Announcement

Midterm 2: Wed. 3/26
7:00-8:30pm, Sidney Lu 1043

Cyclotomic polys. (cont.)

Recall: 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.:

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

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

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

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

d) Φ_n is monic

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!

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

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,

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

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

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

$\square$

Galois theory

Def: A automorphism is a field isom. $\sigma: K \to K$

E.g.: a) $K = \mathbb{C}$, $\quad \sigma: \mathbb{C} \longrightarrow \mathbb{C}$

$$z \longmapsto \bar{z}$$

$$a+bi \longmapsto a-bi$$

Check: bijection, commutes w/ $+, \cdot$

b) $K = \mathbb{Q}(\sqrt{2})$,

$$\sigma(a+b\sqrt{2}) = a - b\sqrt{2}, \quad a,b \in \mathbb{Q}$$

Note that this is induced from $\sqrt{2} \longmapsto -\sqrt{2}$ and

$$\mathbb{Q}(\sqrt{2}) \xrightarrow{\sim} \mathbb{Q}[x]/(x^2-2) \xrightarrow{\sim} \mathbb{Q}(-\sqrt{2})$$

$\mathrm{Aut}(K)$ = gp. of automs. of K
(under function composition)

E.g.: a) $\mathrm{Aut}(\mathbb{Q}) = \mathrm{id}$

b) $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{\mathrm{id}, \sqrt{2} \mapsto -\sqrt{2}\}$

c) $\mathrm{Aut}(\mathbb{C})$ is uncountable...

If K/F field extn., let

$$\mathrm{Aut}(K/F) = \{\sigma \in \mathrm{Aut}(K) \mid \underbrace{\underbrace{\sigma(a) = a}_{\text{"}\sigma\text{ fixes } a\text{"}} \ \forall a \in F}_{\text{"}\sigma\text{ fixes } F\text{"}}\}$$

Remark:

a) $\mathrm{Aut}(K/F) \leq \mathrm{Aut}(K)$

b) $\mathrm{Aut}\left(K/\text{prime subfield}\right) = \mathrm{Aut}(K)$

since every autom. fixes $\langle 1 \rangle$

E.g.: a)

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

$\mathrm{Aut}(K) = \mathrm{Aut}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma \circ \tau\}$

where

$\sigma: \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto i \end{array}$ $\quad$ $\tau: \begin{array}{l} \sqrt{2} \mapsto \sqrt{2} \\ i \mapsto -i \end{array}$

$\sigma \circ \tau: \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto -i \end{array}$

$\underbrace{a + b\sqrt{2} + ci + di\sqrt{2}}_{[K:\mathbb{Q}]=4} \mapsto \quad \cdots$

$\mathrm{Aut}(K/\mathbb{Q}(\sqrt{2})) = \langle \tau \rangle = \{1, \tau\}$

$\mathrm{Aut}(K/\mathbb{Q}(i)) = \langle \sigma \rangle$

b) $K = \mathbb{Q}(\sqrt[3]{2})$

$\mathrm{Aut}(K/\mathbb{Q}) = \{id\}$

Pf: Let $\tau \in \mathrm{Aut}(K/\mathbb{Q})$

Then

$$0 = \tau(0) = \tau(\sqrt[3]{2}^3 - 2) = \tau(\sqrt[3]{2})^3 - 2,$$

so $\tau(\sqrt[3]{2})^3$ is a root of $x^3 - 2$

i.e. it equals $\sqrt[3]{2}$

only such root in K