Chapter 5. Cyclotomic Number Fields

4.1 Definition: For $n \in \mathbf{Z}^+$, the n^{th} **cyclotomic polynomial** is the polynomial

$$\Phi_n(x) = \prod_{k \in U_n} (x - w^k)$$

where $w = e^{i\,2\pi/n}$ and $U_n = \left\{ k \in \mathbf{Z}_n \,\middle|\, \gcd(k,n) = 1 \right\}$.

4.2 Theorem: *The cyclotomic polynomials have the following properties.*
(1) $x^n - 1 = \prod_{d|n} \Phi_d(x)$,
(2) $\Phi_n(x) \in \mathbf{Z}[x]$,
(3) $\Phi_1(0) = -1$ *and* $\Phi_n(0) = 1$ *for* $n \geq 2$,
(4) When p is prime and $k \in \mathbf{Z}^+$, $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ *and* $\Phi_{p^k}(x) = \Phi_p\left(x^{p^{k-1}}\right)$ *and hence* $\Phi_{p^k}(1) = p$.

Proof: The roots of $x^n - 1$ are the elements in the cyclic group $C_n = \left\{ w^k \middle| k \in \mathbf{Z}_n \right\}$. The subgroups of C_n are the cyclic groups $(w^k) = \left\{1, w^k, w^{2k}, \cdots, w^{n-k}\right\}$ where $k \middle| n$. Each element of C_n (that is each root of $x^n - 1$) is a generators of one of these cyclic subgroups. The roots of $\Phi_d(x)$ are the generators of the subgroup $(w^{n/d})$. This proves Part (1).

We prove Part (2) by induction on n. We have $\Phi_1(x) = x - 1 \in \mathbf{Z}[x]$. Suppose, inductively, that $\Phi_k(x) \in \mathbf{Z}[x]$ for all $k < n$. By Part (1), $x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) g(x)$ where $g(x) = \prod_{d|n, d \neq n} \Phi_d(x)$. By our induction hypothesis, $g(x) \in \mathbf{Z}[x]$. Since $x^n - 1 \in \mathbf{Z}[x]$ and $g(x) \in \mathbf{Z}[x]$ and g is monic, it follows that when we perform long division of $x^n - 1$ by $g(x)$, the quotient $\Phi_n(x)$ lies in $\mathbf{Z}[x]$. This proves Part (2).

A similar induction argument may be used to prove Part (3). We have $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$ so that $\Phi_1(0) = -1$ and $\Phi_2(0) = 1$. Suppose, inductively, that $\Phi_k(0) = 1$ for $1 < k < n$. From Part (1) we have $x^n - 1 = \Phi_n(x)\Phi_{-1}(x)h(x)$ where $h(x) = \prod_{d|n, d \neq 1, d \neq n} \Phi_d(x)$. Put in $x = 0$ to get $-1 = \Phi_n(0)(-1)(1)$ and so $\Phi_n(0) = 1$.

Let us prove Part (4). From Part (1) we know that $x^p - 1 = \Phi_p(x)\Phi_1(x) = \Phi_p(x)(x-1)$ and so

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

Similarly, $x^{p^k} - 1 = \Phi_{p^k} \prod_{d|p^{k-1}} \Phi_d(x) = \Phi_{p^k}(x)\left(x^{p^{k-1}} - 1\right)$ and so

$$\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = x^{p^{k-1}(p-1)} + \cdots + x^{p^{k-1}} + 1 = \Phi_p\left(x^{p^{k-1}}\right).$$

4.3 Theorem: *Let p be prime in $\mathbf{Z}^+$ and let $g \in \mathbf{Z}_p[x]$. Then $g(x)^p = g(x^p)$.*

Proof: Let $g(x) = \sum_{i=0}^{m} c_i x^i \in \mathbf{Z}_p[x]$. When $m = 0$, since ${c_0}^p = c_0$ (by Fermat's Little Theorem), we have $g(x)^p = {c_0}^p = c_0 = g(x^p)$. Let $m \geq 1$ and suppose, inductively, that for $h(x) = \sum_{i=0}^{m-1} c_i x^i$ we have $h(x)^p = h(x^p)$. Then

$$\begin{aligned} g(x)^p &= \big(c_0 + c_1 x + \cdots + c_m c^m\big)^p = \big(c_0 + c_1 x + \cdots + c_{m-1} x^{m-1}\big)^p + (c_m x^m)^p \\ &= \big(c_0 + c_1 x^p + c_2 x^{2p} + \cdots + c_{m-1} x^{(m-1)p}\big) + {c_m}^p x^{mp} \\ &= c_0 + c_1 x^p + c_2 x^{2p} + \cdots + c_{m-1} x^{(m-1)p} + {c_m}^{mp} = g(x^p) \end{aligned}$$

where on the first line we used the Binomial Theorem, noting that all terms are 0 mod p except the first and last, and on the second line we used the inductive hypothesis, and on the third line we used the fact that ${c_m}^p = c_m$ which follows from Fermat's Little Theorem.

4.4 Theorem: *(Gauss) Let $n \in \mathbf{Z}^+$. Then $\Phi_n(x)$ is irreducible in $\mathbf{Q}[x]$.*

Proof: Let w be a root of $\Phi_n(x)$. Let $f \in \mathbf{Q}[x]$ be the minimal polynomial of w. Note that $f \big| \Phi_n$. We shall show that $\Phi_n \big| f$ by showing that every root of Φ_n is also a root of f. Note that w is integral over $\mathbf{Z}$,since it is a root of the monic polynomial $\Phi_n \in \mathbf{Z}[x]$, and so we have $f \in \mathbf{Z}[x]$. Also since w is a root of $x^n - 1$ we have $f \big| x^n - 1$ in $\mathbf{Q}[x]$, say $x^n - 1 = f(x)g(x)$ where $g \in \mathbf{Q}[x]$. Since $x^n - 1 \in \mathbf{Z}[x]$ and $f \in \mathbf{Z}[x]$ and f is monic, when we perform long division of $x^n - 1$ by $f(x)$, the quotient $g(x)$ lies in $\mathbf{Z}[x]$. Let u be a root of f. Since $f \big| x^n - 1$, u is also a root of $x^n - 1$, and so u is an n^{th} root of 1. Let p be a prime in $\mathbf{Z}^+$ with $\gcd(p, n) = 1$. Then u^p is also an n^{th} root of 1. Since u^p is a root of $x^n - 1 = f(x)g(x)$, we know that either $f(u^p) = 0$ or $g(u^p) = 0$. Suppose, for a contradiction, that $f(u^p) \neq 0$. Then we must have $g(u^p) = 0$, so u is a root of the polynomial $h(x) = g(x^p)$. Since f is the minimal polynomial of u we have $f \big| h$, say $h = fk \in \mathbf{Q}[x]$. As above, since $h, f \in \mathbf{Z}[x]$ with f monic, we have $k \in \mathbf{Z}[x]$. Reduce the coefficients of h, f and k modulo p to get $\overline{h} = \overline{f}\,\overline{k} \in \mathbf{Z}_p[x]$. Note that $\overline{h}(x) = \overline{g}(x^p) = \overline{g}(x)^p$ from the above Lemma. Let $\overline{\ell}$ be an irreducible factor of $\overline{f}$ in $\mathbf{Z}_p[x]$. Since $\overline{\ell} \big| \overline{f}$ and $\overline{f}\,\overline{k} = \overline{h} = \overline{g}^p$, it follows that $\overline{\ell} \big| \overline{g}^p$ and hence $\overline{\ell} \big| \overline{g}$. Since $x^n - 1 = fg \in \mathbf{Z}[x]$, reducing modulo p gives $x^n - 1 = \overline{f}\,\overline{g} \in \mathbf{Z}_p[x]$. Since $\overline{\ell} \big| f$ and $\overline{\ell} \big| g$ we have $\overline{\ell}^2 \big| x^n - 1$ and hence $\overline{\ell}$ is a common divisor of $x^n - 1$ and $\frac{d}{dx}(x^n - 1)$ in $\mathbf{Z}_p[x]$. But $\frac{d}{dx}(x^n - 1) = n\,x^{n-1}$ and $\gcd(p, n) = 1$ so that n is invertible in $\mathbf{Z}_p$, and so we have $\gcd\big(x^n - 1, \frac{d}{dx}(x^n - 1)\big) = \gcd\big(x^n - 1\,,\, nx^{n-1}\big) = \gcd(-1, nx^{n-1}) = 1$. Thus we have obtained the desired contradiction and so $f(u^p) = 0$.

We have shown that if u is a root of of f and if p is a prime with $\gcd(p, n) = 1$ then u^p is also a root of f. Now let $k \in \mathbf{Z}^+$ with $\gcd(k, n) = 1$. Write $k = p_1 p_2 \cdots p_j$ where each p_i is prime and note that since $\gcd(k, n) = 1$ we have $\gcd(p_i, n) = 1$ for all indices i. Since w is a root of f, we see that each of $w\,,\, w^{p_1}\,,\, w^{p_1 p_2}\,,\, \cdots\,,\, w^{p_1 p_2 \cdots p_j} = w^k$ is also a root of f. Since w^k is a root of f for all $k \in \mathbf{Z}^+$ with $\gcd(k, n) = 1$ it follows that every root of Φ_n is also a root of f and so $\Phi_n(x) \big| f(x)$. Since $\Phi_n \big| f$ and $f \big| \Phi_n$ and f and Φ_n are monic, we have $\Phi_n = f$. Thus Φ_n is equal to the minimal polynomial of w and so Φ_n is irreducible.

4.5 Corollary: *Let w be a primitive n^{th} root of 1. Then $\mathbf{Q}(w)$ is Galois over $\mathbf{Q}$ with $[\mathbf{Q}(w):\mathbf{Q}]=\varphi(n)$, and we have $\text{Aut}_{\mathbf{Q}}\mathbf{Q}(w)\cong U_n$.*

Proof: Since the roots of $\Phi_n(x)$ are the elements w^k with $k\in U_n$, we see that all the roots of Φ_n lie in $\mathbf{Q}(w)$ so that $\mathbf{Q}(w)$ is the splitting field of $\Phi_n(x)$ over $\mathbf{Q}$ (it is also the splitting field of $f(x)=x^n-1$ over $\mathbf{Q}$). Thus $\mathbf{Q}(w)$ is Galois over $\mathbf{Q}$. Since Φ_n is the minimal polynomial of w and $\deg(\Phi_n)=\varphi(n)$, we have $\big[\mathbf{Q}(w):\mathbf{Q}\big]=\varphi(n)$. Again since the roots of Φ_n are the elements w^k with $k\in U_n$, we see that $\text{Hom}_{\mathbf{Q}}\big(\mathbf{Q}(w),\mathbf{C}\big)=\big\{\sigma_k\big|k\in U_n\big\}$ where σ_k is the homomorphism with $\sigma_k(w)=w^k$. Since $\mathbf{Q}(w)$ is Galois over $\mathbf{Q}$, we know that $\text{Aut}_{\mathbf{Q}}\mathbf{Q}(w)=\text{Hom}_{\mathbf{Q}}\big(\mathbf{Q}(w),\mathbf{C}\big)$ and so we can define a bijective map $\psi:U_n\to\text{Aut}_{\mathbf{Q}}\mathbf{Q}(w)$ by $\psi(k)=\sigma_k$. Finally, note that ψ is a homomorphism because for $k,l\in U_n$ we have $\sigma_k\sigma_l(w)=\sigma_k(w^l)=(w^l)^k=w^{kl}=\sigma_{kl}(w)$ so that $\psi(k)\psi(l)=\sigma_k\sigma_l=\sigma_{kl}=\psi(kl)$.

4.6 Corollary: *Let $n\in\mathbf{Z}^+$. Then the regular n-gon is constructible (in the ancient Greek sense) if and only if n is of the form $n=2^kp_1p_2\cdots p_l$ where $l\geq 0$ and each p_i is a Fermat prime (that is a prime p of the form $p=2^m+1$ for some $m\in\mathbf{Z}^+$).*

Proof: I may include a proof later.

4.7 Theorem: *Let $K=\mathbf{Q}(w)$ where w is a primitive n^{th} root of 1. Then $\mathcal{O}_K=\mathbf{Z}[w]$ and $\{1,w,w^2,\cdots,w^{\varphi(n)-1}\}$ is an integral basis for K, and if $n=\prod\limits_{i=1}^{\ell}{p_i}^{k_i}$ where $\ell\in\mathbf{Z}^+$, the p_i are distinct primes, and each $k_i\in\mathbf{Z}^+$, then we have*

$$d(K)=(-1)^a\prod_{i=1}^{\ell}{p_i}^{b_i}$$

where $a=\binom{\varphi(n)}{2}$ and $b_i=\varphi(n)\big(k_i-\frac{1}{p_i-1}\big)$.

Proof: I may include a proof later.