МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Согласовано

Школа естественных наук)
Руководитель ОП
_____ Степанова А.А.
(подпись) (Ф.И.О. рук. ОП)
«11» июля 2019 г.

«УТВЕРЖДАЮ»

Заведующий кафедрой адгебры, геометрии и анализа
_____ Шепелева Р.П.
(подпись) (Ф.И.О. зав. каф.)
«11» июля 2019 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Конечные поля

Направление подготовки 01.04.01 Математика

магистерская программа «Алгебра»

Форма подготовки очная

Школа естественных наук
Кафедра алгебры, геометрии и анализа
курс 1 семестр 1
лекции 36 час.
практические занятия 36 час.
самостоятельная работа студентов 54
контрольные работы 54
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 36 час.
зачет
экзамен 1 семестр

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 10 января 2018 г. № 12

Рабочая программа обсуждена на заседании кафедры Алгебры, геометрии и анализа «8» июля 2019 г.

Заведующий (ая) кафедрой к.ф.-м.н., профессор Р.П.Шепелева
Составитель (ли): к.ф.-м.н, доцент С.Г.Чеканов

Владивосток

2019

Оборотная сторона титульного листа РПУД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

Аннотация рабочей программы учебной дисциплины
«Конечные поля»

Рабочая программа учебной дисциплины «Конечные поля» разработана для студентов 1 курса направления магистратуры 01.04.01 «Математика», магистерской программы «Алгебра», в соответствии с требованиями федерального государственного стандарта высшего образования и образовательного стандарта, самостоятельно устанавливаемого ДВФУ.

Общая трудоемкость освоения дисциплины составляет 5 ЗЕ (180 час.). Учебным планом предусмотрены лекции (36 час.), практические занятия (36 час.), самостоятельная работа студента (54 час.), в том числе на подготовку к экзамену (54 час.). Дисциплина «Конечные поля» входит в часть формируемую участниками образовательных отношений, реализуется на 1 курсе, в 1 семестре.

Дисциплина «Конечные поля» логически и содержательно связана с такими курсами, как «Кольца и модули», «Теория групп», «Криптографические методы защиты информации».

Содержание дисциплины охватывает круг вопросов, связанных с построением конечных полей и их расширений, изучением структурных свойств полей, построением шифров и кодов над конечными полями.

Курс построен на таких ранее изученных дисциплинах как «Алгебра», «Дискретная математика».

Цель преподавания дисциплины - знакомство студентов с современными концепциями и алгоритмами в теории конечных полей, их приложениями в теории информации и криптографии.

Задачи преподавания дисциплины:

1. овладение основными концепциями современной теории конечных полей;
2. ознакомление с современными алгоритмами в конечных полях;

3. изучение основных понятий и конструкций для представления конечных полей;

4. применение полученных знаний при изучении явлений природы и общества и исследование простейших процессов с помощью методов теории конечных полей.

Для успешного изучения дисциплины «Конечные поля» у обучающихся должны быть сформированы следующие предварительные компетенции

- способность видеть методологические аспекты построения математических теорий;
- применять системный подход в формализации математических задач;
- способностью к абстрактному мышлению, анализу, синтезу.

Планируемые результаты обучения по данной дисциплине (знания, умения, владения), соотнесенные с планируемыми результатами освоения образовательной программы, характеризуют этапы формирования следующих профессиональных компетенций:

Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
Тип задач профессиональной деятельности: Научно-исследовательский			

планирование и реализация научно-исследовательской деятельности в области математики и ее приложений	Универсальная алгебра и алгебраические методы криптографии. Методы и концепции математической логики. Алгоритмы и конструкции алгебраической геометрии.	ПК-1. способен к интенсивной научно-исследовательской работе	ПК1.1. Умеет: правильно ставить задачи по выбранной тематике, выбирать для исследования необходимые методы; применять выбранные методы к решению научных задач, оценивать значимость получаемых результатов ПК-1.2. Знает: классические и современные методы решения задач по выбранной тематике научных исследований; новые научные результаты, связанные с тематикой научных исследований работы магистранта ПК-1.3 Владеет: навыками критического анализа и оценки современных достижений и результатов деятельности по решению исследовательских и практических задач; навыками выступлений на научно-тематических конференциях и современными методами решения задач по выбранной тематике научных исследований
Тип задач профессиональной деятельности: Педагогический			
проектирование, планирование и реализация образовательного процесса по математике в образовательном учреждении высшего и общего образования в соответствии с требованиями ФГОС основного общего	Универсальная алгебра и алгебраические методы криптографии. Методы и концепции математической логики. Алгоритмы и конструкции	ПК-3 Способен осуществлять обучение учебному предмету на основе использования предметных методик и современных образовательных технологий	ПКО-3.1. Умеет: проектировать элементы образовательной программы, рабочую программу преподавателя по математике; формулировать дидактические цели и задачи обучения математике и реализовывать их в образовательном процессе по математике; обосновывать выбор методов обучения математике и

образования и ФГОС среднего общего образования	алгебраической геометрии.		образовательных технологий, применять их в образовательной практике, исходя из особенностей содержания учебного материала и образовательных потребностей обучаемых; планировать и комплексно применять различные средства обучения математике ПКО-3.2. Знает: концептуальные положения и требования к организации образовательного процесса по математике; особенности проектирования образовательного процесса по математике в образовательном учреждении высшего образования, подходы к планированию образовательной деятельности; формы, методы и средства обучения математике, современные образовательные технологии, методические закономерности их выбора; особенности частных методик обучения математике ПКО-3.3. Владеет: умениями по планированию и проектированию образовательного процесса; методами обучения математике и современными образовательными технологиями

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

ЛЕКЦИИ (36 ЧАСОВ)

Тема 1. Введение (4 часа).

Группы, кольца, поля. Гомоморфизмы колец. Кольца многочленов.

Тема 2. Характеристика поля (4 часа).

Характеристика поля. Теорема о характеристике. Фактор кольцо по максимальному идеалу.

Тема 3. Простые расширения конечных полей (4 часа).

Кольцо многочленов от одной переменной над конечным полем. Неприводимые многочлены. Идеалы в кольце многочленов. Простые расширения и корни неприводимых многочленов.

Тема 4. Строение конечных полей (4 часа).

Подполя конечных полей. Теорема о существовании и единственности конечного поля.

Тема 5. Мультипликативная группа конечного поля (8 часа).

Теорема о примитивном элементе. Оценка числа примитивных элементов. Примитивные многочлены над конечным полем.

Тема 6. Линейные рекуррентные последовательности (8 часа)

Рекуррентные соотношения и регистры сдвига с обратной связью. Характеристический многочлен и матрица линейной рекуррентной последовательности. Оценка периода линейно рекуррентной последовательности, алгоритм Берлекемпа-Месси.

Тема 7. Алгебраические коды (4 часа).

Линейные пространства над конечными полями. Коды обнаруживающие и исправляющие ошибки.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (_36_час.)

Занятие 1. Введение(3_час.)

1. Рассматриваются примеры группы, колец, полей.

2. Изучается алгоритм деления с остатком.
3. Теорема Безу. Основная теорема алгебры.
4. Гомоморфизмы колец и факторкольца. Алгоритм Евклида.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 2. Характеристика поля (3 час.)

1. Характеристика поля и ее влияние на арифметические и алгебраические свойства поля. Теорема о характеристике поля.
2. Конечное поле как линейное пространство. Различные представления элементов конечного поля.
3. Решение уравнений над конечными полями.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 3. Алгебраические расширения конечных полей (6 час.).

1. Построения простых расширений небольших конечных полей.
2. Кольцо многочленов от одной переменной над конечным полем.
3. Разложение многочленов на неприводимые множители.
4. Вычисление минимальных многочленов для элементов расширения.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 4. Строение конечных полей (6 час.).

1. Теорема о строении конечных полей.
2. Поле разложения многочлена.
3. Характеризация конечных полей с помощью кольца многочленов.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 5. Мультипликативная группа конечного поля (6 час.).

1. Теорема о примитивном элементе. Оценка числа примитивных элементов конечного поля.
2. Построение базисов алгебраических расширений конечных полей.
3. Представления элементов конечных полей.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 6. Линейные рекуррентные последовательности (6 час.).

1. Линейные рекуррентные последовательности над конечными полями.
2. Характеризация последовательностей с помощью рекуррентных соотношений.
3. Характеристический полином и сопровождающая матрица рекуррентной последовательности. Вычисление периода последовательности, алгоритм Берлекемпа-Месси.
4. Линейные группы и рекуррентные последовательности.

Занятие проводится с использованием метода активного обучения «групповая консультация».

Занятие 7. Алгебраические коды и шифры над конечными полями (6 час.).

1. Построение кодов над конечными полями, оценка числа распознаваемых и исправляемых ошибок.
2. Создание генераторов ключевых последовательностей для поточных шифров.

Занятие проводится с использованием метода активного обучения «групповая консультация».

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Конечные поля» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Введение	ПК-1	знает	Конспект (ПР-7)	Вопросы к экзамену 1-5
			умеет	Коллоквиум (УО-2) ИДЗ	Примеры ИДЗ «Алгоритм Евклида»
			владеет	Доклад, сообщение (УО-3)	
2	Характеристика поля	ПК-1	знает		Вопросы к экзамену 6-10
			умеет	Коллоквиум (УО-2)	
			владеет	Контрольная работа (ПР-2)	Примерный вариант КР «Алгоритм Евклида»
3	Простые расширения конечных полей	ПК-1	знает		Вопросы к экзамену 11-12
			умеет	ИДЗ	Примеры ИДЗ «Алгебраические расширения конечных полей»

			владеет	Реферат (ПР-4)	
4	Строение конечных полей	ПК-6	знает	Реферат (ПР-4)	Вопросы к экзамену 13-14
			умеет	Коллоквиум (УО-2) ИДЗ	Примеры ИДЗ «Неприводимость многочленов над конечным полем»
			владеет	Круглый стол (УО-4)	
5	Мультипликативная группа конечного поля	ПК-6	знает	Коллоквиум (УО-2)	Вопросы к экзамену 15
			умеет	ИДЗ	Примеры ИДЗ «Теорема о примитивном элементе»
			владеет	Круглый стол (УО-4)	
6	Линейные рекуррентные последовательности	ПК-6	знает	Коллоквиум (УО-2)	Вопросы к экзамену 16-18
			умеет	ИДЗ	Примеры ИДЗ «Представление элементов конечного поля с помощью многочленов»
			владеет	Контрольная работа (ПР-2)	Примерный вариант КР «Строение конечных полей»
7	Алгебраические коды	ПК-6	знает		Вопросы к экзамену 19
			умеет	Реферат (ПР-4)	
			владеет		

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений,

навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Ю. Л. Сагалович, Введение в алгебраические коды: учебное пособие. Москва : Изд-во Института проблем передачи информации РАН , 2014 http://lib.dvfu.ru:8080/lib/item?id=chamo:756734&theme=FEFU

2. Гаррет Биркгоф, Томас К. Барти, Современная прикладная алгебра : [учебное пособие для втузов]. Санкт-Петербург : Лань, 2009. http://lib.dvfu.ru:8080/lib/item?id=chamo:250614&theme=FEFU

Дополнительная литература

(печатные и электронные издания)

1. А. Г. Курош, Курс высшей алгебры – М.: Наука, 2005.

2. Р. Лидл, Г. Нидеррайтер, Конечные поля – М.: «Мир», Том 1, 2. 1988.

3. Д. К. Фаддеев, И. С. Соминский, Задачи по высшей алгебре. – Санкт-Петербург, «Лань», 1998, - 288 с.

4. Виноградов И.М., Основы теории чисел. – М.: Наука, 1972 – 176 с.. Электронный ресурс]: URL: http://eqworld.ipmnet.ru/ru/library/books/Vinogradov1972ru.djvu (Дата обращения 12.05.2014).

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Allmath.ru – электронная библиотека по различным разделам математики.

2. http://e.lanbook.com/books/element.php?pl1_id=56403 Игнатьев М.В. Введение в метод орбит над конечным полем: Изд-во МЦНМО.-2012
3. http://e.lanbook.com/books/element.php?pl1_id=59284 Кострикин А.И. Введение в алгебру. Часть 3. Основные структуры: Изд-во Физматлит.-2008

Перечень информационных технологий и программного обеспечения

1. Mathcad
2. Maple

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

На изучение дисциплины отводится 72 часа аудиторных занятий. На лекциях преподаватель объясняет теоретический материал. Вводит основные понятия, определения, свойства. Формулирует и доказывает теоремы. Приводит примеры. Необходимо поддерживать непрерывный контакт с аудиторией, отвечать на возникающие у студентов вопросы. На практических занятиях преподаватель разбирает примеры по пройденной теме. Во второй части занятия студентам предлагается работать самостоятельно, выполняя задания по теме. Преподаватель контролирует работу студентов, отвечает на возникающие вопросы, подсказывает ход и метод решения. Если знаний полученных в аудитории оказалось недостаточно, студент может самостоятельно повторно прочитать лекцию. После выполнения задания, студент отправляет его на проверку преподавателю. Работа должна быть отослана в формате PDF одним документом.

По данному курсу разработаны методические указания: Чеканов С.Г., Степанова А.А., Строение конечных полей. Учебно-методическое пособие. Изд. ДВФУ. Владивосток, 2013, 30 с..

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Дисциплина обеспечена учебно-методической литературой посредством библиотечного фонда университета, методическими указаниями,

раздаточными материалами, бланками билетов на экзамен. Учебные аудитории кампуса ДВФУ оборудованы мультимедиа оборудованием.

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Конечные поля»

Направление подготовки 01.04.01 Математика

магистерская программа «Алгебра»

Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1) Характеристика поля	1.09 - 28.09	индивидуальное домашнее задание	1 неделя	Проверка ИДЗ
2) Алгебраические расширения конечных полей	28.09 - 28.10	индивидуальное домашнее задание	1 неделя	Контрольная работа
3) Строение конечных полей	05.11 - 12.11	индивидуальное домашнее задание	1 неделя	Проверка ИДЗ
4) Мультипликативная группа конечного поля	13.11 - 20.11	индивидуальное домашнее задание	1 неделя	Проверка ИДЗ
5) Линейные рекуррентные последовательности	10.03 - 17.03	индивидуальное домашнее задание	1 неделя	Проверка ИДЗ
6) Алгебраические коды и шифры над конечными полями	20.03 - 27.04	индивидуальное домашнее задание	1 неделя	Контрольная работа Проверка ИДЗ
7) Характеристика поля	20.04 - 27.04	индивидуальное домашнее задание	1 неделя	

Методические указания по подготовке к практическим занятиям

Подготовка к практическим занятиям включает в себя изучение конспектов лекций, изучение рекомендуемой литературы и составление опорных конспектов, включающих основные понятия и определения, формулы и приложения. Решение задач для самостоятельного решения.

Методические указания по подготовке к контрольной работе

Подготовка к контрольной работе включает в себя, помимо изучения рекомендуемой литературы, лекционного материала и материалов практических занятий, выполнение индивидуального домашнего задания (ИДЗ).

Методические указания по выполнению ИДЗ

Материалы для самостоятельной работы студентов подготовлены в виде индивидуальных домашних заданий по каждой теме (образцы типовых ИДЗ

представлены в разделе «Материалы для самостоятельной работы студентов»). Работа должна быть отправлена преподавателю на проверку. Оформление в формате PDF. Каждое выполненное задание должно сопровождаться полным текстом его условия и теоретическим материалом, обосновывающим подробное решение без опускания промежуточных расчетов, которые невозможно выполнить устно. ИДЗ выполняются студентами в соответствии с графиком выполнения самостоятельной работы. Критерии оценки: студент получает максимальный балл, если работа выполнена без ошибок и оформлена в соответствии с требованиями преподавателя.

По данной дисциплине разработаны методические рекомендации: Чеканов С.Г., Степанова А.А. Строение конечных полей. Учебно-методическое пособие. Изд. ДВФУ. Владивосток, 2013, 30 с.

Приложение 2

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Конечные поля»

Направление подготовки 01.04.01 Математика

магистерская программа «Алгебра»

Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
Тип задач профессиональной деятельности: Научно-исследовательский			
планирование и реализация научно-исследовательской деятельности в области математики и ее приложений	Универсальная алгебра и алгебраические методы криптографии. Методы и концепции математической логики. Алгоритмы и конструкции алгебраической геометрии.	ПК-1. способен к интенсивной научно-исследовательской работе	ПК1.1. Умеет: правильно ставить задачи по выбранной тематике, выбирать для исследования необходимые методы; применять выбранные методы к решению научных задач, оценивать значимость получаемых результатов ПК-1.2. Знает: классические и современные методы решения задач по выбранной тематике научных исследований; новые научные результаты, связанные с тематикой научных исследований работы магистранта ПК-1.3 Владеет: навыками критического анализа и оценки современных достижений и результатов деятельности по решению исследовательских и практических задач; навыками выступлений на научно-тематических конференциях и современными методами решения задач по выбранной тематике научных исследований
Тип задач профессиональной деятельности: Педагогический			
проектирование, планирование и	Универсальная алгебра и	ПК-3 Способен осуществлять	ПКО-3.1. Умеет: проектировать элементы

реализация образовательного процесса по математике в образовательном учреждении высшего и общего образования в соответствии с требованиями ФГОС основного общего образования и ФГОС среднего общего образования	алгебраические методы криптографии. Методы и концепции математической логики. Алгоритмы и конструкции алгебраической геометрии.	обучение учебному предмету на основе использования предметных методик и современных образовательных технологий	образовательной программы, рабочую программу преподавателя по математике; формулировать дидактические цели и задачи обучения математике и реализовывать их в образовательном процессе по математике; обосновывать выбор методов обучения математике и образовательных технологий, применять их в образовательной практике, исходя из особенностей содержания учебного материала и образовательных потребностей обучаемых; планировать и комплексно применять различные средства обучения математике ПКО-3.2. Знает: концептуальные положения и требования к организации образовательного процесса по математике; особенности проектирования образовательного процесса по математике в образовательном учреждении высшего образования, подходы к планированию образовательной деятельности; формы, методы и средства обучения математике, современные образовательные технологии, методические закономерности их выбора; особенности частных методик обучения математике ПКО-3.3. Владеет: умениями по планированию и проектированию образовательного процесса;

			методами обучения математике и современными образовательными технологиями

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Введение	ПК-1 ПК-3	знает	Конспект (ПР-7)	Вопросы к экзамену 1-5
			умеет	Коллоквиум (УО-2) ИДЗ	Примеры ИДЗ «Алгоритм Евклида»
			владеет	Доклад, сообщение (УО-3)	
2	Характеристика поля	ПК-1 ПК-3	знает		Вопросы к экзамену 6-10
			умеет	Коллоквиум (УО-2)	
			владеет	Контрольная работа (ПР-2)	Примерный вариант КР «Алгоритм Евклида»
3	Простые расширения конечных полей	ПК-1 ПК-3	знает		Вопросы к экзамену 11-12
			умеет	ИДЗ	Примеры ИДЗ «Алгебраические расширения конечных полей»
			владеет	Реферат (ПР-4)	
4	Строение конечных полей	ПК-1 ПК-3	знает	Реферат (ПР-4)	Вопросы к экзамену 13-14
			умеет	Коллоквиум (УО-2) ИДЗ	Примеры ИДЗ «Неприводимость многочленов над конечным полем»

			владеет	Круглый стол (УО-4)	
5	Мультипликативная группа конечного поля	ПК-1 ПК-3	знает	Коллоквиум (УО-2)	Вопросы к экзамену 15
			умеет	ИДЗ	Примеры ИДЗ «Теорема о примитивном элементе»
			владеет	Круглый стол (УО-4)	
6	Линейные рекуррентные последовательности	ПК-1 ПК-3	знает	Коллоквиум (УО-2)	Вопросы к экзамену 16-18
			умеет	ИДЗ	Примеры ИДЗ «Представление элементов конечного поля с помощью многочленов»
			владеет	Контрольная работа (ПР-2)	Примерный вариант КР «Строение конечных полей»
7	Алгебраические коды	ПК-1 ПК-3	знает		Вопросы к экзамену 19
			умеет	Реферат (ПР-4)	
			владеет		

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
ПК-1: способность к интенсивной научно-	знает (пороговый уровень)	классические и современные методы решения задач по выбранной тематике	знание основных понятий и методов научных	-способность наличие знаний основных понятий и методов

исследовательской работе		научных исследований; новые научные результаты, связанные с тематикой научных исследований работы магистранта	исследований в выбранной области математики	научных исследований в выбранной области математики
	умеет (продвинутый)	правильно ставить задачи по выбранной тематике, выбирать для исследования необходимые методы; применять выбранные методы к решению научных задач, оценивать значимость получаемых результатов	умение применять математические методы при исследовании в выбранной области математики	наличие в диссертации результатов эффективного применения методов системного анализа
	владеет (высокий)	навыками критического анализа и оценки современных достижений и результатов деятельности по решению исследовательских и практических задач; навыками выступлений на научно-тематических конференциях и современными методами решения задач по выбранной тематике научных исследований	владение основными математическими методами научных исследований	демонстрация использования основных математических методов научных исследований

ПК-3 Способен осуществлять обучение учебному предмету на основе использования предметных методик и современных образовательных технологий	знает (пороговый уровень)	концептуальные положения и требования к организации образовательного процесса по математике; особенности проектирования образовательного процесса по математике в образовательном учреждении высшего образования, подходы к планированию образовательной деятельности; формы, методы и средства обучения математике, современные образовательные технологии, методические закономерности их выбора; особенности частных методик обучения математике	знание наиболее применяемых пакетов прикладных программ	наличие знаний наиболее применяемых пакетов прикладных программ
	умеет (продвинутый)	проектировать элементы образовательной программы, рабочую программу преподавателя по математике; формулировать дидактические цели и задачи обучения математике и реализовывать их в образовательном процессе по	реализация математически сложных алгоритмов в современных программных комплексах	демонстрация современных методов и технологий программирования с использованием сетей при реализации курсовых работ, ИДК и ВКР

		математике; обосновывать выбор методов обучения математике и образовательных технологий, применять их в образовательной практике, исходя из особенностей содержания учебного материала и образовательных потребностей обучаемых; планировать и комплексно применять различные средства обучения математике		
	владеет (высокий)	умениями по планированию и проектированию образовательного процесса; методами обучения математике и современными образовательными технологиями	использование методов и технологий программирования методами компьютерного и математического моделирования	демонстрация применения методов и технологий программирования для создания моделей, использующих локальные и глобальные сети

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Оценочные средства для промежуточной аттестации

Промежуточная аттестация студентов по дисциплине «Конечные поля» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

По дисциплине «Конечные поля» учебным планом предусмотрен экзамен в первом семестре.

Экзамен проводится в письменно-устной форме. Студент составляет конспект ответа и выполняет письменные задания, затем устно отвечает на вопросы.

Перечень вопросов для подготовки к экзамену

1. Строение циклических групп.
2. Кольца, гоморфизмы колец.
3. Факторкольцо и идеалы колец.
4. Теорема о факторкольце по максимальному идеалу.
5. Кольцо классов вычетов. Поле классов вычетов по простому модулю.
6. Теорема о характеристике конечного поля.
7. Кольцо многочленов над конечным полем.
8. Поле разложения многочлена.
9. Теорема о существовании и единственности конечного поля.
10. Алгоритм Евклида для многочленов.
11. Неприводимые многочлены. Основная теорема арифметики кольца многочленов.
12. Алгебраические расширения конечного поля.
13. Теорема о строении конечных полей.
14. Теорема о примитивном элементе.
15. Группа автоморфизмов конечного поля.
16. Линейные рекуррентные последовательности.
17. Матрица и характеристический многочлен линейной рекуррентной последовательности.
18. Оценка периода линейной рекуррентной последовательности.
19. Алгоритм Берлекемпа-Месси.

Критерии выставления оценки студенту на экзамене по дисциплине «Конечные поля»

Баллы (рейтинговой оценки)	**Оценка зачета/ экзамена** (стандартная)	**Требования к сформированным компетенциям**
100-85	*«зачтено»/ «отлично»*	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
75-84	*«зачтено»/ «хорошо»*	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
61-74	*«зачтено»/ «удовлетворительно»*	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
60 и менее	*«незачтено»/ «неудовлетворительно»*	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства для текущей аттестации

Текущая аттестация студентов по дисциплине «Конечные поля» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация проводится в форме контрольных мероприятий (контрольных работ и индивидуальных домашних заданий) по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Коллоквиум является формой контроля усвоения студентами теоретической части курса. Сдается студентами преподавателю в устной форме в виде собеседования во время лекционных занятий по завершению изучения теоретической части разделов курса и оценивается в форме дифференцированного зачета.

Коллоквиум считается сданным успешно при получении оценок «отлично», «хорошо» или «удовлетворительно». При получении оценки «неудовлетворительно» он считается не сданным, а соответствующий раздел теоретической части неусвоенным.

Студенту предоставляется возможность пересдать коллоквиум один раз во время консультаций по дисциплине с получением оценки на один балл ниже.

Контрольная работа является формой контроля усвоения студентами практической части курса. Выполняется студентами во время практических занятий по завершению изучения практической части разделов курса. Контрольная работа считается выполненной успешно при получении оценок «отлично», «хорошо», «удовлетворительно». При получении оценки «неудовлетворительно» контрольная работа считается не сданной, соответствующий раздел практикума неусвоенным.

Примеры контрольных работ

Тема: Алгоритм Евклида

Вариант 1.

Применяя алгоритм Евклида, найти НОД(f, g) для следующих многочленов f и g с коэффициентами из указанного поля F:

$F = Q$,

$f(x) = x^7 + 2x^5 + 2x^2 - x + 2$,

$g(x) = x^6 - 2x^5 - x^4 + x^2 + 2x + 3$

Тема: Строение конечных полей

Вариант 1.

1. Показать, что для каждого конечного поля, кроме F_2, сумма всех его элементов равна 0.
2. Пусть a, b – элементы поля F_{2^n} (n – нечетное число). Показать, что из равенства $a^2 + ab + b^2 = 0$ вытекает $a = b = 0$.
3. Найти все примитивные элементы поля F_7.

Примеры индивидуальных домашних заданий

Тема: Алгоритм Евклида

Применяя алгоритм Евклида, найти НОД(f, g) для следующих многочленов f и g с коэффициентами из указанного поля F:

(a) $F = Q$, $f(x) = x^7 + 2x^5 + 2x^2 - x + 2$, $g(x) = x^6 - 2x^5 - x^4 + x^2 + 2x + 3$;

(b) $F = F_2$, $f(x) = x^7 + 1$, $g(x) = x^5 + x^3 + x + 1$;

(c) $F = F_2$, $f(x) = x^5 + x + 1$, $g(x) = x^6 + x^5 + x^4 + 1$;

(d) $F = F_2$, $f(x) = x^5 + x^4 + 1$, $g(x) = x^4 + x^2 + 1$;

(e) $F = F_2$, $f(x) = x^5 + x^3 + x + 1$, $g(x) = x^4 + 1$;

(f) $F = F_2$, $f(x) = x^5 + x + 1$, $g(x) = x^4 + x^3 + 1$;

(g) $F = F_2$, $f(x) = x^5 + x^3 + 1$, $g(x) = x^4 + x + 1$;

(h) $F = F_3$, $f(x) = x^8 + 2x^5 + x^3 + x^2 + 1$,

(i) $g(x) = 2x^6 + x^5 + 2x^3 + 2x^2 + 2$.

Тема: Неприводимость многочленов над конечным полем

1. Построить таблицы сложения и умножения для факторкольца $F_2[x]/(x^3+x^2+x)$. Определить, будет ли это кольцо полем.
2. Пусть $[x+1]$ – класс вычетов многочлена $x+1$ в факторкольце $F_2[x]/\langle x^4+1\rangle$. Найти классы вычетов, составляющие главный идеал $\langle [x+1]\rangle$ в указанном факторкольце.
3. Решить сравнение

$$(x^2+1)f(x) \equiv 1\big(mod(x^3+1)\big)$$

в $F_3[x]$, если это возможно.
4. Решить сравнение

$$(x^4+x^3+x^2+1)f(x) \equiv x^2+1\big(mod(x^3+1)\big)$$

в $F_2[x]$, если это возможно.

Тема: Алгебраические расширения конечного поля

1. Показать, что для многочлена f положительной степени над полем F следующие условия эквивалентны:
   (a) многочлен f неприводим над F;
   (b) главный идеал $\langle f\rangle$ кольца $F[x]$ является максимальным идеалом;
   (c) главный идеал $\langle f\rangle$ кольца $F[x]$ является простым идеалом.
2. Доказать, что если F_q - поле из q элементов, то $x^q - x = \prod_{a\in F_q}(x-a)$.

Тема: Представление элементов конечного поля с помощью многочленов

1. Найти число неприводимых унитарных многочленов степени 2 и 3 над полем Z_3.
2. Доказать, что при $a \in Z_p^*$ многочлен $x^p - x - a$ неприводим над Z_p.
3. Доказать, что при $a \neq 1$ многочлен $x^q - ax - b$ имеет в F_q корень.

4. Доказать, что $x^{2n} + x^n + 1$ неприводим над Z_2 тогда и только тогда, когда $n = 3^k$ для некоторого $k \geq 0$.

5. Доказать, что $x^{4n} + x^n + 1$ неприводим над Z_2 тогда и только тогда, когда $n = 3^k 5^m$ для некоторых целых $k, m \geq 0$.

6. Доказать, что многочлен $x^2 + 1$ неприводим над полем F_{11}, и показать непосредственно, что факторкольцо $F_{11}[x]/(x^2 + 1)$ состоит из 121 элемента. Доказать также, что многочлен $x^2 + x + 4$ неприводим над полем F_{11}, и показать, что факторкольца $F_{11}[x]/(x^2 + 1)$ и $F_{11}[x]/(x^2 + x + 4)$ изоморфны.

Тема: Теорема о примитивном элементе

Доказать, что любая конечная подгруппа мультипликативной группы F^* произвольного поля F циклична.

1. Пусть F – поле. Доказать, что если его мультипликативная группа F^* циклична, то F – конечное поле.

2. Пусть F – конечное поле и F^* - его мультипликативная группа. Доказать, что множество $H \cup \{0\}$ для любой подгруппы H группы F^* будет подполем поля F в том и только том случае, если порядок группы F^* равен 1 или простому числу вида $2^p - 1$, где p – простое число.

3. Показать, что каждый элемент конечного поля F_q характеристики p имеет в этом поле один и только один корень -й степени.

4. Показать, что если F_q – конечное поле нечетной характеристики, то элемент $a \in F_q^*$ имеет в поле F_q квадратный корень тогда и только тогда, когда $a^{(q-1)/2} = 1$.

Критерии оценки (письменный ответ)

100-86 баллов - если ответ показывает глубокое и систематическое знание всего программного материала и структуры конкретного вопроса, а также основного содержания и новаций лекционного курса по сравнению с

учебной литературой. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией
соответствующей научной области. Знание основной литературы и знакомство с дополнительно рекомендованной литературой. Логически корректное и убедительное изложение ответа.

85-76 - баллов - знание узловых проблем программы и основного содержания лекционного курса; умение пользоваться концептуально понятийным аппаратом в процессе анализа основных проблем в рамках данной темы; знание важнейших работ из списка рекомендованной литературы. В целом логически корректное, но не всегда точное и аргументированное изложение ответа.

75-61 - балл - фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ.

60-50 баллов - незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе.

Это соответствует: 100-86 баллов – «отлично», 85-76 баллов – «хорошо», 75-61 баллов – «удовлетворительно», не более 60 баллов – «неудовлетворительно».