Announcements

Please fill out midterm course feedback survey

Previous lecture notes updated with justification in two places

---

Finite fields (cont.)

Prop: Let $n > 0$, p: prime. There exists a finite field w/ p^n elts., unique up to isom.

Pf: Existance (last time):

If $f(x) := x^{p^n} - x \in \mathbb{F}_p$, then $Sp_{\mathbb{F}_p}(f)$ is a field of order p^n.

Uniqueness:

Let K be any field of order p^n. Then char $K = p$, $[K : \mathbb{F}_p] = n$.

We have $|K^\times| = |K| - 1 = p^n - 1$, so if $\alpha \in K$, $\alpha^{p^n - 1} = 1$, so $\alpha^{p^n} = \alpha$, α is a root of $x^{p^n} - x$.

Since K has $|K| = p^n$ roots of this poly, it is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, which is unique up to isom. $\square$

Let $\mathbb{F}_{p^n}$ be the unique field of order p^n.

Remark: In practice, we often use the version

$$\mathbb{F}_{p^n} = \mathbb{F}_p/(f) \quad \text{where } f \in \mathbb{F}_p[x] \text{ is irred.}$$

since here the presentation is explicit

Cyclotomic Fields

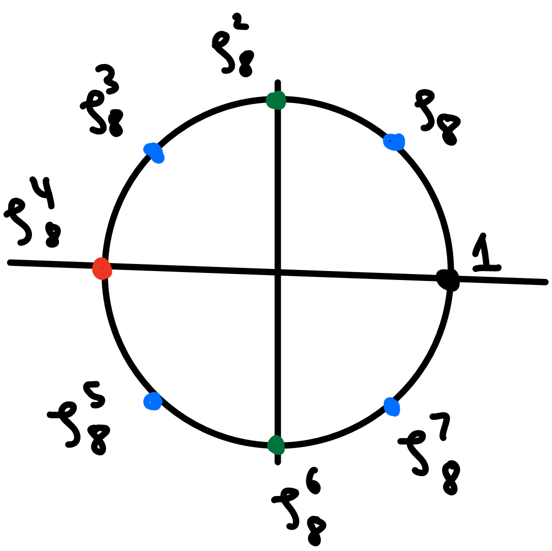
$\mathbb{Q}(\zeta_n)$ where $\zeta_n = e^{2\pi i/n}$

$$\mu_n = \left\{\begin{matrix}\text{all } n\text{th roots} \\ \text{of } 1 \text{ in } \mathbb{C}\end{matrix}\right\} = \{1, \zeta_n, \ldots, \zeta_n^{n-1}\} = \langle \zeta_n \rangle \subseteq \mathbb{Q}(\zeta_n)$$

Primitive nth root: a generator ζ of μ_n ie

$\zeta^d \neq 1$ for $d < n$.

Which ζ_n^k are primitive?



primitive...

- 1st roots of 1
- 2nd roots of 1
- 4th roots of 1
- 8th roots of 1

$$\begin{tikzcd} \mu_n \arrow[r, "\sim"', "\text{gp. isom.}"] & \mathbb{Z}/n\mathbb{Z} \end{tikzcd}$$

under mult. under +

$$\zeta_n^k \longmapsto k$$

So ζ_n^k primitive $\Leftrightarrow \gcd(k,n) = 1$

Euler φ function: $\varphi(n) = |\{0 < k < n \mid \gcd(k,n) = 1\}|$

$= |\{\text{prim. nth roots of } 1\}|$

We can compute φ:

$\varphi(p) = p-1$ $\quad$ $\varphi(ab) = \varphi(a)\varphi(b)$ if $\gcd(a,b) = 1$

p: prime

$\varphi(p^k) = p^{k-1} \cdot (p-1)$ $\quad$ Thus, $\varphi(p_1^{k_1} \cdots p_n^{k_n}) = \prod_{i=1}^{n} p_i^{k_i - 1}(p_i - 1)$

Def: The cyclotomic polynomial is

$$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \text{prim.}}} (x - \zeta) = \prod_{\substack{0 \le k < n \\ \gcd(k,n) = 1}} (x - \zeta_n^k)$$

E.g.:

$\Phi_1 = x - 1$ $\qquad$ $\Phi_4 = x^2 - 1$

$\Phi_2 = x + 1$ $\qquad$ $\Phi_5 = x^4 + x^3 + x^2 + x + 1$

$\Phi_3 = x^2 + x + 1$ $\qquad$ $\Phi_6 = x^2 - x + 1$

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta) = \prod_{d \mid n} \left(\prod_{\substack{\zeta \in \mu_d \\ \text{prim.}}} (x - \zeta) \right) = \prod_{d \mid n} \Phi_d(x)$$

Facts:

a) $\Phi_d(x) \mid x^n - 1$ if $d \mid n$ (or if $d = n$)

b) Every root ζ of unity is a root of precisely one Φ_n

c) Φ_n is monic

d) $\deg \Phi_n = \varphi(n)$

Thm: $\Phi_n(x) \in \mathbb{Z}[x]$ and is irred. (over $\mathbb{Z}$ or $\mathbb{Q}$)

Cor:

a) $m_{\zeta_n, \mathbb{Q}} = \Phi_n(x)$

b) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

Pf of Thm:

$\Phi_n \in \mathbb{Z}[x]$: Induction on n ($n=1$: clear)

Assume that $\Phi_d(x) \in \mathbb{Z}[x]$ for $d<n$

Then $x^n - 1 = f(x)\Phi_n(x)$ where $f(x) = \prod_{\substack{d \mid n \\ d<n}} \Phi_d(x)$

Divide w/ remainder in $\mathbb{Q}[x]$ since x^n-1, $f(x) \in \mathbb{Q}[x]$

$$x^n - 1 = q(x)f(x) + r(x)$$

w/ $q, r \in \mathbb{Q}[x]$, $\deg r < \deg f$

Then in $\mathbb{C}[x]$, we have

$$\Phi_n(x)f(x) = q(x)f(x) + r(x) \Rightarrow (\Phi_n(x) - q(x))f(x) = r(x)$$

$\Rightarrow r(x) = 0$ as $\deg r < \deg f$. Thus, $\Phi_n(x) = q(x) \in \mathbb{Q}[x]$, and by Gauss' Lemma since x^n-1, $f(x) \in \mathbb{Z}[x]$, $\Phi_n \in \mathbb{Z}[x]$ too.

Irreducible: Suppose not!

$\Phi_n(x) = f(x)g(x)$ $\quad$ f, g monic in $\mathbb{Z}[x]$, f irred.

Claim: Let ζ be a root of f. Then ζ^p is a root of f for any prime p coprime to n

Claim $\Rightarrow$ result: Iterating the claim, ζ^m is a root of f for any m coprime to n, so all prim nth roots of 1 are roots of $f \Rightarrow f = \Phi_n$.

Pf of claim: Suppose instead that $g(\zeta^p) = 0$.

Then ζ is a root of $g(x^p)$, so

$$g(x^p) = f(x)h(x) \quad \text{for some } h(x) \in \mathbb{Z}[x]$$

Reduce mod p: $\mathbb{Z}[x] \Rightarrow \mathbb{F}_p[x]$

1) $x^n - 1$ is sep. in $\mathbb{F}_p[x]$ as $nx^{n-1} \neq 0$,

so $\overline{\Phi}_n(x)$ has distinct roots.

2) Frob: $\mathbb{F}_p \to \mathbb{F}_p$ is the identity

$(a \in \mathbb{F}_p^\times \Rightarrow |a| \mid p-1 \Rightarrow a^{p-1} = 1 \Rightarrow a^p = a)$

"Fermat's Little Theorem"

Hence,

$$(\overline{g}(x))^p = \overline{g}(x^p) = \overline{f}(x)\overline{h}(x) \in \mathbb{F}_p[x]$$

3) This means that $\overline{g}$ and $\overline{f}$ have a common root

4) But then $\overline{\Phi}_n = \overline{g}\,\overline{f}$ has a mult. root, a contradiction

$\square$