CHAPTER III

THEOREM 1: PROOF FOR CYCLOTOMIC EXTENSIONS

Cyclotomic extensions will play an important role in the proof for cyclic extensions in Chapter 4. It will be shown (proposition 4.22) that Theorem 1 holds for every subfield of a cyclotomic extension, and (proposition 4.21) that there exist cyclotomic extensions containing subfields with prescribed properties.

If ζ_n is a primitive n-th root of unity, then the conjugates of ζ_n are powers ζ_n^i for $0 < i < n$ and i relatively prime to n. The Galois group $G\big(\mathbf{Q}(\zeta_n) : \mathbf{Q}\big)$ is isomorphic to the multiplicative group $\mathbf{Z}_n^*$ (Chapter 1, cyclotomic extensions).

Lemma 3.1. *Let n be a positive rational integer and ζ_n a primitive n-th root of unity. Rational prime p is ramified in $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ only if p divides n.*

Proof. Let $\mathbf{O}$ be the ring of integers in $\mathbf{Q}(\zeta_n)$. If p is ramified in $\mathbf{Q}(\zeta_n)$ then there exists a non-trivial automorphism σ so that

$$\alpha^\sigma = \alpha (\mathrm{mod}\ \wp) \qquad \text{for } \alpha \in \mathbf{O}_\wp$$

where $\wp$ is a prime of $\mathbf{Q}(\zeta_n)$ dividing p. If $\zeta_n^\sigma = \zeta_n^\ell$, then $\zeta_n^{\ell-1} = 1 (\mathrm{mod}\ \wp)$. Since $\zeta_n^{\ell-1} \neq 1$ then $\zeta_n^{\ell-1}$ is a root of $x^{n-1} + \cdots + x + 1$. Setting $x = \zeta_n^{\ell-1}$ yields $n = 0(\mathrm{mod}\ \wp)$, so n is an element of $\wp \cap \mathbf{Z} = (p)$. Therefore p divides n.

Lemma 3.2. *If rational prime p does not divide n then p is unramified in $\mathbf{Q}(\zeta_n)$ and the action of the Artin symbol in $Q(\zeta_n)$ is*

$$\left(\frac{\mathbf{Q}(\zeta_n) : \mathbf{Q}}{p}\right) \zeta_n = \zeta_n^p.$$

Proof. The Artin symbol raises ζ_n to some power ζ_n^a, where $0 < a < n$, a is relatively prime to n, and $\zeta_n^a = \zeta_n^p (\mathrm{mod}\ \wp)$, where $\wp$ is a prime of $Q(\zeta_n)$ dividing p. Suppose that $a \neq p (\mathrm{mod}\ n)$. Then $\zeta_n^{p-a} = 1 (\mathrm{mod}\ \wp)$ and $\zeta_n^{p-a} \neq 1$, so ζ_n^{p-a} is a root of $x^{n-1} + \cdots + x + 1$. Setting $x = \zeta_n^{p-a}$ yields $n = 0(\mathrm{mod}\ \wp)$, so $(p) = \wp \cap \mathbf{Z}$ divides n. That is impossible, so $a = p(\mathrm{mod}\ n)$.

LEMMA 3.3. *Let* $\mathbf{k}$ *be a finite extension of* $\mathbf{Q}$. *Let* $\wp$ *be a prime of* $\mathbf{k}$ *that divides rational prime* p, *and* p *does not divide* n. *Prime* $\wp$ *is not ramified in* $\mathbf{k}(\zeta_n)$, *and the action of the Artin symbol for* $\wp$ *is*

$$\left(\frac{\mathbf{k}(\zeta_n) : \mathbf{k}}{\wp}\right) \zeta_n = \zeta_n^{\mathrm{N}\wp}.$$

PROOF. By lemma 2.16, $\wp$ is not ramified in $\mathbf{k}(\zeta_n)$, and the Artin symbol for $\wp$ raises ζ_n to the power of p^f where f is the degree of p in extension $\mathbf{k}/\mathbf{Q}$, *i.e.*, to the power $\mathrm{N}\wp$.

LEMMA 3.4. *Let* $\mathbf{k}$ *be a finite extension of* $\mathbf{Q}$. *Let* α *be an element of* $\mathbf{k}^*$. *Then*

$$\prod_{\wp | \alpha} \mathrm{N}\wp^{a_\wp} = \left|\mathbf{N}_{\mathbf{k}/\mathbf{Q}}\alpha\right| \qquad \textit{where } |\alpha|_\wp = \mathrm{N}\wp^{-a_\wp}.$$

PROOF. Principal fractional ideal $(\mathbf{N}_{\mathbf{k}/\mathbf{Q}}\alpha)$ is the norm $\mathbf{N}_{\mathbf{k}/\mathbf{Q}}(\alpha)$ of principal fractional ideal (α) (chapter 1, norm and trace functions). Let the prime factorization of (α) into primes of $\mathbf{k}$ be $(\alpha) = \prod_\wp \wp^{a_\wp}$. Note that $\mathbf{N}_{\mathbf{k}/\mathbf{Q}}\wp = (p)^f = (p^f) = (\mathrm{N}\wp)$. Then

$$\mathbf{N}_{\mathbf{k}/\mathbf{Q}}(\alpha) = \prod_{\wp|\alpha} \mathbf{N}_{\mathbf{k}/\mathbf{Q}}\wp^{a_\wp} = \prod_{\wp|\alpha} (\mathrm{N}\wp)^{a_\wp} = \left(\prod_{\wp|\alpha} \mathrm{N}\wp^{a_\wp}\right).$$

Therefore $\prod_{\wp|\alpha} \mathrm{N}\wp^{a_\wp}$ and $\mathbf{N}_{\mathbf{k}/\mathbf{Q}}\alpha$ generate the same fractional ideal of $\mathbf{Q}$.

REMARK. In proposition 3.5, primes of $\mathbf{k}$ will be denoted by $\wp$ and rational primes by p.

PROPOSITION 3.5. *Let* $\mathbf{k}$ *be a finite extension of* $\mathbf{Q}$, *and let* $\mathbf{K} = \mathbf{k}(\zeta_n)$ *be a cyclotomic extension of* $\mathbf{k}$. *Let* E *contain all infinite primes of* $\mathbf{k}$ *and all finite primes which are ramified in* $\mathbf{K}$. *For* γ *of* $\mathbf{k}^*$, *define*

$$\psi(\gamma) = \prod_{\wp \notin E} \left(\frac{\mathbf{K} : \mathbf{k}}{\wp}\right)^{c_\wp}, \quad \textit{where } |\gamma|_\wp = (\mathrm{N}\wp)^{-c_\wp}.$$

Let the factorization of n *into rational primes be* $n = \prod p^{n_p}$. *For each prime* p *dividing* n, *we have* $(p) = \prod \wp^{e_\wp}$ *in* $\mathbf{o}$. *Set* $m_\wp = e_\wp n_p$. *For real infinite primes of* $\mathbf{k}$, *set* $m_\wp = 1$. *If* $\gamma \in W_\wp(m_\wp)$ *for* $\wp \in E$ *then* $\psi(\gamma) = 1$.

Proof. Let us first show that the conclusion holds for an element α in $\mathbf{o}^*$. Suppose α is in $W_\wp(m_\wp)$ for $\wp$ in E. Then $\wp$ divides (α) only if $\wp$ is not in E. Using lemma 3.3 and lemma 3.1, if $|\alpha|_\wp = \mathrm{N}\wp^{-c_\wp}$ then

$$\psi(\alpha)\zeta_n = \prod_{\wp \notin E} \left(\frac{\mathbf{K}:\mathbf{k}}{\wp}\right)^{c_\wp} \zeta_n = \zeta_n^{\prod_{\wp\notin E} \mathrm{N}\wp^{c_\wp}} = \zeta_n^{\prod_{\wp|\alpha} \mathrm{N}\wp^{c_\wp}}.$$

Applying lemma 3.4, we have

$$\psi(\alpha)\zeta_n = \zeta_n^{|\mathbf{N}_{\mathbf{k}/\mathbf{Q}}\alpha|}.$$

Since the norm is the product of local norms, at $p = p_\infty$ we have

$$\mathbf{N}_{\mathbf{k}/\mathbf{Q}}\alpha = \prod_{\wp|p_\infty} \mathbf{N}_{\mathbf{k}_\wp/\mathbf{Q}_{p_\infty}}\alpha.$$

Since we have chosen $m_\wp = 1$ at all real infinite primes, every local norm in the above product is positive. Therefore $\mathbf{N}_{\mathbf{k}/\mathbf{Q}}\alpha > 0$, so we have

$$\psi(\alpha)\zeta_n = \zeta_n^{\mathbf{N}_{\mathbf{k}/\mathbf{Q}}\alpha}.$$

If $\wp$ is a finite prime in E and α is in $W_\wp(e_\wp n_p)$, then $(\alpha - 1) = \wp^{e_\wp n_p} = (p)^{n_p}$, so $\alpha = 1 + p^{n_p}\alpha'$ for α' in $\mathbf{o}_\wp$. We therefore have $\mathbf{N}_{\mathbf{k}/\mathbf{Q}}\alpha = 1(\mathrm{mod}\ p^{n_p})$. This holds for every rational prime dividing n, so $\mathbf{N}_{\mathbf{k}/\mathbf{Q}}\alpha = 1(\mathrm{mod}\ n)$. We conclude that $\psi(\alpha)\zeta_n = \zeta_n$, so $\psi(\alpha) = 1$.

For the general case, suppose that γ is in $\mathbf{k}^*$ and in $W\wp(m_\wp)$ for $\wp$ in E. If we can find a positive rational integer b so that b is in $W_\wp(m_\wp)$ for $\wp$ in E and γb is in $\mathbf{o}^*$, then $\alpha = \gamma b$ is also in $W\wp(m_\wp)$ for $\wp$ in E. We have already shown $\psi(\alpha) = 1$, and the same argument applies to b, so $\psi(b) = 1$. Therefore $\psi(\gamma) = \psi(\alpha)\psi(b)^{-1} = 1$.

To find b, we will have γb in $\mathbf{o}^*$ if b is divisible by sufficiently high powers of rational primes p that are divisible by the primes $\wp$ which occur to negative powers in the factorization of (α) in $\mathbf{o}$. (None of those $\wp$ are in E.) In addition, b will be in $W_\wp(m_\wp)$ for the finite primes in E if $b - 1$ divisible by sufficiently high powers of primes p that are divisible by finite primes in E. By lemma 2.2, there exists a rational integer satisfying the congruences. Let b be a positive solution by adding a large multiple of all the prime powers occurring in the congruences. Then b is in $W_\wp(m_\wp)$ for all primes of E.

Remark. We return to the usual notation: $\wp$ and p denote primes of $\mathbf{K}$ and $\mathbf{k}$, respectively.

PROPOSITION 3.6. *Let* $\mathbf{k}$ *be a finite extension of* $\mathbf{Q}$*, and let* $\mathbf{K} = \mathbf{k}(\zeta_n)$ *be a cyclotomic extension of* $\mathbf{k}$*. Homomorphism* $\phi_{\mathbf{K}/\mathbf{k}}$ *of (2.1) can be extended to a continuous homomorphism of* $\mathbf{I_k}$ *to* $G[\mathbf{K}:\mathbf{k}]$ *whose kernel contains* $\mathbf{k}^*$*.*

PROOF. Let E consist of all infinite primes of $\mathbf{k}$ and all finite primes that are ramified in $\mathbf{K}$. Choose integers m_p for p in E so that the conditions of proposition 3.5 are satisfied. ϕ_K is defined on $\mathbf{I_k}\{E\}$ by (2.1). Let $\mathbf{i}$ be any idele in $\mathbf{I_k}$. By lemma 2.5, and using the notation of remark 2.2, we can choose α in $\mathbf{k}^*$ so that $\alpha\mathbf{i}$ is in $W_p(m_p)$ for p in E. Define $\phi_{\mathbf{K}/\mathbf{k}}$ by

$$\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i}) = \prod_{p\notin E} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{a_p} \qquad \text{where } |\alpha\,\mathbf{i}|_p = \mathrm{N}p^{-a_p}. \tag{3.1}$$

The kernel contains $\mathbf{k}^*$, because if $\mathbf{i}$ is in $\mathbf{k}^*$ then choose $\alpha = \mathbf{i}^{-1}$. The definition agrees with (2.1) when $\mathbf{i}$ is in $\mathbf{I_k}\{E\}$ because we can take $\alpha = 1$.

We must show that the above definition of $\phi_{\mathbf{K}}$ does not depend on the choice of α. Suppose that β also satisfies $\beta\mathbf{i} \in W_p(m_p)$ for p in E. Then $\alpha\mathbf{i} = \gamma(\beta\mathbf{i})$ where $\gamma = (\alpha\mathbf{i})(\beta\mathbf{i})^{-1}$, so γ is an element of $\mathbf{k}^*$ and is in $W_p(m_p)$ for p in E. Let $|\beta\mathbf{i}|_p = \mathrm{N}p^{-b_p}$ and $|\gamma|_p = \mathrm{N}p^{-c_p}$ for p in E. By proposition 3.5, $\psi(\gamma) = 1$, so

$$\begin{aligned}\prod_{p\notin E} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{a_p} = \prod_{p\notin E} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{b_p+c_p} &= \prod_{p\notin E} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{b_p} \prod_{p\notin E} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{c_p} \\ &= \prod_{p\notin E} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{b_p},\end{aligned}$$

showing that β and α produce the same value of $\phi_{\mathbf{K}}(\mathbf{i})$.

REMARK. When the base field $\mathbf{k}$ is the rational number field $\mathbf{Q}$ and $\mathbf{K} = \mathbf{Q}(\zeta_n)$, the set E consists of primes dividing n and the real infinite prime p_∞. The integers $m_\wp$ become simply $m_p = n_p$ for finite primes in E and $m_{p_\infty} = 1$. The definition of $\phi_{\mathbf{K}/\mathbf{Q}}$ is as follows. If $\mathbf{i}$ is any idele in $\mathbf{I_Q}$, choose α in $\mathbf{Q}^*$ so that $\alpha\mathbf{i}$ is in $W_p(n_p)$ for p in E. Let $\mathbf{n}$ be the modulus $(n)p_\infty$. Then

$$\phi_{\mathbf{K}/\mathbf{Q}}(\mathbf{i}) = \prod_{p\nmid\mathbf{n}} \left(\frac{\mathbf{K}:\mathbf{Q}}{p}\right)^{a_p} \qquad \text{where } |\alpha\,\mathbf{i}|_p = p^{-a_p}. \tag{3.2}$$

This will be of use in the proof of Kronecker's theorem (chapter 9).