ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение высшего профессионального образования
«Уральский государственный университет им. А.М. Горького»

ИОНЦ «Информационная безопасность»

математико-механический факультет

кафедра алгебры и дискретной математики

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

Конечные поля

Вопросы для самоконтроля

Автор: профессор кафедры алгебры
и дискретной математики
В.В. Кабанов

Екатеринбург
2008

1. Вложения областей целостности в поля.
2. Поле частных области целостности, поля рациональных дробей.
3. Китайская теорема об остатках.
4. Конечные расширения поля.
5. Алгебраические и трансцендентные элементы над полем, минимальный многочлен алгебраического элемента.
6. Алгебраические и трансцендентные расширения полей, простое расширение поля.
7. Поле разложения многочлена, существование и единственность.
8. Свойства операции взятия производного многочлена.
9. Характеризация конечных полей и их подполей.
10. Мультипликативная группа конечного поля, примитивные элементы поля, примитивные многочлены над конечным полем.
11. Свойства корней неприводимых многочленов.
12. Автоморфизм Фробениуса, группа автоморфизмов конечного поля.
13. Формула обращения Мебиуса (аддитивный и мультипликативный варианты).
14. Круговые поля (циклотомические поля или поля деления круга).
15. Корни из единицы над конечным полем, первообразные корни из единицы над конечным полем.
16. Круговые многочлены над конечным полем, строение круговых полей над конечным полем.
17. Три способа представления элементов конечного поля.
18. Дискретные логарифмы и антилогарифмы.
19. Алгоритм Берлекемпа разложения многочлена на неприводимые множители.
20. Порядок многочлена, теорема о порядке многочлена и порядке его корней, порядок примитивных многочленов.
21. Теорема о связи примитивных многочленов и круговых многочленов.
22. Метод нахождения минимального многочлена элемента через сопряженные элементы.
23. Два метода построения примитивных многочленов данной степени над конечным полем.
24. Вычисление числа нормированных неприводимых многочленов данной степени над конечным полем.
25. Вычисление произведения всех нормированных неприводимых многочленов данной степени над конечным полем.
26. Второй метод нахождения минимального многочлена элемента.