ЭКЗАМЕНАЦИОННАЯ ПРОГРАММА ПО КУРСУ
«МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»,
НАПРАВЛЕНИЕ ПОДГОТОВКИ ФИИТ, 2 КУРС, 2 СЕМЕСТР 2014–15 УЧ. Г.

КОЛЬЦА. Определение, примеры колец. Обратимые элементы, мультипликативная группа кольца. Делители нуля, необратимость делителя нуля. Поле, примеры полей. Теорема о конечном кольце без делителей нуля, следствие о кольце $\mathbb{Z}_n$. Поле Галуа, пример поля Галуа $\mathbb{F}_4$.

Кольцо многочленов над произвольным полем. Производная многочлена. Корни многочлена, кратные корни. Приводимые и неприводимые многочлены. Неприводимые многочлены над полями $\mathbb{C}$ и $\mathbb{R}$. Неприводимость многочленов с рациональными коэффициентами (лемма Гаусса, теорема Гаусса, признак Эйзенштейна). Неприводимые многочлены в случае конечного поля. Производная многочлена. Критерий простоты корня.

Идеалы, определение, примеры. Критерии равенств $(a)=\{0\}$ и $(a)=R$, следствия. Кольцо главных идеалов, примеры: $\mathbb{Z}$ и $F[x]$. Гомоморфизм и изоморфизм в случае колец. Факторкольцо, канонический гомоморфизм, теорема о гомоморфизмах в случае колец. Максимальный идеал. Критерии максимальности идеала в случаях колец $\mathbb{Z}$ и $F[x]$. Критерий того, что факторкольцо является полем. Структура факторкольца в случае кольца многочленов.

ТЕОРИЯ ПОЛЕЙ. Характеристика поля. Простота характеристики. Теорема о равенстве $ma=na$ для $a\neq 0$. Соотношение $(a\pm b)^p=a^p\pm b^p$, обобщения.

Изоморфизм полей. Подполе, критерий. Расширения полей. Теорема о присоединении корня неприводимого многочлена. Следствие о расширении, в котором полином разлагается на линейные множители.

Конечные расширения полей (определение, степень расширения). Теорема о степенях. Формула $|L|=|K|^n$, следствие о числе элементов конечного поля. Теорема существования поля $\mathcal{GF}(p^k)$.

Алгебраические элементы, минимальный многочлен, степень алгебраического элемента. Критерий того, что аннулирующий многочлен является минимальным. Алгебраичность элементов конечного расширения. Дискретное логарифмирование в конечной циклической группе, свойства дискретного логарифма. Теорема об уравнении $x^n=a$ в конечной циклической группе. Сравнения второй степени по простому модулю. Символ Лежандра. Свойства символа Лежандра. Символ Якоби. Свойства символа Якоби (включая лемму). Сравнения второй степени по модулю p^k. Сравнения второй степени по модулю 2^k.

Литература

1. И.М. Виноградов. Основы теории чисел.
2. Б.Л. ван дер Варден. Алгебра.