

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета

Нестеров П.Н.

23 мая 2023 г.

Рабочая программа дисциплины

Общая алгебра

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 18.04.2023, протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 03.05.2023

1. Цели освоения дисциплины

Целью освоения дисциплины «Общая алгебра» является ознакомление студентов с подходом, основными понятиями, результатами и методами доказательств в современной абстрактной алгебре на примере теории полугрупп, групп, колец, полей и модулей.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Общая алгебра» относится к вариативной части образовательной программы и является дисциплиной по выбору. Она продолжает и базируется на знаниях, полученных студентами в ходе освоения дисциплин «Алгебра», «Линейная алгебра», «Избранные вопросы алгебры», «Алгебраическая алгоритмика».

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Перечень планируемых результатов обучения
Общепрофессиональные компетенции	
ОПК-2 Обладает способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Знать: - основные понятия и результаты теории групп, колец, модулей и алгебр. Уметь: - применять алгебраические знания в конкретной ситуации. Владеть навыками: - вычислений в конечных полях, матричных кольцах, группах подстановок, группах и алгебрах, заданных образующими и соотношениями.
Профессиональные компетенции	
ПК-2 Обладает способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	Знать: - основные понятия и результаты дисциплины. Уметь: - распознавать структуры алгебры в различных ситуациях. Владеть навыками: - устного и письменного логически строгого и корректного изложения научной информации: формулирование задач, описание применяемых средств и методов, изложение подхода к решению и полученных результатов.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 акад. часа.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1.	Алгебраические системы. Множества и операции.	7	2	2		2		4	
2.	Полугруппы и группы	7	8	8		2		10	Задания для самосто- ятельной работы
3.	Представления групп	7	6	6		3		10	Контрольная работа 1
							0,3	8,7	Зачет
	Всего за 7 семестр 72 акад. часа		16	16		7	0,3	32,7	
4.	Кольца и идеалы	8	10	10				2	Задания для самосто- ятельной работы Контрольная работа 2
5.	Модули и алгебры	8	6	6				2	Задания для самосто- ятельной работы
						2	0,5	33,5	Экзамен
	Всего за 8 семестр 72 акад. часа		16	16		2	0,5	37,5	
	ИТОГО		32	32		9	0.8	70,2	

Содержание разделов дисциплины:

1. Алгебраические системы. Множества и операции.

Множества, операции, арности. Общее представление об универсальной алгебре. Гомоморфизмы, изоморфизмы, эндоморфизмы и автоморфизмы алгебраических систем.

2. Полугруппы и группы.

Полугруппы и моноиды. Определения, примеры. Гомоморфизмы и изоморфизмы полугрупп и моноидов. Свободные полугруппы и моноиды. Обобщенная ассоциативность в полугруппе. Операции над степенями элемента полугруппы. Конгруэнции в полугруппе. Теорема о гомоморфизме для полугрупп. Обратимые элементы и их основные свойства. Подполугруппы и подмоноиды. Задание полугрупп и моноидов образующими элементами и определяющими соотношениями. Проблемы равенства и изоморфизма для конечно определенных полугрупп и моноидов. Порождающие элементы группы. Свободные группы. Проблема изоморфизма для групп (проблема Дэна). Определяющие соотношения в группе. Задание группы образующими и определяющими соотношениями. Алгоритмические проблемы для конечно определенных групп. Преобразования Титце. Ширина и длина конечной группы относительно заданной системы образующих. Подгруппы, пересечение подгрупп. Подгруппа, порожденная подмножеством элементов группы. Образующие элементы подгруппы. Нормальное замыкание подмножества в группе. Теорема о гомоморфизме и две теоремы об изоморфизмах для групп. Сопряженные элементы. Разложение группы на классы сопряженных элементов. Нормализатор подмножества. Центр группы. Теоремы Силова. Строение конечных и конечно порожденных абелевых групп.

Коммутант группы и его свойства. Простые, разрешимые и нильпотентные группы. Понятие о теоремах Бернсайда и Фейта – Томпсона. Многообразия групп.

3. Представления групп.

Подпредставления, факторпредставления. Неприводимые, приводимые и вполне приводимые представления. Теорема Машке. Лемма Шура. Характеры линейных представлений. Соотношения ортогональности для характеров и разложение представления на неприводимые с их помощью. Регулярное представление. Неприводимые представления конечных групп и их число. Одномерные комплексные представления конечной группы.

4. Кольца и идеалы.

Классы колец. Примеры колец. Кольца $Z[\sqrt{d}]$. Группа обратимых элементов кольца. Кольца вычетов и обратимые элементы в них. Матричные кольца и обратимые элементы в них. Обратимые элементы в кольце формальных степенных рядов от одной переменной над произвольным коммутативным кольцом с единицей. Сумма и пересечение подколец и идеалов. Идеал, порожденный подмножеством. Прямые суммы колец и идеалов. Поля и тела, их простейшие свойства. Тело кватернионов. Поля вычетов. Поле частных целостного кольца. Поле рациональных дробей над полем. Правильные и простейшие рациональные дроби. Разложение правильной рациональной дроби в сумму простейших. Поле $K((x))$ формальных рядов Лорана от одной переменной. Поле частных кольца $K[[x]]$. Подполя. Простое подполе и его связь с характеристикой поля. Гомоморфизмы полей. Изоморфизм $C \cong R[x]/(x^2 + 1)$. Расширения полей. Типы расширений: конечные, алгебраические, трансцендентные, конечно порожденные, простые. Теоремы о башнях для конечных и алгебраических расширений. Описание и изоморфизм простых расширений поля. Вид элементов конечного расширения поля, вычисления в конечном расширении. Символическое присоединение. Построение поля разложения многочлена. Изоморфизм полей разложения многочлена. Алгебраически замкнутые поля. Алгебраическое замыкание поля. Конечные поля: их существование и единственность. Подполя конечного поля. Цикличность мультипликативной группы конечного поля. Цикличность мультипликативной группы кольца вычетов по модулю p^n . Понятие о группе Галуа расширения. Алгебраические аспекты геометрических построений циркулем и линейкой.

5. Модули и алгебры.

Подмодули, фактормодули, гомоморфизмы модулей. Групповые и матричные алгебры. Прямые произведения и прямые суммы модулей. Образующие модуля. Соотношения. Циклические подмодули и модули. Свободные модули. Базис и размерность свободного модуля. Гомоморфизмы свободных модулей. Условия конечности для модулей. Нетеровы и артиновы модули и кольца. Теорема Гильберта о базисе. Теорема Гильберта о нулях (без доказательства) и ее геометрический смысл. Конечномерные алгебры с делением. Теорема Фробениуса.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:
для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используется:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

- Электронная библиотечная система «Лань» <https://e.lanbook.com>

- Электронная библиотечная система «Юрайт» <https://urait.ru>

- Электронная библиотечная система «Консультант студента»

<https://www.studentlibrary.ru>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Кострикин А. И. Введение в алгебру: учебник для вузов.: в 3 ч. Часть 1. - М.: ФИЗМАТЛИТ, 2003. <https://www.studentlibrary.ru/ru/book/ISBN5922101676.html>

2. Кострикин А. И. Введение в алгебру: учебник для вузов.: в 3 ч. Часть 3. - М.: ФИЗМАТЛИТ, 2004. <https://djvu.online/file/sJxPy5ql9dVbj?ysclid=lrghglvnrc238984730>

б) дополнительная литература

1. Р. Зуланке, А. Л. Онищик Алгебра и геометрия: учебник для вузов: в 3 т.. Т. 1, Введение. - М.: МЦНМО, 2004.

2. Р. Зуланке, А. Л. Онищик Алгебра и геометрия: учебник для вузов: в 3 т.. Т. 2, Модули и алгебры. - М.: МЦНМО, 2008.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Доцент кафедры алгебры
и математической логики, к. ф.-м. н.

М. Е. Сорокина

**Приложение № 1 к рабочей программе дисциплины
«Общая алгебра»**

**Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине**

**1. Типовые контрольные задания и иные материалы,
используемые в процессе текущего контроля успеваемости**

**1.1 Контрольные задания и иные материалы,
используемые в процессе текущей аттестации**

Типовые задачи для самостоятельной работы

- Перечислить все классы изоморфизма абелевых групп порядка 200
- Перечислить все гомоморфизмы симметрической группы на n элементах в группу порядка 2
- Найти все подгруппы в группе классов вычетов данного порядка
- Перечислить все образующие в группе классов вычетов данного порядка
- Перечислить все гомоморфизмы группы в группу (группы берутся из класса: группы классов вычетов и их конечные прямые произведения)
- Выяснить, изоморфны ли две данные конечные группы (задача подразумевает сравнение порядков элементов)
- Построить отношение эквивалентности в кольце целых чисел, не согласованное с операцией сложения
- Перечислите все гомоморфизмы кольца Z_{12} в $Z_2 \oplus Z_3$
- Докажите, что ядро гомоморфизма коммутативного кольца с единицей на поле является максимальным идеалом, а факторкольцо коммутативного кольца с единицей по максимальному идеалу является полем.
- Найдите центр матричной алгебры над полем (любым доступным вам способом).
- Найдите следующие степени расширений: $[Q(\sqrt{2}, \sqrt[3]{3}) : Q]$ и $[Q(\sqrt{6}) : Q(\sqrt{2})]$.
- Опишите все подгруппы в группе Z_{12} и все подкольца в одноименном кольце.
- Найдите все эндоморфизмы и автоморфизмы аддитивной группы Z_6
- Найдите группу всех обратимых элементов кольца классов вычетов Z_{12} . Является ли она циклической?
- Перечислите все гомоморфизмы кольца Z_{12} в $Z_2 \oplus Z_3$
- Изоморфны ли группы $Z_{10} \times Z_{12}$ и $Z_6 \times Z_{20}$? Обоснуйте ответ.
- Перечислите все гомоморфизмы кольца Z_8 в $Z_4 \oplus Z_3$

Вариант контрольной работы № 1

1. Найдите все эндоморфизмы и автоморфизмы аддитивной группы Z_6
2. Доказать, что факторгруппа группы ненулевых комплексных чисел по подгруппе ненулевых вещественных чисел изоморфна группе вращений евклидовой плоскости
3. Перечислите все классы неизоморфных между собой абелевых групп порядка 300.

Вариант контрольной работы № 2

1. Найдите следующие степени расширений: $[Q(\sqrt{2}, \sqrt[3]{3}) : Q]$ и $[Q(\sqrt{6}) : Q(\sqrt{2})]$.

2. Опишите все подгруппы в группе Z_{12} и все подкольца в одноименном кольце.
3. Найдите группу всех обратимых элементов кольца классов вычетов Z_{12} . Является ли она циклической?

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Зачет выставляется по результатам контрольной работы № 1 и собеседования по теории.

Круг вопросов для собеседования к зачету

1. Множества, операции, арности. Полугруппы и моноиды. Определения, примеры. Гомоморфизмы и изоморфизмы полугрупп и моноидов. Свободные полугруппы и моноиды. Обобщенная ассоциативность в полугруппе. Операции над степенями элемента полугруппы. Конгруэнции в полугруппе. Теорема о гомоморфизме для полугрупп. Обратимые элементы и их основные свойства. Подполугруппы и подмоноиды. Задание полугрупп и моноидов образующими элементами и определяющими соотношениями. Проблемы равенства и изоморфизма для конечно определенных полугрупп и моноидов.
2. Группы. Примеры абелевых и неабелевых групп. Таблица Кэли группы. Гомоморфизмы и изоморфизмы групп: определения, примеры, основные свойства. Свободные группы. Проблема изоморфизма для групп. Алгоритмические проблемы для конечно определенных групп.
3. Задание группы образующими и определяющими соотношениями. Преобразования Титце. Ширина и длина конечной группы относительно заданной системы образующих.
4. Подгруппы, пересечение подгрупп. Примеры подгрупп. Вложимость конечной группы в подходящую симметрическую группу. Подгруппа, порожденная подмножеством элементов группы. Образующие элементы подгруппы. Смежные классы, теорема Лагранжа. Нормальная подгруппа. Факторгруппа. Нормальное замыкание подмножества в группе. Ядро и образ гомоморфизма групп. Теорема о гомоморфизме. Две теоремы об изоморфизмах для групп.
5. Сопряженные элементы. Разложение группы на классы сопряженных элементов. Нормализатор подмножества. Центр группы.
6. Действие группы на множестве. Орбита и стабилизатор точки. Теорема об орбите и стабилизаторе (лемма Бернсайда). Действия группы на себе сдвигами и сопряжениями.
7. Первая теорема Силова.
8. Вторая теорема Силова.
9. Третья теорема Силова.
10. Строение конечных и конечно порожденных абелевых групп.
11. Коммутант группы и его свойства. Простые, разрешимые и нильпотентные группы. Многообразия групп.
12. Представления групп. Подпредставления, факторпредставления. Неприводимые, приводимые и вполне приводимые представления. Теорема Машке. Лемма Шура. Характеристики линейных представлений. Соотношения ортогональности для характеров и разложение представления на неприводимые с их помощью. Неприводимые представления конечных групп и их число. Одномерные комплексные представления конечной группы.

Экзамен проводится по билетам; в каждом билете 2 вопроса. Студенту могут быть заданы дополнительные вопросы в рамках вопросов билета или программы, с целью выявить уровень понимания материала, и/или негромоздкая задача.

Список вопросов экзамена

1. Кольца. Основные классы колец. Примеры колец. Кольцо целых чисел, полиномиальные кольца, кольцо формальных степенных рядов. Кольцо целых гауссовых чисел и кольца $Z[\sqrt{d}]$.
2. Группа обратимых элементов кольца. Кольца вычетов и обратимые элементы в них. Матричные кольца и обратимые элементы в них. Обратимые элементы в кольце формальных степенных рядов от одной переменной над произвольным коммутативным кольцом с единицей.
3. Гомоморфизмы и изоморфизмы колец. Подкольца, идеалы и факторкольца. Делители нуля и области целостности. Теорема о гомоморфизме для колец.
4. Главные идеалы. Кольца главных идеалов. Примеры колец, в которых не все идеалы главные.
5. Сумма и пересечение подколец и идеалов. Идеал, порожденный подмножеством.
6. Прямые суммы колец и идеалов. Разложение кольца вычетов в прямую сумму примарных колец.
7. Поле частных целостного кольца. Поле рациональных дробей. Правильные и простейшие рациональные дроби. Разложение правильной рациональной дроби в сумму простейших.
8. Теория делимости в областях целостности. Обратимые, неразложимые и простые элементы в целостном кольце.
9. Кольца главных идеалов. Евклидовы кольца.
10. Обратимые, неразложимые и простые элементы в кольце $K[[x]]$.
11. Факториальные кольца.
12. Поля и тела, их простейшие свойства. Тело кватернионов. Поля вычетов.
13. Подполя. Простое подполе и его связь с характеристикой поля.
14. Гомоморфизм и изоморфизм полей. Изоморфизм $C \cong R[x]/(x^2 + 1)$.
15. Расширения полей. Типы расширений: конечные, алгебраические, трансцендентные, конечно порожденные, простые.
16. Теоремы о башнях для конечных и алгебраических расширений.
17. Символическое присоединение. Вид элементов конечного расширения поля, вычисления в конечном расширении.
18. Алгебраически замкнутые поля. Алгебраическое замыкание поля.
19. Поля Галуа: их существование и единственность. Подполя конечного поля. Цикличность мультипликативной группы конечного поля. Цикличность мультипликативной группы кольца вычетов по модулю p^n .
20. Конечномерные вещественные алгебры с делением. Теорема Фробениуса.
21. Модули, подмодули, фактормодули, гомоморфизмы модулей.
22. Прямые произведения и прямые суммы модулей. Образующие модуля. Соотношения. Циклические подмодули и модули.
23. Свободные модули. Базис и размерность свободного модуля. Гомоморфизмы свободных модулей. Представление модуля.
24. Условия конечности для модулей. Нетеровы и артиновы модули и кольца.
25. Теорема Гильберта о базисе. Эквивалентность бесконечных систем уравнений своим конечным подсистемам. Теорема Гильберта о нулях.

Задания для самопроверки при подготовке к промежуточной аттестации

1 семестр

1. Изоморфны ли группы $Z_{10} \times Z_{12}$ и $Z_6 \times Z_{20}$? Обоснуйте ответ.
2. Найдите группу всех обратимых элементов кольца классов вычетов Z_{12} . Является ли она циклической?
3. Являются ли группами следующие множества: А) целые числа по сложению, Б) целые числа по умножению, В) невырожденные вещественные матрицы по умножению?

4. Перечислите все подгруппы группы Z_6 .
5. Перечислите все нормальные подгруппы группы перестановок трех элементов.

2 семестр

1. Найдите степень поля комплексных чисел как расширения поля вещественных чисел.
2. Укажите размерность и базис алгебры кватернионов как вещественной алгебры.
3. Найдите все обратимые элементы кольца целых гауссовых чисел $Z[i]$.
4. Укажите характеристики следующих колец: А) Z (кольцо целых чисел) Б) $GF(256)$ В) Z_5 .
5. Найдите НОД $(16 + i, 3 - 2i)$ в кольце целых гауссовых чисел $Z[i]$.

Ответы: 1. Да; обе группы изоморфны $Z_2 \times Z_4 \times Z_3 \times Z_5$; 2. $\{1,5,7,11\}$ нециклическая; 3. А) Да, Б) нет, В) да; 4. $\{0\}$, $\{0,2,4\}$, $\{0,3\}$, $\{0,1,2,3,4,5\}$; 5) $\{(1)\}$, $\langle(123)\rangle$, вся группа; 6. 2; 7. 4, базис состоит из $1, i, j, k$; 8) $1, -1, i, -i$; 9) А) 0, Б) 2, В) 5; 10) i .

Каждой задаче присвоено 3 балла. В задачах с пунктами А), Б), В) правильный ответ по каждому пункту дает 1 балл. В задаче 1 результат -1 балл, результат с обоснованием -3 балла. В задаче 2 перечисление обратимых элементов – 1 балл, цикличность – 2 балла. В задачах 4 и 5 полный список – 3 балла, часть списка – 1 балл. В задаче 7 размерность – 1 балл, указание базиса – 2 балла, размерность и базис – 3 балла. В задаче 8 полный список – 3 балла, часть списка – 1 балл. В задаче 10 частичная реализация алгоритма Евклида – 1 балл, полная реализация с ошибкой в вычислении – 2 балла, верная реализация – 3 балла.

По семестрам: «Удовлетворительно» (= «Зачтено») – 8-10 баллов, «Хорошо» – 11-13 баллов, «Отлично» – 14-15 баллов.

Полностью: «Удовлетворительно» – 15-20 баллов, «Хорошо» – 21-26 баллов, «Отлично» – 27- 30 баллов.

Приложение № 2 к рабочей программе дисциплины «Общая алгебра»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Общая алгебра» являются лекции; по всем темам предусмотрены практические занятия, на которых происходит закрепление лекционного материала путем применения его к конкретным задачам и отработка навыков работы с математическим аппаратом.

Для успешного освоения дисциплины очень важно решение достаточно большого количества задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия и основные методы дисциплины.

Задания для самостоятельного решения формулируются на лекциях и практических занятиях. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач.

В конце изучения дисциплины студенты сдают зачет (7 семестр) и экзамен (8 семестр). Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса и задачу. На самостоятельную подготовку к экзамену выделяется 3 дня, в это время предусмотрена и групповая консультация.