МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук

УТВЕРЖДАЮ
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Т.А. Хагуров
подпись
«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.07.01 КОНЕЧНЫЕ ПОЛЯ И НЕКОТОРЫЕ ИХ ПРИЛОЖЕНИЯ

Направление подготовки 02.03.01 Математика и компьютерные науки

Направленность (профиль) Современная алгебра и криптография

Форма обучения очная

Квалификация бакалавр

Краснодар 2024

Р

абочая программа дисциплины КОНЕЧНЫЕ ПОЛЯ И НЕКОТОРЫЕ ИХ ПРИЛОЖЕНИЯ составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.01 Математика и компьютерные науки

Программу составили:

Н.А. Наумова, докт.техн. наук, доцент 

Рабочая программа дисциплины «Конечные поля и некоторые их приложения» утверждена на заседании кафедры (разработчика) функционального анализа и алгебры
протокол № 12 «07» мая 2024 г.

Заведующий кафедрой (разработчика) Барсукова В.Ю. 

Утверждена на заседании учебно-методической комиссии факультета
протокол № 3 « 14 » мая 2024 г.
Председатель УМК факультета Шмалько С.П.

фамилия, инициалы 

Рецензенты:

Пригодина А.Г., кандидат педагогических наук, доцент кафедры высшей математики КубГТУ

Марковский А.Н., кандидат физико-математических наук, доцент кафедры математического моделирования КубГУ

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Цель освоения дисциплины – дальнейшее формирование у студентов приобретенных на первых курсах знаний по алгебре.

1.2 Задачи дисциплины

Задачи освоения дисциплины «Конечные поля и некоторые их приложения»: получение базовых теоретических сведений по теории конечных полей, их приложениям, основам теории Галуа.

При освоении дисциплины вырабатывается общематематическая культура: умение логически мыслить, проводить доказательства основных утверждений, устанавливать логические связи между понятиями, применять полученные знания в теории кодирования. Получаемые знания лежат в основе математического образования и необходимы для понимания и освоения всех курсов математики, а также для продолжения обучения в магистратуре по соответствующему направлению подготовки.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Конечные поля и некоторые их приложения» относится к части, формируемой участниками образовательных отношений Блока 1 “ Дисциплины (модули)” учебного плана. В соответствии с рабочим учебным планом дисциплина изучается на 4 курсе по очной форме обучения. Вид промежуточной аттестации: 8 семестр - зачет.

Курс «Конечные поля и некоторые их приложения» продолжает начатое на первых двух курсах алгебраическое образование студентов соответствующего направления подготовки. Слушатели должны владеть математическими знаниями в рамках программы курса «Алгебра».

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	
ПК-1.1. Способен решать актуальные и важные задачи фундаментальной и прикладной математики	В результате изучения учебной дисциплины обучающийся знает основные понятия, идеи и методы изучаемой дисциплины, применяемые для решения задач фундаментальной и прикладной математики
	В результате изучения учебной дисциплины обучающийся умеет применять основные понятия, идеи и методы изучаемой дисциплины для решения задач фундаментальной и прикладной математики
	В результате изучения учебной дисциплины обучающийся владеет методами решения актуальных и важных задач фундаментальной и прикладной математики
ПК-1.4. Собирает и анализирует научно- техническую информацию с учетом базовых представлений, полученных в области фунда-	В результате изучения учебной дисциплины обучающийся знает методы анализа и обработки научно- технической информации с учетом базовых представлений,

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ментальной математики, механики, естественных наук, программирования и информационных технологий	полученных в области фундаментальной математики, механики, естественных наук, программирования и информационных технологий
	В результате изучения учебной дисциплины обучающийся умеет применять методы анализа и обработки научно- технической информации с учетом базовых представлений, полученных в области фундаментальной математики, механики, естественных наук, программирования и информационных технологий
	В результате изучения учебной дисциплины обучающийся владеет методами анализа и обработки научно-технической информации с учетом базовых представлений, полученных в области фундаментальной математики, механики, естественных наук, программирования и информационных технологий
ПК-5 Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	
ПК-5.1. Анализирует поставленные задачи и выбирает эффективные математические методы при создании алгоритмов и вычислительных программ для решения современных задач математики и механики	В результате изучения учебной дисциплины обучающийся знает эффективные математические методы при создании алгоритмов и вычислительных программ для решения современных задач математики и механики
	В результате изучения учебной дисциплины обучающийся умеет анализировать поставленные задачи и выбирает эффективные математические методы при создании алгоритмов и вычислительных программ для решения современных задач математики и механики
	В результате изучения учебной дисциплины обучающийся владеет навыками применения математических методов при создании алгоритмов и вычислительных программ для решения современных задач математики и механики
ПК-5.2. Описывает математические модели, формулирует, теоретически обосновывает и реализует программно численные методы для решения поставленных задач	В результате изучения учебной дисциплины обучающийся знает математические модели и программно численные методы для решения поставленных задач
	В результате изучения учебной дисциплины обучающийся умеет описывать математические модели, формулировать, теоретически обосновывать и реализовывать программно численные методы для решения поставленных задач
	В результате изучения учебной дисциплины обучающийся владеет методами реализации программно численные методы для решения поставленных задач на основании теоретически обоснованных математических моделей

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2 Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зачетные единицы (72 часа), их распределение по видам работ представлено в таблице

Виды работ		Всего часов	Форма обучения
			очная
			VIII семестр (часы)
Контактная работа, в том числе:		**34,2**	**34,2**
Аудиторные занятия (всего):		**30**	**30**
занятия лекционного типа		10	10
лабораторные занятия		20	20
практические занятия			
семинарские занятия			
Иная контактная работа:			
Контроль самостоятельной работы (КСР)		4	4
Промежуточная аттестация (ИКР)		0,2	0,2
Самостоятельная работа, в том числе:		**37,8**	**37,8**
Курсовая работа/проект (КР/КП) (подготовка)			
Контрольная работа		15	15
Расчётно-графическая работа (РГР) (подготовка)			
Реферат/эссе (подготовка)			
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.)		15	15
Подготовка к текущему контролю		7,8	7,8
Контроль:			
Подготовка к экзамену			
Общая трудоемкость	**час.**	**72**	**72**
	в том числе контактная работа	**34,2**	**34,2**
	зач. ед	**2**	**2**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в **восьмом** семестре:

.

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛЗ	СРС
1.	Кольца, поля, идеалы	8	1		2	5
2.	Многочлены над конечными полями	8	1		2	5
3.	Расширения полей	13,8	2		4	7,8
4.	Строение конечных полей	11	2		4	5

5.	Корни неприводимых многочленов над конечным полем	11	2		4	5
6.	Представление элементов конечных полей	8	1		2	5
7.	Теория кодирования	8	1		2	5
	ИТОГО по разделам дисциплины	67,8	10		20	37,8
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72				

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1	Кольца, поля, идеалы	Кольца, их классификация. Идеалы колец, фактор-кольца. Кольцо классов вычетов. Характеристика кольца. Гомоморфизмы колец. Характеристика конечного поля.	К
2	Многочлены над конечными полями	Кольцо многочленов над конечным полем. Алгоритм Евклида. Неприводимые многочлены. Каноническое разложение. Критерий поля.	К
3	Расширения полей	Простые расширения. Степень расширения. Простые алгебраические расширения. Алгебраические расширения. Теорема о существовании и единственности поля разложения.	К
4	Строение конечных полей	Количество элементов конечного поля. Существование и единственность конечных полей. Поля Галуа. Мультипликативная группа конечного поля.	К
5	Корни неприводимых многочленов над конечным полем	Корни неприводимых многочленов над конечным полем. Число нормированных неприводимых многочленов. Минимальные многочлены. Нахождение примитивных многочленов. Изоморфизм полей разложения неприводимых многочленов. Сопряженные элементы относительно поля. Автоморфизмы поля F_{q^m} над F_q (автоморфизм Фробениуса). Дуальный базис, нормальный базис конечного расширения над конечным полем.	К
6	Представление элементов конечных полей	Представление элементов конечных полей. Круговое поле. Круговые многочлены. Сопровождающая матрица многочлена.	К
7	Теория кодирования	Основная задача теории кодирования. Коды, исправляющие ошибки. Циклические коды. Коды Хэмминга. Коды БЧХ.	К

2.3.2 Занятия семинарского типа (практические / семинарские занятия/ лабораторные работы)

№	Наименование раздела (темы)	Тематика занятий/работ	Форма текущего контроля
1	Кольца, поля, идеалы	Кольца, их классификация. Идеалы колец, фактор-кольца. Кольцо классов вычетов. Характеристика кольца. Гомоморфизмы колец. Характеристика ко-	Проверка домашнего задания. Контрольная работа

		нечного поля.	
2	Многочлены над конечными полями	Кольцо многочленов над конечным полем. Алгоритм Евклида. Неприводимые многочлены. Каноническое разложение. Критерий поля.	Проверка домашнего задания. Контрольная работа
3	Расширения полей	Простые расширения. Степень расширения. Простые алгебраические расширения. Алгебраические расширения. Теорема о существовании и единственности поля разложения.	Проверка домашнего задания. Контрольная работа
4	Строение конечных полей	Количество элементов конечного поля. Существование и единственность конечных полей. Поля Галуа. Мультипликативная группа конечного поля.	Проверка домашнего задания. Контрольная работа
5	Корни неприводимых многочленов над конечным полем	Корни неприводимых многочленов над конечным полем. Число нормированных неприводимых многочленов. Минимальные многочлены. Нахождение примитивных многочленов. Изоморфизм полей разложения неприводимых многочленов. Сопряженные элементы относительно поля. Автоморфизмы поля F_{q^m} над F_q (автоморфизм Фробениуса). Дуальный базис, нормальный базис конечного расширения над конечным полем.	Проверка домашнего задания. Контрольная работа
6	Представление элементов конечных полей	Представление элементов конечных полей. Круговое поле. Круговые многочлены. Сопровождающая матрица многочлена.	Проверка домашнего задания. Контрольная работа
7	Теория кодирования	Основная задача теории кодирования. Коды, исправляющие ошибки. Циклические коды. Коды Хэмминга. Коды БЧХ.	Проверка домашнего задания. Контрольная работа

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

2.3.2 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид самостоятельной работы	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	**2**	**3**
1.	Подготовка к текущему контролю	1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г. 2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

		3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г. 4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г.
2.	Выполнение лабораторных работ и расчетно-графических заданий	1. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г. 2. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.
4.	Подготовка и оформление отчетов по практике	Методические указания по подготовке и оформлению отчета по практике. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.
5.	Выполнение и защита выпускной квалификационной работы	Методические указания по выполнению и защите выпускной квалификационной работы (бакалавриат, магистратура, специалитет). Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

3. Образовательные технологии, применяемые при освоении дисциплины (модуля)

В ходе изучения дисциплины предусмотрено использование следующих образовательных технологий: лекции, лабораторные занятия, проблемное обучение, модульная технология, подготовка письменных аналитических работ, самостоятельная работа студентов.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий и активных методов (проектных методик, мозгового

штурма, разбора конкретных ситуаций, анализа педагогических задач, педагогического эксперимента, иных форм) в сочетании с внеаудиторной работой.

Информационные технологии, применяемые при изучении дисциплины: использование информационных ресурсов, доступных в информационно-телекоммуникационной сети Интернет.

Адаптивные образовательные технологии, применяемые при изучении дисциплины – для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «*Алгебра*».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме разноуровневых заданий для контрольных работ, теоретических вопросов к коллоквиуму, доклада-презентации по проблемным вопросам и **промежуточной аттестации** в форме вопросов и заданий к экзамену.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ПК-1.1. Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	В результате изучения учебной дисциплины обучающийся знает основные понятия, идеи и методы изучаемой дисциплины, применяемые для решения задач фундаментальной и прикладной математики	Контрольная работа №1 Контрольная работа №2	Вопрос на зачете 1-14
		В результате изучения учебной дисциплины обучающийся умеет применять основные понятия, идеи и методы изучаемой дисциплины для решения задач фундаментальной и прикладной математики		
		В результате изучения учебной дисциплины обучающийся владеет методами решения актуальных и важных задач фундаментальной и прикладной математики		
2	ПК-1.4. Собирает и анализирует научно- техническую информацию с учетом базовых представлений, полученных в области фундаментальной математики, механики, естественных наук, программирования и информационных технологий	В результате изучения учебной дисциплины обучающийся знает методы анализа и обработки научно- технической информации с учетом базовых представлений, полученных в области фундаментальной математики, механики, естественных наук, программирования и информа-	Контрольная работа №1 Контрольная работа №2	Вопрос на зачете 1-14

		ционных технологий		
		В результате изучения учебной дисциплины обучающийся умеет применять методы анализа и обработки научно- технической информации с учетом базовых представлений, полученных в области фундаментальной математики, механики, естественных наук, программирования и информационных технологий		
		В результате изучения учебной дисциплины обучающийся владеет методами анализа и обработки научно- технической информации с учетом базовых представлений, полученных в области фундаментальной математики, механики, естественных наук, программирования и информационных технологий		
3	ПК-5.1. Анализирует поставленные задачи и выбирает эффективные математические методы при создании алгоритмов и вычислительных программ для решения современных задач математики и механики	В результате изучения учебной дисциплины обучающийся знает эффективные математические методы при создании алгоритмов и вычислительных программ для решения современных задач математики и механики	Контрольная работа №1 Контрольная работа №2	Вопрос на зачете 1-14
		В результате изучения учебной дисциплины обучающийся умеет анализировать поставленные задачи и выбирает эффективные математические методы при создании алгоритмов и вычислительных программ для решения современных задач математики и механики		
		В результате изучения учебной дисциплины обучающийся владеет навыками применения математических методов при создании алгоритмов и вычислительных программ для решения современных задач математики и механики		
4	ПК-5.2. Описывает математические модели, формулирует, теорети-	В результате изучения учебной дисциплины обучающийся знает математи-	Контрольная работа №1 Контрольная работа №2	Вопрос на зачете 1-14

	чески обосновывает и реализует программно численные методы для решения поставленных задач	ческие модели и программно численные методы для решения поставленных задач		
		В результате изучения учебной дисциплины обучающийся умеет описывать математические модели, формулировать, теоретически обосновывать и реализовывать программно численные методы для решения поставленных задач		
		В результате изучения учебной дисциплины обучающийся владеет методами реализации программно численные методы для решения поставленных задач на основании теоретически обоснованных математических моделей		

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерный перечень вопросов и заданий

1. Доказать, что минимальное подполе любого поля характеристики 0 изоморфно полю рациональных чисел.
2. Доказать, что минимальное подполе любого поля характеристики p изоморфно полю GF(p).
3. Решить уравнение $4x = 1$ в поле Z/(101).
4. Найти 73^{-1} в поле Z/(103).
5. (Теорема Вильсона.) Доказать, что для простого p:

$$(p-1)! \equiv -1 \pmod{p}$$

6. Многочлен $f(x) = x^2+ax+b$, $a,b \in$ GF(5), неприводим над GF(5). Верно ли, что $f(x)$ неприводим над GF(125)?
7. Является ли $x^4 + 1$ неприводимым многочленом над полем GF(3)?
8. Многочлен $x^5+x^3+x^2+1$ разложить на неприводимые множители над полем вычетов по модулю 2.
9. Многочлен $x^3 +2x^2 +4x+1$ разложить на неприводимые множители над полем вычетов по модулю 5.
10. Многочлен x^4+x^3+x+2 разложить на неприводимые множители над полем вычетов по модулю 3.
11. Многочлен $x^4 +3x^3 +2x^2 +x+4$ разложить на неприводимые множители над полем вычетов по модулю 5.
12. Разложить на неприводимые множители над полем вычетов по модулю 2 все нормированные многочлены второй степени от x.
13. Разложить на неприводимые множители над полем вычетов по модулю 2 все нормированные многочлены третьей степени от x.

14. Найти все нормированные многочлены второй степени от x, неприводимые над полем вычетов по модулю 3.
15. а) Проверить, что $F = GF(7)[x]/(x^2 + x - 1)$ является полем.
б) выразите обратный к $(1-x)$ в F в базисе $1,x$.
16. Найти порядок элемента $x+x^2$ в мультипликативной группе
а) поля $GF(2)[x]/(x^4 + x + 1)$;
б) поля $GF(2)[x]/(x^4 + x^3 + 1)$.
17. Найти количество неприводимых многочленов
а) степени 7 над полем GF(2);
б) степени 6 над полем GF(5);
в) степени 24 над полем GF(3).
18. Построить изоморфизм между полями
$GF(7)[x]/(x^2 + x - 1)$ и $GF(7)[x]/(x^2 + 1)$.
19. Представить элементы поля F_{3^2} двумя способами
20. Представить элементы поля F_{2^3} двумя способами
21. В поле $F_p[x]/(f(x))$ (из задания 1) найти значение выражения, представив результат в полиномиальном и матричном видах:
$\frac{\alpha^4 \cdot (\alpha^2 + \alpha + 1)}{\alpha^{10}(\alpha^2 + 1)}$, где α – корень многочлена $f(x) = x^3 + x + 1,\ p = 2$
22. Проверить, что многочлен $f(x)$ над полем F_p свободен от квадратов и, используя алгоритм Берлекемпа, разложить многочлен $f(x)$ на множители.
23. Рассмотрим код Хэмминга систематического кодирования с порождающим примитивным полиномом $a(x) = x^3 + x + 1$ над полем F_2. Требуется декодировать полиномы $w(x)$. После этого проверить, что для исправленного сообщения синдром равен нулю.

Контрольная работа № 1

I. 1.1 Составить таблицу Кэли для аддитивной группы Z_n и ее собственных подгрупп. Выписать различные смежные классы по каждой из них, найти индексы каждой из фактор-групп.
1.2. Составить таблицы Кэли операций + и · для фактор-колец $Z/(n)$
II. 1.1. Применяя алгоритм Евклида, найти НОД (f; g) для данных многочленов из указанного поля F
1.2. Найти все неприводимые многочлены степени n над полем F_p
III. 1.1. Доказать, что многочлен $P(x)$ является неприводимым над полем F_p
1.2. Построить расширение $F_p[x]/(P(x))$ поля F_p, используя идеал $(P(x))$, привести таблицы Кэли операций + и ·.
IV. 1.1. Выяснить, имеет ли многочлен $f(x)$ кратные корни над полем F_p
1.2. Разложить многочлен на неприводимые множители над полем F_p

Контрольная работа № 2

I. 1.1. Найти все примитивные элементы поля F_{p^2}
1.2. Выписать все подполя конечного поля F_k

II. 1.1. Найти минимальный многочлен $m(x) \in F_p[x]$, который имеет корень α^k, где α - примитивный элемент поля $F_p[x] = F_p[x]/(g(x))$

1.2. Найти количество неприводимых многочленов степени n над полем F_p

III. 1.1. Определить степени всех неприводимых многочленов в разложении $x^n - 1$ над полем F_p

1.2. Найти разложение $x^n - 1$ на неприводимые множители над полем F_p

IV. Представить элементы поля F_q двумя способами

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен/зачет)

Примерный перечень вопросов к зачету

1. Группы, кольца, поля (основные определения)
2. Многочлены, кольцо многочленов, неприводимые многочлены над полем F
3. Расширение полей, простые поля, алгебраические расширения над полем К
4. Характеризация конечных полей
5. Корни неприводимых многочленов над полем К
6. Дуальный базис, нормальный базис конечного расширения над конечным полем.
7. Корни из единицы и круговые многочлены
8. Представление элементов конечных полей
9. Теорема Веддерберна
10. Порядки многочленов над конечными полями, примитивные многочлены
11. Неприводимые многочлены над полем F_q
12. Построение неприводимых многочленов
13. Основная задача теории кодирования. Коды, исправляющие ошибки.
14. Циклические коды. Коды Хэмминга. Коды БЧХ.

Критерии оценивания результатов обучения

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает методы доказательства основных утверждений, устанавливает логические связи между понятиями, владеет навыками применения методов изучаемой дисциплины для решения базовых задач, допускает незначительные ошибки; студент умеет правильно объяснять теоретический материал, иллюстрируя его примерами.

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры, иллюстрирующие теоретический материал, имеет довольно ограниченный объем знаний о базовых понятиях изучаемой дисциплины.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1 Учебная литература

1. Кострикин, А.И. Введение в алгебру. Часть 3. Основные структуры [Электронный ресурс] : учеб. — Электрон. дан. — Москва : Физматлит, 2001. — 272 с. — Режим доступа: https://e.lanbook.com/book/59284

2. Туганбаев, А. А. Алгебраические структуры : учебник для вузов / А. А. Туганбаев. — Санкт-Петербург : Лань, 2024. — 164 с. — ISBN 978-5-507-48163-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394511

3. Винберг, Э.Б. Курс алгебры : учебник / Э.Б. Винберг. - Москва : МЦНМО, 2011. - 591 с. - ISBN 978-5-94057-685-3; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=63299

4. . Сергеев, Александр Эдуардович (КубГУ). Основы теории Галуа [Текст] : монография / А. Э. Сергеев, Э. А. Сергеев ; М-во образования и науки Рос. Федерации, Кубанский гос. ун-т. - Краснодар : [Кубанский государственный университет], 2014. - 334 с. - Библиогр.: с. 327-332. - ISBN 9785820910791.

5.2. Периодическая литература

1. Журнал “Вестник Московского университета. Серия 01. Математика. Механика”/ - Издательство Московского университета. – ISSN 0579-9368. - https://dlib.eastview.com/browse/publication/9045

2. Журнал "Известия высших учебных заведений. Математика" ISSN 0021-3446 (Print), ISSN 2076-4626 (Online) . - Учредитель и издатель: Казанский (Приволжский) федеральный университет. - https://dlib.eastview.com/browse/publication/7087

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru

3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;

14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины (модуля)

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, лабораторных занятий, в ходе которых студентами приобретаются и закрепляются основные практически навыки решения различных задач, в том числе с применением полученных теоретических знаний.

Важнейшим этапом курса является самостоятельная работа по дисциплине. Самостоятельная работа студентов является неотъемлемой частью процесса подготовки. Под самостоятельной работой понимается часть учебной планируемой работы, которая выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа направлена на усвоение системы научных и профессиональных знаний, формирования умений и навыков, приобретение опыта самостоятельной творческой деятельности. СРС помогает формировать культуру мышления студентов, расширять познавательную деятельность.

Виды самостоятельной работы по курсу:

а) по целям: подготовка к лекциям, к практическим занятиям, к контрольной работе, к коллоквиуму; подготовка научного доклада и выполнение заданий по НИР.

б) по характеру работы: изучение литературы, конспекта лекций; поиск литературы в библиотеке; конспектирование рекомендуемой для самостоятельного изучения научной литературы; решение задач, тестов; работа с обучающими и контролирующими программами.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведе-	Мебель: учебная мебель	Microsoft Office;

ния занятий лекционного типа	Технические средства обучения: экран, проектор, компьютер	Программы для демонстрации и создания презентаций («Microsoft Power Point»)
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Microsoft Office; Программы для демонстрации и создания презентаций («Microsoft Power Point»)

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, вебкамеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Помещение для самостоятельной работы обучающихся (ауд.302)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, вебкамеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	