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

Экзаменационные материалы

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

Екатеринбург
2008

1. Вложения областей целостности в поля.
2. Китайская теорема об остатках.
3. Свойства конечных расширений полей.
4. Минимальный многочлен алгебраического элемента, строение простого алгебраического расширения.
5. Теорема Кронекера.
6. Существование поля разложения многочлена.
7. Единственность поля разложения многочлен.
8. Свойства операции взятия производного многочлена.
9. Характеризация конечных полей.
10. Характеризация подполей конечного поля.
11. Мультипликативная группа конечного поля, примитивные элементы поля, примитивные многочлены над конечным полем.
12. Свойства корней неприводимых многочленов.
13. Автоморфизм Фробениуса, группа автоморфизмов конечного поля.
14. Формула обращения Мебиуса (аддитивный и мультипликативный варианты).
15. Круговые поля (циклотомические поля или поля деления круга).
16. Корни из единицы над конечным полем, первообразные корни из единицы над конечным полем.
17. Круговые многочлены над конечным полем, строение круговых полей над конечным полем.
18. Первый способ представления элементов конечного поля.
19. Второй способ представления элементов конечного поля.
20. Третий способ представления элементов конечного поля.
21. Дискретные логарифмы и антилогарифмы.
22. Алгоритм Берлекемпа разложения многочлена на неприводимые множители.
23. Порядок многочлена, теорема о порядке многочлена и порядке его корней.
24. Порядок примитивных многочленов.
25. Теорема о связи примитивных многочленов и круговых многочленов.
26. Метод нахождения минимального многочлена элемента через сопряженные элементы.
27. Первый метод построения примитивных многочленов данной степени над конечным полем.
28. Второй метод построения примитивных многочленов данной степени над конечным полем.
29. Вычисление числа нормированных неприводимых многочленов данной степени над конечным полем.
30. Вычисление произведения всех нормированных неприводимых многочленов данной степени над конечным полем.
31. Второй метод нахождения минимального многочлена элемента.