

ЭКЗАМЕНАЦИОННАЯ ПРОГРАММА ПО КУРСУ
«МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»,
НАПРАВЛЕНИЕ ПОДГОТОВКИ ФИИТ, 2 КУРС, 2 СЕМЕСТР 2015–16 уч. г.

Кольца. Определение, примеры колец. Обратимые элементы, мультипликативная группа кольца. Делители нуля, необратимость делителя нуля. Поле, примеры полей. Критерий того, что кольцо $\mathbb{Z}_n$ является полем. Подкольцо, критерий того, что подмножество является подкольцом (б/д). Гомоморфизм колец.

Кольцо многочленов над произвольным полем. Нормированные многочлены. Приводимые и неприводимые многочлены. Свойства неприводимых многочленов. Теорема о разложении многочлена на неприводимые множители. Каноническое разложение многочлена. Корень многочлена, теорема о числе корней многочлена степени n , следствия. Теорема Вильсона. Теорема о циклической группе четного порядка. 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 многочлена.

Идеалы, определение, примеры. Критерии равенств $(a) = \{0\}$ и $(a) = R$, следствия. Теоремы о структуре идеалов в кольцах $\mathbb{Z}$ и $F[x]$. Факторкольцо, канонический гомоморфизм, теорема о гомоморфизмах в случае колец (б/д). Максимальный идеал. Критерий максимальности идеала в случае кольца $\mathbb{Z}$. Критерий того, что факторкольцо является полем (б/д).

ТЕОРИЯ ПОЛЕЙ. Характеристика поля. Свойства характеристики. Соотношения $(a \pm b)^p = a^p \pm b^p$, обобщения.

Подполе, критерий того, что подмножество является подполем (б/д). Простое поле, существование и единственность.

Алгебраические элементы, минимальный многочлен, степень алгебраического элемента. Критерий того, что аннулирующий многочлен является минимальным. Расширение поля алгебраическим элементом.

Конечные расширения полей (определение, степень расширения). Алгебраичность элементов конечного расширения. Теорема о степенях расширений (б/д). Формула $|L| = |K|^{[L:K]}$, следствие о числе элементов конечного поля.

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. Квадратичные вычеты и невычеты, свойства, критерий Эйлера. 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 .

Цикличность групп $\mathbb{Z}_m^*$. Лемма о четности функции Эйлера. Теорема об изоморфизме для группы $\mathbb{Z}_m^*$, следствия. Критерий цикличности группы $\mathbb{Z}_{2^n}^*$. Свойства элемента 5 в группах $\mathbb{Z}_{2^n}^*$. Теорема об изоморфизме $\mathbb{Z}_{2^n}^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}}$

Числа Кармайкла, критерий. Тест Соловея-Штрассена.

Литература

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