Galois Irreducible Polynomials

Number Theory Seminar – October 5, 2018
Dalhousie University

$n :=$ positive integer
$w :=$ n-th primitive root of unity $e^{2\pi i/n}$

$\Phi_n :=$ n-th cyclotomic polynomial, $\Phi_n = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - w^k)$

In a 2017 paper, Miyeon Kwon, Ji-Eun Lee, and Ki-Suk Lee use the fundamental theorem of Galois Theory to generalize the cyclotomic polynomial.

Fundamental Theorem of Galois Theory:

E — F: Finite & Galois extension. ⟷ Gal(E/F): Automorphisms of E fixing F.

intermediate field extensions ⟷ subgroups

Basic Idea

Definition: Let H be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ and $(\mathbb{Z}/n\mathbb{Z})^\times/H = \{h_1 H, h_2 H, \dots h_\ell H\}$ be the corresponding quotient group. For each $k = 1, 2, \dots, \ell$, define $a_k = \sum_{h \in H} w^{h_k h}$. We now consider the monic polynomial having a_k as its roots, denoted by $J_{n,H}(x)$.

$$J_{n,H}(x) = (x-a_1)(x-a_2)\cdots(x-a_\ell).$$

Why is this considered a generalization of the cyclotomic polynomial?

When $H = \{1\}$ is the trivial subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, we recover

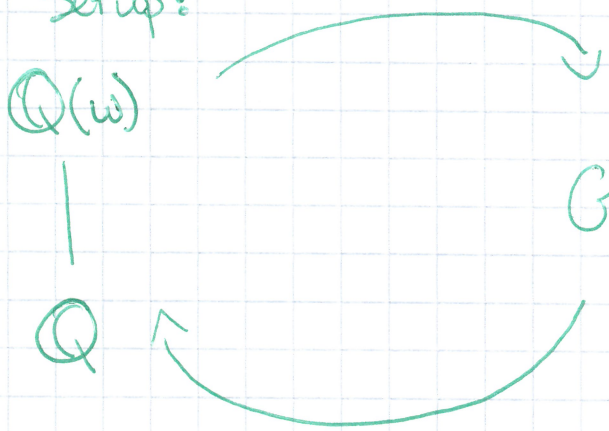
$$J_{n,\{1\}}(x) = \Phi_n(x).$$

Irreducible polynomials with integer coefficients in the form of $J_{n,H}(x)$ will be called Galois irreducible polynomials.

Results

- $J_{n,H}(x)$ is a monic polynomial with integer coefficients.
- If n is a prime number, any $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$.

The Setup:



$$Gal(\mathbb{Q}(\omega)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

$$\theta : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow Gal(\mathbb{Q}(\omega)/\mathbb{Q})$$

$$\theta[k](\omega) = \omega^k$$

$H \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$ and consider $(\mathbb{Z}/n\mathbb{Z})^\times / H$. Let $\xi = \sum_{h \in H} \omega^h$, then

$$a_1 = \sum_{h \in H} \omega^{h_1 h} = \theta[h_1](\xi)$$

$$\vdots$$

$$a_2 = \sum_{h \in H} \omega^{h_2 h} = \theta[h_2](\xi).$$

Example: $n = p = 7$

$\omega = e^{2\pi i/7}$ $\quad (\mathbb{Z}/7\mathbb{Z})^\times = \{1,2,3,4,5,6\}$

$H_1 = \{1\}$, $H_2 = \{1,6\}$, $H_3 = \{1,2,4\}$, $H_4 = \{1,2,3,4,5,6\}$

$J_{7,H_1}(x) = \Phi_n(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

$J_{7,H_4}(x) = x - 1$.

$J_{7,H_2}(x) = (x - (\omega + \omega^6))(x - (\omega^2 + \omega^5))(x - (\omega^3 + \omega^4))$
$= x^3 + x^2 - 2x - 1$.

$J_{7,H_3}(x) = (x - (\omega + \omega^2 + \omega^4))(x - (\omega^3 + \omega^5 + \omega^6))$
$= x^2 + x + 2$.

Theorem: Let H be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ and $(\mathbb{Z}/n\mathbb{Z})^\times / H = \{h_1 H, \dots, h_t H\}$. Let $a_k = \sum_{h \in H} \omega^{h h_k}$, $k = 1, \dots, t$ and $\mathbb{Q}(\omega)_H$ be the subfield of $\mathbb{Q}(\omega)$ fixed by $\{\theta[h] : h \in H\}$. Then $J_{n,H}(x) = (x - a_1) \cdots (x - a_t)$ is irreducible over $\mathbb{Q}$ if and only if $\mathbb{Q}(\xi) = \mathbb{Q}(\omega)_H$, where $\xi = \sum_{h \in H} \omega^h$.

Theorem: Let n be a square free integer. Then $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$ for any subgroup H of $(\mathbb{Z}/n\mathbb{Z})^\times$.

- $J_{n,\{-1,1\}}(x)$ is the minimal polynomial for $\cos(\frac{2\pi k}{n})$ for $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $n > 2$.

- **Theorem:** $J_{p,\{-1,1\}}(x) = U_{\frac{p-1}{2}}(\frac{x}{2}) + U_{\frac{p-1}{2}-1}(\frac{x}{2})$

Where $U_n(x)$:= nth Chebyshev polynomial of the second kind.

Cyclotomic Polynomials	Galois Irreducible Polynomial
• always irreducible	• depends on n, H
• $\prod_{d \mid n} \Phi_d(x) = x^{n-1}$ ↑ allows explicit rational fraction $\Phi_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(\frac{n}{d})}$	• not the case here.
• $\Phi_{2n}(x) = \Phi_n(-x)$	• works for $n = p^k$.
• $\Phi_{p^m r} = \Phi_{pr}(x^{p^{m-1}})$	• not the case here.
• $\rho(\Phi_n, \Phi_m) = \begin{cases} p^{\phi(m)} & \text{if } m/n \text{ is a power of prime } p \\ 1 & \text{otherwise} \end{cases}$	

• Same result but $\Phi_{m/2}$.

Studying the roots/coefficients, we have two approaches:

① Fix the subgroup size while studying $J_{n,H}(x)$.

② Fix the degree of $J_{n,H}(x)$

- Even sized subgroups lead to all real roots
- Odd sized subgroups lead to all complex roots
- If $p = 4n+1$ with n a square:

  $n \equiv 0 \pmod 2$ we have:

$$-\frac{1}{4} \pm \frac{\sqrt{p}}{4} \pm \frac{\sqrt{2p-2\sqrt{p}}}{4}$$

  $n \equiv 1 \pmod 2$ we have:

$$-\frac{1}{4} \pm \frac{\sqrt{p}}{4} \pm i\frac{\sqrt{2p+2\sqrt{p}}}{4}$$

$p = 3n+1$ with n a square is not as nice.

- Cubics have cubes in the coefficients.
- Quartics have ~~fourth~~ powers in the coefficients.
- This trend stops after fourth powers.