

## Программа к экзамену по алгебре

осень 2021, группа 241, лектор И.В. Аржанцев

1. Группа, подгруппа, гомоморфизм, изоморфизм и автоморфизм. Примеры групп: числовые (аддитивные и мультипликативные), вычеты, группы подстановок, группы матриц, группы симметрий, группа диэдра  $D_n$ , группа кватернионов  $Q_8$ .
2. Циклические подгруппы, порядок элемента, циклические группы и их подгруппы.
3. Криптография с открытым ключом. Задача дискретного логарифмирования и метод повторного возведения в квадрат. Система Диффи-Хеллмана обмена ключами. Криптосистема Эль-Гамала.
4. Смежные классы, индекс подгруппы, теорема Лагранжа и пять следствий из нее.
5. Нормальные подгруппы, факторгруппы, теорема о гомоморфизме, примеры.
6. Группа автоморфизмов  $\text{Aut}(G)$ , группы автоморфизмов циклических групп, группа внутренних автоморфизмов  $\text{Inn}(G)$ , центр группы.
7. Классы сопряженности, централизатор элемента, формула для числа элементов в классе сопряженности, классы сопряженности в группах  $S_n$ ,  $D_n$  и  $\text{GL}_n(\mathbb{C})$ .
8. Внешние и внутренние прямые произведения групп, факторизация по сомножителям, разложение конечной циклической группы.
9. Абелевы группы: периодическая часть, группы без кручения, конечно порожденные и свободные группы. Базис и ранг свободной абелевой группы, матрица перехода.
10. Подгруппа свободной абелевой группы ранга  $n$  свободна и ее ранг не превосходит  $n$ , приведение целочисленной матрицы к диагональному виду, теорема о согласованных базисах.
11. Факторгруппы свободных абелевых групп, универсальное свойство свободной абелевой группы, разложение конечно порожденной абелевой группы в прямую сумму циклических, единственность разложения конечной абелевой группы в прямую сумму примарных циклических.
12. Экспонента конечной группы. Конечная подгруппа мультипликативной группы поля циклическая. Единственность разложения конечно порожденной абелевой группы.
13. Порождающие элементы. Группа  $A_n$  порождена тройными циклами и произведениями пар независимых транспозиций ( $n \geq 5$ ). Порождающие группы  $D_n$ . Группа  $\text{GL}_n(F)$  порождена элементарными матрицами, а группа  $\text{SL}_n(F)$  – элементарными матрицами первого типа.
14. Коммутатор элементов, коммутант и его свойства. Характеристические подгруппы.
15. Коммутанты групп  $S_n$ ,  $A_n$ ,  $D_n$ ,  $\text{SL}_n(F)$  и  $\text{GL}_n(F)$ . Кратные коммутанты, их характеристичность и нормальность.
16. Разрешимые группы, основные примеры и свойства, производный ряд, разрешимость группы верхнетреугольных матриц.
17. Простые группы, существование композиционного ряда, абелевы простые группы.
18. Простота группы  $A_n$  ( $n \geq 5$ ).
19. Действие группы на множестве, орбиты и стабилизаторы, транзитивные, свободные и эффективные действия, ядро неэффективности, примеры действий, три действия группы на себе, теорема Кэли.
20. Сопряженность стабилизаторов точек одной орбиты, изоморфизм действий, транзитивное действие изоморфно действию на  $G/H$ , длина орбиты конечной группы, формула Бернсайда.
21.  $p$ -группы, нетривиальность центра и разрешимость.
22. Факторгруппа  $G/Z(G)$  не может быть циклической, коммутативность групп порядка  $p^2$ .
23. Силовские подгруппы. Первая теорема Силова.
24. Вторая теорема Силова.

25. Третья теорема Силова.
26. Группа порядка  $pq$  разрешима степени не выше двух.
27. Представление группы, эквивалентность представлений, подпредставление, неприводимое представление. Примеры представлений. Регулярное представление конечной группы.
28. Мономиальное представление симметрической группы. Неприводимость канонического представления.
29. Прямая сумма представлений, вполне приводимые представления. Примеры отсутствия полной приводимости.
30. Теорема Машке.
31. Инвариантные скалярные произведения над  $\mathbb{R}$  и  $\mathbb{C}$ . Инвариантность ортогонального дополнения.
32. Одномерные представления: сведение к фактору по коммутанту. Описание одномерных комплексных представлений конечных абелевых групп.
33. Неприводимое комплексное представление абелевой группы одномерно.
34. Гомоморфизмы представлений, лемма Шура, усреднение линейных отображений.
35. Характер представления, центральные функции на группе. Пространство комплекснозначных функций на конечной группе как эрмитово пространство.
36. Соотношения ортогональности для характеров.
37. Кратность вхождения неприводимого представления как скалярное произведение характеров, определяемость представления его характером.
38. Число неприводимых представлений конечной группы.
39. Разложение регулярного представления конечной группы на неприводимые. Сумма квадратов размерностей неприводимых представлений.
40. Описание неприводимых представлений групп  $S_3$  и  $S_4$ .
41. Кольца, поля и алгебры: определения и примеры. Групповая алгебра. Делители нуля, обратимые элементы, нильпотенты и идемпотенты. Левые, правые и двусторонние идеалы. Идеалы в коммутативных кольцах. Кольца главных идеалов.
42. Алгебра матриц над полем является центральной простой алгеброй.
43. Факторкольца, теорема о гомоморфизме для колец. Факторкольцо  $F[x]/(f)$  является полем в точности тогда, когда многочлен  $f$  неприводим.
44. Конечное расширение полей и его степень, степень башни расширений, степень расширения  $F \subseteq F[x]/(f)$ . Присоединение корня.
45. Алгебраические и трансцендентные элементы. Минимальный многочлен. Алгебраические элементы образуют подполе.
46. Поле разложения многочлена: существование и единственность.
47. Простое подполе. Порядок конечного поля. Автоморфизм Фробениуса. Теорема существования и единственности для конечных полей.
48. Над  $\mathbb{Z}_p$  существует неприводимый многочлен любой степени. Поле из четырех элементов. Подполя конечного поля.
49. Тела и алгебры с делением. Тело кватернионов. Минимальный многочлен элемента алгебры и его свойства. Конечномерные алгебры с делением над алгебраически замкнутым полем.
50. Теорема Фробениуса.