

МИНПРОСВЕЩЕНИЯ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования  
"Тульский государственный педагогический университет им. Л.Н. Толстого"  
(ФГБОУ ВО "ТГПУ им. Л.Н. Толстого")

## Фундаментальная и компьютерная алгебра

### рабочая программа дисциплины (модуля)

Закреплена за кафедрой	<b>кафедра алгебры, математического анализа и геометрии</b>
ОПОП	<b>Направление 02.03.01 Математика и компьютерные науки направленность (профиль) Математические основы компьютерных наук</b>
Квалификация	<b>Бакалавр</b>
Год начала подготовки	<b>2022</b>
Форма обучения	<b>очная</b>
Общая трудоемкость	<b>8 з.е.</b>

Виды контроля по семестрам:

экзамен 6  
зачет 5  
курсовая работа 6

Семестр(Курс.Номер семестра на курсе)	5(3.1)		6(3.2)		Итого	
	УП	РПД	УП	РПД	УП	РПД
Лекции	30	30	18	18	48	48
Практические	30	30	26	26	56	56
Лабораторные	8	8	8	8	16	16
Итого ауд.	68	68	52	52	120	120
КСР	4	4	2	2	6	6
Контактная работа	72	72	54	54	126	126
Сам. работа	72	72	54	54	126	126
Часы на контроль	0	0	36	36	36	36
Практическая подготовка	0	0	0	0	0	0
Семинары	0	0	0	0	0	0
Консультации	0	0	0	0	0	0
Итого трудоемкость в часах	144	144	144	144	288	288

Программу составил(и):

*д.ф.-м.н., профессор, Балаба И. Н.*

Рабочая программа дисциплины

**Фундаментальная и компьютерная алгебра**

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 02.03.01 Математика и компьютерные науки (приказ Минобрнауки России от 23.08.2017 г. № 807)

составлена на основании учебного плана:

Направление 02.03.01 Математика и компьютерные науки  
направленность (профиль) Математические основы компьютерных наук  
утвержденного Учёным советом вуза от 28.02.2022 протокол № 3.

РПД утверждена Учёным советом университета  
протокол от 1.1.1 г. №

### 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование у студентов базовых знаний по фундаментальной и компьютерной алгебре, рассмотреть основные задачи и алгоритмы в теории многочленов и теории квадратичных форм; познакомиться с основными понятиями теории групп, колец и полей, элементами теории кодирования, с методами и приемами решения различных алгоритмических задач.

### 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.О
<b>2.1</b>	<b>Требования к предварительной подготовке обучающегося:</b>
1.	Дифференциальные и разностные уравнения
2.	Методы и технологии программирования
3.	технологическая (проектно-технологическая) практика
4.	Функциональный анализ
5.	Математический анализ
6.	Педагогика и психология
7.	Программирование
8.	Теория вероятностей и математическая статистика
9.	Архитектура вычислительных систем
10.	Дискретная математика и ее приложения в компьютерных науках
11.	Математическая логика и ее приложение в компьютерных науках
12.	Аналитическая геометрия
13.	Линейная алгебра
<b>2.2</b>	<b>Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>
1.	Вариационное исчисление и методы оптимизации
2.	Математическое моделирование
3.	Моделирование бизнес-процессов
4.	научно-исследовательская работа
5.	Научные основы курса элементарной алгебры
6.	Параллельное программирование
7.	преддипломная практика

### 3. СООТНЕСЕНИЕ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) С ИНДИКАТОРАМИ ДОСТИЖЕНИЯ КОМПЕТЕНЦИЙ

#### 3.1 Компетенции обучающегося и индикаторы их достижения:

ОПК-1: Способен консультировать и использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в профессиональной деятельности	
ОПК-1.2	Умеет использовать базовые знания в области математических и естественных наук в профессиональной деятельности
	умеет применять базовые знания для изучения основных алгебраических структур и для решения алгоритмических задач в кольцах многочленов
ОПК-1.4	Имеет навыки выбора методов решения задач профессиональной деятельности на основе теоретических знаний в области математических и естественных наук
	имеет навыки построения и анализа алгоритмов для решения конкретных задач и конструирования кодов
ОПК-4: Способен находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	
ОПК-4.1	Знает основные понятия, гипотезы, теоремы, методы, математические и алгоритмические модели, составляющие содержание фундаментальной и прикладной математики и связанные с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности
	основные алгебраические структуры и их свойства, особенности представления математических объектов в системах компьютерной алгебры, особенности символьных алгоритмов, основные системы компьютерной алгебры
ОПК-4.2	Умеет осуществлять поиск, анализ и программную реализацию математических алгоритмов
	умеет строить канонические представления базовых математических объектов,

	решать алгоритмические задачи в кольцах многочленов;
ОПК-4.3	Владеет навыками программной реализации математических алгоритмов с применением современных вычислительных систем
	владеет навыками построения и анализа алгоритмов для решения конкретных задач и конструирования кодов; имеет опыт практического использования систем компьютерной алгебры.
<b>3.2 Результаты обучения по дисциплине:</b>	
<b>В результате освоения дисциплины обучающийся должен:</b>	
	<b>Знать:</b>
3.1	основные алгебраические структуры и их свойства;
3.2	особенности представления математических объектов в системах компьютерной алгебры;
3.3	особенности символьных алгоритмов;
3.4	основные системы компьютерной алгебры;
	<b>Уметь:</b>
У.1	строить канонические представления базовых математических объектов;
У.2	решать алгоритмические задачи в кольцах многочленов;
У.3	применять базовые знания для решения алгоритмических задач в кольцах многочленов;
У.4	применять базовые знания для изучения основных алгебраических структур
	<b>Владеть:</b>
В.1	построения и анализа алгоритмов для решения конкретных задач
В.2	конструирования кодов;
В.3	опыт практического использования систем компьютерной алгебры.

#### 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература	Содержание
	<b>Основные алгебраические структуры</b>				
1.1	Группы, кольца поля. /Лек/	5	4	Л1.1 Л1.3Л2.1 Л2.2	Группы. Разложение группы на смежные классы. Теорема Лагранжа. Нормальные подгруппы и фактор-группы. Циклические группы. Кольца и поля. Кольца и поля. Подкольца, идеалы и фактор-кольца.
1.2	Группы, кольца поля. /Пр/	5	4	Л1.1 Л1.3Л2.1 Л2.2	Группы. Разложение группы на смежные классы. Теорема Лагранжа. Нормальные подгруппы и фактор-группы. Циклические группы. Кольца и поля. Кольца и поля. Подкольца, идеалы и фактор-кольца.
1.3	Группы, кольца поля. /Ср/	5	10	Л1.1 Л1.3Л2.1 Л2.2	Группы. Разложение группы на смежные классы. Теорема Лагранжа. Нормальные подгруппы и фактор-группы. Циклические группы. Кольца и поля. Кольца и поля. Подкольца, идеалы и фактор-кольца.
1.4	Поле комплексных чисел. /Лек/	5	2	Л1.1 Л1.3Л2.1 Л2.2	Поле комплексных чисел. Геометрическое представление комплексных чисел. Комплексные числа в алгебраической форме. Комплексные числа в тригонометрической форме. Основные операции.
1.5	Поле комплексных чисел. /Пр/	5	4	Л1.1 Л1.3Л2.1 Л2.2	Поле комплексных чисел. Геометрическое представление комплексных чисел. Комплексные числа в алгебраической форме. Комплексные числа в тригонометрической форме. Основные операции.
1.6	Поле комплексных чисел. /Ср/	5	10	Л1.1 Л1.3Л2.1 Л2.2	Поле комплексных чисел. Геометрическое представление комплексных чисел. Комплексные числа в алгебраической форме. Комплексные числа в тригонометрической форме. Основные операции.

1.7	Кольцо многочленов от одной переменной. /Лек/	5	6	Л1.1 Л1.3Л2.2	Кольцо многочленов от одной переменной. Построение кольца многочленов. Теорема Безу. Схема Горнера. Многочлены над полем. НОД многочленов. Алгоритм Евклида. Евклидовы и факториальные кольца. Вычисление значений и корней полиномов. Многочлены над числовыми полями. Многочлены над полем рациональных чисел. Рациональные корни. Критерий Эйзенштейна. Алгебраическая замкнутость поля комплексных чисел. Многочлены над полем действительных чисел.
1.8	Кольцо многочленов от одной переменной. /Пр/	5	6	Л1.1 Л1.3Л2.2	Кольцо многочленов от одной переменной. Построение кольца многочленов. Теорема Безу. Схема Горнера. Многочлены над полем. НОД многочленов. Алгоритм Евклида. Евклидовы и факториальные кольца. Вычисление значений и корней полиномов. Многочлены над числовыми полями. Многочлены над полем рациональных чисел. Рациональные корни. Критерий Эйзенштейна. Алгебраическая замкнутость поля комплексных чисел. Многочлены над полем действительных чисел.
1.9	Многочлены от одной переменной /Лаб/	5	2	Л1.1 Л1.3Л2.2	НОД многочленов. Алгоритм Евклида. Схема Горнера. Вычисление значений и корней полиномов. Рациональные корни. Многочлены над полями действительных и комплексных чисел
1.10	Кольцо многочленов от одной переменной. /Ср/	5	16	Л1.1 Л1.3Л2.2	Кольцо многочленов от одной переменной. Построение кольца многочленов. Теорема Безу. Схема Горнера. Многочлены над полем. НОД многочленов. Алгоритм Евклида. Евклидовы и факториальные кольца. Вычисление значений и корней полиномов. Многочлены над числовыми полями. Многочлены над полем рациональных чисел. Рациональные корни. Критерий Эйзенштейна. Алгебраическая замкнутость поля комплексных чисел. Многочлены над полем действительных чисел.
1.11	Алгебраические и конечные расширения /Лек/	5	6	Л1.1 Л1.3Л2.2	Алгебраические и конечные расширения. Конечные кольца и поля. Построение конечных полей. Точные вычисления в конечных полях.
1.12	Алгебраические и конечные расширения /Пр/	5	6	Л1.1 Л1.3Л2.2	Алгебраические и конечные расширения. Конечные кольца и поля. Построение конечных полей. Точные вычисления в конечных полях.
1.13	Конечные поля /Лаб/	5	2	Л1.1 Л1.3Л2.1 Л2.2	Построение конечных полей. Точные вычисления в конечных полях. Многочлены над конечными полями
1.14	Алгебраические и конечные расширения /Ср/	5	12	Л1.1 Л1.3Л2.2	Алгебраические и конечные расширения. Конечные кольца и поля. Построение конечных полей. Точные вычисления в конечных полях. Многочлены над конечными полями

1.15	Квадратичные формы /Лек/	5	6	Л1.3Л2.2	Квадратичная форма, матрица и ранг квадратичной формы. Преобразование матрицы квадратичной формы при переходе к новому базису. Приведение квадратичной формы к каноническому и нормальному виду. Закон инерции квадратичных форм. Положительно определенные квадратичные формы. Критерий Сильвестра. Квадратичные формы в евклидовом векторном пространстве. Преобразование матрицы квадратичной формы при переходе к новому базису ортогональным преобразованием. Алгоритм приведения квадратичной формы к каноническому виду ортогональным преобразованием.
1.16	Квадратичные формы /Пр/	5	6	Л1.3Л2.2	Квадратичная форма, матрица и ранг квадратичной формы. Преобразование матрицы квадратичной формы при переходе к новому базису. Приведение квадратичной формы к каноническому и нормальному виду. Закон инерции квадратичных форм. Положительно определенные квадратичные формы. Критерий Сильвестра. Квадратичные формы в евклидовом векторном пространстве. Преобразование матрицы квадратичной формы при переходе к новому базису ортогональным преобразованием. Алгоритм приведения квадратичной формы к каноническому виду ортогональным преобразованием.
1.17	Квадратичные формы /Лаб/	5	2	Л1.3Л2.2	Приведение квадратичной формы к каноническому и нормальному виду. Закон инерции квадратичных форм. Положительно определенные квадратичные формы. Критерий Сильвестра. Приведения квадратичной формы к каноническому виду ортогональным преобразованием.
1.18	Квадратичные формы /Ср/	5	14	Л1.3Л2.2	Квадратичная форма, матрица и ранг квадратичной формы. Преобразование матрицы квадратичной формы при переходе к новому базису. Приведение квадратичной формы к каноническому и нормальному виду. Закон инерции квадратичных форм. Положительно определенные квадратичные формы. Критерий Сильвестра. Квадратичные формы в евклидовом векторном пространстве. Преобразование матрицы квадратичной формы при переходе к новому базису ортогональным преобразованием. Алгоритм приведения квадратичной формы к каноническому виду ортогональным преобразованием.
1.19	Основные алгебраические структуры /КСР/	5	4	Л1.3Л2.1 Л2.2	Отчет по индивидуальным заданиям
	<b>Введение в компьютерную алгебру</b>				
2.1	Компьютерная алгебра и численный анализ. /Лек/	5	2	Л1.3Л2.2	Особенности символьных алгоритмов. Стимулы к развитию систем аналитических вычислений. Соотношение аналитических и численных вычислений. О связи компьютерной алгебры и систем аналитических вычислений. Алгоритмическая неразрешимость. Элементы теории сложности.

2.2	Представление математических объектов. /Лек/	5	2	Л1.2 Л1.3Л2.2	Представления базовых объектов компьютерной алгебры. Канонические и нормальные, плотные и разреженные представления.
2.3	Системы компьютерной алгебры. /Лек/	5	2	Л1.2 Л1.3Л2.2	Основные системы компьютерной алгебры и их классификация. Типовая архитектура. Библиотеки алгоритмов и пакеты расширений. Пользовательские интерфейсы.
2.4	Представление математических объектов. /Пр/	5	4	Л1.2 Л1.3Л2.2	Представления базовых объектов компьютерной алгебры. Канонические и нормальные, плотные и разреженные представления.
2.5	Символьные вычисления в системах компьютерной алгебры /Лаб/	5	2	Л1.2 Л1.3Л2.2	Основные системы компьютерной алгебры и их классификация. Типовая архитектура. Библиотеки алгоритмов и пакеты расширений. Пользовательские интерфейсы.
2.6	Введение в компьютерную алгебру /Ср/	5	10	Л1.2 Л1.3Л2.2	Особенности символьных алгоритмов. Стимулы к развитию систем аналитических вычислений. Соотношение аналитических и численных вычислений. О связи компьютерной алгебры и систем аналитических вычислений. Алгоритмическая неразрешимость. Элементы теории сложности. Представления базовых объектов компьютерной алгебры. Канонические и нормальные, плотные и разреженные представления. Основные системы компьютерной алгебры и их классификация. Типовая архитектура. Библиотеки алгоритмов и пакеты расширений. Пользовательские интерфейсы.
	<b>Алгоритмические задачи в кольце многочленов от одной переменной</b>				
3.1	Факторизация многочленов /Лек/	6	4	Л1.2Л2.2	Разложение полиномов на неприводимые множители. Алгоритм Кронекера. Многочлены свободные от квадратов. Разложение полиномов на свободные от квадратов множители.
3.2	Факторизация многочленов /Пр/	6	4	Л1.2Л2.2	Неприводимые многочлены над различными полями. Разложение полиномов на неприводимые множители. Алгоритм Кронекера. Многочлены свободные от квадратов. Разложение полиномов на свободные от квадратов множители.
3.3	Факторизация многочленов /Лаб/	6	2	Л1.2Л2.2	Разложение полиномов на неприводимые множители над кольцом целых чисел. Алгоритм Кронекера. Многочлены свободные от квадратов. Разложение полиномов на свободные от квадратов множители.
3.4	Факторизация многочленов /Ср/	6	12	Л1.2Л2.2	Неприводимые многочлены над различными полями. Разложение полиномов на неприводимые множители. Алгоритм Кронекера. Многочлены свободные от квадратов. Разложение полиномов на свободные от квадратов множители.
3.5	Отделение корней многочлена /Лек/	6	2	Л1.1Л2.2	Отделение корней многочлена. Теорема Фурье -Бюдана. Метод Штурма. Теорема Сильвестра.
3.6	Отделение корней многочлена /Пр/	6	4	Л1.1Л2.2	Отделение корней многочлена. Теорема Фурье -Бюдана. Метод Штурма. Теорема Сильвестра.

3.7	Отделение корней многочлена /Лаб/	6	2	Л1.1Л2.2	Отделение корней многочлена. Теорема Фурье -Бюдана. Метод Штурма. Теорема Сильвестра.
3.8	Отделение корней многочлена /Ср/	6	10	Л1.1Л2.2	Отделение корней многочлена. Теорема Фурье -Бюдана. Метод Штурма. Теорема Сильвестра.
3.9	Контроль самостоятельной работы студентов /КСР/	6	1	Л1.1 Л1.2Л2.2	Отчет по индивидуальным заданиям
	<b>Кольца многочленов от нескольких переменных</b>				
4.1	Кольцо многочленов от нескольких переменных /Лек/	6	2	Л1.2 Л1.3Л2.2	Кольцо многочленов от нескольких переменных и его основные свойства. Упорядочение мономов в кольце многочленов от $n$ переменных.
4.2	Алгоритмические задачи в кольцах полиномов от нескольких переменных. /Лек/	6	4	Л1.3Л2.2	Системы уравнений и идеалы в кольцах многочленов. Задача полиномиального упрощения. Редукция полиномов. Базис Гребнера полиномиального идеала. Алгоритм Бухбергера вычисления базиса Гребнера. Решение систем полиномиальных уравнений.
4.3	Кольцо многочленов от нескольких переменных /Пр/	6	6	Л1.3Л2.2	Кольцо многочленов от нескольких переменных и его основные свойства. Упорядочение мономов в кольце многочленов от $n$ переменных. Алгоритмические задачи в кольцах полиномов от нескольких переменных. Системы уравнений и идеалы в кольцах многочленов. Задача полиномиального упрощения. Редукция полиномов. Базис Гребнера полиномиального идеала. Алгоритм Бухбергера вычисления базиса Гребнера. Решение систем полиномиальных уравнений.
4.4	Алгоритмические задачи в кольцах полиномов от нескольких переменных. /Лаб/	6	2	Л1.3Л2.2	Базис Гребнера полиномиального идеала. Алгоритм Бухбергера вычисления базиса Гребнера. Решение систем полиномиальных уравнений.
4.5	Кольцо многочленов от нескольких переменных /Ср/	6	16	Л1.3Л2.2	Кольцо многочленов от нескольких переменных и его основные свойства. Упорядочение мономов в кольце многочленов от $n$ переменных. Алгоритмические задачи в кольцах полиномов от нескольких переменных. Системы уравнений и идеалы в кольцах многочленов. Задача полиномиального упрощения. Редукция полиномов. Базис Гребнера полиномиального идеала. Алгоритм Бухбергера вычисления базиса Гребнера. Решение систем полиномиальных уравнений.
4.6	Контроль самостоятельной работы студентов /КСР/	6	1	Л1.2 Л1.3Л2.2	Отчет по индивидуальным заданиям
	<b>Коды, исправляющие ошибки.</b>				
5.1	Кодирование и декодирование. /Лек/	6	2	Л1.3Л2.1 Л2.2	Кодирование и декодирование. Двоичные коды. Коды, исправляющие ошибки. Коды Хемминга. Кодовое расстояние и количество исправляемых ошибок.
5.2	Кодирование и декодирование. /Пр/	6	4	Л1.3Л2.1 Л2.2	Кодирование и декодирование. Двоичные коды. Коды, исправляющие ошибки. Коды Хемминга. Кодовое расстояние и количество исправляемых ошибок. Построение двоичных кодов



5.3	Линейные коды /Лек/	6	2	Л1.3Л2.1 Л2.2	Линейные коды. Порождающая и проверочная матрицы линейного кода. Кодовое расстояние линейного кода. Синдром вектора.
5.4	Линейные коды /Пр/	6	4	Л1.3Л2.1 Л2.2	Линейные коды. Порождающая и проверочная матрицы линейного кода. Кодовое расстояние линейного кода. Синдром вектора.
5.5	Линейные коды Хемминга /Лаб/	6	2	Л1.3Л2.1 Л2.2	Линейные коды Хемминга. Кодирование. Обнаружение и исправление ошибок
5.6	Циклические коды. /Лек/	6	2	Л1.3Л2.2	Циклические коды. Обнаружение и исправление ошибок Порождающая и проверочная матрица циклического кода, порожденного многочленом.
5.7	Циклические коды /Пр/	6	4	Л1.3Л2.2	Циклические коды. Обнаружение и исправление ошибок Порождающая и проверочная матрица циклического кода, порожденного многочленом.
5.8	Коды, исправляющие ошибки /Ср/	6	16	Л1.3Л2.1 Л2.2	Кодирование и декодирование. Двоичные коды. Коды, исправляющие ошибки. Коды Хемминга. Кодовое расстояние и количество исправляемых ошибок. Линейные коды. Порождающая и проверочная матрицы линейного кода. Кодовое расстояние линейного кода. Синдром вектора. Циклические коды. Обнаружение и исправление ошибок Порождающая и проверочная матрица циклического кода, порожденного многочленом.

## 5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

### 5.1. Типовые задания для проведения текущего контроля

Задания, для тренировки навыков решения алгебраических задач в средах систем компьютерной алгебры:

1. Упростите алгебраическое выражение.
2. Раскройте скобки и приведите подобные слагаемые.
3. Разложите алгебраическое выражение на множители.
4. Разложите рациональную дробь на простейшие дроби.
5. Постройте график многочлена и найдите все их корни.

Примерный вариант индивидуального задания по теме «Кольца многочленов от одной переменной»:

1. Найдите произведение многочленов  $f(x)$  и  $g(x)$  в кольце  $Z_6[x]$ .
2. При делении многочлена  $f(x)$  на  $(x - x_1)$  в остатке получили  $r_1$ ; на  $(x - x_2)$  в остатке  $r_2$ . Найдите остаток при делении  $f(x)$  на  $(x - x_1)(x - x_2)$ .
3. Найдите кратность корня  $x_0$  многочлена  $f(x)$ .
4. Используя схему Горнера найти значение многочлена  $f(x)$  и его производных при  $x = x_0$ .
5. При каких значениях  $p$  и  $q$  многочлен  $f(x)$  делится на  $g(x)$ .
6. Используя алгоритм Евклида, найдите НОД многочленов  $f(x)$  и  $g(x)$ , а также его линейное представление.
7. Найти рациональные корни многочлена  $f(x)$ .
8. Разложить многочлен  $f(x)$  на неприводимые многочлены над полями  $Q, R$  и  $C$ .
9. Построение многочлена по его корням

Задания, направленные на формирование умений решать алгоритмические задачи в кольцах многочленов

1. Найдите наибольший общий делитель многочленов и его линейное представление.
2. Освободите многочлен от квадратов (кратных корней).
3. Разложите многочлен на неприводимые множители в  $F_3[x]$ .
4. Найдите все целые числа  $a$ , для которых все корни многочлена являются целыми.
5. Найдите все значения, при которых многочлены имеют общий корень.
6. Найдите все значения, при которых многочлен имеет кратный корень.
7. Постройте над  $Z_7$  многочлен  $f(x)$  наименьшей степени с условием  $f(0) = 1$ ,  $f(1) = 0$  и  $f(k) = k$  для остальных  $k$ .
8. Вычислить  $S$ -полином многочленов и , используя чисто лексикографическое упорядочение.

9. Проведите редукцию многочлена относительно множества , используя чисто лексикографическое упорядочение.
10. Найдите образующий элемент идеала, порожденного в кольце многочленов от одной переменной многочленами  $f(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6$  и  $g(x) = 3x^4 - 4x^3 - x^2 - x - 2$ .
11. Запишите неприводимый многочлен , над полем , определяющий поле  $F_9$ .
12. Покажите, что не является базисом Гребнера для чисто лексикографического упорядочения.
13. Решите систему алгебраических уравнений
14. Используя алгоритм Кронекера, разложить многочлен с целыми коэффициентами на неприводимые множители или доказать, что такого разложения не существует.
15. Построить редуцированный базис Грёбнера полиномиального идеала , считая и рассматривая чисто лексикографическое упорядочение.
16. Найдите базис Гребнера идеала используя упорядочения  $lex$  и  $degrevlex$  с  $x > y > z$ . Убедитесь, что в  $degrevlex$ -случае базис Гребнера выглядит проще.
17. Покажите на примере идеала , что базисы Гребнера при  $lex$ - и  $degrevlex$ -порядках могут совпадать, так что  $degrevlex$ -упорядочение не всегда лучше, чем  $lex$ .

Примерный вариант индивидуального задания на тему «Квадратичные формы»

1. Приведите квадратичную форму к нормальному виду методом Лагранжа, записать формулы преобразования координат, определить сигнатуру.
2. Привести квадратичную форму
  - а) к нормальному виду методом Лагранжа, записать формулы преобразования координат, определить сигнатуру квадратичной формы;
  - б) к каноническому виду методом ортогонального преобразования, написать соответствующее ортогональное преобразование.
  - в) Определите тип квадратичной формы (по каноническому виду квадратичной формы, по собственным значениям, по критерию Сильвестра).
3. Приведите к нормальному виду уравнение квадрики в трехмерном аффинном пространстве, установить вид квадрики, записать формулы преобразования координат.

## 5.2. Типовые задания для проведения промежуточной аттестации

Теоретические вопросы, выносимые на зачет (5 семестр)

1. Особенности символьных алгоритмов. Стимулы к развитию систем аналитических вычислений. Соотношение аналитических и численных вычислений.
2. Представления базовых объектов компьютерной алгебры. Канонические и нормальные, плотные и разреженные представления.
3. Группы. Основные определения. Примеры.
4. Кольца и поля. Основные определения и примеры.
5. Комплексные числа. Алгебраическая и тригонометрическая формы. Геометрическая интерпретация.
6. Операции над комплексными числами. Формула Муавра.
7. Многочлены от одной переменной. Теорема о делении с остатком.
8. Наибольший общий делитель двух многочленов. Алгоритм Евклида.
9. Неприводимые многочлены. Разложимость многочленов.
10. Корни многочлена. Теорема Безу. Схема Горнера.
11. Основная теорема алгебры (без доказательства). Многочлены над кольцом действительных чисел.
12. Квадратичная форма, матрица и ранг квадратичной формы.
13. Приведение квадратичной формы к каноническому и нормальному виду. Закон инерции квадратичных форм.
14. Положительно определенные квадратичные формы. Критерий Сильвестра.
15. Квадратичные формы в евклидовом векторном пространстве. Преобразование матрицы квадратичной формы при переходе к новому базису ортогональным преобразованием.
16. Алгоритм приведения квадратичной формы к каноническому виду ортогональным преобразованием.
17. Конечные поля. Построение конечных полей.

Теоретические вопросы к экзамену (6 семестр)

1. Группы. Основные определения. Примеры.
2. Конечные поля. Построение конечных полей.
3. Кольца и поля. Основные определения и примеры.
4. Расширения полей. Алгебраические и конечные расширения.
5. Отделение корней многочлена. Метод Штурма.
6. Неприводимые многочлены. Факторизация многочленов.
7. Факторизация многочленов над кольцом целых чисел. Алгоритм Кронекера.
8. Разложение полиномов на свободные от квадратов множители.
9. Разложение полиномов на свободные от квадратов множители.
10. Разложение на множители полиномов над конечными полями.

11. Системы уравнений и идеалы в кольцах многочленов.
12. Задача полиномиального упрощения. Редукция полиномов.
13. Идеал кольца. Базис идеала. Кольца главных идеалов.
14. Базис Гребнера полиномиального идеала.
15. Алгоритм Бухбергера вычисления базиса Гребнера.
16. Решение систем полиномиальных уравнений.
17. Двоичные коды. Коды, исправляющие ошибки.
18. Линейные коды. Проверочная и порождающая матрица линейного кода.
19. Циклические коды. Обнаружение и исправление ошибок

### 5.3. Перечень видов оценочных средств

### 5.4. Процедура применения оценочных материалов

Промежуточная аттестация может проводиться с применением электронного обучения и (или) дистанционных образовательных технологий в соответствии с «Порядком проведения промежуточной аттестации с применением электронного обучения и /или дистанционных образовательных технологий».

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, а также выполнения обучающимися индивидуальных заданий, контрольных и проверочных работ. Для активизации работы студентов в течение семестра и лучшего усвоения дисциплины предусмотрена балльно-рейтинговая система оценки успеваемости студентов.

Балльно-рейтинговая система оценки успеваемости студентов

#### 5 семестр

Максимальное количество (100 баллов) распределяется по следующей схеме:

- максимальное число баллов, набранных студентом в течение семестра – 70;
- максимальное число баллов за промежуточную аттестацию (зачет) – 30.

Отметка «зачтено» может выставляться по результатам текущего контроля знаний без промежуточной аттестации только студенту, набравшему в течение семестра не менее 65 баллов. В случае если такой студент желает повысить свой рейтинг, он проходит промежуточный контроль знаний на общих основаниях.

Шкала диапазона отметки на промежуточной аттестации:

БСР	Отметка на промежуточной аттестации	Примечание
41- 100	зачтено	На зачете необходимо набрать не менее 16 баллов.

В течение семестра баллы распределяются следующим образом:

- работа на занятиях, выполнение домашних заданий, письменные и устные опросы (до 30 баллов).
- выполнение и отчет по лабораторным работам (до 40 баллов).

#### 7 семестр

Максимальное количество (100 баллов) распределяется по следующей схеме:

- максимальное число баллов, набранных студентом в течение семестра – 70;
- максимальное число баллов за промежуточную аттестацию (экзамен) – 30.

В течение семестра баллы распределяются следующим образом:

- работа на занятиях, выполнение домашних заданий, письменные и устные опросы (до 30 баллов).
- выполнение и отчет по лабораторным работам (до 40 баллов).

Шкала диапазона отметки на промежуточной аттестации:

БСР	Отметка на промежуточной аттестации	На экзамене необходимо набрать
81- 100	5	не менее 20 баллов
61- 80	4	не менее 20 баллов
41- 60	3	не менее 16 баллов

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 6.1. Рекомендуемая литература

#### 6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год (кол-во экземпляров для печатных изданий)	Ссылка на электронное издание
--	---------------------	----------	---	----------------------------------

	Авторы, составители	Заглавие	Издательство, год (кол-во экземпляров для печатных изданий)	Ссылка на электронное издание
Л1.1	Кострикин А. И.	Введение в алгебру: учебник для студентов высших учебных заведений. Ч.1: Основы алгебры	М: Физматлит, 2009	<a href="http://biblioclub.ru/index.php?page=book&amp;id=62951">http://biblioclub.ru/index.php?page=book&amp;id=62951</a>
Л1.2	Панкратьев Е. В.	Элементы компьютерной алгебры: учебник	, 2007	<a href="http://biblioclub.ru/index.php?page=book&amp;id=233322">http://biblioclub.ru/index.php?page=book&amp;id=233322</a>
Л1.3	Балаба И. Н., Пихтильков С.А.	Абстрактная и компьютерная алгебра: Учебное пособие для студентов вузов	, 2008 (20 шт.)	

#### 6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год (кол-во экземпляров для печатных изданий)	Ссылка на электронное издание
Л2.1	Зяблицева Л. В., Корабельщикова С. Ю., Кузнецова И. В., Тихомиров С. А.	Алгебраические структуры и их приложения: учебное пособие	Архангельск: САФУ, 2015	<a href="http://biblioclub.ru/index.php?page=book&amp;id=436142">http://biblioclub.ru/index.php?page=book&amp;id=436142</a>
Л2.2	Царев А. В., Шеина Г. В.	Элементы абстрактной и компьютерной алгебры: учебное пособие	, 2016	<a href="http://biblioclub.ru/index.php?page=book&amp;id=471787">http://biblioclub.ru/index.php?page=book&amp;id=471787</a>

#### 6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Электронное обучение LMS Moodle
Э2	ЭБС "Университетская библиотека online"

#### 6.3. Информационные технологии

##### 6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения

1.	Операционная система Microsoft Windows Professional 7 Russian. Лицензия №48497058 от 13.05.2011 г., договор № Пр/16/6 от 05 апреля 2016 г.
2.	Операционная система Microsoft Windows 10 Professional Russian. Контракт № ПР/ФЕН/15/18 от 23.10.2015 г., договор № Пр/16/6 от 05 апреля 2016 г.
3.	Программное обеспечение Microsoft Office Enterprise 2007 Russian. Лицензия №46138962 от 16.11.2009
4.	Электронный словарь АBBYY Lingvo X3 Европейская версия - Код позиции AL14-2U1V05-102, АBBYY Lingvo x3 Европейская версия. Именная лицензия Concurrent от 28 июля 2009 г.
5.	Программа просмотра файлов формата RPD Adobe Acrobat Reader DC. Свободно распространяемое ПО
6.	ПО интерактивной доски Elite Panaboard. Свободно распространяемое ПО

##### 6.3.2 Перечень информационных справочных систем и профессиональных баз данных

1.	Портал «Информационно-коммуникационные технологии в образовании» ( <a href="http://www.ict.edu.ru">http://www.ict.edu.ru</a> )
2.	Портал Федеральных государственных образовательных стандартов высшего образования ( <a href="http://fgosvo.ru">http://fgosvo.ru</a> )

#### 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Ауд.	Назначение	Оборудование и технические средства обучения	Вид
4-301	Лекционная	доска учебная, стол преподавателя, столы учебные	Лек
4-324	Учебная аудитория	доска учебная, стол преподавателя, столы учебные, стул преподавателя	Пр
4-324	Учебная аудитория	доска учебная, стол преподавателя, столы учебные, стул преподавателя	Зачёт
4-322	Учебная аудитория	доска учебная, стол преподавателя, столы учебные, стул преподавателя	Пр
4-322	Учебная аудитория	доска учебная, стол преподавателя, столы учебные, стул преподавателя	КСР
4-304	Лекционная с мультимедийным комплексом	доска учебная, проектор, стол преподавателя, столы учебные, стул преподавателя, экран	Лек

Ауд.	Назначение	Оборудование и технические средства обучения	Вид
4-303	Помещение для самостоятельной работы	аудиоколонки, кондиционер, маркерная доска, столы компьютерные, столы учебные, компьютерная техника с возможностью подключения сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета	Ср
4-324	Учебная аудитория	доска учебная, стол преподавателя, столы учебные, стул преподавателя	Экзамен

#### 8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Целью освоения дисциплины является формирование у студентов базовых знаний по фундаментальной и компьютерной алгебре, рассмотреть основные задачи и алгоритмы в теории многочленов и теории квадратичных форм; познакомить с основными понятиями теории групп, колец и полей, элементами теории кодирования, с методами и приемами решения различных алгоритмических задач.

Дисциплина направлена на формирование у студентов навыков решения различных алгоритмических задач в кольцах многочленов от одной и нескольких переменных, знакомит студентов с широким кругом задач компьютерной алгебры, существенно расширяет примеры алгоритмов. Усвоение данной дисциплины поможет лучше осознать проблемы компьютерной безопасности, приобрести опыт практического использования систем компьютерной алгебры, понять важность основных алгебраических структур при построении современного программного обеспечения.

При подготовке к практическим и лабораторным занятиям необходимо проработать рекомендуемую учебно-методическую литературу (основную и дополнительную), чтобы применять знания к доказательству утверждений, решению задач, разработке и анализу алгоритмов.

Самостоятельная (внеаудиторная) работа предполагает такие виды деятельности, как подготовка сообщений, решение задач, выполнение индивидуальных заданий.

Эффективному закреплению полученных знаний по дисциплине способствует систематическая, хорошо организованная самостоятельная (внеаудиторная) работа, в рамках которой осуществляется выполнение индивидуальных заданий, подготовка к практическим занятиям и к зачету и экзамену.