

**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**

**Теория групп**

Направление подготовки (специальности)  
02.03.01 Математика и компьютерные науки

Направленность (профиль)  
«Программирование, алгоритмы и анализ данных»

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

Целями освоения дисциплины «Теория групп» являются: обеспечение подготовки в одной из важных областей математики и ее приложений, знакомство с современными понятиями теории обыкновенных линейных представлений конечных групп и ассоциативных алгебр. Математический аппарат теории групп используется во многих разделах математики и физики, причем сфера его приложений все время расширяется. Более того, будучи относительно законченной, данная теория служит образцом для других алгебраических систем –компактных групп, групп Ли и теории сложности вычислений.

## 2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, и является элективной дисциплиной. Данная дисциплина направлена на освоение алгоритмов, применяемых для анализа представлений конечных групп и ассоциативных алгебр. Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения предшествующих математических дисциплин: теории чисел, линейной алгебры, аналитической геометрии.

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

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

| Формируемая компетенция<br>(код и формулировка)   | Индикатор достижения компетенции<br>(код и формулировка)  | Перечень планируемых результатов обучения  |
|---|---|--|
| <b>Профессиональные компетенции</b>   |   |  |
| <b>ПК-1</b><br>Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий | <b>И-ПК-1.1</b><br>Обладает базовыми знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий | <b>Знать:</b><br>основные методы и формулировки результатов, использующихся в защите информации  |
|   | <b>И-ПК-1.2</b><br>Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в математике и информатике | <b>Уметь:</b><br>обосновывать алгоритмы защиты информации<br><b>Владеть:</b><br>навыками быстрых вычислений в основных алгебраических системах |

## 4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 акад. часов.

| №<br>п/п | Темы (разделы)<br>дисциплины,<br>их содержание   | Семестр | Виды учебных занятий,<br>включая самостоятельную<br>работу студентов,<br>и их трудоемкость<br>(в академических часах) |              |              |              |                             |                           | Формы текущего<br>контроля успеваемости<br><br>Форма промежуточной<br>аттестации<br>(по семестрам) |
|----------|--|---------|---|--------------|--------------|--------------|-----------------------------|---------------------------|--|
|          |  |         | Контактная работа   |              |              |              |                             | самостоятельная<br>работа |  |
|          |  |         | лекции  | практические | лабораторные | консультации | аттестационные<br>испытания |                           |  |
| 1        | Теорема Лагранжа. Действие группы на множестве. Нормализатор и стабилизатор точки. Теоремы Силова и их следствия. Группы малых порядков      | 3       | 5   | 5            |              | 1            |                             | 10                        | Задания для самостоятельной работы. Контрольная работа   |
| 2        | Прямые произведения групп. Абелевы группы. Двойные смежные классы. Нормальные подгруппы и факторгруппы                                       | 3       | 5   | 5            |              | 1            |                             | 10                        | Задания для самостоятельной работы   |
| 3        | Аutomорфизмы и полупрямые произведения. Применения к теории представлений и комбинаторике, быстрым вычисления. Китайская теорема об остатках | 3       | 6   | 6            |              | 2            |                             | 10                        | Задания для самостоятельно работы  |
|          |  |         |   |              |              |              | 0,3                         | 5,7                       | зачет  |
|          | Всего  |         | 16  | 16           |              | 4            | 0,3                         | 35,7                      |  |

## 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 информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).**

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;
- MikTeX (свободно распространяемое ПО);
- GAP (GNU GPL).

**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 используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»  
[http://www.lib.uniyl.ac.ru/opac/bk\\_cat\\_find.php](http://www.lib.uniyl.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. Часть III. Основные структуры алгебры, М: Физматлит, 2001
2. Глухов М. М. Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии: учебное пособие для вузов. / М. М. Глухов, И. А. Круглов; УМО по образованию в обл. информационной безопасности - СПб.: Лань, 2015. - 174 с.
3. Ноден П. Алгебраическая алгоритмика: с упражнениями и решениями.: учебник для вузов. / П. Ноден, К. Китте; пер. с фр. В. А. Соколова; под ред. Л. С. Казарина; Науч.-метод. совет по прикладной математике УМО ун-тов - М.: Мир, 1999. - 719 с.
4. Белоногов В. А. Задачник по теории групп. / В. А.Белоногов; М-во образования РФ - М.: Наука, 2000. - 239с.

**б) дополнительная литература**

1. Струнков С.П. Введение в теорию представлений конечных групп. М: МИФИ, 1999
2. Глухов М.М., Круглов И.А. Элементы теории обыкновенных представлений и характеров с приложениями в криптографии. Лань: Сп-б, 2015

3. Хамермеш М. Теория групп и ее применения к физическим проблемам, Ленанд, 2015

4. Курош А. Г. Теория групп - Москва: ФИЗМАТЛИТ, 2011.

<https://www.studentlibrary.ru/ru/doc/ISBN9785922113496-SCN0000/000.html>

**в) ресурсы сети «Интернет»**

1. <http://mech.math.msu.su/department/>

2. <http://www.tc26.ru>

3. [http://www.nist.gov/manuscript-publication-search.cfm?pub\\_id=919061](http://www.nist.gov/manuscript-publication-search.cfm?pub_id=919061)

4. <http://habrahabr.ru/post/210684/>

5. [http://www.nist.gov/customcf/get\\_pdf.cfm?pub\\_id=919061](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=919061)

6. <http://www.streebog.info/news/opredeleny-pobediteli-konkursa-po-issledovaniyu-khesh-funksii-stribog/>

**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;
- групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
- учебные аудитории для проведения практических занятий (семинаров);
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания оборудования.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

**Автор(ы) :**

Заведующий кафедрой алгебры и математической логики  
профессор, д.ф-м.н.

Казарин Л.С

**Приложение к №1 рабочей программе дисциплины  
«Теория групп»**

**Оценочные средства  
для проведения текущей и/или промежуточной аттестации аспирантов  
по дисциплине**

**1. Типовые контрольные задания или иные материалы,  
необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,  
характеризующих этапы формирования компетенций**

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

**Задания для самостоятельной работы по теме 1**

По задачку Белоногов В.А. Задачник по теории групп. М.Наука, 2000, § 22, задачи из подпунктов 22.1 – 22.19, .

По книге .Кострикина А.И. «Введение в алгебру. Часть III. Основные структуры алгебры», гл.3, §3 и , §4, гл.4, §4

**Задания для самостоятельной работы по теме 2**

По задачку Белоногов В.А. Задачник по теории групп. М.Наука, 2000, , § 22, задачи из подпунктов 22.21 – 22.42, 22.45 – 22.58, .

По книге .Кострикина А.И. «Введение в алгебру. Часть III. Основные структуры алгебры», гл.3, §6 и , §7, гл

**Задания для самостоятельной работы по теме 3**

По книге Ноден П., Китте К. «Алгебраическая алгоритмика», гл.V, упражнения 29 – 36

По книге .Кострикина А.И. «Введение в алгебру. Часть III. Основные структуры алгебры», гл.3, §3 и , §4

**Контрольная работа**

1. Вычислить таблицу подгруппы знакопеременной группы степени 5..
2. Найти формулы для свертки двух многочленов степени 5, используя дискретное преобразование Фурье в конечном поле (в зависимости от значений коэффициентов).
3. Верно ли, что любое точное двумерное представление конечной группы над  $\mathbb{C}$  неприводимо?
4. Пусть  $H$  – подгруппа группы  $G$  индекса 2. Доказать, что она нормальна.
5. Найти все подгруппы группы, являющейся прямым произведением двух групп кватернионов порядка 8.

**Тест для самопроверки по результатам освоения дисциплины**

**1. Группа порядка 36 действует на некотором множестве. Орбиты каких длин возможны?**

- А) 1,2,4,  
Б) 1,3,9,  
В) 1,2,3,4,6,9,12,18,36  
Г) длин, не являющихся делителями 36.

**2. Перечислите число и гомоморфизмы группы кватернионов  $Q_8$**

- А) 5 представлений степеней 1,1,1,1,2

Б) 2 представления степеней 2 и 2

В) 3 представления степени 2

Г) 2 представления степени 3

**3. Регулярное представление конечной нетривиальной группы**

А) имеет степень, равную порядку группы, и неприводимо

Б) имеет степень, равную порядку группы, и всегда приводимо

В) имеет степень, равную 1.

**4. Неприводимые неэквивалентные представления абелевой группы порядка 12**

А) имеют степени 1,2,3,4,12,

Б) имеют степень 1, их 12 штук,

В) имеют степень 1, их 5 штук.

| Вопрос № | Правильный ответ |
|----------|------------------|
| 1        | В                |
| 2        | А                |
| 3        | Б                |
| 4        | Б                |

**Оценка сформированности компетенций**

| Компетенции | Номера вопросов | Уровень формирования | Количество правильных ответов, критерии |
|-------------|-----------------|----------------------|---|
| ПК-2        | 1-4             | Пороговый            | Не менее 2                              |
|             |                 | Продвинутый          | Не менее 3                              |
|             |                 | Высокий              | Не менее 4                              |

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

**Список вопросов к зачету:**

1. Представление группы. Приводимые и неприводимые представления.
2. Центр группы и коммутант.
3. Теорема Лагранжа
4. Малая теорема Ферма.
5. Теорема Эйлера.
6. Конечные абелевы группы.
7. Циклическая свертка и ДПФ.
8. Поле алгебраических чисел.
9. Нормализатор и централизатор.
10. Теоремы Силова.
11. Перечислительная лемма Бернсайда.
12. Теорема Казарина –Бернсайда (без доказательства).
13. Нормальные подгруппы и гомоморфизмы. Определение и примеры.
14. Применения теории групп к физическим задачам.
15. Действие группы на множестве. Орбиты и стабилизаторы.
16. Применение ДПФ к быстрым вычислениям.
17. Обработка сигналов и теория групп.
18. Автоморфизмы и полупрямые произведения.
19. Теорема Ландау.