МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт математики и механики им. Н.И. Лобачевского

подписано электронно-цифровой подписью

Программа дисциплины

Теория конечных полей М2.ДВ.3

Направление подготовки: 010100.68 - Математика
Профиль подготовки: Алгебра
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Тронин С.Н.

Рецензент(ы):

Киндер М.И.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Арсланов М. М.
Протокол заседания кафедры No ___ от "____" _____ 201__г

Учебно-методическая комиссия Института математики и механики им. Н.И. Лобачевского :
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 81728215

Казань
2014

Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Тронин С.Н. Кафедра алгебры и математической логики отделение математики , Serge.Tronin@kpfu.ru

1. Цели освоения дисциплины

Теория конечных полей является одним из важнейших математических инструментов для самых разнообразных прикладных дисциплин, в том числе для теории обработки сигналов и изображений, теории кодирования, криптографии и других разделов того, что называется математическими методами защиты информации. Кроме всего этого, теория конечных полей - это хорошо развитая математическая теория, изучение которой будет способствовать формированию математической культуры студента. Целью изучения теории конечных полей можно считать как развитие этой математической культуры, так и подготовку к возможной будущей работе в области защиты информации, теории связи, обработки сигналов и изображений и т.п.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " М2.ДВ.3 Профессиональный" основной образовательной программы 010100.68 Математика и относится к дисциплинам по выбору. Осваивается на 1 курсе, 1 семестр.

Предполагается знакомство с линейной алгеброй, алгеболй многочленов, с основами теории чисел, и самыми первоначальными сведениями из теории групп и колец.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-4 (общекультурные компетенции)	углубленные знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов
ОК-6 (общекультурные компетенции)	способностью работать самостоятельно, заботой о качестве, стремлением к успеху
ОК-8 (общекультурные компетенции)	инициативностью и лидерством
ПК-12 (профессиональные компетенции)	способность различным образом представлять и адаптировать математические знания с учетом уровня аудитории
ПК-13 (профессиональные компетенции)	способность к управлению и руководству научной работой коллективов
ПК-15 (профессиональные компетенции)	возможность преподавания физико-математических дисциплин и информатики в общеобразовательных учреждениях, образовательных учреждениях начального профессионального, среднего профессионального и высшего профессионального образования на основе полученного фундаментального образования и научного мировоззрения
ПК-16 (профессиональные компетенции)	умение извлекать актуальную научно-техническую информацию из электронных библиотек, реферативных журналов

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-3 (профессиональные компетенции)	способность к интенсивной научно-исследовательской и научно-изыскательской деятельности
ПК-6 (профессиональные компетенции)	самостоятельное построение целостной картины дисциплины
ОК-4 (общекультурные компетенции)	углубленные знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов
ОК-9 (общекультурные компетенции)	способностью к организации и планированию

В результате освоения дисциплины студент:

1. должен знать:

Основные понятия и результаты теории конечных полей

2. должен уметь:

ПРоизводить вычисления в конечных полях

3. должен владеть:

Студент должен владеть меирдологией теории конечных полей

4. должен демонстрировать способность и готовность:

основные понятия и результаты.

4. должен демонстрировать способность и готовность:

решать возникающие в теории конечных полей задачи, в частности, находить корни многочленов над конечными полями и разлагать многочлены над конечными полями на неприводимые множители.

4. должен демонстрировать способность и готовность:

методами теории конечных полей.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины зачет в 1 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Алгебры и многочлены	1	1-2	2	2	0	домашнее задание
2.	Тема 2. Общие сведения о полях и расширениях полей. Характеристика поля и ее свойства	1	3-4	2	2	0	домашнее задание
3.	Тема 3. Теорема о примитивном элементе конечного поля и ее следствия.	1	5-6	2	2	0	домашнее задание
4.	Тема 4. Строение конечных полей	1	7-10	4	4	0	контрольная работа
5.	Тема 5. Неприводимые многочлены над конечными полями.	1	11-12	2	2	0	домашнее задание
6.	Тема 6. Алгоритмы нахождения корней многочленов над конечными полями. Алгоритм разложения многочлена над ко-нечным полем на неприводи-мые множители	1	13-15	0	6	0	контрольная работа
.	Тема . Итоговая форма контроля	1		0	0	0	экзамен
	Итого			12	18	0	

4.2 Содержание дисциплины

Тема 1. Алгебры и многочлены

лекционное занятие (2 часа(ов)):

Алгебры над коммутативными кольцами. Алгебра многочленов и ее свойства. Факторалгебры алгебры многочленов.

практическое занятие (2 часа(ов)):

Вычисления в факторалгебрах алгебры многочленов

Тема 2. Общие сведения о полях и расширениях полей. Характеристика поля и ее свойства

лекционное занятие (2 часа(ов)):

Общие сведения о полях.

практическое занятие (2 часа(ов)):

Вычисления в конечных полях с использованием свойств характеристики

Тема 3. Теорема о примитивном элементе конечного поля и ее следствия.

лекционное занятие (2 часа(ов)):

Леммы о порядках элементов в конечных группах. Теорема о примитивном элементе. Строение конечных полей.

практическое занятие (2 часа(ов)):

Вычисление примитивных элементов

Тема 4. Строение конечных полей

лекционное занятие (4 часа(ов)):

Делимость натуральных чисел и многочленов специального вида над конечныи полями. Порядки и показатели. Теоремы о существовании и единственности конечных полей. Подполя конечных полей.

практическое занятие (4 часа(ов)):

Вычисления в конечных полях

Тема 5. Неприводимые многочлены над конечными полями.

лекционное занятие (2 часа(ов)):

Корни неприводимых многочленов. Существование неприводимых многочленов над конечными полями.

практическое занятие (2 часа(ов)):

Нахождение неприводимых многочленов

Тема 6. Алгоритмы нахождения корней многочленов над конечными полями. Алгоритм разложения многочлена над ко-нечным полем на неприводи-мые множители.

практическое занятие (6 часа(ов)):

Вычисления с использованием указанных алгоритмов

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Алгебры и многочлены	1	1-2	подготовка домашнего задания	10	домашнее задание
2.	Тема 2. Общие сведения о полях и расширениях полей. Характеристика поля и ее свойства	1	3-4	подготовка домашнего задания	14	домашнее задание
3.	Тема 3. Теорема о примитивном элементе конечного поля и ее следствия.	1	5-6	подготовка домашнего задания	14	домашнее задание
4.	Тема 4. Строение конечных полей	1	7-10	подготовка к контрольной работе	15	контрольная работа
5.	Тема 5. Неприводимые многочлены над конечными полями.	1	11-12	подготовка домашнего задания	10	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
6.	Тема 6. Алгоритмы нахождения корней многочленов над конечными полями. Алгоритм разложения многочлена над ко-нечным полем на неприводи-мые множители.	1	13-15	подготовка к контрольной работе	15	контрольная работа
	Итого				78	

5. Образовательные технологии, включая интерактивные формы обучения

лекции, практические занятия, экзамен, компьютеры. В течение семестра студенты решают задачи, указанные преподавателем, к каждому семинару, и выступают с докладами на указанные преподавателем темы.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Алгебры и многочлены

домашнее задание , примерные вопросы:

Решение задач. Темы задач: деление многочленов, нахождение наибольшего общего делителя, расширенный алгоритм Евклида.

Тема 2. Общие сведения о полях и расширениях полей. Характеристика поля и ее свойства

домашнее задание , примерные вопросы:

Решение задач. Кольца вычетов и поля вычетов. Умножение, сложение и деление в кольцах вычетов. Построение поля, в котором данный неприводимый многочлен имеет корень.

Тема 3. Теорема о примитивном элементе конечного поля и ее следствия.

домашнее задание , примерные вопросы:

Решение задач. Нахождение примитивных элементов в конкретных конечных полях.

Тема 4. Строение конечных полей

контрольная работа , примерные вопросы:

Решение задач. Построение конечных полей по заданному неприводимому многочлену. Таблицы умножений и примитивные элементы.

Тема 5. Неприводимые многочлены над конечными полями.

домашнее задание , примерные вопросы:

Решение задач. Нахождение неприводимых многочленов над заданным конечным полем.

Тема 6. Алгоритмы нахождения корней многочленов над конечными полями. Алгоритм разложения многочлена над ко-нечным полем на неприводи-мые множители.

контрольная работа , примерные вопросы:

Решение задач. Использование алгоритмов нахождения корней многочленов над конечными полями, и алгоритма разложения многочлена над конечным полем на неприводимые множители

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

Приложение 1. Вопросы экзаменационных билетов.

1. Конечные поля. Примеры конечных полей. Характеристика поля. Простое подполе.
2. Некоторые общие факты о расширениях полей
3. Корни многочленов над конечными полями. Существование расширения поля, в котором данный многочлен раскладывается на линейные множители.
4. Подполя конечных полей.
5. Теорема о примитивном элементе. Строение конечных полей.
6. Делимость многочленов над конечными полями.
7. Существование конечных полей с любым количеством элементов.
8. Единственность конечного поля с данным количеством элементов.
9. Корни неприводимых многочленов над конечными полями.
10. Алгебраическое замыкание конечного поля.

7.1. Основная литература:

1. Сборник заданий по специальным курсам высшей математики. Типовые расчеты : учебное пособие / В. Ф. Чудесенко Изд. 5-е, стер. Санкт-Петербург [и др.] : Лань, 2010 . 190, [1] с. : ил. ; 21 .(Учебники для вузов, Специальная литература) . Библиогр.: с. 189-190 (22 назв.) . ISBN 978-5-8114-0661-6 ((в пер.)) , 2000.

2. Численные методы. Основы научных вычислений : учебное пособие для бакалавров : для студентов высших учебных заведений, обучающихся по специальности (направлению) подготовки ВПО 010501 (010500.62) "Прикладная математика и информатика" (ОПД.Ф.09-Численные методы) / В. Е. Зализняк ; Сибирский федеральный университет . 2-е изд., перераб. и доп. Москва : Юрайт, 2012 . 356 с. : ил.

3. Игошин В. И. Математическая логика: Учебное пособие / В.И. Игошин. - М.: ИНФРА-М, 2012. - 399 с.: http://znanium.com/bookread.php?book=242738

4. Чикрин, Дмитрий Евгеньевич. Теория информации и кодирования [Текст: электронный ресурс] : курс лекций / Д. Е. Чикрин ; Казан. (Приволж.) федер. ун-т, Высш. шк. информ. технологий и информ. систем, Каф. автоном. робототехн. систем . Электронные данные (1 файл: 4,46 Мб) . (Казань : Казанский федеральный университет, 2013) . Загл. с экрана . Для 3-го семестра . Режим доступа: открытый . http://libweb.kpfu.ru/ebooks/50-ITIS/50_000337.pdf

7.2. Дополнительная литература:

1. Сборник задач по алгебре / [И. В. Аржанцев и др.] ; под ред. А. И. Кострикина . [Новое изд., испр.] . Москва : Изд-во МЦНМО, 2009 . 403 с. ; 22 . Авт. указаны на обороте тит. л. Библиогр.: с. 8-9 . ISBN 978-5-94057-413-2 ((в пер.)) , 1000.

2. Лихтарников Л.М., Сукачева Т.Г. Математическая логика. Курс лекций. Задачник-практикум и решения. СПб.: Лань, 2009. - 288 с. http://e.lanbook.com/view/book/231/

3. Дискретная математика: Учебное пособие / В.В. Куликов. - М.: РИОР, 2007. - 174 с. http://znanium.com/bookread.php?book=126799

7.3. Интернет-ресурсы:

Аблаев Ф.М., Васильев А.В. Классические и квантовые ветвящиеся программы - http://libweb.kpfu.ru/ebooks/09-IVMIT/09_62_2010_000088.pdf

Дискретная математика: Учебное пособие / В.В. Куликов. - М.: РИОР, 2007. - 174 с. - http://znanium.com/bookread.php?book=126799

Игошин В. И. Математическая логика: Учебное пособие / В.И. Игошин. - М.: ИНФРА-М, 2012. - 399 с. - http://znanium.com/bookread.php?book=242738

Лихтарников Л.М., Сукачева Т.Г. Математическая логика. Курс лекций. Задачник-практикум и решения. СПб.: Лань, 2009. - 288 с. - http://e.lanbook.com/view/book/231

Чикрин, Дмитрий Евгеньевич. Теория информации и кодирования [Текст: электронный ресурс] : курс лекций / Д. Е. Чикрин ; Казан. (Приволж.) федер. ун-т, Высш. шк. информ. технологий и информ. систем, Каф. автоном. робототехн. систем .? Электронные данные (1 файл: 4,46 Мб) .? (Казань : Казанский федеральный университет, 2013) - http://libweb.kpfu.ru/ebooks/50-ITIS/50_000337.pdf

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Теория конечных полей" предполагает использование следующего материально-технического обеспечения:

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

учебные аудитории для проведения лекционных и семинарских занятий, библиотека, доступ студентов к Интернету. Большая часть книг имеется в электронном виде на кафедре.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010100.68 "Математика" и магистерской программе Алгебра .

Автор(ы):
Тронин С.Н. _____
"__" _____ 201 __ г.

Рецензент(ы):
Киндер М.И. _____
"__" _____ 201 __ г.