



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
(ФГБОУ ВО «ИГУ»)**

Институт математики и информационных технологий  
Кафедра алгебраических и информационных систем

**«УТВЕРЖДАЮ»**  
Директор ИМИТ ИГУ  
*М. В. Фалалеев*  
**М. В. Фалалеев**  
«17» мая 2023 г.



**Рабочая программа дисциплины (модуля)**

**Б1.О.26 Алгебраические системы**

Направление подготовки информационные технологии	02.03.02	Фундаментальная	информатика	и
Направленность (профиль) подготовки информационные технологии		Фундаментальная	информатика и	
Квалификация выпускника		бакалавр		
Форма обучения		очная		

Иркутск 2023 г.

Согласовано с УМК Института математики  
и информационных технологий  
Протокол № 4 от «10» мая 2023 г.

Председатель \_\_\_\_\_  
Антоник В.Г.

Рекомендовано кафедрой Алгебраических и  
информационных систем ИМИТ ИГУ:  
Протокол № 9 От «4» апреля 2023 г.

Зав. кафедрой \_\_\_\_\_  
Пантелеев В.И.

## СОДЕРЖАНИЕ

1.	Цели и задачи дисциплины	42.	МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО	43.
	ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ	44.	СОДЕРЖАНИЕ И СТРУКТУРА	
	<b>ДИСЦИПЛИНЫ</b>	64.1.	СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ, С УКАЗАНИЕМ ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ И ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ	64.2.
		64.2.	План внеаудиторной самостоятельной работы обучающихся по дисциплине	64.3.
		64.3.	СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА	74.4.
		74.4.	МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ	104.5.
		104.5.	ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ (ПРОЕКТОВ)	
	105.	УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)		
	116.	МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ		117.
	ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ	128.	ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО	
	КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ	12		

## 1. Цели и задачи дисциплины

### Цель

Дать представление о теоретической основе ИТ-дисциплин, в том числе: базы данных, криптография, защита информации

### Задачи:

- Познакомить студентов с основными структурами алгебры: группы, кольца, поля.
- Изучить конечные поля, как основу криптографии.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

2.1. Учебная дисциплина (модуль) относится к обязательной части программы и изучается на третьем курсе.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, сформированные дисциплинами линейная алгебра, дискретная математика, дискретные структуры.

2.3. Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: информационная безопасность, криптография, помехоустойчивое кодирование.

## 3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций (элементов следующих компетенций) в соответствии с ФГОС ВО по соответствующему направлению подготовки.

### Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИДК УК1.1 Анализирует задачу, выделяя ее базовые составляющие	Умеет определять условия в задачах.
	ИДК УК1.2 Определяет и ранжирует информацию, требуемую для решения поставленной задачи	Умеет выделять главное в условиях задач.
	ИДК УК1.3 Осуществляет поиск информации для решения поставленной задачи по различным типам запросов	Знает способы поиска источников информации по различным типам запросов Умеет искать источники информации на русском и иностранном языках Владеет способами поиска источников информации на русском и иностранном языках
	ИДК УК1.4 При обработке информации отличает факты от мнений,	Знает способы нахождения следствий из посылок

	интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы, в том числе с применением философского понятийного аппарата	Умеет находить следствия из посылок Владеет техникой решения задач на нахождение следствий из посылок
ОПК-1 Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	ИДК опк1.1 Знает основы математики и вычислительной техники.	Знает основные структуры алгебры: группы, кольца, поля Умеет решать типовые задачи. Владеет методами формализации и использования средств алгебры при решении профессиональных задач.
	ИДК опк1.2 Решает стандартные профессиональные задачи с применением математических знаний	
	ИДК опк1.3 Способен проводить теоретические и экспериментальные исследования объектов профессиональной деятельности	

#### 4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 4 зачетных единиц, 144 часа, в том числе 35 часов на контроль, практическая подготовка \_\_\_\_\_.  
 Форма промежуточной аттестации: 5 семестр — экзамен.

##### 4.1. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ, С УКАЗАНИЕМ ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ И ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ

№ п/п	Раздел дисциплины/темы	Се мес тр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)				Формы текущего контроля успеваемости
			Контактная работа преподавателя с обучающимися			Самостоя тельная работа + контроль	
			Лекции	Семинарские (практические занятия)	Контроль обучения		
1	Алгебраические системы	3	2	2	1	3	
2	Группы		12	12	3	21	тест
3	Кольца		6	6	3	21	тест
4	Поля		16	14	3	21	тест
<b>Итого часов</b>			34	34	10	66	

##### 4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени (час.)		
3	Алгебраические системы	<i>УИЛТИ<sub>н</sub></i>	1-я половина курса	3	тест	См. страницу курса на ИОС Educa
	Группы	<i>УИЛТИ<sub>н</sub></i>		21		См. страницу курса на ИОС Educa
	Кольца	<i>УИЛТИ<sub>н</sub></i>	2-я половина курса	21	Тест+К.Р	См. страницу курса на ИОС Educa
	Поля	<i>УИЛТИ<sub>н</sub></i>		21	Тесты+К.Р	См. страницу курса на ИОС Educa
Общая трудоемкость самостоятельной работы по дисциплине (час)				66		
Из них объем самостоятельной работы с использованием электронного обучения и дистанционных образовательных технологий (час)				<b>66</b>		

*Виды самостоятельной работы:*

*Р – написание реферата, Д – подготовка доклада, У – выполнение упражнений,*

*Э – написание эссе, Пт – выполнение проекта, К - кейс-задание, Пф – портфолио,*

*И – информационный поиск, Прз – презентация, Л – изучение литературы,*

*Т (по желанию) — заполнение таблицы Донны Огл «Знал, хотел узнать, узнал»*

*Ин (по желанию) — заполнение таблицы, содержащей 4 столбца — «V» - уже знал, «+» — новое, «-» — думал иначе, «?» — не понял, есть вопросы.*

#### 4.3. СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

##### 1. Алгебраические системы

- Множества. Отношения и отображения. Отношение эквивалентности.
- Бинарные алгебраические операции. Свойства. Нейтральные элементы. Обратимость.
- Алгебраические системы, подсистемы. Гомоморфизм алгебраических систем. Изоморфизм алгебраических систем.

##### 2. Группы

- Определение группы.
- Порядок элемента группы. Свойства.
- Подгруппы.
- Циклические подгруппы.

- Смежные классы по подгруппе. Теоремы о смежных классах.
- Теорема Лагранжа. Следствия. Теорема Эйлера.
- Теорема Коши для конечных групп.
- Описание всех групп малых порядков.
- Нормальные подгруппы.
- Факторгруппы.
- Гомоморфизмы групп.
- Свойства гомоморфизма.
- Теоремы о гомоморфизмах групп.

### 3. Кольца

- Кольца.
- Кольцо целых чисел.
- Кольцо многочленов над кольцом  $K$ . Операции над многочленами. Вложимость кольца  $K$  в кольцо многочленов.
- Деление с остатком в кольце многочленов.
- Схема Горнера.
- Идеалы колец и факторкольца.
- Отношение неотличимости по идеалу.
- Кольцо классов вычетов по модулю.
- Обратимость.

### 4. Поля

- Поля.
- Дроби в поле. Свойства дробей.
- Гомоморфизмы и изоморфизмы полей.
- Простые поля. Теорема о простом подполе произвольного поля.
- Характеристика поля.
- Поле комплексных чисел. Операции над комплексными числами. Тригонометрическая и алгебраическая форма комплексных чисел.
- Извлечение корней из комплексных чисел.
- Теорема о комплексных корнях многочлена с действительными коэффициентами.
- Поле разложения многочлена.
- Расширение поля. Конечные расширения.
- Алгебраические элементы поля.
- Теорема об алгебраичности конечных расширений.
- Автоморфизмы поля. Группа автоморфизмов. Свойства простого подполя относительно автоморфизма.
- Конечные поля.





	<ul style="list-style-type: none"> <li>● Деление с остатком в кольце многочленов. Схема Горнера.</li> <li>● Идеалы колец и факторкольца. Отношение неотличимости по идеалу. Кольцо классов вычетов по модулю. Обратимость.</li> </ul> <p><b>4. Поля</b></p> <ul style="list-style-type: none"> <li>● Поля. Дроби в поле. Свойства дробей. Гомоморфизмы и изоморфизмы полей.</li> <li>● Простые поля. Теорема о простом подполе произвольного поля. Характеристика поля. Примеры.</li> <li>● Поле комплексных чисел. Операции над комплексными числами. Тригонометрическая и алгебраическая форма комплексных чисел.</li> <li>● Извлечение корней из комплексных чисел. Теорема о комплексных корнях многочлена с действительными коэффициентами.</li> <li>● Поле разложения многочлена. Расширение поля. Конечные расширения. Алгебраические элементы поля.</li> <li>● Автоморфизмы поля. Группа автоморфизмов. Свойства простого подполя относительно автоморфизма.</li> <li>● Конечные поля. Неподвижные при автоморфизме элементы поля.</li> <li>● Мультипликативная группа поля.</li> <li>● Числе элементов подполя конечного поля.</li> <li>● Конечномерные алгебры над полем. Алгебра кватернионов.</li> </ul>	14	14	упражнения, тесты	
	<b>Всего</b>	34		Контрольные вопросы, упражнения, тесты	

**4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СР)**  
Не предусмотрено.

**4.4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ**

Методические указания находятся на странице курса в ИОС Educa

**4.5. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ (ПРОЕКТОВ)**

Не предусмотрено.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### а) перечень литературы

1. Курош, А. Г. Лекции по общей алгебре : учебник для вузов / А. Г. Курош. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 556 с. — ISBN 978-5-507-44067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/208670>. — Режим доступа: для авториз. пользователей.+
  2. Глухов, М. М. Алгебра : учебник / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. — 3-е изд., стер. — Санкт-Петербург : Лань, 2020. — 608 с. — ISBN 978-5-8114-4775-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/126718>. — Режим доступа: для авториз. пользователей.
  3. Каргаполов, М. И. Основы теории групп : учебное пособие / М. И. Каргаполов, Ю. И. Мерзляков. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 288 с. — ISBN 978-5-8114-0894-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/210266>. — Режим доступа: для авториз. Пользователей
  4. Шилин, И. А. Введение в алгебру. Группы : учебное пособие / И. А. Шилин. — Санкт-Петербург : Лань, 2022. — 208 с. — ISBN 978-5-8114-1419-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/211004>. — Режим доступа: для авториз. пользователей.
  5. Окунев, Л. Я. Сборник задач по высшей алгебре : учебное пособие / Л. Я. Окунев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 192 с. — ISBN 978-5-8114-0900-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/210329>. — Режим доступа: для авториз. пользователей.
  6. Сборник задач по алгебре [Текст] : учеб. пособие / под ред. А. И. Кострикина. - М. : Наука, 1987. - 351 с.

### б) периодические издания

### в) список авторских методических разработок:

электронные варианты лекций в ИОС EDUCA

### г) базы данных, информационно-справочные и поисковые системы

1. <http://www.window.edu.ru> — Единое окно доступа к образовательным ресурсам. Полнотекстовая электронная библиотека учебных и учебно-методических материалов (федеральный ресурс).
2. <http://www.exponenta.ru> — Образовательный математический сайт
3. <http://www.mccme.ru/free-books> — Московский центр непрерывного математического образования. Материалы (полные тексты) свободно распространяемых книг по математике.
4. <https://www.biblio-online.ru/> — Электронно-библиотечная система издательства «ЮРАЙТ»
6. <https://e.lanbook.com/> — Электронно-библиотечная система издательства «Лань»
7. ИОС ИГУ EDuca
8. <https://welcome.stepik.org/ru> — Онлайн-курсы от ведущих вузов и компаний страны
9. <https://openedu.ru/> — Открытое образовани.

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 6.1. УЧЕБНО-ЛАБОРАТОРНОЕ ОБОРУДОВАНИЕ:

Для проведения лекционных занятий необходима аудитория с презентационным оборудованием, для проведения практических занятий необходима аудитория на 25–30 рабочих мест (в зависимости от численности учебной группы), оборудованная доской, презентационной техникой.

### 6.2. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

LaTeX – с использованием сборки TeXLive (или возможность выхода на онлайн-ресурс

Overleaf), pdf-view'ep.

### 6.3. ТЕХНИЧЕСКИЕ И ЭЛЕКТРОННЫЕ СРЕДСТВА:

ИОС EDUCA, DOMIC, презентационное оборудование, персональный компьютер с возможностью демонстрации презентаций в формате pdf.

## 7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При реализации данного курса используются следующие образовательные технологии: технологии традиционного обучения, игровые технологии, технологии проблемного обучения, технологии обучения в сотрудничестве, технологии контекстного обучения, интерактивные технологии, технологии дистанционного обучения, активные педагогические технологии.

## 8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### 8.1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ВХОДНОГО КОНТРОЛЯ

Не предусмотрено

### 8.2. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ТЕКУЩЕГО КОНТРОЛЯ

Тесты по всем разделам в ИОС Educa, контрольные работы по темам Кольцо целых чисел, поле Комплексных чисел.

Образец заданий из контрольной работы по теме Кольцо целых чисел

2. Найти НОД( $a, b$ ) и найти целые  $x, y$  такие, что  $ax + by = \text{НОД}(a, b)$ , если

- 0)  $a = 420, b = 126$ ;    1)  $a = 476, b = 1258$ ;    2)  $a = 988, b = 2014$ ;  
3)  $a = 874, b = 1518$ ;    4)  $a = 1253, b = 252$ ;    5)  $a = 529, b = 1541$ .  
6)  $a = 874, b = 1520$ ;    7)  $a = 1253, b = 251$ ;    8)  $a = 529, b = 1542$ .

3. Найти все целые решения уравнения

- 0)  $21x + 9y = 15$ ;    1)  $27x + 18y = 12$ ;    2)  $275x + 145y = 10$ ;  
3)  $46x + 98y = 106$ ;    4)  $36x + 21y = 123$ ;    5)  $28x - 48y = 60$ ;  
6)  $60x - 35y = 145$ ;    7)  $14x - 38y = 46$ ;    8)  $86x + 74y = 42$ .

Образец заданий из контрольной работы по теме поле Комплексных чисел

1.4. Найти все значения корня из комплексного числа

- 0)  $\sqrt[7]{\frac{(2+2i)^{20}(1-\sqrt{3}i)^5}{(1-i)^8}}$ ;    1)  $\sqrt[7]{\frac{(2-2i)^{20}(1+\sqrt{3}i)^5}{(1-i)^{10}}}$ ;    2)  $\sqrt[7]{\frac{(2-2i)^{20}(1-\sqrt{3}i)^7}{(1-i)^{12}}}$ ;  
3)  $\sqrt[8]{\frac{1+i}{\frac{\sqrt{2}}{2} + \frac{1}{2}i}}$ ;    4)  $\sqrt[10]{\frac{1-i}{\frac{\sqrt{2}}{2} - \frac{1}{2}i}}$ ;    5)  $\sqrt[12]{\frac{1-i}{-\frac{\sqrt{2}}{2} + \frac{1}{2}i}}$ ;  
6)  $\sqrt[7]{\frac{(3+3i)^{10}(2-2\sqrt{3}i)^5}{(1-i)^5}}$ ;    7)  $\sqrt[7]{\frac{(5-5i)^{12}(2+2\sqrt{3}i)^6}{(1+i)^{10}}}$ ;    8)  $\sqrt[7]{\frac{(1-i)^{15}(2-2\sqrt{3}i)^7}{(1+i)^{12}}}$ ;  
9)  $\sqrt[7]{\frac{(1+i)^{15}(2-2\sqrt{3}i)^7}{(1+i)^{12}}}$ .

1.5. Решить систему уравнений

- 0)  $\begin{cases} (2+i)x - (3+i)y = i; \\ (3-i)x + (2+i)y = -i; \end{cases}$     1)  $\begin{cases} (2-i)x - (3+i)y = i; \\ (3-i)x + (2-i)y = -i; \end{cases}$

На странице курса в ИОС Educa находятся типовые задачи, которые рассматриваются на практических занятиях.

### 8.3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

Промежуточный контроль – экзамен по программе курса. Вся необходимая информация находится в ИОС Educa на странице курса. Для допуска к экзамену необходимо выполнить все тесты (уровень  $\geq 60$ ) и все контрольные работы (уровень  $\geq 3$ ). На экзамене необходимо будет показать умение решать типовые задачи и ответить на вопросы билета.

Образцы типовых задач

1. Построить конечное поле из 4 элементов. Указать примитивные элементы.
2. Найти все значения корня из комплексного числа

$$0) \sqrt[7]{\frac{(2+2i)^{20}(1-\sqrt{3}i)^8}{(1-i)^8}}; \quad 1) \sqrt[7]{\frac{(2-2i)^{20}(1+\sqrt{3}i)^8}{(1-i)^{10}}}; \quad 2) \sqrt[7]{\frac{(2-2i)^{20}(1-\sqrt{3}i)^7}{(1-i)^{12}}};$$

3. Построить решетку подполей поля  $F_{2^{20}}$ .

Образец билета

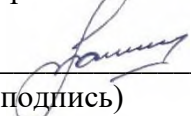
---

#### БИЛЕТ 13(4-5)

- 1 Поле разложения многочлена.
- 2 Покажите, что каждый элемент конечного поля есть сумма двух квадратов.

Экзаменатор \_\_\_\_\_ Пантелеев В.И.

Разработчики

  
\_\_\_\_\_  
(подпись)

Зав. каф. АиИС  
(занимаемая должность)

Пантелеев В.И.  
(Ф.И.О.)

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 02.03.02 «Фундаментальная информатика и информационные технологии» (уровень бакалавриата), утвержденный приказом Министерства образования и науки Российской Федерации от 23 августа 2017 г. N 808, зарегистрированный в Минюсте России «14» сентября 2017 г. № 48185 с изменениями и дополнениями с изменениями и дополнениями от: 26 ноября 2020 г., 8 февраля 2021 г.

Программа рассмотрена на заседании кафедры Алгебраических и информационных систем ИМИТ ИГУ «4» апреля 2023 г.

Протокол № 9 Зав. кафедрой  Пантелеев В.И.

Настоящая программа, не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.