Разговор про конечные поля (схема). 21 июля

Первая часть: Доказываем, что если существует поле F из n элементов, то $n = p^k$ для некоторого простого p.

Шаг 1.1: *Характеристикой* поля F называется наименьшее такое m, что сумма m единиц в F равна 0. Тогда $m = p$ - простое, и F содержит подполе, изоморфное F_p.

Шаг 1.2: Доказываем необходимое утверждение при помощи "вычерпывания": на k-м шаге у нас есть множество из p^k элементов поля. Если в F еще остались элементы, то мы расширяем выбранное множество до p^{k+1} элементов.

Вторая часть: Существует поле из p^k элементов для любого натурального k.

Шаг 2.1: Доказываем существование поля из p^2 элементов, присоединяя к F_p квадратный корень из какого-то квадратичного невычета.

Шаг 2.2: Пусть $g(x)$ - неприводимый многочлен над F. Тогда все остатки по модулю g образуют поле, которое является расширением поля F. Например, при $F = \mathbb{R}$, $g(x) = x^2+1$ мы получаем расширение, изоморфное $\mathbb{C}$.

Шаг 2.3: Применяя описанную выше процедуру, строим цепочку расширений $F^1 \subset F^2 \subset \cdots \subset F^s$, так что $F^1 = F_p$, для любого $1 \leq k < s$ над полем F^{k+1} многочлен $x^{p^n} - x$ раскладывается на большее число неприводимых множителей, нежели над полем F^{k+1}, а над полем F^s он раскладывается на линейные множители.

Шаг 2.4: Пусть $G = \{\alpha \in F^s | \alpha^{p^n} = \alpha\}$. Тогда G замкнуто относительно арифметических операций (для сложения мы используем тот факт, что $C^k_{p^n}$ делится на p для любого $0 < k < p^n$), то есть образует поле.

Шаг 2.5: Чтобы доказать, что в G содержится ровно p^n элементов, теперь достаточно показать, что у $x^{p^n} - x$ нет кратных корней. Для этого вводим понятие *производной* многочлена над полем: если $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$, то $p'(x) := na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1$ и воспользуемся правилом Лейбница $(p_1 p_2)' = p_1' p_2 + p_1 p_2'$.