неравенств $2x \geq 3y$, $3x \geq 4y$, $5x-7y \leq 20$?
6. Найти целую часть выражения $\sqrt{n^2+\sqrt{4n^2+\sqrt{16n^2+8n+3}}}$.
7. Могут ли числа a^2+b и b^2+a, где a, b $\boldsymbol{N}$, одновременно быть полными квадратами?
8. Найти все пары натуральных чисел a и b, для которых числа a^2+3b и $3a+b^2$ одновременно являются квадратами натуральных чисел.
9. Какое число стоит в последовательности 1, 2, 2, 3, 3, 3, 4, 4, 4, 4, ... на 500000-м месте?
10. К десятичной записи числа 2^k приписали десятичную запись числа 5^k. Сколько десятичных знаков содержит получившееся число?
11. Какое наименьшее неотрицательное число можно получить из чисел 1, 2, ... , 2009 путем расстановки перед ними знаков “+” и “–” и последующего выполнения указанных действий?
12. Какое наименьшее неотрицательное число можно получить из чисел $1^2, 2^2, \ldots, 2009^2$ путем расстановки перед ними знаков “+” и “–” и последующего выполнения действий?
13. Решить в $\boldsymbol{Z}$ уравнение (оценка с помощью неравенств + перебор):

а) $x^2+y^2 = x+y+2$.
б) $x^6+3x^3+1 = y^4$.

в) $(x+2)^4 - x^4 = y^3$.
г) $x^2 + xy + y^2 = x^2y^2$.
д) $x^2 + x = y^4 + y^3 + y^2 + y$.