

Вопросы к зачету по Крптологии

1. Линейные группы: определение и примеры.
2. Будет ли (абелевой) подгруппой в группе S_4 следующее множество перестановок: $\{e, (23), (24), (34), (234), (243)\}$?
3. Напишите таблицу сложения и умножения для элементов поля \mathbb{Z}_7 . Укажите каждому элементу противоположный и обратный.
4. Порядки линейных групп над конечными полями.
5. Определена ли операция умножения на множестве

$$S = \{e, (13)(24), (1234), (1432)\} \subseteq S_4?$$

Будет ли S подгруппой группы S_4 ?

6. Вычислите противоположную и обратную матрицы над полем \mathbb{Z}_5 для матрицы

$$A = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 0 & 3 \\ 3 & 4 & 2 \end{pmatrix}.$$

7. Подгруппы проективной линейной группы.
8. Является ли множество всех диагональных $n \times n$ -матриц с ненулевыми элементами из поля на диагонали мультипликативной (аддитивной) группой?
9. В симметрической группе S_4 найдите коммутатор $[\tau_1, \tau_2]$ элементов $\tau_1 = (1234)$, $\tau_2 = (13)(24)$.
10. Теоремы Силова. Доказательство существования примарных подгрупп.
11. Укажите порядки всех элементов циклической группы порядка 96.
12. Вычислите порядки линейных групп $GL(3, 3^2)$, $PSL(3, 13^2)$. Найдите порядок центра группы $SL(3, 13)$.
13. Примеры силовских подгрупп. Силовская p -подгруппа группы $GL(n, q)$ и $SL(n, q)$.
14. В диэдральной группе $D = \langle a, b \mid a^4 = b^2 = 1, a^b = a^3 \rangle$ порядка 8 вычислите a^3bab .
15. В циклической группе $\langle a \rangle$ порядка 24 найдите все элементы g , удовлетворяющие условию $g^6 = 1$, и все элементы порядка 24.
16. Группа порядка 15.
17. Является ли множество всех $n \times n$ -матриц с определителем, равным 1, -1 , мультипликативной (аддитивной) группой?
18. В группе $SL(2, \mathbb{C})$ найдите коммутатор $[a, b]$ элементов

$$a = \begin{pmatrix} i & 1 \\ 0 & -i \end{pmatrix}, b = \begin{pmatrix} 1 & i \\ -i & 2 \end{pmatrix}.$$

19. Лемма Фраттини с доказательством (лемма 1.66).
20. В диэдральной группе $D = \langle a, b \mid a^4 = b^2 = 1, a^b = a^3 \rangle$ порядка 8 перечислите все элементы группы и найдите их порядки.
21. В симметрической группе S_4 найдите коммутатор $[\tau_1, \tau_2]$ элементов $\tau_1 = (12)$, $\tau_2 = (123)$.
22. Примарные группы, их свойства.
23. В группе кватернионов $Q = \langle a, b \mid a^4 = b^4 = 1, a^2 = b^2, a^b = a^3 \rangle$ порядка 8 перечислите все элементы группы и найдите их порядки.

24. Найдите в группе $GL(2, \mathbb{Z}_{11})$ коммутатор $[a^{-1}, b]$ элементов

$$a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}.$$

25. Нильпотентные группы, их свойства.

26. Укажите порядки всех элементов циклической группы порядка 12.

27. Вычислите порядки и перечислите подгруппы группы $PSL(2, 2^6)$.

28. Подгруппа Фраттини и ее свойства.

29. В диэдральной группе $D = \langle a, b \mid a^4 = b^2 = 1, a^b = a^3 \rangle$ порядка 8 вычислите a^2bab .

30. Вычислите порядки линейных групп $SL(3, 13^2)$, $PGL(3, 3^2)$. Найдите порядки центров групп $GL(3, 3^2)$, $SL(3, 13)$.

31. Инъекторы разрешимых групп. Примеры.

32. В группе кватернионов $Q = \langle a, b \mid a^4 = b^4 = 1, a^2 = b^2, a^b = a^3 \rangle$ порядка 8 вычислите a^3bab .

33. Определена ли операция умножения на множестве

$$S = \{e, (13)(24), (1234), (1432)\} \subseteq S_4?$$

Будет ли S подгруппой группы S_4 ?

34. Радикалы и радикальные произведения классов.

35. Покажите, что функции

$$f_1(x) = x, \quad f_2(x) = -x, \quad f_3(x) = \frac{1}{x}, \quad f_4(x) = -\frac{1}{x},$$

определенные на $\mathbb{R} \setminus \{0\}$, с операцией умножения (композиция функций) образуют группу. Постройте таблицу умножения элементов этой группы. Укажите единичный элемент. Для каждого элемента группы найдите обратный.

36. Пусть $f : (3\mathbb{Z}, +) \rightarrow (2\mathbb{Z}, +)$ — такое отображение, что $f : 3k \mapsto 6k$. Докажите, что f — гомоморфизм. Найдите ядро и образ. Будет ли f мономорфизмом, эпиморфизмом, изоморфизмом?

37. Коммутант и его свойства.

38. Будет ли множество

$$H = \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & a & b \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$$

подгруппой мультипликативной группы $GL(4, \mathbb{R})$?

39. Докажите, что в группе порядки элементов ab^{-1} и ba^{-1} равны.

40. Классы Фиттинга. Примеры.

41. Найдите все элементы подгруппы $M = \langle (153)(24) \rangle$ мультипликативной группы S_5 и индекс подгруппы M в группе S_5 .

42. Пусть ϕ — отображение мультипликативной группы

$$M = \left\{ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q}, a^2 + b^2 > 0 \right\}$$

в мультипликативную группу

$$N = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}, a^2 + b^2 > 0\}.$$

Будет ли ϕ гомоморфизмом? Если ϕ — гомоморфизм, то найдите $\text{Ker}\phi$ и $\text{Im}\phi$. Будет ли ϕ мономорфизмом, эпиморфизмом, изоморфизмом?

43. Разрешимые группы, их свойства.

44. Найдите порядок элемента $g = \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$, принадлежащего мультипликативной группе $\mathbb{C}^\#$ комплексных чисел. Вычислите g^{100} .

45. Найдите все элементы циклической подгруппы $H = \langle -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i \rangle$ мультипликативной группы $\mathbb{C}^\#$ комплексных чисел.

46. Формации, насыщенные формации. Примеры.

49. Пусть $A = \langle (1234) \rangle$ и $B = \langle (234) \rangle$ — подгруппы симметрической группы S_4 . Найдите число элементов множества AB . Будет ли подгруппой произведение AB ?

50. Составьте таблицу сложения элементов группы $6\mathbb{Z}/18\mathbb{Z}$.

51. Подгруппа Фиттинга и ее свойства.

52. Составьте таблицу сложения элементов группы $6\mathbb{Z}/18\mathbb{Z}$.

53. Найдите все элементы циклической подгруппы $H = \langle -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i \rangle$ мультипликативной группы $\mathbb{C}^\#$ комплексных чисел.

54. Холловы подгруппы разрешимых групп. Примеры холловых подгрупп в разрешимой группе данного порядка.

55. Пусть ϕ — отображение мультипликативной группы

$$M = \left\{ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q}, a^2 + b^2 > 0 \right\}$$

в мультипликативную группу

$$N = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}, a^2 + b^2 > 0\}.$$

Будет ли ϕ гомоморфизмом? Если ϕ — гомоморфизм, то найдите $\text{Ker}\phi$ и $\text{Im}\phi$. Будет ли ϕ мономорфизмом, эпиморфизмом, изоморфизмом?

56. Докажите, что в группе порядки элементов ab^{-1} и ba^{-1} равны.

57. Сверхразрешимые группы и их свойства.

58. Пусть $f : (3\mathbb{Z}, +) \rightarrow (2\mathbb{Z}, +)$ — такое отображение, что $f : 3k \mapsto 6k$. Докажите, что f — гомоморфизм. Найдите ядро и образ. Будет ли f мономорфизмом, эпиморфизмом, изоморфизмом?

59. Определена ли операция умножения на множестве

$$S = \{e, (13)(24), (1234), (1432)\} \subseteq S_4?$$

Будет ли S подгруппой группы S_4 ?

60. Картеровы и гашюцевы подгруппы.

61. Вычислите порядки линейных групп $\text{SL}(3, 13^2)$, $\text{PGL}(3, 3^2)$. Найдите порядки центров групп $\text{GL}(3, 3^2)$, $\text{SL}(3, 13)$.

62. В симметрической группе S_4 найдите коммутатор $[\tau_1, \tau_2]$ элементов $\tau_1 = (12)$, $\tau_2 = (123)$.

63. Проекторы, примеры. Проекторы в разрешимых группах.

64. Укажите разложение циклической группы порядка 36 в прямое произведение циклических примарных подгрупп.

65. Найдите в группе $\text{GL}(2, \mathbb{Z}_{11})$ коммутатор $[a^{-1}, b]$ элементов

$$a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}.$$

66. Корадикальные произведения.

67. Пусть $A = \langle (1234) \rangle$ и $B = \langle (234) \rangle$ — подгруппы симметрической группы S_4 . Найдите число элементов множества AB . Будет ли подгруппой произведение AB ?

68. Вычислите порядки и перечислите подгруппы группы $\text{PSL}(2, 2^6)$.

69. Прimitивные группы и их свойства.

70. Найдите все элементы циклической подгруппы $H = \langle -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i \rangle$ мультипликативной группы $\mathbb{C}^\#$ комплексных чисел.

71. Вычислите порядки линейных групп $\text{SL}(3, 13^2)$, $\text{PGL}(3, 3^2)$. Найдите порядки центров групп $\text{GL}(3, 3^2)$, $\text{SL}(3, 13)$.

72. Классы Шунка и их свойства.

73. Докажите, что в группе порядки элементов ab^{-1} и ba^{-1} равны.

74. Пусть $f : (3\mathbb{Z}, +) \rightarrow (2\mathbb{Z}, +)$ — такое отображение, что $f : 3k \mapsto 6k$. Докажите, что f — гомоморфизм. Найдите ядро и образ. Будет ли f мономорфизмом, эпиморфизмом, изоморфизмом?

75. Корадикал и его свойства. Абелевы и нильпотентные корадикалы.