Midterm course survey: please fill out

Prop: All irred. polys. over (a) a field of char 0; (b) a finite field are separable

Last time: Proved (a).

Pf of b): If f inseparable, $\exists g \in F[x]$ s.t. $f(x) = g(x^p)$, so

$$f(x) = g(x^p) = a_m x^{mp} + a_{m-1} x^{(m-1)p} + \cdots + a_1 x^p + a_0$$

$$= (b_m x^m)^p + (b_{m-1} x^{m-1})^p + \cdots + (b_1 x)^p + b_0^p$$

use Frobenius endomorphism

$$= \underbrace{(b_m x^m + \cdots + b_1 x + b_0)^p}_{\text{reducible! contradiction}}$$

Def: A field F is called perfect if

- char $F = 0$; or
- char $F = p$, and every elt. of F is a pth power

Cor: Every irred. poly. over a perfect field is separable

Cor (Prop 38): Let char $F = p$, $f(x) \in F[x]$ irred. $\exists!$ irred. separable poly. $f_{sep}(x) \in F[x]$, $k \geq 0$ s.t. $p(x) = p_{sep}(x^{p^k})$

Pf: If f not separable, $f(x) = f_1(x^p)$, $f_1 \in F[x]$. Then f_1 is sep. or $f_1(x) = f_2(x^p)$.

Def: The separable degree $\deg_s f(x) = \deg f_{sep}(x)$

The inseparable degree $\deg_i f(x) = p^k$

$\deg f = \deg_s f \cdot \deg_i f$

E.g.: $F = \mathbb{F}_2(t)$

a) $f(x) = x^2 - t$ $\quad f_{sep}(x) = x - t$

$\deg_s f = 1 \quad \deg_i f = 2$

b) $f(x) = x^{2^m} - t$ $\quad f_{sep}(x) = x - t$

$\deg_s f = 1 \quad \deg_i f = 2^m$

c) $(x^{p^2} - t)(x^p - t)$ is inseparable, but not irred.,

so no f_{sep}, $\deg_s$, $\deg_i$ possible

§13.6: Cyclotomic Fields

$x^n - 1$ has roots $\underbrace{e^{2\pi i/n}}_{\text{form a cyclic gp. } \mu_n \cong \underbrace{\mathbb{Z}/n\mathbb{Z}}_{\text{additive}}} \in \mathbb{C}$, $0 \leq i < n$

If $d \mid n$, $\mu_d \subseteq \mu_n$

Def: A primitive nth root of unity is a generator of μ_n i.e. elt. of μ_n but not an elt of any μ_d, $d<n$.

ζ_n : primitive nth root of 1

other primitive nth roots of 1: ζ_n^a, $\gcd(n,a)=1$

Number of prim. nth roots of 1:

$$\varphi(n) = |\{a \mid 1 \le a \le n,\ \gcd(a,n)=1\}| = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

Euler's φ function

Def: The field $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\mu_n)$ is called the cyclotomic field of nth roots of unity.

Def: The nth cyclotomic polynomial is

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

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

E.g.:

a) $\Phi_1(x) = x-1$

b) If p: prime,

$$x^p - 1 = \underbrace{(x-1)}_{\Phi_1(x)} \underbrace{(x^{p-1} + \cdots + x + 1)}_{\Phi_p(x)}$$

$\Phi_p(x)$ is irred. by §9.4 #12, so

Φ_p is min'l poly for ζ_p over $\mathbb{Q}$ and $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$

$$x^4 - 1 = \Phi_1 \Phi_2 \Phi_4 = (x-1)(x+1)\Phi_4$$

c) $\Phi_4 = x^2 + 1$

Thm 41: Φ_n is irred. monic. poly in $\mathbb{Z}[x]$ of degree $\varphi(n)$.

Pf: Monic, deg $\varphi(n)$ clear from def'n

Coeffs in $\mathbb{Z}$: Use induction. $n=1$ done.

Assume that $\Phi_d \in \mathbb{Z}[x]$ for $1 \le d < n$

Then $x^n - 1 = q(x)\Phi_n(x)$, where $q(x) = \prod_{d|n} \Phi_d(x)$

Since $x^n-1, f(x) \in \mathbb{Q}[x]$, so is $\Phi_n(x)$ by division algorithm

Consequence of Gauss' Lemma: If $f(x) = p(x)q(x)$, with f, p, q monic and $f \in \mathbb{Z}[x]$, $p, q \in \mathbb{Q}[x]$, then $p, q \in \mathbb{Z}[x]$.

So $\Phi_n(x) = \mathbb{Z}[x]$.

Irreducible: Suppose not, and let

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

Claim: If p is any prime w/ $p \nmid n$, then ζ_n^p is a root of f.

This implies that <u>every</u> prim. nth root of 1 is a root of f, so $\Phi_n = f$ is irred.

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

Then $f(x) \mid g(x^p)$, say:

$$g(x^p) = f(x)\,h(x), \qquad h(x) \in \mathbb{Z}[x]$$

Reduce mod p:

$$\underbrace{(\bar{g}(x))^p = \bar{g}(x^p)}_{\text{Frobenius}} = \bar{f}(x)\bar{h}(x) \qquad \text{in } \mathbb{F}_p[x]$$

Since $\mathbb{F}_p[x]$ is a UFD, $\bar{f}(x)$ & $\bar{g}(x)$ have common factor, so $x^n - 1$ has a multiple root over $\mathbb{F}_p$.

But,

$$\gcd(x^n-1, D(x^n-1)) = \gcd(x^n-1, \overset{\neq 0 \text{ in } \mathbb{F}_p}{n}x^{n-1}) = 1$$

Contradiction! $\square$

Remark: many proofs of irreducibility of Φ_n (see link on course website)

Cor. 42: $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

E.g.: $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \varphi(8) = 4$.

$\zeta_8 = \frac{1}{\sqrt{2}}(1+i)$, so $\zeta_8^2 = i$ and $\zeta_8 + \zeta_8^7 = \sqrt{2}$

Therefore, $\mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$

but $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$, so

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8)$$

Next time: start on Galois theory!