

АННОТАЦИЯ

дисциплины «Абелевы группы»

Направление подготовки магистра 01.04.01 МАТЕМАТИКА Программа «Алгебра»

1. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике. Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин: алгебра, теория групп, криптография, защита информации.

2. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к дисциплинам профессионального цикла, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, программа «Алгебра».

Дисциплина изучается в течение одного семестра.

3. Цели изучения дисциплины

Целью курса является изучение методов, задач теории групп и колец, криптографии, коды, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Абелевы группы» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность создавать и исследовать новые математические модели естественных наук (ОПК-2);
- Способность к организации научно-исследовательских и научно-производственных работ, к управлению научным коллективом (ПК-1).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие студентов, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Абелевы группы»:

Студент должен знать

- основы теории групп;
- основы теории полей;
- основы теории колец;
- блочные шифры;

- симметричные криптосистемы;
- асимметричные криптосистемы;
- коды шифрования.

Студент должен уметь:

- применять полученные методы и модели к решению типовых и практических задач с использованием аппарата алгебры, криптографии, основных алгебраических структур (группы, кольца, поля);
- шифрующих кодов;
- пользоваться формулами и теоремами теории групп и теории полей, строить критерии для проверки гипотез;
- пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
- применять полученные знания для изучения других дисциплин.

Студент должен владеть:

- навыки применения криптографических алгоритмов и алгебраических методов для решения различных прикладных задач.

4. Формы работы магистров

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 5 курса, читается в 9 семестре

Лекционные занятия – 18ч

Практические занятия – 18 ч

Самостоятельная работа – 54 ч

экзамен в 9 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А., ст.преп. Джусоева Н.А.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Абелевы группы» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по каждому модулю, зачета и экзамена, также предусматривающего набор необходимого количества баллов.

6. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен экзамен (9 семестр).

За выполнение заданий текущего и промежуточного контроля студент может набрать максимальное количество баллов.

7. Тематический план курса

9 семестр

Номер не де ли	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия		Самостоятельная работа студентов		Формы контр оля	Количе ство баллов		Лит ера тур а
		л	пр	Содержание	Ча сы		mi n	ма х	
1- 2	Векторное пространство. Определение, примеры.	2	2	.	8				[1,3]
3- 4	Л.н.с. и л.з.с. Базис. Переход к координатам в другом базисе.	2	2		6				[1,4]
5- 6	Линейный оператор. Матрица линейного оператора.	2	2		8				[1,4 ,5]
7- 8	Ядро и образ линейного оператора.	2	2		6				[1,3]
9- 10	Собственные значения и собственные векторы.	2	2		6				[1,3]
11 - 12	Жорданова форма матриц.	2	2	Примеры конечных групп	6				[2,6 ,8]
13 - 14	Жорданова форма матриц	2	2	Примеры неизоморфны х конечных групп	6				[2,6 ,8]
15 - 16	Фактор-группа. Примеры	2	2	Примеры бесконечных групп, фактор- группы которых конечны	4				[2,6 ,8]
17 - 18	Гомоморфизмы. Примеры.	2	2	Примеры гомоморфизм ов	4				[2,6 ,8]
	ИТОГО	18	18		54				

Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количес тво часов	Активные формы	Интерактивные формы
------	------	----------------	-------------------------	-------------------	------------------------

1	Построение криптошифрования в кольце Z_{pq} для конкретных p, q	Практическое	2	Диалог	Использование на проекторе таблицы умножения в кольце Z_{pq}
2	Построение (n, k) -пороговой схемы разделения секрета для конкретных n, k	Практическое	2		Использование на проекторе таблицы умножения и сложения для формирования взаимно простых модулей
3	Примеры построения схем разделения секрета	Практическое	2		Использование на проекторе таблицы умножения и сложения для применения китайской теоремы при построении схемы разделения секрета

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

№	Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре
Основная литература:	
1.	Яценко В.В. Введение в криптографию. М.: МЦНМО. 2012. 352 с.
2.	Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005
3.	Алферов А.П. и др. Основы криптографии. – М. Гелиос АРВ. 2005.480 с.
4.	Ноден П., Ките К. Алгебраическая алгоритмика. – М. Мир. 2007. 720 с.
5.	Коблиц Н. Курс теории чисел и криптографии. – М. ТВП. 2007. 261с.
6.	Кострикин А.И. Введение в алгебру. Ч.1-3 – М. МЦНМО. 2009. 838с.
Дополнительная литература	
7.	Баскаков А.Г. Лекции по алгебре. Изд-во ВГУ.2014.
8.	Кострикин А.И. Сборник задач по алгебре.-М. МЦНМО. 2009. 408 с.
Электронный ресурс	
9.	Кострикин А.И. Введение в алгебру http://math-portal.ru/678-vvedenie-v-algebru-chast-3-osnovnye-struktury-kostrikin-ai-3-e-izdanie.html
10.	Коблиц Н. Курс теории чисел и криптографии. http://math-portal.ru/tags/%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F/

Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

дисциплины «Алгебра и криптография»

Направление подготовки магистра 01.04.01 МАТЕМАТИКА Программа «Алгебра»

1. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике. Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин: алгебра, теория групп, криптография, защита информации.

2. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к дисциплинам профессионального цикла, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, программа «Алгебра».

Дисциплина изучается в течение двух семестров.

3. Цели изучения дисциплины

Целью курса является изучение методов, задач теории групп и колец, криптографии, коды, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Алгебра и криптография» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность находить, формулировать и решать актуальные и значимые проблемы фундаментальной и прикладной математики (ОПК-1);
- Способность к интенсивной научно-исследовательской работе (ПК-1).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие студентов, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Алгебра и криптография»:

Студент должен знать

- основы теории групп;
- основы теории полей;
- основы теории колец;
- блочные шифры;
- симметричные криптосистемы;

- асимметричные криптосистемы;
- коды шифрования.

Студент должен уметь:

- применять полученные методы и модели к решению типовых и практических задач с использованием аппарата алгебры, криптографии, основных алгебраических структур (группы, кольца, поля);
- шифрующих кодов;
- пользоваться формулами и теоремами теории групп и теории полей, строить критерии для проверки гипотез;
- пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
- применять полученные знания для изучения других дисциплин.

Студент должен владеть:

- навыки применения криптографических алгоритмов и алгебраических методов для решения различных прикладных задач.

4. Формы работы магистров

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 5 курса, читается в 9, 10 семестрах

Лекционные занятия – 18/16ч

Практические занятия – /16 ч

Самостоятельная работа – 18/76 ч

В интенсивной форме: лекционные занятия – 4ч

практические занятия – 4ч

зачет в 9 семестре

экзамен в 10 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А., ст.преп. Джусоева Н.А.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Алгебра и криптография» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по каждому модулю, зачета и экзамена, также предусматривающего набор необходимого количества баллов.

6. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрены экзамен (10 семестр) и зачет (9 семестр).

За выполнение заданий текущего и промежуточного контроля студент может набрать максимальное количество баллов.

7. Тематический план курса

9 семестр

Но мер нед ели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия		Самостоятельная работа студентов		Формы контрол я	Количество о баллов		Лите ра тура
		л	пр	Содержание	Часы		min	max	
1	История криптографии	2		.					[1,3]
2	Примеры шифров и криптографических систем	2		Шифры простой подстановки и перестановки, усложненные комбинированные шифры	4				[1,4]
3	Использование алгебраического аппарата в криптографии	2							[1,4,5]
4	Симметричные криптографические системы	2		Примеры симметричных криптографических систем	2				[1,3]
5	Асимметричные криптографические системы	2		Примеры асимметричных криптографических систем	2				[1,3]
6	Определение группы. Примеры.	2		Примеры конечных групп	2				[2,6,8]
7	Подгруппы. Примеры подгрупп.	2		Примеры неизоморфных конечных групп	2				[2,6,8]
8	Фактор-группа. Примеры	2		Примеры бесконечных групп, фактор- группы которых конечны	2				[2,6,8]
9	Гомоморфизмы. Примеры.	2		Примеры гомоморфизмов	4				[2,6,8]
	ИТОГО	18			18				

10 семестр

Но мер нед ели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия		Самостоятельная работа студентов		Формы контрол я	Количество о баллов		Лите ра тура
		л	пр	Содержание	Часы		min	max	
1	Теоремы о гомоморфизме.	2	2	Примеры применения теорем о гомоморфизме.	6				[2,6,8]
2	Действие группы на множестве. Стабилизатор.	2	2	Примеры действия группы на множестве. Стабилизаторы	10				[2,6,8]
3	Теоремы Эйлера и Ферма и обращение криптографического шифрования	2	2	Примеры применения теорем Эйлера и Ферма для построения шифрования	10				[2, 5]

4	Китайская теорема об остатках	2	2	Примеры применения китайской теоремы об остатках	10				[4, 5]
5	Криптографическая система RSA	2	2	Обоснование криптографической системы RSA и примеры открытого шифрования	10				[4, 5]
6	Электронная подпись	2	2	Формирование электронной подписи и примеры электронной подписи	10				[4, 5]
7	Схема разделения секрета	2	2	Пример применения схемы разделения секрета на задаче о принятии решения при отсутствии руководителя	10				[1,4]
8	Шифрование с помощью алгоритма рюкзака	2	2	Примеры построения шифрования с помощью алгоритма рюкзака	10				[1,4]
	ИТОГО	16	16		76				

Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение криптошифрования в кольце Z_{pq} для конкретных p, q	Практическое	2	Диалог	Использование на проекторе таблицы умножения в кольце Z_{pq}
2	Построение (n, k) -пороговой схемы разделения секрета для конкретных n, k	Практическое	2		Использование на проекторе таблицы умножения и сложения для формирования взаимно простых модулей
3	Примеры построения схем разделения секрета	Практическое	2		Использование на проекторе таблицы умножения и сложения для применения китайской теоремы при построении

					схемы разделения секрета
--	--	--	--	--	--------------------------

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

№	Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре
Основная литература:	
1.	Ященко В.В. Введение в криптографию. М.: МЦНМО. 2012. 352 с.
2.	Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005
3.	Алферов А.П. и др. Основы криптографии. – М. Гелиос АРВ. 2005.480 с.
4.	Ноден П., Ките К. Алгебраическая алгоритмика. – М. Мир. 2007. 720 с.
5.	Коблиц Н. Курс теории чисел и криптографии. – М. ТВП. 2007. 261с.
6.	Кострикин А.И. Введение в алгебру. Ч.1-3 – М. МЦНМО. 2009. 838с.
Дополнительная литература	
7.	Баскаков А.Г. Лекции по алгебре. Изд-во ВГУ.2014.
8.	Кострикин А.И. Сборник задач по алгебре.-М. МЦНМО. 2009. 408 с.
Электронный ресурс	
9.	Кострикин А.И. Введение в алгебру http://math-portal.ru/678-vvedenie-v-algebru-chast-3-osnovnye-struktury-kostrikin-ai-3-e-izdanie.html
10.	Коблиц Н. Курс теории чисел и криптографии. http://math-portal.ru/tags/%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F/

Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

дисциплины «Алгебраические методы в криптографии»

Направление подготовки магистра 01.04.01 МАТЕМАТИКА Программа «Алгебра»

4. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах:

алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике. Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин:

алгебра, теория групп, криптография, защита информации,

5. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к дисциплинам профессиональной цикла, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, программа «Алгебра».

Дисциплина изучается в течение двух семестров.

6. Цели изучения дисциплины

Целью курса является изучение методов, задач теории групп и колец, криптографии, коды, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Алгебраические методы в криптографии» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность к абстрактному мышлению, анализу, синтезу (ОК-1);
- Готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения (ОК-2);
- Способность к применению методов математического и алгоритмического моделирования при решении теоретических и прикладных задач (ПК-4);
- Способность к собственному видению прикладного аспекта в строгих математических формулировках (ПК-6).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие студентов, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Алгебраические методы в криптографии»:

Студент должен знать

- основы теории групп;
- основы теории полей;
- основы теории колец;

- блочные шифры;
- симметричные криптосистемы;
- асимметричные криптосистемы;
- коды шифрования.

Студент должен уметь:

- применять полученные методы и модели к решению типовых и практических задач с использованием аппарата алгебры, криптографии, основных алгебраических структур (группы, кольца, поля);
- шифрующих кодов;
- пользоваться формулами и теоремами теории групп и теории полей, строить критерии для проверки гипотез;
- пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
- применять полученные знания для изучения других дисциплин.

Студент должен владеть:

- навыками применения криптографических алгоритмов и алгебраических методов для решения различных прикладных задач.

4. Формы работы магистров

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 5 курса,

читается в 9, 10 семестрах

Лекционные занятия – 18/-

Практические занятия – 18/16 ч

Самостоятельная работа – 36/56 ч

В интенсивной форме: практические занятия – 4ч

зачет в 9,10 семестрах

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А., ст.преп. Джусоева Н.А.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Алгебраические методы в криптографии» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по каждому модулю, зачета и экзамена, также предусматривающего набор необходимого количества баллов.

6. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрены зачеты (9, 10 семестры).

7. Тематический план курса

9 семестр

Но мер нед	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия	Самостоятельная работа студентов	Формы контроля	Количество о баллов	Литература
------------	---	---------	----------------------------------	----------------	---------------------	------------

ели		л	пр	Содержание	Часы		min	max	
1	История криптографии	2		.					[1,3]
2	Примеры шифров и криптографических систем	2	4	Шифры простой подстановки и перестановки, усложненные комбинированные шифры	8				[1,4]
3	Использование алгебраического аппарата в криптографии	2							[1,4,5]
4	Симметричные криптографические системы	2	2	Примеры симметричных криптографических систем	4				[1,3]
5	Асимметричные криптографические системы	2	2	Примеры асимметричных криптографических систем	4				[1,3]
6	Определение группы. Примеры.	2	2	Примеры конечных групп	4				[2,6,8]
7	Подгруппы. Примеры подгрупп.	2	2	Примеры неизоморфных конечных групп	4				[2,6,8]
8	Фактор-группа. Примеры	2	2	Примеры бесконечных групп, фактор-группы которых конечны	4				[2,6,8]
9	Гомоморфизмы. Примеры.	2	4	Примеры гомоморфизмов	8				[2,6,8]
	ИТОГО	18	18		36				

10 семестр

Номер недели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия		Самостоятельная работа студентов		Формы контроля	Количество баллов		Литература
		л	пр	Содержание	Часы		min	max	
1	Теоремы о гомоморфизме.		2	Примеры применения теорем о гомоморфизме.	6				[2,6,8]
2	Действие группы на множестве. Стабилизатор.		2	Примеры действия группы на множестве. Стабилизаторы	10				[2,6,8]
3	Теоремы Эйлера и Ферма и обращение криптографического шифрования		2	Примеры применения теорем Эйлера и Ферма для построения шифрования	10				[2, 5]
4	Китайская теорема об остатках		2	Примеры применения китайской	10				[4, 5]

				теоремы об остатках					
5	Криптографическая система RSA		2	Обоснование криптографической системы RSA и примеры открытого шифрования	5				[4, 5]
6	Электронная подпись		2	Формирование электронной подписи и примеры электронной подписи	5				[4, 5]
7	Схема разделения секрета		2	Пример применения схемы разделения секрета на задаче о принятии решения при отсутствии руководителя	5				[1,4]
8	Шифрование с помощью алгоритма рюкзака		2	Примеры построения шифрования с помощью алгоритма рюкзака	5				[1,4]
	ИТОГО		16		56				

Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение криптошифрования в кольце Z_{pq} для конкретных p, q	Практическое	2	Диалог	Использование на проекторе таблицы умножения в кольце Z_{pq}
2	Построение (n, k) -пороговой схемы разделения секрета для конкретных n, k	Практическое	2		Использование на проекторе таблицы умножения и сложения для формирования взаимно простых модулей
3	Примеры построения схем разделения секрета	Практическое	2		Использование на проекторе таблицы умножения и сложения для применения китайской теоремы при построении схемы разделения секрета

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

№	Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре
Основная литература:	
11.	Ященко В.В. Введение в криптографию. М.: МЦНМО. 2012. 352 с.
12.	Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005
13.	Алферов А.П. и др. Основы криптографии. – М. Гелиос АРВ. 2005.480 с.
14.	Ноден П., Ките К. Алгебраическая алгоритмика. – М. Мир. 2007. 720 с.
15.	Коблиц Н. Курс теории чисел и криптографии. – М. ТВП. 2007. 261с.
16.	Кострикин А.И. Введение в алгебру. Ч.1-3 – М. МЦНМО. 2009. 838с.
Дополнительная литература	
17.	Баскаков А.Г. Лекции по алгебре. Изд-во ВГУ.2014.
18.	Кострикин А.И. Сборник задач по алгебре.-М. МЦНМО. 2009. 408 с.
Электронный ресурс	
19.	Кострикин А.И. Введение в алгебру http://math-portal.ru/678-vvedenie-v-algebru-chast-3-osnovnye-struktury-kostrikin-ai-3-e-izdanie.html
20.	Коблиц Н. Курс теории чисел и криптографии. http://math-portal.ru/tags/%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F/

Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Действительный анализ»

для подготовки магистра
по направлению 01.04.01 Математика
программа «Алгебра»

1. Требования к студентам

Изучение данной дисциплины базируется на следующих дисциплинах: «Математический анализ», «Дифференциальные уравнения», «Функциональный анализ». Студенты должны владеть знаниями и компетенциями, соответствующими программам перечисленных дисциплин.

2. Краткая характеристика данной дисциплины, ее особенности

Изложение основ современного математического анализа, нацеленное на использование основных результатов и методов при решении прикладных задач. Основная цель курса - дать возможность студенту не только ознакомиться с современным состоянием этой теории, но и приобрести навыки применения представленных результатов на практике, а также необходимую подготовку для осознанного чтения современной литературы по анализу.

Предлагаемый курс изучается в течение двух семестров. Изложение опирается на теорию интеграла Лебега. Сама теория интеграла Лебега излагается в конспективной манере. Определяется понятие меры, приводятся определения измеримого множества и интеграла Лебега относительно меры, доказывается теорема о построении меры по внешней мере. Дается вывод основных теорем теории интеграла Лебега (теоремы о предельном переходе и теорема Фубини.) Спецкурс ориентирован на творчески работающего слушателя. Он позволит студенту получить первое представление о теории обобщенных функций и о соболевских классах функций. В курсе детально рассматриваются некоторые вопросы, касающиеся соболевских пространств.

Программа рассчитана на магистров 1-го курса факультета математики и информационных технологий.

Дисциплина изучается в течение двух семестров.

3. Цели изучения дисциплины

В результате изучения специальной дисциплины «Действительный анализ» студент должен:

- знать** основные понятия и факты теории, входящие в программу курса,
- уметь** применять аппарат вариационного исчисления при решении задач,
- обладать навыками:**

- ясного, точного, грамотного изложения своих мыслей в устной и письменной речи, использования различных языков математики (словесного, символического, графического), свободного перехода с одного языка на другой для иллюстрации, интерпретации, аргументации и доказательства;
- проведения доказательных рассуждений, аргументации, выдвижения гипотез и их обоснования;
- дальнейшего использования накопленных знаний для решения той или иной проблемы теоретической и прикладной математики.
- поиска, систематизации, анализа и классификации информации, использования разнообразных информационных источников, включая учебную и справочную литературу.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- Способность к абстрактному мышлению, анализу, синтезу (ОК-1);
- Способность к применению методов математического и алгоритмического моделирования при решении теоретических и прикладных задач (ПК-4);

- Способность к собственному видению прикладного аспекта в строгих математических формулировках (ПК-6).

4. Формы работы студентов

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 5 курса,

читается в 9, 10 семестрах

Лекционные занятия – 18/-

Практические занятия – 18/34 ч

Самостоятельная работа – 36/2 ч

зачет в 9 семестре

экзамен в 10 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: доцент Кулаев Р.Ч.

5. Виды контроля

Учебным планом по данной дисциплине предусмотрен зачет в девятом семестре и экзамен в десятом. В течение изучения курса студентам предлагается ряд задач. Зачет выставляется по результатам решенных задач. Экзамен проводится по всем темам курса. Контроль знаний студентов осуществляется в форме тестирования по каждому модулю и экзамена, также предусматривающего набор необходимого количества баллов.

6. Тематический план курса

Распределение разделов по аудиторным часам (ЛЗ – лекционные занятия, ПЗ – практические занятия, СР – самостоятельная работа, АЗ – аудиторные занятия, ЛАБЗ – лабораторные занятия)

№	Название темы	АЗ			СР
		ЛЗ	ПЗ	ЛАБЗ	
1.	Свертка функций: Свертка в физических задачах. Свойства свертки. Дельтаобразные семейства функций. Аппроксимационная теорема Вейерштрасса.	2	8		6
2.	Пространства L^p: Определение пространств L^p . Неравенство Йенсена. Неравенство Гёльдера. Неравенство Минковского. Неравенство Ханнера. Дифференцируемость нормы. Полнота пространств L^p . Проекция на выпуклые множества. Непрерывные линейные функционалы и слабая сходимость. Линейные функционалы разделяют. Полунепрерывность снизу для норм. Принцип равномерной ограниченности. Сильно сходящиеся выпуклые комбинации. Двойственное пространство к L^p . Свертка. Аппроксимация функциями из \tilde{N}^∞ . Сепарабельность пространства L^p . Ограниченные последовательности имеют	4	10		15

	слабые пределы. Аппроксимация функциями из \tilde{N}^∞ .				
3.	Преобразование Фурье: Определение L^1 -преобразования Фурье. Преобразование Фурье функции Гаусса. Теорема Планшереля. Определение L^2 -преобразования Фурье. Формула обращения преобразования Фурье. Преобразование Фурье в L^p . Точное неравенство Хаусдорфа — Юнга. Теорема о свертках.	3	10		13
4.	Обобщенные функции: Введение. Основные функции (пространство $D(\Omega)$). Определение обобщенных функций и сходимость. Локально суммируемые функции L^p_{loc} . Функции однозначно определяются обобщенными функциями. Производные обобщенных функций. Определение пространств $W^{1,p}_{loc}$ и $W^{1,p}$. Перестановочность обобщенных функций со свертками. Основная теорема исчисления обобщенных функций. Эквивалентность классической и обобщенной производных. Обобщенные функции с нулевыми производными суть константы. Умножение и свертка распределений с функциями класса \tilde{N}^∞ . Линейная зависимость обобщенных функций. Плотность \tilde{N}^∞ в $W^{1,p}_{loc}$. Дифференцирование сложной функции. Производная модуля. Минимум и максимум функций из $W^{1,p}$ принадлежат $W^{1,p}$.	4	10		2
5	Пространства Соболева: Определение пространства H^1 . Пространства Соболева. Полнота пространств Соболева. Умножение на гладкие функции. Аппроксимация. Продолжение. Следы.	2	6		2
6	Неравенства Соболева: Неравенства Соболева. Компактность. Неравенства Пуанкаре. Характеризация Фурье. Пространство H^{-1} . Пространства функций, зависящих от времени.	4	6		
	ИТОГО:	18	52		38
	Всего (часы): (аудиторные занятия и самостоятельная работа)	108			

СПИСОК ЛИТЕРАТУРЫ

Основная литература

1. Adams, R. A. *Sobolev spaces*, Academic Press, New York, 2006.
2. Гольдштейн, В. М., Решетняк, Ю. Г., *Введение в теорию функций с обобщенными производными и квазиконформные отображения*, Наука, Москва, 2010.
3. Гилбарг, Д., Трудингер, Н., *Эллиптические дифференциальные уравнения с частными производными второго порядка*, Наука, Москва, 1989.
4. Данфорд, Н., Шварц, Дж. Т., *Линейные операторы. Самосопряженные операторы в гильбертовом пространстве*, Мир, Москва, 2004.
5. Дубровин, Б. А., Новиков, С. П., Фоменко, А. Т., *Современная геометрия. Методы и приложения*, Наука, Москва, 2009.
6. Зорич, В. А., *Математический анализ*, МЦНМО, Москва. Т. 1,2, 2007.
7. Канторович, Л. В., Акилов, Г. П., *Функциональный анализ*, ВНУ, 2004.
8. Либ, Э., Лосс, М., *Анализ*. Новосибирск, Научная книга, 2005.
9. Мазья, В. Г., *Пространства С. Л. Соболева*, ЛГУ, Ленинград, 1985.
10. Полна, Г., Сеге, Г., *Изопериметрические неравенства в математической физике*, Физматгиз, Москва, 1962.
11. Рид, М., Саймон, В., *Методы современной математической физики*, Т. 1, 2, Мир, Москва, 1977, 1978.
12. Рудин, У., *Функциональный анализ*, Мир, Москва, 2005.
13. Соболев, С. Л., *Некоторые применения функционального анализа в математической физике*, 1-е изд., ЛГУ, 1950; 2-е изд., Новосибирск, 1958; 3-е изд., Наука, Москва, 1988.
14. Соболев, С. Л., *Введение в теорию кубатурных формул*, Наука, Москва, 1974.
15. Соболев, С. Л., *Избранные вопросы теории функциональных пространств и обобщенных функций*, Наука, Москва, 1989.
16. Хёрмандер, Л., *Анализ линейных дифференциальных операторов с частными производными*, Т. 1-4, Мир, Москва, 1985.
17. Эдварде, Р., *Функциональный анализ. Теория и приложения*, Мир, Москва, 1969.
18. Эванс, Л. К., *Уравнениями с частными производными*, Новосибирск, Научная книга, 2006.

Дополнительная литература

19. Brezis, H., *Analyse fonctionnelle: Theorie et applications*, Masson, Paris, 1983.
20. Бесов, О. В., Ильин, В. П., Никольский, С. М., *Интегральные представления функций и теоремы вложения*, Наука, Москва, 1997.
21. Гельфанд, И. М., Шилов, Г. Е., *Обобщенные функции и действия над ними*, Физматгиз, Москва, 1950.
22. Гельфанд, И. М., Шилов, Г. Е., *Пространства основных и обобщенных функций (Обобщенные*

- функции, вып. 2), Гос. физ.-мат. изд., Москва, 1958.
23. Гельфанд, И. М., Шилов, Г. Е., *Некоторые вопросы теории дифференциальных уравнений* (Обобщенные функции, вып. 3), Физматгиз, Москва, 1958.
 24. Гельфанд, И. М., Виленкин, Н. Я., *Некоторые применения гармонического анализа. Оснащенные гильбертовы пространства* (Обобщенные функции, вып. 4), Физматгиз, Москва, 1961.
 25. Гельфанд, И. М., Граев, М. И., *Интегральная геометрия и связанные с ней вопросы теории представлений* (Обобщенные функции, вып. 5), Физматгиз, Москва, 1962.
 26. Гельфанд, И. М., Граев, М. И., Пятецкий-Шапиро, И. И., *Теория представлений и автоморфные функции* (Обобщенные функции, вып. 6). Физматгиз, Москва, 1966.

Интернет-ресурсы

Базы данных, информационно-справочные и поисковые системы

- Информационный математический портал вся математика в одном месте:

<http://allmath.ru/mathan.htm>

- <http://bookfi.org> - электронная библиотека

- <http://gen.lib.rus.ec> - библиотека Genesis

- <http://www.twirpx.com> - электронная библиотека

- <http://mathnet.ru> - общероссийский математический портал

- <http://smath.ru/lib/> - полнотекстовые коллекции журналов (библиотека ЮМИ ВНИЦ РАН)

АННОТАЦИЯ

дисциплины «Дополнительные главы алгебры»

Направление подготовки магистра 01.04.01 МАТЕМАТИКА Программа «Алгебра»

7. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике. Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин:

алгебра, теория групп, криптография, защита информации.

8. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к дисциплинам по выбору, обеспечивающих подготовку магистра по направлению 01.04.01 Математика программа «Алгебра».

Дисциплина изучается в течение двух семестров.

9. Цели изучения дисциплины

«Дополнительные главы алгебры» - это специальный курс являющийся неотъемлемой частью широкого круга предметов по математике. Он находится в числе дисциплин, на которых строится все здание современной прикладной математической науки. Целью освоения дисциплины «Дополнительные главы алгебры» является формирование и развитие абстрактного мышления студентов в процессе изучения основных понятий и структур используемых, во всех остальных математических дисциплинах, связанных с теоретическими и прикладными вопросами алгебры. Программа предназначена для магистров первого курса математического факультета.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Дополнительные главы алгебры» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность создавать и исследовать новые математические модели в естественных науках (ОПК-2);
- Способность к интенсивной научно-исследовательской работе (ПК-1).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие студентов, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Дополнительные главы алгебры»:

Студент должен знать основные структуры и понятия алгебры; основные теоремы и конструкции; методы и способы решения задач.

Студент должен уметь: строить абстрактные математические модели; решать типовые задачи по всем изучаемым разделам; применять алгебраические модели для решения прикладных задач.

Студент должен владеть: представление об основных структурах алгебры; понятие о проблемах современной алгебраической науки; навыки самостоятельной работы с учебной, методической и научной литературой.

4. Формы работы магистров

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 5 курса,

читается в 9 семестре

Лекционные занятия – 18ч

Практические занятия – 18ч

Самостоятельная работа – 54 ч

В интенсивной форме: практические занятия – 4ч

зачет в 9 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А., ст.преп. Джусоева Н.А.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Дополнительный главы алгебры» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по каждому модулю, зачета и экзамена, также предусматривающего набор необходимого количества баллов.

6. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен зачет (9 семестр). Максимальное количество баллов, которое может набрать студент, **100**.

За выполнение заданий текущего и промежуточного контроля студент может набрать максимальное количество баллов:

За первый модуль – 50 баллов (текущая работа Т1- 20 баллов и компьютерный тест М1 - 30 баллов).

За второй модуль –50 баллов (текущая работа Т2- 20 баллов и компьютерный тест М2 - 30 баллов).

7. Тематический план курса

Номер недели 9 семI	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия		Самостоятельная работа Студентов		Формы контроля	Количество баллов		Литература
		л	пр	Содержание	Часы		Min	max	
1-2	Группы. Примеры подгрупп. Подгруппы классических групп.	2	2	История возникновения понятия «группа». Группы симметрий.	4	Вопросы На зачете			(2,4)

3-4	Фактор –группа. Примеры построения фактор-групп.	2	2	Множество классов вычетов. Z/nZ	4	Вопросы на зачете			(2,4)
5-6	Гомоморфизм. Примеры. Гомоморфизмы ,связанные с линейными группами над кольцами.	2	2	Виды отображений. Примеры.	4	Вопросы на зачете			(2,4)
7-8	Теоремы о гомоморфизме. Примеры применения теорем о гомоморфизме	2	2	Ядро и образ гомоморфизма. Построение различных гомоморфных отображений.	4	Вопросы на зачете			(2,4)
9-10	Линейные группы. Полная линейная группа над кольцом и её подгруппы.	2	2	Матрицы специального вида. Полная линейная группа над полем.	4	Вопросы на зачете			(2,4)
11-12	Конечные группы	2	2	Группа S_n . Знакопеременная группа.		Вопросы на зачете			(2,4)
13-14	Теоремы Силова	2		Порядок элемента. Циклические группы. Теорема Лагранжа и примеры применения.	4	Вопросы на зачете			(2,4)
15-16	Действие групп на множестве			Коммутант .Свойства.	4	Вопросы на зачете			(2,4)
17-18	Стабилизатор. Примеры стабилизаторов.			Прямое произведение. Полупрямое произведение.	4	Вопросы на зачете			(2,4)
19	Зачетная неделя. Итого	18	18		54				
	Итого	18	18		54				

Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Конечные группы.	Лекционное	2	Диалог	Индивидуальный опрос.

2	Теоремы Силова	Лекционное	2	Диалог	Индивидуальный опрос.
3	Фактор – группы .Примеры фактор – групп	Практическое	2	Диалог	Индивидуальный опрос,
4	Сети . Примеры сетей.	Практическое	2	Диалог	Индивидуальный опрос.

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Основная литература:

1. Белоногов В.А. Задачник по теории групп. М.: Наука. 2000. 238 с.
2. Койбаев В.А. Основы алгебры. – Владикавказ: СОГУ, 2005(\\icd\books\math\Алгебра и Геометрия) (\\icd\books\math\Алгебра и Геометрия) - 10
3. Койбаев В.А. Подгруппы группы $GL(2,k)$, содержащие нерасщепимый максимальный тор. – Математическая монография. Владикавказ. 2009. 182с.
4. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. СПб.:Лань . 2009. 288с.

Дополнительная литература

5. Баскаков А.Г. Лекции по алгебре. – Воронеж. 2001
 6. Кострикин А.И. Сборник задач по алгебре. – М. Физматлит, 2001.-464с
- Электронный ресурс
7. Кострикин А.И. <http://review3d.ru/kostrikin-a-i-vvedenie-v-algebru-v-3-chastyax>
 8. Каргаполов М.И., Мерзляков Ю.И. <http://www.vixri.ru/?p=1212>
 9. Боревич З.И. Подгруппы полной линейной группы, содержащие группу диагональных матриц//Зап. Науч .семинаров ПОМИ РАН.1976, т.64, с.12-29.

http://www.mathnet.ru/php/archive.phtml?jrnid=zns1&wshow=issue&series=0&year=1976&volume=64&issue=0&option_lang=rus&bookID=492

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

а. Материально-техническое оснащение дисциплины:

Компьютерный класс, доступ к сети Интернет (во время самостоятельной работы), оргтехника, электронная база данных библиотеки СОГУ, лекционные аудитории; кабинет, оснащенный интерактивной доской, проектором.

Рекомендуемые интернет-адреса по курсу «Дополнительные главы алгебры»

1. <http://intuit.ru/>
2. <http://mathnet.ru/>

АННОТАЦИЯ

дисциплины «Избранные главы линейной алгебры»

Направление подготовки магистра 01.04.01 МАТЕМАТИКА Программа «Алгебра»

10. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике. Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин: алгебра, теория групп, криптография, защита информации.

11. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к дисциплинам профессионального цикла, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, программа «Алгебра».

Дисциплина изучается в течение одного семестра.

12. Цели изучения дисциплины

Целью курса является изучение методов, задач теории групп и колец, криптографии, коды, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Избранные главы линейной алгебры» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность создавать и исследовать новые математические модели естественных наук (ОПК-2);
- Способность к организации научно-исследовательских и научно-производственных работ, к управлению научным коллективом (ПК-1).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие студентов, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Избранные главы линейной алгебры»:

Студент должен знать

- основы теории групп;
- основы теории полей;
- основы теории колец;

- блочные шифры;
- симметричные криптосистемы;
- асимметричные криптосистемы;
- коды шифрования.

Студент должен уметь:

- применять полученные методы и модели к решению типовых и практических задач с использованием аппарата алгебры, криптографии, основных алгебраических структур (группы, кольца, поля);
- шифрующих кодов;
- пользоваться формулами и теоремами теории групп и теории полей, строить критерии для проверки гипотез;
- пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
- применять полученные знания для изучения других дисциплин.

Студент должен владеть:

- навыки применения криптографических алгоритмов и алгебраических методов для решения различных прикладных задач.

4. Формы работы магистров

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 6 курса, читается в 11 семестре

Лекционные занятия – -

Практические занятия – 38 ч

Самостоятельная работа – 34 ч

зачет в 11 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А., ст.преп. Джусоева Н.А.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Избранные главы линейной алгебры» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по каждому модулю, зачета и экзамена, также предусматривающего набор необходимого количества баллов.

6. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен зачет (11 семестр).

За выполнение заданий текущего и промежуточного контроля студент может набрать максимальное количество баллов.

7. Тематический план курса

11 семестр

Но мер не де ли	Наименование тем (вопросов), изучаемых по данной дисциплине	Занят ия		Самостоятельна я работа студентов		Форм ы контр оля	Количе ство баллов		Лит ера тур а
		л	пр	Содержание	Ча сы		mi n	ма х	
1- 2	Векторное пространство. Определение, примеры.		4						[1,3]
3- 4	Л.н.с. и л.з.с. Базис. Переход к координатам в другом базисе.		4		4				[1,4]
5- 6	Линейный оператор. Матрица линейного оператора.		4						[1,4 ,5]
7- 8	Ядро и образ линейного оператора.		4		4				[1,3]
9- 10	Собственные значения и собственные векторы.		4		4				[1,3]
11 - 12	Жорданова форма матриц.		4	Примеры конечных групп	4				[2,6 ,8]
13 - 14			4	Примеры неизоморфны х конечных групп	4				[2,6 ,8]
15 - 16	Фактор-группа. Примеры		4	Примеры бесконечных групп, фактор- группы которых конечны	2				[2,6 ,8]
17 - 18	Гомоморфизмы. Примеры.		4	Примеры гомоморфизм ов	4				[2,6 ,8]
19			2						
	ИТОГО		38		34				

Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение криптошифрования в кольце Z_{pq} для конкретных p, q	Практическое	2	Диалог	Использование на проекторе таблицы умножения в кольце Z_{pq}
2	Построение (n, k) -пороговой схемы разделения секрета для конкретных n, k	Практическое	2		Использование на проекторе таблицы умножения и сложения для формирования взаимно простых модулей
3	Примеры построения схем разделения секрета	Практическое	2		Использование на проекторе таблицы умножения и сложения для применения китайской теоремы при построении схемы разделения секрета

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

№	Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре
Основная литература:	
21.	Ященко В.В. Введение в криптографию. М.: МЦНМО. 2012. 352 с.
22.	Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005
23.	Алферов А.П. и др. Основы криптографии. – М. Гелиос АРВ. 2005.480 с.
24.	Ноден П., Ките К. Алгебраическая алгоритмика. – М. Мир. 2007. 720 с.
25.	Коблиц Н. Курс теории чисел и криптографии. – М. ТВП. 2007. 261с.
26.	Кострикин А.И. Введение в алгебру. Ч.1-3 – М. МЦНМО. 2009. 838с.
Дополнительная литература	
27.	Баскаков А.Г. Лекции по алгебре. Изд-во ВГУ.2014.
28.	Кострикин А.И. Сборник задач по алгебре.-М. МЦНМО. 2009. 408 с.
Электронный ресурс	
29.	Кострикин А.И. Введение в алгебру http://math-portal.ru/678-vvedenie-v-algebru-chast-3-osnovnye-strukturny-kostrikin-ai-3-e-izdanie.html

30. Коблиц Н. Курс теории чисел и криптографии.

[http://math-](http://math-portal.ru/tags/%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F/)

[portal.ru/tags/%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F/](http://math-portal.ru/tags/%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F/)

Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

дисциплины «Иностранный язык в профессиональной сфере деятельности»

Направление подготовки магистра 01.04.01 МАТЕМАТИКА Программа «Алгебра»

13. Требования к магистрантам

Приступая к изучению данной дисциплины, студент должен владеть общекультурными знаниями и умениями, формируемыми при изучении основных образовательных программ среднего общего и профессионального образования по социально-гуманитарным и естественным наукам, предусмотренных Госстандартом для общеобразовательной средней школы и общеобразовательных циклов основных образовательных программ (ООП) и соответствует требованиям ФГОС ВО.

14. Краткая характеристика данной дисциплины, ее особенности

Особенность дисциплины «Иностранный язык» /английский язык» заключается в том, что она входит в базовую часть «Дисциплины» блока 1 федерального государственного образовательного стандарта высшего профессионального образования.

Предметом дисциплины «Иностранный язык» на неязыковых факультетах университета является изучение иноязычной культуры, фонетического материала, необходимого для коррекции и постановки правильного произношения и интонации, грамматического и лексического материала, необходимого для формирования коммуникативно-познавательной компетенции обучающихся в наиболее распространенных ситуациях официальной и неофициальной сфер общения во всех видах речевой деятельности (аудирование, говорение, чтение, письмо). Дисциплина изучается в течение трех семестров.

Программа курса построена на основе Учебно-методического комплекса «Иностранный язык» в соответствии с Федеральным государственным образовательным стандартом по направлению 01.04.01 Математика.

Целью освоения дисциплины «Иностранный язык» /английский язык» является: совершенствование лингвистической и коммуникативной компетенции студентов средствами обучения иностранного языка на основе социально-бытовых тем письменной и устной речи и текстов по специальности.

Данная цель раскрывается в единстве ее взаимосвязанных компонентов: воспитательного, развивающего, образовательного и практического.

Воспитательный компонент заключается в формировании у студентов уважения и интереса к культуре и народу страны изучаемого языка; воспитании культуры общения; поддержании интереса к учению и формированию познавательной активности; воспитании потребности в практическом использовании иностранного языка в различных сферах деятельности.

Развивающий компонент предусматривает развитие языковых, интеллектуальных и познавательных способностей, ценностных ориентаций студентов, их готовности к коммуникации. В целом развивающий компонент предусматривает гуманистическое развитие личности обучаемых.

Образовательный компонент выражается в расширении эрудиции студентов, их лингвистического, филологического, духовного и общего кругозора.

Указанные воспитательный, развивающий и образовательный компоненты достигаются в процессе и на основе достаточного практического владения студентами иностранным языком.

Практический компонент заключается в формировании умений и развитии навыков устной и письменной речи на иностранном языке, обеспечивающих основные познавательные-коммуникативные

потребности студентов и возможность приобщения их к культурным ценностям народа-носителя иностранного языка.

1.4. Учебные задачи дисциплины:

- формирование речевых экспрессивно-лексических и грамматических навыков на коммуникативном уровне;
- совершенствование необходимых для неязыковых специальностей фонетических навыков;
- совершенствование умений и навыков говорения на социально-бытовые темы;
- формирование навыков и развитие умений письма;
- формирование навыков и развитие умений в диалогической и монологической формах общения;
- формирование и развитие умений в переводе со словарем;
- обучение чтению текста про себя, понимание основного содержания текста средней трудности без использования словаря;
- обучение письменной речи (написание диктантов, сочинений, рефератов по заданной и свободной темам);
- дальнейшее формирование и развитие умений и навыков ценностно-смыслового анализа текста;
- совершенствование умений и навыков краткого изложения выводов по содержанию текста;
- умение использовать грамматические структуры для перевода;
- обучение исправлению ошибок в устном и письменном сообщениях;
- обучение реферированию художественных, аутентичных и др. текстов и неадаптированных текстов средней трудности.
- В задачи курса также входят функционально-стилистические аспекты информации, включающие лингвострановедческие знания, что имеет большое значение для повышения мотивации к овладению иностранным языком, удовлетворения познавательных интересов обучающихся, а также их потребностей в общении на иностранном языке.

1.5. Требования к результатам освоения дисциплины

Целью курса является овладение студентами языковой и коммуникативной компетенциями, необходимыми для активного применения иностранного языка в коммуникации и межличностном общении.

В результате освоения дисциплины формируются следующие компетенции:

- Готовность к коммуникации в устной и письменной формах на государственном языке Российской Федерации и иностранном языке для решения задач профессиональной деятельности (ОПК-4);
- Способность к интенсивной научно-исследовательской работе (ПК-1).

В результате освоения дисциплины студент должен:

Знать:

- структуру языка и правила ее функционирования в процессе иноязычного обучения;
- основные особенности социально-культурного развития страны;
- особенности изучаемого языка в ходе истории и на современном этапе;
- особенности основных правил речевого этикета в изучаемом языке;
- принципы получения и обработки информации, необходимой для работы с иноязычными текстами профессиональной направленности;
- методические приемы обучения иностранному языку;
- методы и приемы лингвистического и переводческого анализа специализированного текста;
- принципы ведения дискуссий в условиях плюрализма мнений и основные способы разрешения конфликтов на изучаемом языке;

- лексический минимум (5000 учебных лексических единиц) в объеме, необходимом для возможности профессионально ориентированной коммуникации и получения информации из зарубежных источников;
- базовую грамматику и основные грамматические явления, характерные для профессиональной речи;
- основную терминологию по специальности на иностранном языке;

Уметь:

- воспринимать и порождать иноязычную речь в соответствии с условиями речевой коммуникации;
- правильно организовывать свой труд в процессе поиска и обработки информации;
- грамотно оформлять результаты своих исследований, логично отстаивать свою точку зрения, а также быть способным осуществлять деловое общение, готовиться к публичным выступлениям;
- вести диалогическую и монологическую речь с использованием наиболее употребительных и относительно простых лексико-грамматических средств в основных коммуникативных ситуациях неофициального и официального общения; понимать диалогическую и монологическую речь в сфере бытовой и профессиональной коммуникации; читать и понимать несложные прагматические тексты и тексты по широкому и узкому профилю специальности;
- осуществлять свое речевое поведение, опираясь на полученные лингвострановедческие знания, переводить тексты общего содержания средней сложности;
- осуществлять педагогическое общение (управление интеллектуальной деятельностью обучаемых, стимулирование речевой деятельности, организация речевой деятельности и ее контроль);
- использовать не менее 900 терминологических единиц и терминологических элементов в рамках устной и письменной коммуникации;
- обмениваться информацией и профессиональными знаниями с коллегами и клиентами устно и письменно, обладать способностью к переговорам на изучаемом языке;
- понимать сущность и значение информации в развитии современного общества;
- получать и обрабатывать информацию из различных источников;
- интерпретировать, структурировать и оформлять информацию в доступном для других видов;

Владеть:

- навыком устной и письменной речи на иностранном языке в рамках лексической тематики программы;
- навыком аудирования;
- навыком фонетически и интонационно правильного оформления своей речи (в соответствии с условиями речевой коммуникации, прежде всего, с учетом адресата и характера диалога);
- навыком техники перевода, а также умением описания, рассуждения, ценностного анализа художественного, научного, научно-популярного, газетно-публицистического и официально делового текстов;
- одним из иностранных языков на уровне социального общения и бытового общения.

Формы работы студентов

Формами работы студентов являются практические занятия, выполнение модульных контрольных работ, контрольное тестирование, самостоятельная работа. Использование аудио-, видео- и компьютерных средств для выполнения практических задач по обучению иностранному языку.

1.6. Виды контроля

Дисциплина «Иностранный язык» /английский язык/ по направлению подготовки 01.04.01 Математика предусматривает практические занятия в течение 3-х семестров. Учебным планом по данной дисциплине предусмотрены зачеты в конце 9-10 семестров и экзамен в конце 11 семестра.

Контроль успеваемости студентов на протяжении всего курса обучения распределяется между *текущим и промежуточным*.

В процессе изучения дисциплины «Иностранный язык» /английский/ осуществляется рейтинговая система оценки знаний студентов, которая предусматривает:

- оценку работы студентов на каждом практическом занятии;
- выполнение домашней работы;
- блиц - опросы на практических занятиях, тестирование, контрольные работы.

В процессе систематической работы студенты набирают баллы, что позволяет каждому студенту, набравшему достаточное количество баллов, получить оценку без сдачи зачета или экзамена. Рейтинговая система разнообразит, активизирует занятия, позволяет более дифференцированно подходить к оценке знаний, дисциплинирует студентов, более полно раскрывает творческий потенциал обучающегося.

Формами текущего контроля являются: индивидуальные ответы, блиц-опросы. Формами промежуточного контроля являются: тестирование, рейтинг. Целью данного вида контроля является закрепление пройденного материала. Время, отводимое на выполнение теста/контрольной работы – 40-50 минут.

6. Методика формирования результирующей оценки

Минимальное количество баллов, которое студент может набрать в ходе изучения курса для получения зачета, – 56; максимальное – 100. Баллы складываются из следующих показателей: за работу в аудитории – 5 баллов, за устную домашнюю работу – 8 баллов, за письменную домашнюю работу – 7 баллов – всего до 20 баллов, за каждое рубежное тестирование – до 30 баллов на каждой рубежной контрольной, до 60 баллов на устном ответе.

Форма контроля	Мин. кол-во баллов	Макс. кол-во баллов
<i>Текущая оценка</i> студента в течение 1-7 недели состоит из: <ul style="list-style-type: none"> • <i>Работа в аудитории</i> • <i>Устная домашняя работа</i> • <i>Письменная домашняя работа</i> 	0	20 5 8 7
<i>1-ое рубежное тестирование</i>	0	30
<i>Текущая оценка</i> студента в течение 9-15 недели состоит из: <ul style="list-style-type: none"> • <i>Работа в аудитории</i> • <i>Устная домашняя работа</i> • <i>Письменная домашняя работа</i> 	0	20 5 8 7
<i>2-ое рубежное тестирование</i>	0	30
Итого	0	100

АННОТАЦИЯ

дисциплины «Коды, исправляющие ошибки»

Направление подготовки магистра

01.04.01 МАТЕМАТИКА

Профиль

«Алгебра»

15. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебры и геометрии, криптография, теория групп.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин: дискретная математика, теория вероятностей, криптография, защита информации.

16. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к блоку Б1.В.ДВ.1.1 Дисциплины (модули). Вариативная часть. Дисциплины по выбору, обеспечивающих подготовку магистра по направлению 01.04.01 Математика профиль «Алгебра».

Дисциплина изучается в течение одного семестра.

17. Цели изучения дисциплины

Целью курса является формирование у магистрантов понятий, знаний и компетенций, позволяющих строить и анализировать модели систем реального мира с помощью структур и их свойств.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Коды, исправляющие ошибки» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность создавать и исследовать новые математические модели в естественных науках (ОПК-2);
- Способность к собственному видению прикладного аспекта в строгих математических формулировках (ПК-6).

Учебные задачи дисциплины:

В результате изучения дисциплины «Коды, исправляющие ошибки»:

Студент должен знать

- Основные понятия теории многочленов;
- перестановки;
- линейные пространства;
- линейные операторы и линейные отображения;
- теорию матриц;
- основы теории групп;
- основы теории полей;
- основы теории колец
- конечные поля;
- неприводимые многочлены над полем из двух элементов
- кодирование с помощью 0-1-матриц
- расстояние между словами

Студент должен уметь:

- применять полученные методы и модели к решению типовых и практических задач теории кодирования, строить матрицы, позволяющие при кодировании распознавать и исправлять ошибки при передаче информации,
- применять полученные знания для изучения других дисциплин.

Студент должен владеть:

- навыки применения алгебраических методов для решения различных прикладных задач, связанных с распознаванием слов, в которых допущено некоторое количество ошибок, навыки построения и исследования различных алгебраических структур.

4. Формы работы магистров

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 2 курса,

читается в 11 семестре

Лекционные занятия – 0 ч

Практические занятия – 18 ч

Самостоятельная работа – 54 ч

зачет в 11 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А., ст.преп. Джусоева Н.А.

8. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Коды, исправляющие ошибки» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по зачету, также предусматривающего набор необходимого количества баллов.

9. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен зачет. Максимальное количество баллов, которое может набрать студент, **100**.

За выполнение заданий текущего и промежуточного контроля студент может набрать максимальное количество баллов:

За первый модуль – 50 баллов (текущая работа Т1- 20 баллов и компьютерный тест М1 - 30 баллов).

За второй модуль – 50 баллов (текущая работа Т2- 20 баллов и компьютерный тест М2 - 30 баллов).

10. Тематический план курса

11 семестр

Номер	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия	Самостоятельная работа студентов	Формы контроля	Количество баллов	Литература
-------	---	---------	----------------------------------	----------------	-------------------	------------

де ли		л	пр	Содержание	Ча сы		mi n	ма х	
1	Группы, кольца, поля		2	Построение конкретных групп, колец, полей, необходимых при кодировании.	6				[1, 4, 7]
2	Неприводимые многочлены над полем из двух элементов		2	Построение неприводимых многочленов над полем из двух элементов.	10				[3, 7]
3	Канал связи.		2	Изучение каналов связи.	2				[2, 3, 10]
4	Исследование кодов, обнаруживающих и исправляющих ошибки.		2	Исследование связи между кодами обнаруживающими и исправляющими ошибки	10				[2, 3, 10]
5	Блочные коды.		2	Изучение блочных кодов.	2				[2, 3, 10]
6	Проблема кодирования.		2	Изучение проблем, связанных с кодированием слов.	2				[2, 3, 10]
7	Расстояние между словами, необходимое для эффективного кодирования		2	Изучение конкретных примеров расстояний между словами, необходимого для эффективного кодирования.	10				[2, 3, 10]

8	Метрика Хэмминга и метрика Ли.		2	Изучение метрики Хэмминга и метрики Ли	2				[2, 3]
9	Описание линейных блочных кодов при помощи матриц. Описание древовидных линейных кодов при помощи матриц.		2	Построение матриц над полем из двух элементов, кодирующих с исправлением ошибок.	10				[2, 3, 10]
ИТОГО			18		54				

1.6 Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение матриц над полем из двух элементов, кодирующих с исправлением ошибок.	Практическое	2	Диалог	Использование на проекторе таблицы умножения групп матриц над полем из двух элементов
2	Построение неприводимых многочленов над полем из двух элементов	Практическое	2		Использование на проекторе таблицы умножения и сложения в кольцах многочленов
3	Исследование связи между кодами обнаруживающими и исправляющими ошибки	Практическое	2		Использование на проекторе таблицы умножения и сложения в полях из двух

1.7. Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

№ Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре

Основная литература:

1. Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005(\\icd\books\math\Алгебра и Геометрия) (\\icd\books\math\Алгебра и Геометрия) - 10
2. Берлекэмен Э. Алгебраическая теория кодирования – М.: ЕЕ Медиа.2012.478с.
3. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М. Мир. 1976
4. Белоногов В.А. Задачник по теории групп. М.: Наука. 2000. 238 с.

Дополнительная литература

5. Чечета С.В. Введение в дискретную теорию информации и кодирования. – М.:МЦНМО. 2011. 224 с.
6. Баскаков А.Г. Лекции по алгебре. – Воронеж. 2001
7. Кострикин А.И. Сборник задач по алгебре. – М. Физматлит, 2001.-464с

Электронный ресурс

8. Фаддеев Д.К., Соминский И.С. Задачи по высшей алгебре.
<http://math-portal.ru/261-zadachi-po-vysshey-algebre-13-e-izdanie.html>
9. Каргаполов М.И., Мерзляков Ю.И. <http://www.vixri.ru/?p=1212>
10. Биркгоф Г, Барти Т. Современная прикладная алгебра. СПб.; лань. 2005
<http://math-portal.ru/805-sovremennaya-prikladnaya-algebra-birkgof-g.html>

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

дисциплины «Компьютерные технологии в науке и образовании»

Направление подготовки магистра
01.04.01 МАТЕМАТИКА
Программа «Алгебра»

18. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: школьный курс информатики (программа средней общеобразовательной школы), «Компьютерные науки (Информатика)», «Компьютерные науки (Практикум на ПК)». Студенты должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике.

2. Краткая характеристика дисциплины

Настоящая дисциплина относится к дисциплинам профессионального цикла, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, программа «Алгебра».

Дисциплина изучается в течение трех семестров.

3. Цели изучения дисциплины

Целью курса является систематизация и расширение знаний в области новых информационных и телекоммуникационных технологий; подготовка слушателей к использованию современных компьютерных технологий в научных исследованиях и в методическом обеспечении преподавательской деятельности.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Готовность самостоятельно создавать прикладные программные средства на основе современных информационных технологий и сетевых ресурсов (ОПК-3);
- Готовность к коммуникации в устной и письменной формах на государственном языке Российской Федерации и иностранном языке для решения задач профессиональной деятельности (ОПК-4);
- Готовность руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия (ОПК-5);
- Способность к творческому применению, развитию и реализации математически сложных алгоритмов в современных программных комплексах (ПК-5);
- Способность к применению методов математического и алгоритмического моделирования при анализе экономических и социальных процессов, задач бизнеса, финансовой и актуарной математики (ПК-7);
- Способность формулировать в проблемно-задачной форме не математические типы знания (в том числе гуманитарные) (ПК-8);
- Способность к преподаванию физико-математических дисциплин и информатики в общеобразовательных организациях, профессиональных образовательных организациях и организациях дополнительного образования (ПК-10).

Основными **задачами** курса является:

- систематизация и углубление знаний о различных видах информации и об основных информационных процессах, сопровождающих человека на протяжении всей истории человеческой цивилизации;

- знакомство с новейшими инновационными информационными и коммуникационными технологиями и электронными образовательными ресурсами;
- знакомство с новейшими разработками программного обеспечения; углубление и систематизация знаний об создании программного обеспечения, принципах его функционирования, современных информационных системах;
- ознакомление слушателей с имеющимися в настоящее время компьютерными приложениями, используемыми в научной работе и для создания обучающих приложений;
- формирование представления о новых информационных и технологиях, а также умения осуществлять их анализ с позиции соответствия целям и задачам своей профессиональной деятельности;
- актуализация знаний в области информационной компьютерной техники, полученных при изучении общепрофессиональных дисциплин, дисциплин предметной подготовки, курсов по выбору.
- изучить тенденции развития пользовательских интерфейсов;
- изучить устройство и режимы человеко-машинного диалога;
- изучить виды представления и визуализации информации;
- изучить средства проектирования экспертных систем;
- ознакомиться с методами принятия решений в условиях неопределенности;
- изучить методы машинного обучения;
- ознакомиться с языками и технологиями искусственного интеллекта
- изучить основные технологии разработки программного обеспечения, а также технологии командной разработки программного обеспечения;
- изучить основные методы управления жизненным циклом приложений;
- изучить основные метрики и методики тестирования программных продуктов, а также методы и алгоритмы тестирования.

В результате освоения дисциплины студент должен:

иметь представление:

1. о тенденциях развития пользовательских интерфейсов,
2. о методах принятия решений в условиях неопределенности,
3. о способах представления и визуализации информации,
4. о языках и технологиях искусственного интеллекта,
5. о методах построения программного обеспечения,
6. о методах тестирования и верификации программного обеспечения.

уметь:

1. разрабатывать человеко-машинные интерфейсы,
2. реализовывать системы на основе нейронных сетей,
3. проектировать экспертные системы,
4. разрабатывать самообучающиеся системы,
5. конструировать сложные программные системы;
6. проводить тестирование программного обеспечения.

приобрести навыки:

1. построения систем на основе подходов искусственного интеллекта,
2. программирования на языках логического программирования,
3. реализации алгоритмов машинного обучения,
4. работы в средах построения экспертных систем;
5. самостоятельной работы с учебной, методической и научной литературой;

владеть, иметь опыт:

1. разработки человеко-машинных интерфейсов,
2. описания структур данных,
3. описания основных базовых конструкций,
4. программирования на языке высокого уровня,
5. работы в различных средах программирования.

4. Формы работы студента

Студенты выполняют лабораторные работы, решение задач с использованием автоматической системы проверки решений, разработкой самостоятельных проектов

Обязательный курс для магистров 5-6 курсов, читается в 9, 10, 11 семестрах

Лекционные занятия – -/-/-ч

Лабораторные занятия – 36/16/38 ч

Самостоятельная работа – 36/20/34 ч

В интенсивной форме: лабораторные занятия – 74ч

зачет в 9-10 семестрах

экзамен в 11 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: ст.преп. Макаренко М.Д., доцент Гутнова А.К.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Компьютерные технологии в науке и образовании» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по каждому модулю, зачета и экзамена, также предусматривающего набор необходимого количества баллов.

6. Методика формирования результирующей оценки

Зачет выставляется по выполнении студентом 70% всей нагрузки.

На экзамен студенту представляется билет, содержащий 3 вопроса (два теоретических и один практический), каждый из которых оценивается в 20 баллов.

7. Тематический план курса

Курс	1	1	2
Семестр	1	2	3
Тематика	Методы машинного обучение без учителя	Методы машинного обучение с учителем	Методы обработки естественного языка
Лабораторные	36	16	38
Контроль	зач	зач	экз

8. Рекомендуемая литература

Рекомендуемая литература:

а) основная литература:

1. Сегаран Т. Програмируем коллективный разум. Символ-плюс, 2008.
2. Коэльо Л., Ричарт В. Построение систем машинного обучения на языке Python. ДМК Пресс, 2016.
3. Николаева И.С., Митренина О.В., Ландо Т.М. Прикладная и компьютерная лингвистика. URSS, 2016.
4. Грант С. Ингерсолл, Томас С. Мортон, Эндрю Л. Фэррис Обработка неструктурированных текстов. Поиск, организация и манипулирование. ДМК Пресс, 2015.
5. Джонс Т. Программирование искусственного интеллекта в приложениях. ДМК Пресс, 2012.
6. Ясницкий Л. Н. Введение в искусственный интеллект. Академия, 2008
7. Чулюков В., Астахова И., Потапов А. Системы искусственного интеллекта. Практический курс. Бином. Лаборатория знаний, 2008.
8. Маккарти Д., Маккарти М. Правила разработки программного обеспечения. Русская Редакция, Питер, 2007.
9. Фримен Э. Паттерны проектирования. Питер, 2011
10. Маклафлин Б. Объектно-ориентированный анализ и проектирование. Питер, 2013

б) дополнительная литература

11. Кохонен Т. Самоорганизующиеся карты. Бином. Лаборатория знаний, Москва, 2008
12. Жданов А. Автономный искусственный интеллект. Бином. Лаборатория знаний, Москва, 2009
13. Костров Б., Ручкин В., Фулин В. Искусственный интеллект и робототехника. Диалог-МИФИ, 2008 г.
14. Джарратано Д., Райли Г. Экспертные системы. Принципы разработки и программирование. Вильямс, 2007 г.
15. Борисов В., Круглов В., Федулов А. Нечеткие модели и сети. Горячая Линия - Телеком, 2012.
16. Ясницкий Л. Н. Искусственный интеллект. Бином. Лаборатория знаний, 2011
17. Джордж Ф. Люгер Искусственный интеллект. Стратегии и методы решения сложных проблем. Вильямс, 2005
18. Боровиков В. Нейронные сети. Statistica Neural Networks. Методология и технологии современного анализа данных. Горячая Линия, - Телеком, 2008 г.

19. Цвалина К., Абрамс Б. Инфраструктура программных проектов. Соглашения, идиомы и шаблоны для многократно используемых библиотек .NET. Вильямс, Москва, 2011
20. Гласс Р. Программирование и конфликты 2.0. Теория и практика программной инженерии. Символ-Плюс, Санкт Петербург – Москва, 2010.
21. Джозэл Х. Спольски Лучшие примеры разработки ПО. Питер, 2007

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;

собственным библиографическим базам данных:

- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

Рекомендуемые интернет-адреса по курсу Компьютерные технологии в науке и образовании

1. <http://intuit.ru/>
2. Ясницкий Л.Н. Искусственный интеллект: популярное введение для учителей и школьников
http://xn--80aawbkjgiswr.xn--1-btbl6aqcj8hc.xn--p1ai/view_article.php?ID=200901703, http://xn--80aawbkjgiswr.xn--1-btbl6aqcj8hc.xn--p1ai/view_article.php?ID=200902104, http://xn--80aawbkjgiswr.xn--1-btbl6aqcj8hc.xn--p1ai/view_article.php?ID=200902404
3. <http://umkd.volpi.ru/course/view.php?id=1813>
4. Основы функционального программирования
http://ru.wikibooks.org/wiki/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D1%8B_%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F
5. Основы программирования python
http://younglinux.info/sites/default/files/python_structured_programming.pdf

АННОТАЦИЯ

Дисциплина «Матричное представление элементов поля»

Направление 01.04.01 МАТЕМАТИКА

Программа подготовки магистра
«Алгебра»

1. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин: алгебра, теория групп, криптография, защита информации,

2. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к дисциплинам профессионального цикла, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, программа «Алгебра».

Дисциплина изучается в течение одного семестра.

3. Цели изучения дисциплины

Целью курса является изучение методов, задач и теорем алгебры, теории групп, теории расположения подгрупп, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Расположение подгрупп в полной линейной группе» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность создавать и исследовать новые математические модели в естественных науках (ОПК-2);
- Способность к интенсивной научно-исследовательской работе (ПК-1);
- Способность к творческому применению, развитию и реализации математически сложных алгоритмов в современных программных комплексах (ПК-5).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие магистров, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Расположение подгрупп в полной линейной группе»:

- **Магистр должен знать** основы теории групп; линейные группы, общую теорию расположения подгрупп, исследование подгрупп полной линейной группы, содержащих группу диагональных матриц, исследование подгрупп полной линейной группы, содержащих нерасщепимый максимальный тор.

- **Магистр должен уметь:** применять полученные методы и модели к решению типовых и практических задач с использованием аппарата алгебры, теории групп, основных алгебраических структур (группы, кольца, поля);
- пользоваться формулами и теоремами теории групп и теории полей, строить критерии проверки гипотез;
- пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
- применять полученные знания для изучения других дисциплин.
- **Магистр должен владеть:** навыками применения теоретико-групповых алгоритмов и алгебраических методов для решения различных прикладных задач.

4. Формы работы магистров

Формами работы магистров являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для 5 курса,
читается в 9 семестре

Лекционные занятия – 18ч

Практические занятия – 0 ч

Самостоятельная работа – 90 ч

В интенсивной форме: лекционные занятия - 4ч

Зачет – 9 семестр

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Матричное представление элементов поля» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по зачету, также предусматривающего набор необходимого количества баллов.

6. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен зачет (9 семестр). Максимальное количество баллов, которое может набрать магистрант, **100**.

За выполнение заданий текущего и промежуточного контроля магистрант может набрать максимальное количество баллов:

За первый модуль – 50 баллов (текущая работа T1- 20 баллов и компьютерный тест M1 - 30 баллов).

За второй модуль – 50 баллов (текущая работа T2- 20 баллов и компьютерный тест M2 - 30 баллов).

Зачет проводится в конце 9 семестра. На экзамене магистрант имеет возможность набрать 0- 60 баллов.

При успешном освоении курса магистрант, набравший 36 баллов может быть допущен к экзамену в 9-10 семестре. При успешном освоении курса магистрант, набравший 56 баллов или более, может быть освобожден от зачета в 9 семестре.

Результирующий балл определяется по формуле: $T1+T2+(M1+M2+3)/2$

7. Тематический план курса

Но ме р не дели	Наименование тем (вопросов), изучаемых по данной дисциплине	Зан ятия		Самостоятельная работа студентов		Формы контрол я	Количес тво баллов		Лите ра тура
		л	р	Содержание	Час ы		min	ма х	
1	Надгруппы группы диагональных матриц.	2		Изучение сетевых групп.	12				[2, 3]
2	Нерасщепимый максимальный тор.	2		Построение нерасщепимого макс. тора, как естественное вложение расширения основного поля.	12				[1-3]
3	Представление матрицами нерасщепимого тора.	2		Конкретные примеры представления тора матрицами.	12				[2-4]
4	Надгруппы нерасщепимого тора.	2		Построение надгрупп нерасщепимого тора.	12				[2, 3, 6]
5	Поле комплексных чисел, как нерасщепимый тор	2		Исследование подгрупп группы $GL(2, \mathbb{R})$, содержащих мультипликативную группу комплексных чисел.	12				[2, 4, 6]
6	Извлечение трансвекций	2		Построение техники извлечения трансвекций.	12				[1, 2, 3]
7	Подгруппы группы $GL(2, \mathbb{R})$, содержащие \mathbb{C}^*	2		Построение техники извлечения общих трансвекций	12				[2, 3, 6]
8	Нормализатор нерасщепимого максимального тора	2		Разложение общей трансвекции в промежуточные подгруппах.	12				[1, 6, 3]
9	Примеры расположения подгрупп. Нормализатор группы диагональных матриц	2		Построение примеров расположения	12				[2, 4, 6]

				подгрупп					
	ИТОГО	1 8			90				

Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение нерасщепимого тора для конечных полей	Практическое	2	Диалог	Использование на проекторе таблицы умножения групп
2	Построение нерасщепимого тора, как вложения расширения конечного поля	Практическое	2		Использование на проекторе таблицы умножения и сложения в кольцах и полях
3	Применение конкретных нерасщепимых торов второй степени	Практическое	2		Использование на проекторе таблицы умножения и сложения в полях

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

№	Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре
Основная литература:	
31. Белоногов В.А. Задачник по теории групп. М.: Наука. 2000. 238 с.	
32. Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005	
33. Койбаев В.А. Подгруппы группы $GL(2,k)$, содержащие нерасщепимый максимальный тор. – Математическая монография. Владикавказ. 2009. 182с.	

34. Каргаполов М.И., Мерзлякеов Ю.И. Основы теории групп. СПб.:Лань . 2009. 288с.
Дополнительная литература
35. Баскаков А.Г. Лекции по алгебре. Изд-во ВГУ. 2014.
36. Кострикин А.И. Сборник задач по алгебре.-М. МЦНМО. 2009. 408 с.
Электронный ресурс
37. Кострикин А.И. http://review3d.ru/kostrikin-a-i-vvedenie-v-algebru-v-3-chastyax
38. Каргаполов М.И., Мерзляков Ю.И. http://www.vixri.ru/?p=1212
39. Борович З.И. Подгруппы полной линейной группы, содержащие группу диагональных матриц//Зап.науч.семинаров ПОМИ РАН.1976, т.64, с.12-29. http://www.mathnet.ru/php/archive.phtml?jrnid=zns1&wshow=issue&series=0&year=1976&volume=64&issue=0&option_lang=rus&bookID=492

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

Дисциплина «Надгруппы нерасщепимого тора»

Направление 01.04.01 МАТЕМАТИКА

Программа подготовки магистра
«Алгебра»

8. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин: алгебра, теория групп, криптография, защита информации,

9. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к блоку Б1.В.ОД.7 Дисциплины (модули). Вариативная часть. Обязательные дисциплины, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, программа «Алгебра».

Дисциплина изучается в течение одного семестра.

10. Цели изучения дисциплины

Целью курса является изучение методов, задач и теорем алгебры, теории групп, теории расположения подгрупп, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Расположение подгрупп в полной линейной группе» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность создавать и исследовать новые математические модели в естественных науках (ОПК-2);
- Способность к интенсивной научно-исследовательской работе (ПК-1).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие магистров, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Надгруппы нерасщепимого тора»:

- *Магистр должен знать* основы теории групп; линейные группы, общую теорию расположения подгрупп, исследование подгрупп полной линейной группы, содержащих группу диагональных матриц, исследование подгрупп полной линейной группы, содержащих нерасщепимый максимальный тор.

- **Магистр должен уметь:** применять полученные методы и модели к решению типовых и практических задач с использованием аппарата алгебры, теории групп, основных алгебраических структур (группы, кольца, поля);
- пользоваться формулами и теоремами теории групп и теории полей, строить критерии проверки гипотез;
- пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
- применять полученные знания для изучения других дисциплин.
- **Магистр должен владеть:** навыками применения теоретико-групповых алгоритмов и алгебраических методов для решения различных прикладных задач.

11. Формы работы магистров

Формами работы магистров являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для 5 курса,
читается в 9 семестре

Лекционные занятия – 18ч

Практические занятия – 18 ч

Самостоятельная работа – 108 ч

В интенсивной форме: практические занятия - 4ч

Экзамен – 9 семестр

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А.

12. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Надгруппы нерасщепимого тора» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по зачету, также предусматривающего набор необходимого количества баллов.

13. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен экзамен (9 семестр). Максимальное количество баллов, которое может набрать магистрант, **100**.

За выполнение заданий текущего и промежуточного контроля магистрант может набрать максимальное количество баллов:

За первый модуль – 50 баллов (текущая работа T1- 20 баллов и компьютерный тест M1 - 30 баллов).

За второй модуль – 50 баллов (текущая работа T2- 20 баллов и компьютерный тест M2 - 30 баллов).

Зачет проводится в конце 9 семестра. На экзамене магистрант имеет возможность набрать 0- 60 баллов.

При успешном освоении курса магистрант, набравший 36 баллов может быть допущен к экзамену в 9-10 семестре. При успешном освоении курса магистрант, набравший 56 баллов или более, может быть освобожден от зачета в 9 семестре.

Результирующий балл определяется по формуле: $T1+T2+(M1+M2+3)/2$

14. Тематический план курса

Но ме р не д ели	Наименование тем (вопросов), изучаемых по данной дисциплине	Зан ятия		Самостоятельная работа студентов		Формы контрол я	Количес тво баллов		Лите ра тура
		л	р	Содержание	Час ы		min	ма х	
1	Надгруппы группы диагональных матриц.	2	2	Изучение сетевых групп.	12				[2, 3]
2	Нерасщепимый максимальный тор.	2	2	Построение нерасщепимого макс. тора, как естественное вложение расширения основного поля.	12				[1-3]
3	Представление матрицами нерасщепимого тора.	2	2	Конкретные примеры представления тора матрицами.	12				[2-4]
4	Надгруппы нерасщепимого тора.	2	2	Построение надгрупп нерасщепимого тора.	12				[2, 3, 6]
5	Поле комплексных чисел, как нерасщепимый тор	2	2	Исследование подгрупп группы $GL(2, \mathbb{R})$, содержащих мультипликативную группу комплексных чисел.	12				[2, 4, 6]
6	Извлечение трансвекций	2	2	Построение техники извлечения трансвекций.	12				[1, 2, 3]
7	Подгруппы группы $GL(2, \mathbb{R})$, содержащие C^*	2	2	Построение техники извлечения общих трансвекций	12				[2, 3, 6]
8	Нормализатор нерасщепимого максимального тора	2	2	Разложение общей трансвекции в промежуточные подгруппах.	12				[1, 6, 3]
9	Примеры расположения подгрупп. Нормализатор группы	2	2	Построение примеров					[2, 4, 6]

	диагональных матриц			расположения подгрупп	12				
	ИТОГО	1 8	18		108				

Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение нерасщепимого тора для конечных полей	Практическое	2	Диалог	Использование на проекторе таблицы умножения групп
2	Построение нерасщепимого тора, как вложения расширения конечного поля	Практическое	2		Использование на проекторе таблицы умножения и сложения в кольцах и полях
3	Применение конкретных нерасщепимых торов второй степени	Практическое	2		Использование на проекторе таблицы умножения и сложения в полях

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

№	Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре
Основная литература:	
40.	Белоногов В.А. Задачник по теории групп. М.: Наука. 2000. 238 с.
41.	Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005
42.	Койбаев В.А. Подгруппы группы $GL(2,k)$, содержащие нерасщепимый максимальный тор. – Математическая монография. Владикавказ. 2009. 182с.
43.	Каргаполов М.И., Мерзлякев Ю.И. Основы теории групп. СПб.:Лань . 2009. 288с.

Дополнительная литература

44. Баскаков А.Г. Лекции по алгебре. Изд-во ВГУ. 2014.

45. Кострикин А.И. Сборник задач по алгебре.-М. МЦНМО. 2009. 408 с.

Электронный ресурс

46. Кострикин А.И. <http://review3d.ru/kostrikin-a-i-vvedenie-v-algebru-v-3-chastyax>

47. Каргаполов М.И., Мерзляков Ю.И. <http://www.vixri.ru/?p=1212>

48. Борович З.И. Подгруппы полной линейной группы, содержащие группу диагональных матриц // Зап. науч. семинаров ПОМИ РАН. 1976, т.64, с.12-29.

http://www.mathnet.ru/php/archive.phtml?jrnid=zns1&wshow=issue&series=0&year=1976&volume=64&issue=0&option_lang=rus&bookID=492

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

Дисциплина «Научно-исследовательская работа (руководство магистрантами)»

Направление 01.04.01 МАТЕМАТИКА

Программа «Алгебра»

1. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике. Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин: алгебра, теория групп, криптография, защита информации,

2. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к дисциплинам научно-исследовательской работе магистра (М3), обеспечивающих подготовку магистра по направлению 01.04.01. «Математика» профиль «Алгебра» и относится к профессиональному циклу для указанного направления.

Дисциплина изучается в течение одного семестра.

3. Цели изучения дисциплины

Целью курса является научно-исследовательская работа, включая изучение методов, задач и теорем алгебры, теории групп, теории расположения подгрупп, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Научно-исследовательская работа (руководство магистрантами)» являются: практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Готовность к саморазвитию, самореализации, использованию творческого потенциала (ОК-3);
- Способность находить, формулировать и решать актуальные и значимые проблемы фундаментальной и прикладной математики (ОПК-1);
- Способность к интенсивной научно-исследовательской работе (ПК-1);
- Способность к организации научно-исследовательских и научно-производственных работ, к управлению научным коллективом (ПК-2);
- Способность публично представить собственные новые научные результаты (ПК-3).

Учебные задачи дисциплины:

- овладение математическими знаниями;

- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;

- изучение методов решения прикладных задач;

- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие магистров, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Научно-исследовательская работа (руководство магистрантами)»:

- **Магистр должен знать** основы научно-исследовательской работы в области теории групп, линейных групп, общей теории расположения подгрупп, исследования подгрупп полной линейной группы, содержащих группу диагональных матриц, исследования подгрупп полной линейной группы, содержащих нерасщепимый максимальный тор.
- **Магистр должен уметь**: применять полученные методы и модели к решению типовых и практических задач с использованием аппарата алгебры, теории групп, основных алгебраических структур (группы, кольца, поля);
 - пользоваться формулами и теоремами теории групп и теории полей, строить критерии проверки гипотез;
 - пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
 - применять полученные знания для изучения других дисциплин.
- **Магистр должен владеть**: навыками применения теоретико-групповых алгоритмов и алгебраических методов для решения различных прикладных задач.

4. Формы работы магистров

Формами работы магистров являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 1 курса,
читается в 9 семестре

Аудиторные занятия – 54 ч

Самостоятельная работа – 198 ч

Зачет – 9, 10, 11

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Научно-исследовательская работа (руководство магистрантами) (сем.9)» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по зачету, также предусматривающего набор необходимого количества баллов.

6. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрены зачет За выполнение заданий текущего и промежуточного контроля магистрант может набрать максимальное количество баллов:

При успешном освоении курса магистрант, может быть освобожден от зачета в 9 семестре.

7. Тематический план курса

9 семестр

Номер недели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия		Самостоятельная работа студентов		Формы контроля	Количество баллов		Литература
		л	р	Содержание	Часы		min	max	
1	Группы, подгруппы, фактор-группы		2	На примерах знакопеременной группы и линейных групп - Изучение различных групп, подгрупп, фактор-групп	22				[2, 3]
2	Линейные группы		2	Изучение линейных групп	22				[1-3]
3	Нерасщепимый тор		2	Конкретные примеры представления тора матрицами. На примере радикального расширения поля рациональных чисел Построение нерасщепимого макс. тора, как естественное вложение расширения основного поля.	22				[2-4]
4	Расщепимый тор		2	техники исследования промежуточных подгрупп - Описание надгрупп расщепимого тора. Извлечение трансвекций	22				[3, 6,9]
5	Элементарные сети		2	Исследование элементарных сетей.	22				[2, 4, 6,9, 10]
6	Замкнутые сети		2	Исследование замкнутых или допустимых сетей.	22				[1, 2, 3, 10]

7	Дополняемые сети	2	. Исследование дополняемых сетей	22				[3, 6,9, 10]
8	Сетевые группы	2	Для колец конечно-порожденных над своим центром - исследование сетевых групп	22				[6, 3,9]
9	Нормализатор тора	2	Нормализатор тора для радикального расширения	22				
	ИТОГО	18		198				

1.6 Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение нерасщепимого тора для конечных полей	Практическое	2	Диалог	Использование на проекторе таблицы умножения групп
2	Построение нерасщепимого тора, как вложения расширения конечного поля	Практическое	2		Использование на проекторе таблицы умножения и сложения в кольцах и полях
3	Применение конкретных нерасщепимых торов второй степени	Практическое	2		Использование на проекторе таблицы умножения и сложения в полях

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

№ Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре

Основная литература:

1. Белоногов В.А. Задачник по теории групп. М.: Наука. 2000. 238 с.

2. Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005
3. Койбаев В.А. Подгруппы группы $GL(2,k)$, содержащие нерасщепимый максимальный тор. – Математическая монография. Владикавказ. 2009. 182с.
4. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. СПб.:Лань . 2009. 288с.

Дополнительная литература

5. Баскаков А.Г. Лекции по алгебре. Изд-во ВГУ.2014.
6. Кострикин А.И. Сборник задач по алгебре.-М. МЦНМО. 2009. 408 с.

Электронный ресурс

7. Кострикин А.И. <http://review3d.ru/kostrikin-a-i-vvedenie-v-algebru-v-3-chastyax>
8. Каргаполов М.И., Мерзляков Ю.И. <http://www.vixri.ru/?p=1212>
9. Борович З.И. Подгруппы полнойлинейной группы, содержащие группу диагональных матриц//Зап.науч.семинаров ПОМИ РАН.1976, т.64, с.12-29.
http://www.mathnet.ru/php/archive.phtml?jrnid=znsl&wshow=issue&series=0&year=1976&volume=64&issue=0&option_lang=rus&bookID=492
10. Койбаев В.А., Нужин Я.Н.Подгруппы групп Шевалле и кольца Ли, определяемые набором аддитивных подгрупп основного кольца//Фунд.и прикладная математика 2013. Т.18. Вып.1. С.75-84. (в пакете УМК)

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

Дисциплина «Расположение подгрупп в полной линейной группе»

Направление 01.04.01 МАТЕМАТИКА

Профиль подготовки магистра
«Алгебра»

15. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин: алгебра, теория групп, криптография, защита информации,

16. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к блоку Б1.В.ДВ.2.1 Дисциплины (модули). Вариативная часть. Дисциплины по выбору, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, профиль «Алгебра».

Дисциплина изучается в течение одного семестра.

17. Цели изучения дисциплины

Целью курса является изучение методов, задач и теорем алгебры, теории групп, теории расположения подгрупп, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Расположение подгрупп в полной линейной группе» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Готовность самостоятельно создавать прикладные программные средства на основе современных информационных технологий и сетевых ресурсов (ОПК-3);
- Способность к применению методов математического и алгоритмического моделирования при анализе экономических и социальных процессов, задач бизнеса, финансовой и актуарной математики (ПК-7).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;

- интеллектуальное развитие магистров, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Расположение подгрупп в полной линейной группе»:

- **Магистр должен знать** основы теории групп; линейные группы, общую теорию расположения подгрупп, исследование подгрупп полной линейной группы, содержащих группу диагональных матриц, исследование подгрупп полной линейной группы, содержащих нерасщепимый максимальный тор.
- **Магистр должен уметь**: применять полученные методы и модели к решению типовых и практических задач с использованием аппарата алгебры, теории групп, основных алгебраических структур (группы, кольца, поля) ;
- пользоваться формулами и теоремами теории групп и теории полей, строить критерии проверки гипотез;
- пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
- применять полученные знания для изучения других дисциплин.
- **Магистр должен владеть**: навыки применения теоретико-групповых алгоритмов и алгебраических методов для решения различных прикладных задач.

18. Формы работы магистров

Формами работы магистров являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 1 курса,

читается в 10 семестре

Лекционные занятия – 0ч

Практические занятия – 16ч

Самостоятельная работа – 56 ч

Экзамен – 9

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А.

11. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Расположение подгрупп в полной линейной группе» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по зачету, также предусматривающего набор необходимого количества баллов.

6.Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен экзамен (10 семестр). Максимальное количество баллов, которое может набрать магистрант, **100**.

7. Тематический план курса

Но ме р не де ли	Наименование тем (вопросов), изучаемых по данной дисциплине	За нятия		Самостоятельная работа студентов		Формы контро ля	Количес тво баллов		Лит ера тура
		л	р	Содержание	Ча сы		mi n	ma x	
1	Надгруппы группы диагональных матриц.		2	Изучение сетевых групп.	8				[2, 3]
2	Нерасщепимый максимальный тор.		2	Построение нерасщепимо го макс.тора, как естественное вложение расширения основного поля.	6				[1-3]
3	Представление матрицами нерасщепимого тора.		2	Конкретные примеры представлени я тора матрицами.	6				[2-4]
4	Надгруппы нерасщепимого тора.		2	Построение надгрупп нерасщепимо го тора.	6				[2, 3, 6]
5	Поле комплексных чисел, как нерасщепимый тор		2	Исследование подгрупп группы $GL(2, \mathbb{R})$, содержащих мультипликат ивную группу комплексных чисел.	6				[2, 4, 6]
6	Извлечение трансвекций		2	Построение техники извлечения трансвекций.	6				[1, 2, 3]
7	Подгруппы группы $GL(2, \mathbb{R})$, содержащие C^*		2	Построение техники извлечения общих трансвекций	6				[2, 3, 6]
8	Нормализатор нерасщепимого максимального тора		1	Разложение общей трансвекции в промежуточн	6				[1, 6, 3]

				ых подгруппах.					
9	Примеры расположения подгрупп. Нормализатор группы диагональных матриц		1	Построение примеров расположения подгрупп	6				[2, 4, 6]
	ИТОГО		16		56				

Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение нерасщепимого тора для конечных полей	Практическое	2	Диалог	Использование на проекторе таблицы умножения групп
2	Построение нерасщепимого тора, как вложения расширения конечного поля	Практическое	2		Использование на проекторе таблицы умножения и сложения в кольцах и полях
3	Применение конкретных нерасщепимых торов второй степени	Практическое	2		Использование на проекторе таблицы умножения и сложения в полях

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

№	Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре
---	--

Основная литература:

11. Белоногов В.А. Задачник по теории групп. М.: Наука. 2000. 238 с.

12. Койбаев В.А. Основы алгебры. – Владикавказ: СОГУ, 2005

13. Койбаев В.А. Подгруппы группы $GL(2, k)$, содержащие нерасщепимый максимальный тор. – Математическая монография. Владикавказ. 2009. 182с.

14. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. СПб.: Лань . 2009. 288с.

Дополнительная литература

15. Баскаков А.Г. Лекции по алгебре. Изд-во ВГУ. 2014.

16. Кострикин А.И. Сборник задач по алгебре.-М. МЦНМО. 2009. 408 с.

Электронный ресурс

17. Кострикин А.И. <http://review3d.ru/kostrikin-a-i-vvedenie-v-algebru-v-3-chastyax>

18. Каргаполов М.И., Мерзляков Ю.И. <http://www.vixri.ru/?p=1212>

19. Борович З.И. Подгруппы полной линейной группы, содержащие группу диагональных матриц // Зап. науч. семинаров ПОМИ РАН. 1976, т.64, с.12-29.

http://www.mathnet.ru/php/archive.phtml?jrnid=zns1&wshow=issue&series=0&year=1976&volume=64&issue=0&option_lang=rus&bookID=492

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):
- библиотеке e-library,

- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

Дисциплина «Расширение полей»

Направление 01.04.01 МАТЕМАТИКА

Профиль подготовки магистра «Алгебра»

19. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин: алгебра, теория групп, криптография, защита информации,

20. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к блоку Б1.В.ДВ.2.2 Дисциплины (модули). Вариативная часть. Дисциплины по выбору, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, профиль «Алгебра».

Дисциплина изучается в течение одного семестра.

21. Цели изучения дисциплины

Целью курса является изучение методов, задач и теорем алгебры, теории групп, теории расположения подгрупп, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Расположение подгрупп в полной линейной группе» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность создавать и исследовать новые математические модели в естественных науках (ОПК-2);
- Способность к собственному видению прикладного аспекта в строгих математических формулировках (ПК-6).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие магистров, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Расположение подгрупп в полной линейной группе»:

- *Магистр должен знать* основы теории групп; линейные группы, общую теорию расположения подгрупп, исследование подгрупп полной линейной группы, содержащих группу диагональных матриц, исследование подгрупп полной линейной группы, содержащих нерасщепимый максимальный тор.

1	Надгруппы группы диагональных матриц.	2	2	Изучение сетевых групп.	12				[2, 3]
2	Нерасщепимый максимальный тор.	2	2	Построение нерасщепимого макс.тора, как естественное вложение расширения основного поля.	12				[1-3]
3	Представление матрицами нерасщепимого тора.	2	2	Конкретные примеры представления тора матрицами.	12				[2-4]
4	Надгруппы нерасщепимого тора.	2	2	Построение надгрупп нерасщепимого тора.	12				[2, 3, 6]
5	Поле комплексных чисел, как нерасщепимый тор	2	2	Исследование подгрупп группы $GL(2, \mathbb{R})$, содержащих мультипликативную группу комплексных чисел.	12				[2, 4, 6]
6	Извлечение трансвекций	2	2	Построение техники извлечения трансвекций.	12				[1, 2, 3]
7	Подгруппы группы $GL(2, \mathbb{R})$, содержащие C^*	2	2	. Построение техники извлечения общих трансвекций	12				[2, 3, 6]
8	Нормализатор нерасщепимого максимального тора	2	2	Разложение общей трансвекции в промежуток	12				[1, 6, 3]

				очных подгруппах.					
9	Примеры расположения подгрупп. Нормализатор группы диагональных матриц	2	2	Построение примеров расположения подгрупп	12				[2, 4, 6]
	ИТОГО	18	18		108				

Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение нерасщепимого тора для конечных полей	Практическое	2	Диалог	Использование на проекторе таблицы умножения групп
2	Построение нерасщепимого тора, как вложения расширения конечного поля	Практическое	2		Использование на проекторе таблицы умножения и сложения в кольцах и полях
3	Применение конкретных нерасщепимых торов второй степени	Практическое	2		Использование на проекторе таблицы умножения и сложения в полях

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

№	Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре
Основная литература:	
20.	Белоногов В.А. Задачник по теории групп. М.: Наука. 2000. 238 с.
21.	Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005
22.	Койбаев В.А. Подгруппы группы $GL(2,k)$, содержащие нерасщепимый максимальный тор. – Математическая монография. Владикавказ. 2009. 182с.
23.	Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. СПб.:Лань . 2009. 288с.
Дополнительная литература	
24.	Баскаков А.Г. Лекции по алгебре. Изд-во ВГУ.2014.
25.	Кострикин А.И. Сборник задач по алгебре.-М. МЦНМО. 2009. 408 с.
Электронный ресурс	
26.	Кострикин А.И. http://review3d.ru/kostrikin-a-i-vvedenie-v-algebru-v-3-chastyax
27.	Каргаполов М.И., Мерзляков Ю.И. http://www.vixri.ru/?p=1212
28.	Боревич З.И. Подгруппы полнойлинейной группы, содержащие группу диагональных матриц//Зап.науч.семинаров ПОМИ РАН.1976, т.64, с.12-29. http://www.mathnet.ru/php/archive.phtml?jrnid=zns1&wshow=issue&series=0&year=1976&volume=64&issue=0&option_lang=rus&bookID=492

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
 - электронному каталогу,
 - электронной картотеке газетно-журнальных статей,
 - электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

дисциплины «Решение криптографических задач»

Направление подготовки магистра 01.04.01 МАТЕМАТИКА Программа «Алгебра»

19. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах:

алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике. Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин:

алгебра, теория групп, криптография, защита информации,

20. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к дисциплинам профессиональной цикла, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, программа «Алгебра».

Дисциплина изучается в течение одного семестра.

21. Цели изучения дисциплины

Целью курса является изучение методов, задач теории групп и колец, криптографии, коды, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Решение криптографических задач» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность создавать и исследовать новые математические модели естественных наук (ОПК-2);
- Способность к организации научно-исследовательских и научно-производственных работ, к управлению научным коллективом (ПК-1).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие студентов, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Решение криптографических задач»:

Студент должен знать

- основы теории групп;
- основы теории полей;
- основы теории колец;
- блочные шифры;
- симметричные криптосистемы;
- асимметричные криптосистемы;

- коды шифрования.

Студент должен уметь:

- применять полученные методы и модели к решению типовых и практических задач с использованием аппарата алгебры, криптографии, основных алгебраических структур (группы, кольца, поля);
- шифрующих кодов;
- пользоваться формулами и теоремами теории групп и теории полей, строить критерии для проверки гипотез;
- пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
- применять полученные знания для изучения других дисциплин.

Студент должен владеть:

- навыками применения криптографических алгоритмов и алгебраических методов для решения различных прикладных задач.

4. Формы работы магистров

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 5 курса,

читается 10 семестре

Лекционные занятия – -

Практические занятия – 16 ч

Самостоятельная работа – 74 ч

Экзамен в 10 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А., ст.преп. Джусоева Н.А.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Решение криптографических задач» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по каждому модулю, зачета и экзамена, также предусматривающего набор необходимого количества баллов.

8. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен экзамен в 10 семестре.

9. Тематический план курса

10 семестр

Номер недели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия		Самостоятельная работа студентов		Формы контроля	Количество баллов		Литература
		л	пр	Содержание	Часы		min	max	
1	История криптографии			.	8				[1,3]

2	Примеры шифров и криптографических систем		4	Шифры простой подстановки и перестановки, усложненные комбинированные шифры	8				[1,4]
3	Использование алгебраического аппарата в криптографии								[1,4,5]
4	Симметричные криптографические системы		2	Примеры симметричных криптографических систем	8				[1,3]
5	Асимметричные криптографические системы		2	Примеры асимметричных криптографических систем	8				[1,3]
6	Определение группы. Примеры.		2	Примеры конечных групп	8				[2,6,8]
7	Подгруппы. Примеры подгрупп.		2	Примеры неизоморфных конечных групп	8				[2,6,8]
8	Фактор-группа. Примеры		2	Примеры бесконечных групп, фактор-группы которых конечны	8				[2,6,8]
9	Гомоморфизмы. Примеры.		2	Примеры гомоморфизмов	16				[2,6,8]
	ИТОГО		16		74				

Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение криптошифрования в кольце Z_{pq} для конкретных p, q	Практическое	2	Диалог	Использование на проекторе таблицы умножения в кольце Z_{pq}
2	Построение (n, k) -пороговой схемы разделения секрета для конкретных n, k	Практическое	2		Использование на проекторе таблицы умножения и сложения для формирования взаимно простых модулей
3	Примеры построения схем разделения секрета	Практическое	2		Использование на проекторе таблицы умножения и сложения для применения китайской теоремы при построении схемы разделения секрета

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

№	Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре
Основная литература:	
29.	Ященко В.В. Введение в криптографию. М.: МЦНМО. 2012. 352 с.
30.	Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005
31.	Алферов А.П. и др. Основы криптографии. – М. Гелиос АРВ. 2005.480 с.
32.	Ноден П., Ките К. Алгебраическая алгоритмика. – М. Мир. 2007. 720 с.
33.	Коблиц Н. Курс теории чисел и криптографии. – М. ТВП. 2007. 261с.
34.	Кострикин А.И. Введение в алгебру. Ч.1-3 – М. МЦНМО. 2009. 838с.
Дополнительная литература	
35.	Баскаков А.Г. Лекции по алгебре. Изд-во ВГУ.2014.
36.	Кострикин А.И. Сборник задач по алгебре.-М. МЦНМО. 2009. 408 с.
Электронный ресурс	
37.	Кострикин А.И. Введение в алгебру http://math-portal.ru/678-vvedenie-v-algebru-chast-3-osnovnye-struktury-kostrikin-ai-3-e-izdanie.html
38.	Коблиц Н. Курс теории чисел и криптографии. http://math-portal.ru/tags/%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F/

Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

Дисциплина «Системы прикладного программного обеспечения»

Направление 01.04.01 МАТЕМАТИКА

Профиль подготовки магистра
«Алгебра»

7. Требования к студентам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике.

8. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина является дисциплиной блока Б1.В.ДВ.3.2 Дисциплины (модули). Вариативная часть. Дисциплины по выбору. Дисциплина «Системы прикладного программного обеспечения» необходима для овладения теоретическими и практическими знаниями, лежащими в основе общенаучных дисциплин компьютерных наук, а также курсов, изучающих конкретные задачи программирования.

Изучению дисциплины «Системы прикладного программного обеспечения» предшествует изучение школьных курсов математики и информатики.

Знания, полученные при изучении дисциплины «Системы прикладного программного обеспечения», могут быть использованы при изучении курсов «Компьютерные технологии в науке и образовании».

Дисциплина изучается в течение одного семестра.

9. Цели изучения дисциплины

- знакомство студентов с типами программного обеспечения, методами и средствами разработки программного обеспечения;
- знакомство с составом и схемой работы систем программирования, основными принципами функционирования операционных систем, их структурой и особенностями;
- принципы управления ресурсами вычислительной системы;
- получения навыков работы с различными типами программного обеспечения;

- знакомство с системным программированием;
- знакомство с методами структурного и объектно-ориентированного программирования как наиболее распространенными и эффективными методами разработки программных продуктов;
- обучение разработке алгоритмов на основе структурного и объектно-ориентированного подхода;
- закрепление навыков алгоритмизации и программирования на основе изучения языка программирования C#;
- знакомство с основными структурами данных и типовыми методами обработки этих структур;
- создание практической базы для изучения других учебных дисциплин.

Достижение этих целей обеспечивает выпускнику получение высшего профессионально профилированного образования и обладание перечисленными ниже общими и предметно-специализированными компетенциями.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность к творческому применению, развитию и реализации математически сложных алгоритмов в современных программных комплексах (ПК-5);
- Способность к применению методов математического и алгоритмического моделирования при анализе экономических и социальных процессов, задач бизнеса, финансовой и актуарной математики (ПК-7).

В результате изучения дисциплины, магистр должен:

знать:

- об уровнях и классификации программного обеспечения;
- структуре сред программирования;
- классификации и эволюции языков программирования;
- управление ресурсами операционной системы, такими как: память, процессор, устройства ввода-вывода;

- о прерываниях;
- многопоточном программировании.

уметь:

- работать с командной строкой операционной системы;
- использовать Системы прикладного программного обеспечения на профессиональном уровне;
- использовать пакеты автоматизации исследовательских работ в учебном процессе и научной деятельности;
- иметь навыки разработки простейших web приложений;
- иметь навыки многопоточного программирования.

владеть:

- профессиональной работой с офисными приложениями;
- построением web- страниц;
- автоматизацией работ с операционной системой;
- основами системного программирования;
- работой со встроенными системами программирования прикладного программного обеспечения,
- работой с командной строкой и командными файлами,
- основами построения многопоточных систем,
- работой с профессиональным программным обеспечением.

10.Формы работы студентов

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

11. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Системы прикладного программного обеспечения» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по зачету, также предусматривающего набор необходимого количества баллов.

12. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен зачет.

Обязательный курс для студентов 5 курса, читается в 9 семестре

Лекционные занятия – 0 часов

Практические занятия – 18 часов

Самостоятельная работа – 90 часов

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: Гутнова А.К.

13. Тематический план курса

Распределение разделов по аудиторным часам (ЛЗ – лекционные занятия, ПЗ – практические занятия, СР – самостоятельная работа, АЗ – аудиторные занятия, ЛАБЗ – лабораторные занятия).

№	Название темы	АЗ			СР
		ЛЗ	ПЗ	ЛАБЗ	

ДЕВЯТЫЙ СЕМЕСТР

1.	Тема 1. Структура программного обеспечения Понятие вычислительной системы. Основные понятия. История и эволюция программного обеспечения. Структура программного обеспечения.		3		18
2.	Тема 2. Системы прикладного программного обеспечения. Классификации прикладного программного обеспечения, основные характеристики, типы информации, примеры реализации программного обеспечения.		3		18
3.	Тема 3. Инструментальное программное обеспечение. Понятие среды программирования. Структура и механизмы функционирования. Эволюция сред программирования. Парадигмы программирования. Обзор языков и платформ программирования.		4		18
4.	Тема 4. Системное программное обеспечение. Понятие ресурса, процесса и потока. Дисциплины диспетчеризации. Способы организации оперативной памяти. Файловые системы. Управление системой ввода вывода. Обзор и сравнение операционных систем.		4		18
5.	Тема 5. Разработка многопоточных приложений. Независимые и взаимодействующие вычислительные процессы. Средства синхронизации и связи при проектировании. Семафоры. Конвейеры и очереди сообщений. Проблемы тупиков и методы борьбы с ними.		4		18
	ИТОГО:		18		90
	Всего (часы): (аудиторные занятия и самостоятельная работа)		108		

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Аладьев В.З. Системы компьютерной алгебры: Maple: искусство программирования. Лаборатория Базовых Знаний, 2006. – 870с.
2. Васильев А. VBA в Office 2000. СПб.: Питер, 2009. – 284 с.
3. Гарнаев А.Ю. Самоучитель VBA. 2-е издание. Издательство «БХВ-Петербург», 2004. – 560с.
4. Гевенян В.Р. Adobe Photoshop CS: волшебные фильтры и спецэффекты. Издательство «БХВ-Петербург», 2004. – 520с.
5. Гельман В. Решение математических задач средствами Excel: практикум. СПб.: Питер, 2012. – 156 с.
6. Кнут Д. Тех. М.: Наука. – 436 с.

7. Молчанов А.Ю. Системное программное обеспечение: Учебник для ВУЗов. СПб.: Питер, 2006. – 396с.
8. Молчанов А.Ю. Системное программное обеспечение. Лабораторный практикум. СПб.: Питер, 2005. – 284с.
9. Моррисон М. HTML и XML. Быстро и эффективно. СПб.: Питер, 2012. – 144 с.
10. Олифер Н.А., Олифер В.Г. Сетевые операционные системы. СПб.: Питер, 2011. – 326 с.
11. Орлов С.А. Технологии разработки программного обеспечения. СПб.: Питер, 2012. – 608с.
12. Пратт Т. Зелковиц М. Языки программирования: реализация и разработка. СПб.: Питер, 2011. – 820 с.
13. Харитонова И. Самоучитель Office Access 2003. Питер, 2010. – 238 с.
14. Чен К. MATLAB в математических исследованиях. б.: Питер, 2012. – 144 с.

б) Дополнительная литература

1. Альтман Р. Microsoft Office PowerPoint 2003 для Windows. СПб.: Питер, 2010. – 256 с.
2. Гайдышев И.П. Решение научных и инженерных задач средствами Excel, VBA и C/C++. Издательство «БХВ-Петербург», 2004. – 512с.
3. Дубина А., Орлова С., Шубина И., Хромов А. Экономические расчеты и оптимизационное моделирование в среде Excel. СПб.: Питер, 2012. – 148 с.
4. Лапин П. Flash MX. СПб.: Питер, 2013. – 188 с.
5. Роман С. Использование макросов в Excel. СПб.: Питер, 2013. – 204 с.
6. Рычков В. Самоучитель. Компьютер для студента. СПб.: Питер, 2010.- 248 с.

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

Рекомендуемые интернет-адреса по предмету:

- http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5
- <http://www.intuit.ru/studies/courses/3632/874/info>
- <http://www.intuit.ru/studies/courses/1053/150/info>
- <http://www.intuit.ru/studies/courses/7/7/info>

АННОТАЦИЯ

«Современные проблемы математики»

Направление 01.04.01 МАТЕМАТИКА

Программа «Алгебра»

1. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин: теория графов, алгебра, теория групп, криптография, защита информации,

2. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к дисциплинам базовой части блока общенаучного цикла, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, программа «Алгебра».

Дисциплина изучается в течение одного семестра.

3. Цели изучения дисциплины

Целью курса является изучение методов, задач и теорем алгебры, теории групп, теории расположения подгрупп, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Современные проблемы математики» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность к абстрактному мышлению, анализу, синтезу (ОК-1);
- Готовность к саморазвитию, самореализации, использованию творческого потенциала (ОК-3);
- Способность находить, формулировать и решать актуальные и значимые проблемы фундаментальной и прикладной математики (ОПК-1);
- Способность создавать и исследовать новые математические модели в естественных науках (ОПК-2);
- Способность к организации научно-исследовательских и научно-производственных работ, к управлению научным коллективом (ПК-2);
- Способность и предрасположенность к просветительной и воспитательной деятельности, готовность пропагандировать и популяризировать научные достижения (ПК-11).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие магистров, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины «Современные проблемы математики»:

- **Магистр должен знать** основы теории графов, основы теории групп; линейные группы, общую теорию расположения подгрупп, исследование подгрупп полной линейной группы, содержащих группу диагональных матриц, исследование подгрупп полной линейной группы, содержащих нерасщепимый максимальный тор.
- **Магистр должен уметь:** применять полученные методы и модели к решению типовых и практических задач с использованием аппарата алгебры, теории групп, основных алгебраических структур (группы, кольца, поля);
- пользоваться формулами и теоремами теории групп и теории полей, строить критерии
- проверки гипотез;
- пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
- применять полученные знания для изучения других дисциплин.
- **Магистр должен владеть:** навыками применения теоретико-групповых алгоритмов и алгебраических методов для решения различных прикладных задач.

4. Формы работы магистров

Формами работы магистров являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 5 курса,

читается в 9 семестре

Лекционные занятия – 18

Практические занятия – 0

Самостоятельная работа – 90 ч

экзамен в 9 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Современные проблемы математики» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по зачету, также предусматривающего набор необходимого количества баллов.

6. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен экзамен (9 семестр). Максимальное количество баллов, которое может набрать магистрант, **100**.

За выполнение заданий текущего и промежуточного контроля магистрант может набрать максимальное количество баллов:

За первый модуль – 50 баллов (текущая работа T1- 20 баллов и компьютерный тест M1 - 30 баллов).

За второй модуль – 50 баллов (текущая работа T2- 20 баллов и компьютерный тест M2 - 30 баллов).

Экзамен проводится в конце 9 семестра. На экзамене магистрант имеет возможность набрать наивысший балл

7. Тематический план курса

Номер недели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия		Самостоятельная работа студентов		Формы контроля	Количество баллов		Литература
		л	пр	Содержание	Часы		Min	max	
1	Возникновение теории групп. Группа, как способ характеристики симметрии.	2		Группы. Подгруппы. Нормальные подгруппы .Факторизация Абелевы группы.	10	Экзаменационные вопросы			[1, т.3 §2,4], [4, §1,2,7-10]
2	Проблема классификации конечных групп.	2		Гомоморфизмы .Конечные группы .Силовские p -подгруппы. Теоремы Силова	10	Экзаменационные вопросы			[1, т.3 гл2 §1-3], [4, §11-13]
3-5	Группы матриц. Матрицы специального вида .Полная линейная группа над полем .Вопросы расположения подгрупп в $GL(n, K)$.	6		Группа S_n . Матрицы трансвекции .Сети и сетевые группы. Веерные подгруппы Элементарные сети. Тор , классификация.	30	Экзаменационные вопросы			[1, т.1 гл.2 §1-3], [2, гл1,2,3]
6-7	Группы Шевалле .Графы. Современное состояние развития теории графов.	4		Возникновение понятия графа. Графы как модели при решении задач Классификация конечных групп и симметрических графов.	20	Экзаменационные вопросы			[1, §2], [4, §1]
8-9	Универсальная алгебра			Алгебра над		Экзаменационные			[1, т.3, гл.4, гл.5],

.Основные направления её развития. Элементы универсальной алгебры в теории кодирования и защиты информации.	4		полем. Алгебра ассоциативная с делением. Алгебра кватернионов. Алгебра над полем конечная.	20	вопросы			[4, §23-25]
Итого	18			90				

1.6 Образовательные технологии

Лекции, лекции-беседы, самостоятельная работа студентов.

№/п	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Возникновение теории групп .Группа как способ характеристики симметрии.	Лекционное	2	Диалог	
2	Проблема классификации конечных групп.	Лекционное	2	Диалог	

1.7 Учебно-методическое обеспечение самостоятельной работы.

Рекомендуемая литература:

а) основная литература:

1. Кострикин А.И. Введение в алгебру. Ч.1-3 . М.,МЦМНО,2009
2. Койбаев В. А .Подгруппы группы $GL(2,k)$, содержащие нерасщепимый тор . Серия Математическая монография ЮМИ ВЦ РАН и PCO-A,2009 г.
3. Махнев А.А.

б) дополнительная литература

4. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. Лань, 2009

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
 - электронной библиотеке диссертаций РГБ,
 - университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
 - электронной картотеке газетно-журнальных статей,
 - электронной картотеке авторефератов диссертаций и диссертаций.

Рекомендуемые интернет-адреса по курсу «Современные проблемы математики»

2. <http://intuit.ru/>
2. <http://mathnet.ru>

АННОТАЦИЯ

дисциплины «Теория графов»

Направление подготовки магистра 01.04.01 МАТЕМАТИКА Программа «Алгебра»

22. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике. Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин: алгебра, теория групп, криптография, защита информации.

23. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к дисциплинам профессионального цикла, обеспечивающих подготовку магистра по направлению 01.04.01 Математика, программа «Алгебра».

Дисциплина изучается в течение одного семестра.

24. Цели изучения дисциплины

Целью курса является изучение методов, задач теории групп и колец, криптографии, коды, их применение к решению задач прикладной математики и информатики.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Теория графов» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность создавать и исследовать новые математические модели естественных наук (ОПК-2);
- Способность к организации научно-исследовательских и научно-производственных работ, к управлению научным коллективом (ПК-1).

Учебные задачи дисциплины:

- овладение математическими знаниями;
- приближение преподавания математики к реальным потребностям подготовки специалиста данного профиля;
- изучение методов решения прикладных задач;
- систематизация по методам решений всех типов прикладных задач;
- интеллектуальное развитие студентов, формирование качеств мышления, характерных для математической деятельности.

В результате изучения дисциплины студент должен:

иметь представление:

1. об основных понятиях и методах, используемых в современной теории графов
2. о многообразии задач, возникающих на графах и сетях, и алгоритмах их решения
3. об особенностях применения алгоритмов при решении прикладных и теоретических задач
4. о взаимосвязи между различными разделами теории графов

знать:

- основные типы объектов и структур, изучаемых теорией графов
- различные свойства графов и связанных с ними объектов в рамках предлагаемого курса
- типовые методы, используемые при работе с графами, орграфами, мультиграфами и сетями
- постановки наиболее известных задач на графах и сетях и эффективные алгоритмы их решения

уметь:

1. формулировать прикладные и теоретические задачи на языке графов и сетей, осуществлять подбор эффективных алгоритмов для их решения
2. разработать программную реализацию выбранного алгоритма, произвести отладку программы и интерпретировать результаты ее работы
применять полученные теоретические знания для доказательства различных свойств графов и связанных с ними объектов.

4. Формы работы магистров

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 5 курса, читается в 10 семестре

Лекционные занятия – -ч

Практические занятия – 16 ч

Самостоятельная работа – 74 ч

экзамен в 10 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: доцент Гутнова А.К.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Теория графов» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по каждому модулю, зачета и экзамена, также предусматривающего набор необходимого количества баллов.

6. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен экзамен (10 семестр).

За выполнение заданий текущего и промежуточного контроля студент может набрать максимальное количество баллов.

7. Тематический план курса

Номер недели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия		Самостоятельная работа Студентов		Формы контроля	Количество баллов		Литература
		л	пр	Содержание	Часы		min	max	
10 семестр									
1-2	Введение. Основные понятия теории графов		2	Возникновение понятия графа. Графы как модели при решении задач. Задача Эйлера о кенигсбергских мостах. Задача Гамильтона. Исследования деревьев Кирхгофом и Кэли.	8	Конспект, вопросы в рубеж.контр	0	5	[1]
3-4	Виды и примеры симметричных графов. Понятие дистанционно транзитивного графа		2	Мультиграфы, ориентированные графы и сети. Алгоритмы на графах и сетях. Современное состояние развития теории графов.	8		0	5	[7]
5-6	Частичные геометрии		2		8		0	5	[10]
7-8	Система Штейнера		2		8		0	5	[6; 7]
9	Система Штейнера				8		0	30	
10-11	Псевдогеометрические графы		2		8		0	5	[2]
12-13	Границы Хоффмана, Цветковича и Крейна для клик и клик		2		8		0	5	[7; 6]

14-15	Аutomорфизмы дистанционно транзитивных графов. Метод Хигмена	2		10		0	5	[2; 9]
16-17	Классификация конечных групп и симметричных графов	1		8		0	5	[5; 9; 12]
18	Классификация конечных групп и симметричных графов	1				0	30	
ИТОГО		16		74	экзамен	0	100	

Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Простейшие алгоритмы на графах и сетях	Практическое	4	Диалог	Использование интерактивных приложений для демонстрации графов на интерактивной доске
2	Связность и факторизации	Практическое	4	Диалог	Использование интерактивных приложений для демонстрации графов на интерактивной доске
3	Планарность и раскраски	Практическое	4	Диалог	Использование интерактивных приложений для демонстрации графов на интерактивной доске
4	Перечисление и кодирование графов	Практическое	4	Диалог	Использование интерактивных приложений для демонстрации графов на интерактивной доске

Учебно-методическое обеспечение самостоятельной работы.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Рекомендуемая литература:

а) основная литература:

1. Берж К. Теория графов и ее применения. Издательство иностранной литературы. Москва. 2009. 329с.
2. Камерон П., ван Линт Дж. Теория графов, теория кодирования и блок-схемы. – М.: Наука, 2004, 140с.
3. Мельников О.И. Теория графов в занимательных задачах. Изд.3. 2009, 232с.
4. Оре О. Графы и их применение. М.: Мир, 2005, 182с.
5. Харари Ф. Теория графов. Изд.2. М.: Едиториал УРСС, 2007, 296с.

Статьи

6. Веденев А.А., Кузнецов А.Н., Махнев А.А., Носов В.В. О хороших парах в реберно регулярных графах. //Дискрет.матем. 2003, т.15, с.77-97
7. Кабанов В.В., Махнев А.А. Кореберно регулярные графы, в которых окрестности вершин кореберно регулярны. Тез.докл. //III Международная конференция по алгебре, Красноярск, 1993, с.139
8. Махнев А.А. О псевдогеометрических графах некоторых частичных геометрий. //Вопросы алгебры, Гомель. Издательство Гомельского университета, 1997, Вып.11, с.60-67
9. Махнев А.А. О расширениях некоторых частичных геометрий, содержащих малые μ -подграфы. //Дискрет.анализ и исслед.операций. 1996, Т3, №3, с.71-83
10. Махнев А.А. О группах автоморфизмов частичных геометрий и их расширениях. //В: Международный алгебраический семинар, посвященный 70-летию кафедры высшей алгебры МГУ. Тез. Докладов 1999. – Москва.: Издательство мех-мата МГУ . – С.41-42
11. Махнев А.А. О сильной регулярности некоторых реберно регулярных графов. //Известия РАН, сер.матем. 2004, т.68, с.159-172

б) дополнительная литература

12. Ловас Л., Пламмер М. Прикладные задачи теории графов. Теория паросочетаний в математике, физике, химии. М.: Мир, 2008, 653с.
13. Татт. Теория графов. М.: Мир, 2008, 424с.
14. Уилсон Р. Введение в теорию графов. М.: Мир, 2007, 208с.

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
 - электронной библиотеке диссертаций РГБ,
 - университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
 - электронной картотеке газетно-журнальных статей,
 - электронной картотеке авторефератов диссертаций и диссертаций.

Рекомендуемые интернет-адреса по дисциплине

1. <http://www.mathnet.ru>
2. <http://www.intuit.ru/>

АННОТАЦИЯ

дисциплины «Теория групп»

Направление подготовки магистра

01.04.01 МАТЕМАТИКА

Профиль

«Алгебра»

25. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике. Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин:

алгебра, теория групп, криптография, защита информации,

26. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к блоку Б1.В.ОД.4 Дисциплины (модули). Вариативная часть. Обязательные дисциплины, обеспечивающих подготовку магистра по направлению 01.04.01 Математика профиль «Алгебра».

Дисциплина изучается в течение одного семестра.

27. Цели изучения дисциплины

Целью курса является формирование у магистрантов понятий, знаний и компетенций, позволяющих строить и анализировать модели систем реального мира с помощью структур и их свойств.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Теория групп» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность создавать и исследовать новые математические модели в естественных науках (ОПК-2);
- Способность к интенсивной научно-исследовательской работе (ПК-1).

Учебные задачи дисциплины:

В результате изучения дисциплины «Теория групп» магистрант должен:

Знать:

перестановки;
линейные пространства;
линейные операторы и линейные отображения;
теорию матриц;
основы теории групп;
основы теории полей;
основы теории колец
структуру расположения подгрупп
линейные группы

конечные группы
абелевы группы

Уметь:

применять полученные методы и модели к решению типовых и практических задач с использованием аппарата теории групп, основных алгебраических структур (группы, кольца, поля) ;
пользоваться формулами теории расположения подгрупп, теоремами теории конечных групп; классификацией конечных абелевых групп, теоремами Силова, строить критерии для проверки гипотез;
пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
применять полученные знания для изучения других дисциплин.

Иметь:

навыки применения алгебраических методов (в частности, теорем Силова) для решения различных прикладных задач;
навыки построения и исследования различных алгебраических структур.

4. Формы работы магистров

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 6 курса,
читается в 11 семестре

Лекционные занятия – 18 ч

Практические занятия – 18 ч

Самостоятельная работа – 36 ч

зачет в 11 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А., ст.преп. Джусоева Н.А.

12. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Теория групп» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по зачету, также предусматривающего набор необходимого количества баллов.

13. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен зачет (11 семестр). Максимальное количество баллов, которое может набрать студент, **100**.

За выполнение заданий текущего и промежуточного контроля студент может набрать максимальное количество баллов:

За первый модуль – 50 баллов (текущая работа Т1- 20 баллов и компьютерный тест М1 - 30 баллов).

За второй модуль –50 баллов (текущая работа Т2- 20 баллов и компьютерный тест М2 - 30 баллов).

14. Тематический план курса

11 семестр

Номер недели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия		Самостоятельная работа студентов		Формы контроля	Количество баллов		Литература
		л	пр	Содержание	Часы		мин	сек	
1	Линейные группы. Полная линейная группа над кольцом и ее подгруппы	2	2	Гомоморфизм линейных групп, фактор-группы.	4				[1, 2, 6,]
2	Группы перестановок	2	2	Симметрическая, знакопеременная группы и их подгруппы и порождающие элементы	4				[1, 4, 6,]
3	Теоремы Силова	2	2	Применение трех теорем Силова к группам небольших порядков, классы сопряженных элементов	4				[1, 2, 4,]
4	Действие группы на множестве.	2	2	Разбор различных примеров действия группы на множестве, построение орбит	4				[2, 4, 6,]
5	Стабилизатор. Примеры стабилизаторов	2	2	Применение стабилизаторов к классам сопряженных элементов	4				[1, 4, 6,]

6	Коммутант группы. Коммутант поной линейной группы.	2	2	Построение коммутантов известных групп. Фактор по коммутанту	4				[1, 2, 4, 6,]
7	Сети и сетевые группы над кольцом.	2	2	Действие группы перестановок на сетях, клеточные сети	4				[1, 2,, 6,]
8	Расположение подгрупп. Общая теория.	2	2	Построение графа по решетке промежуточных подгрупп, содержащих фиксированную подгруппу	4				[1, 4, 6,]
9	Порождающие элементы полной линейной группы	2	2	Трансвекции и псевдоотражения	4				[1, 2, 4,]
	ИТОГО	18	18		36				

1.6 Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение конечных групп небольших порядков	Практическое	2	Диалог	Использование на проекторе таблицы умножения групп
2	Построение конкретных колец классов вычетов	Практическое	2		Использование на проекторе таблицы умножения и сложения в кольцах
3	Применение теорем Силова	Практическое	2		Использование на проекторе

					таблицы умножения и сложения в полях
--	--	--	--	--	---

10.7. Учебно-методическое обеспечение самостоятельной работы.
Оценочные средства для текущего контроля успеваемости,
промежуточной аттестации по итогам освоения дисциплины.

№ Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре

Основная литература:

49. Белоногов В.А. Задачник по теории групп. М.: Наука. 2000. 238 с.
50. Койбаев В.А. Основы алгебры. – Владикавказ: СОГУ, 2005 (\\icd\books\math\Алгебра и Геометрия) (\\icd\books\math\Алгебра и Геометрия) - 10
51. Койбаев В.А. Подгруппы группы $GL(2,k)$, содержащие нерасщепимый максимальный тор. – Математическая монография. Владикавказ. 2009. 182с.
52. Каргаполов М.И., Мерзлякеов Ю.И. Основы теории групп. СПб.:Лань . 2009. 288с.

Дополнительная литература

53. Баскаков А.Г. Лекции по алгебре. – Воронеж. 2001
54. Кострикин А.И. Сборник задач по алгебре. – М. Физматлит, 2001.-464с

Электронный ресурс

6. Кострикин А.И. <http://review3d.ru/kostrikin-a-i-vvedenie-v-algebru-v-3-chastyax>
7. Каргаполов М.И., Мерзляков Ю.И. <http://www.vixri.ru/?p=1212>

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

дисциплины «Теория колец»

Направление подготовки магистра

01.04.01 МАТЕМАТИКА

Профиль

«Алгебра»

28. Требования к магистрантам

Изучение данной дисциплины базируется на следующих дисциплинах: алгебра и геометрия, теория чисел. Магистры должны владеть знаниями и компетенциями, соответствующими программе бакалавриата по математике. Основные положения дисциплины должны быть использованы в дальнейшем при изучении дисциплин:

алгебра, Теория колец, криптография, защита информации,

29. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина относится к дисциплинам профессионального цикла, обеспечивающих подготовку магистра по направлению 01.04.01 Математика профиль «Алгебра».

Дисциплина изучается в течение одного семестра.

30. Цели изучения дисциплины

Целью курса является формирование у магистрантов понятий, знаний и компетенций, позволяющих строить и анализировать модели систем реального мира с помощью структур и их свойств.

Фундаментальность и прикладная направленность обучения реализуется путем тщательного отбора учебного материала в соответствии с классическими и современными результатами. Основными видами занятий при изучении дисциплины «Теория колец» являются: лекции, практические занятия и самостоятельная работа.

В рамках лекционных занятий основное внимание уделяется изложению теоретических основ курса, доказательству основных теорем. Для закрепления теоретического материала на лекциях целесообразно проведение мини-опросов и коротких тестов. Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Содержание лекций определяется рабочей программой курса.

Целью практических занятий является закрепление теоретических знаний, выработка навыков решения задач.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

- Способность создавать и исследовать новые математические модели в естественных науках (ОПК-2);
- Способность к интенсивной научно-исследовательской работе (ПК-1).

Учебные задачи дисциплины:

В результате изучения дисциплины «Теория колец» магистрант должен:

Знать:

линейные пространства;
линейные операторы и линейные отображения;
теорию матриц;
основы теории групп;
основы теории полей;
основы теории колец
идеалы и операции над ними
линейные группы

конечные группы
абелевы группы

Уметь:

применять полученные методы и модели к решению типовых и практических задач с использованием аппарата теории колец, основных алгебраических структур (группы, кольца, поля) ;
пользоваться формулами и теоремами теории колец и идеалов;
строить критерии для проверки гипотез;
пользоваться библиотекой прикладных программ для вычислительных методов алгебры;
применять полученные знания для изучения других дисциплин.

Иметь:

навыки применения алгебраических методов (в частности, методов теории колец) для решения различных прикладных задач;
навыки построения и исследования различных алгебраических структур.

4. Формы работы магистров

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

Обязательный курс для магистров 6 курса,
читается в 11 семестре

Лекционные занятия – 18 ч

Практические занятия – 18 ч

В интенсивной форме практические занятия – 4ч

Самостоятельная работа – 72 ч

Контроль – 36 ч

экзамен в 11 семестре

За курс отвечает кафедра алгебры и геометрии,

Авторы программы: профессор Койбаев В.А., ст.преп. Джусоева Н.А.

15. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Теория колец» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по зачету, также предусматривающего набор необходимого количества баллов.

16. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен экзамен (11 семестр). Максимальное количество баллов, которое может набрать студент, **100**.

За выполнение заданий текущего и промежуточного контроля студент может набрать максимальное количество баллов:

За первый модуль – 50 баллов (текущая работа Т1- 20 баллов и компьютерный тест М1 - 30 баллов).

За второй модуль –50 баллов (текущая работа Т2- 20 баллов и компьютерный тест М2 - 30 баллов).

17. Тематический план курса

11 семестр

Номер недели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия		Самостоятельная работа студентов		Формы контроля	Количество баллов		Литература
		л	пр	Содержание	Часы		мин	сек	
1	Примеры коммутативных и некоммутативных колец	2	2	.Области целостности, области главных идеалов, кольца Безу, евклидовы кольца	10				[1,3,4,12]
2	Гомоморфизмы колец. Примеры. Гомоморфизмы, связанные с линейными группами над кольцами.	2	2	Гомоморфизмы, связанные с линейными группами над кольцами. Линейные группы над кольцами	16				[3,4,12]
3	Идеалы, простые и максимальные идеалы, операции над идеалами. Область главных идеалов.	2	2	Сужение и расширение как операции над идеалами,. Идеалы некоммутативных колец	14				[1,4]
4	Фактор-кольцо по простому и максимальному идеалу. Существование максимального идеала в коммутативном кольце	2	2	Поля и области целостности – как фактор-кольца по простым и максимальным идеалам. Примеры	16				[1,4]
5	Радикал кольца, локальные	2	2	Радикал	14				[1,4]

	кольца			кольца, локальные кольца, радикал Джекобсона, критерий локальности кольца]
6	Нильпотентные элементы и делители нуля	2	2	Нильпотентные элементы и делители нуля. Примеры в кольце классов вычетов	10				[2,4 ,12]
7	Кольцо классов вычетов и применение в криптосистеме RSA	2	2	Теоремы теории колец в кольце классов вычетов, объясняющие алгоритм криптосистемы RSA	16				[2,4]
8	ОГИ. Факториальные кольца. Конечные коммутативные кольца	2	2	Конечные коммутативные кольца. Классификация конечных коммутативных колец	12				[3,1 2]
9	Кольца частных	2	2						[4,1 2]
	ИТОГО	18	18		108				

1.6 Образовательные технологии

Лекции, практические занятия, самостоятельная работа студентов.

Используются интерактивные методы обучения: творческие задания, разработка проектов, исследовательский метод обучения.

№/п.	Тема	Вид занятия	Количество часов	Активные формы	Интерактивные формы
1	Построение конечных колец небольших порядков	Практическое	2	Диалог	Использование на проекторе таблицы умножения и сложения в кольцах

2	Построение конкретных колец классов вычетов	Практическое	2		Использование на проекторе таблицы умножения и сложения в кольцах
3	Примеры неизоморфных колец одинаковых порядков	Практическое	2		Использование на проекторе таблицы умножения и сложения в полях

10.8. Учебно-методическое обеспечение самостоятельной работы.
Оценочные средства для текущего контроля успеваемости,
промежуточной аттестации по итогам освоения дисциплины.

№ Перечень основной и дополнительной литературы, методических разработок; с указанием наличия в библиотеке, на кафедре

Основная литература:

55. Ван дер Варден Б. Л. Алгебра. – М.: Лань, 2004. 648с.

56. Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005(\\icd\books\math\Алгебра и Геометрия) (\\icd\books\math\Алгебра и Геометрия) - 10

57. Кострикин А.И. Введение в алгебру. Ч.1-3 М., МЦМНО, 2009. 838с.

58. Атья М., Макдональд И. Введение в коммутативную алгебру. - Факториал, 2003. 160с.

<http://math-portal.ru/2729-vvedenie-v-kommutativnuyu-algebru-atiya-m.html>

59. Курош А.Г. Курс высшей алгебры. 17-е изд., стер. - СПб. :Лань, 2008. - 432 с

60. Кострикин А.И. Сборник задач по алгебре.-М., Физматлит, 2001.-464 с.

Дополнительная литература

61. Баскаков А.Г. Лекции по алгебре. – Воронеж. 2001

62. Кострикин А.И. Сборник задач по алгебре. – М. Физматлит, 2001.-464с

Электронный ресурс

63. Фаддеев Д.К., Соминский И.С. Задачи по высшей алгебре.

<http://math-portal.ru/izdatelstvo/261-zadachi-po-vysshey-algebre-13-e-izdanie.html>

64. Кострикин А.И. Введение в алгебру.

<http://math-portal.ru/190-vvedenie-v-algebru-osnovy-algebry.html>

65. Курош А.Г. Курс высшей алгебры.

<http://math-portal.ru/izdatelstvo/182-kurs-vysshey-algebry.html>

66. Ленг С. Алгебра

<http://math-portal.ru/260-algebra-leng.html>

67. Ван дер Варден. Алгебра.

<http://math-portal.ru/276-algebra-bl-van-der-varden.html>

68. Атья М., Макдональд И. Введение в коммутативную алгебру.

<http://math-portal.ru/2729-vvedenie-v-kommutativnuyu-algebru-itya-m.html>

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

АННОТАЦИЯ

КУРСА «Теория разделения секрета»

ДЛЯ МАГИСТРОВ

ПО НАПРАВЛЕНИЮ 01.04.01 «Математика», ПРОФИЛЬ «Алгебра»

1. Требования к студентам

Изучение данной дисциплины базируется на следующих дисциплинах: школьный курс математики (программа средней общеобразовательной школы), «Алгебра». Студенты должны владеть знаниями и компетенциями, соответствующими школьной программе по математике.

2. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина является дисциплиной блока Б1.В.ДВ.1.2 Дисциплины (модули). Вариативная часть. Дисциплины по выбору. Дисциплина «Теория разделения секрета» необходима для овладения теоретическими и практическими знаниями, лежащими в основе общенаучных дисциплин компьютерных наук, а также курсов, изучающих конкретные задачи программирования.

Изучению дисциплины «Теория разделения секрета» предшествует изучение школьных курсов математики, а также курсов «Алгебра».

Знания, полученные при изучении дисциплины «Теория разделения секрета», могут быть использованы при изучении курсов «Алгебра и криптография» и др.

Дисциплина изучается в течение одного семестра.

3. Цели изучения дисциплины

«Теория разделения секрета» – это специальный курс, являющийся неотъемлемой частью широкого круга предметов по математике. Он в числе тех дисциплин, на которых строится все здание современной прикладной математической науки.

Задачей дисциплины «Теория разделения секрета» является формирование и развитие абстрактного мышления студентов в процессе изучения основных понятий и структур, используемых во всех остальных математических дисциплинах, связанных с прикладными вопросами алгебры и криптографии. Программа предназначена для студентов первого курса магистратуры математического факультета и учитывает специфику данного факультета.

Рабочая программа составлена на основе государственного образовательного стандарта, определяющего государственные требования к минимуму содержания и уровню подготовки специалистов с высшим образованием по программе «Алгебра» направления «Математика».

Достижение этих целей обеспечивает выпускнику получение высшего профессионально профилированного образования и обладание перечисленными ниже общими и предметно-специализированными компетенциями.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

а) общепрофессиональных (ОПК):

- Способность создавать и исследовать новые математические модели в естественных науках (ОПК-2).

б) профессиональных (ПК):

- Способность к собственному видению прикладного аспекта в строгих математических формулировках (ПК-6).

В результате изучения дисциплины, бакалавр должен:

знать:

1. основные понятия и определения алгебры и их взаимосвязь;
2. освоить различные методы решения алгебраических задач по изучаемым темам;
3. иметь представления о современных направлениях развития и использования аппарата в других математических дисциплинах;
4. обладать навыками самостоятельной работы с учебной, методической и научной литературой.

уметь:

1. применять полученные методы и модели к решению типовых и практических задач криптографии и теории кодирования, строить матрицы, позволяющие при кодировании распознавать и исправлять ошибки при передаче информации,
2. применять полученные знания для изучения других дисциплин.

иметь:

1. навыки применения алгебраических методов для решения различных прикладных задач, связанных криптографией, с распознаванием слов, в которых допущено некоторое количество ошибок,
2. навыки построения и исследования различных алгебраических структур.

4. Формы работы студентов

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

5. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Теория разделения секрета» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по зачету, также предусматривающего набор необходимого количества баллов.

6. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен зачет. Максимальное количество баллов, которое может набрать студент, **100**.

За выполнение заданий текущего и промежуточного контроля студент может набрать максимальное количество баллов:

За первый модуль – 50 баллов (текущая работа Т1- 20 баллов и компьютерный тест М1 - 30 баллов).

За второй модуль –50 баллов (текущая работа Т2- 20 баллов и компьютерный тест М2 - 30 баллов).

Зачет проводится в конце 11 семестра. На зачете студент имеет возможность набрать 3- 60 баллов. Результирующий балл определяется по формуле: $T1+T2+(M1+M2+3)/2$. Студент, набравший более 56 баллов в течение семестра, от зачета может быть освобожден. Допуск к зачету (экзамену) по дисциплине разрешен при наличии у студента 36 баллов за работу в течение семестра.

Обязательный курс для студентов 5 курса магистратуры, читается в 10 семестре

Лекционные занятия – 0 часов

Практические занятия – 18 часов

Самостоятельная работа – 54 часов

За курс отвечает кафедра алгебры и геометрии,

Автор программы: Койбаев В.А.

7. Тематический план курса

Распределение разделов по аудиторным часам (ЛЗ – лекционные занятия, ПЗ – практические занятия, СР – самостоятельная работа, АЗ – аудиторные занятия, ЛАБЗ – лабораторные занятия).

Аудиторные занятия (лекции, лабораторные, практические, семинарские) по алгебре.

Кол. часов	Вид занятия, тема и краткое содержание
Лекции	Лекции
2	Теория сравнений
2	Разделение секрета на основе китайской т. об остатках Теория распознавания сигналов
2	Кодирующие матрицы
2	Распознавание ошибок

2	Исправление ошибок на основе кодирующих матриц
2	Задача о принятии решения на основе разделения секрета
4	Разделение секрета на основе матриц Практическое применение теории разделения секрета

2.2. Самостоятельная работа студента

Темы, разделы, вынесенные на самостоятельную подготовку, вопросы к практическим занятиям; тематика рефератной работы; рекомендации по использованию литературы. Самостоятельное изучение отдельных тем курса.	Методы
. Общая теория передачи информации	И
(m, n)-коды и кодирующие матрицы	И
Матрицы, распознающие одну ошибку	И
Матрицы, исправляющие одну ошибку	И

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Яценко В.В. Введение в криптографию. – М. ЧеРо. 2000.
2. Алферов А.П. и др. Основы криптографии. – М. Гелиос АРВ. 2001.
3. Кострикин А.И. Введение в алгебру – М. Наука. 1977.
4. Борович З.И., Шафаревич И.Р. Теория чисел. – М. Наука. 1985.
5. Виноградов И.М. Основы теории чисел. – М. Наука. 2008.
6. Ноден П., Ките К. Алгебраическая алгоритмика. – М. Мир. 1999.
7. Коблиц Н. Курс теории чисел и криптографии. – М. ТВП. 2001.

АННОТАЦИЯ КУРСА

«Элементарные сети в линейных группах»

ДЛЯ МАГИСТРОВ

ПО НАПРАВЛЕНИЮ 01.04.01 «Математика», ПРОФИЛЬ «Алгебра»

4. Требования к студентам

Изучение данной дисциплины базируется на следующих дисциплинах: школьный курс математики (программа средней общеобразовательной школы), «Алгебра». Студенты должны владеть знаниями и компетенциями, соответствующими школьной программе по математике.

5. Краткая характеристика данной дисциплины, ее особенности

Настоящая дисциплина является дисциплиной блока Б1.В.ОД.3 Дисциплины (модули). Вариативная часть. Обязательные дисциплины. Дисциплина «Элементарные сети в линейных группах» необходима для овладения теоретическими и практическими знаниями, лежащими в основе общенаучных дисциплин компьютерных наук, а также курсов, изучающих конкретные задачи программирования.

Изучению дисциплины «Элементарные сети в линейных группах» предшествует изучение школьных курсов математики, а также курсов «Алгебра».

Знания, полученные при изучении дисциплины «Элементарные сети в линейных группах», могут быть использованы при изучении курсов «Алгебра и криптография» и др.

Дисциплина изучается в течение одного семестра.

6. Цели изучения дисциплины

«Элементарные сети в линейных группах» – это специальный курс, являющийся неотъемлемой частью широкого круга предметов по математике. Он в числе тех дисциплин, на которых строится все здание современной прикладной математической науки.

Задачей дисциплины «Элементарные сети в линейных группах» является формирование и развитие абстрактного мышления студентов в процессе изучения основных понятий и структур, используемых во всех остальных математических дисциплинах, связанных с прикладными вопросами алгебры и криптографии. Программа предназначена для студентов первого курса магистратуры математического факультета и учитывает специфику данного факультета.

Рабочая программа составлена на основе государственного образовательного стандарта, определяющего государственные требования к минимуму содержания и уровню подготовки специалистов с высшим образованием по программе «Алгебра» направления «Математика».

Достижение этих целей обеспечивает выпускнику получение высшего профессионально профилированного образования и обладание перечисленными ниже общими и предметно-специализированными компетенциями.

Решение познавательных задач в соответствии с поставленной целью выражается в формировании следующих **компетенций**:

а) профессиональных (ПК):

- Способность к интенсивной научно-исследовательской работе (ПК-1);
- Способность к собственному видению прикладного аспекта в строгих математических формулировках (ПК-6).

В результате изучения дисциплины, бакалавр должен:

знать:

5. основные понятия и определения алгебры и их взаимосвязь;
6. освоить различные методы решения алгебраических задач по изучаемым темам;
7. иметь представления о современных направлениях развития и использования аппарата в других математических дисциплинах;
8. обладать навыками самостоятельной работы с учебной, методической и научной литературой.

уметь:

3. применять полученные методы и модели к решению типовых и практических задач криптографии и теории кодирования, строить матрицы, позволяющие при кодировании распознавать и исправлять ошибки при передаче информации,
4. применять полученные знания для изучения других дисциплин.

иметь:

3. навыки применения алгебраических методов для решения различных прикладных задач, связанных криптографией, с распознаванием слов, в которых допущено некоторое количество ошибок,
4. навыки построения и исследования различных алгебраических структур.

8. Формы работы студентов

Формами работы студентов являются лекции, практические занятия, выполнение контрольных работ, контрольные модульные тестирования, самостоятельная работа.

9. Виды контроля

Модульный принцип выстраивания познавательного комплекса дисциплины «Элементарные сети в линейных группах» основывается на организации учебного процесса, предусматривающей оценку интеллектуальной активности студента в баллах. Выполнение комплекса учебных заданий, выраженное в набранном количестве баллов, определяет промежуточный, а также итоговый результат в виде экзамена за усвоение дисциплины. Изучение материала в рамках отдельного модуля осуществляется в форме аудиторных занятий (лекции и лабораторные занятия), но с акцентом на выполнение самостоятельной работы.

Контроль знаний студентов осуществляется в форме тестирования по зачету, также предусматривающего набор необходимого количества баллов.

10. Методика формирования результирующей оценки

Учебным планом по данной дисциплине предусмотрен зачет. Максимальное количество баллов, которое может набрать студент, **100**.

За выполнение заданий текущего и промежуточного контроля студент может набрать максимальное количество баллов:

За первый модуль – 50 баллов (текущая работа Т1- 20 баллов и компьютерный тест М1 - 30 баллов).

За второй модуль –50 баллов (текущая работа Т2- 20 баллов и компьютерный тест М2 - 30 баллов).

Экзамен проводится в конце 10 семестра. На зачете студент имеет возможность набрать 3- 60 баллов. Результирующий балл определяется по формуле: $T1+T2+(M1+M2+3)/2$. Студент, набравший более 56 баллов в течение семестра, от зачета может быть освобожден. Допуск к зачету (экзамену) по дисциплине разрешен при наличии у студента 36 баллов за работу в течение семестра.

Обязательный курс для студентов 5 курса магистратуры, читается в 10 семестре

Лекционные занятия – 16 часов

Практические занятия – 16 часов

Самостоятельная работа – 76 часов

За курс отвечает кафедра алгебры и геометрии,

Автор программы: Койбаев В.А.

11. Тематический план курса

Распределение разделов по аудиторным часам (ЛЗ – лекционные занятия, ПЗ – практические занятия, СР – самостоятельная работа, АЗ – аудиторные занятия, ЛАБЗ – лабораторные занятия).

Аудиторные занятия (лекции, лабораторные, практические, семинарские) по алгебре.

10 семестр

Но ме р не де ли	Наименование тем (вопросов), изучаемых по данной дисциплине	За нятия		Самостоятельная работа студентов		Формы контро ля	Количес тво баллов		Лит ера тура
		л	р	Содержание	Ча сы		mi n	ma x	
1	Теоремы о гомоморфизме.	2	2	Примеры применения теорем о гомоморфизм е.	6				[2,6, 8]
2	Действие группы на множестве. Стабилизатор.	2	2	Примеры действия группы на	10				[2,6, 8]

				множестве. Стабилизатор ы					
3	Теоремы Эйлера и Ферма и обращение криптографического шифрования	2	2	Примеры применения теорем Эйлера и Ферма для построения шифрования	10				[2, 5]
4	Китайская теорема об остатках	2	2	Примеры применения китайской теоремы об остатках	10				[4, 5]
5	Криптографическая система RSA	2	2	Обоснование криптографической системы RSA и примеры открытого шифрования	10				[4, 5]
6	Электронная подпись	2	2	Формирование электронной подписи и примеры электронной подписи	10				[4, 5]
7	Схема разделения секрета	2	2	Пример применения схемы разделения секрета на задаче о принятии решения при отсутствии руководителя	10				[1,4]
8	Шифрование с помощью алгоритма рюкзака	2	2	Примеры построения шифрования с помощью алгоритма рюкзака	10				[1,4]
	ИТОГО	16	16		76				

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Яценко В.В. Введение в криптографию. – М. ЧеРо. 2000.

2. Алферов А.П. и др. Основы криптографии. – М. Гелиос АРВ. 2001.
3. Кострикин А.И. Введение в алгебру – М. Наука. 1977.
4. Боревич З.И., Шафаревич И.Р. Теория чисел. – М. Наука. 1985.
5. Виноградов И.М. Основы теории чисел. – М. Наука. 2008.
6. Ноден П., Ките К. Алгебраическая алгоритмика. – М. Мир. 1999.
7. Коблиц Н. Курс теории чисел и криптографии. – М. ТВП. 2001.

*Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Северо-Осетинский государственный университет
имени Коста Левановича Хетагурова»*

ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

«Утверждаю»

Первый проректор

_____ Л.А.Агузарова

« _____ » _____ 2018 г.

ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА магистров

по направлению 01.04.01 «Математика»

Программа «Алгебра»

Владикавказ, 2018

Государственный экзамен является составной частью итоговой государственной аттестации по направлению 01.04.01 «Математика», Программа «Алгебра» проводится в соответствии с Положением о государственной итоговой аттестации и определяет уровень усвоения студентом материала, охватывающего содержание общепрофессиональных и специальных дисциплин, содержащихся в учебных планах специализированных программ подготовки магистра.

Программа итогового государственного экзамена по направлению 01.04.01 «Математика» специализированной магистерской подготовки по программе «Алгебра» разработана в соответствии с Федеральным Государственным образовательным стандартом высшего образования подготовки магистров по направлению 01.04.01 «Математика».

Программа содержит список дисциплин, включенных в итоговый государственный экзамен, с раскрытием тематики каждого курса согласно ФГОС ВО и рабочим программам, разработанным на кафедрах факультета математики и информационных технологий. По каждой дисциплине приводится список источников, необходимых для подготовки к экзамену.

Программа включает в себя дисциплины: Теория групп, Теория колец, Компьютерные технологии в науке и образовании, Расширение полей

ТЕМАТИКА ДИСЦИПЛИН, ВХОДЯЩИХ В ИТОГОВЫЙ ГОСУДАРСТВЕННЫЙ ЭКЗАМЕН

«Теория групп»

«Теория групп» – это специальный курс, являющийся неотъемлемой частью широкого круга предметов по математике. Он в числе тех дисциплин, на которых строится все здание современной прикладной математической науки.

Задачей дисциплины «Теория групп» является формирование и развитие абстрактного мышления студентов в процессе изучения основных понятий и структур, используемых во всех остальных математических дисциплинах, связанных с теоретическими и прикладными вопросами алгебры. Программа предназначена для студентов первого курса магистратуры факультета математики и информационных технологий и учитывает специфику данного факультета.

Содержание курса:

Линейные группы. Полная линейная группа над кольцом и ее подгруппы.

Конечные группы

Теоремы Силова.

Действие группы на множестве.

Стабилизатор. Примеры стабилизаторов.

Конечные абелевы группы. Сети и сетевые группы над кольцом.

Расположение подгрупп. Общая теория.
Сетевые кольца.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература

1. Атья М., Макдональд И. Введение в коммутативную алгебру. - Факториал, 2003. 160с.
2. Баскаков А.Г. Лекции по алгебре. – Воронеж. 2001.
3. Борович З.И. Определители и матрицы. – М. Наука. 1988.
4. Ван дер Варден Б. Л. Алгебра. – М.: Лань, 2004. 648с.
5. Койбаев В.А. Основы алгебры. – Владикавказ. Изд-во СОГУ. 2005. 201с.
6. Койбаев В.А. Подгруппы группы $GL(2, k)$, содержащие нерасщепимый тор. – Итоги науки. Южный федеральный округ. ЮМИ ВНЦ РАН. Математическая монография. 2009. Владикавказ. 183 с. Кострикин А.И. Введение в алгебру. Ч.1-3 М., МЦМНО, 2009. 838с.
7. Кострикин А.И. Сборник задач по алгебре.-М., Физматлит, 2001.-464 с.
8. Курош А.Г. Курс высшей алгебры. 17-е изд., стер. - СПб. : Лань, 2008. - 432 с

Дополнительная литература (электронные ресурсы)

9. Борович З.И., Шафаревич И.Р.
http://vmate.ru/load/uchebniki/teorija_chisel/z_i_borevich_i_r_shafarevich_teoriya_chisel/35-1-0-354
10. Ван дер варден <http://www.twirpx.com/file/55725/>
11. Виноградов И.М.
http://vmate.ru/load/uchebniki/teorija_chisel/vinogradov_i_m_osnovy_teorii_chisel/35-1-0-267
12. Каргаполов М.И., Мерзляков Ю.И. <http://www.vixri.ru/?p=1212>
13. Кострикин А.И. <http://review3d.ru/kostrikin-a-i-vvedenie-v-algebru-v-3-chastyax>
14. Ленг С. <http://log-in.ru/books/algebra-leng-s-nauka-i-obrazovanie/>
15. Фаддеев, Соминский И.С. <http://lib.convdocs.org/docs/index-47661.html>

«Теория колец»

«Теория колец» – один из специальных курсов по программе «Алгебра» подготовки магистров по направлению «Математика».

Основы теории колец были заложены в 19 веке, в период становления алгебры. Одним из ярчайших основателей алгебры является Э.Галуа, создавший теорию конечных полей. Теория колец представляет собой один из основных разделов алгебры и вместе со своими разнообразными приложениями хорошо представлено в монографической литературе. Она позволяет охватить алгебраическими методами важные аспекты современной математики.

Основная цель курса «Теории колец» – дать студентам представление о принципах и методах данной теории.

Задачи курса – научить студентов использовать методологию теории колец.

Содержание курса

Идеалы, простые и максимальные идеалы, операции над идеалами.

Область главных идеалов.

Фактор-кольцо по простому и максимальному идеалу. Существование максимального идеала в коммутативном кольце

Радикал кольца, локальные кольца

Нильпотентные элементы и делители нуля

Кольцо классов вычетов и применение в криптосистеме RSA

ОГИ. Факториальные кольца.

Конечные коммутативные кольца

Кольца частных

Области целостности, области главных идеалов, кольца Безу, евклидовы кольца

Гомоморфизмы, связанные с линейными группами над кольцами. Линейные группы над кольцами

Сужение и расширение как операции над идеалами, Идеалы некоммутативных колец

Поля и области целостности – как фактор-кольца по простым и максимальным идеалам. Примеры

Радикал кольца, локальные кольца, радикал Джекобсона, критерий локальности кольца

Нильпотентные элементы и делители нуля. Примеры в кольце классов вычетов

Теоремы теории колец в кольце классов вычетов, объясняющие алгоритм криптосистемы RSA

Конечные коммутативные кольца. Классификация конечных коммутативных колец

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература:

1. Ван дер Варден Б. Л. Алгебра. – М.: Лань, 2004. 648с.
2. Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005(\\icd\books\math\Алгебра и Геометрия) (\\icd\books\math\Алгебра и Геометрия) - 10
3. Кострикин А.И. Введение в алгебру. Ч.1-3 М., МЦМНО, 2009. 838с.
4. Атья М., Макдональд И. Введение в коммутативную алгебру. - Факториал, 2003. 160с.
<http://math-portal.ru/2729-vvedenie-v-kommutativnuyu-algebru-aty-a-m.html>

5. Курош А.Г. Курс высшей алгебры. 17-е изд., стер. - СПб. :Лань, 2008. - 432 с
6. Кострикин А.И. Сборник задач по алгебре.-М., Физматлит, 2001.-464 с.
Дополнительная литература
7. Баскаков А.Г. Лекции по алгебре. – Воронеж. 2001
8. Кострикин А.И. Сборник задач по алгебре. – М. Физматлит, 2001.-464с
Электронный ресурс
9. Фаддеев Д.К., Соминский И.С. Задачи по высшей алгебре.
<http://math-portal.ru/izdatelstvo/261-zadachi-po-vysshey-algebre-13-e-izdanie.html>
10. Кострикин А.И. Введение в алгебру.
<http://math-portal.ru/190-vvedenie-v-algebru-osnovy-algebry.html>
11. Курош А.Г. Курс высшей алгебры.
<http://math-portal.ru/izdatelstvo/182-kurs-vysshey-algebry.html>
12. Ленг С. Алгебра
<http://math-portal.ru/260-algebra-leng.html>
13. Ван дер Варден. Алгебра.
<http://math-portal.ru/276-algebra-bl-van-der-varden.html>
14. Атья М., Макдональд И. Введение в коммутативную алгебру.
<http://math-portal.ru/2729-vvedenie-v-kommutativnuyu-algebru-atiya-m.html>

в) Интернет-ресурсы

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):

- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;
- собственным библиографическим базам данных:
- электронному каталогу,
- электронной картотеке газетно-журнальных статей,
- электронной картотеке авторефератов диссертаций и диссертаций.

а. Материально-техническое оснащение дисциплины:

Компьютерный класс, доступ к сети Интернет (во время самостоятельной работы), оргтехника, электронная база данных библиотеки СОГУ, лекционные аудитории; кабинет, оснащенный интерактивной доской, проектором.

«Компьютерные технологии в науке и образовании»

В условиях информатизации науки и образования, формирования глобального информационно-коммуникационного пространства, а также единой информационной научно-образовательной среды, к качеству труда и уровню квалификации научно-педагогических кадров предъявляются особые требования, соответствие которым, как правило, не обеспечивается освоением базового курса информатики и спецкурсов информационных технологий в рамках основных специальностей и направлений подготовки. С этих позиций освоение вопросов эффективного использования всего спектра доступных информационных и телекоммуникационных технологий, изложенных в программе, будет способствовать формированию у магистрантов готовности выполнять профессиональные функции, в соответствии с принятыми нормами и стандартами. Цель дисциплины – повышение профессиональной подготовки магистров на основе использования современных информационных технологий.

Задачи дисциплины: формировать у магистрантов представления о характере и тенденциях развития современных информационных технологий; формировать потребность в углубленном изучении компьютерных технологий как фактора повышения профессиональной компетентности; совершенствовать способы и средства получения, анализа и обобщения научных данных, их математико-статистической обработки; углубить изучение современных компьютерных средств коммуникационного общения и современных средств информатизации научной и образовательной деятельности.

Содержание курса

Основные понятия и термины информатики. Анализ основных понятий «информация», «информатика», «информационные процессы», «информационные технологии», «информационные системы», «информационные ресурсы». Различные трактовки и различные аспекты использования понятия «информация» в некоторых науках. Характеристика информатики как научной дисциплины.

Структура и виды информационных технологий научного и образовательного направлений. Структура информационных технологий. Виды информационных технологий. Информационная технология обработки данных. Информационная технология управления. Информационная технология поддержки принятия решений. Информационная технология экспертных систем. Авторские информационные технологии: гипертекст, мультимедиа; информационное моделирование. Интегрированные информационные технологии: информационные хранилища, системы электронного документооборота; геоинформационные системы; видеоконференция. Информационные технологии дистанционного обучения. Технологии искусственного интеллекта. Сетевые информационные технологии.

Информатизация общества и образования: исторический и методологический аспекты. Информатизация общества и проблемы образования. Вызовы XXI века в контексте информатизации образования: информационный вызов, динамический вызов. Информатизация общества: исторический аспект (основные информационные революции). Признаки

информационного общества. Информатизация системы образования. Этапы информатизации образования. Информатизация образования как глобальная проблема современности.

Педагогическая информатика как межпредметная и научная дисциплина. Краткая характеристика педагогической информатики как новой научной дисциплины, изучающей различные аспекты использования информационных технологий в системе образования.

Информационное общество и информационная культура человека. Признаки информационного общества. Характеристика понятия «информационная культура человека». Четыре уровня приобщения человека к миру информатики. Составные части информационной культуры человека.

Методология «компьютерного обучения». Характеристика методологии «компьютерного обучения». Классификация программных средств учебного назначения. Модели обучения с использованием информационных технологий («лекция с обратной связью», «лекция без обратной связи», «диагностика», «дистанционное обучение», «инструмент преподавателя», «инструмент учащегося»). Методы компьютерного обучения; метод информирования; ассоциативный метод; метод программирования учебной деятельности; метод компьютерного моделирования; метод проектов; метод «непоставленных задач»; метод ситуационного моделирования

Методические аспекты применения информационных технологий в обучении. Классификация программных средств учебного назначения. Программные средства в зависимости от вида управляющих воздействий. Программные средства в зависимости от этапа обучения. Программные средства для решения дидактических задач. Классификация инструментальных средств педагогического назначения. Классификация программных средств, ориентированных на организацию учебного процесса.

Образование в информационном обществе: современные тенденции развития информатизации образования. Современные проблемы образования. Современные тенденции развития информатизации образования. Информатизация – ведущая тенденция развития образования.

Технология создания и обработки текстовой информации. Этапы создания текстовых документов. Основные операции с текстом: ввод, редактирование, форматирование, оформление, печать документа. Проверка правописания. Ввод в документ формул, графических объектов. Редактирование вставленных графических материалов. Создание рисунков с помощью средств Word. Подготовка научной публикации.

Технология обработки числовой информации в электронных таблицах. Основные принципы работы с электронными таблицами. Способы адресации, ввод данных и формул. Построение диаграмм, графиков. Форматирование и оформление таблиц. Анализ и математико-статистическая обработка данных.

Технология создания мультимедийных программно-педагогических средств. Технология работы с программно-педагогическими средствами. Создание образовательного контента, с использованием текстовой информации, графических файлов, аудио - и видеоматериалов. Создание мультимедийных

обучающих систем. Технологии работы с базами данных образовательного назначения. Технология создания Web-страниц физкультурно-спортивной тематики.

Интернет-технологии в процессе поиска и обмена профессионально-значимой информацией. Характеристика Интернет-технологий. Популярные браузеры. Поиск и получение научной и спортивно-педагогической информации в Интернете. Электронная почта и Internet-сервисы электронной почты. Телеконференции (Internet News).

Технология подготовки компьютерных презентаций. Программы подготовки презентаций. Создание новой презентации. Анимация объектов слайда и эффекты при смене слайдов. Операции со слайдами: создание, добавление, перемещение. Графические объекты в презентациях. Приемы анимации. Модификация и демонстрация презентаций. Создание и применение шаблонов презентации. Подготовка презентации к демонстрации. Демонстрация презентации.

Технология создания и обработки аудио и видеоматериалов. Технология записи на диски CD и DVD. Возможности информационных технологий в создании и использовании аудио- и видео материалов в профессиональной деятельности. Встроенные функции Windows, обеспечивающие работу со звуком. Создание и обработка аудиоматериалов с помощью специальных программ. Создание видеозаписей. Обработка видеoinформации на компьютере. Технологии записи на диски *CD* и *DVD*.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература

1. Биллиг В.А. Объектное программирование в классах на С# 3.0 ИНТУИТ: национальный открытый университет.
http://www.intuit.ru/goods_store/ebooks/8476
2. Комлев Н. Объектно Ориентированное Программирование. Хорошая книга для Хороших Людей. Солон-Пресс. 2012 г. 298 стр.
3. Непейвода Н. Стили и методы программирования. Курс лекций. Учебное пособие. Интернет-университет информационных технологий. 2005. 320 стр.
4. Петрухин В.А., Лаврищева Е.М. Методы и средства инженерии программного обеспечения. ИНТУИТ: национальный открытый университет.
http://www.intuit.ru/goods_store/ebooks/8367

Дополнительная литература

5. Захарова И.Г. Информатика. Введение в Internet – технологии. Технологии работы с правовыми базами данных. Учебно-методический комплекс / И.Г. Захарова - 2-е издание. Тюмень: Издательство Тюменского госуниверситета, 2002. 252 с.
6. Захарова И.Г. Возможности информационных технологий в совершенствовании образовательного процесса высшей школы: Монография. / И.Г. Захарова. Тюмень: Издательство Тюменского госуниверситета, 2002. 176 с

7. Советов Б.Я. Информационные технологии :учебник для вузов / Б.Я. Советов, В.В.Цехановский.–3-е изд., стер. – М.: Высшая школа, 2006. 263 с.
8. Федоров А.И. Методологические аспекты информатизации высшего физкультурного образования: Учебное пособие / А.И.Федоров. Челябинск: УралГАФК, 2001. 248 с.
9. Федоров А.И Информационные технологии в физической культуре и спорте: Учебное пособие / А.И Федоров, Д.Л.Куликов. Челябинск: УралГАФК, ЧГНОЦ УрО РАО, 2003. 96 с.
- 10.Шестаков М.П. Статистика. Обработка спортивных данных на компьютере: учеб. пособие / ред. М. П. Шестаков, Г. И. Попов. – М.: СпортАкадемПресс, 2002. – 271 с.

«Расширение полей»

Изучение данной дисциплины позволяет формировать у магистрантов понятия, знания и компетенции, позволяющих строить и анализировать модели систем реального мира с помощью структур и их свойств.

Содержание курса

Коммутативные кольца

Кольцо классов вычетов по модулю n

Характеристика поля, простое подполе

Поле, как факторкольцо по максимальному идеалу

Расширение полей

Степень последовательного расширения полей

Примеры расширения полей

Расширение полей как фактор-кольцо по идеалу, порожденному неприводимым многочленом

Примеры конечных полей – как расширения простых полей

Операции над идеалами коммутативного кольца

Нильпотентные элементы, делители нуля, обратимые элементы

Обоснование простоты характеристики поля, существование простого подполя

Необходимые и достаточные условия поля при факторизации

Примеры расширения полей

Проверка на примерах: степень последовательного расширения равна произведению расширений

Примеры асширения полей как фактор-кольцо по идеалу, порожденному неприводимым многочленом

Поля из 8, 9 и 16 элементов

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература:

Атья М., Макдональд И. Введение в коммутативную алгебру. – Изд-во: Книга по требованию 2012.

Койбаев В.А. Основы алгебры. –Владикавказ: СОГУ, 2005
Ван дер Варден Б. Л. Алгебра. – М.: Лань, 2004.

Ноден П., Ките К. Алгебраическая алгоритмика. – М. Мир. 2007. 720 с.

Каргаполов М.И., Мерзлякеов Ю.И. Основы теории групп. СПб.:Лань . 2009. 288с.
Кострикин А.И. Введение в алгебру. Ч.1-3 – М. МЦНМО. 2009. 838с.
Дополнительная литература
Баскаков А.Г. Лекции по алгебре. Изд-во ВГУ.2014.
Кострикин А.И. Сборник задач по алгебре.-М. МЦНМО. 2009. 408 с.

Электронный ресурс

Кострикин А.И. Введение в алгебру <http://math-portal.ru/678-vvedenie-v-algebruchast-3-osnovnyye-struktury-kostrikin-ai-3-e-izdanie.html>

Коблиц Н. Курс теории чисел и криптографии.
[#### **в\) Интернет-ресурсы**](http://math-</p></div><div data-bbox=)

Обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам (библиотека СОГУ):
- библиотеке e-library,
- электронной библиотеке диссертаций РГБ,
- университетской библиотеке online;

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПОДГОТОВКИ К СДАЧЕ ИТОГОВОГО ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

1. Группы. Примеры групп.
2. Подгруппы. Примеры подгрупп.
3. Гомоморфизм групп.
4. Примеры гомоморфизмов групп
5. Изоморфизм групп. Примеры изоморфизмов групп.
6. Теорема о гомоморфизме.
7. Циклические группы. Порядок элемента.
8. Коммутатор элемента.
9. Коммутант группы .
10. Действие группы на множестве.
11. Стабилизаторы.
12. Кольца. Примеры колец.
13. Кольцо классов вычетов по модулю (делители нуля и нильпотенты в этом кольце).
14. Алгебраическое обоснование криптографической системы RSA.

15. Идеалы колец.
16. Простые и максимальные идеалы в кольце целых чисел.
17. Фактор-кольцо.
18. Поля. Примеры полей.
19. Поле (область целостности) как фактор-кольцо по максимальному (простому) идеалу.
20. Сети и операции над сетями.
21. Действие симметрической группы на сетях.
22. Сетевые группы.
23. Максимальные сети.
24. Расширения полей.
25. Представление элементов поля или нерасщепимый тор.
26. Расположение подгрупп. Общая теория.
27. Надгруппы группы диагональных матриц.
28. Надгруппы нерасщепимого максимального тора (примеры).
29. Основные понятия теории меры.
30. Определение измеримой функции и интеграла.
31. Монотонная сходимостъ. Лемма Фату. Теорема Лебега.
32. Произведение мер. Теорема Фубини.
33. Теорема Витали и теорема Безиковича о покрытии. Дифференцирование мер Радона. Производная меры Радона. Интегрирование производных.
34. Теорема Лебега о разложении. Точки Лебега. Теорема Лебега – Безиковича о дифференцировании.
35. Определение пространств. Неравенство Йенсена. Неравенство Гёльдера. Неравенство Минковского. Неравенство Ханнера.
36. Определение - преобразования Фурье. Преобразование Фурье функции Гаусса.
37. Теорема Планшереля. Определение -преобразования Фурье. Формула обращения преобразования Фурье.
38. Аппроксимация функциями из . Аппроксимация функциями из . Определение пространства H^1 . Пространства Соболева. Полнота пространств Соболева.
39. Продолжение. Следы. Неравенства Соболева. Компактность. Неравенства Пуанкаре.
40. Выпуклые множества и полунормы. Теорема Хана-Банаха.
41. Топологические векторные пространства. Локально выпуклые пространства. Следствия теоремы Хана – Банаха.

42. Персептроны. Представимость и разделимость. Алгоритм обучения персептрона. Сходимости алгоритма обучения и подбора количественных характеристик весовых коэффициентов.
43. Многослойные персептроны и возможности их обучения. Процедура обратного распространения - алгоритм обучения многослойного персептрона с учителем.
44. Сети встречного распространения. Архитектура, функционирование и методы обучения сетей встречного распространения. Использование данной сети рассматриваются методы сжатия данных.
45. Нейронные сети Хопфилда и Хэмминга. Архитектура и устойчивости сети. Понятие ассоциативности памяти и задача распознавания образов.
46. Жизненный цикл программных систем (ПС). Методы разработки структуры ПС. Восходящая и нисходящая разработка ПС. Архитектурный подход разработки ПС.
47. Парадигмы программирования. Структурное программирование. Объектно-ориентированное программирование.
48. Основные понятия отладки и тестирования. Различие между отладкой и тестированием. Технологии тестирования. Проверка программ в нормальных, экстремальных и исключительных ситуациях.
49. Системы искусственного интеллекта. Классификация. Экспертные системы. Многоагентные системы. Генетические алгоритмы.
50. Основы искусственных нейронных сетей. Биологический прототип.
51. Структура однослойных и многослойных нейронных сетей.
52. Однослойные искусственные нейронные сети.
53. Обучение искусственных нейронных сетей.
54. Персептроны и зарождение искусственных нейронных сетей.
55. Персептроны. Обучение персептрона.
56. Алгоритм обучения однослойного персептрона.