3 Поля

3.4 Конечные поля

Теорема 1. *Для любого простого p и любого целого положительного n $\exists$ с точностью до изоморфизма единственное конечное поле, состоящее из p^n элементов.*

Доказательство. Рассмотрим поле разложения E многочлена
$f(X) = X^{p^n} - X$ над $F_p \Rightarrow f(X)$ имеет p^n корней в E с учетом их кратности
Докажем $|E| = p^n$
Рассмотрим $f'(X) = p^n X^{p^n - 1} - 1 = -1(mod\ p)$
В силу теорым о кратности корней: НОД$(f, f') = const \Rightarrow$ корни $f(X)$ имеют кратность $1 \Rightarrow f(X)$ рассkладывается на линейно неповторяющиеся множители в $E \Rightarrow f(X)$ имеет p^n различных корней в E
С другой стороны, множество корней многочлена $f(X)$ в E замкнуто относительно операций сложения, вычитания, усножения и деления на ненулевые элементы $\Rightarrow$ множество корней многочлена $f(X)$ образует расширение поля $F_p \Rightarrow E$ - расширение поля $F_p \Rightarrow |E| = p^n$
(От противного)
Пусть $\exists K \neq E \big| |K| = p^n \Rightarrow K$ имеет подполе, изоморфное полю F_p
Ненулевые элементы в K образуют мультипликативную группу порядка $p^n - 1$
Рассмотрим $\alpha \in K^* \Rightarrow \alpha^{p^n - 1} = 1(mod\ p) \Rightarrow \alpha^{p^n} = \alpha(mod\ p) \Rightarrow \alpha$ - корень $f(X)$ в $K \Rightarrow K$ - поле разложения многочлена $f(X)$ на F_p
Таким образом $E = {}^{F_p[X]}/_{(f(X))}$ и $K = {}^{F_p[X]}/_{(f(X))} \Rightarrow E \cong K$ □

Теорема 2. *F_{p^n} изоморфно как группа $\underbrace{F_p \oplus F_p \oplus ... \oplus f_p}_{n}$ относительно сложения.*
F_{p^n} изоморфна как группа отсносительно умножения $\mathbb{Z}_{p^n - 1}$.

Следствие 1. $[F_{p^n} : F_p] = n$

Следствие 2. *Пусть $(F_{p^n})^* =< \alpha >$. Тогда α - алгебраический на F_p и степень минимального многочлена элемента $\alpha = n$.*

Теорема 3. *Для любого $m|n$ поле F_{p^n} имеет! подполе порядка p^m.*