

Список вопросов к экзамену по компьютерной алгебре

1. Группы, подгруппы, гомоморфизмы групп. Ядро и образ гомоморфизма.
2. Мономорфизмы, эпиморфизмы и изоморфизмы групп. Понятие нормального делителя (нормальной подгруппы). Факторгруппа.
3. Характеризация мономорфизмов в терминах ядра. Основная теорема о гомоморфизме.
4. Группа подстановок (симметрическая группа). Четные и нечетные подстановки. Теорема о том, что всякая группа есть подгруппа симметрической группы (для конечных групп).
5. Левые классы смежности по подгруппе. Индекс подгруппы. Теорема об индексе $[G : K] = [G : H][H : K]$.
6. Действие группы на множестве. Орбиты. Разбиение множества на орбиты и формула орбит. Стабилизатор.
7. Действие группы на себе сопряжениями. Сопряженные элементы. Классы сопряженности. Формула классов.
8. Свободная группа. Теорема: всякая группа есть факторгруппа свободной группы.
9. Прямое произведение групп. Свойства прямого произведения групп.
10. Коммутативные кольца. Гомоморфизмы колец. Моно- и эпиморфизмы. Характеризация мономорфизмов.
11. Идеалы и факторкольца. Определение простого и максимального идеала.
12. Поля и области целостности. Характеризация простого и максимального идеалов в терминах факторкольца.
13. Кольцо полиномов над полем. Кольца главных идеалов. Алгоритм Евклида в кольце полиномов.
14. Существование максимального идеала в кольце. Лемма Цорна.
15. Модули и их гомоморфизмы. Моно, эпиморфизмы и изоморфизмы модулей. Примеры.
16. Китайская теорема об остатках. Целочисленный вариант. Использование в модулярной арифметике.
17. Общий вариант китайской теоремы об остатках. Применение ее к кольцу полиномов.
18. Расширения полей. Конечные и алгебраические расширения. Теорема: любое конечное расширение является алгебраическим.
19. Неприводимые полиномы над полем. Неразложимые элементы кольца. Понятие факториального кольца. Существование неприводимых полиномов над конечными полями.
20. Характеристика поля. Простое подполе. Поля конечной характеристики. Конечные поля. Построение полей Галуа F_q^n .
21. Алгебраическое замыкание поля. Поле разложения многочлена. Существование поля разложения. Поле Галуа, как поле разложения полинома $x^q - x$.
22. Определение и свойства автоморфизма Фробениуса.
23. Факториальные кольца. Задача о разложении полиномов на множители в кольце многочленов. Приведение к случаю свободного от квадратов.
24. Теорема Берлекэмпа.
25. Алгоритм Берлекэмпа для разложения полиномов над конечным полем.