Lecture 9: Cyclotomic Fields

Aim Lecture: Study Galois group of important field ext^{n} arising in number theory.

Frobenius Homomorphism

Fix prime p.

Prop^{n}-Def^{n}: Let F = field char. p.

(a) $\sigma_p : F \to F : \alpha \mapsto \alpha^p$ is a field hom called the **Frobenius homomorphism**

(b) If F is finite then $\sigma_p \in Gal(F/\mathbb{F}_p)$

Proof: (a) $1^p = 1$ $(\alpha\beta)^p = \alpha^p\beta^p$ & $(\alpha+\beta)^p = \alpha^p + \binom{p}{1}\alpha^{p-1}\beta + \ldots + \beta^p = \alpha^p + \beta^p$ (the binomial coefficients $\binom{p}{1}, \ldots$ are 0)

(b) σ_p surjective $\because |F| < \infty$ & σ_p fixes $\mathbb{F}_p$ $\because \sigma_p(1) = 1$.

Cyclotomic Fields

Fix integer $m > 1$. Let $\zeta_m \in \mathbb{C}$ be a primitive m-th root of 1.

Def^{n} 1: The **cyclotomic field of mth roots of unity** is the splitting field $\mathbb{Q}(\zeta_m)$ for $x^m - 1 / \mathbb{Q}$

Rem: If field F char. 0 then $F \supseteq \mathbb{Q}$ & splitting field K for $x^m - 1 / F$ contains $\mathbb{Q}(\zeta_m)$.

Lemma: Let K = splitting field of $x^m - 1$ / field F char 0. There's an inj. group hom

$\psi: G := Gal(K/F) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$

Proof: Let $\sigma, \tau \in G$. Note σ uniquely determined by $\sigma(\zeta_m)$ which is another primitive m-th root of 1 i.e. $\zeta_m^{i(\sigma)}$ where $i(\sigma)$ is rel. prime to m.

Check $\psi(\sigma) := i(\sigma) + m\mathbb{Z}$ defines a group hom. i.e.

$\psi(\sigma\tau) \overset{??}{=} \psi(\sigma)\psi(\tau)$

$\zeta_m^{i(\sigma\tau)} = (\sigma\tau)(\zeta_m) = \sigma(\zeta_m^{i(\tau)}) = \sigma(\zeta_m)^{i(\tau)}$

$= \zeta_m^{i(\sigma)i(\tau)}$

$\Rightarrow i(\sigma\tau) \equiv i(\sigma)i(\tau) \bmod m$ □

Thm: The above hom.

$\psi: G := Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$

is an isom.

Proof: Lect. 2 Thm $\Rightarrow$ monic min poly. $f(x) \in \mathbb{Z}[x]$ for $\zeta_m/\mathbb{Q}$ has complex lin. factors $x - \zeta_m^j$ for $j + m\mathbb{Z} \in \operatorname{im}\psi$.

Since $(\mathbb{Z}/m\mathbb{Z})^*$ gen. by primes p not dividing m, suff show $x - \zeta_m^p \mid f(x)$.

Suppose not so factorising $x^m - 1 = f(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$

(by Gauss's lemma), we assume ζ_m^p is a root of $g(x)$.

$\Rightarrow$ ζ_m is a root of $g(x^p)$ so
(*) $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$.

Let $\bar{g}, \bar{f}, \bar{h}$ denote images of g, f, h under quotient map $\mathbb{Z}[x] \longrightarrow (\mathbb{Z}/p\mathbb{Z})[x]$, where $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

(*) $\Rightarrow$ for $\alpha \in F =$ splitting field of $x^m - 1 / \mathbb{F}_p$ & $\sigma_p : F \to F$ Frob. hom

$$\bar{g}(\sigma_p(\alpha)) = \bar{f}(\alpha)\bar{h}(\alpha)$$

$\therefore$ α a root of $\bar{f}$ $\Rightarrow$ $\sigma_p(\alpha)$ a root of $\bar{g}$ $\xRightarrow{\text{Prop-Def (b)}}$ α is a root of $\bar{g}$.

Hence roots of $x^m - 1 = \bar{f}(x)\bar{g}(x)$ are not distinct. But $p \nmid m$ so this contradicts the fact that

$$\frac{d}{dx}(x^m - 1) \neq 0 \quad \text{in } \mathbb{F}_p[x].$$

$\square$

Cor: The min. poly. of $\zeta_m / \mathbb{Q}$ is

$$\Phi_m(x) = \prod_{\substack{1 \le j < m \\ j, m \text{ rel. prime}}} (x - \zeta_m^j)$$

Application to Constructing Regular Polygons

Eg 1 $G = Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq \mathbb{F}_5^* \simeq \mathbb{Z}/4\mathbb{Z}$
gen. by $\sigma \in G$ corresp. to $2+5\mathbb{Z} \in \mathbb{F}_5^*$

$\therefore$

$$\zeta_5 \xmapsto{\sigma} \zeta_5^2 \xmapsto{\sigma} \zeta_5^4 \xmapsto{\sigma} \zeta_5^3 \xmapsto{\sigma} \zeta_5$$

Galois corresp. here is

$$\begin{array}{ccc} G = \langle\sigma\rangle & & \mathbb{Q} \\ \vee & & \cap \\ \langle\sigma^2\rangle & & \mathbb{Q}(\zeta_5)^{\sigma^2} = \mathbb{Q}(\zeta_5 + \sigma^2(\zeta_5)) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1}) \\ \vee & & \mathbb{Q}(2\cos 2\pi/5) \\ 1 & & \mathbb{Q}(\zeta_5) \end{array}$$

RHS is a quadratic tower $\therefore$ chain of groups on LHS double in order $\Rightarrow$

Cor: The regular pentagon is constructible.

Eg. 2. The regular 18-gon is not constructible.

Why? $\varphi(18) = \#\{1,5,7,11,13,17\} = 6$.
$= |Gal(\mathbb{Q}(\zeta_{18})/\mathbb{Q})| = [\mathbb{Q}(\zeta_{18}) : \mathbb{Q}]$

$\therefore$ Multiplicativity of degrees $\Rightarrow$
ζ_{18} cannot lie in a radical ext^n of $\mathbb{Q}$ of degree 2^n, $n \in \mathbb{N}$.

Upshot The arguments in these 2 examples shows that the regular n-gon is constructible iff $\varphi(n)$ is a power of 2!