CHAPTER II

FUNDAMENTAL THEOREMS

Let $\mathbf{k}$ be a finite extension of the rational number field $\mathbf{Q}$. $\mathbf{K}$ is an abelian extension of $\mathbf{k}$ if $\mathbf{K}/\mathbf{k}$ is a finite normal extension and the Galois group $G(\mathbf{K}:\mathbf{k})$ is abelian. If p is a finite prime of $\mathbf{k}$ that is not ramified in $\mathbf{K}$ then the Artin symbol $\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)$ is defined by (1.7). Let E be a finite set of primes of $\mathbf{k}$ containing all infinite primes and all primes that ramify in $\mathbf{K}$. Let $\mathbf{I}_{\mathbf{k}}\{E\}$ be the subgroup of idele group $\mathbf{I}_{\mathbf{k}}$ defined by

$$\mathbf{I}_{\mathbf{k}}\{E\} = \left\{\mathbf{i} \in \mathbf{I}_{\mathbf{k}} \;\middle|\; \mathbf{i}_p = 1 \text{ for } p \in E\right\}.$$

Define $\phi_{\mathbf{K}/\mathbf{k}} : \mathbf{I}_{\mathbf{k}}\{E\} \to G(\mathbf{K}:\mathbf{k})$ by

$$\text{(2.1)} \qquad \phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i}) = \prod_{p \notin E} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{n_p} \qquad \text{where } |\mathbf{i}|_p = (\mathrm{N}p)^{-n_p} \text{ for } p \notin E.$$

The homomorphism $\mathbf{N}_{\mathbf{K}/\mathbf{k}} : \mathbf{I}_{\mathbf{K}} \to \mathbf{I}_{\mathbf{k}}$ of idele groups is defined by

$$\left(\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{i}\right)_p = \prod_{\wp | p} \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{i}_p \qquad \text{for } \mathbf{i} \in \mathbf{I}_{\mathbf{K}}.$$

THEOREM 1. *Homomorphism (2.1) can be extended in a unique way to a continuous homomorphism $\phi_{\mathbf{K}/\mathbf{k}}$ of $\mathbf{I}_{\mathbf{k}}$ onto $G(\mathbf{K}:\mathbf{k})$ whose kernel contains $\mathbf{k}^*$. The extension is independent of E, the image is all of $G(\mathbf{K}:\mathbf{k})$, and the kernel consists exactly of the subgroup $\mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{k}}$.*

THEOREM 2. *The abelian extension $\mathbf{K}$ of $\mathbf{k}$ is uniquely determined by the kernel of $\phi_{\mathbf{K}/\mathbf{k}}$. If H is a closed subgroup of finite index in $\mathbf{I}_{\mathbf{k}}$ and contains $\mathbf{k}^*$ then there is a unique abelian extension $\mathbf{K}$ of $\mathbf{k}$ such that H is the kernel of $\phi_{\mathbf{K}/\mathbf{k}}$.*

REMARK. Theorems 1 and 2 are the fundamental theorems of class field theory. The proof of Theorem 1 is the subject of this chapter through chapter 8. Theorem 2 is proved in chapter 12. In this chapter, we develop basic properties of the fundamental homomorphism $\phi_{\mathbf{K}/\mathbf{k}}$.

Lemma 2.1. *A closed subgroup of finite index in $\mathbf{I_k}$ contains a subgroup of the form*

$$\prod_{p\notin E'} \mathbf{u}_p \times \prod_{\text{finite } p\in E'} W'_p(\epsilon_p) \times \prod_{\text{real } p} \mathbf{k}_p^+ \times \prod_{\text{complex } p} \mathbf{k}_p^*,$$

where E' is a finite set of finite primes, the ϵ_p are real numbers satisfying $\epsilon_p \le 1$ for $p \in E'$, sets $\mathbf{u}_p$ and $W'_p(\epsilon_p)$ are defined by

$$\mathbf{u}_p = \left\{\alpha \in \mathbf{k}_p^* \;\middle|\; |\alpha|_p = 1\right\} \quad W'_p(\epsilon_p) = \left\{\alpha \in \mathbf{k}_p^* \;\middle|\; |\alpha - 1|_p < \epsilon_p\right\},$$

and $\mathbf{k}_p^+ \simeq \left\{x \in \mathbf{R}^* \;\middle|\; x > 0\right\}$ for p infinite real.

Proof. A closed subgroup H of finite index must be open, so there is a basic neighborhood $U(E', \{\epsilon'_p\})$ of the identity of $\mathbf{I_k}$ contained in H. Take $\epsilon_p = \min(\epsilon'_p, 1)$ for finite p and $\epsilon_p = \min\left(\epsilon'_p, \frac{1}{2}\right)$ for infinite p. Then

$$U(E', \{\epsilon'_p\}) = \prod_{p\notin E'} \mathbf{u}_p \quad \times \prod_{\text{finite } p\in E'} W'_p(\epsilon'_p) \quad \times \prod_{\text{infinite } p\in E'} W'_p(\epsilon'_p).$$

H contains the subgroup generated by $U(E', \{\epsilon'_p\})$ which is the subgroup claimed by the lemma.

Lemma 2.2 (Chinese Remainder Theorem). *Let a_1 and a_2 be non-zero ideals of $\mathbf{o}$ and let α_1 and α_2 be integers of $\mathbf{o}$. There exists α in $\mathbf{o}$ so that $\alpha - \alpha_1 \in a_1$ and $\alpha - \alpha_2 \in a_2$ if and only if $\alpha_1 - \alpha_2 \in a_1 + a_2$.*

Proof. Remark: $a_1 + a_2$ is the greatest common divisor of a_1 and a_2. Put $a = a_1 + a_2$. a is invertible, and a divides both a_1 and a_2. Suppose that $\alpha_1 - \alpha_2 \in a$. $a_1 a^{-1} + a_2 a^{-1} = \mathbf{o}$, so there exist integers $\beta_1 \in a_1 a^{-1}$ and $\beta_2 \in a_2 a^{-1}$ so that $\beta_1 + \beta_2 = 1$. Put $\alpha = \beta_1 \alpha_2 + \beta_2 \alpha_1$. Then

$$\alpha - \alpha_1 = \beta_1(\alpha_2 - \alpha_1) \in a_1$$
$$\alpha - \alpha_2 = \beta_2(\alpha_1 - \alpha_2) \in a_2$$

Conversely if $\alpha - \alpha_1 \in a_1$ and $\alpha - \alpha_2 \in a_2$ then $\alpha_1 - \alpha_2 \in a_1 + a_2$.

Corollary. *Let $p_1, \ldots, p_k$ be distinct non-trivial prime ideals of $\mathbf{o}$ and let $n_1, \ldots, n_k$ be rational integers greater than or equal to zero. Let $\alpha_1, \ldots, \alpha_k$ be elements of $\mathbf{o}$. There exists an element α of $\mathbf{o}$ so that $\alpha - \alpha_1 \in p_1^{n_1}, \ldots, \alpha - \alpha_k \in p_k^{n_k}$.*

Proof. Since ideals have unique factorization then the greatest common divisor $p_1^{n_1} \ldots p_{k-1}^{n_{k-1}} + p_k^{n_k}$ is $\mathbf{o}$. Use lemma 2.2 and induction.

Lemma 2.3. *Let* $\alpha_1, \dots, \alpha_n$ *be a basis for* $\mathbf{k}$ *over* $\mathbf{Q}$*. Let* $\mathbf{k}$ *have* r_1 *real and* r_2 *complex infinite primes, and let the distinct isomorphisms of* $\mathbf{k}$ *into* $\mathbf{R}$ *or* $\mathbf{C}$ *be* $\sigma_1, \dots, \sigma_n$*, where* $\sigma_1, \dots, \sigma_{r_1}$ *are the* r_1 *isomorphisms into* $\mathbf{R}$ *and* $\sigma_{r_1+1}, \dots, \sigma_n$ *are the* $2r_2$ *isomorphisms into* $\mathbf{C}$*, Then* $\det \|\alpha_i^{\sigma_j}\|$ *is not zero.*

Proof. It is enough to show that the determinant is not zero for some basis. Let α generate $\mathbf{k}$ over $\mathbf{Q}$. Then $1, \alpha, \dots, \alpha^{n-1}$ is a basis. The elements $\alpha^{\sigma_1} \dots \alpha^{\sigma_n}$ are distinct, so $\| (\alpha^{\sigma_j})^{i-1} \|$ is a non-singular Vandermonde matrix.

Lemma 2.4 Approximation theorem. *Let* E' *be a finite set of primes and for each prime* p *in* E' *an element* α_p *in* $\mathbf{k}_p$ *and a positive real number* ϵ_p *are given. Then there is an* α *in* $\mathbf{k}$ *so that* $|\alpha - \alpha_p|_p < \epsilon_p$ *for all* p *in* E'*.*

Proof. There exists a non-zero β in $\mathbf{o}$ so that $\beta\alpha_p \in \mathbf{o}_p$ for all finite $p \in E'$. By the corollary to lemma 2.2, there is an $\alpha' \in \mathbf{k}$ satisfying the conditions $\alpha' - \beta\alpha_p \in p^{m_p}$ for all finite p in E'. By taking m_p sufficiently large we have $|\alpha' - \beta\alpha_p|_p < |\beta|_p \epsilon_p$, or $|\beta^{-1}\alpha' - \alpha_p|_p < \epsilon_p$ for the finite primes p in E'. Put $\alpha'' = \beta^{-1}\alpha'$. Let a be an ideal in $\mathbf{o}$ so that if $\gamma \in a$ then $|\gamma|_p < \epsilon_p$ for the finite primes p in E'. Take a very large rational integer m which is not divisible by any of the finite primes in E', *i.e.,* $|m|_p = 1$ for finite p in E'. Then

$$|m\alpha'' - \gamma - m\alpha_p|_p \le \max\left(|\gamma|_p, |m(\alpha'' - \alpha_p)|_p\right) < \epsilon_p \text{ for finite } p \text{ in } E' \text{ and } \gamma \in a.$$

Therefore
$$\left|\alpha'' - \frac{\gamma}{m} - \alpha_p\right|_p \le \epsilon_p \text{ for finite } p \in E' \text{ and } \gamma \in a,$$

so $\alpha = \alpha'' - \gamma/m$ satisfies our condition for the finite primes in E'. We must show how to choose γ and m so that α also satisfies the required condition for infinite primes in E'. We claim that there is a positive constant M depending only on ideal a, an element $\gamma = \gamma_0$ in a, and an element η in $\mathbf{k}^*$ so that,

$$(2) \qquad |(\alpha'' m - \alpha_p m) - (\gamma_0 + \eta)|_p < \frac{\epsilon_p}{2} \quad \text{and} \quad |\eta|_p < M \text{ for all infinite } p \text{ in } E'.$$

Then

$$\left|(\alpha'' - \alpha_p) - \frac{\gamma_0}{m}\right|_p < \frac{\epsilon_p}{2m} + \frac{|\eta|_p}{m} \le \frac{\epsilon_p}{2m} + \frac{M}{m} \quad \text{for all infinite } p \text{ in } E'.$$

If integer m is chosen large enough so that $\frac{M}{m} < \frac{1}{2}\epsilon$, then

$$\left|\alpha'' - \frac{\gamma_0}{m} - \alpha_p\right|_p < \epsilon_p \quad \text{for all infinite } p \in E'$$

It remains to establish the claim about M and to choose γ_0 and η. It is possible to choose a basis $\alpha_1, \ldots, \alpha_n$ for $\mathbf{k}$ over $\mathbf{Q}$ so that each basis element α_i belongs to ideal a. If $\sigma_1, \ldots, \sigma_n$ are the distinct isomorphisms of $\mathbf{k}$ into $\mathbf{R}$ or $\mathbf{C}$, then by lemma 2.3 the mapping

$$k \xrightarrow{\sigma_1 \oplus \cdots \oplus \sigma_n} \mathbf{R}^{r_1} \oplus \mathbf{C}^{r_2}$$

takes $\alpha_1\mathbf{Z} + \cdots + \alpha_n\mathbf{Z}$ to a non-degenerate n-dimensional lattice. Any element in $\mathbf{R}^{r_1} \oplus \mathbf{C}^{r_2}$ can be closely approximated by an element $u_1\alpha_1 + \cdots + u_n\alpha_n$ where the u_i are elements of $\mathbf{Q}$. Write $u_i = k_i + v_i$ where k_i is in $\mathbf{Z}$ and $0 \leq v_i < 1$. Choose $\gamma_0 = k_1\alpha_1 + \cdots + k_n\alpha_n$ and $\eta = v_1\alpha_1 + \cdots + v_n\alpha_n$. Then $\gamma_0 \in a$ and the $|\eta|_{\sigma_i}$, for $i = 1, \ldots, n$, are all bounded by a constant M that depends only on the basis, so condition (2) is satisfied. This completes the proof of the lemma.

Lemma 2.5. *Let E' be a finite set of primes and for each prime p in E' an element α_p in $\mathbf{k}_p^*$ and a positive real number ϵ_p are given. Then there is an α in $\mathbf{k^*}$ so that $\left|\alpha\alpha_p^{-1} - 1\right|_p < \epsilon_p$ and $\left|\alpha^{-1}\alpha_p - 1\right|_p < \epsilon_p$.*

Proof. Put $\epsilon'_p = \min(1, \epsilon_p)$ for finite p in E', and put $\epsilon'_p = \min\left(\frac{1}{2}, \frac{1}{2}\epsilon_p\right)$ for infinite p in E'. By lemma 2.4 there is an α in $\mathbf{k}$ so that $|\alpha - \alpha_p|_p < |\alpha_p|_p\epsilon'_p$ for all p in E'. Therefore $|\alpha\alpha_p^{-1} - 1|_p < \epsilon'_p$ for all p in E'. A simple calculation shows that $|\alpha^{-1}\alpha_p - 1|_p < \epsilon_p$ for both finite p and infinite p in E'.

Proposition 2.6. *Let E be a finite set of primes of $\mathbf{k}$. Let ϕ_1 and ϕ_2 be two homomorphisms of $\mathbf{I_k}$ into a finite group G with closed kernels that contain $\mathbf{k}^*$. If ϕ_1 and ϕ_2 agree on $\mathbf{I_K}\{E\}$ then $\phi_1 = \phi_2$ on all of $\mathbf{I_k}$.*

Proof. Put $H = \ker(\phi_1) \cap \ker(\phi_2)$; H is a closed subgroup of finite index in G. By lemma 2.1, H contains a closed subgroup U, where

$$U = \prod_{p \notin E'} \mathbf{u}_p \quad \times \prod_{\text{finite } p \in E'} W'_p(\epsilon'_p) \quad \times \prod_{\text{real } p \in E'} \mathbf{k}_p^+ \quad \times \prod_{\text{complex } p \in E'} \mathbf{k}_p^*$$

Take $\mathbf{i}$ in $\mathbf{I_k}$. For infinite p take $\epsilon'_p = \frac{1}{2}$. By lemma 2.5, there exists α in $\mathbf{k}^*$ so that $\left|\alpha^{-1}\mathbf{i}_p - 1\right|_p < \epsilon'_p$ for all p in E'. Define $\mathbf{j}$ and $\mathbf{j}'$ in $\mathbf{I_k}$ as follows, so that $\mathbf{j}$ is in U, and $\mathbf{j}'$ is in $\mathbf{I_k}\{E\}$.

$$\begin{aligned} \mathbf{j}_p &= 1 \quad\quad\ \text{for } p \notin E \qquad & \mathbf{j}_p &= \alpha^{-1}\mathbf{i}_p \text{ for } p \in E \\ \mathbf{j}'_p &= \alpha^{-1}\mathbf{i}_p \text{ for } p \notin E \qquad & \mathbf{j}'_p &= 1 \quad\quad\ \text{for } p \in E \end{aligned}$$

(If p is in E but not E' then $\mathbf{j}_p = 1$, so $\mathbf{j}$ is in U.) Since the kernels of ϕ_1 and ϕ_2 contain $\mathbf{k}^*$, we have

$$\phi_1(\mathbf{i}) = \phi_1(\alpha^{-1}\mathbf{i}) = \phi_1(\mathbf{j}\,\mathbf{j}') = \phi_1(\mathbf{j}') = \phi_2(\mathbf{j}') = \phi_2(\mathbf{j}\,\mathbf{j}') = \phi_2(\alpha^{-1}\mathbf{i}) = \phi_2(\mathbf{i}).$$

Proposition 2.7. *If ϕ is a homomorphism from $\mathbf{I_k}\{E\}$ to a finite group and the kernel of ϕ has closed kernel of finite index, then any extension of ϕ to $\mathbf{I_k}$ whose kernel contains $\mathbf{k}^*$ is independent of E.*

Proof. Suppose that ϕ_1 defined on $\mathbf{I_K}\{E_1\}$ and ϕ_2 defined on $\mathbf{I_k}\{E_2\}$ can be extended to $\mathbf{I_k}$ with kernels containing $\mathbf{k}^*$. Then ϕ_1 and ϕ_2 agree on $\mathbf{I_k}\{E_1 \cap E_2\}$. Therefore $\phi_1 = \phi_2$ by Proposition 2.6.

Composite fields of finite extensions. Let Ω be an algebraic closure of $\mathbf{k}$. All of our extensions of $\mathbf{k}$ will be subfields of Ω. If $\mathbf{K}_1$ and $\mathbf{K}_2$ are subfields of Ω then the *composite field* $\mathbf{K}_1\mathbf{K}_2$ is the smallest subfield of Ω that contains $\mathbf{K}_1$ and $\mathbf{K}_2$.

Lemma 2.8. *If $\mathbf{K}_1$ and $\mathbf{K}_2$ are finite extensions of $\mathbf{k}$, then composite $\mathbf{K}_1\mathbf{K}_2$ is a finite extension of $\mathbf{k}$ and*

$$[\mathbf{K}_1\mathbf{K}_2 : \mathbf{k}] \leq [\mathbf{K}_1 : \mathbf{k}]\,[\mathbf{K}_2 : \mathbf{k}]\,.$$

If $\mathbf{K}_2 = \mathbf{k}(\beta)$ then $\mathbf{K}_1\mathbf{K}_2 = \mathbf{K}_1(\beta)$.

Proof. Since $\mathbf{K}_1/\mathbf{k}$ and $\mathbf{K}_2/\mathbf{k}$ are finite separable extensions, let α and β be elements so that $\mathbf{K}_1 = \mathbf{k}(\alpha)$ and $\mathbf{K}_2 = \mathbf{k}(\beta)$. Let $[\mathbf{K}_1 : \mathbf{k}] = m$ and $[\mathbf{K}_2 : \mathbf{k}] = n$. The mn products $\alpha^i\beta^j$ $(0 \leq i < m,\ 0 \leq j < n)$ span an algebra A over $\mathbf{k}$ that is contained in $\mathbf{K}_1\mathbf{K}_2$. It is enough to show that every non-zero element of A has an inverse in A. Let γ be a non-zero element of A.

$$\gamma = \sum_{j=0}^{n-1}\sum_{i=0}^{m-1} \mu_{ij}\alpha^i\beta^j \qquad \mu_{ij} \in \mathbf{k}$$

Let $f(Y)$ be the polynomial

$$f(Y) = \sum_{j=0}^{n-1}\left(\sum_{i=0}^{m-1} \mu_{ij}\alpha^i\right) Y^j.$$

Then $f(Y)$ is a polynomial in $\mathbf{K}_1[Y]$ and $f(\beta) = \gamma$. Let $g(Y)$ be the minimum polynomial of β over $\mathbf{K}_1$. Since $f(\beta) \neq 0$ then $f(Y)$ is not divisible by $g(Y)$. There exist polynomials $h_1(Y)$ and $h_2(Y)$ in $\mathbf{K}_1(Y)$ so that

$$h_1(Y)f(Y) + h_2(Y)g(Y) = 1.$$

We have $h_1(\beta)f(\beta) = 1$, so γ has an inverse in A. Since β can be any element that generates $\mathbf{K}_2$ over $\mathbf{k}$, we also have shown that $\mathbf{K}_1\mathbf{K}_2 = \mathbf{k}(\beta)$.

LEMMA 2.9. *If* $\mathbf{K}_1/\mathbf{k}$ *and* $\mathbf{K}_2/\mathbf{k}$ *are finite normal extensions then composite* $\mathbf{K}_1\mathbf{K}_2/\mathbf{k}$ *is a finite normal extension.*

PROOF. Suppose that σ is an isomorphism of $\mathbf{K}_1\mathbf{K}_2$ into a subfield of Ω and σ fixes elements of $\mathbf{k}$. Then $(\mathbf{K}_1\mathbf{K}_2)^\sigma$ contains both $\mathbf{K}_1^\sigma = \mathbf{K}_1$ and $\mathbf{K}_2^\sigma = \mathbf{K}_2$, so $(\mathbf{K}_1\mathbf{K}_2)^\sigma \supset \mathbf{K}_1\mathbf{K}_2$. From the proof of lemma 2.8, elements of composite $\mathbf{K}_1\mathbf{K}_2$ have the form $\gamma = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \mu_{ij}\alpha^i\beta^j$ with μ_{ij} in $\mathbf{k}$, α in $\mathbf{K}_1$, β in $\mathbf{K}_2$. Then $\gamma^\sigma = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \mu_{ij}(\alpha^i)^\sigma(\beta^j)^\sigma$, so $(\mathbf{K}_1\mathbf{K}_2)^\sigma \subset \mathbf{K}_1\mathbf{K}_2$. This shows that $\mathbf{K}_1\mathbf{K}_2$ is invariant under any isomorphism that fixes $\mathbf{k}$.

LEMMA 2.10. *If* $\mathbf{K}_1/\mathbf{k}$ *and* $\mathbf{K}_2/\mathbf{k}$ *are finite normal extensions then*

$$[\mathbf{K}_1\mathbf{K}_2 : \mathbf{K}_1] = [\mathbf{K}_2 : \mathbf{K}_1 \cap \mathbf{K}_2]\,,$$
$$[\mathbf{K}_1\mathbf{K}_2 : \mathbf{k}] = [\mathbf{K}_1 : \mathbf{k}]\,[\mathbf{K}_2 : \mathbf{k}] \ \text{ if and only if } \mathbf{K}_1 \cap \mathbf{K}_2 = \mathbf{k}.$$

PROOF. Let $\mathbf{K}_2 = \mathbf{k}(\beta)$. Then $\mathbf{K}_1\mathbf{K}_2 = \mathbf{K}_1(\beta)$. Let $f(x)$ be the minimum polynomial of β over $\mathbf{k}$. Let $g(x)$ be the minimum polynomial of β over $\mathbf{K}_1$. Then $g(x)$ divides $f(x)$. Since $\mathbf{K}_2/\mathbf{k}$ is normal, $f(x)$ splits completely into linear factors over $\mathbf{K}_1$. The coefficients of $g(x)$ must be in $\mathbf{K}_1 \cap \mathbf{K}_2$, so $g(x)$ is the minimum polynomial for β over $\mathbf{K}_1 \cap \mathbf{K}_2$. We have $[\mathbf{K}_1\mathbf{K}_2 : \mathbf{K}_1] = \deg(g) = [\mathbf{K}_2 : \mathbf{K}_1 \cap \mathbf{K}_2]$.

Using the first equality, we have $[\mathbf{K}_1\mathbf{K}_2 : \mathbf{k}] = [\mathbf{K}_1\mathbf{K}_2 : \mathbf{K}_1][\mathbf{K}_1 : \mathbf{k}] = [\mathbf{K}_2 : \mathbf{K}_1 \cap \mathbf{K}_2][\mathbf{K}_1 : \mathbf{k}]$. Then $[\mathbf{K}_1\mathbf{K}_2 : \mathbf{k}][\mathbf{K}_1 \cap \mathbf{K}_2 : \mathbf{k}] = [\mathbf{K}_2 : \mathbf{k}][\mathbf{K}_1 : \mathbf{k}]$, so the second equality holds if and only if $[\mathbf{K}_1 \cap \mathbf{K}_2 : \mathbf{k}] = 1$.

LEMMA 2.11. *Let* $\mathbf{K}_1/\mathbf{k}$ *and* $\mathbf{K}_2/\mathbf{k}$ *be finite normal extensions. There is a natural homomorphism*

$$G\,(\mathbf{K}_1\mathbf{K}_2 : \mathbf{k}) \longrightarrow G\,(\mathbf{K}_1 : \mathbf{k}) \times G\,(\mathbf{K}_2 : \mathbf{k})$$

sending σ *in* $G\,(\mathbf{K}_1\mathbf{K}_2 : \mathbf{k})$ *to* $(\sigma|\mathbf{K}_1, \sigma|\mathbf{K}_2)$. *The mapping is an injection, and the image consists of all* (σ_1, σ_2) *in* $G\,(\mathbf{K}_1 : \mathbf{k}) \times G\,(\mathbf{K}_2 : \mathbf{k})$ *such that* $\sigma_1|(\mathbf{K}_1 \cap \mathbf{K}_2) = \sigma_2|(\mathbf{K}_1 \cap \mathbf{K}_2)$.

PROOF. Put $G = G\,(\mathbf{K}_1\mathbf{K}_2 : \mathbf{k})$. Let H_1 be the subgroup of G that leaves elements of $\mathbf{K}_1$ fixed; Let H_2 be the subgroup of G that leaves elements of $\mathbf{K}_2$ fixed. Then $H_1 \cap H_2 = \{1\}$. Both H_1 and H_2 are normal subgroups of G, and we have $G(\mathbf{K}_1 : \mathbf{k}) = G/H_1$ and $G(\mathbf{K}_2 : \mathbf{k}) = G/H_2$. The mapping $\sigma \rightarrow (\sigma|\mathbf{K}_1, \sigma|\mathbf{K}_2)$ is the natural homomorphism

$$G \xrightarrow{\ \ f\ \ } \tfrac{G}{H_1} \times \tfrac{G}{H_2}.$$

The smallest subgroup of G containing H_1 and H_2 is $H = H_1H_2 = H_2H_1$. We have $G(\mathbf{K}_1 \cap \mathbf{K}_2 : \mathbf{k}) = G/H$. The restrictions from $\mathbf{K}_1$ and $\mathbf{K}_2$ to $\mathbf{K}_1 \cap \mathbf{K}_2$ are the natural homomorphisms $G/H_1 \xrightarrow{g_1} G/H$ and $G/H_2 \xrightarrow{g_2} G/H$. We have

$$G \xrightarrow{\ \ f\ \ } \tfrac{G}{H_1} \times \tfrac{G}{H_2} \xrightarrow{\ g_1 \times g_2\ } \tfrac{G}{H} \times \tfrac{G}{H}.$$

Every element of G maps to the diagonal of $G/H \times G/H$. The mapping f is an injection because $H_1 \cap H_2 = \{1\}$. The order of the image(f) is $[G : 1]$, and

$$[G : 1] = [G : H][H : H_1][H_1 : 1].$$

The order of $\ker(g_1 \times g_2)$ is $[H : H_1][H : H_2]$, so the number of pairs in $G/H_1 \times G/H_2$ which map to the diagonal of $G/H \times G/H$ is $[G : H][H : H_1][H : H_2]$. By lemma 2.10 we have $[H_1 : 1] = [H : H_2]$, so the number of pairs which map to the diagonal is $[G : 1]$. This shows that the image of f consists exactly of pairs which map to the diagonal, *i.e.,* whose restrictions to $\mathbf{K}_1 \cap \mathbf{K}_2$ coincide.

LEMMA 2.12. *If* $\mathbf{K}_1/\mathbf{k}$ *and* $\mathbf{K}_2/\mathbf{k}$ *are finite abelian extensions then the composite* $\mathbf{K}_1\mathbf{K}_2$ *is an abelian extension of* $\mathbf{k}$.

PROOF. $G(\mathbf{K}_1\mathbf{K}_2 : \mathbf{k})$ is isomorphic to a subgroup of abelian group $G(\mathbf{K}_1 : \mathbf{k}) \times G(\mathbf{K}_2 : \mathbf{k})$.

LEMMA 2.13. *If* $\mathbf{K}/\mathbf{k}$ *is abelian and* $\mathbf{K} \supset \mathbf{K}' \supset \mathbf{k}$, *then* $\mathbf{K}'/\mathbf{k}$ *is abelian and Artin symbol* $\left(\frac{\mathbf{K}':\mathbf{k}}{p}\right)$ *is the restriction of* $\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)$ *to* $\mathbf{K}'$ *when* p *is not ramified in* K. *If Theorem 1 holds for* $\mathbf{K}/\mathbf{k}$ *and* $\mathbf{K}'/\mathbf{k}$, *then* $\phi_{\mathbf{K}'/\mathbf{k}}$ *is the restriction of* $\phi_{\mathbf{K}/\mathbf{k}}$ *to* $\mathbf{K}'$.

PROOF. The Artin symbol of $\mathbf{K}'$ is the only automorphism of $G(\mathbf{K}' : \mathbf{k})$ satisfying the condition

$$\alpha^\sigma = \alpha^{\mathrm{N}p}(\bmod \wp') \text{ for all } \alpha \in \mathbf{O}'_{\wp'} \text{ and } \wp'|p \tag{3}$$

where $\mathbf{O}'$ is the ring of integers in $\mathbf{K}'$ and $\wp'$ is prime in $\mathbf{O}'$. The Artin symbol of $\mathbf{K}$ is the only automorphism of $G(\mathbf{K} : \mathbf{k})$ satisfying the condition

$$\alpha^\sigma = \alpha^{\mathrm{N}p}(\bmod \wp) \text{ for all } \alpha \in \mathbf{O}_{\wp'} \text{ and } \wp|p$$

where $\mathbf{O}$ is the ring of integers in $\mathbf{K}$ and $\wp$ is prime in $\mathbf{O}$. If $\sigma = \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)$ and $\alpha \in \mathbf{O}'_{\wp'}$ then

$$\alpha^\sigma - \alpha^{\mathrm{N}p} \in \wp \cap \mathbf{O}'_{\wp'} = \wp'.$$

For every prime $\wp'$ of $\mathbf{O}'$ there is a prime $\wp$ of $\mathbf{O}$ so that $\mathbf{O} \cap \wp = \wp'$. Therefore the restriction of $\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)$ to $\mathbf{K}'$ satisfies condition (3), proving the first assertion.

Assume that Theorem 1 holds for $\mathbf{K}/\mathbf{k}$ and $\mathbf{K}'/\mathbf{k}$. Let E contain all infinite primes of $\mathbf{k}$ and all primes which ramify in $\mathbf{K}$. For $\mathbf{i}$ in $\mathbf{I}_\mathbf{k}\{E\}$, the restriction of $\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i})$ to $\mathbf{K}'$ is the restriction of $\prod_{p \notin E} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{\mathrm{ord}_p(\mathbf{i})}$ to $\mathbf{K}'$, which coincides with $\prod_{p \notin E} \left(\frac{\mathbf{K}':\mathbf{k}}{p}\right)^{\mathrm{ord}_p(\mathbf{i})}$, which coincides with $\phi_{\mathbf{K}'/\mathbf{k}}(\mathbf{i})$. The extension to $\mathbf{I}_\mathbf{k}$ is unique, so the two homomorphisms $\mathbf{I}_\mathbf{k} \to G(\mathbf{K}_1 : \mathbf{k})$ must be identical.

Corollary. *Let* $\mathbf{K}_1/\mathbf{k}$ *and* $\mathbf{K}_2/\mathbf{k}$ *be finite abelian extensions, and suppose that Theorem 1 holds for* $\mathbf{K}_1\mathbf{k}$, $\mathbf{K}_2/\mathbf{k}$ *and* $\mathbf{K}_1\mathbf{K}_2/\mathbf{k}$. *Then the homomorphism of lemma 2.11 maps* $\phi_{\mathbf{K}_1\mathbf{K}_2/\mathbf{k}}(\mathbf{i})$ *to the pair* $\big(\phi_{\mathbf{K}_1/\mathbf{k}}(\mathbf{i}), \phi_{\mathbf{K}_2/\mathbf{k}}(\mathbf{i})\big)$ *for all* $\mathbf{i}$ *in* $\mathbf{I}_\mathbf{k}$.

Proposition 2.14. *Suppose that Theorem 1 holds for a given* $\mathbf{k}$ *and all finite abelian extensions of* $\mathbf{k}$. *Let* $\mathbf{K}_1/\mathbf{k}$ *and* $\mathbf{K}_2/\mathbf{k}$ *be finite abelian extensions. If* $\phi_{\mathbf{K}_1/\mathbf{k}}$ *and* $\phi_{\mathbf{K}_2/\mathbf{k}}$ *have the same kernels then* $\mathbf{K}_1 = \mathbf{K}_2$.

Proof. The map $\mathbf{G}(\mathbf{K}_1\mathbf{K}_2 : \mathbf{k}) \to G(\mathbf{K}_1 : \mathbf{k}) \times G(\mathbf{K}_2 : \mathbf{k})$ is an injection (lemma 2) which maps $\phi_{\mathbf{K}_1\mathbf{K}_2/\mathbf{k}}(\mathbf{i})$ to the pair $\big(\phi_{\mathbf{K}_1\mathbf{k}}(\mathbf{i}), \phi_{\mathbf{K}_2/\mathbf{k}}(\mathbf{i})\big)$ (corollary to lemma 2.13). Suppose that $\ker(\phi_{\mathbf{K}_1/\mathbf{k}}) = \ker(\phi_{\mathbf{K}_2/\mathbf{k}})$. If $\mathbf{i}$ is in $\ker(\phi_{\mathbf{K}_1/\mathbf{k}})$ then $\big(\phi_{\mathbf{K}_1/\mathbf{k}}(\mathbf{i}), \phi_{\mathbf{K}_2/\mathbf{k}}(\mathbf{i})\big)$ is trivial, so $\phi_{\mathbf{K}_1\mathbf{K}_2/\mathbf{k}}(\mathbf{i})$ is trivial, showing that $\ker(\phi_{\mathbf{K}_1/\mathbf{k}})$ is contained in $\ker(\phi_{\mathbf{K}_1\mathbf{K}_2/\mathbf{k}})$. Applying Theorem 1, we have $[\mathbf{K}_1 : \mathbf{k}] \geq [\mathbf{K}_1\mathbf{K}_2 : \mathbf{k}]$. By the same argument we have $[\mathbf{K}_2 : \mathbf{k}] \geq [\mathbf{K}_1\mathbf{K}_2 : \mathbf{k}]$. This shows that $\mathbf{K}_1 = \mathbf{K}_2$

Proposition 2.15. *Suppose that Theorem 1 holds for a given* $\mathbf{k}$ *and all finite abelian extensions of* $\mathbf{k}$. *Let* $\mathbf{K}_1/\mathbf{k}$ *and* $\mathbf{K}_2/\mathbf{k}$ *be finite abelian extensions then* $\mathbf{K}_1 \supset \mathbf{K}_2$ *if and only if* $\ker(\phi_{\mathbf{K}_1/\mathbf{k}}) \subset \ker(\phi_{\mathbf{K}_2/\mathbf{k}})$.

Proof. Assume that $\mathbf{K}_1 \supset \mathbf{K}_2$. Then $\phi_{\mathbf{K}_1/\mathbf{k}}(\mathbf{i})|\mathbf{K}_2 = \phi_{\mathbf{K}_2/\mathbf{k}}(\mathbf{i})$, just as in the proof of proposition 2.14. If $\phi_{\mathbf{K}_1/\mathbf{k}}(\mathbf{i}) = 1$ then $\phi_{\mathbf{K}_2/\mathbf{k}}(\mathbf{i}) = 1$, so $\ker(\phi_{\mathbf{K}_1/\mathbf{k}}) \subset \ker(\phi_{\mathbf{K}_2/\mathbf{k}})$.

Assume that $\ker(\phi_{\mathbf{K}_1/\mathbf{k}}) \subset \ker(\phi_{\mathbf{K}_2/\mathbf{k}})$. According to theorem 1, $\mathbf{I}_\mathbf{k}/\ker(\phi_{\mathbf{K}_1/\mathbf{k}})$ is isomorphic to $G(\mathbf{K}_1 : \mathbf{k})$. Let the image of $\ker(\phi_{\mathbf{K}_2/\mathbf{k}})/\ker(\phi_{\mathbf{K}_1/\mathbf{k}})$ be subgroup G' of $G(\mathbf{K}_1 : \mathbf{k})$. Let $\mathbf{K}'$ be the subfield of $\mathbf{K}_1$ fixed by G'. Then $\ker(\phi_{\mathbf{K}'/\mathbf{k}}) = \ker(\phi_{\mathbf{K}_2/\mathbf{k}})$ because

$$\begin{aligned} \mathbf{i} \in \ker(\phi_{\mathbf{K}'/\mathbf{k}}) &\iff \phi_{\mathbf{K}'/\mathbf{k}}(\mathbf{i}) = 1 \iff \phi_{\mathbf{K}_1/\mathbf{k}}(\mathbf{i})|\mathbf{K}' = 1 \\ &\iff \phi_{\mathbf{K}_1/\mathbf{k}}(\mathbf{i}) \in G' \iff \mathbf{i} \in \ker(\phi_{\mathbf{K}_2/\mathbf{k}}). \end{aligned}$$

Then $\mathbf{K}' = \mathbf{K}_2$ by proposition 2.14, so $\mathbf{K}_1 \supset \mathbf{K}_2$.

Lemma 2.16. *Let* $\mathbf{T}/\mathbf{k}$ *be a finite extension, and let* $\mathbf{K}/\mathbf{k}$ *be a finite abelian extension. Then* $\mathbf{KT}/\mathbf{T}$ *is abelian. Let* $\wp$ *be a prime ideal of* $\mathbf{T}$, *and let* $p = \wp \cap \mathbf{o}$. *If* p *is not ramified in* $\mathbf{K}$ *then* $\wp$ *is not ramified in* $\mathbf{KT}$. *Put* $\mathrm{N}\wp = (\mathrm{N}p)^f$. *Then*

$$\left(\frac{\mathbf{KT} : \mathbf{T}}{\wp}\right)\Big|_{\mathbf{K}} = \left(\frac{\mathbf{K} : \mathbf{k}}{p}\right)^f.$$

Proof. We first show that $\mathbf{KT}/\mathbf{T}$ is normal. (This is like the proof of lemma 2.10, except that here $\mathbf{T}/\mathbf{k}$ may not be normal.) Let $\mathbf{K} = \mathbf{k}(\alpha)$ and let $f(x)$ be the minimum polynomial for α over $\mathbf{k}$. Then $\mathbf{KT} = \mathbf{T}(\alpha)$ by lemma 2.8. Let $g(x)$

be the minimum polynomial for α over $\mathbf{T}$. Then $g(x)$ divides $f(x)$ in $\mathbf{T}(x)$. Since $f(x)$ splits completely into linear factors over $\mathbf{K}$ (and over $\mathbf{KT}$) then $g(x)$ splits completely over $\mathbf{KT}$. Therefore $\mathbf{KT}/\mathbf{T}$ is normal. By restriction to $\mathbf{K}$ we have a homomorphism $G(\mathbf{KT}:\mathbf{T}) \longrightarrow G(\mathbf{K}/\mathbf{k})$. The kernel is trivial, so $G(\mathbf{KT}:\mathbf{T})$ is isomorphic to a subgroup of $G(\mathbf{K}/\mathbf{k})$. Therefore $G(\mathbf{KT}:\mathbf{T})$ is abelian.

Let $\wp'$ be any prime of $\mathbf{KT}$ that divides $\wp$. Let $p' = \wp' \cap \mathbf{O_K}$ be the prime of $\mathbf{K}$ that $\wp'$ divides. We need to show that $\wp$ is not ramified in $\mathbf{KT}$. Let $S_{\wp'}(\mathbf{KT}:\mathbf{T})$ be the splitting group of $\wp'$ in $G(\mathbf{KT}:\mathbf{T})$. Automorphisms σ' in $S_{\wp'}(\mathbf{KT}:\mathbf{T})$ satisfy the condition $(\wp')^{\sigma'} = \wp'$. We have $(\wp' \cap \mathbf{O_K})^{\sigma'} = \wp' \cap \mathbf{O_K}$, or $p'^{\sigma'} = p'$. ($\mathbf{O_K}^{\sigma'} = \mathbf{O_K}$ because $\mathbf{K}/\mathbf{k}$ is normal.) Therefore σ' restricted to $\mathbf{K}$ is in the splitting group $S_{p'}(\mathbf{K}:\mathbf{k})$, and extends to an automorphism of $\mathbf{K}_{p'}$ over $\mathbf{k}_p$.

To show that $\wp$ is not ramified in $\mathbf{KT}$ we need to show that the inertial subgroup of $S_{\wp'}(\mathbf{KT}/\mathbf{T})$ is trivial (Chapter 1, *normal extensions*). An automorphism σ' in the inertial subgroup satisfies the condition

$$\alpha^{\sigma'} = \alpha (\text{mod } \wp') \text{ for all } \alpha \in \mathbf{O}_{\wp'}.$$

The restriction of σ' to $\mathbf{K}$ satisfies

$$\alpha^{\sigma'} = \alpha (\text{mod } \wp' \cap \mathbf{O}_{p'}) \text{ for all } \alpha \in \mathbf{O}_{p'}$$

The restriction of σ' to $\mathbf{K}$ is therefore trivial since the inertial group of p' is trivial, so σ' is trivial on both $\mathbf{K}$ and $\mathbf{T}$.

Let σ' be the Artin symbol $\left(\frac{\mathbf{KT}:\mathbf{T}}{\wp}\right)$. Then $\alpha^{\sigma'} = \alpha^{\mathrm{N}\wp} (\text{mod } \wp')$ for all α in $\mathbf{O}_{\wp'}$, so we have

$$\alpha^{\sigma'} - \alpha^{\mathrm{N}\wp} \in \wp' \cap \mathbf{O}_{p'} \text{ for all } \alpha \in \mathbf{O}_{p'}.$$

Since $\mathrm{N}\wp = (\mathrm{N}p)^f$, we have

$$\alpha^{\sigma'} - \alpha^{(\mathrm{N}p)^f} \in p' \text{ for all } \alpha \in \mathbf{O}_{p'}.$$

By (1.14′), this shows that σ' restricted to $\mathbf{K}$ is $\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^f$ as claimed.

Remark 2.1. To say that "$\phi_{\mathbf{K}/\mathbf{k}}$ can be defined on $\mathbf{I_k}$" means that the homomorphism $\phi_{\mathbf{K}/\mathbf{k}}$ defined by (1) on $\mathbf{I_k}\{E\}$ for some finite set of primes E can be extended to a continuous homomorphism defined on all of $\mathbf{I_k}$. By propositions 2.7 and 2.8, the extension is unique and does not depend on the choice of E.

Remark 2.2. The subgroups of lemma 2.1 may also be described using the fact that p-adic valuations take only discrete values $\{\mathrm{N}p^{-m_p}\}$ for rational integers m_p. We have

$$\begin{aligned} W'_p\left(\mathrm{N}p^{-(m_p-1)}\right) &= \left\{\alpha \in \mathbf{k}_p \middle| \quad |\alpha - 1|_p < \mathrm{N}p^{-(m_p-1)}\right\} \\ &= \left\{\alpha \in \mathbf{k}_p \middle| \quad |\alpha - 1|_p \le \mathrm{N}p^{-m_p}\right\}. \end{aligned}$$

Put

$$W_p\,(m_p) = W_p'\left(\mathrm{N}p^{-(m_p-1)}\right).$$

Note that $W_p\,(0) = \mathbf{u}_p$. For real infinite p put $W_p(0) = \mathbf{k}_p^*$ and $W_p(1) = \mathbf{k}_p^+$; for complex infinite p put $W_p(0) = W_p(1) = \mathbf{k}^*$. We can choose integers m_p, taking $m_p = 0$ for p not in E', so that the subgroup of lemma 2.1 can be written

$$\prod_p W_p\,(m_p)\,. \tag{4}$$

Since all but a finite number of m_p are zero, the formal product $\prod_p p^{m_p}$ over finite and infinite primes is a generalized ideal or *modulus* of $\mathbf{k}$. Subgroup (4) is *the subgroup belonging to* $\prod_p p^{m_p}$.

Lemma 2.17. *Let $\mathbf{T}_\wp/\mathbf{k}_p$ be a finite extension of local fields with $p = \wp^e$. If α in $\mathbf{O}_{\mathbf{T}_\wp}$ satisfies $\alpha = 1(\text{mod } \wp^{em})$ then*

$$\mathbf{N}_{\mathbf{T}_\wp/\mathbf{k}_p}(\alpha) = 1(\text{mod } p^m).$$

Proof. Let π be a generator of principal ideal p in $\mathbf{o}_p$. Then $\wp^{em} = \pi^m\mathbf{O}_{\mathbf{T}_\wp}$. $\mathbf{O}_{\mathbf{T}_\wp}$ is a free $\mathbf{o}_p$-module of degree $n = ef$, so let $x_1, \ldots, x_n$ be a basis. If $\alpha = 1(\text{mod } \wp^{em})$ then $(\alpha-1)x_i \in \wp^{em}$ so

$$(\alpha-1)x_i = \pi^m(a_{i1}x_1 + \cdots + a_{in}x_n) \text{ for } i = 1, \ldots, n.$$

The matrix with respect to basis $x_1, \ldots, x_n$ for linear transformation T_α satisfies $T_\alpha = I(\text{mod } p^m)$. Therefore $\mathbf{N}_{\mathbf{T}_\wp/\mathbf{k}_p}(\alpha) = \det(T_\alpha) = 1(\text{mod } p^m)$.

Lemma 2.18. *Let $\mathbf{T}/\mathbf{k}$ be a finite extension, let $\mathbf{i}$ be an element of $\mathbf{I_T}$, and let $a = \prod_p p^{m_p}$ be an ideal of $\mathbf{o}_k$. There exists β in $\mathbf{T}^*$ so that $\beta^{-1}\mathbf{i}$ is in the subgroup belonging to ideal $a\mathbf{O_T}$, and then we have $\mathbf{N}_{\mathbf{T}/\mathbf{k}}(\beta^{-1}\mathbf{i})$ is in the subgroup belonging to $\prod_p p^{m_p}$.*

Proof. In the extension $\mathbf{T}$, $p\mathbf{O_T}$ splits into a product $p = \wp_1^{e_1}\ldots\wp_g^{e_g}$ of primes $\wp_i$ of $\mathbf{O_T}$. By lemma 2.5, we can find β in $\mathbf{T}^*$ so that $\beta^{-1}\mathbf{i}$ is in the subgroup of $\mathbf{I_T}$ belonging to $a\mathbf{O_T} = \prod_p\prod_{\wp|p}\wp^{m_p e_\wp}$. By Lemma 2.17, $\mathbf{N}_{\mathbf{T}_\wp/k_p}\left(\beta^{-1}\mathbf{i}_\wp\right) = 1(\text{mod } p^{m_p})$ if $m_p > 0$ and p finite. If $m_p = 0$ then $\beta^{-1}\mathbf{i}_\wp$ is in $\mathbf{u}_\wp$ and $|\mathbf{N}_{\mathbf{T}_\wp/k_p}\left(\beta^{-1}\mathbf{i}_\wp\right)|_p = |\beta^{-1}\mathbf{i}_\wp|_\wp = 1$, so $\mathbf{N}_{\mathbf{T}_\wp/k_p}\left(\beta^{-1}\mathbf{i}_\wp\right)$, which is in $\mathbf{u}_p$. If $\wp$ is complex infinite and p is real infinite then $\mathbf{N}_{\mathbf{T}_\wp/k_p}\left(\beta^{-1}\mathbf{i}_\wp\right) = \left(\beta^{-1}\mathbf{i}_\wp\right)\overline{\left(\beta^{-1}\mathbf{i}_\wp\right)}$, which is in $\mathbf{k}_p^+$. Therefore

$$\left(\mathbf{N}_{\mathbf{T}/\mathbf{k}}(\beta^{-1}\mathbf{i})\right)_p = \prod_{\wp|p}\mathbf{N}_{\mathbf{T}_\wp/\mathbf{k}_p}(\beta^{-1}\mathbf{i}_\wp) \quad \begin{cases} = 1(\text{mod } p^{m_p}) \text{ if } m_p > 0 \text{ and } p \text{ finite,} \\ \in \mathbf{u}_p \text{ if } m_p = 0, p \text{ finite,} \\ \in k_p^+ \text{ if } p \text{ real and } \wp \text{ complex} \end{cases}$$

Therefore $\mathbf{N}_{\mathbf{T}/\mathbf{k}}(\beta^{-1}\mathbf{i})$ is in the subgroup belonging to $\prod_p p^{m_p}$.

PROPOSITION 2.19. *Let* $\mathbf{T}/\mathbf{k}$ *be a finite extension, and let* $\mathbf{K}/\mathbf{k}$ *be a finite abelian extension. Suppose that* $\phi_{\mathbf{K}/\mathbf{k}}$ *can be defined on* $\mathbf{I_k}$ *and the kernel contains* $\mathbf{k}^*$*, and that* $\phi_{\mathbf{KT}/\mathbf{T}}$ *can be defined on* $\mathbf{I_T}$ *and the kernel contains* $\mathbf{T}^*$*. Then*

$$\phi_{\mathbf{KT}/\mathbf{T}}(\mathbf{i}) = \phi_{\mathbf{K}/\mathbf{k}}(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i}) \text{ for } \mathbf{i} \in \mathbf{I_T}.$$

PROOF. By lemma 2.1, $\ker(\phi_{\mathbf{KT}/\mathbf{T}})$ contains a subgroup of $\mathbf{I_T}$ belonging to ideal $\prod_{\wp\in E} \wp^{n_\wp}$ of $\mathbf{T}$, and $\ker(\phi_{\mathbf{K}/\mathbf{k}})$ contains a subgroup belonging to ideal $\prod_{p\in F} p^{m_p}$ of $\mathbf{k}$. Add to E all primes $\wp$ of $\mathbf{T}$ which are infinite or ramified in $\mathbf{TK}$. Add to F all primes p of $\mathbf{k}$ which are infinite or ramified in $\mathbf{T}$. Now to F all primes divisible by a prime of E, then add to E all primes which divide a prime of F. A prime of $\mathbf{T}$ is in E if and only if it divides a prime of F. For those finite primes added to E (or F) set $m_\wp = 0$ (or $m_p = 0$; for those infinite primes added to E (or F) set $m_\wp = 1$ (or $m_p = 1$).

Let $\mathbf{i}$ be an element of $\mathbf{I_T}$. We claim that we can choose β in $\mathbf{T}^*$ so that $(\beta\mathbf{i})_\wp$ is in $W_\wp(n_\wp)$ for all finite $\wp$ in E and $\mathbf{N}_{\mathbf{T}_\wp/\mathbf{k}_p}(\beta\mathbf{i})_\wp$ is in $W_p(m_p)$ for all finite p in F. By lemma 2.18, the latter condition will be satisfied if $(\beta\,\mathbf{i})_\wp$ is in $W_\wp(e_\wp m_\wp)$ for all $\wp$ dividing finite p in F. Both conditions can be satisfied by applying lemma 2.5, choosing β so that $(\beta\,\mathbf{i})_\wp$ is in $W_\wp\,(\max(n_\wp, e_\wp m_\wp))$ for finite $\wp$ in E.

Define $\mathbf{j}$ and $\mathbf{j}'$ in $\mathbf{I}_T$ so that

$$\begin{array}{llll} \mathbf{j}_\wp = (\beta\mathbf{i})_\wp & \text{for } \wp \in E & \mathbf{j}_\wp = 1 & \text{for } \wp \notin E \\ \mathbf{j}'_\wp = 1 & \text{for } \wp \in E & \mathbf{j}'_\wp = (\beta\mathbf{i})_\wp & \text{for } \wp \notin E \end{array}$$

Then $\mathbf{j}$ is in $\ker(\phi_{\mathbf{KT}/\mathbf{T}})$ and $\mathbf{N}_{\mathbf{T}/\mathbf{k}}(\mathbf{j})$ is in $\ker(\phi_{\mathbf{K}/\mathbf{k}})$. We have

$$\begin{aligned} \phi_{\mathbf{KT}/\mathbf{T}}(\mathbf{i}) &= \phi_{\mathbf{KT}/\mathbf{T}}(\beta\mathbf{i}) = \phi_{\mathbf{KT}/\mathbf{T}}(\mathbf{j}\,\mathbf{j}') = \phi_{\mathbf{KT}/\mathbf{T}}(\mathbf{j}') \\ &= \prod_{\wp\notin E} \left(\frac{\mathbf{KT}:\mathbf{T}}{\wp}\right)^{b_\wp} \text{ where } |\,\mathbf{j}'|_\wp = |\beta\mathbf{i}|_\wp = \mathrm{N}\wp^{-b_\wp} \end{aligned}$$

By lemma 2.16, we have

$$\phi_{\mathbf{KT}/\mathbf{T}}(\mathbf{i}) = \prod_{p\notin F}\prod_{\wp|p} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{f_\wp b_\wp} = \prod_{p\notin F} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{\sum_{\wp|p} f_\wp b_\wp}. \tag{5}$$

We turn to the computation of $\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{N}_{\mathbf{T}/\mathbf{k}}(\mathbf{i}))$, which is equal to $\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{N}_{\mathbf{T}/\mathbf{k}}(\beta\,\mathbf{i}))$ because $\mathbf{N}_{\mathbf{T}/\mathbf{k}}(\beta)$ is in $\mathbf{k}^*$, *i.e.,* in the kernel of $\phi_{\mathbf{K}/\mathbf{k}}$. Since

$$\left(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i}\right)_p = \prod_{\wp|p} \mathbf{N}_{\mathbf{T}_\wp/\mathbf{k}_p}\mathbf{i}_p \qquad \text{for } \mathbf{i} \in \mathbf{I_T},$$

we have

$$\left|\mathbf{N}_{\mathbf{T}/\mathbf{k}}(\beta\,\mathbf{i})\right|_p = \prod_{\wp|p} \left|\mathbf{N}_{\mathbf{T}_\wp/\mathbf{k}_p}(\beta\,\mathbf{i}_\wp)\right|_p = \prod_{\wp|p} |\beta\,\mathbf{i}|_\wp = \prod_{\wp|p} \mathrm{N}\wp^{-b_\wp}$$
$$= \prod_{\wp|p} \mathrm{N}p^{-f_\wp b_\wp} = \mathrm{N}p^{-\sum_{\wp|p} f_\wp b_\wp}.$$

Therefore

$$\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{N}_{\mathbf{T}/\mathbf{k}}(\mathbf{i})) = \phi_{\mathbf{K}/\mathbf{k}}(\mathbf{N}_{\mathbf{T}/\mathbf{k}}(\beta\,\mathbf{i})) = \prod_{p\notin F} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{\sum_{\wp|p} f_\wp b_\wp}. \tag{6}$$

Comparison of (5) and (6) shows that $\phi_{\mathbf{KT}/\mathbf{T}}(\mathbf{i}) = \phi_{\mathbf{K}/\mathbf{k}}(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i})$, as claimed by the proposition.

Proposition 2.20. *If $\phi_{\mathbf{K}}$ can be extended to a homomorphism of $\mathbf{I}_{\mathbf{k}}$ to $G(\mathbf{K}:\mathbf{k})$ with closed kernel containing $\mathbf{k}^*$, then the kernel contains $\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}$.*

Proof. Apply proposition 2.19 with $\mathbf{T} = \mathbf{K}$. If $\mathbf{i}$ is in $\mathbf{I}_{\mathbf{K}}$, we have

$$\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{N}_{\mathbf{K}/\mathbf{k}}(\mathbf{i})) = \phi_{\mathbf{K}/\mathbf{K}}(\mathbf{i}).$$

But $\phi_{\mathbf{K}/\mathbf{K}}$ maps $\mathbf{I}_{\mathbf{K}}$ to a trivial group $G(\mathbf{K}:\mathbf{K})$.

Remark 2.3. The proof of theorem 1 will require the following fundamental inequalities of class field theory, which will be proved in chapter 7 and chapter 8, respectively.

First fundamental inequality of class field theory. *If $\mathbf{Z}$ is a finite cyclic extension of $\mathbf{k}$ then subgroup $\mathbf{k}^*\mathbf{N}_{\mathbf{Z}/\mathbf{k}}(\mathbf{I}_{\mathbf{Z}})$ of $\mathbf{I}_{\mathbf{k}}$ is a closed subgroup of finite index in $\mathbf{I}_{\mathbf{k}}$ and the index $\left[\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{N}_{\mathbf{Z}/\mathbf{k}}(\mathbf{I}_{\mathbf{Z}})\right]$ is divisible by $[\mathbf{Z}:\mathbf{k}]$.*

Second fundamental inequality of class field theory. *If $\mathbf{K}$ is a finite abelian extension of $\mathbf{k}$ then subgroup $\mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{k}}$ is closed and of finite index in $\mathbf{I}_{\mathbf{k}}$ and the index $\left[\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}(\mathbf{I}_{\mathbf{K}})\right]$ divides $[\mathbf{K}:\mathbf{k}]$.*

Proposition 2.21 (Corollary to the first fundamental inequality). *Let $\mathbf{K}/\mathbf{k}$ be a finite abelian extension. If $\phi_{\mathbf{K}/\mathbf{k}}$ can be extended to a continuous homomorphism of $\mathbf{I}_{\mathbf{k}}$ whose kernel contains $\mathbf{k}^*$, then the image of $\mathbf{I}_{\mathbf{k}}$ is all of $G(\mathbf{K}:\mathbf{k})$.*

Proof. Suppose that the image M of $\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{I}_{\mathbf{k}})$ is not all of $G = G(\mathbf{K}:\mathbf{k})$. We will show this to be impossible. Let $\mathbf{L}$ be the fixed field of M. Take E to be the set of primes of $\mathbf{k}$ containing all infinite primes and all finite primes which are ramified in $\mathbf{K}$. $\phi_{\mathbf{K}/\mathbf{k}}$ is defined on $\mathbf{I}\{E\}$ by (2.1), and by proposition 2.7. Let p be a prime of $\mathbf{k}$ that is not in E. Ideal p of $\mathbf{o}_p$ is principal, so $p = (\pi)$ for an element π of $\mathbf{o}_p$. Take idele $\mathbf{i}$ to have component $\mathbf{i}_p = \pi^{-1}$; take all other components of $\mathbf{i}$ to be 1. Then $\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right) = \phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i})$, so the Artin symbol $\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)$ is an element of M for each prime p not in E. By lemma 2.13, $\left(\frac{\mathbf{L}:\mathbf{k}}{p}\right)$ is the restriction to L of $\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)$, so $\left(\frac{\mathbf{L}:\mathbf{k}}{p}\right) = 1$ because $\mathbf{L}$ is the fixed field of subgroup M.

The finite abelian group G/M is not trivial, so there exists a subgroup M' so that $M \subset M' \subset G$ and G/M' is a non-trivial cyclic group. Let $\mathbf{Z}$ be the fixed field of M'. Then $\mathbf{L} \supset \mathbf{Z} \supset \mathbf{k}$ and $G(\mathbf{Z}/\mathbf{k})$ is a cyclic group isomorphic to G/M'.

Artin symbol $\left(\frac{\mathbf{Z}:\mathbf{k}}{p}\right)$ is the restriction of $\left(\frac{\mathbf{L}:\mathbf{k}}{p}\right)$ to $\mathbf{Z}$, so $\left(\frac{\mathbf{Z}:\mathbf{k}}{p}\right) = 1$. The Artin symbol $\left(\frac{\mathbf{Z}:\mathbf{k}}{p}\right)$ generates the Galois group $G(\mathbf{Z}_\wp : \mathbf{k}_p)$ for each prime $\wp$ of $\mathbf{Z}$ that divides an unramified prime p (Chapter 1, *normal extensions*). Therefore if p is unramified in K then $\mathbf{Z}_\wp = \mathbf{k}_p$. For each $\mathbf{i}$ in $\mathbf{I}_\mathbf{k}\{E\}$, this allows us to construct an idele $\mathbf{j}$ in $\mathbf{I}_\mathbf{Z}$ such that $\mathbf{N}_{\mathbf{Z}/\mathbf{k}}(\mathbf{j}) = \mathbf{i}$. For each prime p not in E, select one prime $\wp(p)$ of $\mathbf{Z}$ which divides p. Put $\mathbf{j}_{\wp(p)} = \mathbf{i}_p$, and put $\mathbf{j}_\wp = 1$ at other primes $\wp$ dividing p. At primes $\wp$ of $\mathbf{Z}$ dividing primes in E, put $\mathbf{j}_\wp = 1$. We have

$$\left(\mathbf{N}_{\mathbf{Z}/\mathbf{k}}(\mathbf{j})\right)_p = \prod_{\wp | p} \mathbf{N}_{\mathbf{Z}_\wp/\mathbf{k}_p}(\mathbf{j}_\wp) = \begin{cases} \mathbf{N}_{\mathbf{Z}_{\wp(p)}/\mathbf{k}_p}(\mathbf{j}_{\wp(p)}) = \mathbf{i}_p & \text{for } p \in E \\ 1 & \text{for } p \notin E \end{cases}$$

Therefore $\mathbf{I}_\mathbf{K}\{E\}$ is contained in $\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I}_\mathbf{Z}$. Consider two homomorphisms from $\mathbf{I}_\mathbf{k}$ to $\mathbf{I}_\mathbf{k}/\mathbf{k}^*\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I}_\mathbf{Z}$. The first is the natural homomorphism sending each idele to its own coset and the second sends each idele to 1. Both homomorphisms agree on $\mathbf{I}_\mathbf{k}\{E\}$. Both are continuous homomorphisms whose kernels are closed and contain $\mathbf{k}^*$. By proposition 2.6, the two homomorphisms are identical, so $\mathbf{I}_\mathbf{k}/\mathbf{k}^*\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I}_\mathbf{Z}$ must be trivial. By the first fundamental inequality, degree $[\mathbf{Z} : \mathbf{k}]$ divides index $[\mathbf{I}_\mathbf{k} : \mathbf{k}^*\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I}_\mathbf{Z}]$, so the group $\mathbf{I}_\mathbf{k}/\mathbf{k}^*\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I}_\mathbf{Z}$ cannot be trivial, and we have reached our contradiction. It must be that M is all of $G(\mathbf{K} : \mathbf{k})$.

Proposition 2.22 (Corollary to the second fundamental inequality). *Suppose* $\mathbf{K}/\mathbf{k}$ *is a finite abelian extension. If* $\phi_{\mathbf{K}/\mathbf{k}}$ *can be extended to a continuous homomorphism of* $\mathbf{I}_\mathbf{k}$ *whose kernel contains* $\mathbf{k}^*$*, then the kernel of* $\phi_{\mathbf{K}/\mathbf{k}}$ *is* $\mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_\mathbf{K}$.

Proof. By proposition 2.1, $\phi_{\mathbf{K}/\mathbf{k}}$ maps $\mathbf{I}_\mathbf{k}$ onto $G(\mathbf{K} : \mathbf{k})$, so $\left[\mathbf{I}_\mathbf{k} : \ker(\phi_{\mathbf{K}/\mathbf{k}})\right] = [\mathbf{K} : \mathbf{k}]$. By proposition 2.20, $\mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_\mathbf{K}$ is contained in $\ker(\phi_{\mathbf{K}/\mathbf{k}})$, so

$$\left[\mathbf{I}_\mathbf{k} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_\mathbf{K}\right] = \left[\mathbf{I}_\mathbf{k} : \ker(\phi_{\mathbf{K}/\mathbf{k}})\right]\left[\ker(\phi_{\mathbf{K}/\mathbf{k}}) : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_\mathbf{K}\right].$$

Therefore $[\mathbf{K} : \mathbf{k}]$ divides $\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}}\,\mathbf{I_K}\right]$. $\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}}\,\mathbf{I_K}\right]$ divides $[\mathbf{K} : \mathbf{k}]$ by the second fundamental inequality, so $\left[\ker(\phi_{\mathbf{K/k}}) : \mathbf{k}^*\mathbf{N_{K/k}}\,\mathbf{I_K}\right] = 1$, which proves the proposition.

Remark 4. We have shown that if $\phi_{\mathbf{K/k}}$ can be extended to a homomorphism of $\mathbf{I_k}$ whose kernel contains $\mathbf{k}^*$ then the extension is unique (proposition 2.6), is independent of E (proposition 2.7), and the kernel is exactly $\mathbf{k}^*\mathbf{N_{K/k}}\mathbf{I_k}$. It remains to show that $\phi_{\mathbf{K/k}}$ can be extended, and to prove the two fundamental inequalities.