

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

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета

\_\_\_\_\_  
Нестеров П.Н.

18 мая 2021 г.

**Рабочая программа дисциплины**

**Избранные вопросы алгебры**

Направление подготовки (специальности)  
10.05.01 Компьютерная безопасность

Направленность (профиль)  
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена  
на заседании кафедры  
от 16.04.2021, протокол № 8

Программа одобрена НМК  
математического факультета  
протокол № 5 от 18.05.2021

## 1. Цели освоения дисциплины

Целью освоения данной дисциплины является ознакомление слушателей с основными понятиями и результатами абстрактной алгебры. Данный курс вырабатывает у студентов навыки распознавания структур и использования понятий и результатов современной алгебры в конкретных математических задачах.

## 2. Место дисциплины в структуре образовательной программы

Дисциплина «Избранные вопросы алгебры» относится к базовой части образовательной программы.

Для освоения данной дисциплиной студенты должны обладать начальной алгебро-геометрической подготовкой, полученной в ходе освоения курсов «Алгебра» и «Геометрия».

Знания, полученные в курсе «Избранные вопросы алгебры», необходимы для изучения последующих математических дисциплин и дисциплин информационно-технологической направленности.

## 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<br>(код и формулировка)  | Перечень<br>планируемых результатов обучения  |
|--|---|
| <b>Общепрофессиональные компетенции</b>  |   |
| <b>ОПК-2</b><br>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 | <b>Знать:</b><br>- основные понятия теории алгебраических систем, понятия, результаты и методы теории полугрупп, групп и колец<br><b>Уметь:</b><br>- применять алгебраические знания в конкретной ситуации<br><b>Владеть:</b><br>- навыками вычислений в конкретных алгебраических системах   |
| <b>Профессиональные компетенции</b>  |   |
| <b>ПК-2</b><br>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  | <b>Знать:</b><br>- основные алгебраические понятия и возможности их применения для анализа моделей механизмов защиты информации<br><b>Уметь:</b><br>- проводить доказательства соответствия механизмов защиты информации выбранным моделям<br><b>Владеть:</b><br>- навыками анализа математических моделей механизмов защиты информации |

#### 4. Объем, структура и содержание дисциплины

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

| №<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             |  |
|----------|--|---------|---|--------------|--------------|--------------|-----------------------------|---------------------------|---|--|
|          |  |         | Контактная работа   |              |              |              |                             | самостоятельная<br>работа | Форма промежуточной<br>аттестации<br>(по семестрам) |  |
|          |  |         | лекции  | практические | лабораторные | консультации | аттестационные<br>испытания |                           |   |  |
| 1        | Множества и операции                           | 3       | 2   | 2            |              |              |                             |                           |   |  |
| 2        | Группы   | 3       | 8   | 8            |              |              |                             | 2                         | Дом. контр. работа 1                                |  |
| 3        | Кольца   | 3       | 6   | 6            |              |              |                             | 2                         | Дом. контр. работа 2                                |  |
|          |  |         |   |              |              | 2            | 0,5                         | 33,5                      | экзамен   |  |
|          | ИТОГО  |         | 16  | 16           |              | 2            | 0,5                         | 37,5                      |   |  |

#### Содержание разделов дисциплины:

##### Тема 1. Множества и операции.

Арности. Полугруппа. Моноид. Эквивалентность. Эквивалентность, согласованная с операцией. Гомоморфизм алгебраических систем. Гомоморфизм полугрупп. Ядро гомоморфизма полугрупп. Теорема о гомоморфизме для полугрупп.

##### Тема 2. Группы.

Абелевы и неабелевы группы, примеры. Симметрические группы, группы симметрий правильных многоугольников. Группы классов вычетов. Представление об образующих и соотношениях (пример). Подгруппа, смежные классы, теорема Лагранжа. Действие группы, примеры действий и лемма об орбите и стабилизаторе. Гомоморфизм групп. Изоморфизм групп. Нормальная подгруппа. Факторгруппа. Ядро, образ гомоморфизма групп и теорема о гомоморфизме для групп. Теоремы об изоморфизме для групп. Циклические группы.

##### Тема 3. Кольца.

Понятие кольца, примеры колец. Коммутативные и некоммутативные, ассоциативные и неассоциативные кольца. Кольца с единицей, обратимые элементы кольца. Примеры. Подкольцо, идеал. Факторкольцо. Гомоморфизм колец. Ядро и образ гомоморфизма колец. Теорема о гомоморфизме для колец. Характеристика кольца. Делители нуля в кольцах. Области целостности. Характеристика области целостности. Главные идеалы и кольца главных идеалов. Примеры. Евклидовы кольца. Примеры. Алгоритм Евклида в евклидовом кольце. Понятие о кольцах с разложением и о факториальных кольцах. Понятие поля. Примеры полей.

#### 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:

**Вводная лекция** – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, место предметной области в теории и приложениях математики и в истории математики. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

**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, стимулировать интерес и расставлять акценты, 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. На практическом занятии проводится также разбор вызвавших затруднение задач из заданий для самостоятельной работы.

**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 используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

[http://www.lib.uniyar.ac.ru/opac/bk\\_cat\\_find.php](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. Тимофеева Н. В. Алгебраические структуры. Часть 1: учеб. пособие — Ярославль: ЯрГУ, 2021

**б) дополнительная литература**

1. Кострикин А. И. Введение в алгебру: учебник для вузов.: в 3 ч. Часть 1. Основы алгебры: Учеб. для вузов. - Москва: 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. Основные структуры алгебры - Москва: ФИЗМАТЛИТ, 2001.
3. Р. Зуланке, А. Л. Онищик Алгебра и геометрия: учебник для вузов: в 3 т.. Т. 1, Введение. - М.: МЦНМО, 2004.
4. 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.

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):**

Профессор кафедры АМЛ, д.ф.-м. н.

Н. В. Тимофеева

**Приложение № 1 к рабочей программе дисциплины  
«Избранные вопросы алгебры»**

**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**

**Домашняя контрольная работа № 1 (ОПК-2)**

1. Выведите формулу элемента, обратного к произведению обратимых элементов моноида.
2. Постройте отношение эквивалентности на группе целых чисел, не согласованное с операцией сложения.
3. Опишите все подгруппы в группе  $Z_{12}$ .
4. Найдите все образующие аддитивной группы  $Z_8$ .
5. Докажите, что группы  $S_3$  и  $D_3$  изоморфны.
6. Перечислите все гомоморфизмы группы  $Z_6$  в группу  $Z_4 \times Z_4$ .
7. Перечислите все гомоморфизмы группы  $S_3$  в группу  $Z_4$ .
8. Докажите, что подгруппа индекса 2 является нормальной.
9. Доказать, что факторгруппа группы ненулевых комплексных чисел по подгруппе ненулевых вещественных чисел изоморфна группе вращений евклидовой плоскости
10. Перечислите все факторгруппы группы  $Z_{12} \times Z_2$ .

**Домашняя контрольная работа № 2 (ПК-2)**

1. В кольце кватернионов вычислите  
 $(1 + i - 2j + 5k)(i + 2j + 2k)^{-1} + (6 - i - j)(1 + k)$ .
2. Перечислите все гомоморфизмы колец из  $Z_6$  в  $Z_8$ .
3. Перечислите все подкольца кольца  $Z_3 \times Z_4$ .
4. Перечислите все идеалы в кольце  $Z_3 \times Z_4$ .
5. Найдите характеристику кольца  $Z_3 \times Z_5$ .
6. Перечислите все ненулевые делители нуля в кольце задачи 5.
7. Вычислите в поле  $Q[\sqrt{3}]$  значение выражения  $\frac{1+\sqrt{3}}{1-\sqrt{3}} + 4 - 2\sqrt{3}$ .
8. Перечислите все нормальные подгруппы в группе кватернионных единиц  $H = \{\pm 1, \pm i, \pm j, \pm k\}$
9. Перечислите все гомоморфизмы группы  $S_3 \times Z_4$  в группу  $Z_{24}$ . Обоснуйте, почему других гомоморфизмов нет.

Каждая полностью решенная задача оценивается в один балл. При наличии пропусков и/или ошибок в решении задача оценивается в долях балла.

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

**Зачёт** выставляется на основании выполненных самостоятельных работ. Каждая самостоятельная работа считается зачётной, если она оценена не менее чем половиной максимального количества баллов.

## **Приложение № 2 к рабочей программе дисциплины «Избранные вопросы алгебры»**

### **Методические указания для студентов по освоению дисциплины**

Основной формой изложения учебного материала по дисциплине «Избранные вопросы алгебры» являются лекции. По большинству тем предусмотрены практические занятия, на которых происходит закрепление лекционного материала путем применения его к конкретным математическим задачам и отработка навыков работы с понятийным аппаратом абстрактной алгебры.

Для успешного освоения дисциплины очень важно решение достаточно большого количества задач, как в аудитории, так и в процессе самоподготовки. Для решения всех задач необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины материала, законспектированный на лекциях, необходимо еще раз изучить и при необходимости дополнять информацией, полученной на практических занятиях, из учебной литературы или задав вопросы преподавателю. Выделение трудных мест, формулировка вопросов, вызывающих затруднение или исследовательскую любознательность, является неотъемлемой частью изучения математики.

Большое внимание должно быть уделено выполнению домашней работы. Методологической особенностью абстрактно-математических курсов является невозможность построить, описать и предоставить алгоритмы для большинства выполняемых действий. Научиться эффективно работать в такой ситуации можно лишь набором опыта решения задач различного уровня и разной направленности: как на поиск доказательства достаточно общих утверждений, так и на изучение конкретных математических, в частности, алгебраических, объектов.

Для контроля усвоения теоретического материала, приобретенных практических умений и навыков проводятся самостоятельные работы. Также проводятся консультации (при необходимости) по разбору заданий для самостоятельной работы, которые вызвали затруднения.

В конце курса при успешной сдаче самостоятельных работ студенты получают зачёт.