ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

Решением Ученого совета
АНО ВО «Центральный университет»
«07» марта 2024 г.
Протокол №1

Рабочая программа дисциплины (модуля)
«Алгебра»

Направление подготовки: *02.03.01 Математика и компьютерные науки*

Направленность (профиль) подготовки: *Программа двух дипломов НИУ ВШЭ и ЦУ «Прикладная математика и информатика»*

Квалификация (степень) выпускника: *бакалавр*

Форма обучения: *очная*

Срок освоения программы: *4 года*

Год набора: *2024*

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0215B0C000D1B3FEB44A37EE631E0C27D4
Владелец: Ивашкевич Евгений Васильевич
Действителен: с 13.01.2026 до 13.04.2027

Электронный документ

Москва
2024

Содержание

1. **Краткая характеристика дисциплины (модуля)** 3
2. **Перечень планируемых результатов обучения** 5
3. **Тематический план** 7
4. **Содержание дисциплины (модуля)** 7
5. **Учебно-методическое обеспечение** 9
6. **Материально-техническое обеспечение** 9
7. **Методические и оценочные материалы** 11

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Алгебра» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению 02.03.01 «Математика и компьютерные науки», профиль «Программа двух дипломов НИУ ВШЭ и ЦУ «Прикладная математика и информатика», утвержденный приказом Министерства науки и высшего образования Российской Федерации № 807 от 23.08.2017 года.

Изучение дисциплины (модуля) дает развитие аналитического мышления, навыков работы с математическими моделями и понимания пространственных структур, что является основой для дальнейшего изучения более сложных математических и компьютерных дисциплин.

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебный план по программе подготовки бакалавриата по направлению 02.03.01 «Математика и компьютерные науки», профиль «Программа двух дипломов НИУ ВШЭ и ЦУ «Прикладная математика и информатика» и входит в вариативную часть Блока 1, как дисциплина по выбору.

Дисциплина (модуль) изучается на 3, 4 курсах в 6, 7 или 8 семестрах на выбор.

Цель изучения дисциплины (модуля): формирование у студентов основных понятий и методов линейной алгебры, необходимых для решения задач в области математики и компьютерных наук.

Задачи изучения дисциплины (модуля):

— ознакомить студентов с ключевыми понятиями и структурами современной алгебры, такими как группы, кольца, поля, модули и векторные пространства, а также их свойствами и взаимосвязями;

— развить навыки логического мышления, доказательства теорем и решения алгебраических задач, включая работу с абстрактными объектами и применение алгебраических методов к конкретным примерам;

— подготовить студентов к интеграции алгебраических знаний в компьютерные науки, в частности, для понимания алгоритмов, криптографии, теории кодирования и вычислительной математики;

— сформировать умения применять алгебраические методы в анализе и моделировании сложных систем, способствуя развитию компетенций, необходимых для дальнейшего обучения и профессиональной деятельности в области математики и компьютерных наук.

В результате освоения дисциплины (модуля) обучающийся должен:

знать:

— основные определения и классификацию алгебраических структур: группы, кольца, поля, идеалы;

— фундаментальные теоремы структурной алгебры: теорема Лагранжа, теоремы о гомоморфизмах для групп и колец, китайская теорема об остатках;

— основные свойства и строение конечных полей, включая их цикличность мультипликативной группы;

— базовые принципы работы алгоритмов символьных вычислений: алгоритм Евклида для многочленов, алгоритм Бухбергера построения базисов Грёбнера;

— основные понятия и конструкции прикладной алгебры: расстояние Хэмминга, принцип работы криптосистем RSA и Диффи-Хеллмана;

уметь:

— определять, является ли данное множество с операциями группой, кольцом, полем; находить подгруппы, идеалы, проверять нормальность;

— работать с фактор-структурами (группами и кольцами) по подгруппе и идеалу, применяя теоремы о гомоморфизмах;

— выполнять арифметические операции в полях вычетов и конечных полях, раскладывать многочлены на неприводимые множители над заданным полем;

— строить базисы Грёбнера для систем полиномиальных уравнений и использовать их для решения задачи принадлежности идеалу и исключения переменных;

— производить простейшие криптографические вычисления (шифрование/расшифрование, обмен ключами) и оценивать корректирующую способность линейных кодов по их параметрам;

владеть:

— аппаратом теории групп для анализа симметрий и структуры объектов: порядков элементов, смежных классов, прямых произведений;

— методами факторизации колец и полей для решения задач о делимости и построения расширений полей;

— навыками работы с многочленами от одной и нескольких переменных: деление с остатком, нахождение НОД, редукция относительно мономиальных порядков;

— языком и основными техниками теории линейных кодов для обнаружения и исправления ошибок (на примере кодов Хэмминга);

— фундаментальной связью между абстрактными алгебраическими понятиями (свободные объекты, факторизация) и их прикладными реализациями (базисы Грёбнера, кодирование, криптография).

2. Перечень планируемых результатов обучения

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

Компетенция	Содержание компетенции	Индикатор компетенции	Перечень планируемых результатов обучения по дисциплине (модулю)
УК-1.	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1.	Знает методы поиска и анализа информации в области искусственного интеллекта, основные принципы критической оценки источников информации и их релевантности.
		УК-1.2.	Умеет критически оценивать источники информации и синтезировать данные из различных источников для решения задач, применять системный подход к анализу и решению комплексных проблем
		УК-1.3.	Имеет практический опыт работы с современными инструментами и технологиями для обработки информации, формулировании и структурировании задач на основе полученной информации
УК-2.	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1.	Знает действующие правовые нормы, регулирующие деятельность в области решения задач, основные методы и подходы к определению круга задач
		УК-2.2.	Умеет определять круг задач в рамках поставленной цели, выбирать оптимальные способы решения задач, учитывая имеющиеся ресурсы и ограничения
		УК-2.3.	Имеет практический опыт применения знаний о правовых нормах и ресурсах в реальных ситуациях, разработки и реализации решений в соответствии с установленными ограничениями
ОПК-1.	Способен находить, формулировать и решать актуальные и значимые проблемы прикладной и компьютерной математики	ОПК-1.1.	Знает основные методы и подходы к решению задач прикладной и компьютерной математики, включая алгоритмы, математическое моделирование и теорию оптимизации, а также современные инструменты и технологии, используемые в этой области
		ОПК-1.2.	Умеет анализировать и формулировать математические задачи, применять соответствующие методы и алгоритмы для их решения, а также интерпретировать и

			представлять результаты в понятной и доступной форме
		ОПК-1.3.	Имеет практический опыт работы над проектами или исследованиями в области прикладной и компьютерной математики, включая участие в конкурсах, олимпиадах или научных публикациях, где были решены актуальные и значимые задачи
ПК-1.	Способен формулировать задачи с математической точностью, обосновывать утверждения строго и анализировать полученные результаты в области математики и компьютерных наук	ПК-1.1.	Знает методы и подходы к формулированию задач, а также основные принципы математического доказательства и анализа результатов.
		ПК-1.2.	Умеет корректно ставить и формулировать математические задачи, применять строгие методы доказательства и анализировать полученные результаты.
		ПК-1.3.	Имеет опыт работы с задачами в области математики и компьютерных наук, включая применение математических методов для решения практических задач
ПК-2.	Способен решать типовые задачи профессиональной деятельности в области искусственного интеллекта, опираясь на информационную и библиографическую культуру, используя информационно-коммуникационные технологии и учитывая основные требования информационной безопасности	ПК-2.1.	Знает основы информационной и библиографической культуры, а также принципы информационной безопасности и применения информационно-коммуникационных технологий в профессиональной деятельности
		ПК-2.2.	Умеет эффективно использовать информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности, учитывая требования информационной безопасности
		ПК-2.3.	Имеет опыт работы с информационными ресурсами и технологиями в области искусственного интеллекта, включая соблюдение норм информационной безопасности

3. Тематический план

№п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Аудиторная работа		Контроль	Самостоятельная работа	
		Лекции	Семинары (практические занятия)			
1	Целые числа и делимость	6	6		16	Домашнее задание
2	Начала теории групп	6	6		16	Домашнее задание
3	Начала теории колец	6	6		16	Домашнее задание
4	Поля	2	2		14	Домашнее задание
5	Формальные степенные ряды	2	2		14	Домашнее задание
6	Алгебраические приложения	2	2		14	Домашнее задание
7	Модули и абелевы группы	4	4		16	Домашнее задание
8	Теория категорий	2	2	2	16	Контрольная работа
	Зачет с оценкой			***4***		
	Итого:	***30***	***30***	***6***	***124***	
Объем дисциплины (модуля) (в ак. ч.)		***190***				
Объем дисциплины (модуля) (в зач. ед.)		***5***				

4. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Целые числа и делимость	Целые числа: делимость, НОД, алгоритм Евклида, основная теорема арифметики Сравнения по модулю, классы вычетов, китайская теорема об остатках, малая теорема Ферма Многочлены одной переменной: деление с остатком, НОД, теорема Безу
2	Начала теории групп	Группы: определение, примеры, гомоморфизмы, подгруппы Порядок элемента и группы, циклические группы, порождающие элементы Нормальные подгруппы, факторгруппы, прямые произведения групп
3	Начала теории колец	Кольца: определение, примеры, подкольца, гомоморфизмы Идеалы, факторкольца, кольца вычетов Кольца частных, китайская теорема об остатках для колец, примеры факторколец
4	Поля	Определение и примеры полей, конечные поля, построение конечных полей
5	Формальные степенные ряды	Производящие функции
6	Алгебраические приложения	Дискретный логарифм, RSA, протокол Диффи — Хеллмана
7	Модули и абелевы группы	Модули над кольцами, их примеры, свободные модули Конечнопорождённые абелевы группы и их строение

8	Теория категорий	Объекты и морфизмы, категории алгебраических структур, функторы

5. Учебно-методическое обеспечение

Университет располагает полным набором лицензионного и свободно распространяемого программного обеспечения, включая продукты отечественного производства.

Каждый студент в течение всего периода обучения получает индивидуальный неограниченный доступ к электронно-библиотечной системе и электронной информационно-образовательной среде университета. Эти системы предоставляют возможность доступа к ресурсам из любой точки, где есть подключение к сети Интернет, как на территории университета, так и за его пределами.

Студентам обеспечен удаленный доступ к современным профессиональным базам данных и информационным справочным системам.

Основная литература:

1. Кашапова, Ф. Р. Высшая математика. Общая алгебра в задачах : учебник для вузов / Ф. Р. Кашапова, И. А. Кашапов, Т. Н. Фоменко. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 128 с. — (Высшее образование). — ISBN 978-5-534-09499-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/585819.

2. Пожидаев, А. П. Высшая алгебра : учебник для вузов / А. П. Пожидаев, С. Р. Сверчков, И. П. Шестаков. — Москва : Издательство Юрайт, 2025. — 203 с. — (Высшее образование). — ISBN 978-5-534-20177-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/569208.

3. Фоменко, Т. Н. Высшая математика. Общая алгебра. Элементы тензорной алгебры : учебник и практикум для вузов / Т. Н. Фоменко. — Москва : Издательство Юрайт, 2025. — 121 с. — (Высшее образование). — ISBN 978-5-534-08097-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/563714.

Дополнительная литература:

1. Бурмистрова, Е. Б. Линейная алгебра : учебник и практикум для вузов / Е. Б. Бурмистрова, С. Г. Лобанов. — Москва : Издательство Юрайт, 2025. — 421 с. — (Высшее образование). — ISBN 978-5-534-15839-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560017.

6. Материально-техническое обеспечение

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины (модуля) обеспечивается в учебных аудиториях, оснащенных:

— столами и стульями;

— компьютерной техникой;

— механическими калькуляторами;

— специализированным оборудованием, включая демонстрационное оборудование.

Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Наименование портала (издания, курса, документа)	Ссылка
1.	Научная электронная библиотека elibrary.ru библиотека	https://elibrary.ru/defaultx.asp
2.	База данных для IT-специалистов	https://habr.com
3.	База данных ScienceDirect	https://www.sciencedirect.com
4.	Официальный сайт Министерства науки и высшего образования Российской Федерации	https://minobrnauki.gov.ru/
5.	Федеральный портал «Российское образование"	https://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/

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), в том числе комплект лицензионного программного обеспечения, современные профессиональные базы данных и информационные справочные системы:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		
Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное
Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное

Справочно-правовые системы:		
КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное
Среды разработки:		
Visual Studio Code	зарубежное	свободно распространяемое
Bash (Unix shell)	зарубежное	свободно распространяемое
Anaconda	зарубежное	свободно распространяемое
Robotic Operating System	зарубежное	свободно распространяемое
CopelliaSim	зарубежное	свободно распространяемое
Google Colaboratory	зарубежное	свободно распространяемое
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

7. Методические и оценочные материалы

Методические указания для обучающихся по освоению дисциплины (модуля)

В процессе изучения дисциплины (модуля) «Алгебра» в рамках текущего контроля успеваемости используются такие виды учебной работы, как лекция, семинары, контрольные работы и домашние задания, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков профессиональной лексики, закрепление практических профессиональных компетенций, поощрение инициатив.

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект лекций: кратко и схематично фиксировать основные идеи, выводы и обобщения лекции; выделять важные мысли, ключевые слова и термины. Необходимо отметить вопросы или материалы, которые вызывают затруднения, и попытаться найти ответы в рекомендованной литературе. Если разобраться в материале не удается, следует сформулировать вопрос и задать его преподавателю на консультации или во время семинарского (практического) занятия.

Семинар — это форма учебной деятельности, проводимая в учебном заведении под руководством преподавателя, где студенты активно участвуют в обсуждениях, практических заданиях и других формах взаимодействия.

Для успешной подготовки к семинару рекомендуется заранее ознакомиться с темой занятия и основными материалами, чтобы иметь возможность активно участвовать в обсуждении. Также полезно подготовить вопросы и идеи для обсуждения, что поможет глубже понять материал и продемонстрировать заинтересованность.

Домашнее задание – набор задач по темам недели.

При работе над домашними заданиями важно внимательно ознакомиться с

требованиями и сроками выполнения. Рекомендуется разбивать задания на этапы, чтобы избежать перегрузки и лучше усвоить материал. Использовать различные источники информации, включая учебники и онлайн-ресурсы, для более глубокого понимания темы.

Контрольная работа – письменная работа с набором задач, которые нужно решить за ограниченное время.

Цель контрольной работы - получить специальные знания по одной или нескольким темам дисциплины (модуля) и продемонстрировать навыки их практического применения.

Самостоятельная работа – работа студентов, направленная на углубленное изучение отдельных тем и вопросов учебной дисциплины (модуля).

В процессе самостоятельной работы студенты взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи студента включают работу с конспектами лекций (обработка текста), повторное изучение учебных материалов планов и тезисов ответов, изучение дополнительных тем, выполнение учебно-исследовательских заданий и другое.

Система оценивания результатов обучения по дисциплине (модулю)

Критерии получения уровня и оценивания сформированности компетенций по дисциплине «Алгебра»

Оценивание уровня учебных достижений, обучающихся по дисциплине (модулю), осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме ***зачета с оценкой***, при этом проводится оценка компетенций, сформированных по дисциплине.

Для оценивания текущего контроля успеваемости и промежуточной аттестации используется десятибалльная шкала оценивания, которая соотносится с традиционной пятибалльной шкалой следующим образом, если иное не указано в силлабусе дисциплины:

Десятибалльная оценка	**Пятибалльная оценка**	**Оценка за зачет**	**Общая характеристика результата обучения по дисциплине (модулю)**
10	Отлично	Зачтено	Студент полностью владеет знаниями, изложенными в рабочей программе, и глубоко осмысляет дисциплину. Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя ключевые моменты и устанавливая причинно-следственные связи. Четко формулирует ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет
9	Отлично	Зачтено	
8	Отлично	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
			связывать теоретические аспекты дисциплины (модуля) с практическими задачами.
7	Хорошо	Зачтено	Студент обладает знаниями предмета почти в полном объеме рабочей программы и самостоятельно, логически последовательно и всесторонне отвечает на все вопросы, акцентируя внимание на наиболее значимых моментах. Он умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя его ключевые аспекты и устанавливая причинно-следственные связи. Формулирует свои ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные ситуационные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами.
6	Хорошо	Зачтено	
5	Удовлетворительно	Зачтено	Студент обладает базовыми знаниями по дисциплине (модулю), но испытывает трудности при самостоятельных ответах и использует неточные формулировки. В ходе ответов он допускает ошибки, касающиеся сути вопросов. Студент способен решать только самые простые задачи и владеет лишь минимальным набором методов исследования.
4	Удовлетворительно	Зачтено	
3	Не сдан	Не зачтено	Студент не овладел обязательным минимумом знаний по предмету и не может ответить на вопросы, даже если преподаватель задает дополнительные наводящие вопросы.
2	Не сдан	Не зачтено	
1	Не сдан	Не зачтено	

Дисциплина (модуль) «Алгебра» оценивается следующим образом:

Активность	Вес	Количество	Описание
Домашние задания	30%	4	Набор задач по темам недели
Контрольные работы	30%	1	Письменная работа с набором задач, которые нужно решить за ограниченное время
Зачет с оценкой	40%	1	Письменная работа с набором задач, которые нужно решить за ограниченное время

Электронный документ

Формула расчёта итоговой оценки по дисциплине (модулю) «Алгебра»: «0,3 × среднее за домашние задания + 0,3 × среднее за контрольные работы + 0,4 × зачет с оценкой».

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

Примерные домашние задания

Домашнее задание 1

1. Дайте определение группы и приведите примеры абелевой и неабелевой групп. Объясните свойства ассоциативности, единичного элемента и обратного элемента.

2. Для группы Z6 (аддитивная группа целых чисел по модулю 6) найдите порядок каждого элемента и определите все подгруппы.

3. Сформулируйте теорему Лагранжа и проиллюстрируйте её примером для симметрической группы S3.

4. Объясните понятия смежных классов и нормальных подгрупп. Приведите пример нормальной подгруппы в группе Z12.

5. Докажите, что прямое произведение двух циклических групп Cn и Cm является циклической группой тогда и только тогда, когда gcd(n, m) = 1. Приведите пример для n=2, m=3.

Домашнее задание 2

1. Дайте определения кольца и поля. Приведите примеры кольца, которое не является полем, и поля, которое не является кольцом с единицей.

2. Для многочленов над полем Q найдите НОД многочленов x^3 - 1 и x^2 + x + 1. Проверьте, являются ли они неприводимыми.

3. Опишите строение конечных полей. Постройте поле GF(4) и найдите его мультипликативную группу.

4. Объясните принцип работы криптосистемы RSA: выберите простые числа p=7, q=11, e=13, зашифруйте сообщение m=5 и расшифруйте его.

5. Опишите протокол Диффи–Хеллмана для обмена ключами. Выполните вычисление общего ключа для параметров g=5, p=23, a=6, b=15.

Домашнее задание 3

1. Объясните понятие расстояния Хэмминга для линейных кодов. Для кода [7,4,3] (код Хэмминга) найдите минимальное расстояние и максимальное количество исправляемых ошибок.

2. Для многочленов от двух переменных x и y над Q с лексикографическим порядком найдите базис Грёбнера для идеала (x^2 - y, xy - 1).

3. Сформулируйте теорему о гомоморфизме для групп и колец. Приведите пример факторизации кольца Z по идеалу 4Z.

4. Объясните понятие свободной абелевой группы. Постройте свободную абелеву группу ранга 2 и найдите её базис.

5. Для идеала (x^2 + y - 1, x + y^2) над Q[x,y] решите проблему принадлежности: принадлежит ли многочлен x + y идеалу? Используйте базис Грёбнера для проверки.

Примерные задания по контрольной работе

Контрольная работа

1. Дайте определение группы и перечислите её основные свойства. Приведите пример группы, которая не является абелевой, и объясните, почему она не абелева.
2. Для группы симметрии треугольника (группы D3) найдите порядок группы, порядок каждого элемента и все подгруппы.
3. Сформулируйте теорему Лагранжа и докажите её для группы Z8 (аддитивная группа по модулю 8).
4. Объясните понятия смежных классов и нормальных подгрупп. Покажите, что подгруппа 2Z является нормальной в Z, и найдите факторгруппу Z/2Z.
5. Опишите, что такое гомоморфизм групп, ядро и образ. Приведите пример гомоморфизма из Z в Z6 с ненулевым ядром.
6. Дайте определения кольца и поля. Приведите пример кольца без единицы и поля характеристики 2.
7. Для многочленов над полем R найдите НОД многочленов x^4 - 1 и x^2 + 1. Определите, являются ли они неприводимыми.
8. Постройте поле GF(8) и найдите его мультипликативный порядок. Объясните, почему оно является циклическим.
9. Реализуйте протокол Диффи–Хеллмана: выберите p=17, g=3, a=5, b=7, вычислите общий секретный ключ. Объясните, почему протокол безопасен.
10. Объясните понятие расстояния Хэмминга для линейного кода. Для кода Рида–Соломона над GF(5) с параметрами n=4, k=2 найдите минимальное расстояние.
11. Для многочленов над Q[x,y] с лексикографическим порядком постройте базис Грёбнера для идеала (x^2 - y^2, x y - 1).
12. Опишите критерий Бухбергера для базиса Грёбнера. Приведите пример редукции многочлена относительно базиса.
13. Решите проблему принадлежности: принадлежит ли многочлен x^3 + y^2 + 1 идеалу (x^2 + y, x y - 1) над Q[x,y]? Используйте базис Грёбнера для проверки.

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1	Определите порядок группы симметрии треугольника.	6	УК-1
2	Назовите теорему, утверждающую, что порядок подгруппы делит порядок группы.	теорема Лагранжа	УК-1
3	Найдите число смежных классов по подгруппе 2Z в группе Z.	2	УК-1
4	Определите, является ли подгруппа 3Z нормальной в Z.	да	УК-1
5	Назовите свойство группы, при котором операция коммутативна.	абелева	УК-2
6	Определите порядок элемента 2 в группе Z5.	4	УК-2
7	Найдите ядро гомоморфизма φ: Z → Z6, заданного φ(n) = n mod 6.	6Z	УК-2
8	Назовите прямое произведение двух групп A и B.	A × B	УК-2
9	Определите характеристику поля рациональных чисел.	0	ОПК-1
10	Найдите НОД многочленов x^2 + 1 и x^2 - 1 над Q.	x^2 - 1	ОПК-1
11	Определите, является ли многочлен x^2 + 1 неприводимым над R.	да	ОПК-1
12	Найдите порядок мультипликативной группы поля GF(7).	6	ОПК-1
13	Назовите криптографический протокол, основанный на дискретном логарифме.	Диффи–Хеллман	ПК-1

Электронный документ

14	Определите, что такое расстояние Хэмминга для двух слов длины 3: 101 и 011.	2	ПК-1
15	Найдите минимальное расстояние кода Хэмминга (7,4).	3	ПК-1
16	Назовите алгоритм построения базиса Грёбнера.	алгоритм Бухбергера	ПК-1
17	Определите, принадлежит ли многочлен x^2 идеалу (x).	да	ПК-2
18	Найдите факторгруппу Z/4Z.	Z4	ПК-2
19	Назовите теорему о гомоморфизме для колец.	основная теорема о гомоморфизме	ПК-2
20	Определите, является ли свободная абелева группа ранга 2 абелевой.	да	ПК-2