

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное бюджетное образовательное учреждение высшего образования

«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет математики и компьютерных наук

УТВЕРЖДАЮ:  
Проректор по учебной работе,  
качеству образования – первый  
проректор

подпись

Хагуров Т.А.

«27» мая 2022 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
Б1.В.ДВ.03.02 ПОЛИНОМЫ НАД КОНЕЧНЫМИ ПОЛЯМИ**

Направление подготовки 01.04.01 Математика

Направленность (профиль) Алгебраические методы защиты информации

Форма обучения Очная

Квалификация Магистр

Краснодар 2022

Рабочая программа дисциплины Полиномы над конечными полями  
составлена в соответствии с федеральным государственным образовательным  
стандартом высшего образования (ФГОС ВО) по направлению подготовки  
01.04.01 Математика

Программу составил(и):

А.В. Рожков, профессор, д.ф.-м.н., профессор



---

Рабочая программа дисциплины Полиномы над конечными полями  
утверждена на заседании кафедры функционального анализа и алгебры  
протокол № 9 «13» апреля 2022 г.

Заведующий кафедрой функционального анализа и алгебры

Барсукова В.Ю.



---

Утверждена на заседании учебно-методической комиссии факультета мате-  
матики и компьютерных наук протокол № 5 «05» мая 2022 г.

Председатель УМК факультета/института Шмалько С.П.



---

Рецензенты:

Соколова И.В., кандидат педагогических наук, доцент кафедры высшей мате-  
матики КубГАУ

Марковский А.Н., кандидат физико-математических наук, доцент кафедры  
математических и компьютерных методов КубГУ

## 1 Цели и задачи изучения дисциплины

### 1.1 Цель дисциплины

Целью изучения теории конечных полей можно считать как развитие математической культуры, так и подготовку к возможной будущей работе в области защиты информации, теории связи и т.д.

### 1.2 Задачи дисциплины

Теория конечных полей является одним из важнейших математических инструментов для разнообразных прикладных дисциплин, в частности для обработки сигналов и отображений, теории кодирования, криптографии и других математических методов защиты информации. Кроме того, теория конечных полей и их приложений - это хорошо развитая математическая теория, изучения которой будет способствовать формированию математической культуры магистра.

### 1.3 Место дисциплины в структуре образовательной программы

Дисциплина Полиномы над конечными полями относится к части, формируемой участниками образовательных отношений дополнительного Блока 1 "Дисциплины (модули)" учебного плана и является дисциплиной по выбору Б1.В.ДВ.03.02.

Данная дисциплина, как математическая основа теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров.

### 1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
<b>ПК-1</b> Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	
ПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа Уметь: Применять основные математические методы, используемые в анализе типовых алгоритмов Владеть навыками: использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.
ПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области	
ПК-1.3 Самостоятельно и корректно решает стандартные задачи фундаментальной и прикладной математики	
ПК-1.4 Имеет навыки решения математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований	

## 2 Структура и содержание дисциплины

### 2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часа, из них – 26,2 часа контактной работы (12 часов лекций, 14 лабораторных занятий, 0,2 часа ИКР); 45,8 часов самостоятельной работы).

Вид учебной работы	Всего часов	Семестры (часы)
--------------------	-------------	-----------------

		2			
<b>Контактная работа, в том числе:</b>					
<b>Аудиторные занятия (всего):</b>		<b>26</b>	<b>26</b>		
Занятия лекционного типа		12	12	-	-
Лабораторные занятия		14	14	-	-
Занятия семинарского типа (семинары, практические занятия)				-	-
<b>Иная контактная работа:</b>					
Контроль самостоятельной работы (КСР)					
Промежуточная аттестация (ИКР)		0,2	0,2		
<b>Самостоятельная работа, в том числе:</b>		<b>45,8</b>	<b>45,8</b>		
Курсовая работа		-	-	-	-
Проработка учебного (теоретического) материала		14	14	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		15	15	-	-
Реферат				-	-
Подготовка к текущему контролю		16,8	16,8	-	-
<b>Контроль:</b>					
Подготовка к зачету		-	-		
<b>Общая трудоемкость</b>	<b>час.</b>	<b>72</b>	<b>72</b>	<b>-</b>	<b>-</b>
	<b>в том числе контактная работа</b>	<b>26,2</b>	<b>26,2</b>		
	<b>зач. ед</b>	<b>2</b>	<b>2</b>		

## 2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
1	2	3	4	5	6	7
1	Поля, расширения полей	14	2		4	8
2	Конечные поля	18	4		4	10
3	Неприводимые полиномы над конечными полями	14	2		2	10
4	Факторизация полиномов над конечными полями	23,8	4		2	17,8
	<b>Итого по дисциплине:</b>		<b>12</b>		<b>14</b>	<b>45,8</b>

## 2.3 Содержание разделов дисциплины

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Поля, расширения полей	Характеристика поля. Свойства конечных и алгебраических расширений. Примеры. Теорема о применении элемента	Проверка домашнего задания

			дания, реферативный доклад.
2	Конечные поля	Существование конечных полей, их порядки. Строение конечных полей. Автоморфизм Ферробенауса	Проверка домашнего задания, реферативный доклад.
3	Неприводимые полиномы над конечными полями	Алгоритмы построения неприводимых полиномов над конечным полем. Примеры. Прimitивные полиномы, их свойства	Проверка домашнего задания, реферативный доклад.
4	Факторизация полиномов над конечными полями	Алгоритм Берлекэмпса. Примеры. Метод нахождения минимального полинома элемента конечного поля. Примеры	Проверка домашнего задания, реферативный доклад.

### 2.3.1 Занятия лекционного типа

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Кольца вычетов. Китайская теорема об остатках.	Теория делимости в кольцах. НОД и НОК. Алгоритм Евклида. Решение модульных уравнений. Решение систем по разным модулям. Квадратичный закон взаимности.	Проверка домашнего задания, устный опрос
2	Решение уравнений в кольцах. В кольцах матриц над полем и в кольце целых чисел.	Обратимые матрицы. Решение систем линейных уравнений в кольце целых чисел. Приложения в криптографии. Эллиптические кривые.	Проверка домашнего задания, контрольная работа
3	Поля Галуа. Структура полей. Неприводимые многочлены над полями Галуа.	Простое поле Галуа. Расширение полей Галуа. Автоморфизмы полей Галуа. Неприводимые многочлены над полем Галуа. Регистры сдвига с обратной связью.	Проверка домашнего задания

### 2.3.2 Занятия лабораторного типа

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Кольца вычетов. Китайская теорема об остатках.	НОД и НОК. Алгоритм Евклида. Решение модульных уравнений. Решение систем по разным модулям.	Проверка домашнего задания, устный опрос

Решение уравнений в кольцах. В кольцах матриц над полем и в	Обратимые матрицы. Решение систем линейных уравнений в кольце целых чисел. Приложения в криптографии
---	--

Поля Галуа. Структура полей. Неприводимые многочлены над полями Галуа.	Простое поле Галуа. Расширение полей Галуа. Автоморфизмы полей Галуа. Неприводимые многочлены над полем Галуа. Регистры сдвига с обратной связью.
--	---

2	Кольца вычетов. Китайская теорема об остатках.	Решение систем линейных уравнений в кольце целых чисел. Приложения в криптографии. Эллиптические кривые.	Проверка домашнего задания, контрольная работа
3	Кольца вычетов. Китайская теорема об остатках.	Простое поле Галуа. Расширение полей Галуа. Неприводимые многочлены над полем Галуа. Регистры сдвига с обратной связью.	Проверка домашнего задания

Решение уравнений в кольцах. Примеры как матриц над полем и в

**3.3.4. Примерная тематика курсовых работ (проектов)** курсовые работы не предусмотрены

**3.4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)**

1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

5. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

6. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,

**3. Образовательные технологии:** активные и интерактивные формы, лекции, лабораторные занятия, контрольные работы, реферативные доклады (по некоторым темам в виде презентации) и зачет. В течение семестра студенты решают задачи, указанные преподавателем, к каждому лабораторному занятию. Проводятся три контрольных работы (каждая продолжительностью в 1 акад. час) по темам разделов 1-6. Зачет выставляется после выполнения определенного количества (практических и теоретических) заданий контрольных работ и от-

чета по реферативному докладу. В случае невыполнения какого-то из приведенных требований, студенту для сдачи зачета предлагаются по усмотрению преподавателя некоторые практические и теоретические задания.

К образовательным технологиям также относятся интерактивные методы обучения. Интерактивность подачи материала по дисциплине «Конечные поля и некоторые их приложения» предполагает не только взаимодействия вида «преподаватель - студент» и «студент - преподаватель», но и «студент - студент». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на лабораторных занятиях в ходе изложения студентами реферативных докладов (возможно в виде презентации).

### 3.1. Дискуссия

Возможность дискуссии предполагает умение высказать собственную идею, предложить свой путь решения, аргументировано отстаивать свою точку зрения, связно излагать мысли. Полезны следующие задания: составление плана решения задачи, поиск другого способа решения, сравнение различных способов решения, проведение выкладок для решения задачи и выкладок для проверки правильности полученного решения, рассмотрение задач с лишними и недостающими данными, реферативно-творческие доклады. Студентам предлагается проанализировать варианты решения, обсудить доклад, высказать своё мнение. Основным объемом использования интерактивных методов обучения реализуется именно в ходе дискуссий, как на лекционных, так и на лабораторных занятиях.

Общие вопросы, которые выносятся на дискуссию:

- 1) Составления плана доказательства утверждения или решения задачи.
- 2) Определение возможных способов доказательства утверждения или поиск различных способов решений задачи.
- 3) Выбор среди рассматриваемых способов наиболее рационального.
- 4) Обсуждение логической составляющей в формулировке той или иной теоремы, а также обсуждение возможности построения иллюстрирующих ее примеров и контр-примеров.
- 5) Самостоятельное составление студентами опорных заданий по теме, характеризующих глубину понимания соответствующего материала.

### 3.2. Использование компьютерных технологий

Применение на занятии компьютерных технологий позволяет студентам при рассмотрении определенных тем курса более глубоко освоить соответствующие понятия. В этой связи определенные лекционные и лабораторные занятия преподавателю целесообразно проводить в виде презентации. Также в виде презентации в соответствии с темой лабораторного занятия студенты могут излагать подготовленные ими некоторые свои реферативные доклады.

Вид занятия (Л, ЛЗ)	Используемые интерактивные образовательные технологии	Количество часов
	«Неприводимость многочленов над конечными полями» - лекция в виде презентации.	2
Л	«Подполя конечных полей» - лабораторное занятие в виде презентации.	2

## 4 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Контрольные работы и реферативные доклады оцениваются по пятибалльной системе. Зачет оценивается по системе: зачтено, не зачтено. На лабораторных занятиях контроль осуществляется при ответе у доски и при проверке домашних заданий.

Самостоятельная работа студента включает в себя повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным занятиям, к контрольным работам и к зачету. Такой вид СРС контролируется в ходе проверки домашних заданий, заданий контрольных работ и в ходе зачета. Контроль осуществляется во время консультаций (вызывных или по желанию студента), а также на лабораторных занятиях.

Обязательными при изучении дисциплины «Полиномы над конечными полями» являются следующие виды самостоятельной работы:

- разбор и самостоятельное изучение теоретического материала по конспектам лекций и по учебным пособиям из списка источников литературы;
- самостоятельное решение задач по темам лабораторных занятий;
- подготовка к контрольным работам;
- подготовка к зачету.

#### **4.1 Фонд оценочных средств для проведения текущей аттестации**

**Список типовых практических заданий** (для практических занятий и зачета)

1. Построение конечного поля  $GF(5^2)$ .
2. Построение неприводимых полиномов степеней 2, 3, 4 над  $GF(2)$ ,  $GF(3)$ ,  $GF(5)$ .
3. Нахождение примитивного элемента конечного поля.
4. Нахождение обратного элемента в конечном поле.
5. Расширение конечных полей.
6. Структура поля  $GF(2^8)$ .
7. Факторизация круговых полиномов над  $GF(p)$ .
8. Нахождение примитивных полиномов над  $GF(2)$ .
8. Квадратичный закон взаимности.
10. Факторизация квадратичных полиномов над  $GF(p)$ .
11. Факторизация кубических полиномов над  $GF(p)$ .
12. Теорема Штикрбергера и ее применение.
13. Применение алгоритма Берлекэмна для факторизации полиномов.
14. Нахождение порождающих элементов конечного поля.

**Примерные контрольные (самостоятельные) работы**

Не предусмотрены

Для выполнения домашнего практического задания необходимо разобрать материал по соответствующей теме лабораторного занятия. При этом используются указания, данные преподавателем в ходе занятия, а также теоретико-практический материал, имеющийся в источниках из списка основной литературы. Если магистр не смог понять приведенный в указанных источниках разбор типовых примеров в той степени, чтобы самостоятельно использовать предложенный алгоритм для решения задания, то он может получить консультацию преподавателя

#### **4.2 Фонд оценочных средств для проведения промежуточной аттестации**

**Список теоретических вопросов** (для зачета)

1. Конечные расширения полей, их свойства.
2. Алгебраические расширения полей, их свойства.
3. Квадратичные расширения полей.
4. Поля расщеплений кубических полиномов.
5. Конечное поле  $GF(2^3)$ , его построение, свойства.
6. Конечное поле  $GF(3^2)$ , его построение, свойства.



7. Круговые полиномы  $F_n(x)$ , их свойства.
8. Группы Галуа конечного поля.
9. Порядок полинома над конечным полем, его свойства.
10. Факторизация круговых полиномов над  $GF(p)$ .
11. Построение неприводимых полиномов над  $GF(p)$ .
12. Алгоритм Берлекэмпа факторизации полинома над  $GF(p)$ .

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

### **Критерии оценивания по промежуточной аттестации**

Зачет выставляется по результатам работы студента в течение семестра. Отметка «зачтено» выставляется студентам, которые регулярно посещали занятия, выполняли домашние работы, написали контрольные работы на положительные оценки. Отметка «незачтено» выставляется студентам, которые пропустили более 60 % занятий и написали контрольные работы на неудовлетворительные оценки.

### **4.3 Методические рекомендации к самостоятельной подготовке магистров к реферативному докладу**

Каждый магистр должен подготовить в течение семестра реферативный доклад по одной из тем, предназначенной для самостоятельного изучения. Для подготовки доклада желательно кроме основных источников литературы использовать дополнительные источники, а также Интернет-ресурс. Доклад может быть представлен магистром на лабораторном занятии, возможно, в виде презентации, если тема занятия соответствует теме доклада. Также магистр может представить отчет о подготовке реферативного доклада в письменной форме в конце семестра. Оформление письменного отчета должно удовлетворять требованиям: а) текст набирается 14 шрифтом на бумаге формата А 4; б) на титульном листе кроме темы также указывается факультет, направление (бакалавриат), курс, группа, ФИО магистра; в) содержание материала по объему составляет 4-5 страниц; г) список литературы содержит не менее двух источников (возможно, из списка литературы в пункте 7).

### **Примерные темы реферативных докладов**

1. Связь теории Галуа с факторизацией полиномов над конечными полями.
2. Свойства корней неприводимых полиномов.
3. Автоморфизм Феробенауса.
4. Группа автоморфизмов конечного поля
5. Метод построения примитивных полиномов над конечным полем
6. Корни из единицы и круговые полиномы
7. Порядки полиномов и примитивные полиномы
8. Число неприводимых
9. Поточный шифры.
10. Шифр A5.
11. Шифрование трафика мобильной связи.

### **Критерии оценивания результатов обучения**

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает формы допускает незначительные ошибки; студент умеет правильно объяснять материал, иллюстрируя его примерами

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры, довольно ограниченный объем знаний программного материала.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

## **5 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

### **5.1 Основная литература:**

1. Сергеев А.Э., Сергеев Э.А., Основы теории Галуа, Краснодар, 2014.
2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2022. - URL: <https://reader.lanbook.com/book/187793>

### **5.2 Дополнительная литература:**

1. Курош А.Г. Курс высшей алгебры, 23-е изд. [Электронный ресурс]. - СПб.: Лань, 2022. - URL: <https://reader.lanbook.com/book/183725>
2. Фаддеев Д.К. Лекции по алгебре, 7-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: <https://e.lanbook.com/reader/book/126709/>

### **5.3 Периодические издания:**

Не предусмотрены

### **6. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы**

#### **Электронно-библиотечные системы (ЭБС):**

1. ЭБС «ЮРАЙТ» <https://urait.ru/>
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» [www.biblioclub.ru](http://www.biblioclub.ru)
3. ЭБС «BOOK.ru» <https://www.book.ru>
4. ЭБС «ZNANIUM.COM» [www.znanium.com](http://www.znanium.com)
5. ЭБС «ЛАНЬ» <https://e.lanbook.com>

#### **Профессиональные базы данных:**

1. Web of Science (WoS) <http://webofscience.com/>
2. Scopus <http://www.scopus.com/>
3. ScienceDirect [www.sciencedirect.com](http://www.sciencedirect.com)
4. Журналы издательства Wiley <https://onlinelibrary.wiley.com/>
5. Научная электронная библиотека (НЭБ) <http://www.elibrary.ru/>
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН <http://archive.neicon.ru>
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) <https://rusneb.ru/>
8. Президентская библиотека им. Б.Н. Ельцина <https://www.prilib.ru/>
9. Электронная коллекция Оксфордского Российского Фонда <https://ebookcentral.proquest.com/lib/kubanstate/home.action>
10. Springer Journals <https://link.springer.com/>
11. Nature Journals <https://www.nature.com/siteindex/index.html>
12. Springer Nature Protocols and Methods <https://experiments.springernature.com/sources/springer-protocols>
13. Springer Materials <http://materials.springer.com/>
14. zbMath <https://zbmath.org/>
15. Nano Database <https://nano.nature.com/>
16. Springer eBooks: <https://link.springer.com/>
17. "Лекториум ТВ" <http://www.lektorium.tv/>
18. Университетская информационная система РОССИЯ <http://uisrussia.msu.ru>

#### **Информационные справочные системы:**

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

#### **Ресурсы свободного доступа:**

1. Американская патентная база данных <http://www.uspto.gov/patft/>
2. Полные тексты канадских диссертаций <http://www.nlc-bnc.ca/thesescanada/>
3. КиберЛенинка (<http://cyberleninka.ru/>);
4. Министерство науки и высшего образования Российской Федерации <https://www.minobrnauki.gov.ru/>;
5. Федеральный портал "Российское образование" <http://www.edu.ru/>;

6. Информационная система "Единое окно доступа к образовательным ресурсам" <http://window.edu.ru/>;
7. Единая коллекция цифровых образовательных ресурсов <http://school-collection.edu.ru/> .
8. Федеральный центр информационно-образовательных ресурсов (<http://fcior.edu.ru/>);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" <https://pushkininstitute.ru/>;
10. Справочно-информационный портал "Русский язык" <http://gramota.ru/>;
11. Служба тематических толковых словарей <http://www.glossary.ru/>;
12. Словари и энциклопедии <http://dic.academic.ru/>;
13. Образовательный портал "Учеба" <http://www.uceba.com/>;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы [http://xn--273--84d1f.xn--plai/voprosy\\_i\\_otvety](http://xn--273--84d1f.xn--plai/voprosy_i_otvety)

#### **Собственные электронные образовательные и информационные ресурсы КубГУ:**

1. Среда модульного динамического обучения <http://moodle.kubsu.ru>
2. База учебных планов, учебно-методических комплексов, публикаций и конференций <http://mschool.kubsu.ru/>
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий [http://mschool.kubsu.ru/](http://mschool.kubsu.ru;);
4. Электронный архив документов КубГУ <http://docspace.kubsu.ru/>
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" <http://icdau.kubsu.ru/>

### **7 Методические указания для обучающихся по освоению дисциплины**

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, лабораторных занятий, в ходе которых студентами приобретаются и закрепляются основные практически навыки решения различных задач, в том числе с применением полученных теоретических знаний.

Важнейшим этапом курса является самостоятельная работа по дисциплине. Самостоятельная работа студентов является неотъемлемой частью процесса подготовки. Под самостоятельной работой понимается часть учебной планируемой работы, которая выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа направлена на усвоение системы научных и профессиональных знаний, формирования умений и навыков, приобретение опыта самостоятельной творческой деятельности. СРС помогает формировать культуру мышления студентов, расширять познавательную деятельность.

Виды самостоятельной работы по курсу:

**а) по целям:** подготовка к лекциям, к практическим занятиям, к контрольной работе, к коллоквиуму; подготовка научного доклада и выполнение заданий по НИР.

**б) по характеру работы:** изучение литературы, конспектирование рекомендуемой для самостоятельного изучения научной литературы; решение задач, тестов; работа с обучающими и контролирующими программами.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

## **8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)**

### **8.1. Перечень информационных технологий.**

#### **8.2 Перечень необходимого программного обеспечения**

- Microsoft Windows
- Microsoft Office
- Wolfram Research Mathematica
- MATLAB

#### **8.3 Перечень необходимых информационных справочных систем**

Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru/>)

## **9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине**

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»). Программы для демонстрации и создания презентаций («Microsoft Power Point»).
2.	Семинарские занятия	Не предусмотрены
3.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами
4.	Курсовое проектирование	Не предусмотрено
5.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
6.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий
7.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

## РЕЦЕНЗИЯ

на рабочую программу дисциплины  
**Полиномы над конечными полями** по направлению подготовки **01.04.01**  
**Математика**, подготовленную кандидатом  
физ-мат. наук, доцентом каф. функционального анализа и алгебры  
КубГУ А.Э. Сергеевым,

Рабочая программа дисциплины «Полиномы над конечными полями» охватывает материал одного семестра.

Цель освоения дисциплины – дальнейшее формирование у студентов знаний по алгебре и фундаментальной алгебре.

Задачи освоения дисциплины: получение базовых теоретических сведений по приложениям конечных полей, линейным и циклическим кодам, поточным шифрам.

При освоении дисциплины вырабатывается общематематическая культура: умение логически мыслить, проводить доказательства основных утверждений, устанавливать логические связи между понятиями, применять полученные знания для решения задач. Получаемые знания лежат в основе математического образования и необходимы для понимания и освоения всех курсов математики, а также для продолжения обучения в магистратуре по соответствующему направлению подготовки.

Учитывая вышеизложенное, считаю, что рабочая программа доцента А.Э. Сергеева, соответствует государственным требованиям к минимуму содержания и уровню подготовки выпускников по направлению подготовки 01.04.01 Математика, и может быть рекомендована для высших учебных заведений.

Рецензент,  
кандидат физ.-мат. наук, доцент кафедры  
математических и компьютерных  
методов КубГУ



Марковский А.Н.

## РЕЦЕНЗИЯ

на рабочую программу дисциплины  
**Полиномы над конечными полями** по направлению подготовки **01.04.01**  
**Математика**, подготовленную кандидатом  
физ-мат. наук, доцентом каф. функционального анализа и алгебры  
КубГУ А.Э. Сергеевым,

Рабочая программа дисциплины «Полиномы над конечными полями» охватывает материал одного семестра.

Цель освоения дисциплины – дальнейшее формирование у студентов знаний по алгебре и фундаментальной алгебре.

Задачи освоения дисциплины: получение базовых теоретических сведений по приложениям конечных полей, линейным и циклическим кодам, поточным шифрам.

При освоении дисциплины вырабатывается общематематическая культура: умение логически мыслить, проводить доказательства основных утверждений, устанавливать логические связи между понятиями, применять полученные знания для решения задач. Получаемые знания лежат в основе математического образования и необходимы для понимания и освоения всех курсов математики, а также для продолжения обучения в магистратуре по соответствующему направлению подготовки.

Учитывая вышеизложенное, считаю, что рабочая программа доцента А.Э. Сергеева, соответствует государственным требованиям к минимуму содержания и уровню подготовки выпускников по направлению подготовки 01.04.01 Математика, и может быть рекомендована для высших учебных заведений.

Рецензент,  
канд. пед. наук,  
доцент кафедры высшей  
математики КубГАУ



Соколова И.В.

Личную подпись тов.  
ЗАВЕРЯЮ: И.В. Соколова  
СПЕЦИАЛИСТ ПО КАДРАМ

И.В. Соколова

