МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Минзарипов Р.Г.

Программа дисциплины

Общая алгебра и теория чисел Б3.ДВ.5

Направление подготовки: 010400.62 - Прикладная математика и информатика
Профиль подготовки: Математическое и программное обеспечение вычислительных машин и сетей
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Кугураков В.С.

Рецензент(ы):

Столов Е.Л.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Аблаев Ф. М.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 986315

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

Казань
2015

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

Содержание

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Кугураков В.С. кафедра теоретической кибернетики отделение фундаментальной информатики и информационных технологий , Vladimir.Kugurakov@kpfu.ru

1. Цели освоения дисциплины

Дисциплина знакомит студентов с основными алгебраическими структурами. В процессе обучения студенты должны усвоить методику построения алгебраических структур и приобрести навыки использования абстрактного алгебраического аппарата при решении прикладных задач. Курс "Общая алгебра" служит основой при изучении других дисциплин специальности "Прикладная математика и информатика" и её специализации "Математическая кибернетика" (Теория информации и кодирования, теория автоматов, криптография и др.).

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б3.ДВ.5 Профессиональный" основной образовательной программы 010400.62 Прикладная математика и информатика и относится к дисциплинам по выбору. Осваивается на 3 курсе, 6 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 3 курсе 5семестр для студентов, обучающихся по направлению "Прикладная математика и информатика".

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-9 (профессиональные компетенции)	способность осуществлять на практике современные методологии управления жизненным циклом и качеством систем, программных средств и сервисов информационных технологий

В результате освоения дисциплины студент:

1. должен знать:

роль языка алгебраических структур при описании различных объектов исследования;

2. должен уметь:

ориентироваться в иерархии алгебраических структур;

3. должен владеть:

теоретическими знаниями о базовых алгебраических системах - группах, кольцах, полях и др.;

приобрести навыки использования алгебраического аппарата при решении прикладных задач.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины зачет в 6 семестре.

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Введение.	6	18	0	0	4	домашнее задание
2.	Тема 2. Множества и отображения.	6	18	0	0	4	домашнее задание
3.	Тема 3. Арифметика целых чисел.	6	18	0	0	4	домашнее задание
4.	Тема 4. Введение в алгебраические структуры.	6	18	0	0	4	тестирование
5.	Тема 5. Группы.	6	18	0	0	4	домашнее задание
6.	Тема 6. Кольца и поля.	6	18	0	0	4	домашнее задание
7.	Тема 7. Многочлены и кольца многочленов.	6	18	0	0	4	домашнее задание
8.	Тема 8. Теория полей.	6	18	0	0	4	домашнее задание
9.	Тема 9. Строение конечных полей.	6	18	0	0	4	письменная работа
.	Тема . Итоговая форма контроля	6		0	0	0	зачет
	Итого			0	0	36	

4.2 Содержание дисциплины

Тема 1. Введение.

лабораторная работа (4 часа(ов)):

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

Введение. Предмет дисциплины ?Общая алгебра и теория чисел?. Исторические сведения о развитии данного раздела математики. Роль и место общей алгебры в системе математического образования.

Тема 2. Множества и отображения.

лабораторная работа (4 часа(ов)):

Множества и отображения. Отношения эквивалентности. Факторизация отображений

Тема 3. Арифметика целых чисел.

лабораторная работа (4 часа(ов)):

Арифметика целых чисел. Основная теорема арифметики. НОД и НОК. Алгоритм деления в Z. Некоторые теоретико-числовые функции. Мультипликативные функции. Функции Мебиуса и Эйлера. Формула обращения Мебиуса. Сравнения в Z. Полная и приведенная системы вычетов по mod n. Теоремы Эйлера и Ферма. Китайская теорема об остатках.

Тема 4. Введение в алгебраические структуры.

лабораторная работа (4 часа(ов)):

Введение в алгебраические структуры. Множества с бинарной операцией. Группоиды. Полугруппы. Моноиды. Группы. Кольца и поля.

Тема 5. Группы.

лабораторная работа (4 часа(ов)):

Группы. Симметрическая и знакопеременная группы. Морфизмы групп. Теорема Кэли. Смежные классы по подгруппе. Теорема Лагранжа. Циклические группы. Нормальные подгруппы. Факторгруппы. Мультипликативная группа целых чисел по mod n.

Тема 6. Кольца и поля.

лабораторная работа (4 часа(ов)):

Кольца и поля. Общие свойства колец. Типы колец. Сравнения. Кольцо классов вычетов по mod n. Факторкольца. Гомоморфизмы и идеалы колец. Области целостности и поля. Характеристика кольца и поля. Простые поля.

Тема 7. Многочлены и кольца многочленов.

лабораторная работа (4 часа(ов)):

Многочлены и кольца многочленов. Элементарные свойства многочленов. Алгоритм Евклида. Однозначность разложения на простые множители. Факториальность евклидовых колец. Поле отношений целостного кольца. Поле рациональных функций. Простейшие дроби. Корни многочленов. Интерполяционные формулы.

Тема 8. Теория полей.

лабораторная работа (4 часа(ов)):

Теория полей. Присоединение. Простые расширения полей. Конечные и алгебраические расширения. Алгебраическое замыкание. Поля разложения. Конечные поля Галуа.

Тема 9. Строение конечных полей.

лабораторная работа (4 часа(ов)):

Строение конечных полей. Характеризация конечных полей. Цикличность мультипликативной группы поля. Единственность конечного поля заданного порядка. Критерий подполя. Корни многочленов. Разложение многочленов на неприводимые сомножители. Представление элементов конечных полей. Вычисления в конечных полях. Некоторые приложения конечных полей.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Введение.	6	18	подготовка домашнего		

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

задания

8	домашнее

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

задание

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Множества и отображения.	6	18	подготовка домашнего задания	8	домашнее задание
3.	Тема 3. Арифметика целых чисел.	6	18	подготовка домашнего задания	8	домашнее задание
4.	Тема 4. Введение в алгебраические структуры.	6	18	подготовка к тестированию	8	тестирование
5.	Тема 5. Группы.	6	18	подготовка домашнего задания	8	домашнее задание
6.	Тема 6. Кольца и поля.	6	18	подготовка домашнего задания	8	домашнее задание
7.	Тема 7. Многочлены и кольца многочленов.	6	18	подготовка домашнего задания	8	домашнее задание
8.	Тема 8. Теория полей.	6	18	подготовка домашнего задания	8	домашнее задание
9.	Тема 9. Строение конечных полей.	6	18	подготовка к письменной работе	8	письменная работа
	Итого				72	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекций, а также самостоятельной работы студентов.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Введение.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме.

Тема 2. Множества и отображения.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Решение задач на тему "Множества и отображения"

Тема 3. Арифметика целых чисел.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Решение задач на тему "Арифметика простых чисел"

Тема 4. Введение в алгебраические структуры.

тестирование , примерные вопросы:

Тестирование по пройденным темам. Примерные вопросы: 1. Свойства отображений: инъективность, сюръективность, биективность. 2. Композиция отображений. 3. Бинарные отношения. Отношения эквивалентности и порядка. 4. Основная теорема арифметики кольца . 5. Алгоритм деления в . 6. Наибольший общий делитель и наименьшее общее кратное. 7. Свойства сравнений в . 8. Полная и приведенная система вычетов по модулю n. 9. Малая теорема Ферма. 10. Теорема Эйлера. 11. Китайская теорема об остатках.

Тема 5. Группы.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Решение задач на тему "Группы"

Тема 6. Кольца и поля.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Решение задач на тему "Кольца и поля""

Тема 7. Многочлены и кольца многочленов.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Решение задач на тему "Многочлены"

Тема 8. Теория полей.

домашнее задание , примерные вопросы:

Углубленное изучение литературы по теме. Решение задач на тему "Теория полей"

Тема 9. Строение конечных полей.

письменная работа , примерные вопросы:

Письменная работа по пройденным темам. Примерные вопросы: 1. Алгебраические структуры: группоиды, полугруппы, моноиды, группы. 2. Симметрическая и знакопеременная группы. 3. Теорема Кэли. 4. Циклические группы. Основные свойства. 5. Смежные классы по подгруппе. 6. Теорема Лагранжа. 7. Подгруппы. Нормальные делители. 8. Фактор-группа. 9. Морфизмы групп: изоморфизм и гомоморфизм. 10. Теорема о гомоморфизмах групп. 11. Кольца. Определение и общие свойства колец. 12. Поле. Характеристика поля.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

По данной дисциплине предусмотрено проведение зачета. Примерные вопросы для зачета - Приложение 1.

ВОПРОСЫ К ЗАЧЕТУ

1. Свойства отображений: инъективность, сюръективность, биективность.
2. Композиция отображений.
3. Бинарные отношения. Отношения эквивалентности и порядка.
4. Основная теорема арифметики кольца .
5. Алгоритм деления в .
6. Наибольший общий делитель и наименьшее общее кратное.
7. Свойства сравнений в .
8. Полная и приведенная система вычетов по модулю n.
9. Малая теорема Ферма.
10. Теорема Эйлера.
11. Китайская теорема об остатках.
12. Алгебраические структуры: группоиды, полугруппы, моноиды, группы.
13. Симметрическая и знакопеременная группы.
14. Теорема Кэли.
15. Циклические группы. Основные свойства.
16. Смежные классы по подгруппе.
17. Теорема Лагранжа.

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

18. Подгруппы. Нормальные делители.
19. Фактор-группа.
20. Морфизмы групп: изоморфизм и гомоморфизм.
21. Теорема о гомоморфизмах групп.
22. Кольца. Определение и общие свойства колец.
23. Поле. Характеристика поля.
24. Идеалы колец . Классы вычетов и фактор-кольца.
25. Кольцо классов вычетов по модулю n.
26. Теорема о гомоморфизмах колец.
27. Характеристика кольца и поля.
28. Простое поле. Два типа простых полей.
29. Поле отношений.
30. Интерполяционная формула Лагранжа.
31. Расширения полей: простое, конечное, алгебраическое, трансцендентное.
32. Поле разложения многочлена.
33. Конечное поле. Число элементов. Почему не существует полей порядка 6 и 10, но существуют поля порядков 7 и 9.
34. Цикличность мультипликативной группы конечного поля.
35. Неприводимые многочлены над конечными полями. Основная теорема арифметики кольца F_q [x].
36. Построение полей малого порядка q (= 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23,25).
37. Вычисления в конечных полях.

7.1. Основная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2

http://znanium.com/bookread.php?book=405000

2. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с.

http://znanium.com/catalog.php?bookinfo=441493

3. Ишмухаметов Ш. Т. Методы факторизации натуральных чисел: учебное пособие. Казанский (Приволжский) федеральный университет: Факультет вычислительной математики и кибернетики, 2011

http://libweb.ksu.ru/ebooks/publicat/0-787702.pdf

7.2. Дополнительная литература:

1.Общая алгебра : лекции 1969 - 1970 учебного года / А. Г. Курош .? Москва : Наука, 1974 .? 159с

2.Алгебраическая теория полугрупп : в 2-х т. / А. Клиффорд, Г. Престон .? М. : Мир, Б.г.

Т. 1 / ред. Л. Н. Шеврин .? 1972 .? 285 с.

7.3. Интернет-ресурсы:

Бухштаб А.А. Теория чисел. - http://eek.diary.ru/p54405820.htm

Википедия - http://ru.wikipedia.org/wiki/%D2%E5%EE%F0%E8%FF_%F7%E8%F1%E5%EB

Дэвенпорт Г. Высшая арифметика. Введение в теорию чисел. - http://eek.diary.ru/p54405820.htm

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

З. И. Боревич, И. Р. Шафаревич Теория чисел. - http://eek.diary.ru/p54405820.htm

Кузьмин М.С. - http://inc.istu.ru/index.php/remository?func=fileinfo&id=253

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Общая алгебра и теория чисел" предполагает использование следующего материально-технического обеспечения:

Лекционные занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом(маркером)

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010400.62 "Прикладная математика и информатика" и профилю подготовки Математическое и программное обеспечение вычислительных машин и сетей .

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

Автор(ы):
Кугураков В.С. _____
"__" _____ 201 __ г.

Рецензент(ы):
Столов Е.Л. _____
"__" _____ 201 __ г.

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ