Семинар 5. Конечные поля

Задача 5.1. Докажите, что для заданного числа N в поле $\Bbbk$ или нет примитивных корней из 1 степени N, или их число равно значению функции Эйлера $\varphi(n)$.

Задача 5.2. Пусть p – простое. Для каких натуральных m и n

(а) существует гомоморфизм полей $\mathbb{F}_{p^m} \to \mathbb{F}_{p^n}$.

(б) число $p^n - 1$ делится на $p^m - 1$.

Задача 5.3. Пусть $f(x) \in \mathbb{F}_q[x]$ – неприводимый многочлен степени d. Докажите, что

(а) $f(x)$ имеет корень в $\mathbb{F}_{q^d}$;

(б) если $f(x)$ имеет корень в $\mathbb{F}_{q^n}$, то он раскладывается на линейные множители;

(в) $f(x)$ делит многочлен $x^{q^d} - x$.

Задача 5.4.

(а) Докажите, что отображение $a \mapsto a^p$ является автоморфизмом конечного поля характеристики p (называемое автоморфизмом Фробениуса); Каков порядок автоморфизма Фробениуса?

(б)* Докажите, что любой автоморфизм конечного поля $\mathbb{F}_{p^n}$ является степенью автоморфизма Фробениуса, тем самым $Aut(\mathbb{F}_{p^n}) = \mathbb{Z}/(n\mathbb{Z})$.

(в) Опишите подмножество элементов инвариантных относительно некоторой заданной степени автоморфизма Фробениуса и убедитесь, что это подполе в $\mathbb{F}_{p^n}$. Более того, любое подполе в $\mathbb{F}_{p^n}$ может быть представлено таким образом.

Тем самым, имеется биекция между подполями в $\mathbb{F}_{p^n}$ и подгруппами в $\mathbb{Z}/(n\mathbb{Z}) = Aut(\mathbb{F}_{p^n})$.

Задача 5.5. Пусть $\mathbb{F} := \cup_{n \geqslant 1} \mathbb{F}_{p^{n!}}$ объединение возрастающей цепочки вложенных полей. Докажите, что **(а)** $\mathbb{F}$ – поле, **(б)** Любой многочлен над $\mathbb{F}_p$ разложим на линейные множители над $\mathbb{F}$;

(в) $\mathbb{F}$ – алгебраическое замыкание поля $\mathbb{F}_p$.