Cyclotomic fields

Marco Streng

November 22, 2011

Recap

Recall that a *primitive nth root of unity* in a field K is an element of K^* of order n, and that the n-th cyclotomic polynomial is defined as $\Phi_n = \prod_\zeta (X - \zeta) \in \mathbf{C}[X]$, where ζ ranges over the primitive nth roots of unity in $\mathbf{C}$. We have

$$\Phi_n = \frac{X^n - 1}{\prod_{d|n, d \neq n} \Phi_d},$$

so a long division and induction show that Φ_n is a monic polynomial in $\mathbf{Z}[X]$ for all n. Recall also that if K has a primitive nth root of unity ζ, then it has exactly $\phi(n)$ and they are ζ^k where k ranges over the integers coprime to n modulo n.

Irreducibility of Φ_n

Let $\zeta \in \mathbf{C}$ be a primitive nth root of unity and $f = f_\zeta^{\mathbf{Q}} \in \mathbf{Q}[X]$ its minimal polynomial over $\mathbf{Q}$. Then f divides Φ_n (because $\Phi_n(\zeta) = 0$), so all roots of f are of the form ζ^k with k coprime to n, It follows that $\mathbf{Q}(\zeta) \cong \mathbf{Q}[X]/(f)$ is the splitting field of f and is Galois over $\mathbf{Q}$. This also defines an injective map

$$\begin{aligned} \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) &\to (\mathbf{Z}/n\mathbf{Z})^* \\ \sigma &\mapsto k, \qquad \text{where } \sigma(\zeta) = \zeta^k. \end{aligned} \tag{1}$$

It is straightforward to check that this map is a homomorphism. The order of the domain is $\deg f$ and the order of the codomain is $\deg \Phi_n$, so the polynomial Φ_n is irreducible if and only if this map is surjective.

Theorem 1. *The homomorphism* (1) *is an isomorphism and* Φ_n *is irreducible.*

Proof. We only need to show that this injective homomorphism is surjective. Then it will follow that Φ_n is irreducible. To show surjectivity of this homomorphism, it suffices to show for every prime $p \nmid n$ that $p \mod n$ is in the image (because k is a product of such primes). In other words, it suffices to show that ζ^p is a conjugate of ζ.

Let f be the minimal polynomial of ζ and g the minimal polynomial of ζ^p. Then f and g are irreducible monic divisors of Φ_n, so by Gauss' Lemma they are in $\mathbf{Z}[X]$. Note that ζ is also a root of $g(X^p)$, so f divides $g(X^p)$. This divisibility then also holds modulo p, i.e., if $\overline{f}, \overline{g} \in \mathbf{F}_p[X]$ are the reductions of f and g modulo p, then $\overline{f}(X) \mid \overline{g}(X^p)$ in $\mathbf{F}_p[X]$. Next, note that $\mathbf{F}_p[X]$ has a (Frobenius) endomorphism $x \mapsto x^p$ (because the binomial coefficients are divisible by p) and that it restricts to the identity on the coefficients in $\mathbf{F}_p$ (by Fermat's little theorem). We find $\overline{g}(X)^p = \overline{g}(X^p)$, so $\overline{f} \mid \overline{g}^p$, and we conclude that $\overline{f}$ and $\overline{g}$ are not coprime in $\mathbf{F}_p[X]$.

Now suppose that ζ^p is not a conjugate of ζ, i.e., that f and g are distinct irreducible polynomials. Then fg divides $X^n - 1$, so $\overline{f}\overline{g}$ divides $X^n - 1 \in \mathbf{F}_p[X]$. As $\overline{f}$ and $\overline{g}$ are not coprime, the polynomial $X^n - 1 \in \mathbf{F}_p[X]$ has a square factor d^2 for $d = \gcd(\overline{f}, \overline{g})$. This implies that d is a common factor of $X^n - 1$ and its derivative $nX^{n-1} \in \mathbf{F}_p[X]$. But as n is invertible modulo p, these polynomials are coprime ($-(X^n - 1) + n^{-1}nX^{n-1} = 1$), contradiction. □

Abelian extensions of Q

The isomorphism (1) shows that $\mathbf{Q}(\zeta)/\mathbf{Q}$ is an *abelian extension*, i.e., a Galois extension with abelian Galois group.

Proposition 2. *Let L/K be an abelian extension and M an intermediate field. Then M/K is also an abelian extension.*

Proof. As the group $\mathrm{Gal}(L/K)$ is abelian, all its subgroups are normal. By the fundamental theorem of Galois theory, this implies that M/K is Galois. Its Galois group is a quotient of the abelian group $\mathrm{Gal}(L/K)$, hence is abelian as well. □

We conclude that all subfields of $\mathbf{Q}(\zeta)$ for all roots of unity ζ are abelian over $\mathbf{Q}$. The converse is the famous Kronecker-Weber theorem, but its proof uses algebraic number theory.

Theorem 3 (Kronecker-Weber theorem)**.** *Every abelian extension of $\mathbf{Q}$ is contained in $\mathbf{Q}(\zeta)$ for some root of unity ζ.*

(In)constructibility of the regular n-gon

Recall that a finite extension L/K with $\mathrm{char}(K) = 0$ is called *constructible* if and only if there exists some tower of fields $K = K_0 \subset K_1 \subset \cdots \subset K_s$ with $L \subset K_s$ and $[K_{i+1} : K_i] \in \{1, 2\}$. By the tower law, all constructible extensions have degree a power of two. A point (x, y) in the plane can be constructed from $(0, 0)$ and $(1, 0)$ if and only if $\mathbf{Q}(x, y)/\mathbf{Q}$ is a constructible extension.

Theorem 4. *Let $n > 2$ be an integer. It is possible to construct a regular n-gon from two points in the plane by ruler and compass if and only if n is of the form $2^m \prod_{i=1}^k p_i$, where the p_i are distinct* Fermat primes*, i.e., primes of the form $2^{j_i} + 1$.*

Proof. By standard ruler and compass constructions that we skip, there is no loss of generality in assuming that the two given points are $(0, 0)$ and $(1, 0)$, and that $(0, 0)$ is the centre of the n-gon and $(1, 0)$ one of its vertices. In this case, constructibility of the whole n-gon is equivalent to constructibility of just the vertex (x, y), where $x = \cos(2\pi i/n)$ and $y = \sin(2\pi i/n)$. Indeed, if we can construct (x, y), then by repeating the construction with $(1, 0)$ replaced with the previous vertex, we find all vertices.

Let $\zeta = \exp(2\pi i/n) = x + iy$. Then $x = \frac{1}{2}(\zeta + \zeta^{-1})$ and $y = \frac{1}{2i}(\zeta - \zeta^{-1})$, so we find $\mathbf{Q}(\zeta, i) = \mathbf{Q}(x, y, i)$. As this field has degree 1 or 2 over $\mathbf{Q}(x, y)$ and over $\mathbf{Q}(\zeta)$, the extension $\mathbf{Q}(x, y)/\mathbf{Q}$ is constructible if and only if $\mathbf{Q}(\zeta)/\mathbf{Q}$ is.

Write $n = 2^m \prod_{i=1}^k p_i^{m_i}$ for distinct odd primes p_i and $m_i \geq 1$. The degree of $\mathbf{Q}(\zeta)$ is $\phi(n) = 2^{m-1} \prod_{i=1}^k (p_i - 1)p_i^{m_i - 1}$. In particular, if $m_i > 1$ or $p_i - 1$ is not a power of 2, then $\phi(n)$ is not a power of 2, so $\mathbf{Q}(\zeta)$ is not constructible. This proves the "only if".

Now assume n is of the form in the theorem. Then $\mathbf{Q}(\zeta)/\mathbf{Q}$ is an abelian extension of degree a power of 2. By the structure theorem for finite abelian groups, we can find subgroups $\{\mathrm{id}\} = A_s \subset A_{s-1} \subset \cdots \subset A_1 \subset A_0 = \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ such that $[A_i : A_{i+1}] = 2$. By taking $K_i = \mathbf{Q}(\zeta)^{A_i}$, we find that $\mathbf{Q}(\zeta)/\mathbf{Q}$ is a constructible extension, so the n-gon is constructible. This proves the "if". □