МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____ А.В. Замятин
«_02_» _____ 2022 г.

Фонд оценочных средств по дисциплине

Общая алгебра

Специальность
10.05.01 Компьютерная безопасность
код и наименование специальности

Анализ безопасности компьютерных систем
наименование специализации

Томск–2021

ФОС составил(и):
канд. физ.-мат. наук, доцент
доцент кафедры компьютерной безопасности М.А. Приходовский

Рецензент:
канд. физ.-мат. наук, доцент
доцент кафедры компьютерной безопасности Е.Г. Пахомова

Фонд оценочных средств одобрен на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор С.П. Сущенко

Фонд оценочных средств (ФОС) является элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ФОС разрабатывается в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения, характеризующие этапы формирования компетенций)	**Критерии оценивания результатов обучения**			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ИОПК-3.1 Демонстрирует навыки выполнения стандартных действий, решения типовых задач, формулируемых в рамках базовых математических дисциплин; ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности; ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения.	ОР-3.1 Знает основные алгебраические структуры, свойства матриц и определителей, алгоритмы решения систем линейных уравнений, свойства векторных пространств, свойства кольца многочленов. ОР-3.2 Умеет решать системы линейных уравнений, вычислять определители, производить действия над матрицами, производить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами. ОР-3.3 Владеет навыками вычисления определителей, решения систем линейных уравнений, навыками решения задач в векторных пространствах, полях, группах и кольцах.	Знает основные алгебраические структуры (группа, кольцо, поле векторное пространство), свойства матриц и определителей, алгоритмы решения систем линейных уравнений, алгоритмы разложения многочленов на неприводимые множители, поиска НОД.	Знает основные алгебраические структуры, методы решения систем линейных уравнений, свойства матриц и определителей.	Знает некоторые понятия курса алгебры, может решать некоторые задачи.	Не знает основные понятия курса

2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)
1.	Линейная алгебра	ОР-3.1-3.3.	Контрольные задания, тесты,
2.	Элементы теории чисел. Многочлены	ОР-3.1-3.3.	Контрольные задания, тесты
3.	Теория групп	ОР-3.1-3.3.	Контрольные задания, Теоретический зачёт
4.	Теория колец и полей	ОР-3.1-3.3.	Экзамен

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине.

1 семестр (зачёт)

1. Решить систему уравнений в поле вычетов Z_5 $\begin{cases} \overline{4}\overline{x} + \overline{3}\overline{y} = \overline{1} \\ \overline{2}\overline{x} + \overline{1}\overline{y} = \overline{3} \end{cases}$

2. Дана подстановка. Найти: число инверсий, разложение в произведение циклов, декремент.

1 2 3 4 5 6

3 6 4 5 2 1

3. $A = \begin{pmatrix} 1 & 2 & 5 \\ 0 & 1 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 4 \\ 1 & 1 \\ 3 & 1 \end{pmatrix}$ Найти AB, BA.

4. Найти параметр с, при котором $\begin{vmatrix} 1 & 2 & c \\ 0 & 1 & 1 \\ 1 & 3 & 2 \end{vmatrix} = -3$

5. Найти обратную матрицу $\begin{pmatrix} 3 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 2 \end{pmatrix}^{-1}$

6. Найти параметр a, такой, что ранг матрицы $\begin{pmatrix} 1 & 1 & 0 & 4 \\ 1 & 2 & 2 & 1 \\ 3 & 4 & 2 & a \end{pmatrix}$ равен 2.

7. Решить систему уравнений. $\begin{cases} x_1 + x_2 + 2x_3 = 9 \\ 3x_1 + 6x_2 + 10x_3 = 45 \\ x_1 + 7x_2 + 12x_3 = 51 \end{cases}$

8. Решить однородную систему уравнений, построить ФСР.

$$\begin{cases} x_1 + x_2 + 2x_3 + x_4 = 0 \\ 3x_1 + 6x_2 + 10x_3 + 4x_4 = 0 \\ 4x_1 + 7x_2 + 12x_3 + 5x_4 = 0 \end{cases}$$

2 семестр (зачёт с оценкой).

1. Векторы a,b выражены через p,q: $a = p + 2q$, $b = 4p + 3q$. $|p| = 2, |q| = 1$, угол между ними 60 градусов. Найти (a, b).

2. Найти собственные числа и векторы для линейного оператора, заданного матрицей $\begin{pmatrix} 2 & 0 & 0 \\ 1 & 3 & 2 \\ 0 & 2 & 3 \end{pmatrix}$

3. Найти d = НОД (a,b) и разложение d = au+bv для двух чисел: 150 и 84. 4. Найти НОК двух чисел: 150 и 84.

5. Найти функцию Эйлера для числа 21.

6. Найти остаток от деления 5^{1202} на 13

7. Найти остаток от деления 8559 на 11

8. Найти наименьшее натуральное число, удовлетворяющее системе сравнений: $\begin{cases} x \equiv 1(3) \\ x \equiv 2(5) \\ x \equiv 1(7) \end{cases}$

9. Умножить $(2 + i)(1 + 2i)$

10. Вычислить $\frac{-6 + 4i}{2 + 3i}$

11. Вычислить $\left(1 + i\sqrt{3}\right)^6$

12. Дано универсальное множество $U = \{1,2,3,4,5,6,7\}$ и множества: $A = \{2,4,6,7\}$, $B = \{1,2,6\}$, $C = \{1,3,4,5\}$. Найти $(A \cup B) \cap C$.

13. Есть 3 множества по 10 элементов, пересечение каждой пары содержит 3 элемента. Пересечение всех трёх - один элемент. Сколько всего элементов в объединении трёх множеств?

14. Поделить с помощью схемы Горнера в поле R: $f(x) = x^3 + 2x^2 + 8x + 12$ на $g(x) = x - 3$

15. Поделить с помощью схемы Горнера в поле Z_5: $f(x) = x^3 + 2x^2 + 3x + 4$ на $g(x) = x + 3$

16. Найти НОД двух многочленов $f(x) = x^3 + 11x^2 + 34x + 24$, $g(x) = x^2 + 8x + 12$.

17. Найти НОД и коэффициенты Безу для $f(x) = x^3 + 6x^2 + 13x + 10$, $g(x) = x^2 + 5x + 7$.

18. Устраните иррациональность в знаменателе дроби $\frac{1}{g(x)} = \frac{1}{x^2 + 5x + 7}$, если $f(x) = x^3 + 6x^2 + 13x + 10 = 0$.

19. Найти многочлен 3-й степени с помощью интерполяции, если
$f(-1) = 3,\ \ f(0) = 3,\ \ f(1) = 7,\ \ f(2) = 21$.

(метод неопределённых коэффициентов либо Лагранжа).

20 .Выполните разложение $f(x) = x^4 + 5x^3 + 9x^2 + 7x + 2$ на неприводимые многочлены с помощью метода Кронекера.

21. Найдите кратные корни и выполните разложение на неприводимые многочлены в поле R с помощью НОД многочлена и его производной (либо с помощью матрицы Сильвестра):
$f(x) = x^3 - 4x^2 + 5x - 2$.

22. Найти результант двух многочленов с помощью определителя Сильвестра $f(x) = x^2 + x + 5$
$g(x) = x^2 + 2$

23. При каком минимально возможном натуральном параметре C многочлен
$f(x) = x^3 + Cx^2 + 21x + 21$ неприводим над полем Q согласно признаку Эйзенштейна?

24. Сколько есть способов выбрать 2 объекта из 5 (без учёта порядка)?

25. Есть большое множество шаров 3 разных цветов. Сколько есть различных способов составить наборы из 6 шаров, где k одного цвета, m второго n третьего, k+m+n=6.

26. Есть 6 шаров: 4 белых, 1 красный, 1 чёрный. Сколько способов расположить их по порядку, если шары одного цвета можно не различать?

3 семестр. Теория групп.

ВАРИАНТ 1

1. Какими свойствами обладает бинарная алгебраическая операция < $\mathbb{Z}$, * >, где $a*b = \sqrt{a^2+b^2}$.

2. Пусть $G = \mathbb{R}\backslash\{0\}$, $<G, \cdot>$, $G' = \{g^n \mid n \in \mathbb{Z}\}$, g – фиксированный элемент из G. Будет ли G' подгруппой группы G?

ВАРИАНТ 2

1. Какими свойствами обладает бинарная алгебраическая операция < $\mathbb{Z}$, * >, где $a*b = 4ab$.

2. Пусть $G = M(2, \mathbb{R})$, $<G, +>$, $G' = \left\{\begin{pmatrix} a & b \\ ab & a \end{pmatrix}\right\}$ (где $\forall a, b \in \mathbb{R}$). Будет ли G' подгруппой группы G?

ВАРИАНТ 3

1. Какими свойствами обладает бинарная алгебраическая операция < $\mathbb{Q}$, * >, где $a*b = a + b - 2ab$.

2. Пусть $G = \mathbb{R}$, $<G, +>$, $G' = \{\alpha + \beta\sqrt[3]{2} + \gamma\sqrt[3]{4} \mid \forall \alpha, \beta, \gamma \in n \in \mathbb{Q}\}$. Будет ли G' подгруппой группы G?

4 семестр. Теория колец и полей.

ВАРИАНТ 1

1. Пусть $K = M(2, \mathbb{R})$, $K' = \left\{\begin{pmatrix} a & b \\ -b & 0 \end{pmatrix}\right\}$ (где $\forall a, b \in \mathbb{R}$). Будет ли K' подкольцом кольца K?

2. С помощью многочлена $f(x) = x^2 + x + 2$ построить расширение поля GF(3).

ВАРИАНТ 2

1. Пусть $P = \mathbb{Q}$, $P' = \{2\alpha + 3\beta \mid \forall \alpha, \beta \in \mathbb{Z}\}$. Будет ли P' подполем поля P?

2. С помощью многочлена $f(x) = x^2 + 2x + 2$ построить расширение поля GF(3).

ВАРИАНТ 3

1. Пусть $K = M(2, \mathbb{R})$, $K' = \left\{ \begin{pmatrix} a & b \\ a & -a \end{pmatrix} \right\}$ (где $\forall a, b \in \mathbb{R}$). Будет ли K' подкольцом кольца K?

2. С помощью многочлена $f(x) = x^4 + x + 1$ построить расширение поля GF(2).

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

Кольца и поля

Определение кольца; теорема об основных соотношениях в кольце.

Кольцо многочленов.

Определение поля; 2 примера поля.

Кольцо классов вычетов по идеалу.

Понятие делимости и алгоритм деления Евклида для целых чисел.

Кольцо классов вычетов целых чисел; доказать, что совокупность целых чисел образует идеал тогда и только тогда, когда она состоит из всех чисел, кратных некоторому целому числу.

Кольцо классов вычетов целых чисел.

Кольцо классов вычетов целых чисел. Простые поля Галуа.

Полная и приведенная система вычетов (с примерами).

Функция Эйлера. Теорема о мультипликативности функции Эйлера.

Системы сравнений. Китайская теорема об остатках.

Многочлены над полем: нормированный многочлен, неприводимый многочлен, теорема деления для многочленов, алгоритм деления Евклида для многочленов.

Теорема Безу (с доказательством).

Идеал в кольце многочленов; сформулировать три теоремы для кольца многочленов, аналогичные теоремам для идеала в кольце целых чисел. Определения расширения и характеристики поля Галуа.

Доказать, что в поле характеристики p имеет место равенство $(a + b)^p = a^p + b^p$.

Минимальная функция; 2 теоремы о свойствах минимальной функции (с доказательством).

Определение системы линейных уравнений над полем; совместные и несовместные системы; однородные и неоднородные системы.

Примитивный элемент в поле Галуа. Дискретное логарифмирование в полях Галуа.

Метод решения однородной системы линейных уравнений над полем.

Пример экзаменационных билетов

БИЛЕТ № 1

1. Понятие группы; пример группы; теоремы единственности единичного и обратного элементов в группе (с доказательством).

2. Доказать, что в поле характеристики p имеет место равенство $(a + b)^p = a^p + b^p$.

3. Доказать, что для любых элементов a и b группы G элементы ab и ba имеют одинаковый порядок.

БИЛЕТ № 2

1. Индекс подгруппы в группе; теорема Лагранжа (с доказательством).

2. Кольцо классов вычетов целых чисел; доказать, что совокупность целых чисел образует идеал тогда и только тогда, когда она состоит из всех чисел, кратных некоторому целому числу.

3. Доказать, что в поле нет делителей нуля.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

Зачёт с оценкой формируется на основании контрольных работ, принцип формирования оценки: свыше 90% (4,5 из 5,0, округляется до 5) отлично, свыше 70% (3,5 из 5,0, округляется до 4) хорошо, свыше 50% (2,5 и выше) удовлетворительно, ниже 50% неудовлетворительно.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Критерии оценки:

Отлично: знание и понимание материала в полном объеме.
Хорошо: хорошее знание материала за исключением некоторых деталей.
Удовлетворительно: не глубокое понимание материала, на уровне общих представлений.