

# АБСТРАКТНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА

## 1. Цель освоения дисциплины

Формирование систематизированных знаний в области абстрактной и компьютерной алгебры.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Абстрактная и компьютерная алгебра» относится к вариативной части блока дисциплин.

Для освоения дисциплины «Абстрактная и компьютерная алгебра» обучающиеся используют знания, умения, способы деятельности и установки, сформированные в ходе изучения дисциплин «Естественнонаучная картина мира», «Информационные технологии в образовании», «Основы математической обработки информации», «Педагогика», «Психология», «Алгебра», «Вводный курс математики», «Геометрия», «Математический анализ», «Операционная система Linux», «Построение Windows-сетей», «Разработка электронных образовательных ресурсов», «Разработка эффективных алгоритмов», «Теория вероятностей и математическая статистика», «Теория функций действительного переменного», «Технологии Интернет-обучения», «Физика», «Численные методы», прохождения практик «Научно-исследовательская работа», «Практика по получению первичных профессиональных умений и навыков».

Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин «Алгебраические системы», «Анализ эволюционных задач», «Дифференциальные уравнения», «Дополнительные главы математического анализа», «Информационные технологии в математике», «Исследование операций и методы оптимизации», «Компьютерная алгебра», «Компьютерное моделирование», «Метрические пространства», «Основы искусственного интеллекта», «Основы теории решеток», «Основы универсальной алгебры», «Перспективные направления искусственного интеллекта», «Перспективные направления компьютерного моделирования», «Проектирование информационных систем», «Современные языки программирования», «Специализированные математические пакеты», «Теория алгоритмов», «Теория функций комплексного переменного», «Эксплуатация компьютерных систем», «Элементы общей алгебры», «Элементы статистической обработки данных», прохождения практик «Практика по получению первичных умений и навыков научно-исследовательской деятельности», «Практика по получению профессиональных умений и опыта профессиональной деятельности», «Преддипломная практика».

## 3. Планируемые результаты обучения

В результате освоения дисциплины выпускник должен обладать следующими компетенциями:

- способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве (ОК-3);
- способностью руководить учебно-исследовательской деятельностью обучающихся (ПК-12).

**В результате изучения дисциплины обучающийся должен:**

### *знать*

- способы представления на компьютере классических алгебраических структур, границы применимости символьных вычислений на компьютере;
- базовые методы перечисления конечных алгебраических объектов;
- основные методы и алгоритмы компьютерной алгебры;

### **уметь**

- решать с использованием математических пакетов базовые задачи, относящиеся к компьютерной алгебре;
- решать типовые задачи на разбиение множества равномошных конечных алгебраических объектов с одинаковой сигнатурой на классы изоморфных;
- применять основные алгоритмы, реализованные в системе компьютерной алгебры, для решения задач теории чисел;

### **владеть**

- представлением о связи абстрактной алгебры и символьных вычислений на компьютере;
- приемами реализации базовых алгоритмов на графах;
- приемами использования системы компьютерной алгебры для решения задач теории чисел.

## **4. Общая трудоёмкость дисциплины и её распределение**

количество зачётных единиц – 2,

общая трудоёмкость дисциплины в часах – 72 ч. (в т. ч. аудиторных часов – 12 ч., СРС – 56 ч.),

распределение по семестрам – 4 курс, зима,

форма и место отчётности – зачёт (4 курс, зима).

## **5. Краткое содержание дисциплины**

Символьные вычисления на компьютере.

Символьные вычисления на компьютере. Предмет компьютерной алгебры. Проблемы разбухания данных. Алгоритмическая неразрешимость проблемы тождества слов в основных алгебраических структурах и ее влияние на развитие компьютерной алгебры. Основные формы и представления алгебраических объектов и выражений на компьютере.

Работа с конечными алгебраическими структурами.

Особенности работы с конечными алгебраическими структурами на компьютере. Работа с группами подстановок: перевод подстановки, заданной второй строкой двухстрочной записи, в цикловую форму, и обратно; построение подгруппы группы подстановок с заданным множеством образующих. Алгоритмы на графах. Перечисление всех квазигрупп (луп) фиксированного порядка с точностью до изоморфизма. Проверка выполнимости тождеств и квазитожеств в конечных алгебраических структурах.

Арифметика целых чисел на компьютере.

Сравнение, сложение, вычитание и умножение целых чисел в компьютерной алгебре.

Деление с остатком. Возведение в степень по модулю, числа Кармайкла. Бинарный алгоритм и алгоритм Евклида. Сильный тест проверки на псевдопростоту Рабина-Миллера.

Детерминированные тесты. Простые числа Мерсенна. Тест Люка-Лемера и проект GIMPS.

Классические и современные алгоритмы факторизации натуральных чисел: метод Ферма; метод Моррисона-Бриллхарта; метод квадратичного решета. Проблема надежности RSA-шифрования с открытым ключом.

## **6. Разработчик**

Лецко Владимир Александрович, доцент кафедры алгебры, геометрии и математического анализа ФГБОУ ВО "ВГСПУ".