5-9-25 (WEEK 12)

Shun/翔海 (@shun4midx)

FINITE FIELDS

WARM UP

Say $|K|=p^n$, K is a field. Then, $(K^\times, \cdot)$ is cyclic

FACT

$ab=ba$, $\text{ord}(a)=\alpha$, $\text{ord}(b)=\beta \Rightarrow \exists c\in\langle a,b\rangle$, s.t. $\text{ord}(c)=\text{lcm}(\alpha,\beta)$

Proof

Write $\alpha=\prod_i p_i^{m_i}$, $\beta=\prod_i p_i^{n_i}$

For each i, $(M_i,N_i)=\begin{cases}(m_i,0), & m_i\ge n_i\\ (0,n_i), & \text{otherwise}\end{cases}$

Set $\alpha'=\prod_i p_i^{M_i}$, $\beta'=\prod_i p_i^{N_i} \Rightarrow \text{lcm}(\alpha',\beta')=\text{lcm}(\alpha,\beta)$

Also, $\alpha'|\alpha$ and $\beta'|\beta \Rightarrow c=a^{\frac{\alpha}{\alpha'}}b^{\frac{\beta}{\beta'}} \Rightarrow \text{ord}(c)=\text{lcm}(\alpha,\beta)$ □

Let $d=\text{lcm}$ of the orders of all $a\in K^\times$

∴ $\forall a\in K^\times$, $a^d=1 \Rightarrow a^{d+1}=a \Rightarrow (x-a)|x^{d}-1 \Rightarrow |K^\times|=p^n-1\le d$

However, $\forall a\in K^\times$, $d|p^n-1$, $a^{p^n}=a$

∴ $d=p^n-1$

∴ By fact and induction, $\exists g\in K^\times$, s.t. $K^\times=\langle g\rangle$ □

THEOREM 1

$\exists$ a finite field K, s.t. $|K|=q \Leftrightarrow q=p^n$ for some prime p and $n\in\mathbb{N}$. Moreover, K is unique up to isomorphism, denoted by $\mathbb{F}_{p^n}$

Proof

"$\Rightarrow$": Let $\text{char} K=p$, $[K:\mathbb{Z}/p\mathbb{Z}]=n \Rightarrow q=p^n$

"$\Leftarrow$": Let K be a splitting field for $f(x)=x^{p^n}-x$ over $\mathbb{Z}/p\mathbb{Z}$.

Claim: The set of all roots of f forms a field

Proof

$(\alpha\pm\beta)^{p^n}=\alpha^{p^n}\pm\beta^{p^n}=\alpha\pm\beta$, $(\alpha\beta)^{p^n}=\alpha^{p^n}\beta^{p^n}=\alpha\beta$, $(\alpha^{-1})^{p^n}=(\alpha^{p^n})^{-1}=\alpha^{-1}$ with $\alpha\neq0$ ✓

As K is the smallest field containing all roots of $f(x)$ of f, $K=$ set of all roots of f

As $f'=-1$ has no roots, there is no multiple root, i.e. $|K|=p^n$

Note: $\mathbb{Z}/p\mathbb{Z} \leftarrow x^p-x=0$ and $x^p-x\,|\,x^{p^n}-x$, so $\mathbb{Z}/p\mathbb{Z}\hookrightarrow K$

∵ K is a splitting field for f

∴ K is unique up to isom □

THEOREM 2

(1) If $n\in\mathbb{Z}^{>0}$ and $\mathbb{F}_q$ is a finite field, then $\exists!\ \mathbb{F}_{q^n}/\mathbb{F}_q$, s.t. $[\mathbb{F}_{q^n}:\mathbb{F}_q]=n$ and it is Galois.

Proof

By thm 1, $q=p^r$ for some prime p and $r\in\mathbb{N}$.

Then, $q^n=p^{nr}\Rightarrow \mathbb{F}_{q^n}=\mathbb{F}_{p^{nr}}$ is Galois over $\mathbb{F}_p$, so $\mathbb{F}_{q^n}$ is Galois over $\mathbb{F}_{q^n}\supseteq\mathbb{F}_q\supseteq\mathbb{F}_p$ □

(2) $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)=\langle\sigma_q\rangle$, $\sigma_q:\mathbb{F}_{q^n}\longrightarrow\mathbb{F}_{q^n}$, $\alpha\longmapsto\alpha^q$ (q-Frobenius automorphism)

Proof

- $\sigma_q\in\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$
  - ↳ Homo since $q=p^r$
  - ↳ Isom since σ_q is not trivial
  - ↳ Fixes $\mathbb{F}_q$ since $\forall\alpha\in\mathbb{F}_q$, $\alpha^q=\alpha$

- $\forall \alpha \in \mathbb{F}_{q^n}$, $\sigma_q^n(\alpha) = \alpha^{q^n} = \alpha$ so $\sigma_q^n = Id$
  If $\sigma_q^m = Id$ with $1 \le m < n$, then $\sigma_q^m(\alpha) = \alpha^{q^m} = \alpha$ $\forall \alpha \in \mathbb{F}_{q^n} \Rightarrow$ number of $x^{q^m} - x = q^m < q^n$ —✗—
- $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma_q \rangle$ since $|\langle \sigma_q \rangle| = n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = |Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)|$ □

REMARK

1. The subfields of $\mathbb{F}_{p^n}$ are Galois over $\mathbb{F}_p$ and they are $\mathbb{F}_{p^d}$, $d \mid n$, fixed by $\langle \sigma_p^d \rangle$
2. $\bigcup_{n \ge 1} \mathbb{F}_{p^n} = \overline{\mathbb{F}_p}$ is also a field ($\because \forall n_1, n_2$, $\mathbb{F}_{p^{n_1}}, \mathbb{F}_{p^{n_2}} \subseteq \mathbb{F}_{p^{n_1 n_2}}$)

THEOREM 3

$x^{p^n} - x$ = the product of all distinct monic irr poly in $\mathbb{F}_p[x]$ of deg d where d runs through all the divisors of n

Proof

Since $\mathbb{F}_p$ is a perfect field ($\mathbb{F}_p = \mathbb{F}_p^p$), all irr poly in $\mathbb{F}_p[x]$ are separable (no multiple root)

Also, if $f(x), g(x)$ are two monic irr poly in $\mathbb{F}_p[x]$ with $f(\alpha) = g(\alpha)$, then $f = m_{\alpha, \mathbb{F}_p} = g$

Hence, we can get the equality by checking that they have the same roots

"LHS|RHS": $\forall \alpha \in \mathbb{F}_{p^n}$, $\deg m_{\alpha, \mathbb{F}_p} = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] \mid [\mathbb{F}_{p^n}(\alpha) : \mathbb{F}_p] = n$ and $m_{\alpha, \mathbb{F}_p}$ appears in RHS

"RHS|LHS": If β is a root of $p(x)$ in RHS with $d = \deg p \mid n$, then $p(x) = m_{\beta, \mathbb{F}_p}$
We have $|\mathbb{F}_p(\beta)| = p^d$ and $\beta^{p^d} = \beta$, so $\beta = \beta^{p^d} = (\beta^{p^d})^{p^d} = \beta^{p^{2d}} = \ldots = \beta^{p^n}$

EXAMPLE

$$\left.\begin{array}{l} p = 2,\ \deg 1 \Rightarrow x^2 - x = x(x-1) \Rightarrow x, x-1 \\ \quad \deg 2 \Rightarrow x^{2^2} - x = x(x-1)(x^2+x+1) \Rightarrow x^2+x+1 \\ \quad \deg 3 \Rightarrow \underbrace{x^{2^3} - x}_{2 \nmid 3\text{, so no repeated factors from deg 2}} = x(x-1)(x^3+x+1)(x^3+x^2+1) \Rightarrow x^3+x+1,\ x^3+x^2+1 \end{array}\right\} \text{Corr. irr. poly}$$

REMARK (Yes I've gone insane, don't question my sanity pls ty ボクは問題ない(www))

If $\psi_p(d)$ = number of irr poly of deg d in $\mathbb{F}_p[x]$, then $p^n = \sum_{d \mid n} d\,\psi_p(d)$ (The following part of this note will try to prove it)

DEFINITION

Möbius μ-function:

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & n \text{ has square power} \\ (-1)^n, & n \text{ is a product of distinct prime factors} \end{cases}$$

FACT 1

If $n \ge 1$, then $\sum_{d \mid n} \mu(d) = [\frac{1}{n}] = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$

Proof

- $n = 1$: OK
- $n > 1$: Write $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $\sum_{d \mid n} \mu(d) = \mu(1) + \mu(p_1) + \ldots + \mu(p_k) + \mu(p_1 p_2) + \ldots + \mu(p_1 p_2 \cdots p_k)$
  $= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \ldots + \binom{k}{k}(-1)^k = (1 + (-1))^k = 0$ □

DEFINITION

Let f, g be two arithmetic functions

The Dirichlet product of f and g is defined to be $f * g(n) = \sum_{d \mid n} f(d) g(\frac{n}{d})$ ($\Rightarrow f*g = g*f$, $(f*g)*h = f*(g*h)$)

- $I(n) = [\frac{1}{n}]$ is called the identity function
- $u(n) = 1$ $\forall n$ is the inverse of μ: $\mu * u(n) = \sum_{d \mid n} \mu(d) = I(n)$, $u * \mu = I$

FACT 2

Möbius inversion formula: $f(n) = \sum_{d \mid n} g(d) \Rightarrow g(n) = \sum_{d \mid n} \mu(d) f(\frac{n}{d})$

Proof

$f(n) = g * u(n)$ $\forall n \Rightarrow f = g * u \Rightarrow f * \mu = g * u * \mu = g$ □

By fact 2, $n\Psi_p(n) = \sum_{d|n} \mu(d) p^{\frac{n}{d}} \Rightarrow \Psi_p(n) = \frac{1}{n}\sum_{d|n} \mu(d) p^{\frac{n}{d}} \Rightarrow \Psi_2(3)=2,\ \Psi_3(3)=8,\ \Psi_3(2)=3$

Shun/羊羽海 (@shun4midx)

GALOIS POLYNOMIAL EXAMPLE

Let $f(x)\in\mathbb{Q}[x]$ be irr of deg p, where p is a prime.
If f has exactly $p-2$ real roots and 2 complex roots, then the Galois group G of f over $\mathbb{Q}$ is S_p

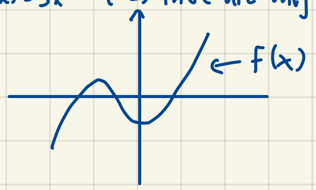
EXAMPLE OF USAGE

Consider $f(x)=x^5-4x+2$

↳ It is irr by Eisenstein criterion

↳ $f'(x)=5x^4-4 \Rightarrow$ There are only two real turning points

∴



∴ The Galois group is S_5, so it is unsolvable.

PROOF

Let $R=\{\alpha_1,\dots,\alpha_p\}$ be the set of roots of f

$\alpha_i\sim\alpha_j \Leftrightarrow (\alpha_i\ \alpha_j)\in G$

- $\alpha_i\sim\alpha_i$
- $\alpha_i\sim\alpha_j \Rightarrow \alpha_j\sim\alpha_i$
- $\alpha_i\sim\alpha_j,\ \alpha_j\sim\alpha_k \Rightarrow (\alpha_i\ \alpha_j)(\alpha_j\ \alpha_k)(\alpha_i\ \alpha_j)^{-1}=(\alpha_i\ \alpha_k)\in G$ ✓

$[\cdot]$ is equivalence class

Claim: $|[\alpha_i]| = |[\alpha_j]|$

Proof

$\sigma: [\alpha_i] \hookrightarrow [\alpha_j]$

$\alpha_t \longmapsto \sigma(\alpha_t) \longrightarrow (\alpha_j\ \sigma(\alpha_t)) = (\sigma(\alpha_i)\ \sigma(\alpha_t)) = \underset{G}{\underset{\Uparrow}{\sigma}}\underset{G}{\underset{\Uparrow}{(\alpha_i\ \alpha_t)}}\underset{G}{\underset{\Uparrow}{\sigma^{-1}}}$

$(\alpha_i\ \alpha_t)\in G$

$$\begin{tikzcd}
L \arrow[r, "\exists\sigma", "\sim"'] & L \\
\mathbb{Q}(\alpha_i) \arrow[u, hook] \arrow[r, "\tau", "\sim"'] & \mathbb{Q}(\alpha_j) \arrow[u, hook] \\
& \mathbb{Q} \arrow[ul] \arrow[u]
\end{tikzcd}
\rightsquigarrow \sigma(\alpha_i)=\alpha_j$$

Now, since $f(\bar{\alpha}_i) = \overline{f(\alpha_i)} = 0$,

$\tau: L \longrightarrow L$

$\alpha_i \longmapsto \bar{\alpha}_i$

$\tau\in G$

Then, $\alpha_1,\dots,\alpha_{p-2}\in\mathbb{R}$, $\alpha_{p-1},\alpha_p\in\mathbb{C}$ $\Rightarrow (\alpha_{p-1}\ \alpha_p)\in G$ ∴ $|[\alpha_{p-1}]|\geq 2$

$R=\bigcup[\alpha_i] \Rightarrow |[\alpha_i]|\ \big|\ p \Rightarrow |[\alpha_i]|=p$

$[\alpha_i]=R$, $(\alpha_1\ \alpha_2), (\alpha_1\ \alpha_3), \dots, (\alpha_1\ \alpha_p)\in G$, so $G=S_p$ □