

**МИНОБРНАУКИ РОССИИ**  
**Ярославский государственный университет им. П.Г. Демидова**

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

**Рабочая программа дисциплины**

**Алгебра**

Направление подготовки (специальности)  
10.05.01 Компьютерная безопасность

Направленность (профиль)  
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена  
на заседании кафедры  
от 12 апреля 2024 г., протокол № 8

Программа одобрена НМК  
математического факультета  
протокол № 9 от 3 мая 2024 г.

## 1. Цели освоения дисциплины

Целью изучения дисциплины Алгебра является обеспечение фундаментальной подготовки в одной из основных областей современной математики, освоение языка и методов одного из наиболее мощных инструментов современной математики. Курс лежит в основе большей части численных методов алгебры, имеющих применение во многих областях естествознания. Его главной задачей является обучение основным методам решения алгебраических задач, ознакомление с историей развития линейной алгебры и вкладом в неё российских математиков.

Основная задача дисциплины – научить студентов пониманию языка алгебры, воспитанию культуры вычислений с помощью матричной алгебры и алгебры многочленов, умениям применять основной аппарат алгебры в различном контексте, в том числе в полях положительной характеристики. Содержание курса является базой для дальнейшего развития содержания дисциплины в специальных курсах.

## 2. Место дисциплины в структуре образовательной программы

Дисциплина «Алгебра» – одна из основных дисциплин цикла «Математические и естественные науки» учебного плана по специальности «компьютерная безопасность». Она обеспечивает приобретение знаний в соответствии с требованиями Государственных образовательных стандартов, содействует фундаментализации математического образования, формированию научного мировоззрения, логического мышления.

Данная дисциплина относится к базовой части образовательной программы. Она имеет разнообразные связи с основными и специальными математическими дисциплинами.

Полученные в курсе «Алгебры» знания необходимы для изучения дисциплин «Линейная алгебра», «Фундаментальная и компьютерная алгебра», «Дискретная математика», «Математическая логика и теория алгоритмов», специальных курсах «Методы и средства криптографической защиты информации», «Теория кодирования», «Криптографические протоколы» и многих других.

## 3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Перечень планируемых результатов обучения
<b>Общепрофессиональные компетенции</b>	
<b>ОПК-2</b> Обладает способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	<b>Знать:</b> - основные методы и формулировки результатов, использующихся в защите информации - основные алгебраические модели и конструкции <b>Уметь:</b> - обосновывать алгоритмы защиты информации - решать системы линейных уравнений <b>Владеть:</b> - навыками быстрых вычислений в основных алгебраических системах

	- навыками вычислений в основных алгебраических системах
--	--

#### 4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **12** зачетных единиц, **432** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости  Форма промежуточной аттестации (по семестрам)
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационны е испытания		
1.	Вводная лекция	1	3						
2	Системы линейных уравнений над полем R	1	6	6		2		15	Самостоятельная работа №1
3.	Приведение к ступенчатому виду уравнений и матриц (алгоритм Гаусса)	1	5	5		2		15	Самостоятельная работа №2
4.	Определители малых порядков и решение систем линейных уравнений по методу Крамера	1	5	5				10	
5.	Векторное пространство $R^n$ и его свойства	1	5	5				10	Контрольная работа 1
6.	Базис и размерность	1	5	5		2		10	
7.	Линейные отображения и их матрицы	1	5	5		2		10	
8.	Ассоциативность умножения матриц и ассоциативность умножения отображений	1	5	5		1		10	
9.	Обратная матрица и ее свойства	1	6	6		1		10	
10.	Определители	1	3	6		1		10	
							0,3	8,7	Зачет
	Всего за 1 семестр 216 акад. часов		48	48		11	0,3	108,7	
11.	Группы, полугруппы, моноиды	2	3	3		1		6	Самостоятельная работа №4
12.	Комплексные числа	2	3	3		1		6	Контрольная работа 2
13.	Формула Муавра	2	3	3		1		6	Самостоятельная работа №5

14.	Арифметика целых чисел	2	3	3		1		6	Проверка домашних заданий
15.	Многочлены одной переменной	2	4	4		1		6	Контрольный опрос
16.	НОД и НОК многочленов	2	4	4		1		6	Контрольная работа 3
17.	Лемма Гаусса	2	4	4				6	
18.	Корни многочленов	2	4	4		1		6	
19.	Симметрические многочлены	2	4	4		1		6	Самостоятельная работа №6
20.	Дискриминант и результат	2	4	4				6	
21.	Интерполяция	2	4	4		1		6	
22.	Таблица Кэли	2	4	4		1		6	Самостоятельная работа №7
23.	Кольцо вычетов по модулю целого числа	2	4	4		1		1	
						2	0,5	33,5	экзамен
	<b>Всего за 2 семестр 216 акад. часов</b>		48	48		13	0,5	106,5	
	<b>ИТОГО</b>		96	96		24	0,8	215,2	

### Содержание разделов дисциплины

#### 1. Вводная лекция.

Предмет и методы современной прикладной алгебры. Некоторые проблемы. Краткий исторический очерк. Место прикладной алгебры в системе математического знания и взаимодействие «чистой» и «прикладной» математики. Алгебра и алгоритмика.

#### 2. Системы линейных уравнений над полем $\mathbf{R}$ .

Матричная запись. Виды систем линейных уравнений. Примеры. Эквивалентность систем линейных уравнений. Элементарные преобразования.

#### 3. Алгоритм Гаусса.

Приведение к ступенчатому виду уравнений и матриц. Определение вида системы с помощью алгоритма Гаусса. Количество арифметических операций в алгоритме Гаусса.

#### 4. Определители малых порядков и решение систем линейных уравнений по методу Крамера.

Перестановки и подстановки. Четность перестановки. Умножение подстановок.

#### 5. Векторное пространство $\mathbf{R}^n$ и его свойства.

Линейные комбинации векторов. Линейная оболочка. Подпространства пространства  $\mathbf{R}^n$ . Линейная зависимость и линейная независимость системы векторов. Теорема о линейной зависимости.

#### 6. Базис и размерность.

Теорема о базисе. Ранг системы векторов. Теорема о ранге. Теорема Кронекера - Капелли.

#### 7. Линейные отображения и их матрицы.

Операции над матрицами (сумма, произведение матриц и умножение матрицы на число) и их свойства. Связь операций над матрицами и операций над отображениями

#### 8. Ассоциативность умножения матриц и ассоциативность умножения отображений.

Ранг произведения матриц.

#### 9. Обратная матрица и ее свойства.

Нахождение обратной матрицы с помощью алгоритма Гаусса. Решение систем линейных уравнений. Общее решение системы линейных уравнений. Фундаментальная система решений однородной системы линейных уравнений.

### **10. Определители.**

Определение и основные свойства. Разложение определителя по строке и столбцу. Формулы Крамера для систем с квадратной матрицей. Вычисление определителя с помощью теоремы Лапласа. Примеры вычислений. Определитель произведения матриц

### **11. Группы, полугруппы, моноиды.**

Примеры групп (конечных и бесконечных). Изоморфизмы групп. Определения и примеры. Гомоморфизмы. Ядро гомоморфизма

### **12. Комплексные числа.**

Поле комплексных чисел. Комплексная плоскость. Геометрическая интерпретация комплексных чисел. Тригонометрическая форма комплексного числа. Умножение комплексных чисел.

### **13. Формула Муавра.**

Возведение в степень комплексных чисел. Автоморфизм сопряжения поля комплексных чисел. Извлечение корней. Первообразные корни из единицы и квантовых вычислениях.

### **14. Арифметика целых чисел.**

Делимость в кольце целых чисел. Наибольший общий делитель и наименьшее общее кратное целых чисел. Коэффициенты Безу.

### **15. Многочлены одной переменной.**

Кольцевые свойства. Степень многочлена. Многочлены многих переменных. Деление с остатком многочленов

### **16. НОД и НОК многочленов.**

Неприводимые многочлены над полем. Однозначность разложения на неприводимые множители

### **17. Многочлены над полем рациональных чисел.**

Лемма Гаусса. Критерий Эйзенштейна. Поле отношений

### **18. Корни многочленов.**

Теорема Безу. Кратность корня. Отделение кратных корней. Формулы Виета. Основная теорема алгебры.

### **19. Симметрические многочлены.**

Основная теорема о симметрических многочленах. Метод неопределенных коэффициентов для симметрических многочленов

### **20. Дискриминант и результат.**

### **21. Интерполяция.**

Полином Лагранжа. Алгебраическая замкнутость поля комплексных чисел. Многочлены с вещественными коэффициентами. Вычисление корней многочленов

### **22. Таблица Кэли.**

Циклические группы. Смежные классы. Теорема Лагранжа.

### **23. Кольцо вычетов по модулю целого числа.**

Характеристика конечного поля. Простое подполе

## **5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине**

В процессе обучения используются следующие образовательные технологии:

**Вводная лекция** – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и

организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

**Академическая лекция с элементами лекции-беседы** – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

**Практическое занятие** – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

**Консультации** – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

## **6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине**

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader.

## **7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)**

В процессе осуществления образовательного процесса по дисциплине используется:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

[http://www.lib.uniyar.ac.ru/opac/bk\\_cat\\_find.php](http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php)

- Электронная библиотечная система «Лань» <https://e.lanbook.com>

- Электронная библиотечная система «Юрайт» <https://urait.ru>

- Электронная библиотечная система «Консультант студента»

<https://www.studentlibrary.ru>

## **8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины**

### **а) основная литература**

1. Кострикин, А. И. Введение в алгебру. Часть I. Основы алгебры : Учеб. для вузов. / Кострикин А. И. - 2-е изд., исправл. - Москва : ФИЗМАТЛИТ, 2003. - 272 с. - ISBN 5-9221-0167-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN5922101676.html>

2. Артамонов, В. А. Сборник задач по алгебре. Т. 2. / Ч. III. / В. А. Артамонов, Ю. А. Бахтурин, Э. Б. Винберг, Е. С. Голод, В. А. Исковских, А. И. Кострикин, В. Н. Латышев, А. В. Михалев, А. П. Мишина, А. Ю. Олышанский, А. А. Панчишкин, И. В. Проскуряков, А. Н. Рудаков, Л. А. Скорняков, А. Л. Шмелькин - Москва : ФИЗМАТЛИТ, 2006. - 168 с. - ISBN 5-9221-0726-7. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN5922107267.html>

3. Курош А. Г. Курс высшей алгебры: учебник для вузов — Санкт-Петербург: Лань, 2022. <https://reader.lanbook.com/book/183725>

#### **б) дополнительная литература**

1. Проскуряков И. В. Сборник задач по линейной алгебре: учебное пособие для вузов— Санкт-Петербург: Лань, 2022. <https://e.lanbook.com/book/183752>

2. И. Х. Сабитов, А. А. Михалев. Линейная алгебра и аналитическая геометрия: учебное пособие для вузов — Москва: Издательство Юрайт, 2022. <https://urait.ru/viewer/lineynaya-algebra-i-analiticheskaya-geometriya-493221>

3. М. М. Глухов, В. П. Елизаров, А. А. Нечаев Алгебра: учебник для вузов — Санкт-Петербург: Лань, 2022. <https://reader.lanbook.com/book/187793>

### **9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине**

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

#### **Автор(ы) :**

зав. кафедрой алгебры и математической логики ЯрГУ,  
д-ф.м.н, профессор

Казарин Л. С.

**Фонд оценочных средств  
для проведения текущей и промежуточной аттестации студентов  
по дисциплине**

**1. Типовые контрольные задания или иные материалы,  
используемые в процессе текущей аттестации**

**Задания по теме №1 «Введение»**

Раздел 1.1. Модельные задачи, приводящие к решению уравнений в радикалах и к системам линейных уравнений. Учебник А.И.Кострикина, § 1-3.

Раздел 1.2. Начала теории множеств. Отображения. Суперпозиция отображений. Обратимость отображений. Упражнения 1-7 из §5 учебника А.И.Кострикина

Раздел 1.3. Бинарные отношения. Эквивалентность. Классы эквивалентности и факторизация отображений. Частичный порядок. Мощность множества и математическая индукция. Упражнения 1-5 из §6 и упражнения 1-2 из §7 учебника А.И.Кострикина.

**Задания по теме №2 «Системы линейных уравнений над полем вещественных чисел».**

Раздел 2.1 Задачи на приведение системы линейных уравнений к ступенчатому виду методом Гаусса.

Раздел 2.2. Матричная запись системы линейных уравнений и исследование системы линейных уравнений с помощью метода Гаусса.

Раздел 2.4. Введение в теорию определителей. Определители малых порядков и их свойства. Теорема Крамера (случай малой размерности). Решение задач из задачника Сборник задач по алгебре под ред. А.И.Кострикина, игра в определитель.

**Задания по теме №3 Арифметические линейные векторные пространства.**

Раздел 3.1. Отработка основных понятий. Доказательства того, что данное множество объектов является векторным пространством.

Раздел 3.2. Решение задач из задачника Сборник задач по алгебре под ред. А.И.Кострикина, Упражнения из §1-2 гл. 2 учебника А.И.Кострикина

**Задания по теме №4. Матрицы и линейные отображения.**

Разделы 4.1. – 4.2 -- Решение задач из задачника Сборник задач по алгебре под ред. А.И.Кострикина, Упражнения из §3 гл. 2 учебника А.И.Кострикина.

Разделы 4.3 – 4.4 -- Решение задач из задачника Сборник задач по алгебре под ред. А.И.Кострикина, Задачи на нахождение матриц линейных отображений из одного пространства в другое и нахождения ядра и образа линейного отображения, заданного матрицей. Например, матрицы оператора дифференцирования на пространстве многочленов ограниченной степени.

**Задания по теме №5. Определители.**

Раздел 5.1. Подстановки и перестановки. Нахождение четности случайно выбранной подстановки. Умножение подстановок. Подстановки – матрицы.

Разделы 5.2 - 5.3. Вычисления слагаемых, входящих в определитель. Использование свойств определителя для быстрых вычислений. Вычисление обратной матрицы и решение матричных уравнений вида  $AX=B=C$ .

Разделы 5.4 – 5.6. Вычисления определителей с помощью разложения по строке или столбцу. Упражнения из §2 гл. 3 учебника А.И.Кострикина, вычисления рангов матриц с помощью определителей и метода Гаусса. Решение систем линейных уравнений с помощью правила Крамера. Вычисление определителей специального вида. Решение задач из Сборника задач по алгебре под ред. А.И.Кострикина,

**Задания по теме №6. Алгебраические структуры.**



Раздел 6.1. Различные примеры групп. Упражнения из §2 гл. 4 учебника А.И.Кострикина и Сборника задач по алгебре под ред. А.И.Кострикина.

Раздел 6.2. – 6.3. Поля. Примеры полей. Кольца и алгебры. Гомоморфизмы колец. Упражнения Упражнения из §3 гл. 4 учебника А.И.Кострикина и Сборника задач по алгебре под ред. А.И.Кострикина.

**Задания по теме №7. Поля. Поле комплексных чисел и его свойства.**

Раздел 7.1. Задачи на проверку является ли множество чисел определенного вида полем. Например, числа вида  $a+bx$ , где  $a$  и  $b$  – рациональные числа, а  $x$  – корень из целого числа. Вычисления с комплексными числами. Решение систем линейных уравнений и матричных уравнений с комплексными коэффициентами.

Раздел 7.2. Решение задач, использующих тригонометрическую форму комплексного числа. Задачи из Сборника задач по алгебре под ред. А.И.Кострикина.

**Задания по теме №8. Кольцо многочленов.**

Разделы 8.1 – 8.2. Решение простейших задач с многочленами одной и несколькими переменными над полями и кольцами матриц.

Раздел 8.3. Алгоритм деления многочленов. Задачи вычислительного плана. Нахождение частного и остатка для конкретных многочленов. Решение задач из Сборника задач по алгебре под ред. А.И.Кострикина. Гомоморфизмы кольца многочленов и идеалы.

**Задания по теме №9. Теория делимости в кольцах многочленов и целых чисел**

Раздел 9.1. Нахождение НОД и НОК многочленов и целых чисел. Матричная форма алгоритма Евклида. Решение задач §3 гл. 5 учебника А.И.Кострикина Раздел 9.2. Упражнения из §3 гл. 5 учебника А.И.Кострикина. Различные задачи на применения критерия Эйзенштейна.

**Задания по теме №10. Корни многочленов. Многочлены с вещественными и целыми коэффициентами. Теорема Штурма. Интерполяция. Теорема Гаусса.**

Разделы 10.1 – 10.3 Вычислительные задачи, касающиеся многочленов и их корней.. Упражнения из §1 гл. 6 учебника А.И.Кострикина и приближенное вычисление корней многочлена одной переменной над полем вещественных чисел. Решение из Сборника задач по алгебре под ред. А.И.Кострикина

**Задания по теме №11. Поле рациональных дробей. Многочлены многих переменных**

Разделы 11.1 – 11.2. Разложение рациональной дроби в сумму простейших методом неопределенных коэффициентов. Вычисление разложения симметрического многочлена через элементарные функции. Дискриминант многочлена. Вычисление результатов пар многочленов.

**Задания по теме №12. Кольца вычетов по модулю многочлена и целого числа. Конечные поля.**

Разделы 12.1 – 12.3. Построение полей небольшого порядка. Решение численных задач с помощью колец вычетов.

**Самостоятельная работа №1**

1. Решить систему линейных уравнений (варианты из задачника под ред. А.И.Кострикина).
2. Найти декартово произведение двух заданных конечных множеств.
3. Показать, что декартова степень счетного множества является счетным множеством.
4. Заданы два отображения  $f$  и  $g$  множества чисел  $\{1, 2, \dots, n\}$  в себя. Найти результирующее отображение  $fg$  и сравнить с  $gf$ .
5. Найти формулу для суммы квадратов последовательных  $n$  натуральных чисел.
6. Привести примеры отношения эквивалентности, отличные от равенства.

**Самостоятельная работа №2**

1. Решить систему линейных уравнений с помощью метода Крамера (варианты из задачника под ред. А.И.Кострикина).
2. Доказать тождественное равенство двух определителей 3 порядка, не разворачивая их.

3. Исследовать систему линейных уравнений с параметром методом Гаусса.
4. Сколько требуется операций сложения и умножения чисел в худшем случае для решения системы из 10 уравнений с 10 неизвестными? Обосновать ответ.

### **Самостоятельная работа №3**

1. Будет ли линейным векторным пространством множество кососимметрических матриц порядка  $n$ ? Если да, то найти его размерность.
2. Пусть  $a, b, c$  – линейно независимые векторы. Будут ли векторы  $a, a+b, a+b+c$  линейно независимы? Тот же вопрос для векторов  $a-b, b-c, a-c$ .
3. Найти размерность подпространства, натянутого на заданную систему векторов.
4. Предложить алгоритм для нахождения базиса системы векторов, заданных своими координатами.
5. Вычислить ранг заданной матрицы.
6. Заданы 2 линейно независимые системы векторов трехмерного пространства. Найти выражение векторов первой системы через вторую и обратно.

### **Контрольная работа №1**

1. Перемножить две заданные матрицы с числовыми коэффициентами.
2. Найти ядро и образ линейного отображения, заданного своей матрицей.
3. Найти матрицу линейного отображения, переставляющего циклически координаты вектора.
4. Будет ли совокупность линейных отображений векторного пространства в себя само векторным пространством (относительно операций сложения и умножения)?
5. Найти матрицу отображения двумерного пространства в себя, заданного умножением координат векторов на фиксированную матрицу размера 2.
6. Найти условия, при которых отображение двумерного пространства самого в себя будет обратимым.
7. Найти общее решение системы из двух заданных линейных уравнений с 5 неизвестными.

### **Домашняя самостоятельная работа**

1. Найти перестановку  $n$  –элементного множества, обладающую наибольшим числом инверсий.
2. Найти наибольший порядок элемента в симметрической группе степени 11.
3. Решить матричное уравнение  $AXB=C$ , где  $A, B, C$  – заданные матрицы.
4. Вычислить определитель матрицы с помощью разложения по строке или столбцу.
5. В каком случае вычисление обратной матрицы проще делать с помощью вычисления матрицы, составленной из алгебраических дополнений (присоединенной), а в каком случае с помощью метода Гаусса?
6. Найти обратную матрицу к заданной треугольной.
7. Вычислить определитель заданной трехдиагональной матрицы с помощью рекуррентных соотношений.

### **Самостоятельная работа №4**

1. Является ли группой по сложению множество всех кососимметрических матриц с целыми коэффициентами?
2. Является ли группой по умножению множество всех целочисленных матриц с определителем, равным 1?
3. Найти все подгруппы аддитивной группы целых чисел. В каких случаях эта подгруппа будет кольцом?
4. В каком случае кольцо вычетов по модулю простого числа будет полем?
5. Найти все идеалы кольца целых чисел.

6. Как проверить, что система, заданная таблицами сложения и умножения, будет полем? Сколько операция вычислительной машине потребуется для проверки? Изложить соображения.

### **Самостоятельная работа №5**

1. Будет ли полем совокупность чисел вида  $a+bx$ , где  $x$ —корень квадратный из 6?
2. Решить систему из 2 линейных уравнений с 6 неизвестными с комплексными коэффициентами.
3. Решить матричное уравнение  $AXB=C$ , где  $A$ ,  $B$ ,  $C$  – матрицы с комплексными коэффициентами.
4. Найти все комплексные числа, сопряженные своему кубу.
5. Изобразить на комплексной плоскости множество точек  $z$ , удовлетворяющих неравенству  $|z-1|+|z+1|>5$ .
6. Найти сумму всех комплексных корней 6 степени из  $z=1+2i$ .

### **Контрольная работа №2**

1. Найти частное и остаток от деления многочлена  $f(x)$  на  $g(x)$  для многочленов с коэффициентами из поля  $GF(2)$ .
2. Найти ядро и образ оператора дифференцирования в кольце  $R[x,y]$  многочленов двух переменных.
3. В каких случаях теорема о степени произведения многочленов неверна? Привести примеры для многочленов нескольких переменных.
4. Чему равно число различных одночленов от  $n$  независимых переменных, имеющих полную степень 3?
5. Доказать, что если  $F$  – поле, то все автоморфизмы  $f$  кольца  $F[X]$ , тождественные на  $F$ , имеют вид:  $f(X) = aX+b$ , где  $a, b \in F$ .
6. Доказать, что для целостного кольца  $K$  и для любого многочлена  $f$  в  $K[X]$  и многочлена  $g$  из  $K[X]$  с обратимым старшим коэффициентом существуют частное и остаток, причем эта пара единственна.

### **Контрольная работа №3**

1. Разложить по степеням  $(x-a)$  многочлен  $f(x)$  с заданными коэффициентами, используя схему Горнера.
2. Для заданного многочлена  $f(x)$  с вещественными коэффициентами построить многочлен  $g(x)$ , имеющий те же корни, что и  $f(x)$ , но кратности 1.
3. Найти НОД и НОК двух заданных многочленов над полем  $GF(2)$ .
4. Доказать, что для любой степени  $n>0$  существует многочлен, неприводимый над полем рациональных чисел.
5. Найти формулу для суммы кубов первых  $n$  натуральных чисел, используя полином Лагранжа.
6. Локализовать вещественные корни заданного многочлена 5 степени с вещественными коэффициентами, используя систему Штурма.

### **Самостоятельная работа №6**

1. Представить заданную рациональную дробь в виде суммы элементарных дробей.
2. Найти дискриминант заданного многочлена.
3. Найти сумму кубов корней заданного уравнения с целыми коэффициентами.
4. Найти результат пары многочленов с вещественными коэффициентами.
5. Найти все неприводимые многочлены степени 3 над полем  $GF(2)$ .
6. Написать программу вычисления корня многочлена на отрезке  $[a,b]$  с заданной точностью на языке ПАСКАЛЬ.

### **Самостоятельная работа №7**

1. Доказать, что все подгруппы конечной циклической группы циклические.
2. Построить таблицу умножения для поля  $\mathbb{Z}_9$  элементов.
3. Найти все примитивные элементы поля  $\text{GF}(17)$ .
4. Когда возведение элементов в квадрат определяет автоморфизм группы?
5. Найти все гомоморфизмы кольца целых чисел.
6. Написать таблицу умножения группы подстановок степени 3.

## **2. Список вопросов и (или) заданий для проведения промежуточной аттестации**

### **Вопросы к зачету по алгебре**

1. Что такое система линейных уравнений?
2. Какие бывают системы линейных уравнений?
3. Что такое решение системы линейных уравнений?
4. Что такое линейное векторное пространство.
5. Какие операции определяются над матрицами?
6. Что такое фундаментальная система решений однородной системы линейных уравнений?
7. Что такое линейно зависимая и что такое линейно независимая система векторов?
8. Что такое подпространство линейного векторного пространства?
9. Дайте формулировку правила Крамера.
10. Как вычисляется ранг матрицы и ранг системы векторов?
11. Как используется понятие ранга матрицы при решении системы линейных уравнений?
12. Что такое отношение эквивалентности? Приведите примеры.
13. Как складываются и умножаются матрицы? Привести примеры.
14. Напишите формулу определения определителя.
15. Как вычисляются определители?
16. Что такое подстановка? Как умножаются подстановки?
17. Как найти обратную матрицу к заданной?
18. Приведите примеры группы, полугруппы, кольца, поля.

### **Вопросы к экзамену по алгебре**

1. Конечное и бесконечное поле. Характеристика поля. Существование поля комплексных чисел. Его свойства. Геометрическая интерпретация. Операция сопряжения.
2. Тригонометрическая формула комплексного числа. Формула Муавра. Возведение в степень и извлечение корней из комплексных чисел.
3. Корни из единицы.
4. Кольцо многочленов одной переменной над кольцом. Операции над многочленами. Запись многочленов одной переменной в виде функций.
5. Степень многочлена. Умножение многочленов. Степень суммы и произведения многочленов.
6. Многочлены многих переменных.
7. Деление многочленов с остатком. Алгоритм деления. Единственность частного и остатка.
8. Кольца главных идеалов. Гомоморфизмы кольца многочленов.
9. Наибольший общий делитель в кольцах целых чисел и многочленов. Свойства НОД.
10. Алгоритм Евклида и его матричная версия.

11. Неприводимые многочлены и простые числа. Существование и единственность разложений в кольцах многочленов и целых чисел. Коэффициенты Безу.
12. Неприводимые многочлены над кольцом целых чисел и полем рациональных чисел.
13. Лемма Гаусса. Критерий Эйзенштейна.
14. Кратность корня. Связь корней многочлена с неприводимыми многочленами степени 1. Дифференцирование в кольце многочленов и отделение кратных корней. Схема Горнера.
15. Теорема Гаусса об алгебраической замкнутости поля комплексных чисел. Неприводимые многочлены над полями вещественных и комплексных чисел.
16. Локализация корней. Теорема Штурма. Приближенное вычисление корней многочлена.
17. Формулы Виета. Симметрические многочлены. Элементарные симметрические многочлены. Основная теорема о симметрических многочленах.
18. Дискриминант многочлена.
19. Результант двух многочленов.
20. Поле рациональных дробей.
21. Кольца, подкольца, идеалы.
22. Факторкольцо. Построение кольца  $Z_n$ .
23. Построение конечного поля как поля вычетов по модулю неприводимого многочлена.
24. Таблица Кэли.
25. Циклические группы.
26. Нормальные подгруппы.
27. Смежные классы. Теорема Лагранжа.
28. Теоретико-числовые следствия теоремы Лагранжа.

### **3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

#### **3.1 Критерии оценивания степени овладения знаниями, умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций**

**Пороговый уровень** (общие характеристики):

- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

**Продвинутый уровень (общие характеристики):**

- достаточно полные и систематизированные знания в объёме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;
- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

**Высокий уровень (общие характеристики):**

- систематизированные, глубокие и полные знания по всем разделам дисциплины;
- точное использование терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

### **3.2 Описание процедуры выставления оценки**

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка («зачтено», «незачтено»), которая определяется рабочей программой дисциплины в соответствии с учебным планом первого семестра. Оценка «зачет» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «незачтено» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Оценка «отлично» выставляется студенту, у которого каждая компетенция сформирована на высоком уровне. Оценка «хорошо» выставляется студенту, у которого каждая компетенция сформирована не ниже, чем на продвинутом уровне. Оценка «удовлетворительно» выставляется студенту, у которого каждая компетенция сформирована не ниже, чем на пороговом уровне.

## Приложение №2 к рабочей программе дисциплины «Алгебра»

### Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Алгебра» являются лекции, причем в достаточно большом объеме. Это связано с тем, что алгебра представляет собой особый математический аппарат, с помощью которого математика решает довольно сложные и громоздкие задачи. По большинству тем предусмотрены практические занятия, на которых происходит закрепление лекционного материала путем применения его к конкретным задачам и отработка навыков работы с математическим аппаратом алгебры.

Особенность дисциплины состоит в ее существенно более абстрактный характер по сравнению со школьной математикой. Для успешного освоения дисциплины очень важно решение достаточно большого количества задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. В течение всего обучения на лекциях предлагаются нестандартные задачи, решая которые студент может повысить свой уровень освоения теоретического материала. Основная цель решения задач – помочь усвоить фундаментальные понятия и основы алгебры. Для решения всех задач необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, практических занятиях или из учебной литературы.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с аппаратом алгебры в течение обучения проводятся мероприятия текущей аттестации в виде контрольной работы и 3 самостоятельных работ в 1-ом семестре и двух контрольных и 2 самостоятельных работ (в аудитории) в обоих семестрах изучения дисциплины. Также проводятся консультации (при необходимости) по разбору заданий для самостоятельной работы, которые вызвали затруднения.

В конце первого семестра изучения дисциплины студенты сдают зачет и экзамен, в конце всего курса – еще один зачет и экзамен. Зачет по итогам первого семестра выставляется по итогам тестирования и краткого собеседования по его результатам. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя теоретический вопрос и задачу. На самостоятельную подготовку к экзамену выделяется 3 дня, во время подготовки к экзамену предусмотрена групповая консультация.

Освоить вопросы, излагаемые в процессе изучения дисциплины «Алгебра» самостоятельно студенту крайне сложно. Это связано со сложностью и абстрактностью изучаемого материала и большим объемом курса. Поэтому посещение всех аудиторных занятий является совершенно необходимым. Без упорных и регулярных занятий в течение семестра сдать зачет и экзамен по итогам изучения дисциплины в каждом семестре студенту практически невозможно.

## Методические указания для преподавателей дисциплины

1. Дисциплина является одной из основных (наряду с математическим анализом, геометрией, дискретной математикой и компьютерными технологиями) для образования в области математики и компьютерных наук. От ее усвоения зависит математическая культура обучающегося.
2. Основная трудность в усвоении дисциплины, помимо большого количества новых для слушателя понятий и испорченности школьным образованием, является большая абстрактность изложения в большинстве учебников и задачников. Поэтому при введении новых понятий необходимо преследовать следующие цели: а) не упускать возможностей прокомментировать важность новых понятий;  
б) приводить побольше примеров их использования;  
в) придумывать, по-возможности, способы манипулирования этими понятиями.
3. Я предпочитаю откладывать введение абстрактных алгебраических систем как можно дольше. Для начала надо научить работать с системами линейных уравнений, векторами над полем вещественных чисел, определителями и матрицами. При этом привыкать к определителям лучше с небольших размеров, но общее определение вводить инвариантным образом. После выяснения свойств определителя показать, как он вычисляется методом Гаусса, не упуская существующих теоретических открытых проблем.
4. Только после этого можно вводить понятия группы, кольца и поля, но акцентируя изложение на понятии поля. Показать существование полей из 2 и 3 элементов, сделать замечания по поводу характеристики поля и поля рациональных чисел. Наконец, заняться введением поля комплексных чисел и работой в этом поле. Обязательно сообщить слушателям, что большинство теорем, касающихся линейных уравнений, определителей и т.п. справедливы в случае почти любого поля.
5. Далее следуют материалы, касающиеся многочленов одной и нескольких переменных, а заключается курс работой в группах, теоремой Лагранжа и ее применением в теории чисел. При этом материал о неприводимых многочленах и основной теоремой арифметики многочленов излагается параллельно. Этим экономится время, и снимаются трудности с пониманием материала, маскирующиеся трудоемкими вычислениями. При этом знакомство с полями из 2 и 3 элементов оказывает существенную помощь в обходе вычислительных трудностей.
6. Я не привожу формулировок задач к разделам с конкретными числовыми данными. Имеется большое количество таких задач, так что преимущество одной конкретной задачи перед другой кажется сомнительным. Нюансы опытный преподаватель может разглядеть, но тренировка на фиксированных конкретных примерах может нечаянно вылиться в сентенцию студента: «а мы **такую** задачу не решали...».
7. Для самостоятельного чтения студентам рекомендованы учебники А.И.Кострикина и А.Г.Куроша. При этом для слабо подготовленных студентов можно рекомендовать учебник А.Г.Куроша в качестве стартового материала, а затем, по мере накопления опыта, переход к учебнику А.И. Кострикина. Для наиболее продвинутых можно рекомендовать учебник Э.Б.Винберга, содержащий достаточно большой материал геометрического плана.