Cyclotomic Polynomials

Goal: Determine $F_n := m_{e^{2\pi i/n}, \mathbb{Q}}$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Defn The Euler ϕ-function $\phi: \mathbb{Z}^+ \to \mathbb{Z}^+$

$$n \longmapsto |\{i \mid 0 \le i < n, \gcd(i,n) = 1\}|$$

Note $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Lemma (a) If $\gcd(n,m) = 1$, then $\phi(nm) = \phi(n)\phi(m)$.

(b) If $n > 1$, $\phi(n) = n \prod_{\substack{p \mid n \\ \text{prime}}} (1 - \frac{1}{p})$.

Pf (a) Assume $\gcd(n,m) = 1$. Then Sun Zi's Thm implies

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

so $(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$.

(b) For p prime, $\phi(p^a) = p^a - |\{j \mid 0 \le j < p^a, p \mid j\}|$

$$= p^a - |\{pl \mid 0 \le l < p^{a-1}\}|$$

$$= p^a - p^{a-1} = p^a(1 - \tfrac{1}{p}).$$

So if $n = p_1^{a_1} \cdots p_s^{a_s}$ for p_i distinct primes, then

$$\phi(n) = \prod_{p_i \mid n} \phi(p_i^{a_i})$$

$$= n \prod_{p \mid n} (1 - \tfrac{1}{p}). \qquad \square$$

Let $\zeta = \zeta_n = e^{2\pi i/n}$. Then $x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta^i)$. Define the n-th cyclotomic polynomial $\Phi_n(x) = \prod_{\substack{0 \le i < n \\ \gcd(i,n) = 1}} (x - \zeta^i)$.

Thus $\deg \Phi_n = \phi(n)$ and roots of Φ_n = primitive nth roots of 1

e.g. $\Phi_4 = (x-i)(x+i) = x^2+1$.

$$\Phi_p = (x-\zeta_p)(x-\zeta_p^2)\cdots(x-\zeta_p^{p-1}) = \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\cdots+1.$$

Prop $\Phi_n \in \mathbb{Z}[x]$ monic of deg $\phi(n)$. Furthermore,

$$x^n-1 = \prod_{d\mid n} \Phi_d(x)$$

where the product is over positive integers d dividing n.

Pf We have $x^n-1 = \prod_{0\le i<n}(x-\zeta^i) = \prod_{d\mid n}\ \prod_{\substack{0\le i<n \\ \gcd(i,n)=d}} (x-\zeta^i)$

If $\gcd(i,n)=d$, then $i=dj$ and $n=d\frac{n}{d}$ for $\gcd(j,\frac{n}{d})=1$.

Also $0\le i<n \iff 0\le dj < d\frac{n}{d} \iff 0\le j<\frac{n}{d}$

and $\zeta_n^d = \zeta_{n/d}$, so $x-\zeta_n^i = x-\zeta_n^{dj} = x-\zeta_{n/d}^j$

Thus $\prod_{\substack{0\le i<n \\ \gcd(i,n)=d}} (x-\zeta^i) = \prod_{\substack{0\le j<\frac{n}{d} \\ \gcd(j,\frac{n}{d})=1}} (x-\zeta_{\frac{n}{d}}^j) = \Phi_{\frac{n}{d}}(x)$

so $x^n-1 = \prod_{d\mid n} \Phi_{\frac{n}{d}}(x) = \prod_{d\mid n}\Phi_d(x)$.

Now show $\Phi_n(x)\in\mathbb{Z}[x]$ by strong induction on n.

For $n=1$, $\Phi_1(x)=x-1\in\mathbb{Z}[x]$. If $n>1$,

$$x^n-1 = \Phi_n(x)\prod_{\substack{d\mid n \\ d<n}}\Phi_d(x) = \Phi_n(x)\,g(x)$$

($g(x)$: monic in $\mathbb{Z}[x]$)

By the division algorithm, $\Phi_n(x)\in\mathbb{Z}[x]$. □

Now compute $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Lemma $f\in\mathbb{Z}[x]$ monic of pos degree, p prime. If f_p is the monic polynomial whose roots are the p-th powers of the roots of f, then

$f_p \in \mathbb{Z}[x]$ and the coeffs of f, f_p are congruent mod p.

Pf Read lemma 9.1.8. (Play w/ symm polys)

Thm The cyclotomic polynomial $\Phi_n(x)$ is irred/$\mathbb{Q}$ so $\Phi_n = m_{\zeta_n, \mathbb{Q}}$ and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Pf Let $f \in \mathbb{Q}[x]$ be an irred factor of Φ_n. By Gauss's lemma, $\Phi_n = f \cdot g$ for $f, g \in \mathbb{Z}[x]$, monic.

Take p prime $\nmid n$. Step 1 $f(\zeta) = 0 \Rightarrow f(\zeta^p) = 0$.

Suppose for ζ, $f(\zeta) = 0$ but $f(\zeta^p) \neq 0$. Take f as in lemma.

Ex 7 – HW: roots of f_p are distinct prim nth roots of 1.

Thus $f_p \mid \Phi_n$. If f, f_p share a root, then $f = f_p$ ($f \mid f_p$ b/c f irred, have same degree). But this contradicts $f(\zeta^p) \neq 0$.

Thus f, f_p have no common roots so

$$\Phi_n = f f_p h \Rightarrow h \in \mathbb{Z}[x], \text{monic}.$$

Let $\bar{\ } : \mathbb{Z}[x] \to \mathbb{F}_p[x]$ reduce coeffs mod p. Since $\bar{f} = \bar{f}_p$ by the lemma, get $\bar{f}^2 \mid \bar{\Phi}_n \mid x^n - 1 \Rightarrow x^n - 1$ not separable in $\mathbb{F}_p[x]$. $\lightning$ since $p \nmid n$, completing Step 1.

Now let ζ be a fixed root of f, ζ' any prim nth root of 1.

HW: $\zeta' = \zeta_n^j$ for some $\gcd(j, n) = 1$. Let $j = p_1 \cdots p_r$ be prime factn. Note each $p_i \nmid n$. By Step 1,

$$\zeta, \zeta^{p_1}, \zeta^{p_1 p_2}, \ldots, \zeta^{p_1 \cdots p_r} = \zeta^j$$

are roots of f. Thus every prim nth root of 1 is a root of $f \Rightarrow f = \Phi_n$.

Thm $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/n\mathbb{Z})^\times$

$\sigma \longmapsto [k]$ iff $\sigma(\zeta_n) = \zeta_n^k$. $\square$