Санкт-Петербургский филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет "Высшая школа экономики"»

Факультет Санкт-Петербургская школа
физико-математических и компьютерных наук
Департамент информатики

Рабочая программа дисциплины
Алгебра

для образовательной программы «Прикладная математика и информатика»
направления подготовки 01.03.02 «Прикладная математика и информатика»
уровень бакалавриат

Разработчик: Чепуркин Константин Михайлович, kchepurkin@hse.ru

Утверждена Академическим руководителем образовательной программы

«31» августа 2018 г.

А.В. Омельченко

Санкт-Петербург, 2018

1. Область применения и нормативные ссылки

Настоящая программа учебной дисциплины устанавливает требования к образовательным результатам и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих дисциплину «Алгебра», учебных ассистентов и студентов направления 01.03.02 «Прикладная математика и информатика» подготовки бакалавра, обучающихся по бакалаврской программе «Прикладная математика и информатика» и изучающих дисциплину «Алгебра».

Рабочая программа дисциплины разработана в соответствии с:

- Образовательным стандартом НИУ ВШЭ по направлению подготовки 01.03.02 «Прикладная математика и информатика» (уровень бакалавриата), утвержденным ученым советом Национального исследовательского университета «Высшая школа экономики», протокол от 03.03.2017 №02.
- Основной профессиональной образовательной программой «Прикладная математика и информатика» направления подготовки 01.03.02 «Прикладная математика и информатика»;
- Объединенным учебным планом университета по образовательной программе «Прикладная математика и информатика», утвержденным в 2018 г.

2. Цели освоения дисциплины

Целью освоения дисциплины «Алгебра» является формирование у студентов теоретических знаний и практических навыков по основам теории чисел, теории колец, теории делимости, в частности, делимости целых чисел, делимости многочленов, а так же базовым применениям этих теорий для решения задач криптографии, построения кодов, исправляющих ошибки и других алгоритмических вопросах.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен:

- Знать основные понятия и факты теории колец и делимости, такие, как кольцо, поле, фактор кольца по идеалу, кольцо многочленов, теорема о делении с остатком, линейное разложение наибольшего общего делителя, первообразный корень из единицы, китайская теорема об остатках, разложение дробно-рациональной функции в сумму простейших, основная теорема арифметики в кольце многочленов над полем, строение конечных полей, протокол шифрования RSA, коды БЧХ.
- Уметь находить линейное разложение наибольшего общего делителя целых чисел и многочленов, находить явно класс обратного элемента в кольце вычетов по простому модулю, находить решения сравнений по составному модулю, владеть основными приёмами для проверки многочлена на неприводимость, иметь представление об алгоритмах разложения на множители,
- Иметь навыки (приобрести опыт) обращения с основными алгебраическими объектами и конструкциями, уметь привести примеры таких объектов, знать основные идеи их практического применения.

В результате освоения дисциплины студент осваивает следующие компетенции:

Компетенция	Код по ОСНИУ ВШЭ	Уровень формирования компетенции	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции	Форма контроля уровня сформированности компетенции
Способность учиться, приобретать новые знания, умения, в том числе в области, отличной от профессиональной	УК-1	РБ СД МЦ	Знает основные способы познания, их эволюцию. Применяет знания об алгебраических структурах и методах работы с ними в рамках профессиональной деятельности. Анализирует и применяет различные методы работы с алгебраическими структурами, а также методы теории чисел.	Лекции, семинары, подготовка к семинарам и практическим занятиям, работа на практических занятиях, самостоятельная работа	Домашние задания, контрольные работы, устный экзамен
Способен выявлять научную сущность проблем в профессиональной области	УК-2	РБ СД МЦ	Знает основные принципы построения логически и математически корректных доказательств. Доказывает принципами математической индукции математические утверждения. Использует алгебраический подход для анализа задач профессиональной области.	Лекции, семинары, подготовка к семинарам и практическим занятиям, работа на практических занятиях, самостоятельная работа	Домашние задания, контрольные работы, устный экзамен
Способен применять фундаментальные знания, полученные в области	ОПК-1	РБ СД	Описывает математические модели поставленных практических задач.	Лекции, семинары, подготовка к практическим занятиям и семинарам,	Домашние задания, контрольные работы, устный экзамен

математических и (или) естественных наук, и использовать их в профессиональной деятельности		МЦ	Математически корректно и адекватно записывает логические формулы и другие условия, описывающие дискретные объекты прикладной задачи. Применяет полученные знания к математическому моделированию практических задач.	работа на практических занятиях, самостоятельная работа	
Способен применять и модифицировать математические модели для решения задач в области профессиональной деятельности	ОПК-3	РБ СД МЦ	Знает основные принципы построения современной математики. Применяет современные математические методы к решению математических задач. Использует полученные навыки в решении практических задач.	Лекции, семинары, подготовка к семинарам и практическим занятиям, работа на практических занятиях, самостоятельная работа	Домашние задания, контрольные работы, устный экзамен

4. Место дисциплины в структуре образовательной программы.

Для образовательной программы «Прикладная математика и информатика» направления подготовки 01.03.02 «Прикладная математика и информатика» настоящая дисциплина относится к базовой части блока дисциплин.

Основные положения данной дисциплины используются для освоения следующих дисциплин:

- Линейная алгебра и геометрия
- Дифференциальные уравнения
- Теория вероятностей и математическая статистика
- Функциональное программирование

5. Тематический план учебной дисциплины

Курс рассчитан на 182 часа аудиторной нагрузки, из них 90 часов лекций и 58 часов семинарских занятий, 34 часа практических занятий, общим объемом 8 зачетных

единиц (304 часа).

№	Название раздела	Всего часов	Аудиторные часы			Самостоя-тельная работа
			Лекции	Семи-нары	Практические занятия	
1	Основы теории колец	82	24	26	-	32
2	Многочлены от многих переменных	108	32	32	-	44
3	Конечные поля и коды, исправляющие ошибки, базовые конструкции теории числе	114	34	-	34	46
ИТОГО		304	90	58	34	122

6. Содержание дисциплины

Раздел 1 Основы теории колец	
Тема 1	Понятие кольца, поля, целые числа, делимость для целых чисел, общая теория делимости, понятие идеала, факторизация кольца по идеалу, область главных идеалов, основная теорема арифметики для области главных идеалов, китайская теорема об остатках для области главных идеалов, кольцо многочленов над полем, как область главных идеалов, цикличность конечной подгруппы мультипликативной группы поля, тесты на простоту, криптосистема RSA
Тема 2	Комплексные числа, тригонометрическая запись, корни из единицы, основная теорема алгебры(формулировка). Производная многочлена. Различные интерполяционные задачи для многочленов, дробно-рациональные функции, разложение дробно-рациональной функции в сумму простейших.
Раздел 2 Многочлены от многих переменных	
Тема 1	Лемма Гаусса, факториальность кольца многочленов от многих переменных над полем, критерии неприводимости для многочленов от одной переменной, способы разложения целочисленного многочлена на неприводимые множители
Тема 2	Симметрические многочлены, элементарные симметрические многочлены, основная теорема о симметрических многочленах, результант и дискриминант.
Раздел 3 Конечные поля и коды исправляющие ошибки. Базовые конструкции теории чисел	

Тема 1	Строение конечных полей, алгоритмы Берлекэмпа и Кантора-Цассенхауза, коды исправляющие ошибки, коды БЧХ
Тема 2	Базовые конструкции теории чисел. Арифметические функции. Производящие функции Дирихле. Свёртка Дирихле. Формула обращения Мёбиуса. Примеры использования.

7. Оценочные средства

7.1. Формы контроля знаний студентов

Тип контроля	Форма контроля	1 год	2 год	Параметры
		2 модуль	1 модуль	
Текущий	Домашнее задание №1	*		Письменное домашнее задание
	Домашнее задание №2	*		Письменное домашнее задание
	Контрольная работа №1	*		Письменная контрольная работа
	Домашнее задание №3		*	Письменное домашнее задание
	Домашнее задание №4		*	Письменное домашнее задание
	Контрольная работа № 2		*	Письменная контрольная работа
Итоговый	Устный экзамен		*	Экзамен в устной форме

7.2. Критерии оценки и шкалы, примеры заданий

7.2.1. Текущий контроль

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств.

ДОМАШНЕЕ ЗАДАНИЕ №1

Домашнее задание №1 выдается студентам в одном варианте и состоит из 10 задач. Срок выполнения домашнего задания - 2 недели. Форма представления обучающимися домашнего задания - представленные в письменном виде решения задач.

Пример домашнего задания №1:

Задача 1. Покажите, что сумма двух нильпотентов в коммутативном кольце -- снова нильпотент.

Задача 2. Покажите, что в конечном кольце любой элемент либо обратим, либо делитель нуля.

Задача 3. Опишите все нильпотенты в Z/n. Сколько их?

Задача 4. Докажите, что среди значений многочлена с целыми коэффициентами на

целых числах бесконечно много составных.

Задача 5. Покажите, что у многочлена x^3+33x^2+91x+182 нет целых корней используя редукцию многочлена по какому-нибудь n.

Задача 6. Решите x^5=16 в кольце Z/129.

Задача 7. Доказать, что (k!)^2 =(-1)^{k+1} (mod p), где p=2k+1 — простое.

Задача 8. Сколько решений может иметь уравнение x^3+ax^2+bx+c в Z/70 при различных целых a,b,c?

Задача 9. Покажите, что числа Кармайкла не могут делиться на квадрат простого.

Задача 10. Найти линейное разложение наибольшего общего делителя многочленов x^5+x^4+1 и x^4+x^3+1 в кольце F_2[x].

Критерии оценивания и шкала оценки домашнего задания №1

Оценка	Критерии выставления оценки
«Отлично» (8-10)	Решено 8-10 задач
«Хорошо» (6-7)	Решено 6-7 задач
«Удовлетворительно» (4-5)	Решено 4-5 задач
«Неудовлетворительно» (0-3)	Решено менее 4 задач

ДОМАШНЕЕ ЗАДАНИЕ №2

Домашнее задание №2 выдается студентам в одном варианте и состоит из 10 задач. Срок выполнения домашнего задания - 2 недели. Форма представления обучающимися домашнего задания - представленные в письменном виде решения задач.

Пример домашнего задания №2:

Задача 1. Нарисуйте на комплексной плоскости множество точек, удовлетворяющих неравенствам

5<= |(3+4i)z+2-i|<10

Задача 2. Нарисуйте на комплексной плоскости множество точек, удовлетворяющих неравенствам 0< Re(iz) <= 1

Задача 3. Нарисуйте на комплексной плоскости множество точек, удовлетворяющих неравенству

Re(z^2)<=1.

Задача 4. Найдите все комплексные решения уравнения (x+1)^n=(x-1)^n при фиксированном n. Какие из них вещественные?

Задача 5. Решить квадратное уравнение x^2-(3-2i)x+5-5i=0 в C.

Задача 6. Найти сумму sin^2 x+ sin^2 2x+...+ sin^2 nx.

Задача 7. Найти остаток от деления x^500 на x^7+2.

Задача 8. Разложить дробь x/(x+1)(x^2+x+1)^2 на простейшие дроби над R и над C.

Задача 9. Разложить 1/(x^n+1) на простейшие дроби над C.

Задача 10. Покажите, что если для двух элементов a,b в коммутативном кольце R найдутся такие x,y, что ax+by=1, то то же будет верно для a^n и b^m.

Критерии оценивания и шкала оценки домашнего задания №2

Оценка	Критерии выставления оценки

«Отлично» (8-10)	Решено 8-10 задач
«Хорошо» (6-7)	Решено 6-7 задач
«Удовлетворительно» (4-5)	Решено 4-5 задач
«Неудовлетворительно» (0-3)	Решено менее 4 задач

ДОМАШНЕЕ ЗАДАНИЕ №3

Домашнее задание №3 выдается студентам в одном варианте и состоит из 9 задач. Срок выполнения домашнего задания - 2 недели. Форма представления обучающимися домашнего задания - представленные в письменном виде решения задач.

Пример домашнего задания №3:

Задача 1. Пусть f(x) многочлен с целыми коэффициентами, а несократимая дробь p/q – его рациональный корень. Покажите, что p - mq есть делитель f (m) при любом целом m.

Задача 2. Покажите, что многочлен (x-a_1)...(x-a_n)-1 неприводим над Z при различных целых a_i.

Задача 3. Докажите неприводимость многочленов над Q: x^5+x^4+x^3+2x^2+5x+2, x^5-4x^2+2x+5.

Задача 4. Разложите многочлен x^5-x^4-x^3+x+1 на множители над Z/3 и поднимите разложение до разложения над Z/9.

Задача 5. Найдите коэффициенты многочлена p(x) из Q[x], корнем которого является x_1^2+x_1, если x_1 есть корень уравнения $x^4 +x +1$.

Задача 6. Найдите результант двух многочленов x^3-3x^2+2x+1 и $2x^2-x-1$.

Задача 7. Покажите, что D(x^n+ax+b)=(-1)^(n(n-1)/2) (n^n b^{n-1}+ (-1)^{n-1}(n-1)^{n-1}a^n).

Задача 8. Решите систему уравнений: x + y + z = 0, x^2 + y^2 + z^2 = x^3 + y^3 + z^3, xyz = 2.

Задача 9. Покажите, что для данного целочисленного многочлена f без кратных множителей существует бесконечно много простых, по модулю которых у f нет кратных множителей.

Критерии оценивания и шкала оценки домашнего задания №3

Оценка	Критерии выставления оценки
«Отлично» (8-10)	Решено 8-9 задач
«Хорошо» (6-7)	Решено 6-7 задач
«Удовлетворительно» (4-5)	Решено 4-5 задач
«Неудовлетворительн»	Решено менее 4 задач

(0-3)	

ДОМАШНЕЕ ЗАДАНИЕ №4

Домашнее задание №4 выдается студентам в одном варианте и состоит из 6 задач. Срок выполнения домашнего задания - 2 недели. Форма представления обучающимися домашнего задания - представленные в письменном виде решения задач.

Пример домашнего задания №4:

Задача 1. Докажите неприводимость над конечным полем, используя алгоритм Берлекэмпа:

а) x^7+x^5+x^2+x+1 над F_2;

б) x^6-x^3-x-1 над F_3.

Задача 2. Найдите поле разложения x^4+x^3+4x+1 над F_5 и примитивный элемент в нём.

Задача 3. Рассмотрим F_{81}. Опишите все подполя внутри этого поля. Посчитайте число первообразных элементов в группе F_{81}^* и найдите число элементов, порождающих F_{81} над F_3.

Задача 4. Рассмотрим поле L=F_3[\alpha], где \alpha корень многочлена x^2+1. Покажите, что многочлен f(x)=x^4+1 раскладывается на множители над L. Найдите первообразный корень в F_3[\alpha]^* и выразите через него корни f(x).

Задача 5. Постройте изоморфизм F_3[t]/t^2+1 и F_3[x]/x^2+x+2.

Задача 6. Покажите, что свёртка Дирихле двух мультипликативных функций снова мультипликативна.

Критерии оценивания и шкала оценки домашнего задания №4

Оценка	Критерии выставления оценки
«Отлично» (8-10)	Решено 5-6 задач
«Хорошо» (6-7)	Решены 4 задачи
«Удовлетворительно» (4-5)	Решены 3 задачи
«Неудовлетворительно» (0-3)	Решены менее 3 задач

КОНТРОЛЬНАЯ РАБОТА №1

Вариант контрольной выдается студентам на занятии и состоит из 4 задач. Студенты решают задания индивидуально и сдают их в письменном виде.

Пример варианта задач для контрольной:

Задача 1. [максимум 2,5 балла за правильно выполненную задачу]

Решить уравнение x^29 = 2 mod 693.

Задача 2. [максимум 2,5 балла за правильно выполненную задачу]

Для какого наименьшего k верно, что a^k= a^(k-φ(n)) (mod n) для всех a из Z/n?

Задача 3. [максимум 2,5 балла за правильно выполненную задачу]

Разложите дробь (x^2+1)/(x^2n+1) на простейшие над комплексными числами.

Задача 4. [максимум 2,5 балла за правильно выполненную задачу]

Докажите тождество Σ_{k=0}^n (-1)^{n-k}C_n^k k^m=0 при 0<=m<n.

Критерии оценивания и шкала оценки контрольной работы №1

Оценка	Критерии выставления оценки
«Отлично» (8-10)	Решено задач на 8 и более баллов
«Хорошо» (6-7)	Решено задач на 6-7 баллов
«Удовлетворительно» (4-5)	Решено задач на 4-5 баллов
«Неудовлетворительно» (0-3)	Решено задач менее чем на 4 балла

КОНТРОЛЬНАЯ РАБОТА №2

Вариант контрольной работы выдается студентам на занятии и состоит из 4 задач. Студенты решают задания индивидуально и сдают их в письменном виде.

Пример варианта задач для контрольной:

Задача 1. [максимум 2,5 балла за правильно выполненную задачу]

Доказать неприводимость x^5+2x^3+3x^2 -6x-5.

Задача 2. [максимум 2,5 балла за правильно выполненную задачу]

Найдите дискриминант полинома x^n+ax^{n-1}+...+ax+a.

Задача 3. [максимум 2,5 балла за правильно выполненную задачу]

Разложите многочлен f(x)=x^3+x^2+1 на множители над F_8=F_2[t]/t^3+t+1.

Задача 4. [максимум 2,5 балла за правильно выполненную задачу]

Покажите, что любое расширение L/K степени 2 имеет вид K[\sqrt{d}], d из K, если char K не равно 2.

Критерии оценивания и шкала оценки контрольной работы №2

Оценка	Критерии выставления оценки
«Отлично» (8-10)	Решено задач на 8 и более баллов
«Хорошо» (6-7)	Решено задач на 6-7 баллов
«Удовлетворительно» (4-5)	Решено задач на 4-5 баллов
«Неудовлетворительно» (0-3)	Решено задач менее чем на 4 балла

7.2.3. Итоговый контроль по дисциплине

УСТНЫЙ ЭКЗАМЕН

Устный проводится в форме ответов на вопросы экзаменационного билета. Экзаменационный билет содержит вопрос из перечня вопросов к экзамену и задачу. На подготовку ответа выделяется 2,5 часа.

Примерный перечень вопросов к экзамену:

1. Понятие кольца. Кольцо целых чисел, кольцо вычетов по модулю n, кольцо многочленов и кольцо формальных степенных рядов. Группа обратимых элементов кольца.
2. Теорема о делении с остатком для целых чисел. Линейное разложение НОД-а.

Следствие про кольцо Z/n. Разрешимость и общее описание всех решений линейного диофантового уравнения.

3. Алгоритм Евклида для нахождения НОД-а двух чисел. Расширенный алгоритм Евклида для нахождения линейного разложения. Оценка на число делений с остатком в алгоритме Евклида.
4. Гомоморфизмы колец. Характеристика кольца.
5. Устройство гомоморфизмов из кольца многочленов в другое кольцо. Критерий неразрешимости уравнений. Примеры.
6. Понятие идеала в кольце. Фактор по идеалу. Универсальное свойство.
7. Примеры идеалов. Примеры использования теоремы о гомоморфизме и универсального свойства.
8. Идеалы и линейные уравнения. Идеал порождённый множеством.
9. Понятие делителя нуля, нильпотента. Примеры. Область целостности. Примеры.
10. Понятия теории делимости. Ассоциированность. Простой и неприводимый элементы.
11. Область главных идеалов. Простота и неприводимость элементов в области главных идеалов. Простота и максимальность.
12. Факториальное кольцо. Критерий делимости и вычисление НОД-а в факториальном кольце. Лемма про цепочку идеалов. Единственность разложения на множители в области главных идеалов.
13. Кольцо многочленов. Степень многочлена. Теорема о делении с остатком. Кольцо многочленов над полем как область главных идеалов. Описание фактора кольца многочленов.
14. Делимость многочленов. Теорема о формальном и функциональном равенстве многочленов. Число корней целочисленного многочлена.
15. Теорема Вильсона. Описание фактора $K[x]/(x-a)$ при помощи гомоморфизма подстановки. Схема Горнера вычисления значения многочлена. Лемма про нахождение неполного частного.
16. Произведение колец. Группа обратимых элементов произведения колец. Решение системы уравнений в произведении колец.
17. Китайская теорема об остатках. Системы сравнений. Пример решения системы сравнений над целыми числами. Пример решения уравнений по непростому модулю.
18. Общие факты про группу обратимых элементов кольца $\mb Z/n$. Функция Эйлера от произведения взаимно-простых показателей. Теорема Эйлера. Теорема Ферма.
19. Критерий цикличности группы. Цикличность конечной подгруппы в группе обратимых элементов поля. Описание группы $\mb Z/p^*$.
20. Строение группы ${\mb Z/p^k}^*$, для нечётного простого p. Лемма о разложении в произведение.
21. Строение группы ${\mb Z/2^k}^*$. Описание группы обратимых элементов кольца $\mb Z/n$. Критерий цикличности.
22. Тесты на простоту. Тест Ферма. Тест Эйлера. Общая схема. Тест Рабина-Миллера, его корректность.
23. Извлечения корня по модулю n для специальных показателей. Алгоритм RSA-шифрования с открытым ключом.
24. Понятие комплексного числа. Сопряжение. Модуль комплексного числа, формула для обратного. Тригонометрическая запись. Аргумент произведения.
25. Корни из единицы. Извлечение корня из комплексного числа. Основная теорема алгебры. Классификация неприводимых вещественных многочленов.

26. Производная многочлена. Основные свойства. Кратность множителя и производная. Формула Тейлора для многочлена.
27. Задача интерполяции. Интерполяция по Эрмиту.
28. Дискретное преобразование Фурье и способ его вычислить.
29. Конструкция локализации области целостности. Корректность. Универсальное свойство. Примеры использования.
30. Поле дробно-рациональных функций. Разложение на простейшие дроби – существование. Пример использования задачи интерполяции для разложения на простейшие.
31. Лемма Гаусса. Содержание многочлена. Переформулировка на языке содержания.
32. Факториальность кольца многочленов над факториальным кольцом.
33. Редукционный критерий. Примеры.
34. Признак Эйзенштейна.
35. Трюк Кронекера и алгоритм разложения рациональных многочленов на множители.
36. Оценка на коэффициенты сомножителей многочлена.
37. Лемма Гензеля. Альтернативный алгоритм разложения на множители.
38. Симметрические многочлены. Элементарные симметрические многочлены. Основная теорема.
39. Степенные суммы. Тождества Ньютона.
40. Результант. Результант как определитель матрицы Сильвестра.
41. Основные формулы. Пример вычисления.
42. Дискриминант. Связь с результантом. Пример вычисления.
43. Расширения полей. Теорема о башне полей.
44. Поле разложения. Единственность.
45. Конечные поля. Автоморфизм Фробениуса. Лемма про тождество в конечном поле.
46. Существование и единственность конечного поля из p^n элементов.
47. Характеризация подполей в конечном поле.
48. Избавление от кратных множителей над конечным полем. Разделение многочлена на множители с одинаковой степенью неприводимых.
49. Алгоритм Берлекемпа и Кантора-Цассенхауза.
50. Коды, исправляющие ошибки. Основные определения.
51. Коды БЧХ. Оценка числа исправляемых битов.
52. Арифметические функции. Производящие функции Дирихле. Свёртка Дирихле
53. Обращение в кольце арифметических функций. Функция Мёбиуса. Формула обращения Мёбиуса
54. Среднее число взаимнопростых пар чисел.

Примеры экзаменационных задач:

Задача 1. Пусть K -- поле из $\mb q$ элементов, а L -- расширение K степени n. Определим отображение $N_{L/K} \colon L^* \to K^*$ по правилу $u \to u\cdot u^q \cdots u^{q^{n-1}}$. Покажите, что отображение $N_{L/K}$ корректно задано и является сюръективным.

Задача 2. Пусть степень расширения [K: Q]=2. Покажите, что любой неприводимый многочлен либо остаётся неприводимым над K, либо раскладывается на два неприводимых множителя одинаковой степени.

Задача 3. Доказать, что полином f(x)=x^p-x-a при a<>0 (mod p) неприводим над полем F_p.

Задача 4. Доказать, что если n наименьшее такое, что x^n = x для всех элементов x

из поля K, то K конечно, и его характеристика делит n.

Задача 5. Рассмотрим неприводимые многочлены f,g из F_p[x]. Пусть deg f=deg g. Докажите, что g(x) имеет корень в F_p[t]/f(t).

Задача 6. Рассмотрим неприводимые многочлены f,g из F_p[x]. Пусть deg f делится на deg g. Докажите, что g(x) имеет корень в F_p[t]/f(t).

Задача 7. Покажите, что если комплексные x и y корни уравнений с целыми коэффицинетами и старшим коэффициентом единица, то их сумма и произведение тоже обладают таким свойством.

Задача 8. Покажите неприводимость над Q полинома (x-a_1)^2(x-a_2)^2\dots (x-a_n)^2, если a_1,a_2,...,a_n -- различные между собой целые числа.

Критерии оценивания и шкала оценки устного экзамена

Оценка	Критерии выставления оценки
«Отлично» (8-10)	Дан развернутый ответ на вопрос. Материал изложен последовательно, все утверждения имеют полные доказательства. Экзаменуемый ответил на все дополнительные вопросы. Задача решена.
«Хорошо» (6-7)	Дан развернутый ответ на вопрос. Материал в целом изложен последовательно, утверждения имеют доказательства. Экзаменуемый верно ответил более чем на 75% дополнительных вопросов. Задача решена.
«Удовлетворительно» (4-5)	Дан ответ на вопрос. В целом верно сформулированы утверждения и определения, написаны все формулы. Экзаменуемый ответил более чем на 50% дополнительных вопросов. Задача решена с недочетами.
«Неудовлетворительно» (0-3)	Обучающийся не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями решает задачу.

7.3 Порядок формирования оценок по дисциплине

Преподаватель учитывает работу на практических занятиях и оценку за текущий контроль (домашние задания).

$$О_{накопленная} = 0{,}15*О_{д/з1} + 0{,}15*О_{д/з2} + 0{,}15*О_{д/з3} + 0{,}15*О_{д/з4} + 0{,}2*О_{к/р1} + 0{,}2О_{к/р2}$$

Действует следующий способ округления накопленной оценки: при значениях от 0,1 до 0,4 оценка округляется в меньшую сторону, от 0,5 до 0,9 – в большую.

Результирующая оценка за дисциплину рассчитывается следующим образом:

$$О_{Результирующая} = 0{,}5О_{экзамен} + 0{,}5\ О_{накопленная}$$

На экзамене студенту не предоставляется возможность получить дополнительный балл для компенсации оценки за текущий контроль.

8. Образовательные технологии

Основными образовательными технологиями являются: интерактивные лекции, работа в группах на семинарах и практических занятиях.

9. Учебно-методическое и информационное обеспечение дисциплины

9.1 Основная литература

1. Бурмистрова Е. Б., Лобанов С. Г.Линейная алгебра. Учебник и практикум для академического бакалавриата/ Е. Б. Бурмистрова, С. Г. Лобанов. — М. : Издательство Юрайт, 2019. — 421 с.
2. Кремер, Н. Ш. Линейная алгебра : учебник и практикум для академического бакалавриата / под ред. Н. Ш. Кремера. — 3-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 422 с.

9.2. Дополнительная литература

1. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7
2. Линейная алгебра и геометрия: учеб. пособие для вузов / И. Р. Шафаревич, А. О. Ремизов. – М.: Физматлит, 2009. – 511 с.

10. Рекомендации для самостоятельной работы студентов

Самостоятельная работа может рассматриваться как организационная форма обучения – система педагогических условий, обеспечивающих управление учебной деятельностью по освоению знаний и умений в области учебной деятельности без посторонней помощи. Студенту нужно четко понимать, что самостоятельная работа – не просто обязательное, а необходимое условие для получения знаний по дисциплине и развитию компетенций, необходимых в будущей профессиональной деятельности.

Самостоятельная работа проводится с целью:

- систематизации и закрепления полученных на лекциях теоретических знаний;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- формирования практических (общеучебных и профессиональных) умений и навыков;
- развития исследовательских умений;
- получения навыков эффективной самостоятельной профессиональной (практической и научно-теоретической) деятельности.

В учебном процессе выделяют два вида самостоятельной работы:

- аудиторная;
- внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа - планируемая учебная работа студентов, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа, не предусмотренная программой учебной дисциплины, раскрывающей и конкретизирующей ее содержание, осуществляется студентом инициативно, с целью реализации собственных учебных и научных интересов.

Для более эффективного выполнения самостоятельной работы по дисциплине преподаватель рекомендует источники для работы, характеризует наиболее рациональную методику самостоятельной работы, демонстрирует ранее выполненные студентами работы и т. п.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференцированный характер, учитывать индивидуальные особенности студента.

Самостоятельная работа может осуществляться индивидуально или группами студентов online и на занятиях в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности.

Контроль результатов внеаудиторной самостоятельной работы осуществляется в пределах времени, отведенного на обязательные учебные занятия по дисциплине на практических занятиях.

11. Материально-техническое обеспечение дисциплины и информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения информационных справочных систем (при необходимости).

Для проведения всех занятий используется проектор и компьютер для проекции слайдов.

12. Особенности организации обучения для лиц с ограниченными возможностями здоровья

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться следующих варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

1) *для лиц с нарушениями зрения:* в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

2) *для лиц с нарушениями слуха*: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

3) *для лиц с нарушениями опорно-двигательного аппарата*: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.