

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Общая алгебра

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

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

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля (ИОПК-3.1):

контрольная работа;

1 семестр (зачёт)

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

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 c , 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 $d = \text{НОД}(a, b)$ и разложение $d = au + bv$ для двух чисел: 150 и 84. 4. Найти НОК двух чисел: 150 и 84.

4. Найти остаток от деления 8559 на 11

5. Умножить $(2 + i)(1 + 2i)$

6. Вычислить $\frac{-6 + 4i}{2 + 3i}$

7. Вычислить $(1 + i\sqrt{3})^6$

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

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

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

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

12. Найти многочлен 3-й степени, если: $f(-1) = 3$, $f(0) = 3$, $f(1) = 7$, $f(2) = 21$.

(интерполяция, метод неопределённых коэффициентов либо Лагранжа).

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

14. Найдите кратные корни и выполните разложение на неприводимые многочлены в поле $\mathbb{R}$ с помощью НОД многочлена и его производной (либо с помощью матрицы Сильвестра):

$$f(x) = x^3 - 4x^2 + 5x - 2.$$

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

3 семестр. Теория групп (экзамен).

ВАРИАНТ 1

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

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

ВАРИАНТ 2

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

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

4 семестр. Теория колец и полей (экзамен).

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 $\text{GF}(3)$.

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).

Критерии оценивания: суммарно за всю работу в семестре студент можно получить 3,5 балла из 5,0, то есть 70% от итоговой оценки. Ещё 30% - за ответ по теории на экзамене.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания (ИОПК-3.2, ИОПК-3.3)

Экзамен проводится по билетам, билет состоит из 2 теоретических вопросов. За верный ответ по теории студент получает 1,5 балла из 5 баллов оценки. При сложении с семестровым рейтингом за практику (3,5 балла из итоговой оценки) студент получает 5,0 баллов. В случае получения дробной оценки, итоговая оценка определяется по правилам округления.

Вопросы к дифференцированному зачёту (2 семестр).

1. Доказать, что линейная комбинация собственных векторов, соответствующих одному и тому же числу λ , тоже является собственным вектором, соответствующим λ .
2. Доказать, что любые два собственных вектора, соответствующих различным собственным числам, образуют ЛНС.
3. Доказать, что если x является собственным вектором линейного оператора L , соответствующим λ , то он также является собственным и для обратного оператора L^{-1} , и соответствует числу $1/\lambda$.
4. Доказать, что λ является собственным для линейного оператора, заданного матрицей A , тогда и только тогда, когда $|A - \lambda E| = 0$.
5. Доказать, что если базис состоит из собственных векторов, то матрица оператора относительно этого базиса диагональна.
6. Доказать, что ядро и образ линейного оператора являются подпространствами.
7. Доказать, что матрица A симметрична $\Leftrightarrow (Ax, y) = (x, Ay)$.
8. Доказать, что собственные векторы симметрического оператора, соответствующие разным λ , ортогональны.
9. Доказать, что поле комплексных чисел изоморфно полю матриц вида $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.
10. Доказать формулы $x = \frac{z + \bar{z}}{2}$, $y = \frac{z - \bar{z}}{2i}$

11. Доказать формулы умножения и деления в тригонометрической форме

$$\rho_1 \rho_2 (\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)) = \frac{z_1}{z_2} = \frac{\rho_1}{\rho_2} (\cos(\varphi_1 - \varphi_2) + i \sin(\varphi_1 - \varphi_2)) .$$

12. Доказать формулу Эйлера $e^{ix} = \cos x + i \sin x$.

13. Доказать формулу Муавра $z^n = \rho^n (\cos(n\varphi) + i \sin(n\varphi))$

14. Доказать, что $\sqrt[n]{z} = \sqrt[n]{\rho} \left(\cos \frac{\varphi + 2\pi k}{n} + i \sin \frac{\varphi + 2\pi k}{n} \right)$

15. Доказать, что множество всех корней степени n из 1 является абелевой группой.

16. Доказать, что $\langle U_n, \cdot \rangle \cong \langle Z_n, + \rangle$ (группа корней степени n из единицы изоморфна аддитивной группе вычетов по модулю n).

17. Доказать, что если ε_k первообразный корень n -й степени из 1, то $(k, n) = 1$.

18. Доказать, что если $(k, n) = 1$, то ε_k первообразный корень n -й степени из 1.

19. Доказать, что сумма всех корней степени n из 1 равна 0.

20. Доказать, что $\cos z = \frac{e^{iz} + e^{-iz}}{2}$, $\sin z = \frac{e^{iz} - e^{-iz}}{2i}$.

21. Доказать, что $\operatorname{Ln}(z) = \ln \rho + i(\varphi + 2\pi k)$ ($\forall k \in Z$)

22. Доказать теорему о делении с остатком: Для любых $a, b \in Z, b \neq 0$ найдутся $q \in Z$, $0 \leq r < |b|$, что $a = bq + r$. Причём q, r находятся единственным образом.

23. Доказать, что 2 числа имеют одинаковые остатки от деления на $m \Leftrightarrow (a-b):m$.

24. Доказать, что если $d = \operatorname{НОД}(a, b)$, то существуют такие $u, v \in Z$, что $d = au + bv$ (коэффициенты Безу).

25. Доказать, что для того, чтобы a, b были взаимно простыми, необходимо и достаточно существование целых чисел $u, v \in Z$, таких что $au + bv = 1$.

26. Доказать, что если произведение двух целых чисел ab делится на целое число c , и первый множитель a взаимно прост с c , то $b:c$.

27. Доказать, что последний ненулевой остаток, полученный в алгоритме Евклида, является общим делителем для a, b

28. Доказать, что последний ненулевой остаток, полученный в алгоритме Евклида, является наибольшим общим делителем a, b .

29. Докажите рекурсивные формулы для коэффициентов Безу: $u_k = u_{k-2} - q_k u_{k-1}$,

$$v_k = v_{k-2} - q_k v_{k-1} .$$

30. Доказать, что все решения диофантового уравнения $ax + by = c$, где $a, b, c \in \mathbb{Z}$

задаются формулой
$$\begin{aligned} x &= uc - bk \\ y &= vc + ak \end{aligned} \quad (k \in \mathbb{Z}),$$
 где u, v коэффициенты Безу для a, b .

31. Докажите, что для любого простого $p \geq 5$ верно $p \equiv \pm 1 \pmod{6}$.

32. Докажите, что всякое натуральное число, большее 1, делится по крайней мере на одно простое число.

33. Докажите теорему Евклида о бесконечности множества простых чисел.

34. Докажите, что если $n \in \mathbb{N}$ не делится ни на одно простое число, меньшее или равное $[\sqrt{n}]$, то оно простое.

35. (Основная теорема арифметики). Доказать, что всякое натуральное число $n > 1$ может быть представлено в виде произведения простых чисел: $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$, две таких записи могут отличаться лишь порядком следования сомножителей.

36. Докажите, что если $a = p_1^{s_1} \cdot \dots \cdot p_m^{s_m}$, $b = p_1^{t_1} \cdot \dots \cdot p_m^{t_m}$, то

$\text{НОД}(a, b) = p_1^{k_1} \cdot \dots \cdot p_m^{k_m}$, где $k_i = \min(s_i, t_i)$,

$\text{НОК}(a, b) = p_1^{k_1} \cdot \dots \cdot p_m^{k_m}$, где $k_i = \max(s_i, t_i)$.

37. Докажите формулу взаимосвязи НОД и НОК: $[a, b] = \frac{ab}{(a, b)}$.

38. Докажите универсальный признак делимости.

39. Доказать, что если старший коэффициент многочлена $g(x)$ обратим, то любой многочлен $f(x)$ можно разделить на $g(x)$ с остатком.

40. Доказать, что остаток от деления многочлена $f(x)$ на $x - a$ равен $f(a)$. В частности, a является корнем многочлена $\Leftrightarrow f(x) : (x - a)$.

41. Доказать, что последний ненулевой остаток в алгоритме Евклида является наибольшим общим делителем двух многочленов.

42. Доказать, что кольцо K коммутативно $\Leftrightarrow$ кольцо многочленов $(K[x], +, \cdot)$ коммутативно.

43. Доказать, что кольцо K не содержит делителей нуля $\Leftrightarrow$ кольцо $(K[x], +, \cdot)$ без делителей нуля.

44. Доказать, что если многочлены взаимно просты попарно, то они взаимно просты в совокупности.

45. Доказать формулу взаимосвязи НОК и НОД: $[f, g] = \frac{fg}{(f, g)}$.

46. Доказать, что если многочлен степени $n \geq 2$ неприводим в поле P , то он не имеет корней в поле P .

47. Доказать основную теорему о разложении многочлена на неприводимые множители.

48. Доказать формулу вычисления определителя Вандермонда.

49. Доказать, что если в поле P есть n попарно различных элементов $\alpha_1, \dots, \alpha_n$, то для любых $\beta_1, \dots, \beta_n \in P$ существует единственный многочлен $f(x) \in P[x]$, такой, что $f(\alpha_i) = \beta_i \quad \forall i = 1 \dots n$.

50. Доказать, что многочлен степени $k > 0$ над полем P имеет не более k корней в этом поле.

51. Доказать интерполяционную формулу Лагранжа.

$$y = \sum_{i=1}^n y_i \frac{(x - x_1) \cdot \dots \cdot (x - x_{i-1})(x - x_{i+1}) \cdot \dots \cdot (x - x_n)}{(x_i - x_1) \cdot \dots \cdot (x_i - x_{i-1})(x_i - x_{i+1}) \cdot \dots \cdot (x_i - x_n)}$$

52. Вывести интерполяционную формулу Лагранжа для $n=2$ из канонического уравнения прямой.

53. Интерполяция Эрмита: доказать, что по значениям f и f' в 2 точках можно построить единственную кубическую параболу, которая совпадает с указанной функцией и имеет общую касательную с ней в этих двух точках.

56. Доказать, что если c является корнем кратности k для $f(x)$, то он является корнем кратности $k-1$ для $f'(x)$.

57. Доказать, что всякий многочлен степени $n \geq 1$ с комплексными коэффициентами имеет n корней (если учитывать их столько раз, какова кратность корня).

58. Доказать теорему Виета о взаимосвязи корней с коэффициентами многочлена.

59. Доказать, что если комплексное число z является корнем многочлена $f(x) \in R[x]$, то и $\bar{z}$ является корнем (той же кратности, что и z).

60. Доказать, что всякий многочлен нечётной степени с действительными коэффициентами имеет хотя бы один действительный корень

61. Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ - многочлен с целыми коэффициентами.

Если $\frac{p}{q}$, где $p \in Z, q \in N$, является корнем многочлена $f(x)$, то: 1) $a_n \vdots q$, 2) $a_0 \vdots p$.

62. Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ - многочлен с целыми коэффициентами.

Если $\frac{p}{q}$, где $p \in Z, q \in N$, является корнем многочлена $f(x)$, то $f(m) \vdots (p - mq)$ для любого целого m .

63. Для каждого ненулевого многочлена $f(x) \in \mathbb{Q}[x]$ с рациональными коэффициентами существует ассоциированный с ним примитивный многочлен с целыми коэффициентами, $f(x) \in \mathbb{Z}[x]$.

64. Лемма Гаусса. Произведение примитивных многочленов есть примитивный многочлен.

65. Теорема Эйзенштейна. Если для многочлена $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ с целыми коэффициентами существует простое число p , удовлетворяющее условиям:

- 1) a_n не делится на p .
- 2) $a_{n-1}, \dots, a_2, a_1, a_0$ делятся на p .
- 3) a_0 не делится на p^2 . то $f(x)$ неприводим над полем $\mathbb{Q}$.

66. Докажите одну из формул представления результата: $R(f, g) = a_n^s \prod_{i=1}^n g(\alpha_i)$,

$$R(g, f) = b_s^n \prod_{j=1}^s f(\beta_j)$$

67. Докажите, что результат равен определителю матрицы Сильвестра.

68. $D(f) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$. Доказать взаимосвязь между дискриминантом и

результантом: $R(f, f') = (-1)^{\frac{n(n-1)}{2}} a_n D(f)$.

69. Доказать, что замена $x = y - \frac{b}{3a}$ сводит многочлен 3 степени $ax^3 + bx^2 + cx + d$ к виду, не содержащему 2-й степени.

70. Доказать, что дискриминант уравнения $x^3 + px + q = 0$ равен $D = -4p^3 - 27q^2$.

71. Доказать, что $\alpha + \beta$ является корнем уравнения $x^3 + px + q = 0$, где

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad \beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

72. Доказать, что счётное множество счётных множеств счётно и что $\mathbb{Q}$ тоже счётно.

73. Доказать, что множество всех подмножеств счётного множества не является счётным (теорема Кантора) и что интервал $(0,1)$ не является счётным.

74. Теорема Кантора-Бернштейна. Если множество A равномощно подмножеству множества B , а B равномощно подмножеству множества A , то A и B равномощны.

75. Вывести формулы числа размещений и сочетаний

$$A_n^m = \frac{n!}{(n-m)!} \quad C_n^m = \frac{n!}{m!(n-m)!}$$

76. Вывести формулу числа сочетаний с повторениями $\tilde{C}_n^m = C_{n-1+m}^{n-1} = \frac{(n-1+m)!}{m!(n-1)!}$

77. Доказать свойство Паскаля. $C_n^k + C_n^{k-1} = C_{n+1}^k$.

78. Доказать, что C_n^m это коэффициенты бинома Ньютона $(a+b)^n$.

79. Вывести формулу субфакториала $!n = n! \left(\frac{1}{2!} - \frac{1}{3!} - \dots + (-1)^n \frac{1}{n!} \right)$.

80. Вывести рекурсивную формулу $!(n+1) = n \cdot (!n + !(n-1))$.

81. Числа Стирлинга 2 рода: число разбиений n -элементного множества на k подмножеств. Вывод формулы

$$S(n, k) = S(n-1, k-1) + S(n-1, k) \cdot k$$

82. Числа Стирлинга 1 рода: число перестановок порядка n с k циклами. Вывод формулы $c(n, k) = c(n-1, k-1) + (n-1) \cdot c(n-1, k)$

Пример экзаменационных билетов (3,4 семестр)

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. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Для проверки остаточных знаний можно использовать задачи из типовых контрольных работ, выполнявшихся в течение семестра (приведены в пункте 2).

Информация о разработчиках

Приходовский Михаил Анатольевич, к.ф.м.н., доцент кафедры компьютерной безопасности ИПМКН ТГУ.