CHAPTER II

FUNDAMENTAL THEOREMS

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

\[
I_k \{E\} = \{ i \in I_k \mid i_p = 1 \text{ for } p \in E \}.
\]

Define \( \phi_{K/k} : I_k \{E\} \rightarrow G(K : k) \) by

\[
\phi_{K/k}(i) = \prod_{p \notin E} \left( \frac{K}{k} \right)^{n_p} \quad \text{where } |i_p| = (Np)^{-n_p} \text{ for } p \notin E.
\]

The homomorphism \( N_{K/k} : I_K \rightarrow I_k \) of idele groups is defined by

\[
(N_{K/k} i)_p = \prod_{\varphi|p} N_{K_{\varphi/k_p}} i_p \quad \text{for } i \in I_K.
\]

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

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

**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 \( \phi_{K/k} \).
Lemma 2.1. A closed subgroup of finite index in $I_k$ contains a subgroup of the form

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

where $E'$ is a finite set of finite primes, the $\epsilon_p$ are real numbers satisfying $\epsilon_p \leq 1$ for $p \in E'$, sets $u_p$ and $W'_p(\epsilon_p)$ are defined by

$$
u_p = \{ \alpha \in k^*_p \mid |\alpha|_p = 1 \} \quad W'_p(\epsilon_p) = \{ \alpha \in k^*_p \mid |\alpha - 1|_p < \epsilon_p \},$$

and $k^+_p \simeq \{ x \in \mathbb{R}^* \mid x > 0 \}$ 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 $I_k$ 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

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

$H$ 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 $\mathfrak{o}$ and let $\alpha_1$ and $\alpha_2$ be integers of $\mathfrak{o}$. There exists $\alpha$ in $\mathfrak{o}$ 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 $\alpha_1 - \alpha_2 \in a$. $a_1a^{-1} + a_2a^{-1} = \mathfrak{o}$, so there exist integers $\beta_1 \in a_1a^{-1}$ and $\beta_2 \in a_2a^{-1}$ 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 $\mathfrak{o}$ 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 $\mathfrak{o}$. There exists an element $\alpha$ of $\mathfrak{o}$ 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 $p_1^{n_1} \cdots p_{k-1}^{n_{k-1}} + p_k^{n_k}$ is $\mathfrak{o}$. Use lemma 2.2 and induction.
LEMMA 2.3. Let $\alpha_1, \ldots, \alpha_n$ be a basis for $k$ over $Q$. Let $k$ have $r_1$ real and $r_2$ complex infinite primes, and let the distinct isomorphisms of $k$ into $R$ or $C$ be $\sigma_1, \ldots, \sigma_n$, where $\sigma_1, \ldots, \sigma_{r_1}$ are the $r_1$ isomorphisms into $R$ and $\sigma_{r_1+1}, \ldots, \sigma_n$ are the $2r_2$ isomorphisms into $C$, Then $\det \parallel \alpha_i^\sigma_j \parallel$ is not zero.

PROOF. It is enough to show that the determinant is not zero for some basis. Let $\alpha$ generate $k$ over $Q$. Then $1, \alpha, \ldots, \alpha^{n-1}$ is a basis. The elements $\alpha^{\sigma_1} \ldots \alpha^{\sigma_n}$ are distinct, so $\parallel (\alpha^{\sigma_j})^{-1} \parallel$ 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 $\alpha_p$ in $k_p$ and a positive real number $\epsilon_p$ are given. Then there is an $\alpha$ in $k$ so that $|\alpha - \alpha_p|_p < \epsilon_p$ for all $p$ in $E'$.

PROOF. There exists a non-zero $\beta$ in $o$ so that $\beta \alpha_p \in o_p$ for all finite $p \in E'$. By the corollary to lemma 2.2, there is an $\alpha' \in k$ satisfying the conditions $\alpha' - \beta \alpha_p \in p^{m_r}$ 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 $o$ 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

$$|ma'' - \gamma - m \alpha_p|_p \leq \max (|\gamma|_p, |m(\alpha'' - \alpha_p)|_p) < \epsilon_p$$

for finite $p$ in $E'$ and $\gamma \in a$.

Therefore

$$|a'' - \gamma/m - \alpha_p|_p \leq \epsilon_p$$

for finite $p \in E'$ and $\gamma \in a$,

so $\alpha = a'' - \gamma/m$ satisfies our condition for the finite primes in $E'$. We must show how to choose $\gamma$ and $m$ so that $\alpha$ 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 $\eta$ in $k^*$ so that,

$$1. \quad |(a''m - \alpha_p)m - (\gamma_0 + \eta)|_p < \frac{\epsilon_p}{2} \quad \text{and} \quad |\eta|_p < M \quad \text{for all infinite} \ p \in E'.$$

Then

$$|(a'' - \alpha_p) - \gamma_0/m|_p < \frac{\epsilon_p}{2m} + \frac{|\eta|_p}{m} \leq \frac{\epsilon_p}{2m} + \frac{M}{m}$$

for all infinite $p \in E'$.

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

$$|a'' - \gamma_0/m - \alpha_p|_p < \epsilon_p$$

for all infinite $p \in E'$. 

II. FUNDAMENTAL THEOREMS
II. FUNDAMENTAL THEOREMS

13

It remains to establish the claim about $M$ and to choose $\gamma_0$ and $\eta$. It is possible to choose a basis $\alpha_1, \ldots, \alpha_n$ for $k$ over $\mathbb{Q}$ so that each basis element $\alpha_i$ belongs to ideal $a$. If $\sigma_1, \ldots, \sigma_n$ are the distinct isomorphisms of $k$ into $R$ or $C$, then by lemma 2.3 the mapping

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

takes $\alpha_1Z + \cdots + \alpha_nZ$ to a non-degenerate $n$-dimensional lattice. Any element in $R^{r_1} \oplus C^{r_2}$ can be closely approximated by an element $u_1\alpha_1 + \cdots + u_n\alpha_n$ where the $u_i$ are elements of $Q$. Write $u_i = k_i + v_i$ where $k_i$ is in $Z$ 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 $\alpha_p$ in $k_p^*$ and a positive real number $\epsilon_p$ are given. Then there is an $\alpha$ in $k^*$ so that $|\alpha\alpha_p^{-1} - 1|_p < \epsilon_p$ and $|\alpha^{-1}\alpha - 1|_p < \epsilon_p$.

**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 $\alpha$ in $k$ 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 $|\alpha^{-1}\alpha - 1|_p < \epsilon_p$ for both finite $p$ and infinite $p$ in $E'$.

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

**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

$$U = \prod_{p \not\in E'} u_p \times \prod_{p \in E'} W'_p(\epsilon'_p) \times \prod_{p \in E'} k_+^p \times \prod_{p \in E'} k_p^*$$

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

$$j_p = 1 \quad \text{for } p \not\in E \quad j_p = \alpha^{-1}i_p \quad \text{for } p \in E$$

$$j'_p = \alpha^{-1}i_p \quad \text{for } p \not\in E \quad j'_p = 1 \quad \text{for } p \in E$$

(If $p$ is in $E$ but not $E'$ then $j_p = 1$, so $j$ is in $U$.) Since the kernels of $\phi_1$ and $\phi_2$ contain $k^*$, we have

$$\phi_1(i) = \phi_1(\alpha^{-1}i) = \phi_1(jj') = \phi_1(j') = \phi_2(j') = \phi_2(jj') = \phi_2(\alpha^{-1}i) = \phi_2(i).$$
Proposition 2.7. If $\phi$ is a homomorphism from $I_k \{E\}$ to a finite group and the kernel of $\phi$ has closed kernel of finite index, then any extension of $\phi$ to $I_k$ whose kernel contains $k^*$ is independent of $E$.

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

Composite fields of finite extensions. Let $\Omega$ be an algebraic closure of $k$. All of our extensions of $k$ will be subfields of $\Omega$. If $K_1$ and $K_2$ are subfields of $\Omega$ then the composite field $K_1 K_2$ is the smallest subfield of $\Omega$ that contains $K_1$ and $K_2$.

Lemma 2.8. If $K_1$ and $K_2$ are finite extensions of $k$, then composite $K_1 K_2$ is a finite extension of $k$ and

$$[K_1 K_2 : k] \leq [K_1 : k] [K_2 : k].$$

If $K_2 = k(\beta)$ then $K_1 K_2 = K_1(\beta)$.

Proof. Since $K_1 / k$ and $K_2 / k$ are finite separable extensions, let $\alpha$ and $\beta$ be elements so that $K_1 = k(\alpha)$ and $K_2 = k(\beta)$. Let $[K_1 : k] = m$ and $[K_2 : k] = n$. The $mn$ products $\alpha^i \beta^j$ ($0 \leq i < m$, $0 \leq j < n$) span an algebra $A$ over $k$ that is contained in $K_1 K_2$. It is enough to show that every non-zero element of $A$ has an inverse in $A$. Let $\gamma$ be a non-zero element of $A$.

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

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 $K_1[Y]$ and $f(\beta) = \gamma$. Let $g(Y)$ be the minimum polynomial of $\beta$ over $K_1$. 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 $K_1(Y)$ so that

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

We have $h_1(\beta) f(\beta) = 1$, so $\gamma$ has an inverse in $A$. Since $\beta$ can be any element that generates $K_2$ over $k$, we also have shown that $K_1 K_2 = k(\beta)$. 


Lemma 2.9. If \( K_1/k \) and \( K_2/k \) are finite normal extensions then composite \( K_1K_2/k \) is a finite normal extension.

Proof. Suppose that \( \sigma \) is an isomorphism of \( K_1K_2 \) into a subfield of \( \Omega \) and \( \sigma \) fixes elements of \( k \). Then \( (K_1K_2)^\sigma \) contains both \( K_1^\sigma = K_1 \) and \( K_2^\sigma = K_2 \), so \( (K_1K_2)^\sigma \supset K_1K_2 \). From the proof of lemma 2.8, elements of composite \( K_1K_2 \) have the form \( \gamma = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \mu_{ij} \alpha^i \beta^j \) with \( \mu_{ij} \) in \( k \), \( \alpha \) in \( K_1 \), \( \beta \) in \( K_2 \). Then \( \gamma^\sigma = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \mu_{ij} (\alpha^i)^\sigma (\beta^j)^\sigma \), so \( (K_1K_2)^\sigma \subset K_1K_2 \). This shows that \( K_1K_2 \) is invariant under any isomorphism that fixes \( k \).

Lemma 2.10. If \( K_1/k \) and \( K_2/k \) are finite normal extensions then

\[
[K_1K_2 : K_1] = [K_2 : K_1 \cap K_2],
\]

\[
[K_1K_2 : k] = [K_1 : k] [K_2 : k] \text{ if and only if } K_1 \cap K_2 = k.
\]

Proof. Let \( K_2 = k(\beta) \). Then \( K_1K_2 = K_1(\beta) \). Let \( f(x) \) be the minimum polynomial of \( \beta \) over \( k \). Let \( g(x) \) be the minimum polynomial of \( \beta \) over \( K_1 \). Then \( g(x) \) divides \( f(x) \). Since \( K_2/k \) is normal, \( f(x) \) splits completely into linear factors over \( K_1 \). The coefficients of \( g(x) \) must be in \( K_1 \cap K_2 \), so \( g(x) \) is the minimum polynomial for \( \beta \) over \( K_1 \cap K_2 \). We have \( [K_1K_2 : K_1] = \deg(g) = [K_2 : K_1 \cap K_2] \).

Using the first equality, we have \( [K_1K_2 : k] = [K_1K_2 : K_1][K_1 : k] = [K_2 : K_1 \cap K_2][K_1 : k] \). Then \( [K_1K_2 : k][K_1 \cap K_2 : k] = [K_2 : k][K_1 : k] \), so the second equality holds if and only if \( [K_1 \cap K_2 : k] = 1 \).

Lemma 2.11. Let \( K_1/k \) and \( K_2/k \) be finite normal extensions. There is a natural homomorphism

\[
G(K_1K_2 : k) \longrightarrow G(K_1 : k) \times G(K_2 : k)
\]

sending \( \sigma \) in \( G(K_1K_2 : k) \) to \( (\sigma|K_1, \sigma|K_2) \). The mapping is an injection, and the image consists of all \( (\sigma_1, \sigma_2) \) in \( G(K_1 : k) \times G(K_2 : k) \) such that \( \sigma_1|(K_1 \cap K_2) = \sigma_2|(K_1 \cap K_2) \).

Proof. Put \( G = G(K_1K_2 : k) \). Let \( H_1 \) be the subgroup of \( G \) that leaves elements of \( K_1 \) fixed; Let \( H_2 \) be the subgroup of \( G \) that leaves elements of \( K_2 \) fixed. Then \( H_1 \cap H_2 = \{1\} \). Both \( H_1 \) and \( H_2 \) are normal subgroups of \( G \), and we have \( G(K_1 : k) = G/H_1 \) and \( G(K_2 : k) = G/H_2 \). The mapping \( \sigma \to (\sigma|K_1, \sigma|K_2) \) is the natural homomorphism

\[
G \overset{f}{\longrightarrow} \frac{G}{H_1} \times \frac{G}{H_2}.
\]

The smallest subgroup of \( G \) containing \( H_1 \) and \( H_2 \) is \( H = H_1H_2 = H_2H_1 \). We have \( G(K_1 \cap K_2 : k) = G/H \). The restrictions from \( K_1 \) and \( K_2 \) to \( K_1 \cap K_2 \) are the natural homomorphisms \( G/H_1 \overset{g_1}{\longrightarrow} G/H \) and \( G/H_2 \overset{g_2}{\longrightarrow} G/H \). We have

\[
G \overset{f}{\longrightarrow} \frac{G}{H_1} \times \frac{G}{H_2} \overset{g_1 \times g_2}{\longrightarrow} \frac{G}{H_1} \times \frac{G}{H_2}.
\]
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 of $f$ 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 $K_1 \cap K_2$ coincide.

**Lemma 2.12.** If $K_1/k$ and $K_2/k$ are finite abelian extensions then the composite $K_1K_2$ is an abelian extension of $k$.

**Proof.** $G(K_1K_2 : k)$ is isomorphic to a subgroup of abelian group $G(K_1 : k) \times G(K_2 : k)$.

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

**Proof.** The Artin symbol of $K'$ is the only automorphism of $G(K' : k)$ satisfying the condition

$$\alpha^\sigma = \alpha^{Np}(\mod \varphi') \text{ for all } \alpha \in O'_{\varphi'} \text{ and } \varphi'|p$$

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

$$\alpha^\sigma = \alpha^{Np}(\mod \varphi) \text{ for all } \alpha \in O_{\varphi} \text{ and } \varphi|p$$

where $O$ is the ring of integers in $K$ and $\varphi$ is prime in $O$. If $\sigma = (K/k)_p$ and $\alpha \in O'_{\varphi'}$, then

$$\alpha^\sigma - \alpha^{Np} \in \varphi \cap O'_{\varphi'} = \varphi'.$$

For every prime $\varphi'$ of $O'$ there is a prime $\varphi$ of $O$ so that $O \cap \varphi = \varphi'$. Therefore the restriction of $(K/k)_p$ to $K'$ satisfies condition (3), proving the first assertion.

Assume that Theorem 1 holds for $K/k$ and $K'/k$. Let $E$ contain all infinite primes of $k$ and all primes which ramify in $K$. For $i$ in $I_k\{E\}$, the restriction of $\phi_{K/k}(i)$ to $K'$ is the restriction of $\prod_{p \notin E} (K/k)_{op}(i)$ to $K'$, which coincides with $\prod_{p \notin E} (K'/k)_{op}(i)$, which coincides with $\phi_{K'/k}(i)$. The extension to $I_k$ is unique, so the two homomorphisms $I_k \rightarrow G(K_1 : k)$ must be identical.
II. FUNDAMENTAL THEOREMS 17

COROLLARY. Let $K_1/k$ and $K_2/k$ be finite abelian extensions, and suppose that Theorem 1 holds for $K_1$, $K_2$ and $K_1K_2/k$. Then the homomorphism of lemma 2.11 maps $\phi_{K_1K_2/k}(i)$ to the pair $(\phi_{K_1/k}(i), \phi_{K_2/k}(i))$ for all $i \in I_k$.

PROPOSITION 2.14. Suppose that Theorem 1 holds for a given $k$ and all finite abelian extensions of $k$. Let $K_1/k$ and $K_2/k$ be finite abelian extensions. If $\phi_{K_1/k}$ and $\phi_{K_2/k}$ have the same kernels then $K_1 = K_2$.

PROOF. The map $G(K_1K_2 : k) \rightarrow G(K_1 : k) \times G(K_2 : k)$ is an injection (lemma 2) which maps $\phi_{K_1K_2/k}(i)$ to the pair $(\phi_{K_1/k}(i), \phi_{K_2/k}(i))$ (corollary to lemma 2.13). Suppose that $\ker(\phi_{K_1/k}) = \ker(\phi_{K_2/k})$. If $i$ is in $\ker(\phi_{K_1/k})$ then $(\phi_{K_1/k}(i), \phi_{K_2/k}(i))$ is trivial, so $\phi_{K_1k/k}(i)$ is trivial, showing that $\ker(\phi_{K_1/k})$ is contained in $\ker(\phi_{K_1K_2/k})$. Applying Theorem 1, we have $[K_1 : k] \geq [K_1K_2 : k]$. By the same argument we have $[K_2 : k] \geq [K_1K_2 : k]$. This shows that $K_1 = K_2$.

PROPOSITION 2.15. Suppose that Theorem 1 holds for a given $k$ and all finite abelian extensions of $k$. Let $K_1/k$ and $K_2/k$ be finite abelian extensions then $K_1 \supset K_2$ if and only if $\ker(\phi_{K_1/k}) \subset \ker(\phi_{K_2/k})$.

PROOF. Assume that $K_1 \supset K_2$. Then $\phi_{K_1/k}(i)K_2 = \phi_{K_2/k}(i)$, just as in the proof of proposition 2.14. If $\phi_{K_1/k}(i) = 1$ then $\phi_{K_2/k}(i) = 1$, so $\ker(\phi_{K_1/k}) \subset \ker(\phi_{K_2/k})$.

Assume that $\ker(\phi_{K_1/k}) \subset \ker(\phi_{K_2/k})$. According to theorem 1, $I_{k/k}(\phi_{K_1/k})$ is isomorphic to $G(K_1 : k)$. Let the image of $\ker(\phi_{K_2/k})/\ker(\phi_{K_1/k})$ be subgroup $G'$ of $G(K_1 : k)$. Let $K'$ be the subfield of $K_1$ fixed by $G'$. Then $\ker(\phi_{K'/k}) = \ker(\phi_{K_2/k})$ because

\[ i \in \ker(\phi_{K'/k}) \iff \phi_{K'/k}(i) = 1 \iff \phi_{K_1/k}(i)K' = 1 \iff \phi_{K_1/k}(i) \in G' \iff i \in \ker(\phi_{K_2/k}). \]

Then $K' = K_2$ by proposition 2.14, so $K_1 \supset K_2$.

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

\[ \left( \frac{KT : T}{\wp} \right) \bigg|_k = \left( \frac{K : k}{p} \right)^f. \]

PROOF. We first show that $KT/T$ is normal. (This is like the proof of lemma 2.10, except that here $T/k$ may not be normal.) Let $K = k(\alpha)$ and let $f(x)$ be the minimum polynomial for $\alpha$ over $k$. Then $KT = T(\alpha)$ by lemma 2.8. Let $g(x)$
be the minimum polynomial for $\alpha$ over $T$. Then $g(x)$ divides $f(x)$ in $T(x)$. Since $f(x)$ splits completely into linear factors over $K$ (and over $KT$) then $g(x)$ splits completely over $KT$. Therefore $KT/T$ is normal. By restriction to $K$ we have a homomorphism $G(KT : T) \rightarrow G(K/k)$. The kernel is trivial, so $G(KT : T)$ is isomorphic to a subgroup of $G(K/k)$. Therefore $G(KT : T)$ is abelian.

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

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

$$\alpha^{\sigma'} = \alpha(\text{mod } \varphi') \text{ for all } \alpha \in O_{\varphi'}.$$

The restriction of $\sigma'$ to $K$ satisfies

$$\alpha^{\sigma'} = \alpha(\text{mod } \varphi' \cap O_{p'}) \text{ for all } \alpha \in O_{p'}.$$

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

Let $\sigma'$ be the Artin symbol $\left( \frac{KT : T}{\varphi} \right)$. Then $\alpha^{\sigma'} = \alpha^{\varphi'}(\text{mod } \varphi')$ for all $\alpha$ in $O_{\varphi'}$, so we have

$$\alpha^{\sigma'} - \alpha^{\varphi'} \in \varphi' \cap O_{p'} \text{ for all } \alpha \in O_{p'}.$$

Since $N\varphi' = (Np)^f$, we have

$$\alpha^{\sigma'} - \alpha^{(Np)^f} \in p' \text{ for all } \alpha \in O_{p'}.$$

By (1.14'), this shows that $\sigma'$ restricted to $K$ is $\left( \frac{Kk}{p} \right)^f$ as claimed.

**Remark 2.1.** To say that "$\phi_{K/k}$ can be defined on $I_k$" means that the homomorphism $\phi_{K/k}$ defined by (1) on $I_k\{E\}$ for some finite set of primes $E$ can be extended to a continuous homomorphism defined on all of $I_k$. 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 $\{Np^{-mp}\}$ for rational integers $m_p$. We have

$$W'_p \left( Np^{-(m_p-1)} \right) = \left\{ \alpha \in k_p \mid |\alpha - 1|_p < Np^{-(m_p-1)} \right\}$$

$$= \left\{ \alpha \in k_p \mid |\alpha - 1|_p \leq Np^{-m_p} \right\}.$$
Put
\[ W_p(m_p) = W_p' \left( Np^{-(m_p-1)} \right). \]
Note that \( W_p(0) = u_p \). For real infinite \( p \) put \( W_p(0) = k^*_p \) and \( W_p(1) = k^+_p \); for complex infinite \( p \) put \( W_p(0) = W_p'(1) = k^* \). 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
\[ \prod_p W_p(m_p). \]
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 \( k \). Subgroup (4) is the subgroup belonging to \( \prod_p p^{m_p} \).

**Lemma 2.17.** Let \( T_p/k_p \) be a finite extension of local fields with \( p = \varphi^e \). If \( \alpha \) in \( O_{T_p} \) satisfies \( \alpha = 1(\mod \varphi^m) \) then
\[ N_{T_p/k_p}(\alpha) = 1(\mod p^m). \]

**Proof.** Let \( \pi \) be a generator of principal ideal \( p \) in \( o_p \). Then \( \varphi^m = \pi^m o_{T_p} \).
\( O_{T_p} \) is a free \( o_p \)-module of degree \( n = ef \), so let \( x_1, \ldots, x_n \) be a basis. If \( \alpha = 1(\mod \varphi^m) \) then \( (\alpha - 1)x_i \in \varphi^m \) 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 \( T_\alpha \) satisfies \( T_\alpha = I(\mod p^m) \). Therefore \( N_{T_p/k_p}(\alpha) = \det(T_\alpha) = 1(\mod p^m) \).

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

**Proof.** In the extension \( T, pO_T \) splits into a product \( p = \varphi_1^{e_1} \cdots \varphi_g^{e_g} \) of primes \( \varphi_i \) of \( O_T \). By lemma 2.5, we can find \( \beta \) in \( T^* \) so that \( \beta^{-1}i \) is in the subgroup of \( I_T \) belonging to \( aO_T = \prod_p \prod_{\varphi|p} \varphi^{m_{\varphi}e_{\varphi}} \). By Lemma 2.17, \( N_{T_{\varphi}/k_p} \left( \beta^{-1}i_\varphi \right) = 1(\mod p^m) \) if \( m_\varphi > 0 \) and \( p \) finite. If \( m_\varphi = 0 \) then \( \beta^{-1}i_\varphi \) is in \( u_\varphi \) and \( |N_{T_\varphi/k_p}(\beta^{-1}i_\varphi)|_p = |\beta^{-1}i_\varphi|_\varphi = 1 \), so \( N_{T_{\varphi}/k_p} \left( \beta^{-1}i_\varphi \right) \) is in \( u_p \). If \( \varphi \) is complex infinite and \( p \) is real infinite then \( N_{T_{\varphi}/k_p} \left( \beta^{-1}i_\varphi \right) = \left( \beta^{-1}i_\varphi \right) \left( \beta^{-1}i_\varphi \right)^{-1} \), which is in \( k^+_p \). Therefore
\[ \left( N_{T/k}(\beta^{-1}i) \right)_p = \prod_{\varphi|p} N_{T_{\varphi}/k_p}(\beta^{-1}i_\varphi) \]
where
\[ = 1(\mod p^m) \text{ if } m_\varphi > 0 \text{ and } p \text{ finite,} \]
\[ \in u_p \text{ if } m_\varphi = 0, p \text{ finite,} \]
\[ \in k^+_p \text{ if } p \text{ real and } \varphi \text{ complex.} \]
Therefore \( N_{T/k}(\beta^{-1}i) \) is in the subgroup belonging to \( \prod_p p^{m_p} \).
PROPOSITION 2.19. Let $T/k$ be a finite extension, and let $K/k$ be a finite abelian extension. Suppose that $\phi_K/k$ can be defined on $I_k$ and the kernel contains $k^*$, and that $\phi_{KT/T}$ can be defined on $I_T$ and the kernel contains $T^*$. Then

$$\phi_{KT/T}(i) = \phi_K/k (N_{T/k}i) \text{ for } i \in I_T.$$  

PROOF. By lemma 2.1, $\ker(\phi_{KT/T})$ contains a subgroup of $I_T$ belonging to ideal $\prod_{\wp \in E} \wp^{n_\wp}$ of $T$, and $\ker(\phi_K/k)$ contains a subgroup belonging to ideal $\prod_{p \in F} p^{m_p}$ of $k$. Add to $E$ all primes $\wp$ of $T$ which are infinite or ramified in $TK$. Add to $F$ all primes $p$ of $k$ which are infinite or ramified in $T$. 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 $T$ 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 $m_p = 1$ (or $m_p = 1$).

Let $i$ be an element of $I_T$. We claim that we can choose $\beta$ in $T^*$ so that $(\beta i)_\wp$ is in $W_\wp(n_\wp)$ for all finite $\wp$ in $E$ and $N_{T,\wp/k_p}(\beta i)_\wp$ in $W_\wp(m_\wp)$ for all finite $p$ in $F$. By lemma 2.18, the latter condition will be satisfied if $(\beta i)_\wp$ 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 $\beta$ so that $(\beta i)_\wp$ is in $W_\wp(max(n_\wp, e_\wp m_\wp))$ for finite $\wp$ in $E$.

Define $j$ and $j'$ in $I_T$ so that

$$j_\wp = (\beta i)_\wp \text{ for } \wp \in E \quad j_\wp = 1 \text{ for } \wp \notin E$$

$$j'_\wp = 1 \text{ for } \wp \in E \quad j'_\wp = (\beta i)_\wp \text{ for } \wp \notin E$$

Then $j$ is in $\ker(\phi_{KT/T})$ and $N_{T/k}(j)$ is in $\ker(\phi_K/k)$. We have

$$\phi_{KT/T}(i) = \phi_K/k (\beta i) = \phi_{KT/T}(jj') = \phi_{KT/T}(j')$$

$$= \prod_{\wp \notin E} \left( \frac{KT:T}{\wp} \right)^{b_\wp} \text{ where } |j'|_\wp = |\beta i|_\wp = N_{\wp}^{-b_\wp}$$

By lemma 2.16, we have

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

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

$$(N_{T/k}i)_p = \prod_{\wp|p} N_{T,\wp/k_p}i_p \text{ for } i \in I_T,$$
we have
\[ |N_{T/k}(\beta i)|_p = \prod_{\nu \mid p} |N_{T_{\nu}/k_{\nu}}(\beta i_{\nu})|_p = \prod_{\nu \mid p} |\beta i|_p = \prod_{\nu \mid p} N_{\nu}^{-b_\nu} \]
\[ = \prod_{\nu \mid p} N_{\nu}^{-f_\nu b_\nu} = N_p^{-\sum_{\nu \mid p} f_\nu b_\nu}. \]

Therefore
\[ (6) \quad \phi_{K/k}(N_{T/k}(i)) = \phi_{K/k}(N_{T/k}(\beta i)) = \prod_{p \notin F} \left( \frac{K:k}{p} \right) \sum_{\nu \mid p} f_\nu b_\nu. \]

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

**Proposition 2.20.** If \( \phi_K \) can be extended to a homomorphism of \( I_k \) to \( G(K:k) \) with closed kernel containing \( k^* \), then the kernel contains \( N_{K/k}I_K \).

**Proof.** Apply proposition 2.19 with \( T = K \). If \( i \) is in \( I_K \), we have
\[ \phi_{K/k}(N_{K/k}(i)) = \phi_{K/K}(i). \]

But \( \phi_{K/K} \) maps \( I_K \) to a trivial group \( G(K:k) \).

**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 \( Z \) is a finite cyclic extension of \( k \) then subgroup \( k^* N_{Z/k}(I_Z) \) of \( I_k \) is a closed subgroup of finite index in \( I_k \) and the index \( [I_k : k^* N_{Z/k}(I_Z)] \) is divisible by \( [Z:k] \).

**Second fundamental inequality of class field theory.** If \( K \) is a finite abelian extension of \( k \) then subgroup \( k^* N_{K/k}I_k \) is closed and of finite index in \( I_k \) and the index \( [I_k : k^* N_{K/k}(I_K)] \) divides \( [K:k] \).

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

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

Artin symbol \( \left( \frac{Z_k}{p} \right) \) is the restriction of \( \left( \frac{L_k}{p} \right) \) to \( Z \), so \( \left( \frac{Z_k}{p} \right) = 1 \). The Artin symbol \( \left( \frac{Z_k}{p} \right) \) generates the Galois group \( G(Z_\phi : k_p) \) for each prime \( \phi \) of \( Z \) that divides an unramified prime \( p \) (Chapter 1, normal extensions). Therefore if \( p \) is unramified in \( K \) then \( Z_\phi = k_p \). For each \( i \) in \( I_k \{ E \} \), this allows us to construct an idele \( j \) in \( I_Z \) such that \( N_{Z/k}(j) = i \). For each prime \( p \) not in \( E \), select one prime \( \phi(p) \) of \( Z \) which divides \( p \). Put \( j_{\phi(p)} = i_p \), and put \( j_{\phi} = 1 \) at other primes \( \phi \) dividing \( p \). At primes \( \phi \) of \( Z \) dividing \( p \) in \( E \), put \( j_{\phi} = 1 \). We have

\[
(\mathcal{N}_{Z/k}(j))_p = \prod_{\phi | p} \mathcal{N}_{Z_\phi/k_p}(j_\phi) = \begin{cases} 
\mathcal{N}_{Z_{\phi(p)}/k_p}(j_{\phi(p)}) = i_p & \text{for } p \in E \\
1 & \text{for } p \notin E 
\end{cases}
\]

Therefore \( I_k \{ E \} \) is contained in \( \mathcal{N}_{Z/k}I_Z \). Consider two homomorphisms from \( I_k \) to \( I_k/k^*\mathcal{N}_{Z/k}I_Z \). 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 \( I_k \{ E \} \). Both are continuous homomorphisms whose kernels are closed and contain \( k^* \). By proposition 2.6, the two homomorphisms are identical, so \( I_k/k^*\mathcal{N}_{Z/k}I_Z \) must be trivial. By the first fundamental inequality, degree \([ Z : k ] \) divides index \([ I_k : k^*\mathcal{N}_{Z/k}I_Z ] \), so the group \( I_k/k^*\mathcal{N}_{Z/k}I_Z \) cannot be trivial, and we have reached our contradiction. It must be that \( M \) is all of \( G(K : k) \).

**Proposition 2.22 (Corollary to the Second Fundamental Inequality).** Suppose \( K/k \) is a finite abelian extension. If \( \phi_{K/k} \) can be extended to a continuous homomorphism of \( I_k \) whose kernel contains \( k^* \), then the kernel of \( \phi_{K/k} \) is \( k^*\mathcal{N}_{K/k}I_K \).

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

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

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