Семинар 16.

Подполя $\mathbb{F}_{p^n}$. (Этот материал войдет в тесты)

Утв 1. Если $K \simeq \mathbb{F}_{p^n}$, L – подполе K, то $L \simeq \mathbb{F}_{p^d}$, $d \in \mathbb{N} : d \mid n$.

Док-во: $\mathbb{F}_p \subset L \subset K$

$$\dim_{\mathbb{F}_p} K = \dim_{\mathbb{F}_p} L \cdot \dim_L K$$

Пусть $\dim_{\mathbb{F}_p} L = d \Rightarrow \begin{cases} n = d \cdot \dim_L K \\ |L| = p^d \end{cases} \Leftrightarrow \begin{cases} L \simeq \mathbb{F}_{p^d} \\ d \mid n \end{cases}$

Лемма. Если $k, m \in \mathbb{N} : k \mid m$, то $(x^k - 1) \mid (x^m - 1)$.

Док-во: Пусть $m = kl \Rightarrow x^m - 1 = x^{kl} - 1 = (x^k)^l - 1$.

Обозначим $x^k = y$. $\Rightarrow x^m - 1 = y^l - 1$ имеет корень $y = 1 \Rightarrow$

$\Rightarrow (y-1) \mid (y^l - 1)$, т.е. $(x^k - 1) \mid (x^m - 1)$.

Утв 2. Если $p, d, n \in \mathbb{N} : d \mid n \Rightarrow (x^{p^d} - x) \mid (x^{p^n} - x)$.

Док-во: $d \mid n \Rightarrow$ из лекции $(p^d - 1) \mid (p^n - 1) \Rightarrow$

$\Rightarrow$ из лекции $(x^{p^d - 1} - 1) \mid (x^{p^n - 1} - 1) \Rightarrow (x^{p^d} - x) \mid (x^{p^n} - x)$.

Утв 3. Пусть $K \simeq \mathbb{F}_{p^n}$, $d \in \mathbb{N} : d \mid n$, тогда существует единственное подполе L поля K : $L \simeq \mathbb{F}_{p^d}$.

Док-во: K – поле разложения $x^{p^n} - x$.

$(x^{p^d} - x) \mid (x^{p^n} - x)$.

Рассмотрим L – множество корней $(x^{p^d} - x)$ – поле разложения $(x^{p^d} - x)$ – подполе поля разложения K $(x^{p^n} - x)$.

$|L| = |p^d|$, $L \simeq \mathbb{F}_{p^d}$.

Следствие. Количество собственных подполей в $\mathbb{F}_{p^n}$ равно количеству натуральных делителей n, меньших n.

Пример: $\mathbb{F}_{p^8}$, $n = 8$, делители n, меньшие n : $1, 2, 4 \Rightarrow$

$\Rightarrow \exists$ 3 собственных подполя $\mathbb{F}_{p^8}$, изоморфные $\mathbb{F}_p$, $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^4}$.

Тесты

① Сколько существует собственных подполей в поле $\mathbb{F}_{p^{12}}$?

1) 1
2) 11
3) 7
4) 5

② Сколько собственных подполей имеет поле K: $|K|=81$?

1) 1
2) 2
4) 4

③ Какое из перечисленных колец является полем?

1) $\mathbb{Z}[x]/(x^2+1)$
2) $\mathbb{Z}[i]/(i)$
3) $\mathbb{Z}[i]/(2)$
4) $\mathbb{Z}[i]/(3)$

④ Для какого из перечисленных колец не существует поля отношений?

1) $\mathbb{Z}[i]$
2) $\mathbb{Z}[x]/(x^3-7)$
3) $\mathbb{Z}_3[x]/(x^4+1)$
4) $\mathbb{Q}[x]/(x^2-3)$

⑤ Каков порядок группы обратимых элементов A^* кольца A?

$$\mathbb{Z}_{11}[x]/(x^2+5)$$

1) 120
2) 100
3) 10
4) 20