Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гробова Татьяна Анатольевна
Должность: и.о. декана факультета математики и компьютерных наук имени профессора Н.И. Червякова
Дата подписания: 21.07.2023 11:22:27
Уникальный программный ключ:
bd39d4208aa94cf4422feb787c81619d42de79a7

Аннотация дисциплины

Наименование дисциплины (модуля)	**Спецглавы алгебры и их приложения**
Краткое содержание	**Строение конечных полей.** Теорема существования и единственности конечных полей. Критерий подполя. Цикличность мультипликативной группы конечного поля. Примитивные элементы поля. Число примитивных элементов конечного поля. Полиномиальное представление элементов конечных полей. Представление элементов конечного поля. **Многочлены над конечными полями.** Неприводимые многочлены над конечными полями и их простейшие свойства. Применение критерия Батлера для проверки неприводимости многочлена над конечным полем. Понятие порядка многочлена. Порядок неприводимого многочлена. Число нормированных неприводимых многочленов степени n и порядка e. Формула для нахождения порядка многочлена. Понятие примитивного многочлена. Порядок примитивного многочлена. Разложение многочленов на множители над малыми конечными полями. Разложение многочленов на множители над большими конечными полями. Нахождение корней многочленов над простым полем. **Алгоритмы теории корректирующих кодов.** Понятие кодирования информации. Цели кодирования информации. Понятия блокового (n,k)-кода в алфавите A, кодового слова, кодового расстояния. Способности кода к исправлению ошибок. Понятие линейного (n,k)-кода над полем F_p. Порождающая и проверочная матрица линейного кода. Процесс кодирования. Информационные и проверочные символы. Понятие систематического кода. Декодирование линейных кодов. Алгоритм декодирования по лидеру смежного класса. Коды Хэмминга. Определение циклического кода. Порождающий и проверочный многочлены циклического кода. БЧХ-коды. Декодирование БЧХ-кодов.
Результаты освоения дисциплины (модуля)	Знает основные свойства конечных полей; способы представления элементов конечного поля. Умеет оперировать с элементами конечных полей; представлять элементы конечного поля разными способами; строить неприводимые многочлены; находить порядок многочлена, корни многочлена, каноническое разложение многочлена; строить таблицы кодирования и декодирования для линейного кода над конечным полем, циклического кода и БЧХ-кода. Владеет навыками проведения операций с элементами конечных полей; представления элементов конечного поля разными способами; построения неприводимых многочленов; нахождения порядка многочлена, корней многочлена, канонического разложения многочлена; построения таблиц кодирования и декодирования для линейного кода над конечным полем, циклического кода и БЧХ-кода.
Трудоемкость, з.е.	4
Форма отчетности	зачет с оценкой
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)	
Основная литература	1. Лыткина Д.В. Алгебраические структуры [Электронный ресурс]: учебное пособие / Д.В. Лыткина, Т.В. Храмова. − Электрон. текстовые данные. − Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2016. − 108 с. − 2227-8397. Режим доступа: http://www.iprbookshop.ru/69535.html 2. Алгебраические структуры и их приложения: учебное пособие / Л.В. Зяблицева, С.Ю. Корабельщикова, И.В. Кузнецова, С.А.

	Тихомиров; Министерство образования и науки Российской Федерации, Северный (Арктический) федеральный университет имени М.В. Ломоносова. - Архангельск: САФУ, 2015. − 169 с.: ил., табл. - Библиогр. в кн. - ISBN 978-5-261-01074-6. Режим доступа: http://biblioclub.ru/index.php?page=book&id=436142
Дополнительная литература	1. Кострикин А.И. Введение в алгебру: учебник / А.И. Кострикин. − Москва: МЦНМО, 2009. − Ч. 3. Основные структуры алгебры. − 272 с. − ISBN 978-5-94057-455-2. Режим доступа: http://biblioclub.ru/index.php?page=book&id=62951 2. Царев А. В., Шеина Г. В. Элементы абстрактной и компьютерной алгебры: учебное пособие [Электронный ресурс] / Москва: МПГУ,2016. − 116с. − ISBN 978-5-4263-0393-5. Режим доступа: http://biblioclub.ru/index.php?page=book&id=471787 3. Кочеров Ю.Н. Разработка методов и алгоритмов разделения и восстановления данных в модулярных пороговых структурах для распределенных вычислительных сетей: монография / Ю.Н. Кочеров, Н.И. Червяков; Министерство образования и науки РФ. − Ставрополь: СКФУ, 2016. − 239 с.: ил. − Библиогр. с. 105-115.Режим доступа: http://biblioclub.ru/index.php?page=book&id=466993 4. Алешников С.И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях [Электронный ресурс]: практическое пособие / С.И. Алешников, Е.В. Козьминых. − Электрон. текстовые данные. − Калининград: Балтийский федеральный университет им. Иммануила Канта, 2006. − 97 с. − 5-88874-689-4. Режим доступа: http://www.iprbookshop.ru/23851.html