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 (РПУД)
Алгебраические основы криптографии

Направление подготовки: 01.04.01 Математика
Форма подготовки: очная

Школа естественных наук
Кафедра алгебры, геометрии и анализа
курс 1 семестр 2
лекции 18 час.
практические занятия 18 час.
самостоятельная работа студентов 72
контрольные работы не предусмотрены
всего часов аудиторной нагрузки 36 час.
в том числе с использованием МАО 27 час.
зачет 2 семестр
экзамен не предусмотрен

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 кафедрой к.ф.-м.н., профессор Р.П.Шепелева
Составитель: к.ф.-м.н, доцент С.Г. Чеканов

Владивосток
2019

Оборотная сторона титульного листа РПУД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 200 г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 200 г. № _____

Заведующий кафедрой _____ _____

(подпись) (И.О. Фамилия)

Аннотация рабочей программы учебной дисциплины
«Алгебраические основы криптографии»

Рабочая программа учебной дисциплины «Алгебраические основы криптографии» 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 3 ЗЕ (108 час.). Учебным планом предусмотрены лекции (18 час.), практические занятия (18 час.), самостоятельная работа студента (72 час.). Дисциплина «Алгебраические основы криптографии» входит в часть, формируемую участниками образовательных отношений, реализуется на 1 курсе в 2 семестре.

Цель преподавания дисциплины: - является развитие логического и алгоритмического мышления.

Задачи преподавания дисциплины:

1. исследования социальных, технических, экономических и других проблем науки и производства;
2. умение мыслить научными категориями в области науки, техники, экономики и социальной сферы;
3. умение строго доказывать утверждение, сформулировать результат, увидеть следствия полученного результата;
4. применение полученных знаний при изучении явлений природы и общества и исследование простейших моделей с помощью методов теории групп, колец и полей.

Полученные навыки по курсу «Алгебраические основы криптографии» в дальнейшем будут использоваться при изучении таких дисциплин как Математический анализ, ТФКП, ФА, аналитическая геометрия,

дифференциальная геометрия и топология, дифференциальные уравнения, дискретная математика и математическая логика, теория вероятностей, математическая статистика и случайные процессы, численные методы, теоретическая механика.

Для успешного изучения дисциплины «Алгебраические основы криптографии» 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: Проектно-технологический			
разработка и реализация технологических проектов на основе математических моделей в предметных областях	Универсальная алгебра и алгебраические методы криптографии. Методы и концепции математической логики. Алгоритмы и конструкции алгебраической геометрии.	ПК-5 способен разрабатывать и применять математические методы для решения задач научной и проектно-технологической деятельности	ПК-5.1. Умеет: анализировать поставленную задачу и находить алгоритм ее решения; выбирать оптимальные системы программирования, наиболее подходящие для решения поставленной задачи ПК-5.2. Знает: современные методы цифровой обработки изображений и средства компьютерной графики ПК-5.3. Владеет: методами моделирования

			информационных процессов; навыками работы над производственным проектом в составе группы научных специалистов
		ПК-6 способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности	ПК-6.1. Умеет: проводить анализ и обосновывать необходимость работы над данным проектом и оценивать его эффективность; обосновывать и защищать предлагаемый проект, доказывать его эффективность и востребованность на выбранном рынке ПК-6.2. Знает: особенности рынка данного региона ПК-6.3. Владеет: навыками работы над проектами по выбранной тематике; методами построения, анализа и применения математических моделей для оценки состояния, и прогноза развития экономических процессов и явлений; владеть опытом выражения своих мыслей и мнения

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА (18 час.)

Тема 1. Конечные группы. Представление групп подстановками (4 час.)

Группы. Индекс подгруппы. Теорема Лагранжа. Подстановки и их криптографические свойства. Теорема Кели.

Занятие проводится с использованием метода активного обучения «лекция-беседа».

Тема 2. Кольца и поля (4 час.)

Идеалы колец и факторкольца. Характеристика кольца. Конечные расширения полей. Теоремы о строении конечных полей

Занятие проводится с использованием метода активного обучения «лекция-беседа».

Тема 3. Линейные рекуррентные последовательности над конечными полями (4 час.)

Характеризация последовательностей с помощью матриц и полиномов. Оценка периода ЛРП. Применение последовательностей в криптографических целях

Занятие проводится с использованием метода активного обучения «лекция-беседа».

Тема 4. Полугруппы и конечные автоматы (2 час.)

Определение автомата и представление с помощью графа и полугруппы

Занятие проводится с использованием метода активного обучения «лекция-беседа».

Тема 5. Решетки и решеточно продолженные булевы функции (4 час.)

Булевы функции и булевы решетки. Продолжение булевых функций с единичного куба на множество рациональных точек

Занятие проводится с использованием метода активного обучения «лекция-беседа».

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (18 час.)

Занятие 1. Конечные группы (3 часа).

Группы. Индекс подгруппы. Теорема Лагранжа. Подстановки и их криптографические свойства. Теорема Кели.

Занятие 2. Кольца и поля (3 часа).

Идеалы колец и факторкольца. Характеристика кольца. Конечные поля и их алгебраические расширения. Теорема о строении конечных полей. Вычисления в конечных полях.

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

Занятие 3. Линейные рекуррентные последовательности над конечными полями (3 часа).

Рекуррентные соотношения. Характеризация последовательностей с помощью матриц и полиномов. Вычисление периода последовательности. Криптографические приложения последовательностей.

Занятие 4. Полугруппы и конечные автоматы (3 часа).

Полугруппы и их представления. Конечные автоматы и их связь с полугруппами. Представление автомата графом. Криптографические приложения автоматов.

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

Занятие 5. Решетки и решеточные продолжения булевых функций (3 часа).

Определение решетки. Дистрибутивные решетки. Булевы функции и решетки. Криптоанализ блочных шифров и дистрибутивные решетки.

Занятие 6. Эллиптические кривые (3 часа).

Эллиптические кривые над конечными полями. Группа точек эллиптической кривой. Вычисление порядка группы эллиптической кривой и порядка элементов группы. Криптографические приложения эллиптических кривых.

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

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Алгебраические основы криптографии» 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	Конечные группы	способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5), способен разрабатывать концептуальные и теоретические модели	УО-3 ПР-2	УО-2

		решаемых задач проектной и производственно-технологической деятельности (ПК-6)		
2	Кольца и поля	способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5),	ПР-11	
3	Линейные рекуррентные последовательности над конечными полями	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6)	УО-3 ПР-2	УО-2
4	Полугруппы и конечные автоматы	способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5),	УО-3 ПР-2	УО-2
5	Решетки и решеточные продолжения булевых функций	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6)	ПР-11	
6	Эллиптические кривые	способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5),	УО-3 ПР-2	УО-2

Типовые контрольные задания и вопросы для зачета представлены в Приложении 2.

V. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. а) основная литература:

1. Алферов Н.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии, М. Гелиос АРВ, 2012 г.
http://lib.dvfu.ru:8080/lib/item?id=chamo:1640&theme=FEFU
2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии, М.: МЦНМО, 2003 г.
http://lib.dvfu.ru:8080/lib/item?id=chamo:5790&theme=FEFU
3. Коблиц Н. Курс теории чисел и криптографии, М.: ТВМ, 2001 г.
http://lib.dvfu.ru:8080/lib/item?id=chamo:16477&theme=FEFU

б) дополнительная литература:

1. Д. К. Фаддеев, И. С. Соминский. Задачи по высшей алгебре. – Санкт-Петербург, «Лань», 1998, - 288 с.
http://lib.dvfu.ru:8080/lib/item?id=Lan:Lan-399&theme=FEFU
4. Виноградов И.М. Основы теории чисел. – СПб.: Лань, 2009. – 176 с.
http://lib.dvfu.ru:8080/lib/item?id=Lan:Lan-46&theme=FEFU
5. Кострикин А.И. и др. Сборник задач по алгебре. – СПб.: Лань, 2011. – 450 с.
http://lib.dvfu.ru:8080/lib/item?id=chamo:103102&theme=FEFU

Интернет-ресурсы

1. http://e.lanbook.com/books/element.php?pl1_id=13653

Аграновский А.В., Хади Р.А. Практическая криптография: алгоритмы и их программирование: Изд-во САЛОН-Пресс-пресс.-2009

VI. МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

На изучение дисциплины отводится 36 часов 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 и лабораторных 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.

По данному курсу разработаны методические указания:

1. Чеканов С.Г., Степанова А.А. Строение конечных полей. Учебно-методическое пособие. Изд. ДВФУ. Владивосток, 2013, 30 с..
2. Чеканов С.Г., Степанова А.А. Основы теории конечных групп. Учебно-методическое пособие. Изд. ДВФУ. Владивосток, 2014, 36 с.

VII МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные аудитории кампуса ДВФУ.

Программа составлена в соответствии с требованиями ФГОС ВПО с учётом рекомендаций и ПрООП ВПО по Направление подготовки:01.04.01 Математика

Автор (ы) __С.Г. Чеканов

Рецензент (ы) _____

Программа одобрена на заседании_____

(Наименование уполномоченного органа вуза (УМК, НМС, Ученый совет)

от _____ года, протокол № _____.

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 «Алгебраические основы криптографии»
Направление подготовки: 01.04.01 «Математика»
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
1. Теория групп	28.02 - 8.03	индивидуальное домашнее задание	1 неделя
2. Кольца и поля	8.03 - 28.03	индивидуальное домашнее задание	1 неделя
3. Линейные рекуррентные последовательности	28.03 – 14.04	индивидуальное домашнее задание	1 неделя
4. Полугруппы и конечные автоматы	14.04 - 28.04	индивидуальное домашнее задание	1 неделя
5. Решетки и булевы функции	28.04 - 10.05	индивидуальное домашнее задание	1 неделя
6. Эллиптические кривые	10.05 - 28.05	индивидуальное домашнее задание	1 неделя

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. Критерии оценки: студент получает максимальный балл, если работа выполнена без ошибок и оформлена в соответствии с требованиями преподавателя.

По данной дисциплине разработаны методические рекомендации:

1. Чеканов С.Г., Степанова А.А. Строение конечных полей. Учебно-методическое пособие. Изд. ДВФУ. Владивосток, 2013, 30 с.
2. Чеканов С.Г., Степанова А.А. Основы теории конечных групп. Учебно-методическое пособие. Изд. ДВФУ. Владивосток, 2014, 36

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 «Алгебраические основы криптографии»
Направление подготовки: 01.04.01 «Математика»
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

по дисциплине «Алгебраические основы криптографии»

Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
Тип задач профессиональной деятельности: Проектно-технологический			
разработка и реализация технологических проектов на основе математических моделей в предметных областях	Универсальная алгебра и алгебраические методы криптографии. Методы и концепции математической логики. Алгоритмы и конструкции алгебраической геометрии.	ПК-5 способен разрабатывать и применять математические методы для решения задач научной и проектно-технологической деятельности	ПК-5.1. Умеет: анализировать поставленную задачу и находить алгоритм ее решения; выбирать оптимальные системы программирования, наиболее подходящие для решения поставленной задачи ПК-5.2. Знает: современные методы цифровой обработки изображений и средства компьютерной графики ПК-5.3. Владеет: методами моделирования информационных процессов; навыками работы над производственным проектом в составе группы научных специалистов
		ПК-6 способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности	ПК-6.1. Умеет: проводить анализ и обосновывать необходимость работы над данным проектом и оценивать его эффективность; обосновывать и защищать предлагаемый проект, доказывать его эффективность и востребованность на выбранном рынке ПК-6.2. Знает: особенности рынка данного региона ПК-6.3. Владеет: навыками

			работы над проектами по выбранной тематике; методами построения, анализа и применения математических моделей для оценки состояния, и прогноза развития экономических процессов и явлений; владеть опытом выражения своих мыслей и мнения

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций	Оценочные средства	
			текущий контроль	промежуточная аттестация
1	Конечные группы	способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5), способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6)	УО-3 ПР-2	УО-2
2	Кольца и поля	способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5),	ПР-11	
3	Линейные рекуррентные последовательности над конечными полями	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6)	УО-3 ПР-2	УО-2
4	Полугруппы и конечные автоматы	способен разрабатывать и применять математические методы решения задач	УО-3 ПР-2	УО-2

		научной и проектно-технологической деятельности (ПК-5),		
5	Решетки и решеточные продолжения булевых функций	способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности (ПК-6)	ПР-11	
6	Эллиптические кривые	способен разрабатывать и применять математические методы решения задач научной и проектно-технологической деятельности (ПК-5),	УО-3 ПР-2	УО-2

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
ПК-5: способен разрабатывать и применять математические методы для решения задач научной и проектно-технологической деятельности	знает (пороговый уровень)	классические и современные методы цифровой обработки изображений и средства компьютерной графики	знание основных понятий и методов научных исследований в выбранной области математики	-способность наличие знаний основных понятий и методов научных исследований в выбранной области математики
	умеет (продвинутый)	анализировать поставленную задачу и находить алгоритм ее решения; выбирать оптимальные системы программирования, наиболее подходящие для	умение применять математические методы при исследовании в выбранной области математики	наличие в диссертации результатов эффективного применения методов системного анализа

		решения поставленной задачи		
	владеет (высокий)	методами моделирования информационных процессов; навыками работы над производственным проектом в составе группы научных специалистов	владение основными математическими методами научных исследований	демонстрация использования основных математических методов научных исследований
ПК-6 способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности	знает (пороговый уровень)	особенности рынка данного региона	знание наиболее применяемых пакетов прикладных программ	наличие знаний наиболее применяемых пакетов прикладных программ
	умеет (продвинутый)	проводить анализ и обосновывать необходимость работы над данным проектом и оценивать его эффективность; обосновывать и защищать предлагаемый проект, доказывать его эффективность и востребованность на выбранном рынке	реализация математически сложных алгоритмов в современных программных комплексах	демонстрация современных методов и технологий программирования с использованием сетей при реализации курсовых работ, ИДК и ВКР
	владеет (высокий)	навыками работы над проектами по выбранной тематике;	использование методов и технологий программирования методами компьютерного и	навыками построения непротиворечивых математических теорий

		методами построения, анализа и применения математических моделей для оценки состояния, и прогноза развития экономических процессов и явлений; владеть опытом выражения своих мыслей и мнения	математического моделирования	

Вопросы к сдаче зачета

1. Группы. Теорема Лагранжа.
2. Циклические группы.
3. НОД. Алгоритм Евклида. Теорема и линейном представлении НОД. НОК. Взаимно простые числа. Теорема Евклида.
4. Бесконечность количества простых чисел. Основная теорема арифметики.
5. Формула для вычисления функции Эйлера. Целая часть числа.
6. Свойства сравнений. Полная и приведенная системы представителей.
7. Теорема Эйлера. Малая теорема Ферма. Кольцо классов вычетов. Поле классов вычетов по простому модулю.
8. Гомоморфизмы групп.
9. Факторгруппы и нормальные подгруппы.
10. Действия групп на множествах, теорема о стабилизаторе.
11. Идеалы в кольцах многочленов.
12. Неприводимые многочлены. Основная теорема арифметики кольца многочленов.
13. Характеристика поля.

14.Сочетания. Перестановки. Группа подстановок. Инверсии. Транспозиции.

15.Алгебраические расширения конечных полей.

16.Рекуррентные последовательности над конечными полями.

17.Алгоритм Берлекемпа-Месси.

18.Эллиптические кривые над конечными полями.

19.Теорема о порядке группы точек эллиптической кривой.

Примеры контрольных работ

Тема: Группы и поля

Вариант 1

1. Вычислить порядок группы порожденной подстановками:

(123), (24), (15)

2. Построить расширение поля F_3 присоединением корня полинома

x^2+3x+1

3. Доказать, что кольце $F_3[x]$ все идеалы главные

Тема: Многочлены

1 вариант

1. Разложите многочлен $8x^4+8x^3-27x-27$ на множители.
2. Найдите наибольший общий делитель двух многочленов и его линейное представление:
   $x^5+3x^4+x^3-5x^2-6x-2$ и $x^5+2x^4-3x^2-4x-2$.
3. Отделите кратные множители:
   $x^7+6x^6-5x^5-80x^4-185x^3-194x^2-99x-20$.
4. Решите уравнение 3 степени: $x^3+3x^2-3x+4=0$.
5. Решите уравнение 4 степени: $x^4-2x^3+2x^2+4x-8=0$.
6. Для многочлена $3x^5+2x^4+x^3-10x-8$ определите кратность корня с=-1.
7. Разложите многочлен $x^4-8x^3+24x^2-50x+22$ по степеням $x-2$.

8. Найдите многочлен наименьшей степени с вещественными коэффициентами, имеющий тройной корень *i*, простые корни 2 и 3.
9. Найдите коэффициент *a* так, чтобы многочлен $x^5 - ax^2 - ax + 1$ имел –1 корнем не ниже второй кратности.
10. Запишите в лексикографическом виде: $2x^2y - 3x^2y^2 + y^5 + 4x^3y^2 + 7xy - 2x + 3$.
11. Выразите через элементарные симметрические многочлены: $x_1^3 + x_2^3 + x_3^3 - 3x_1x_2x_3$.
12. Представьте в виде суммы простейших дробей над полем действительных чисел: $\frac{2x^4 + 3}{x^3(x^2 - 1)}$.

Примеры индивидуальных домашних заданий

Тема: Кольца и поля

1. Докажите, что в кольце многочленов над конечным полем все идеалы главные.
2. Постройте пример бесконечного поля простой характеристики.
3. Найти все автоморфизмы поля комплексных чисел, которые оставляют на месте действительные числа.
4. Определите условия, прикоторых факторкольцо кольца многочленов над полем будет полем.

Тема: Группы

Пусть A, B, C подгруппы конечной группы G. Докажите, что

1) если $B \le A$, то $|A:B| \ge |C \cap A : C \cap B|$;
2) $|G:A \cap B| \le |G:A||G:B|$;
3) $A \cup B$ является подгруппой G, если и только если $A \subseteq B$ или $B \subseteq A$;
4) если $G = AA^g$ для некоторого $g \in G$, тогда $G = A$.
5) группа G имеет четный порядок, если и только если число инволюций (элементов второго порядка) нечетно;
6) если каждый элемент группы имеет порядок два, то группа абелева;
7) если группа содержит точно одну максимальную подгруппу, то она циклическая.