

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор физтех-школы
прикладной математики и
информатики**

А.М. Райгородский

	Рабочая программа дисциплины (модуля)
по дисциплине:	Основы высшей алгебры и теории кодирования
по направлению:	Прикладная математика и информатика
профиль подготовки:	Прикладная математика, компьютерные науки и инженерия Физтех-школа Прикладной Математики и Информатики кафедра математических основ управления
курс:	1
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 2 (весенний) - Дифференцированный зачет

Аудиторных часов: 60 всего, в том числе:

лекции: 30 час.

семинары: 0 час.

лабораторные занятия: 30 час.

Самостоятельная работа: 75 час.

Всего часов: 135, всего зач. ед.: 3

Количество контрольных работ, заданий: 3

Программу составил: М.Н. Вялый, канд. физ.-мат. наук, доцент

Программа обсуждена на заседании кафедры математических основ управления 15.05.2023

Аннотация

В курсе рассматриваются основные понятия высшей алгебры - группы, кольца, поля - и их приложения к теории чисел, комбинаторным задачам перечисления и теории корректирующих кодов. Особое внимание в курсе уделено конечным полям. Конечные поля являются одним из фундаментальных инструментов в современной теоретической информатике, необходимым в таких областях как математическая криптография, теория кодирования, теория планирования эксперимента, дерандомизация алгоритмов.

Для успешного освоения курса предполагается интенсивное самостоятельное решение задач студентами. В результате такого освоения студенты приобретают как полезные для многих дальнейших курсов знания, так и навыки работы с абстрактными понятиями, которые необходимы при изучении практически всех курсов по математике и теоретической информатике.

1. Цели и задачи

Цель дисциплины

Изучение основ теории групп и теории колец, включая теорию конечных полей, и приложений этих алгебраических дисциплин к перечислительной комбинаторике и теории корректирующих кодов.

Задачи дисциплины

- освоение студентами базовых знаний (понятий, концепций, методов и моделей) о группах, кольцах, полях и корректирующих кодах;
- приобретение теоретических знаний и практических умений и навыков оперирования с конкретными примерами групп, колец и полей;
- оказание консультаций и помощи студентам в изучении дополнительных разделов алгебры, необходимых для их собственных теоретических исследований в области дискретной математики.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	УК-6.1 Определяет приоритеты профессиональной деятельности и способы ее совершенствования на основе самооценки
	УК-6.2 Способен планировать самостоятельную деятельность в решении профессиональных задач; подвергать критическому анализу проделанную работу; находить и творчески использовать имеющийся опыт в соответствии с задачами саморазвития
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук и использовать их в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
	ОПК-1.3 Способен определять границы применимости полученных результатов

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- основные понятия, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть данной дисциплины;
- основные свойства групп, колец, полей, корректирующих кодов;
- подходы и методы для решения типовых задач о группах, кольцах, полях и корректирующих кодах.

уметь:

- понять поставленную задачу;
- использовать свои знания для решения фундаментальных и прикладных задач ОВАТК;
- оценивать корректность постановок задач;
- строго доказывать или опровергать утверждение;
- самостоятельно находить алгоритмы решения задач ОВАТК, в том числе и нестандартных, и проводить их анализ;
- самостоятельно видеть следствия полученных результатов;
- точно представить математические знания в области ОВАТК в устной и письменной форме.

владеть:

- навыками освоения большого объема информации и решения задач ОВАТК (в том числе, сложных);
- навыками самостоятельной работы и освоения новых дисциплин;
- культурой постановки, анализа и решения математических и прикладных задач, требующих для своего решения использования математических подходов и методов ОВАТК;
- предметным языком алгебры и навыками грамотного описания решения задач и представления полученных результатов.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Алгебраические структуры.	2		2	7
2	Основные примеры групп.	2		2	7
3	Структурные свойства групп.	3		3	7
4	Гомоморфизмы групп.	4		4	7
5	Приложения теории групп к элементарной теории чисел.	2		2	7
6	Приложения теории групп к перечислительной комбинаторике, лемма Бернсайда.	2		2	7
7	Кольца и основные свойства колец.	2		2	7
8	Идеалы, кольца классов вычетов, гомоморфизмы колец.	2		2	7
9	Евклидовы кольца, их свойства и примеры.	4		4	6
10	Поля, примеры полей. Свойства конечных полей.	3		3	7
11	Корректирующие коды. Конструкции корректирующих кодов, основанные на теории конечных полей.	4		4	6
Итого часов		30		30	75
Подготовка к экзамену		0 час.			
Общая трудоёмкость		135 час., 3 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 2 (Весенний)

1. Алгебраические структуры.

Определения бинарной операции, полугрупп, моноидов, групп.

2. Основные примеры групп.

Циклические группы. Аддитивная группа вычетов по модулю n . Группа перестановок (симметрическая группа). Цикловое разложение перестановки. Четные и нечетные перестановки. Подгруппы. Порождающие или образующие элементы группы. Прямые произведения групп.

3. Структурные свойства групп.

Левые и правые смежные классы группы по подгруппе. Индекс подгруппы. Порядок элемента группы. Теорема Лагранжа.

Сопряженные элементы и сопряженные подгруппы. Нормальные подгруппы.

4. Гомоморфизмы групп.

Комбинаторные задачи о числе функций, слов в алфавите и размещений объектов по ячейкам при различных ограничениях. Числа Стирлинга первого рода, рекуррентное соотношение для них.

5. Приложения теории групп к элементарной теории чисел.

Мультипликативная группа вычетов по модулю n . Малая теорема Ферма, теорема Эйлера.

6. Приложения теории групп к перечислительной комбинаторике, лемма Бернсайда.

Действия групп. Лемма Бернсайда.

7. Кольца и основные свойства колец.

Примеры колец. Кольцо целых чисел. Кольцо многочленов над кольцом (полем). Кольца классов вычетов в кольце целых чисел и кольце многочленов. Прямые суммы колец. Подкольцо. Обратимые элементы кольца, группа обратимых элементов кольца, делители нуля. Нильпотентные элементы.

8. Идеалы, кольца классов вычетов, гомоморфизмы колец.

Левые, правые и двусторонние идеалы. Главные идеалы. Максимальные и простые идеалы. Кольца классов вычетов. Идеалы в кольцах многочленов. Факторкольцо. Теорема о гомоморфизме колец.

9. Евклидовы кольца, их свойства и примеры.

Деление с остатком в кольцах целых чисел и многочленов над кольцом целых чисел. Евклидовы кольца. Идеалы в евклидовых кольцах. Факториальность евклидовых колец. Китайская теорема об остатках.

Алгоритм Евклида. Решение линейных диофантовых уравнений.

10. Поля, примеры полей. Свойства конечных полей.

Поля. Примеры полей. Поле классов вычетов. Характеристика поля. Простое подполе. Конечные и алгебраические расширения полей. Поле разложения. Конечные поля.

Циклическость мультипликативной группы конечного поля. Первообразные корни.

11. Корректирующие коды. Конструкции корректирующих кодов, основанные на теории конечных полей.

Код Хэмминга, коды БЧХ. Оценка размерности и кодового расстояния для кодов БЧХ.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Учебная аудитория, оснащенная мультимедиапроектором и экраном.

6. Перечень рекомендуемой литературы

Основная литература

1. Дискретный анализ. Основы высшей алгебры [Текст] : учеб. пособие для вузов / Ю. И. Журавлев, Ю. А. Флеров, М. Н. Вялый ; М-во образования и науки Рос. Федерации, Моск. физ.-техн. ин-т (гос. ун-т) .— 2-е изд., испр. и доп. — М. : МЗ Пресс, 2007 .— 224 с.
2. Введение в алгебру [Текст] : в 3 ч. : учебник для вузов / А. И. Кострикин .— М. : МЦНМО, 2012 .— Ч. 1 : Основы алгебры. - 2012. - 272 с.
3. Алгебра [Текст] : Определения, теоремы, формулы : [учебник для вузов] / Б. Л. Ван дер Варден ; пер. с нем. А. А. Бельского .— 3-е изд., стереотип. — СПб. : Лань, 2004 .— 624 с.

Дополнительная литература

1. Курс высшей алгебры [Текст] : учебник для вузов / А. Г. Курош .— 10-е изд., стереотип. — : Наука, 1971 .— 431 с.
2. Основы теории групп [Текст] : [учеб. пособие для вузов] / М. И. Каргаполов, Ю. И. Мерзляков .— 4-е изд., перераб. — М. : Наука ; Физматлит, 1996 .— 288 с.
3. Основы теории чисел [Текст] : учеб. пособие для вузов / И. М. Виноградов .— 11-е изд., стереотип. — СПб. : Лань, 2006 .— 176 с.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

<http://www.mou.mipt.ru>
<http://vyalyy.narod.ru/da2.html>

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

Не предусмотрено.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Студент, изучающий курс «Основы высшей алгебры и теории кодирования», должен с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике.

В результате изучения дисциплины студент должен знать основные определения, понятия, аксиомы, методы доказательств.

Успешное освоение курса требует напряжённой самостоятельной работы студента. В программе курса приведено минимально необходимое время для работы студента над темой. Самостоятельная работа включает в себя:

- чтение и конспектирование рекомендованной литературы;
- проработку учебного материала (по конспектам лекций, учебной и научной литературе), подготовку ответов на вопросы, предназначенных для самостоятельного изучения, доказательство отдельных утверждений, свойств;

- решение задач, предлагаемых студентам на занятиях и в качестве курсового задания;
- подготовку к занятиям.

Руководство и контроль за самостоятельной работой студента осуществляется в форме индивидуальных консультаций.

Показателем владения материалом служит умение решать задачи. Для формирования умения применять теоретические знания на практике студенту необходимо решать как можно больше задач. При решении задач каждое действие необходимо аргументировать, ссылаясь на известные теоретические сведения.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов, следует обращаться за консультациями к лектору или преподавателю, ведущему практические занятия.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению:	Прикладная математика и информатика
профиль подготовки:	Прикладная математика, компьютерные науки и инженерия Физтех-школа Прикладной Математики и Информатики кафедра математических основ управления
курс:	<u>1</u>
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 2 (весенний) - Дифференцированный зачет

Разработчик: М.Н. Вялый, канд. физ.-мат. наук, доцент

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	УК-6.1 Определяет приоритеты профессиональной деятельности и способы ее совершенствования на основе самооценки
	УК-6.2 Способен планировать самостоятельную деятельность в решении профессиональных задач; подвергать критическому анализу проделанную работу; находить и творчески использовать имеющийся опыт в соответствии с задачами саморазвития
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук и использовать их в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
	ОПК-1.3 Способен определять границы применимости полученных результатов

2. Показатели оценивания компетенций

В результате изучения дисциплины «Основы высшей алгебры и теории кодирования» обучающийся должен:

знать:

- основные понятия, методы доказательств и доказательства основных теорем в разделах, входящих в базовую часть данной дисциплины;
- основные свойства групп, колец, полей, корректирующих кодов;
- подходы и методы для решения типовых задач о группах, кольцах, полях и корректирующих кодах.

уметь:

- понять поставленную задачу;
- использовать свои знания для решения фундаментальных и прикладных задач ОБАТК;
- оценивать корректность постановок задач;
- строго доказывать или опровергать утверждение;
- самостоятельно находить алгоритмы решения задач ОБАТК, в том числе и нестандартных, и проводить их анализ;
- самостоятельно видеть следствия полученных результатов;
- точно представить математические знания в области ОБАТК в устной и письменной форме.

владеть:

- навыками освоения большого объема информации и решения задач ОБАТК (в том числе, сложных);
- навыками самостоятельной работы и освоения новых дисциплин;
- культурой постановки, анализа и решения математических и прикладных задач, требующих для своего решения использования математических подходов и методов ОБАТК;
- предметным языком алгебры и навыками грамотного описания решения задач и представления полученных результатов.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Вопросы представлены в приложении.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Вопросы представлены в приложении.

Критерии оценивания

отлично 10 оценка «отлично (10)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

9 оценка «отлично (9)» выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

8 оценка «отлично (8)» выставляется студенту, показавшему всесторонние систематизированные, глубокие знания учебной программы дисциплины и умение применять их на практике при решении конкретных задач, и правильное обоснование принятых решений;

хорошо 7 оценка «хорошо (7)» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

6 оценка «хорошо (6)» выставляется студенту, если он знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

5 оценка «хорошо (5)» выставляется студенту, если он знает материал, и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

удовлетворительно 4 оценка «удовлетворительно (4)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

3 оценка «удовлетворительно (3)» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет фрагментарно основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

неудовлетворительно 2 оценка «неудовлетворительно (2)» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач;

1 оценка «неудовлетворительно (1)» выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения дифференцированного зачета обучающиеся могут пользоваться только письменными принадлежностями. Дифференцированный зачет проводится путем организации специального опроса, проводимого в устной форме и/или в форме теста.

3. Перечень типовых (примерных) вопросов, заданий, тем, используемых для оценки знаний, умений, навыков

1. Алгебраические структуры. Бинарные операции. Полугруппы и моноиды. Группы.
2. Примеры групп. Циклические группы. Аддитивная группа вычетов по модулю n . Группа перестановок (симметрическая группа). Цикловое разложение перестановки. Четные и нечетные перестановки. Подгруппы. Порождающие или образующие элементы группы. Прямые произведения групп.
3. Левые и правые смежные классы группы по подгруппе. Индекс подгруппы. Порядок элемента группы. Теорема Лагранжа.
4. Изоморфизмы, автоморфизмы и гомоморфизмы групп. Теорема Кэли.
5. Мультипликативная группа вычетов по модулю n . Малая теорема Ферма, теорема Эйлера.
6. Сопряженные элементы и сопряженные подгруппы. Нормальные подгруппы.
7. Действия групп. Лемма Бернсайда.
8. Фактор-группы. Ядро гомоморфизма. Внутренние автоморфизмы. Теорема о гомоморфизме групп.
9. Кольца. Примеры колец. Кольцо целых чисел. Кольцо многочленов над кольцом (полем). Кольца классов вычетов в кольце целых чисел и кольце многочленов. Прямые суммы колец. Подкольцо. Обратимые элементы кольца, группа обратимых элементов кольца, делители нуля. Нильпотентные элементы.
10. Левые, правые и двусторонние идеалы. Главные идеалы. Максимальные и простые идеалы. Кольца классов вычетов. Идеалы в кольцах многочленов. Факторкольцо. Теорема о гомоморфизме колец.
11. Деление с остатком в кольцах целых чисел и многочленов над кольцом целых чисел. Евклидовы кольца. Идеалы в евклидовых кольцах. Факториальность евклидовых колец. Китайская теорема об остатках.
12. Алгоритм Евклида. Решение линейных диофантовых уравнений.
13. Поля. Примеры полей. Поле классов вычетов. Характеристика поля. Простое подполе. Конечные и алгебраические расширения полей. Поле разложения. Конечные поля.
14. Циклическость мультипликативной группы конечного поля. Первообразные корни.
15. Корректирующие коды. Код Хэмминга, коды БЧХ. Оценка размерности и кодового расстояния для кодов БЧХ.

Курс включает курсовые задания.

Примеры задач для курсовых заданий

Обязательные задачи

1. Корни уравнения $x^n = I$, как действительные, так и комплексные, называются корнями n -й степени из единицы. Проверить, что корни n -й степени образуют группу по умножению. (а) Верно ли, что всякий корень 35-й степени из единицы является кубом некоторого корня 35-й степени из единицы? (б) Тот же вопрос про корни 36-й степени из единицы.
2. C_{360} - циклическая группа порядка 360. Найти число решений уравнения $x^k = e$ и количество элементов порядка k в группе C_{360} при а) $k = 7$; б) $k = 12$; в) $k = 48$. Сколько в C_{360} порождающих элементов?
3. Уравнение $x^{12} = e$ имеет 14 решений в группе G . Доказать, что группа G не является циклической.
4. Доказать, что в группе S_8 нет элементов порядка 56.
5. Найти порядок перестановки $(123)(4567)(89)$ и количество сопряженных ей перестановок в группе S_9 . Является ли эта перестановка четной?
6. Доказать, что все элементы порядка 11 сопряжены в S_{11} .
7. Порождают ли перестановки порядка 11 группу S_{11} ?
8. Построить некоммутативную группу минимального порядка.
9. Вычислить (а) $12^{257} \bmod 17$; (б) $10^{111} \bmod 121$.
10. Найти порядок элемента $(2,5)$ в прямом произведении циклических групп $C_{16} \times C_{12}$.
11. Доказать, что группа вращений трехмерного куба изоморфна группе S_4 .
12. Пусть G – группа вращений трехмерного куба, а H_v - ее подгруппа, состоящая из тех вращений, которые оставляют вершину v на месте. Указать повороты на 90° и на 180° из одного левого смежного класса по подгруппе H_v .
13. Существует ли сюръективный гомоморфизм а) $C_{24} \times C_{18}$ на C_{16} ; б) $C_{25} \times C_{18}$ на C_{15} ?
14. Доказать, что подгруппа, порожденная некоторым классом сопряженных элементов группы G , является нормальным делителем группы G .
15. Найти число различных раскрасок ребер трехмерного куба в два цвета. Две раскраски считаются различными, если нельзя добиться совпадения цветов ребер вращениями куба.

16. (а) Построить гомоморфизм φ аддитивной группы рациональных чисел $(\mathbb{Q}, +)$, ядром которого является подгруппа целых чисел $(\mathbb{Z}, +)$. (б) Проверить, что $(\mathbb{Q}, +) / \text{Ker } \varphi$ бесконечна, но все ее элементы имеют конечный порядок.

17. Доказать, что если элемент a кольца R не является делителем нуля, то из $ax = ay$ следует $x = y$. И наоборот: если элемент a кольца R является делителем нуля, то для некоторых $x \neq y$ выполняется $ax = ay$.

18. Ненулевой элемент кольца K называется нильпотентным, если при некотором n . Показать, что:

а) нильпотентность x влечет обратимость $1-x$, если K – кольцо с единицей;

б) кольцо содержит нильпотентные элементы в том и только том случае, если m делится на квадрат натурального числа, большего единицы;

в) множество нильпотентных элементов коммутативного кольца вместе с нулевым элементом образует подкольцо. Привести опровергающий пример в некоммутативном случае.

19. Является ли кольцом главных идеалов кольцо \mathbb{Z}_{72} ?

20. Решить линейное диофантово уравнение $33x + 23y = 4$.

21. Решить сравнения: $21x \equiv 13 \pmod{34}$, $7x \equiv 2 \pmod{73}$.

22. Решить систему сравнений

1. $x \equiv 1 \pmod{33}$,

2. $x \equiv -1 \pmod{23}$.

23. Найти наибольший общий делитель многочленов $x^{48} - 1$ и $x^{20} - 1$.

24. Найти порядок группы обратимых элементов кольца \mathbb{Z}_{72} .

25. Сумма идеалов $I_1 + I_2$ – это идеал, порожденный всеми суммами элементов из идеалов I_1, I_2 . Аналогично, произведение идеалов $I_1 I_2$ – это идеал, порожденный всеми произведениями элементов из I_1, I_2 . Пусть I_1 порожден в $\mathbb{Q}[x]$ многочленом $x^2 - x$, а I_2 порожден многочленом $x^2 + x$. Найти $I_1 + I_2, I_1 I_2, I_1 \cap I_2$.

26. Являются ли полями следующие кольца вычетов:

а) $\mathbb{Q}[x]/(x^3+1)$; б) $\mathbb{F}_3[x]/(x^3+2)$; в) $\mathbb{F}_7[x]/(x^3+3)$;

г) $\mathbb{Q}[x]/(x^4+1)$; д) $\mathbb{F}_3[x]/(x^4+1)$; е) $\mathbb{F}_{17}[x]/(x^4+1)$?

27. Многочлен $f(x)$ над полем \mathbb{F}_5 степени 2 принимает значение 1 в точке 1, значение 2 в точке 3 и значение 3 в точке 4. Найти $f(x)$.

28. Ненулевой элемент a поля называется квадратичным вычетом по модулю p , если

уравнение $x^2 = a$ имеет решение в поле Z_p . В противном случае a называется квадратичным невычетом. а) Найти сумму всех квадратичных вычетов по модулю 73. б) Найти произведение всех квадратичных невычетов по модулю 103.

29. Найти все первообразные корни по модулю 29.

30. Решить уравнение

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \equiv 0 \pmod{29}.$$

31. а) Доказать, что в любом поле характеристики 2 уравнение $x^2 + x + 1$ либо имеет ровно 2 различных корня, либо не имеет корней вовсе. б) Сколько решений имеет уравнение $x^2 + x + 1$ в поле из 512 элементов?

Дополнительные задачи

Д1. Построить группу G , в которой уравнение $x^{12} = e$ имеет ровно 14 решений.

Д2. Пусть G – группа, порожденная элементами a и b , для которых выполняются соотношения $ab = ba$, $a^2 = b^2$, $a^4 b^4 = e$. Найти порядок группы G . Является ли эта группа циклической?

Д3. Построить подгруппу порядка 56 группы S_8 . (Указание: используйте поле из 8 элементов.)

Д4. Указать две несопряженные изоморфные подгруппы порядка 12 в S_{11} .

Д5. Доказать, что если H – собственная подгруппа конечной группы G , то объединение сопряженных с H подгрупп не содержит всех элементов группы.

Д6. Пусть G – абелева группа и H – подгруппа всех ее элементов конечного порядка. Тогда в фактор – группе G/H все неединичные элементы имеют бесконечный порядок.

Д7. Укажите такую абелеву группу G и две такие ее изоморфные подгруппы H_1, H_2 , что фактор – группы G/H_1 и G/H_2 неизоморфны.

Д8. Доказать, что группа автоморфизмов циклической группы абелева. Найти порядок группы автоморфизмов циклической группы порядка 12. Является ли эта группа циклической?

Д9. Доказать, что нормальная подгруппа индекса k содержит все элементы, порядки которых взаимно просты с k .

Д10. Построить некоммутативную группу порядка 8, все подгруппы которой нормальны.

Д11. Доказать, число элементов, сопряженных с элементом a в группе G , равно индексу $N(a)$ в группе G , т.е. числу смежных классов по подгруппе $N(a)$ – нормализатору элемента a :

Д12. Коммутант группы – это подгруппа, порожденная коммутаторами, то есть элементами вида $x y x^{-1} y^{-1}$. Доказать, что коммутант является нормальной подгруппой.

Д13. Доказать, что фактор – группа G/H абелева тогда и только тогда, когда H содержит коммутант K группы G .

Д14. Доказать, что если порядок абелевой группы G равен nm , где $(n, m) = 1$, то G изоморфна прямому произведению групп порядков n и m .

Д15. Группа называется p -группой, если ее порядок является степенью простого числа p . Центром группы называется множество элементов, коммутирующих со всеми элементами группы. Доказать, что центр p -группы состоит не только из единичного элемента.

Д16. Доказать, что всякая группа порядка p^2 , где p – простое число, абелева.

Д17. Пусть порядок группы G равен $p^n m$, где p – простое число и $(p, m) = 1$. (а) Доказать, что в группе G есть подгруппа порядка p^n (силовская p -подгруппа). (б) Доказать, что любая p -подгруппа группы G содержится в силовской p -подгруппе. (в) Доказать, что все силовские p -подгруппы сопряжены. (г) Доказать, что количество силовских p -подгрупп равно 1 по модулю p .

Д18. Пусть n делит порядок группы G . Доказать, что число решений уравнения $x^n = e$ делится на n (а) для абелевой группы; (б) для p -группы; (в) для произвольной группы.

Д19. Указать пример коммутативного кольца с единицей R и его подкольца R_1 таких, что R_1 также является кольцом с единицей u , но $1 \neq u$.

Д20. Построить кольцо из 21 элемента, в котором произведения принимают ровно три различных значения.

Д21. В коммутативном кольце R с $0 \neq 1$ уравнение $x^2 = 2$ имеет три различных решения. Доказать, что в R есть делители нуля.

Д22. Доказать, что кольцо гауссовых целых чисел

$$Z(i) = \{a + bi : a, b - \text{целые}\}, i^2 = -1,$$

евклидово.

Д23. Проверить простоту элементов $17, 11, 2 + 3i$ в кольце $Z(i)$.

Д24. Является ли кольцо $Z(j) = \{a + bj : a, b - \text{целые}\}, j^2 = -6$,

евклидовым кольцом?

Д25. Доказать, что любой элемент кольца $Z/143Z$ является суммой двух делителей нуля. Найти представление в виде суммы двух делителей нуля для элемента 17 .

Д26. Найти все идеалы в кольце F_2^n (n -я прямая степень поля F_2).

Д27. Доказать, что идеал (x) в кольце многочленов $Z[x]$ над кольцом целых чисел Z имеет в качестве собственного делителя идеал $(2, x)$. Показать, что оба идеала при этом являются простыми.

Д28. Доказать, что кольцо многочленов $Z[x]$ над кольцом целых чисел Z не является евклидовым.

Д29. (а) Привести пример коммутативного кольца с единицей, в котором некоторый

простой элемент порождает идеал, не являющийся простым. (б) Привести пример коммутативного кольца с единицей, в котором некоторый простой идеал не является идеалом, порожденным простым элементом.

Д30. Построить пример коммутативного кольца с единицей, в котором разложение на простые множители неоднозначно.

Д31. Найти наибольший порядок элемента мультипликативной группы кольца Z_{72} .

Д32. Найти количество нильпотентных элементов в кольце

$$F_7[x]/(x^{14} + x^7 + 2).$$

Д33. Найти порядок группы обратимых элементов колец

$$(a) F_7[x]/(x^2 + 3x - 5); (б) F_3[x]/(x^2 + x + 1).$$

Д34. Построить изоморфизм полей $F_5[x]/(x^2 - 2)$ и $F_5[x]/(x^2 - 3)$.

Д35. Найти наименьшее конечное поле характеристики 2, в котором многочлен $x^{14} + 1$ раскладывается на линейные множители.

Д36. Сколько различных решений имеет уравнение $1 + x^2 + x^8 + x^{26} = 0$ в поле F_{81} из 81 элемента?

Д37. Элемент a порождает мультипликативную группу поля F из 343 элементов. Является ли многочлен $x^2 + ax - a + 2a^2$ неприводимым в кольце многочленов $F[x]$?

Д38. Указать степени неприводимых делителей многочленов (а) $x^5 - 2$ из кольца $F_{67}[x]$; (б) $x^{28} - 1$ из кольца $F_3[x]$.

Д39. Найти порядок группы $GL(2,4)$ обратимых линейных отображений векторного пространства F_2^4 в себя. Существует ли в этой группе элемент порядка 5?

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся по итогам обучения

Перечень контрольных вопросов:

1. Найдите количество элементов порядка 16 в циклической группе порядка 96.
2. Порядок элемента g группы G равен 104. Чему равен порядок элемента g^{39} ?
3. Постройте циклическую группу, в которой уравнение $x^{14} = e$ имеет 7 решений.
4. Найдите наименьший порядок группы G , содержащей по крайней мере пять элементов порядка 12.

5. Существует ли подгруппа группы \mathbb{Z} , изоморфная \mathbb{Z}^2 ?
6. Числа $1/2$ и 2 принадлежат одному смежному классу по подгруппе G группы $(\mathbb{Q}, +)$ ненулевых рациональных чисел относительно умножения. Докажите, что 4 и $1/16$ также принадлежат одному смежному классу по G .
7. Может ли так быть, что элементы x и y группы G принадлежат одному левому классу смежности по подгруппе H , а элементы x^5 и y^5 принадлежат разным классам смежности по H ?
8. Пусть H — такая нормальная подгруппа группы G , что факторгруппа G/H коммутативна. Докажите, что для любых $x, y \in G$ выполняется $x^{-1}yxy^{-1}xy^{-1}x^{-1}y \in H$.
9. \mathbb{C}^* — группа ненулевых комплексных чисел по умножению. Докажите, что в \mathbb{C}^* есть ровно одна подгруппа порядка 8 . Обозначим эту подгруппу через U_8 . Верно ли, что $\mathbb{C}^* \mathbb{C}^* U_8$?
10. Укажите четную перестановку порядка 6 в группе перестановок S_8 .
11. Приведите пример перестановки на 11 элементах, порядок которой равен 12 и которая не имеет неподвижных точек (ни один элемент не переходит в себя).
12. Укажите две несопряженные изоморфные подгруппы порядка 12 в группе S_{11} перестановок 11 элементов.
13. Группа перестановок S_n состоит из перестановок множества $\{0, 1, \dots, n-1\}$. Пусть G — множество перестановок из S_{11} , которые четные числа переводят в четные.
а) Проверьте, что G — подгруппа группы S_{11} . б) Найдите максимальный порядок элементов G .
14. Существует ли в S_{25} подгруппа порядка 1000 ?
15. Порождают ли перестановки порядка 17 группу S_{17} ?
16. Сколько подгрупп порядка 3 содержит группа S_6 ?
17. Чему равен индекс подгруппы в S_8 , порожденной перестановками $(12)(34)(5678)$ и $(12)(34)(56)$?
18. В подгруппе H группы перестановок S_{37} содержится 48 четных перестановок. Укажите возможные значения порядка подгруппы H .
19. Найдите все классы сопряженности, образованные перестановками порядка 28 в группе S_{13} .
20. Порядки элементов x и y в группе G равны 20 и 15 соответственно. Найдите порядок элемента yx^2y^{-1} .

21. Пусть H — нормальная подгруппа группы G , индекс H в G равен 28, а порядок элемента $x \in G$ равен 15. Принадлежит ли x подгруппе H ? Если ответ «да», то объясните, почему. Если ответ «нет» — приведите пример.
22. Пусть G — группа. Нормализатор $N(a)$ элемента $a \in G$ — это множество $\{g \in G : ag = ga\}$. Найдите нормализатор $(12345678) \in S_8$.
23. Пусть $\varphi: (\mathbb{Q}, +) \rightarrow \mathbb{Z}^2$ — гомоморфизм групп. Найдите возможные значения $\varphi(1/2)$.
24. Пусть $\varphi: G_1 \rightarrow G_1$ — инъективный гомоморфизм групп. Про элементы x, y известно, что они принадлежат одному классу смежности по ядру φ . Следует ли из этого, что $x = y$?
25. Постройте инъективный гомоморфизм $C_{42} \rightarrow S_{12}$.
26. Приведите пример таких гомоморфизмов групп $\varphi: C_{15} \rightarrow G, \psi: C_{15} \rightarrow G$, что $\text{Ker} \varphi = \text{Ker} \psi$, а $\text{Im} \varphi \neq \text{Im} \psi$. (C_n — циклическая группа порядка n .)
27. Элементы вида $a^4, a \in (\mathbb{Z}(41))^*$, образуют подгруппу $G < (\mathbb{Z}(41))^* ((\mathbb{Z}(41))^*)^*$ — мультипликативная группа кольца вычетов $\mathbb{Z}(41)$. Существует ли гомоморфизм G в циклическую группу C_{28} , который переводит класс вычетов, содержащий 16, в элемент 14?
28. Существует ли автоморфизм группы $C_7 \wr C_7$, который переводит (a, a) в (a^6, a^7) (a — порождающий элемент C_7)?
29. Существует ли автоморфизм циклической группы порядка 48 с порождающим элементом a , который переводит a^{14} в a^{16} ?
30. Приведите пример таких неизоморфных групп G_1 и G_2 , что для каждой из них существует сюръективный гомоморфизм на группу C_7 , ядро которого изоморфно C_7 . (C_n — циклическая группа порядка n .)
31. Пусть $G = (\mathbb{Q}, +)$ — группа рациональных чисел по сложению, $G_1 = G/\langle 1 \rangle, G_2 = G/\langle 1/2 \rangle$. Изоморфны ли группы G_1 и G_2 ? ($\langle a \rangle$ обозначает подгруппу, порожденную a .)
32. Постройте некоммутативную группу порядка 21.
33. Найдите 9^{-1} в кольце $\mathbb{Z}(110)$.
34. Постройте кольцо из 21 элемента, в котором произведения принимают ровно 3 различных значения.
35. Многочлены $x^2 - 2$ и $x^2 + 3x - 1$ принадлежат идеалу I кольца многочленов $\mathbb{Q}[x]$. Верно ли, что многочлен $x^3 - 1$ также принадлежит I ?

36. Найдите количество собственных идеалов в кольце $\mathbb{Z}(900)$. (Идеал собственный, если он не совпадает со всем кольцом и не равен (0) .)
37. Верно ли, что всякий собственный идеал в кольце вычетов целых чисел по модулю 10000 является максимальным?
38. Сколько решений имеет уравнение $x^6 = 1$ в кольце $F_{17}[x]/(x^2 - x + 4)$?
39. Образуют ли подкольцо делители нуля в кольце $F_7[x]/(x^2 + x + 2)$?
40. Найдите порядок класса вычетов, содержащего многочлен x^{81} , в мультипликативной группе кольца $F[x]/((x + 1)^{81})$.
41. Существует ли такой гомоморфизм колец $\varphi: F_{121} \rightarrow F_{11} \oplus F_{11}$, что $(2, 2)$ принадлежит образу этого гомоморфизма?
42. Найдите все гомоморфизмы кольца вычетов $\mathbb{Z}(120)$ в кольцо многочленов $F_5[x]$.
43. Изоморфны ли кольца $\mathbb{Z}(81)$ и $F_3[x]/(x^4)$?
44. Изоморфны ли кольца $F_{13}[x]/(x^4 - 1)$ и $F_{13}[x]/(x^4 + 1)$?
45. Разложите на неприводимые множители в кольце $F_4[x]$ многочлен $x^{12} - 1$.
46. Сколько обратимых элементов в кольце $F_{37}[x]/(x^2 + 3)$?
47. Сколько различных решений имеет уравнение $1 + x^4 + x^{24} = 0$ в поле F_{125} из 125 элементов?
48. Сколько различных значений принимает многочлен x^{12} в поле из 121 элемента?
49. Элемент a порождает мультипликативную группу поля F из 343 элементов. Является ли многочлен $x^2 + ax + a + 2a^2 \in F[x]$ неприводимым?
50. Верно ли что класс вычетов, содержащий многочлен $x^3 + 1$, принадлежит лишь конечному числу идеалов кольца вычетов $F_5[x]/(x^{15} + 1)$?
51. Многочлен $x^{48} - 1$ раскладывается на линейные множители в конечном поле F характеристики 5. Верно ли, что в поле F больше 1000 элементов?
52. Найдите количество нильпотентных элементов в кольце $F_5[x]/(x^{10} + x^5 - 1)$.
53. Постройте изоморфизм между кольцами $F_{43}[x]/(x^2 + x - 12)$ и $F_{43}[x]/(x^2 + 37)$.
54. Постройте неприводимый многочлен степени 2 над полем из 4 элементов.
55. Существует ли сюръективный гомоморфизм кольца $\mathbb{C}[x]$ на кольцо $\mathbb{Q}[x]$?

56. Существует ли такой неприводимый многочлен $f(x)$ в кольце $F_7[x]$, что в некотором поле характеристики 7 существуют два корня a, b этого многочлена, для которых выполняется условие $a + b = 1$?
57. Решите уравнение $x^2 + x - 1 = 0$ в кольце $F_7[t]/(t^2 + 1)$.
58. Пусть $\varphi: F_9 \rightarrow F_3[x]$ — гомоморфизм колец. Найдите возможные значения $\varphi(-1)$.
59. Многочлен $x^{48} - 1$ раскладывается на линейные множители в конечном поле F характеристики 5. Верно ли, что в поле F больше 2014 элементов?
60. Может ли так быть, что элементы x и y группы G принадлежат одному классу смежности по нормальной подгруппе H , а элементы x^5 и y^5 принадлежат разным классам смежности по H ?
61. Пусть $\varphi: G_1 \rightarrow G_1$ — сюръективный гомоморфизм групп. Про элементы x, y известно, что они принадлежат одному классу смежности по ядру φ . Следует ли из этого, что $x = y$?
62. Решите уравнение $x^2 = 1$ в кольце $\mathbb{Z}(143)$.
63. Существуют ли ненулевые нильпотентные элементы в кольце $F_4[x]/(x^2 + 1)$?
64. Пусть $\alpha \in F_{16}$ — корень неприводимого многочлена $f \in F_2[x]$ степени 4. Докажите, что тогда α^5 является корнем многочлена $g \in F_2[x]$ степени 2.
65. Укажите в мультипликативной группе кольца $\mathbb{Z}(77)$ элемент порядка 30.
66. Решите уравнение $19x = 2$ в поле F_{169} .
67. Пусть a — класс вычетов, содержащий число 8 в кольце вычетов $\mathbb{Z}(144)$, b — класс вычетов, содержащий 56. Верно ли, что a содержится в идеале, порожденном b ?
68. Существует ли автоморфизм кольца $F_{11}[x]$, который переводит многочлен $x^2 - 1$ в многочлен $x^2 + 1$?
69. Пусть a — порождающий мультипликативной группы поля F_{32} . Найдите наименьшую степень многочлена из $F_2[x]$, корнями которого являются a^3, a^9, a^{15} .
70. Содержит ли кольцо $F_{121}[x]/((x-1)(x-2)(x-3)\dots(x-13)(x-14))$ ненулевые нильпотентные элементы? Если да, укажите один из них.
71. Укажите степени неприводимых делителей многочлена $x^7 - 3 \in F_{47}[x]$.
72. Остаток от деления многочлена $f(x) \in \mathbb{Q}[x]$ на $(x - 1)^2$ равен 1, остаток от деления на $(x + 1)^2$ равен 1, остаток от деления на $(x - 2)^2$ равен 4. Найдите остаток от деления $f(x)$ на $(x - 1)(x + 1)(x - 2)$.

73. Минимальный многочлен элемента $a \in F_4$ равен $x^2 + x + 1$. Является ли неприводимым в кольце $F_4[x]$ многочлен $x^3 + ax + 1$?
74. Сколько обратимых элементов в кольце $\mathbb{Z}/(552)$?
75. Может ли пересечение двух различных максимальных идеалов евклидова кольца содержать простой элемент? Если ответ «да», приведите пример. Если ответ «нет», докажите это утверждение.
76. Изоморфны ли кольца $F_{13}[x]/(x^2 - 1)$ и $F_{13}[x]/(x^2 + 1)$?
77. Многочлены $x^2 + 3$ и $x^4 + 4$ принадлежат собственному идеалу I кольца $F[x]$, где F — некоторое поле. Докажите, что многочлен $x^3 - 10x$ также принадлежит идеалу I .
78. Найдите количество неприводимых многочленов степени 3 в кольце многочленов $F_{25}[x]$.
79. Найдите количество собственных идеалов в кольце $F[x]/(x^9 - x^3 + 1)$.
80. Известно, что наибольший общий делитель элементов a^2bc и ab^2c евклидова кольца равен abc . Следует ли из этого, что уравнение $ax + by = 1$, $x, y \in R$, имеет решение?
81. Пусть идеал I_1 порожден в $Q[x]$ многочленом $x^2 - x$, а идеал I_2 порожден многочленом $x^2 + x$. Найдите $I_1 \cap I_2$.
82. Найдите количество идеалов в поле F_{27} и в кольце $F_3 \oplus F_3 \oplus F_3$.
83. Сколько решений имеет уравнение $x^{4+x+1} = 0$ в поле из 512 элементов?
84. Является ли неприводимым над полем F_9 многочлен $x^{12} - x^9 + 1$?

Примеры задач:

- Идеал J в кольце R называется простым, если кольцо R/J не содержит делителей нуля. Является ли простым идеал, порожденный элементами 351 и 468 в кольце целых чисел?
- Укажите какое-нибудь решение уравнения $x(23)(456) = (1435)(26)x$ в группе S_6 или объясните, почему решений не существует.
- Найдите обратный к (а) элементу, содержащему 131, в кольце $\mathbb{Z}/(20)$; (б) элементу, содержащему $x^5 - x^2 + x$, в кольце $\mathbb{Q}[x]/(x^4 + 1)$.
- Существует ли в группе $(\mathbb{Q} \setminus \{0\}, \cdot)$ подгруппа, изоморфная \mathbb{Z}^2 ?
- Известно, что x и y — элементы группы G , которые принадлежат одному классу смежности по нормальной подгруппе H ; элементы u и v также принадлежат одному классу смежности по H . Следует ли из этого, что $xuv^{-1}y^{-1}$ принадлежит H ?

6. Существует ли автоморфизм группы C_{52} остатков от деления на 52 с операцией сложения, который переводит остаток 20 в остаток 16?
7. Про многочлен $f(x) \in F_{11}[x]$ известно, что $f(x)^{12} - 1$ делится на $x^2 + x - 1$. Найдите возможные значения остатка от деления $f(x)$ на $x^2 + x - 1$.
8. Пусть a — порождающий элемент мультипликативной группы поля F_{729} . Существует ли многочлен третьей степени в $F_3[x]$, корнем которого является $a^{56} - a^{84}$?

Примеры билетов:

Билет №1

1. Кольца. Примеры колец. Кольцо целых чисел. Кольцо многочленов над кольцом (полем).
2. Задача.

Билет №2

1. Левые, правые и двусторонние идеалы. Главные идеалы. Максимальные и простые идеалы.
2. Задача.