Fields

Fall 2016 #5

$$X^{p^\ell} - X = \prod L_i(x) \qquad p^\ell = \sum_{d \mid \ell} (\#\deg d)\cdot d$$

(monic, irr, $\deg \mid \ell$; $\deg$ ℓ)

How many monic irr. polys $p(x) \in \mathbb{F}_p[x]$ of degree ℓ (prime)?

Notes

$\#\mathbb{F}_p[x]_\ell = p^{\ell+1}$ (write $p(x) = \sum_{j=0}^{\ell} a_j x^j$, p choices for each a_j)

$\Rightarrow \#\text{monic irr} < p^\ell$. ↳ $x^\ell + \sum_{j=0}^{\ell-1} a_j x^j \Big]^{p}_{\ell}$

See D&F p.580?

$f(n) = \sum_{d \mid n} g(n)$

$g(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) f(d)$

$\alpha^{p^\ell} - \alpha = 0$

① $X^{p^\ell} - X$ is separable (no repeated roots)

② $\mathbb{F}_{p^\ell}$ is the splitting field of $X^{p^\ell} - X$

③ $X^{p^\ell} - X = \prod L_i(x)$ where $L_i(x)$ ranges over all monic irr polys of degree dividing ℓ

✱Proof

Idea: $X^{p^\ell} - X = \prod L_i(x)$: Take degrees.

- $p^\ell = \deg(X^{p^\ell} - X) = \deg \prod L_i(x) = \sum \deg L_i(x)$
- ℓ prime forces $\deg L_i(x) = 1, \ell$

$\Rightarrow p^\ell = (\#\deg \ell)\cdot \ell + (\#\deg 1)\cdot 1$ (general: $p^\ell = \sum_{k \mid \ell} (\#\deg k)\cdot k$)

want; need to count

Actual Proof

- $\deg L = 1 \Rightarrow L$ is linear, $L(x) = (x-\alpha)$, $\alpha \in \mathbb{F}_p \Rightarrow p$ choices!

Need $x^{p^\ell} - x$ has distinct roots $\Rightarrow L(x)$ does too.

- $p^\ell = (\#\deg \ell)\cdot \ell + (\#\deg 1)\cdot 1$

$$\Rightarrow \#\deg \ell = \frac{p^\ell - \#\deg 1}{\ell} = \boxed{\frac{p^\ell - p}{\ell}}.$$

Proofs

① Prop (D&F 13.33, p. 547)

f has a multiple root α $\Leftrightarrow$ α is a root of f' and f

Proof

($\Rightarrow$) $f(x) = (x-\alpha)^n g(x)$, $n \geq 2$

$\Rightarrow \frac{d}{dx} f(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n g'(x)$

$= (x-\alpha)\left[n(x-\alpha)^{n-2} g(x) + (x-\alpha)^{n-1} g'(x)\right]$

$\Rightarrow (x-\alpha) \mid \frac{d}{dx} f(x) \Rightarrow \alpha$ is a root of f'

($\Leftarrow$) Assume α is a root of f'.

$\Rightarrow f(x) = (x-\alpha) g(x)$

$\Rightarrow f'(x) = 1 \cdot g(x) + (x-\alpha) g'(x)$

$\Rightarrow f'(\alpha) = g(\alpha) + (\alpha - \alpha) g(\alpha)$

(assume) $= 0$, $= g(\alpha)$

$\Rightarrow \alpha$ is a root of g

$\Rightarrow \alpha$ is a multiple root of f.

Cor: f sep. $\Leftrightarrow \gcd(f, f') = 1$

$(A \Leftrightarrow B)$

Pf:

$\neg B \Rightarrow \neg A$: If $\gcd(f, f') = \ell(x)$, $\deg \ell \geq 1$, then any root α of ℓ is a root of f and f' $\Leftrightarrow$ multiple root of f

$\neg A \Rightarrow \neg B$: f not sep $\Leftrightarrow$ multiple root α

$\Leftrightarrow (x-\alpha) \mid \gcd(f, f') =: \ell(x)$

$\rightarrow \ell(x) \neq 1$.

Cor: $x^{p^\ell} - x \in \mathbb{F}_p[x]$ is separable

Pf Set $g(x) := x^{p^\ell} - x$.

- $g'(x) = p^\ell x^{p^\ell - 1} - 1 \equiv_{\mathbb{F}_p} -1$
- $\gcd(g, g') = \gcd(g, -1) = 1$. (no roots)

② $\mathbb{F}_{p^\ell}$ is the splitting field of $x^{p^\ell} - x$

- $x^{p^\ell} - x \in \overline{\mathbb{F}}[x]$ separable $\Rightarrow$ exactly p^ℓ distinct roots.
- $K := \{\text{roots of } x^{p^\ell} - x \text{ in } \overline{\mathbb{F}}\}$ is a field $\subseteq SF(x^{p^\ell} - x)$

  Both have size p^ℓ $\Rightarrow$ equality.
- $\mathbb{F}_{p^\ell} = K$, and SFs are uniq up to iso.

$\alpha \in \mathbb{F}_{p^\ell} \setminus \{0\} \Rightarrow \alpha \in \mathbb{F}_{p^\ell}^\times \in Grp$, size $p^\ell - 1$

$\Rightarrow \alpha^{p^\ell - 1} = 1$ by Lagrange $\left(H \leq G \Rightarrow o(H) \mid o(G);\ H = \langle \alpha \rangle,\ G = \mathbb{F}_{p^\ell}^\times\right)$

$\Rightarrow \alpha^{p^\ell - 1} \cdot \alpha = \alpha$

$\Rightarrow \alpha^{p^\ell} - \alpha = 0$

$\Rightarrow \alpha \in K$

So $\mathbb{F}_{p^\ell} \subseteq K$, and both have p^ℓ elts $\rightsquigarrow$ equality.

③ $x^{p^\ell} - x = \prod L_i(x)$ where $L_i(x)$ ranges over all monic irr polys of degree dividing ℓ (in $\mathbb{F}_p[x]$)

- $f(x) \in K[x]$ separable $\Rightarrow$ a product of some distinct irr.

  (D&F Prop 13.34 + 13.37: Irr $\Rightarrow$ sep, sep $\Leftrightarrow$ prod. distinct irr)
- $f(x) \mid x^{p^\ell} - x \Rightarrow \deg f \mid \ell$ since

$\mathbb{F}_{p^\ell}$ (b) / $SF(f)$ (a) / $\mathbb{F}_p$ — $\deg \ell$, $\ell = ab$

$g(x) := x^{p^\ell} - x = \prod_{f \mid g \text{ irr}} f(x) = \prod_{d \mid \ell} \left(\prod_{\alpha \in S_d} \min(\alpha, \mathbb{F}_p) \right)$ $\left(S_d = \{\alpha \in \mathbb{F}_{p^\ell} \mid \deg \min(\alpha, \mathbb{F}_p) = d\}\right)$

$\prod (x - \alpha_i)$

group by degree of minimal polynomials of roots

$\alpha \in \mathbb{F}_{p^\ell} \Rightarrow \min(\alpha) \mid x^{p^\ell} - x$