

УТВЕРЖДЕНА

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

**Рабочая программа дисциплины (модуля)
«Алгебра»**

Направление подготовки: 38.03.05 Бизнес-информатика

Направленность (профиль) подготовки: Бизнес-аналитика

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Срок освоения программы: 4 года

Год набора: 2024

**Москва
2024**

Содержание

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

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Алгебра» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по специальности 38.03.05 Бизнес-информатика, профиль Бизнес-аналитика, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 838 от 29.07.2020 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 38.03.05 Бизнес-информатика, профиль Бизнес-аналитика и входит в вариативную часть Блока 1, как дисциплина по выбору.

Дисциплина (модуль) изучается на 1 или 3, 4 курсах во 2, 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 свойства бинарных операций и критерии их замкнутости, ассоциативности, коммутативности;

— определения групп, подгрупп, порядок элементов, циклические и абелевы группы;

— понятия гомоморфизма и изоморфизма групп, теоремы об изоморфизмах;

— формулировку и обоснование Китайской теоремы об остатках;

— основные свойства колец и полей, примеры конечных и бесконечных полей;

— алгебраическую структуру кодов с исправлением ошибок, включая линейные коды;

— основные операции с многочленами: деление, НОД, кратные корни, неприводимость;

— определение базиса Грёбнера и назначение алгоритма Бухбергера в вычислительной алгебре;

уметь:

- проверять свойства бинарных операций и строить таблицы Кэли для конечных множеств;
- находить порождающие множества и определять подгруппы в заданных группах;
- конструировать и интерпретировать гомоморфизмы и изоморфизмы между группами;
- применять Китайскую теорему об остатках для решения систем сравнений;
- выполнять операции в кольцах и полях, в том числе в конечных полях \mathbb{F}_p , \mathbb{F}_{p^n} ;
- определять параметры линейных кодов и применять синдромную декодировку;
- выполнять деление многочленов, находить остатки и применять алгоритм Евклида;
- реализовывать алгоритм Бухбергера для построения базиса Грёбнера;

владеть:

- навыками формального описания алгебраических структур и операций над ними;
- методами анализа групповых структур в симметриях, криптографических схемах и арифметических операциях;
- применением Китайской теоремы об остатках в криптографии и системах остаточных классов;
- использованием полей и колец в задачах кодирования, деления информации и вычислений по модулю;
- практическими приёмами построения и анализа линейных кодов с коррекцией ошибок;
- алгебраическим моделированием задач с помощью многочленов и систем полиномиальных уравнений;
- эффективной работой с базисами Грёбнера при решении систем уравнений и анализе идеалов в кольцах многочленов.

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 аналитики, 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
ОПК-4.	Способен понимать принципы работы информационных технологий; использовать информацию, методы и программные средства ее сбора, обработки и анализа для информационно-аналитической поддержки принятия управленческих решений	ОПК-4.1.	Знает основные принципы работы информационных технологий и их влияние на бизнес-процессы
		ОПК-4.2.	Умеет использовать методы и программные средства для сбора, обработки и анализа информации, обеспечивая качественную информационно-аналитическую поддержку
		ОПК-4.3.	Имеет практический опыт в применении аналитических инструментов для поддержки принятия управленческих решений в организациях
ПК-2.	Способен использовать соответствующий математический аппарат и инструментальные средства для обработки, анализа и систематизации информации по теме исследования для решения задач профессиональной деятельности	ПК-2.1.	Знает основные математические методы и инструментальные средства, применяемые для обработки и анализа информации
		ПК-2.2.	Умеет эффективно использовать математический аппарат для систематизации данных и решения профессиональных задач
		ПК-2.3.	Имеет практический опыт работы с инструментами анализа информации в рамках исследовательских проектов

3. Тематический план

№п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Контактная работа		Контроль	Самостоятельная работа	
Лекции	Семинары (практические занятия)					
1	Основы теории групп	7	7		31	Домашнее задание
2	Кольца, поля и приложения в криптографии	8	8		31	Домашнее задание
3	Алгебраические коды и вычислительная алгебра	8	8	2	31	Домашнее задание Контрольная работа
4	Факторструктуры и общая алгебра	7	7		31	Домашнее задание
	<i>Зачет с оценкой</i>			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	Основы теории групп	Группы: определение, свойства, подгруппы, порядок элемента. Смежные классы, нормальные подгруппы, теорема Лагранжа. Гомоморфизмы групп, ядро и образ, прямые произведения. Конечные абелевы группы и китайская теорема об остатках
2	Кольца, поля и приложения в криптографии	Кольца и поля: структура, идеалы, гомоморфизмы. Многочлены над полями: деление, НОД, неприводимость, факторизация. Конечные поля: строение, цикличность, построение. Криптографические приложения: дискретный логарифм, RSA, Диффи–Хеллман
3	Алгебраические коды и вычислительная алгебра	Коды с исправлением ошибок: расстояние Хэмминга, линейные коды, коды Хэмминга и Рида–Соломона. Многочлены от нескольких переменных: мономиальные порядки, редукция. Базисы Грёбнера: определение, критерий Бухбергера, алгоритм построения. Проблема принадлежности идеалу и исключение переменных
4	Факторструктуры и общая алгебра	Отношения эквивалентности и факторизация: группы и кольца. Теоремы о гомоморфизме для групп и колец. Свободные алгебраические структуры: свободные абелевы группы, свободные алгебры, связь с базисами Грёбнера

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. Ларин, С. В. Алгебра и теория чисел. Группы, кольца и поля : учебник для вузов / С. В. Ларин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 160 с. — (Высшее образование). — ISBN 978-5-534-05567-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/563870>.

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. Журавлев, Ю. И. Дискретный анализ. Основы высшей алгебры : учебник для вузов / Ю. И. Журавлев, Ю. А. Флеров, М. Н. Вялый. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 216 с. — (Высшее образование). — ISBN 978-5-534-06277-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/559327>.

4. 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 удастся, 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:

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
9	Отлично	Зачтено	
8	Отлично	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
			исследований, а также решает сложные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет 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	Описание
Домашние задания	30%	Набор задач по темам недели

Активность	Вес	Описание
Контрольные работы	30%	Письменная работа с набором задач, которые нужно решить за ограниченное время
Зачет с оценкой	40%	Письменная работа с набором задач, которые нужно решить за ограниченное время

Формула расчёта итоговой оценки по дисциплине (модулю) «Алгебра»:
« $0,3 \times$ среднее за домашние задания + $0,3 \times$ среднее за контрольные работы + $0,4 \times$ экзамен».

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 Z_6 (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 S_3 .
4. Объясните понятия смежных классов и нормальных подгрупп. Приведите пример нормальной подгруппы в группе Z_{12} .
5. Докажите, что прямое произведение двух циклических групп C_n и C_m 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 $\mathbb{Q}[x, y]$ 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 D_3) найдите порядок группы, порядок каждого элемента и все подгруппы.

3. Сформулируйте теорему Лагранжа и докажите её для группы Z_8 (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 Z_6 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 $\mathbb{Q}[x, y]$ 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 $\mathbb{Q}[x, y]$? 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	ОПК-4
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	ОПК-4

6	Определите порядок элемента 2 в группе Z_5 .	4	УК-1
7	Найдите ядро гомоморфизма $\varphi: Z \rightarrow Z_6$, заданного $\varphi(n) = n \pmod 6$.	$6Z$	УК-1
8	Назовите прямое произведение двух групп A и B.	$A \times B$	УК-1
9	Определите характеристику поля рациональных чисел.	0	ОПК-4
10	Найдите НОД многочленов $x^2 + 1$ и $x^2 - 1$ над Q .	$x^2 - 1$	ПК-2
11	Определите, является ли многочлен $x^2 + 1$ неприводимым над R .	да	ПК-2
12	Найдите порядок мультипликативной группы поля $GF(7)$.	6	ОПК-4
13	Назовите криптографический протокол, основанный на дискретном логарифме.	Диффи–Хеллман	ОПК-4
14	Определите, что такое расстояние Хэмминга для двух слов длины 3: 101 и 011.	2	ПК-2
15	Найдите минимальное расстояние кода Хэмминга (7,4).	3	ПК-2
16	Назовите алгоритм построения базиса Грёбнера.	алгоритм Бухбергера	ПК-2
17	Определите, принадлежит ли многочлен x^2 идеалу (x) .	да	ПК-2
18	Найдите факторгруппу $Z/4Z$.	Z_4	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