

Frank Moore
Algebra 901 Notes
Professor: Tom Marley

Let n be a positive integer and let ω be a primitive n th root of unity over \mathbb{Q} . Then $\{\omega^i \mid \gcd(i, n) = 1\}$ is the set of all the primitive n th roots of unity.

Definition: The n th cyclotomic polynomial is

$$\Phi_n = \prod_i (x - \omega_i)$$

Where the product is taken over all $i \in \{0, 1, \dots, n-1\}$ such that $\gcd(i, n) = 1$. For example, we have that

1. $\Phi_1(x) = x - 1$
2. $\Phi_2(x) = x + 1$
3. $\Phi_3(x) = x^2 + x + 1$
4. $\Phi_4(x) = x^2 + 1$
5. $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$.

Remark: Note that $x^n - 1 = \prod_{d|n} \phi_d(x)$. Furthermore, $\deg \Phi_n(x) = \phi(n)$ (the Euler phi function). To see this, note that $x^n - 1 = \prod_{i=0}^{n-1} (x - \omega^i)$. Then group the factors $x - \omega^i$ according to the order of ω^i in the group of units. If ω^i has order d then $d \mid n$ and ω^i is a primitive d th root of unity. The statement about the degree is clear from the definition of the cyclotomic polynomial.

Example: Find $\Phi_9(x)$. Note that $x^9 - 1 = \Phi_1(x)\Phi_3(x)\Phi_9(x) = (x^3 - 1)(x^6 + x^3 + 1)$. Therefore, we have that $\Phi_9(x) = x^6 + x^3 + 1$.

Lemma: $\Phi_n(x) \in \mathbb{Z}[x]$.

Proof: We induce on n , with the statement being true for the cases computed above. Assume that it is true for $1 \leq d < n$. Then $x^n - 1 = f(x)\Phi_n(x)$, where $f(x) \in \mathbb{Z}[x]$ by induction (since $f(x)$ is the product of all the cyclotomic polynomials of integers that divide n). We have $x^n - 1 = f(x)\Phi_n(x)$ in $\mathbb{Q}(\omega)[x]$. But $f(x)$ is monic, and the division algorithm works in any polynomial ring $R[x]$ with R commutative as long as the leading coefficient of $f(x)$ is a unit. So, in $\mathbb{Z}[x]$, we have $x^n - 1 = f(x)q(x) + r(x)$ where $q, r \in \mathbb{Z}[x]$ and $\deg r < \deg f$. This equation also holds true in $\mathbb{Q}(\omega)[x]$. Hence $r(x) = 0$ and $q(x) = \Phi_n(x)$. Thus $\Phi_n(x) \in \mathbb{Z}[x]$.

Theorem: $\Phi_n(x)$ is irreducible for all $n \geq 1$.

Proof: Let $f(x) \in \mathbb{Q}[x]$ be an irreducible factor of $\Phi_n(x)$. By Gauss' Lemma, we may choose $f(x) \in \mathbb{Z}[x]$. We'll show that $f(x) = \Phi_n(x)$. Write $\Phi_n(x) = f(x)g(x)$, where $g(x) \in \mathbb{Z}[x]$. Let ω be a root of $f(x)$. Then ω is a primitive n th root of unity. Assuming the below claim, we inductively have that ω^i is a root of f for any $i > 0$ such that $\gcd(i, n) = 1$. Hence all the primitive n th roots of unity are roots of $f(x)$ and hence $\Phi_n(x) = f(x)$.

Claim: If p is a prime not dividing n , then ω^p is also a root of $f(x)$.

Proof of Claim: Certainly ω^p is another primitive n th root of unity, hence a root of $\Phi_n(x)$. Suppose that $f(\omega^p) \neq 0$. Then $g(\omega^p) = 0$. Therefore ω is a root of $g(x^p)$. As $f(x)$ is irreducible, and $f(\omega) = 0$, we have that $f(x) \mid g(x^p)$. So $g(x^p) = f(x)h(x)$ with $h(x) \in \mathbb{Z}[x]$. In $\mathbb{Z}_p[x]$, we get that $(\bar{g}(x))^p = \bar{g}(x^p) = \bar{f}(x)\bar{h}(x)$, since we have that $a^p = a$ for any $a \in \mathbb{Z}_p$. Therefore, $\bar{f}(x)$ and $\bar{g}(x)$ must share some common root in some algebraic closure of \mathbb{Z}_p . But since $\bar{\Phi}_n(x) = \bar{f}(x)\bar{g}(x)$, $\Phi_n(x)$ has multiple roots. Therefore $\bar{x}^n - \bar{1}$ has multiple roots. But $\gcd(\bar{x}^n - 1, n\bar{x}^{n-1}) = 1$ as $p \nmid n$, a contradiction. Therefore, ω^p is also a root of $f(x)$.

Corollary: Let ω be a primitive n th root of unity over \mathbb{Q} . Then $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$. The above extension is called a cyclotomic extension.

Definition: Let E/F be a finite extension. If $E = F(\alpha)$ for some $\alpha \in E$, then α is called a primitive element for E/F . We have a couple theorems giving criterion for when a primitive element exists.

Primitive Element Theorem I: Let E/F be a finite extension. Then $E = F(\alpha)$ for some $\alpha \in E \Leftrightarrow$ there exist only finitely many intermediate fields between E and F .

Proof: " \Leftarrow ": We break the argument into cases. If $|F| < \infty$, then $|E| < \infty$ also. Then $E^\times = \langle \alpha \rangle$ for some $\alpha \in E$. Then we immediately have that $E = F(\alpha)$. For the case when $|F| = \infty$, as E is finite, we have that $E = F(\alpha_1, \dots, \alpha_n)$. By induction, it is enough to consider the case where $n = 2$. Let $E = F(\alpha, \beta)$. Consider the set of fields $\Lambda = \{F(\alpha + c\beta) \mid c \in F\}$. Since F is infinite and by our hypothesis, there exists $c_1 \neq c_2 \in F$ such that $L = F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$. Therefore, we have that $(c_1 - c_2)\beta \in L$ and hence $\beta \in L$ and $\alpha \in L$. Thus, we have that $F(\alpha, \beta) = L = F(\alpha + c_1\beta)$.

" \Rightarrow ": Let $\Lambda = \{L \mid L \text{ is a field and } F \subset L \subset E\}$. For each $L \in \Lambda$, let $g_L = \text{Irr}(\alpha, L)$. Recall that $g_L(x) \mid g_F(x)$ since $F \subseteq L$. As g_L is monic, there are only finitely many possible g_L 's. So we have reduced the problem to the following claim:

Claim: L is uniquely determined by $g_L(x)$.

Proof of Claim: Let $g_L(x) = x^m + c_{m+1}x^{m+1} + \dots + c_1x + c_0 \in L[x]$, with $g_L(x)$ irreducible and α a root of $g_L(x)$. Note that $g_L(x) \in F(c_{m-1}, \dots, c_1, c_0)[x] \subseteq L[x]$. Certainly $g_L(x)$ is irreducible in $F(c_{m-1}, \dots, c_1, c_0)[x]$. Consider the degrees of these field extensions to E . Note that $[E : L] = [F(\alpha) : L] = \deg g_L$. Also, $[E : F(c_0, \dots, c_{m-1})] = \deg g_L$. So, we have that $L = F(c_{m-1}, \dots, c_1, c_0)[x]$, since $F(c_{m-1}, \dots, c_1, c_0)[x] \subseteq L$. Therefore, we there are only finitely many g_L 's, there are only finitely many elements in Λ , as desired.

Primitive Element Theorem II: If E/F is a finite separable extension then $E = F(\alpha)$ for some $\alpha \in E$ (and hence there are only finitely many intermediate fields between E and F by the last theorem).

Proof: By induction again, we may assume that $E = F(\alpha, \beta)$. Let $\{\sigma_1, \dots, \sigma_n\}$ be the distinct embeddings of $E \hookrightarrow \bar{F}$, which fix F . As E/F is separable, $n = [E : F]$. Also, by the previous theorem, we may assume that $|F| = \infty$, and that $[E : F] > 1$. Set

$$p(x) = \prod_{i \neq j}^n \left[(\sigma_i(\beta) - \sigma_j(\beta))x - (\sigma_j(\alpha) - \sigma_i(\alpha)) \right] \in \bar{F}[x]$$

First note that $p(x) \neq 0$ as $\sigma_i \neq \sigma_j$ and hence $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ or $\sigma_i(\beta) \neq \sigma_j(\beta)$. Since F is infinite, $\exists c \in F$ such that $p(c) \neq 0$. So,

$$0 \neq p(c) = \prod_{i \neq j}^n \left[(\sigma_i(\beta) - \sigma_j(\beta))c - (\sigma_j(\alpha) - \sigma_i(\alpha)) \right]$$

$$= \prod_{i \neq j}^n [\sigma_i(\alpha + c\beta) - \sigma(\alpha + c\beta)]$$

So, $\sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta)$ for all $i \neq j$. Then $\sigma_i|_{F(\alpha+c\beta)} : F(\alpha+c\beta) \hookrightarrow \bar{F}$ are distinct embeddings that fix F . So $[F(\alpha+c\beta) : F]_s \geq n$ and $[F(\alpha+c\beta) : F] \geq n$ implies that $F(\alpha+c\beta) = E$ as $F(\alpha+c\beta) \subseteq E$. Note that the above works for all but finitely many of the $c \in F$, namely at most $\binom{n}{2}$ of them.