Chapter 33 Cyclotomic Extensions

Motivation

Use Galois theory to prove the result of Gauss about the construtibility of regular n-gons.

Definition Let $w_1, \ldots, w_{\phi(n)}$ be the primitive roots of unity. Then $\Phi_n(x) = (x - w_1) \cdots (x - w_{\phi(n)})$ is the nth cyclotomic polynomials over $\mathbb{Q}$.

Examples $x^6 - 1 = (x-1)(x^2+x+1)(x+1)(x^2-x+1)$.

$\Phi_1(x) = x - 1, \Phi_2(x) = x + 1, \Phi_3(x) = x^2 + x + 1, \Phi_6(x) = x^2 - x + 1$.

$x^7 - 1 = (x-1)(x^6 + \cdots + 1)$.

$x^p - 1 = (x-1)(x^p + \cdots + 1)$ for any prime p.

Basic results

Theorem 33.1 $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Proof. Partition the zeros of $x^n - 1$ into those of $\Phi_d(x)$.

[Each collection corresponds to the set of generators of the subgroup of order n/d.]

Theorem 33.2 $\Phi_n(x)$ is monic and has integer coefficients.

Proof. By induction assumption on n. The result holds for $n = 1$.

Assume that it is true for all $\Phi_d(x)$ for $d < n$.

Then $g(x) = \prod_{d|n, d<n} \Phi_d(x)$ has integer coefficients.

Now, $x^n - 1 = \Phi_n(x)g(x)$. Applying long division, we get the result. □

Remark Up to $n = 15$, the coefficients of $\Phi_n(x)$ are always in $\{1, -1\}$.

Every integer is a coefficient of some cyclotomic polynomial.

Theorem 33.3 The cyclotomic polynomials $\Phi_n(x)$ are irreducible over $\mathbb{Z}$.

Proof. Suppose $f(x)$ is a (monic) irreducible factor of $\Phi_n(x)$.

We only need to show that every zero of $\Phi_n(x)$ is a zero of $f(x)$.

It will then follow that $\Phi_n(x)|f(x)$.

Now, $\Phi_n(x)$ divides $x^n - 1$. So, $x^n - 1 = f(x)g(x)$.

Suppose w is a primitive nth root of unity that is a zero of $f(x)$.

Then $f(x)$ is a minimal polynomial for w over $\mathbb{Q}$.

For any prime p not dividing n, we have $0 = (w^p)^n - 1 = f(w^p)g(w^p)$.

If $f(w^p) \neq 0$, then $g(w^p) = 0$ so that w is a zero of $g(x^p)$.

Hence, $f(x)|g(x^p)$. Else, we get an anihilating polynomial of lower degree.

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

Let $\bar{f}(x), \bar{h}(x) \in \mathbb{Z}_p[x]$ obtained from $f(x), h(x)$ by changing the coefficients $c \in \mathbb{Z}$ to $c \in \mathbb{Z}_p$.

Then $(\bar{g}(x))^p = (\bar{g}(x^p)) = \bar{f}(x)\bar{h}(x)$.

Because $\mathbb{Z}_p[x]$ is a unique factorization domain, $\bar{f}(x), \bar{g}(x) \in \langle m(x) \rangle$ for some irreducible $m(x) \in \mathbb{Z}_p[x]$.

Thus, $\bar{g}(x) = k_1(x)m(x), \bar{f}(x) = k_2(x)m(x)$.

But then $x^n - 1 = k_1(x)k_2(x)m(x)^2 \in \mathbb{Z}_p[x]$.

So, nx^{n-1} and $x^n - 1$ are nonzero polynomials in $\mathbb{Z}_p[x]$ have a common factor of positive degree, which is impossible.

For every prime $p \not| n$, w^p is another primitive root and is a zero of $f(x)$.

If q is a prime not dividing n, then $(w^p)^q$ is a zero of $f(x)$.

Every primitive root of unity has the form $w^{p_1 \cdots p_k}$ for some primes $p_1, \ldots, p_k$ not dividing n, we get the conclusion. □

Theorem 33.4 Let $w = e^{i2\pi/n}$. Then $\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q}) = U(n)$ has $\phi(n)$ elements.

Proof. Every field automorphism that fixes $\mathbb{Q}$ will send w to w^k for some k relatively prime to n.

Every $k \in \{1, \ldots, n\}$ relatively prime to n gives rise to such a ϕ_k.

So, the mapping sending $k \in U(n)$ to ϕ_k is a group isomorphism and bijective:

$$\phi_r\phi_s(w) = w^{rs} = \phi_{rs}(w); \ \phi_r(w) \neq \phi_s(w) \text{ if } r \neq s \text{ in } U(n).$$

The result follows. □

Theorem 33.5 An n-gons is constructible by a strightedge and compass if and only if $n = 2^k p_1 \cdots p_\ell$ for ℓ distinct odd primes of the form $2^m + 1$.

Proof. Note that $\mathbb{Q}(\cos(2\pi/n)) \subseteq \mathbb{Q}(w)$ with $w = e^{i2\pi/n}$ because $\cos(2\pi/n) = (w + 1/w)/2$.

Now, $\cos(2\pi/n)$ is constructible if and only if $[\mathbb{Q}(\cos(2\pi/n)), \mathbb{Q}] = 2^m$.

We have

$$\begin{aligned}[\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q})] &= |\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q})|/|\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q}(\cos 2\pi/n))| \\ &= \phi(n)/|\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q}(\cos 2\pi/n))|.\end{aligned}$$

Now, $\sigma \in \mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q})$ implies that $\sigma(w) = w^k$.

If $\sigma \in \mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q}(\cos 2\pi/n))$, then σ fixes $\cos 2\pi/n$ so that

$\cos 2\pi/n = \phi(w + 1/w) = w^k + 1/w^k = \cos 2k\pi/n.$

This holds if and only if $k \in \{1, n-1\}$. So,

$|\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q}(\cos 2\pi/n))| = 2$ and $[\mathbb{Q}(\cos 2\pi/n) : \mathbb{Q})] = \phi(n)/2.$

Thus, if an n-gon is constructible, then $\phi(n)/2 = 2^m$.

Let $n = 2^k p_1^{n_1} \cdots p_t^{n_t}$, where $k \geq 0$ and $p_1, \ldots, p_r$ are distinct odd prime.

Then

$$|U(n)| = |U(2^k)||U(p_1^{n_1})| \cdots |U(p_t^{n_t})| = 2^{k-1} \prod_{j=1}^{t} p_j^{n_j - 1}(p_j - 1)$$

is a power of 2, i.e., $p_j = 2^{m_j} + 1$ for all j.

Conversely, suppose n has the asserted form.

Then $\mathbb{Q}(w)$ is the splitting field of some $f(x) \in \mathbb{Q}[x]$
and $\phi(n) = [\mathbb{Q}(w) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q})|$.

Since $|\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q})| = 2^m$ and the group is Abelian, we have

$$\{e\} = H_0 < \cdots < H_\ell = \mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q})$$

such that $|H_{i+1}/H_i| = 2$.

Therefore, one gets

$$\mathbb{Q} \subseteq \mathbb{Q}(\beta_1) \subseteq \mathbb{Q}(\beta_1, \beta_2) \subseteq \cdots$$

such that β_i is a zero of a quadratic polynomial in $\mathbb{Q}(\beta_1, \ldots, \beta_{i-1})[x]$.

Thus, $\cos(2\pi/n))$ is constructible. □