

# Основы высшей алгебры и теории кодирования

## Предварительная программа экзамена

(МФТИ, весенний семестр 2017 года)

Экзамен состоит из трёх частей: определения и формулировки основных теорем; доказательства фактов из курса; решение задач.

Экзамен начинается с беседы по первой части и при неудовлетворительном ответе на ней же и заканчивается с результатом 0 баллов.

При удовлетворительном ответе на вопросы по первой части экзаменуемый получает от 10 до 20 баллов (в зависимости от полноты ответов) и ему выдаются теоретический вопрос (легкий или трудный, по выбору студента) и задача (трудность задачи на выбор студента: простая, средняя, трудная).

Полный ответ на легкий теоретический вопрос оценивается в 30 баллов.

Полный ответ на трудный теоретический вопрос оценивается в 40 баллов.

Полное решение простой задачи оценивается в 10 баллов.

Полное решение средней задачи оценивается в 20 баллов.

Полное решение трудной задачи оценивается в 40 баллов.

## 1 Определения, формулировки теорем

1. Группа.
2. Примеры групп: аддитивная группа вычетов по модулю  $n$ , мультипликативная группа вычетов по модулю  $n$ , группа комплексных корней из единицы, группа перестановок (симметрическая группа), знакопеременная группа, циклическая группа, группа диэдра.
3. Порядок группы, порядок элемента группы.
4. Четность перестановки.
5. Цикловое разложение перестановки. Формула для порядка перестановки.
6. Подгруппа.
7. Описание подгрупп циклической группы порядка  $n$ .
8. Описание подгрупп бесконечной циклической группы.
9. Смежные классы по подгруппе.
10. Теорема Лагранжа. Малая теорема Ферма. Теорема Эйлера.
11. Прямое произведение групп.
12. Сопряженные элементы. Сопряженные подгруппы. Нормальные подгруппы.
13. Критерий сопряженности перестановок.
14. Гомоморфизмы групп. Сюръективные и инъективные гомоморфизмы. Изоморфизмы и автоморфизмы.

15. Ядро гомоморфизма.
16. Факторгруппа.
17. Теорема о гомоморфизмах групп.
18. Действия групп. Орбита, стабилизатор.
19. Теорема Кэли.
20. Лемма Бернсайда.
21. Кольцо.
22. Примеры колец: кольца вычетов по модулю  $n$ , кольца функций, кольца многочленов с коэффициентами в кольце.
23. Степень многочлена. Логарифмическое свойство степени.
24. Корень многочлена. Лемма о количестве корней многочлена.
25. Квадратичные вычеты. Критерий квадратичного вычета по простому модулю.
26. Виды элементов кольца: обратимые элементы, нильпотентные, делители нуля.
27. Виды колец: коммутативные, целостные, поля.
28. Прямая сумма колец.
29. Идеалы в кольце.
30. Кольца классов вычетов по модулю идеала.
31. Теорема о максимальных идеалах.
32. Евклидовы кольца.
33. Теорема об идеалах в евклидовых кольцах.
34. Основная теорема арифметики для евклидовых колец.
35. Китайская теорема об остатках для евклидовых колец.
36. Функция Эйлера. Свойство мультипликативности функции Эйлера.
37. Характеристика поля. Простые поля.
38. Векторное пространство над полем. Базис.
39. Алгебраическое расширение поля.
40. Минимальный многочлен.
41. Теорема о поле разложения многочлена.
42. Существование и единственность поля с  $p^n$  элементами.
43. Цикличность мультипликативной группы конечного поля.
44. Первообразные корни.
45. Корректирующий код. Кодовое расстояние.
46. Циклический код.
47. Код Хэмминга.
48. Код BCH.
49. Граница Хэмминга.

## 2 Теоретический вопрос

### 2.1 Лёгкие вопросы

1. Критерий обратимости вычета по модулю  $n$ .
2. Порядок элемента в прямом произведении групп.
3. Лемма о пересечении классов смежности.
4. Теорема Лагранжа.
5. Малая теорема Ферма.
6. Теорема Эйлера.
7. Лемма о пересечении классов сопряжённости.
8. Действие группы на смежных классах по подгруппе.
9. Обратимые элементы кольца образуют группу.
10. Кольцо многочленов с коэффициентами в поле не содержит делителей нуля.
11. Логарифмическое свойство степени в кольце многочленов с коэффициентами в поле.
12. Критерий делимости многочлена на многочлен первой степени  $x - a$  (в кольце многочленов с коэффициентами в поле).
13. Ядро гомоморфизма колец является двусторонним идеалом.
14. Пересечение идеалов является идеалом.
15. Все идеалы в евклидовых кольцах главные.
16. Алгоритм Евклида нахождения НОД.
17. Расширенный алгоритм Евклида.
18. Алгоритм решения общего линейного диофантова уравнения.
19. Все идеалы в кольце вычетов  $F[x]/I$  — главные. ( $F$  — поле.)
20. Критерий неприводимости многочленов степени не выше 3 в кольце многочленов с коэффициентами в поле.
21. Количество корней многочлена из  $F[x]$  не превосходит степени многочлена. ( $F$  — поле.)
22. Критерий квадратичного вычета.
23. Формула для количества первообразных корней по модулю  $n$ .
24. Характеристика поля — простое число.
25. Минимальный многочлен неприводим.
26. Необходимое условие существования подполя из  $p^k$  элементов в поле из  $p^n$  элементов.
27. Автоморфизм Фробениуса.
28. Граница Хэмминга.
29. Построение кода Хэмминга.

## 2.2 Трудные вопросы

1. Соотношение между порядком группы, порядком и индексом подгруппы.
2. Теорема о гомоморфизмах групп.
3. Сюръективный гомоморфизм из симметрической группы в группу порядка 2.
4. Критерий сопряжённости перестановок.
5. Соотношение между мощностью орбиты, порядком стабилизатора и порядком группы.
6. Лемма Бернсайда.
7. Теорема Кэли.
8. Действие группы сопряжениями.
9. Теорема о максимальных идеалах.
10. Основная теорема арифметики для евклидовых колец.
11. Китайская теорема об остатках.
12. Мультипликативность функции Эйлера.
13. Формула для функции Эйлера.
14. Мощности базисов в конечномерном векторном пространстве над полем одинаковы.
15. Теорема о поле разложения многочлена.
16. Существование поля с  $p^n$  элементами.
17. Единственность поля с  $p^n$  элементами.
18. Цикличность мультипликативной группы конечного поля.
19. Размерность циклического кода.
20. Построение кода BCH.

## 3 Типовые задачи

Приводятся примерные задачи, на экзамене могут быть другие похожего уровня сложности.

### 3.1 Простые задачи

1. Порядок элемента  $g$  группы  $G$  равен 104. Чему равен порядок элемента  $g^{39}$ ?
2. В группе  $(\mathbb{Q}, +)$  рациональных чисел по сложению рассмотрим подгруппу  $G$ , порождённую числами  $1/2, 1/6, 1/7$  (наименьшую подгруппу, которая содержит все эти числа). Верно ли, что числа  $1/9$  и  $-7/27$  принадлежат одному классу смежности по подгруппе  $G$ ?
3. Вычислите (а)  $12^{257} \bmod 17$ ; (б)  $10^{111} \bmod 121$ ; (в)  $26^{21^{100500}} \bmod 14$ .
4. Делится ли  $25^{54} - 1$  на 107?
5. Найти порядок перестановки  $(12345)(6789)$ .
6. Решите уравнение  $x \circ (14)(23)(7869) = (123)(456)(789)$  в группе  $S_9$  перестановок из 9 элементов.

7. Существует ли элемент порядка 48 в  $S_{12}$ ?
8. Докажите, что все элементы в классе сопряжённости имеют одинаковый порядок.
9. Докажите, что если элементы  $x, y$  в конечной группе сопряжены, то наименьший порядок нормальной подгруппы, содержащей  $x$ , равен наименьшему порядку нормальной подгруппы, содержащей  $y$ .
10. Пусть  $\varphi: G_1 \rightarrow G_1$  — инъективный гомоморфизм групп. Про элементы  $x, y$  известно, что они принадлежат одному классу смежности по ядру гомоморфизма  $\varphi$ . Следует ли из этого, что  $x = y$ ?
11. Найдите вычет, обратный 13 в мультипликативной группе кольца  $\mathbb{Z}/109\mathbb{Z}$ .
12. Решите диофантово уравнение  $23x - 33y = 2$ .
13. Решите уравнение  $17x = 9$  в кольце  $\mathbb{Z}/(71)$ .
14. Решите систему сравнений
 
$$\begin{cases} x \equiv 2 \pmod{39} \\ x \equiv -2 \pmod{29} \end{cases}$$
15. Докажите, что множество решений сравнения  $x^2 \equiv 1 \pmod{n}$  образует подгруппу в  $\mathbb{Z}/n\mathbb{Z}$ .
16. Найдите все решения сравнения  $x^2 \equiv 1 \pmod{200}$ .
17. Решите уравнение  $x^2 - 1 = 0$  в кольце  $\mathbb{Z}/143\mathbb{Z}$ .
18. Найдите порядок группы обратимых элементов кольца  $\mathbb{Z}/480\mathbb{Z}$ .
19. Найдите порядок элемента  $t^8$  в мультипликативной группе кольца  $\mathbb{F}_7[t]/(t^6 - 3)$ .
20. Решите уравнение  $(t + 1)^2 x = t^2$  в кольце вычетов  $\mathbb{Q}[t]/(t^3 + 3t + 1)$ .
21. Проверьте, является ли полем кольцо вычетов  $\mathbb{F}_5[x]/(x^2 - x + 1)$ .
22. Равны ли  $3^{-1}$  и  $18^{-1}$  в поле из 25 элементов?
23. Про элементы  $x, y$  поля из 169 элементов известно, что  $x = 2y$ . Следует ли из этого равенство  $12x = 37y$ ?

### 3.2 Задачи средней трудности

1. Решите уравнение  $x^2 \circ (14)(23)(7869) = (123)(456)(789)$  в группе  $S_9$  перестановок из 9 элементов.
2. Найдите наименьший порядок группы  $G$ , содержащей по крайней мере семь элементов порядка 14.
3. Докажите, что количество элементов в классе сопряжённости является делителем порядка группы.
4. Найдите все классы сопряженности в  $S_{11}$ , которые содержат перестановку порядка 12.
5. Существует ли гомоморфизм группы  $S_9$ , ядром которого является подгруппа  $G$ , состоящая из перестановок, которые элемент 1 переводят в себя?
6. Для каких групп отображение  $x \mapsto x^{-1}$  является автоморфизмом?

7. Многочлены  $x + 1$  и  $x^3 + x$  принадлежат одному классу вычетов по модулю идеала  $I$  кольца  $\mathbb{Q}[x]$  многочленов с рациональными коэффициентами. Докажите, что многочлены  $x^3 - x^2$  и  $x^6 - x^2$  также принадлежат одному классу вычетов по модулю идеала  $I$ .
8. Найдите наибольший общий делитель многочленов  $x^{84} - 1$  и  $x^{35} - 1$ .
9. Двусторонний идеал  $I$  кольца  $R$  порождён всеми элементами вида  $x^2$ , где  $x \in R$ . Докажите, что кольцо классов вычетов  $R/I$  антикоммутативно:  $ab = -ba$  для всех  $a, b \in R/I$ .
10. Докажите, что множество нильпотентных элементов коммутативного кольца вместе с нулевым элементом образует идеал.
11. Может ли пересечение двух различных максимальных идеалов евклидова кольца содержать простой элемент?
12. Найдите все гомоморфизмы поля  $\mathbb{F}_{81}$  в кольцо вычетов  $\mathbb{Z}/(81)$ .
13. Докажите, что для простого  $p$  сравнение  $x^2 \equiv 1 \pmod{p}$  имеет ровно два решения.
14. Найдите количество решений уравнения  $x^2 + 14 = 0$  в кольце  $\mathbb{Z}/(483)$ .
15. Найдите количество решений уравнения
 
$$x^{25} + x^5 + x = 1$$
 (а) в поле из 125 элементов; (б) в поле из 625 элементов.
16. Найдите сумму всех квадратичных вычетов по модулю 323.
17. Найдите все первообразные корни по модулю 23.
18. Проверьте, является ли полем кольцо вычетов  $\mathbb{F}_7[x]/(x^4 - x^2 + 1)$ .

### 3.3 Трудные задачи

1. Докажите, что множество тех элементов  $g$  группы  $G$ , сопряжение которыми переводит элемент  $a \in G$  в себя, является подгруппой (называется нормализатором элемента). Найдите нормализатор перестановки  $(12345)(678) \in S_8$ .
2. Найдите порядок группы  $G = \text{Aut}(C_3 \times C_3)$  автоморфизмов прямого произведения двух циклических групп  $C_3$ .
3. Постройте сюръективный гомоморфизм  $\text{Aut}(C_3 \times C_3) \rightarrow S_4$ .
4. Докажите, что в группе  $G$  порядка  $p^n$ , где  $p$  — простое число, найдется элемент  $z \neq e$ , который коммутирует со всеми элементами группы:  $zg = gz$  для всех  $g \in G$ .
5. Докажите, что количество внутренних автоморфизмов (т.е. автоморфизмов вида  $x \mapsto gxg^{-1}$ ) конечной группы делит порядок группы.
6. Найдите количество нильпотентных элементов в кольце  $F_7[x]/(x^{14} + x^7 + 2)$ .
7. Известно, что минимальный многочлен элемента  $a \in \mathbb{F}_4$  равен  $x^2 + x + 1$ . Следует ли из этого, что многочлен  $x^3 + ax^2 + a$  неприводим в кольце  $\mathbb{F}_4[x]$ ?
8. (а)  $a \in \mathbb{F}_{121}$  — корень многочлена  $x^2 - 2x + 4$  в поле из 121 элемента. Найдите возможные значения  $a^{12}$ . (б) Тот же вопрос для многочлена  $x^2 + 6x + 4$ .
9. Пусть  $a$  — порождающий мультипликативной группы поля  $\mathbb{F}_{32}$ . Найдите наименьшую степень многочлена из  $\mathbb{F}_2[x]$ , корнями которого являются  $a^3, a^9, a^{15}$ .
10. Укажите степени неприводимых делителей многочлена  $x^{28} - 1 \in F_3[x]$ .

11. Существует ли такой многочлен  $f \in \mathbb{F}_2[x]$  степени 10, что в его поле разложения не менее  $2^{30}$  элементов?
12. Проверьте, является ли полем кольцо вычетов  $\mathbb{F}_{11}[x]/(x^{11} - x + 1)$ .