CHAPTER VII

FIRST FUNDAMENTAL INEQUALITY

In this chapter, we will prove that if $\mathbf{K}$ is a finite cyclic extension of $\mathbf{k}$ then $\mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}$ is a closed subgroup of finite index in $\mathbf{I}_{\mathbf{k}}$ and $\left[\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}\right]$ is divisible by $[\mathbf{K} : \mathbf{k}]$. We begin with an algebraic lemma.

Lemma 7.1 (Herbrand's lemma). *Let L be a subgroup of finite index in abelian group J, and let $f : J \to J$ and $g : J \to J$ be two homomorphisms such that $f(L) \subset L$ and $g(L) \subset L$, and $fg = gf = 1$. Let f_1 and g_1 be the restrictions to L of f and g, respectively. If $[\ker(f_1) : Im(g_1)]$ and $[\ker(g_1) : Im(f_1)]$ are both finite then $[\ker(f) : Im(g)]$ and $[\ker(g) : Im(f)]$ are finite and*

$$\frac{[\ker(f) : Im(g)]}{[\ker(f_1) : Im(g_1)]} = \frac{[\ker(g) : Im(f)]}{[\ker(g_1) : Im(f_1)]}.$$

Proof. Consider the composite $J \xrightarrow{f} \mathrm{Im}(f) \xrightarrow{\iota} \frac{\mathrm{Im}(f)}{\mathrm{Im}(f_1)}$. If $f(j)$ is in $\mathrm{Im}(f_1)$ then $f(j) = f(\ell)$ with ℓ in L, so $j = j\ell^{-1}\ell$ is in $\ker(f)L$. Therefore $\ker(\iota f) = \ker(f)L$, and

$$\frac{J}{\ker(f)L} \simeq \frac{\mathrm{Im}(f)}{\mathrm{Im}(f_1)}.$$

Both sides are finite groups since $[J : L]$ is finite. In addition, we have

$$\frac{\ker(f)L}{L} \simeq \frac{\ker(f)}{\ker(f) \cap L} \simeq \frac{\ker(f)}{\ker(f_1)}.$$

Homomorphism g satisfies the same hypotheses as f, so we have also

$$\frac{J}{\ker(g)L} \simeq \frac{\mathrm{Im}(g)}{\mathrm{Im}(g_1)} \qquad \text{and} \qquad \frac{\ker(g)L}{L} \simeq \frac{\ker(g)}{\ker(g) \cap L} \simeq \frac{\ker(g)}{\ker(g_1)}.$$

Therefore, with every index in the following being finite, we have

$$\begin{aligned}[J : L] &= [\mathrm{Im}(f) : \mathrm{Im}(f_1)]\,[\ker(f) : \ker(f_1)] \\ &= [\mathrm{Im}(f) : \mathrm{Im}(f_1)]\,\frac{[\ker(f) : \mathrm{Im}(g_1)]}{[\ker(f_1) : \mathrm{Im}(g_1)]} \\ &= [\mathrm{Im}(f) : \mathrm{Im}(f_1)]\,[\mathrm{Im}(g) : \mathrm{Im}(g_1)]\,\frac{[\ker(f) : \mathrm{Im}(g)]}{[\ker(f_1) : \mathrm{Im}(g_1)]},\end{aligned}$$

or

$$\frac{[J:L]}{[\mathrm{Im}(f):\mathrm{Im}(f_1)]\,[\mathrm{Im}(g):\mathrm{Im}(g_1)]} = \frac{[\ker(f):\mathrm{Im}(g)]}{[\ker(f_1):\mathrm{Im}(g_1)]}.$$

The left side is symmetric in f and g so we have the desired result,

$$\frac{[\ker(f):\mathrm{Im}(g)]}{[\ker(f_1):\mathrm{Im}(g_1)]} = \frac{[\ker(g):\mathrm{Im}(f)]}{[\ker(g_1):\mathrm{Im}(f_1)]}.$$

LEMMA 7.2 (HILBERT'S THEOREM 90). *Let* $\mathbf{Z}/\mathbf{F}$ *be a finite cyclic extension of degree* n *with Galois group generated by* σ. *If* α *in* $\mathbf{Z}^*$ *satisfies* $\alpha^{1+\sigma+\cdots+\sigma^{n-1}} = 1$ *then there exists* β *in* $\mathbf{Z}^*$ *such that* $\alpha = \beta^{1-\sigma}$.

PROOF. Suppose that $\mathbf{Z} = \mathbf{F}(\theta)$. Put $\theta_i = \theta^{\sigma^i}$. Then $\theta_i^\sigma = \theta_{i+1}$ for $0 \le i < n-1$, and $\theta_{n-1}^\sigma = \theta = \theta_0$. Put $\alpha_0 = 1$, $\alpha_1 = \alpha$, ..., $\alpha_i = \alpha^{1+\sigma+\cdots+\sigma^{i-1}}$ for $1 \le i \le n-1$. Then $\alpha\alpha_i^\sigma = \alpha_{i+1}$ for $0 \le i < n-1$, and $\alpha\alpha_{n-1}^\sigma = \alpha^{1+\sigma+\cdots+\sigma^{n-1}} = 1 = \alpha_0$. Finally, put

$$\beta_j = \alpha_0\theta_0^j + \alpha_1\theta_1^j + \cdots + \alpha_{n-1}\theta_{n-1}^j \quad \text{for } 0 \le j < n.$$

Then $\alpha\beta_j^\sigma = \beta_j$. The n elements $\theta_0, \ldots, \theta_{n-1}$ are all distinct (otherwise θ would have fewer than n conjugates, which is impossible), so the Vandermonde matrix $\left(\theta_i^j\right)$ is non-singular. Therefore $\beta_j \neq 0$ for at least one value of j, and we have $\alpha = \beta_j/\beta_j^\sigma = \beta_j^{1-\sigma}$ as desired.

Computation of $[\mathbf{k}_p^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*]$ for cyclic extensions. In the proof of the first fundamental inequality for cyclic extensions, we begin by showing that $[\mathbf{k}_p^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*] = [\mathbf{K}_\wp : \mathbf{k}_p]$, and we will need only that local extension $\mathbf{K}_\wp/\mathbf{k}_p$ is cyclic. Let $[\mathbf{K}_\wp : \mathbf{k}_p] = n = ef$, where $p\mathbf{O}_\wp = \wp^e$ and $\mathrm{N}\wp = \mathrm{N}p^f$. Let principal ideals $\wp$ and p be generated by elements Π in $\mathbf{O}_\wp$ and π in $\mathbf{o}_p$, respectively. Denote the unit group $\mathbf{O}_\wp^*$ by $\mathbf{U}_\wp$ and the unit group $\mathbf{o}_p^*$ by $\mathbf{u}_p$. The index $[\mathbf{k}_p^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*]$ is the product of two factors.

$$(7.1) \qquad [\mathbf{k}_p^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*] = [\mathbf{k}_p^* : \mathbf{u}_p\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*][\mathbf{u}_p\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*]$$

We will show that the first factor of the right side is f and the second factor is e.

Computation of the first factor. Since $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}(\Pi) = (\pi)^f$, we have $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\Pi = \mu\pi^f$ where μ is in $\mathbf{u}_p$. Then $\mathbf{K}_\wp^* = \mathbf{U}_\wp\langle\Pi\rangle$, so $\mathbf{u}_p\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = \mathbf{u}_p\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{U}_\wp\langle\pi^f\rangle = \mathbf{u}_p\langle\pi^f\rangle$. We also have $\mathbf{k}_p^* = \mathbf{u}_p\langle\pi\rangle$, so

$$(7.2) \quad [\mathbf{k}_p^* : \mathbf{u}_p\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*] = [\mathbf{u}_p\langle\pi\rangle : \mathbf{u}_p\langle\pi^f\rangle]$$
$$= [\langle\pi\rangle : \mathbf{u}_p\langle\pi^f\rangle \cap \langle\pi\rangle] = [\langle\pi\rangle : \langle\pi^f\rangle] = f.$$

Computation of the second factor. We have

$$[\mathbf{u}_p \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*] = [\mathbf{u}_p : \mathbf{u}_p \cap \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*] = [\mathbf{u}_p : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{U}_\wp]. \tag{7.3}$$

To compute $[\mathbf{u}_p : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{U}_\wp]$, we apply Herbrand's lemma with $J = \mathbf{U}_\wp$, and homomorphisms $f : J \to J$ and $g : J \to J$ defined by $f(\alpha) = \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha = \alpha^{1+\sigma+\cdots+\sigma^{n-1}}$ and $g(\beta) = \beta^{1-\sigma}$. Then $\ker(g) = \left\{\beta \in \mathbf{U}_\wp \mid \beta/\beta^\sigma = 1\right\} = \mathbf{U}_\wp \cap \mathbf{k}_p^* = \mathbf{u}_p$, and $\mathrm{Im}(f) = \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{U}_\wp$. Lemma 7.1 (Herbrand's) asserts that

$$\left[\mathbf{u}_p : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{U}_\wp\right] = [\ker(g) : \mathrm{Im}(f)] = \frac{[\ker(f) : \mathrm{Im}(g)]\,[\ker(g_1) : \mathrm{Im}(f_1)]}{[\ker(f_1) : \mathrm{Im}(g_1)]}. \tag{7.4}$$

It remains to choose L and compute the three indices on the right side of (7.1)

Computation of $[\ker(f) : Im(g)]$. We have

$$\mathrm{Im}(g) = \left\{\alpha \in \mathbf{U}_p \;\middle|\; \alpha = \beta^{1-\sigma} \text{ with } \beta \in \mathbf{U}_\wp\right\},$$

and, by lemma 7.2,

$$\ker(f) = \left\{\alpha \in \mathbf{U}_\wp \;\middle|\; \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha = 1\right\} = \left\{\alpha \in \mathbf{U}_\wp \;\middle|\; \alpha = \beta^{1-\sigma} \text{ with } \beta \in \mathbf{K}_\wp^*\right\}.$$

Let $g' : \mathbf{K}_\wp^* \to \mathbf{K}_\wp^*$ be the map $g'(\alpha) = \alpha^{1-\sigma}$. Then $\ker(f) = \mathrm{Im}(g')$, and $\mathrm{Im}(g) = g(\mathbf{U}_\wp) = g'(\mathbf{k}_p^*\mathbf{U}_\wp)$. Both rows are exact in the following commutative diagram.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbf{k}_p^* & \longrightarrow & \mathbf{K}_\wp^* & \xrightarrow{g'} & \ker(f) & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & \mathbf{k}_p^* & \longrightarrow & \mathbf{k}_p^*\mathbf{U}_\wp & \xrightarrow{g'} & \mathrm{Im}(g) & \longrightarrow & 1
\end{array}$$

We have $[\ker(f) : \mathrm{Im}(g)] = \left[\mathbf{K}_\wp^* : \mathbf{k}_p^*\mathbf{U}_\wp\right] = [\mathbf{U}_\wp\langle\Pi\rangle : \mathbf{U}\wp\langle\pi\rangle] = [\langle\Pi\rangle : \langle\Pi^e\rangle]$, and therefore

$$[\ker(f) : \mathrm{Im}(g)] = e. \tag{7.5}$$

Choice of subgroup L. By the normal basis theorem, there exists an element θ in $\mathbf{K}_\wp$ so that $\theta, \theta^\sigma, \ldots, \theta^{\sigma^{n-1}}$ is a basis of $\mathbf{K}_\wp$ over $\mathbf{k}_p$. If α is in $\mathbf{k}_p^*$ then $\alpha\theta, \alpha\theta^\sigma, \ldots, \alpha\theta^{\sigma^{n-1}}$ is also a basis, so we can assume that $\mathrm{ord}_\wp(\theta^{\sigma^j}) > \frac{b}{q-1}$, where b is as defined in lemma 4.8, and q is the *rational* prime which p divides. Put

$$M = \mathbf{o}_p\theta + \mathbf{o}_p\theta^\sigma + \cdots + \mathbf{o}_p\theta^{\sigma^{n-1}}.$$

Then $exp(x)$ is defined on M and maps M isomorphically onto a subgroup L of $\mathbf{U}_\wp$, where

$$L = \exp(M) = \left\{ y \in \mathbf{U}_\wp \;\middle|\; \operatorname{ord}_\wp(y-1) > \frac{b}{q-1} \right\}.$$

If m is sufficiently large, we will show that M contains $\wp^{em}$. Let $x_1, \ldots, x_n$ be a basis for $\mathbf{O}_\wp$ over $\mathbf{o}_p$. Then $x_i = \sum_{j=0}^{n-1} \beta_{ij}\theta^{\sigma^j}$ for $1 \le i \le n$, with β_{ij} in $\mathbf{o}_p$. There is a constant c_0 so that $\operatorname{ord}_p(\beta_{ij}) > -c_0$ for $0 \le j < n$ and $1 \le i \le n$. If x is in $\wp^{em} = (\Pi^{em}) = \pi^m \mathbf{O}_\wp$ then $x = \sum_{i=1}^n \alpha_i \pi^m x_i = \sum_{i=1}^n \sum_{j=0}^{n-1} \alpha_i \pi^m \beta_{ij}\theta^{\sigma^j} = \sum_{j=0}^{n-1} \gamma_j \theta^{\sigma^j}$, where α_i is in $\mathbf{o}_p$, $1 \le i \le n$, and $\gamma_j = \sum_{j=0}^{n-1} \alpha_i \pi^m \beta_{ij}$. We have

$$\operatorname{ord}_p(\gamma_j) \ge \min\big(\operatorname{ord}(\alpha_i \pi^m \beta_{ij})\big) > m - c_0.$$

If we take $m \ge c_0$ then the γ_j are all in $\mathbf{o}_p$, so x is in M, and $\wp^{em} \subset M \subset \mathbf{O}_\wp$. Since $[\mathbf{O}_\wp : \wp^{em}]$ is finite, we see that $[M : \wp^{em}]$ is finite. Since $\wp^{em}$ is mapped isomorphically onto $1 + \wp^{em}$ by the exponential function, then $[L : 1 + \wp^{em}]$ is finite.

$$\begin{array}{ccc}
\mathbf{O}_\wp & & \mathbf{U}_\wp \\
\uparrow & & \uparrow \\
M & \xrightarrow{\exp} & L \\
\uparrow & & \uparrow \\
\wp^{em} & \xrightarrow{\exp} & 1 + \wp^{em}
\end{array}$$

We can carry out the computation of $[\ker(g_1) : \operatorname{Im}(f_1)]$ and $[\ker(f_1) : \operatorname{Im}(g_1)]$ in M. Since $M^\sigma = M$, we can define $\tilde{f}_1 : M \to M$ by $\tilde{f}(x) = x + x^\sigma + \cdots + x^{\sigma^{n-1}}$, and $\tilde{g}_1 : M \to M$ by $\tilde{g}(y) = y - y^\sigma$. Each automorphism of $\mathbf{K}_\wp/\mathbf{k}_p$ is an isometry, so if $\lim_{n\to\infty} \alpha_n = \alpha$ then we have $|\alpha_n - \alpha|_\wp = |\alpha_n^\sigma - \alpha^\sigma|_\wp$, so $\lim_{n\to\infty} \alpha_n^\sigma = \alpha^\sigma$. Therefore $\exp(x^\sigma) = \big(\exp(x)\big)^\sigma$. We have

$$\begin{aligned}
\exp\big(\tilde{f}_1(\alpha)\big) = \exp\Big(x + x^\sigma + \cdots + x^{\sigma^{n-1}}\Big) &= \exp(x)\exp(x^\sigma)\ldots\exp\big(x^{\sigma^{n-1}}\big) \\
&= \exp(x)\exp(x)^\sigma \ldots \exp(x)^{\sigma^{n-1}} = f_1\big(\exp(\alpha)\big)
\end{aligned}$$

Likewise, we have $\exp\big(\tilde{g}_1(y)\big) = g_1\big(\exp(y)\big)$. Since exp is an isomorphism, we have

$$\begin{aligned}
&[\ker(f_1) : \operatorname{Im}(g_1)] = [\ker(\tilde{f}_1) : \operatorname{Im}(\tilde{g}_1)] \\
(7.6)\qquad &[\ker(g_1) : \operatorname{Im}(f_1)] = [\ker(\tilde{g}_1) : \operatorname{Im}(\tilde{f}_1)].
\end{aligned}$$

Computation of $[\ker(f_1) : Im(g_1)]$. Let x be in M. Then $x = \sum_{i=0}^{n-1} \alpha_i \theta^{\sigma^i}$, with α_i in $\mathbf{o}_p$. We have

$$\text{(7.7)} \quad \tilde{f}_1(x) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} \alpha_i \theta^{\sigma^i} \right)^{\sigma^j} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \alpha_i \theta^{\sigma^{i+j}}$$
$$= \left(\sum_{i=0}^{n-1} \alpha_i \right) \left(\sum_{k=0}^{n-1} \theta^{\sigma^k} \right) = \left(\sum_{i=0}^{n-1} \alpha_i \right) \mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p} \theta.$$

If $\mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p} \theta = 0$, then replace θ with $\theta + 1$, which also generates a cyclic basis and $\mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p}(\theta + 1) \neq 0$. Therefore $\ker(\tilde{f}_1) = \left\{ x \in M \mid \sum_{i=0}^{n-1} \alpha_i = 0 \right\}$.

For $y = \sum_{j=0}^{n-1} \beta_j \theta^{\sigma^j}$, we have $\tilde{g}_1(y) = \tilde{g}_1 \left(\sum_{j=0}^{n-1} \beta_j \theta^{\sigma^j} \right) = \left(\sum_{j=0}^{n-1} \beta_j \theta^{\sigma^j} \right) - \left(\sum_{j=0}^{n-1} \beta_j \theta^{\sigma^{j+1}} \right)$, so

$$\text{(7.8)} \quad \tilde{g}_1(y) = (\beta_0 - \beta_{n-1})\theta + (\beta_1 - \beta_0)\theta^\sigma + \cdots + (\beta_{n-1} - \beta_{n-2})\theta^{\sigma^{n-1}}.$$

We show $\ker(\tilde{f}_1) \subset \operatorname{Im}(\tilde{g}_1)$. If $\sum_{i=0}^{n-1} \alpha_i = 0$, put $\beta_0 = \alpha_0$, $\beta_1 = \alpha_0 + \alpha_1$, $\ldots$, $\beta_{n-1} = \alpha_0 + \cdots + \alpha_{n-1} = 0$. Then

$$\beta_0 - \beta_{n-1} = \alpha_0, \quad \beta_1 - \beta_0 = \alpha_1, \quad \ldots, \quad \beta_{n-1} - \beta_{n-2} = \alpha_{n-1},$$

so

$$\text{(7.9)} \quad [\ker(\tilde{f}_1) : \operatorname{Im}(\tilde{g}_1)] = 1.$$

Computation of $[\ker(\tilde{g}_1) : Im(\tilde{f}_1]$. By (7.8), we have $\tilde{g}_1(y) = 0$ if and only if $\beta_0 = \beta_{n-1}$, $\beta_1 = \beta_0, \ldots$, $\beta_{n-1} = \beta_{n-2}$, so $\ker(\tilde{g}_1) = \mathbf{o}_p \left(\sum_{j=1}^{n-1} \theta^{\sigma^j} \right)$. Comparison with (7.7) shows that $\operatorname{Im}(\tilde{f}_1)$ is the same set. Therefore

$$\text{(7.10)} \quad [\ker(\tilde{g}_1) : \operatorname{Im}(\tilde{f}_1)] = 1.$$

Proposition 7.3. *If extension $\mathbf{K}_\wp/\mathbf{k}_p$ is normal with cyclic Galois group, then* $\left[\mathbf{u}_p : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p} \mathbf{U}_\wp \right] = e$.

Proof. Using (7.6), substituting the results of (7.5), (7.9) and (7.10) into the right side of (7.4), we obtain

$$\text{(7.11)} \quad \left[\mathbf{u}_p : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p} \mathbf{U}_\wp \right] = e.$$

Remark. Lemma 4.7 was the unramified case of lemma 7.3.

PROPOSITION 7.4. *If extension $\mathbf{K}_\wp/\mathbf{k}_p$ is normal with cyclic Galois group, then $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}}\mathbf{K}_\wp^*$ is an open subgroup of $\mathbf{k}_p^*$ and $\left[\mathbf{k}_p^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*\right] = n$.*

PROOF. Applying the results of (7.2), (7.3) and (7.11) to the right side of (7.1) produces

$$\left[\mathbf{k}_p^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}}\mathbf{K}_\wp^*\right] = ef = n.$$

LEMMA 7.5. *If $\mathbf{i}$ is an idele in $\mathbf{I_k}$ and $G(\mathbf{K} : \mathbf{k})$ is abelian then $\mathbf{i}$ is in $\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I_K}$ if and only if $\mathbf{i}_p$ is in $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp$ for every prime p of $\mathbf{k}$ and some prime $\wp$ of $\mathbf{K}$ dividing p.*

PROOF. Suppose that for every p we have $\mathbf{i}_p = \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha_\wp$ for $\alpha_\wp$ in $\mathbf{K}_\wp^*$ for some $\wp$ dividing p. This gives a set U of primes of $\mathbf{K}$. Let $\mathbf{j}$ in $\mathbf{I_K}$ have components $\mathbf{j}_\wp = \alpha_\wp$ for $\wp$ in U and $\mathbf{j}_\wp = 1$ for $\wp$ not in U. Then $\prod_{\wp|p} \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{j}_\wp = \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha_\wp = \mathbf{i}_p$ for each p, so $\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{j} = \mathbf{i}$.

Conversely, suppose that $\mathbf{i} = \mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{j}$ for some $\mathbf{j}$ in $\mathbf{I_K}$. Then $\mathbf{i}_p = \prod_{\wp|p} \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{j}_\wp$ for each p. Let the primes of $\mathbf{K}$ dividing p be $\wp_1, \ldots, \wp_g$. For abelian extensions, the splitting groups $S_{\wp_i}$ all coincide, so put $S_p = S_{\wp_j}$. (Chapter I, *Splitting groups and inertial groups in normal extensions.*) Let $\sigma_1, \ldots, \sigma_g$ be a set of coset representatives for splitting group S_p in $G(\mathbf{K} : \mathbf{k})$. Then $\wp_1^{\sigma_j} = \wp_j$, and $\sigma_j : \mathbf{K}_{\wp_1} \to \mathbf{K}_{\wp_j}$ is an isomorphism. Put $\tau_j = \sigma_j^{-1}$. Then $\wp_j^{\tau_j} = \wp_1$ and $\tau_j : \mathbf{K}_{\wp_j} \to \mathbf{K}_{\wp_1}$ is an isomorphism, and we have

$$\mathbf{N}_{\mathbf{K}_{\wp_j}/\mathbf{k}_p}\mathbf{j}_{\wp_j} = \left(\mathbf{N}_{\mathbf{K}_{\wp_j}/\mathbf{k}_p}\mathbf{j}_{\wp_j}\right)^{\tau_j} = \prod_{\sigma\in S(p)} \left(\mathbf{j}_{\wp_j}^{\sigma}\right)^{\tau_j} = \prod_{\sigma\in S(p)} \left(\mathbf{j}_{\wp_j}^{\tau_j}\right)^{\sigma} = \mathbf{N}_{\mathbf{K}_{\wp_1}/\mathbf{k}_p}\mathbf{j}_{\wp_j}^{\tau_j},$$

and $\mathbf{i}_p = \prod_{j=1}^g \mathbf{N}_{\mathbf{K}_{\wp_j}/\mathbf{k}_p}\mathbf{j}_{\wp_j} = \prod_{j=1}^g \mathbf{N}_{\mathbf{K}_{\wp_1}/\mathbf{k}_p}\mathbf{j}_{\wp_j}^{\tau_j} = \mathbf{N}_{\mathbf{K}_{\wp_1}/\mathbf{k}_p}\left(\prod_{j=1}^g \mathbf{j}_{\wp_j}^{\tau_j}\right)$, showing that $\mathbf{i}_p$ is in $\mathbf{N}_{\mathbf{K}_{\wp_1}/\mathbf{k}_p}\mathbf{K}_{\wp_1}$.

LEMMA 7.6. *$\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I_K}$ is an open subgroup of $\mathbf{I_k}$.*

PROOF. If p is a ramified finite prime in $\mathbf{K}$ then by lemma 4.14 there is an integer m_p so that

$$W_p'(m_p) = \left\{\alpha \in \mathbf{k}_p^* \;\middle|\; \operatorname{ord}_p(\alpha) > m_p\right\} \subset \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*.$$

If p is an unramified finite prime, then every unit of $\mathbf{o}_p$ is a norm by lemma 4.7, so $W_p'(0) = \mathbf{u}_p \subset \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$; set $m_p = 0$. If p is a real infinite prime, then $W_p'(1) \subset \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$; set $m_p = 1$. For a complex infinite prime, set $m_p = 0$. Then $\prod_p W_p'(m_p)$ is an basic open neighborhood contained in $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$.

LEMMA 7.7. *If* $\mathbf{J}$ *is an open subgroup of* $\mathbf{I}_k$ *so that* $\mathbf{I}_k = \mathbf{J}\mathbf{I}^0_{\mathbf{k}}$ *then* $\mathbf{k}^*\mathbf{J}$ *is a subgroup of finite index in* $\mathbf{I}_{\mathbf{k}}$.

PROOF. We have

$$\frac{\mathbf{I}_{\mathbf{k}}}{\mathbf{k}^*\mathbf{J}} = \frac{\mathbf{k}^*\mathbf{J}\mathbf{I}^0_{\mathbf{k}}}{\mathbf{k}^*\mathbf{J}} \simeq \frac{\mathbf{I}^0_{\mathbf{k}}}{\mathbf{k}^*\mathbf{J}\cap\mathbf{I}^0_{\mathbf{k}}} \simeq \frac{\mathbf{I}^0_{\mathbf{k}}/\mathbf{k}^*}{\left(\mathbf{k}^*\mathbf{J}\cap\mathbf{I}^0_{\mathbf{k}}\right)/\mathbf{k}^*}.$$

$\mathbf{J}$ is open, so $\mathbf{k}^*\mathbf{J} = \cup_{\alpha\in\mathbf{k}^*}\mathbf{J}$ is open. Therefore $\mathbf{k}^*\mathbf{J}\cap\mathbf{I}^0_{\mathbf{k}}$ is an open subgroup of $\mathbf{I}^0_{\mathbf{k}}$, and $\left(\mathbf{k}^*\mathbf{J}\cap\mathbf{I}^0_{\mathbf{k}}\right)/\mathbf{k}^*$ is open in the quotient topology. We have an open covering of $\mathbf{I}^0_{\mathbf{k}}/\mathbf{k}^*$, which is compact by Proposition 6.9; therefore $\mathbf{I}^0_{\mathbf{k}}/\mathbf{k}^*$ is covered by a finite number of cosets of $\left(\mathbf{k}^*\mathbf{J}\cap\mathbf{I}^0_{\mathbf{k}}\right)/\mathbf{k}^*$.

LEMMA 7.8. *If* $\mathbf{K}/\mathbf{k}$ *is abelian then* $\mathbf{I}_{\mathbf{k}} = \left(\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}\right)\mathbf{I}^0_{\mathbf{k}}$.

PROOF. Choose one infinite prime p_0 of $\mathbf{k}$ and one infinite prime $\wp_0$ of $\mathbf{K}$ which divides p_0. Given $\mathbf{i}$ in $\mathbf{I}_{\mathbf{k}}$, define ideles $\mathbf{i}'$ and $\mathbf{i}''$ of $\mathbf{I}_{\mathbf{k}}$ as follows. At primes p such that $p \neq p_0$, put $\mathbf{i}'_p = \mathbf{i}_p$ and $\mathbf{i}''_p = 1$. Put $\mathbf{i}'_{p_0} = \mathbf{i}_{p_0}/c$ and $\mathbf{i}''_{p_0} = c$, where c in $\mathbf{k}_{p_0}$ satisfies $|c|_{p_0} = |\mathbf{i}|$. (If p_0 is real and $\sigma : \mathbf{k}_{p_0} \simeq \mathbf{R}$, choose c so that $\sigma(c) = |\mathbf{i}|$; if p_0 is complex and $\sigma : \mathbf{k}_{p_0} \simeq \mathbf{C}$, choose c so that $\sigma(c) = \sqrt{|\mathbf{i}|}$, taking the positive real square root.) Then $\mathbf{i} = \mathbf{i}'\mathbf{i}''$. To show that $|\mathbf{i}'|$ is in $\mathbf{I}^0_{\mathbf{k}}$, consider

$$|\mathbf{i}'| = \left(\prod_{p\neq p_0}|\mathbf{i}'|_p\right)|\mathbf{i}'|_{p_0} = \left(\prod_{p\neq p_0}|\mathbf{i}|_p\right)\left(\frac{|\mathbf{i}_{p_0}|_{p_0}}{|c|_{p_0}}\right) = \frac{|\mathbf{i}|}{|c|_{p_0}} = 1.$$

We have $|c|_{p_0} = |\sigma(c)| = |\mathbf{i}|$ if p_0 is real, and $|c|_{p_0} = |\sigma(c)|^2 = |\mathbf{i}|$ if p_0 is complex. To show that $\mathbf{i}''$ is in $\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}$, for $p \neq p_0$ we have $\mathbf{i}''_p = 1 \in \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}^*_\wp$, and $\mathbf{i}''_{p_0} = c$. Since $\sigma(c) > 0$, then c is in $\mathbf{N}_{\mathbf{K}_{\wp_0}/\mathbf{k}_{p_0}}\mathbf{K}_{\wp_0}$. By lemma 7.5, $\mathbf{i}'' \in \mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_K$, and we have shown $\mathbf{i} \in \left(\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}\right)\mathbf{I}^0_{\mathbf{k}}$.

COROLLARY 7.9. $\mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}$ *is a subgroup of finite index in* $\mathbf{I}_{\mathbf{k}}$.

LEMMA 7.10. *For any finite set* E *of primes of* $\mathbf{k}$ *containing the infinite primes, let*

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

Then $\mathbf{k}^*\mathbf{I}_{\mathbf{k}}(E)$ *is a subgroup of finite index in* $\mathbf{I}_{\mathbf{k}}$.

PROOF. By lemma 7.7, we need to show that $\mathbf{I}_k(E)$ is open and $\mathbf{I}_{\mathbf{k}} = \mathbf{I}_{\mathbf{k}}(E)\mathbf{I}^0_{\mathbf{k}}$. We have $\prod_p W'(0) \subset \mathbf{I}_{\mathbf{k}}(E)$, so $\mathbf{I}_{\mathbf{k}}(E)$ is open. For the other requirement, let $\mathbf{i}$ be in $\mathbf{I}_{\mathbf{k}}$. choose one infinite prime p_0. Define ideles $\mathbf{i}'$, $\mathbf{i}''$, and c in $\mathbf{k}_{p_0}$ as in the proof of lemma 7.8. Then $\mathbf{i} = \mathbf{i}''\mathbf{i}'$, $\mathbf{i}'$ is in $\mathbf{I}^0_{\mathbf{k}}$, and $\mathbf{i}''$ is in $\mathbf{I}_{\mathbf{k}}(E)$. Therefore $\mathbf{I}_{\mathbf{k}} \subset \mathbf{I}_{\mathbf{k}}(E)\mathbf{I}^0_{\mathbf{k}}$.

Lemma 7.11. *Let E be a finite set of primes of $\mathbf{k}$ containing the infinite primes. There exists a finite set F of primes such that $E \subset F$ and $\mathbf{I_k} = \mathbf{k}^*\mathbf{I_k}(F)$.*

Proof. By lemma 7.10, $\mathbf{k}^*\mathbf{I_k}(E)$ is a subgroup of finite index in $\mathbf{I_k}$, so there are ideles $\mathbf{i}_1, \ldots, \mathbf{i}_r$ such that $\mathbf{I_k} = \cup_{j=1}^r \mathbf{k}^*\mathbf{I_k}(E)\mathbf{i}_j$. Let F consist of the primes in E and all primes such that $|\mathbf{i}_j|_p \neq 1$ for $1 \leq j \leq r$. Then F is a finite set of primes, and $\mathbf{I_k}(E)\mathbf{i}_j \subset \mathbf{I_k}(F)$. Therefore $\mathbf{I_k} \subset \mathbf{k}^*\mathbf{I_k}(F)$.

Lemma 7.12. *Let H_1, H_2 and H_3 be subgroups of abelian group H. If $H_1 \subset H_3$ then*

$$\frac{H_1H_2}{H_3} \simeq \frac{H_2}{H_2 \cap H_3}.$$

Proof. The natural homomorphism $H_2 \to (H_1H_2)/H_3$ is onto and the kernel is $H_2 \cap H_3$. (Note: the case in which $H_1 = H_3$ has been used on several occasions.)

Computation of $[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}I_K}]$. $\mathbf{K}$ is a finite cyclic extension of $\mathbf{k}$ of degree n. Let σ be a generator of Galois group $G(\mathbf{K} : \mathbf{k})$. Let E be a set of primes of $\mathbf{k}$ that contains all infinite primes, all primes that are ramified in $\mathbf{K}$, and primes such that $\mathbf{I_k} = \mathbf{k}^*\mathbf{I_k}(E)$. Let E' be a set of primes of $\mathbf{K}$ containing all primes that divide a prime of E and such that $\mathbf{I_K} = \mathbf{K}^*\mathbf{I_K}(E')$. Add to E all primes of $\mathbf{k}$ that are divisible by a prime of E'. Then add to E' primes that divide a prime in E. (Now E' is closed under that action $\wp \to \wp^\sigma$, and if $\wp$ divides p then $\wp \in E'$ if and only if $p \in E$.) Since $\mathbf{N_{K/k}K}^* \subset \mathbf{k}^*$, we have

$$[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}I_K}] = [\mathbf{k}^*\mathbf{I_k}(E) : \mathbf{k}^*\mathbf{N_{K/k}}(\mathbf{K}^*\mathbf{I_K}(E'))] = [\mathbf{k}^*\mathbf{I_k}(E) : \mathbf{k}^*\mathbf{N}(\mathbf{I_K}(E'))].$$

Using lemma 7.12, we obtain

$$[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}I_K}] = [\mathbf{I_k}(E) : \mathbf{k}^*\mathbf{N_{K/k}}(\mathbf{I_K}(E')) \cap \mathbf{I_k}(E)].$$

Since $\mathbf{N_{K/k}}(\mathbf{I_K}(E')) \subset \mathbf{I_k}(E)$, we have

$$[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}I_K}] = \frac{[\mathbf{I_k}(E) : \mathbf{N_{K/k}}(\mathbf{I_K}(E'))]}{[\mathbf{k}^*\mathbf{N_{K/k}}(\mathbf{I_K}(E')) \cap \mathbf{I_k}(E) : \mathbf{N_{K/k}}(\mathbf{I_K}(E'))]}.$$

Again, since $\mathbf{N_{K/k}}(\mathbf{I_K}(E')) \subset \mathbf{I_k}(E)$, we have

$$\mathbf{k}^*\mathbf{N_{K/k}}(\mathbf{I_K}(E')) \cap \mathbf{I_k}(E) = \mathbf{k}^*(E)\mathbf{N_{K/k}}(\mathbf{I_K}(E')),$$

where $\mathbf{k}^*(E) = \mathbf{k}^* \cap \mathbf{I_k}(E)$ is the group of E-units of $\mathbf{k}$. Therefore

$$[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}I_K}] = \frac{[\mathbf{I_k}(E) : \mathbf{N_{K/k}}(\mathbf{I_K}(E'))]}{[\mathbf{k}^*(E)\mathbf{N_{K/k}}(\mathbf{I_K}(E')) : \mathbf{N_{K/k}}(\mathbf{I_K}(E'))]}. \tag{7.12}$$

We need to compute the numerator and the denominator of (7.12).

The numerator of (7.12). We have a map $\prod_{p\in E}\mathbf{k}_p^* \to \mathbf{I_k}(E)$, and we can identify an element of $\prod_{p\in E}\mathbf{k}_p^*$ with its image in $\mathbf{I_k}(E)$. Define $\mathbf{I_k}\{E\}$ to be

$$\mathbf{I_k}\{E\} = \left\{\mathbf{i}\in\mathbf{I_k}\ \middle|\ \mathbf{i}_p = 1 \text{ for } p\in E\right\}.$$

Then

$$\mathbf{I_k}(E) = \left(\prod_{p\in E}\mathbf{k}_p^*\right)(\mathbf{I_k}(E)\cap\mathbf{I_k}\{E\}).$$

By lemma 4.7 and lemma 7.5, we have $(\mathbf{I_k}(E)\cap\mathbf{I_k}\{E\})\subset\mathbf{N_{K/k}}\mathbf{I_K}(E')$, so

$$\mathbf{I_k}(E) = \left(\prod_{p\in E}\mathbf{k}_p^*\right)\mathbf{N_{K/k}}\mathbf{I_K}(E'). \tag{7.13}$$

Substituting (7.13) into the numerator of (7.12) gives

$$\left[\mathbf{I_k}(E):\mathbf{N_{K/k}}\big(\mathbf{I_K}(E')\big)\right] = \left[\left(\prod_{p\in E}\mathbf{k}_p^*\right)\mathbf{N_{K/k}}\mathbf{I_K}(E'):\mathbf{N_{K/k}}\mathbf{I_K}(E')\right].$$

Applying lemma 7.12, we have

$$\left[\mathbf{I_k}(E):\mathbf{N_{K/k}}\big(\mathbf{I_K}(E')\big)\right] = \left[\left(\prod_{p\in E}\mathbf{k}_p^*\right):\left(\prod_{p\in E}\mathbf{k}_p^*\right)\cap\mathbf{N_{K/k}}\big(\mathbf{I_K}(E')\big)\right].$$

For each p in E, choose one $\wp$ in E' that divides p. By lemma 7.5, we have

$$\left(\prod_{p\in E}\mathbf{k}_p^*\right)\cap\mathbf{N_{K/k}}\big(\mathbf{I_K}(E')\big) = \prod_{p\in E}\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*.$$

Therefore

$$\begin{aligned}\left[\mathbf{I_k}(E):\mathbf{N_{K/k}}\big(\mathbf{I_K}(E')\big)\right] &= \left[\left(\prod_{p\in E}\mathbf{k}_p^*\right):\prod_{p\in E}\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*\right]\\ &= \prod_{p\in E}\left[\mathbf{k}_p^*:\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*\right]\end{aligned}$$

The degree $n_p = [\mathbf{K}_\wp : \mathbf{k}_p]$ does not depend of the choice of $\wp$, so we obtain the following formula for the numerator of (7.12).

$$\left[\mathbf{I_k}(E):\mathbf{N_{K/k}}\big(\mathbf{I_K}(E')\big)\right] = \prod_{p\in E} n_p \tag{7.14}$$

The denominator of (7.12). Applying lemma 7.12 to the denominator, we have

$$\big[\mathbf{k}^*(E)\mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{I}_{\mathbf{K}}(E')\big) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{I}_{\mathbf{K}}(E')\big)\big] = \big[\mathbf{k}^*(E) : \mathbf{k}^*(E) \cap \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{I}_{\mathbf{K}}(E')\big)\big],$$

from which we obtain

$$(7.15)\quad \big[\mathbf{k}^*(E)\mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{I}_{\mathbf{K}}(E')\big) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{I}_{\mathbf{K}}(E')\big)\big] = \frac{\big[\mathbf{k}^*(E) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{K}(E')\big)\big]}{\big[\mathbf{k}^*(E) \cap \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{I}_{\mathbf{K}}(E')\big) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{K}(E')\big)\big]}.$$

Substituting (7.14) and (7.15) into (7.12) gives the following formula.

$$(7.16)\quad [\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}] = \left(\frac{\prod_{p\in E} n_p}{\big[\mathbf{k}^*(E) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{K}(E')\big)\big]}\right)\big[\mathbf{k}^*(E) \cap \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{I}_{\mathbf{K}}(E')\big) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{K}(E')\big)\big]$$

Computation of $\big[\mathbf{k}^*(E) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{K}(E')\big)\big]$. By the unit theorem 6.13, if E contains $s+1$ primes $p_0, \ldots, p_s$ then $\mathbf{k}^*(E)$ is the product of a finite group and a free abelian group on s generators. Each prime p_i is divisible by g_i primes of $\mathbf{K}$. The number of primes in E' is $s'+1 = \sum_{i=1}^{s} g_i$, and $\mathbf{K}^*(E')$ is the product of a finite group and a free abelian group on s' generators.

If $\wp$ is a prime of $\mathbf{K}$ dividing prime p of $\mathbf{k}$, then $\wp$ is in E' if and only if p is in E. Therefore

$$\mathbf{k}^*(E) = \big\{\alpha \in \mathbf{K}^*(E') \;\big|\; \alpha^\tau = \alpha \text{ for } \tau \in G[\mathbf{K} : \mathbf{k}]\big\}.$$

The cyclic Galois group $G(\mathbf{K} : \mathbf{k})$ is generated by σ, so

$$(7.17)\qquad \mathbf{k}^*(E) = \big\{\alpha \in \mathbf{K}^*(E') \;\big|\; \alpha^\sigma = \alpha\big\} = \big\{\alpha \in \mathbf{K}^*(E') \;\big|\; \alpha^{1-\sigma} = 1\big\}.$$

We will apply Herbrand's lemma with $J = \mathbf{K}^*(E')$. Note that $\mathbf{K}^*(E')^\sigma \subset \mathbf{K}^*(E')$ since $\wp^\sigma \in E'$ if and only if $\wp \in E'$. Put $g : \mathbf{K}^*(E') \to \mathbf{K}^*(E')$ by $g(\alpha) = \alpha^{1-\sigma}$. Put $f : \mathbf{K}^*(E') \to \mathbf{K}^*(E')$ by $f(\alpha) = \mathbf{N}_{\mathbf{K}/\mathbf{k}}\alpha = \alpha^{1+\sigma+\cdots+\sigma^{n-1}}$. Then $fg = gf = 1$, so the requirements of Herbrand's lemma are met. We have $\mathrm{Im}(f) = \mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{K}^*(E')$, and by formula (7.17), we have $\ker(g) = \mathbf{k}^*(E)$, so

(7.18)

$$\big[\mathbf{k}^*(E) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{K}(E')\big)\big] = [\ker(g) : \mathrm{Im}(f)] = [\ker(f) : \mathrm{Im}(g)]\frac{[\ker(g_1) : \mathrm{Im}(f_1)]}{[\ker(f_1) : \mathrm{Im}(g_1)]}.$$

It remains to compute $[\ker(f) : \mathrm{Im}(g)]$, to choose subgroup L, and to compute $[\ker(g_1) : \mathrm{Im}(f_1)]$ and $[\ker(f_1) : \mathrm{Im}(g_1)]$.

Computation of $[\ker(f) : Im(g)]$. By Hilbert theorem 90, if $f(\alpha) = 1$ with $\alpha \in \mathbf{k}^*(E)$ then there is an element $\beta \in \mathbf{K}^*$ such that $\alpha = \beta^{1-\sigma}$. The following lemma is needed to insure that β may be chosen from $\mathbf{K}^*(E')$, which will show that $\ker(f) \subset \mathrm{Im}(g)$, so we have

$$[\ker(f) : \mathrm{Im}(g)] = 1. \tag{7.19}$$

LEMMA 7.13. *If* $\alpha \in \mathbf{k}^*(E)$ *and* $\mathbf{N}_{\mathbf{K}/\mathbf{k}}\alpha = 1$, *then there is an element* $\beta' \in \mathbf{K}^*(E')$ *such that* $\alpha = (\beta')^{1-\sigma}$.

PROOF. Let $\alpha = \beta^{1-\sigma}$ with $\beta \in \mathbf{K}^*$. If we can find γ in $\mathbf{k}^*$ so that $\beta\gamma \in \mathbf{K}^*(E')$, then $(\beta\gamma)^{1-\sigma} = \beta^{1-\sigma} = \alpha$, so $\beta' = \beta\gamma$ will satisfy the conclusion. Let $\wp$ be any prime not in E'. Put $\wp_i = \wp^{\sigma^{-i}}$ for $0 \le i < g_i$. Then $\wp_i \notin E'$, so $|\alpha|_{\wp_i} = 1$. We have

$$1 = |\alpha|_{\wp_i} = \left|\alpha^{\sigma^i}\right|_{\wp} = \left|\beta^{\sigma^i - \sigma^{i+1}}\right|_{\wp} = \left|\beta^{\sigma^i}\right|_{\wp} \left|\beta^{\sigma^{i+1}}\right|_{\wp}^{-1}.$$

Therefore $|\beta^{\sigma^i}|_{\wp} = |\beta^{\sigma^{i+1}}|_{\wp}$, so for any $\wp$ not in E we have

$$|\beta|_{\wp} = |\beta^{\sigma}|_{\wp} = \cdots = \left|\beta^{\sigma^{n-1}}\right|_{\wp}.$$

This also applies to $\wp_i$, so we have $|\beta|_{\wp_i} = |\beta^{\sigma}|_{\wp_i} = |\beta|_{\wp_i^{-\sigma}} = |\beta|_{\wp_{i+1}}$. Therefore

$$|\beta|_{\wp} = |\beta|_{\wp_0} = |\beta|_{\wp_1} = \cdots = |\beta|_{\wp_{g_i - 1}}.$$

Because $\wp$ is not in E', the extension $\mathbf{K}_{\wp}/\mathbf{k}_p$ is not ramified, so there are elements in $\mathbf{k}_p^*$ of every value. In particular, there exist an element $\lambda_p \in \mathbf{k}_p^*$ such that $|\lambda_p|_{\wp_0} = |\beta|_{\wp_0}$. Since λ_p is fixed by σ, we have

$$|\beta|_{\wp_i} = |\beta|_{\wp_0} = |\lambda_p|_{\wp_0} = \left|\lambda_p^{\sigma^{-i}}\right|_{\wp_0^{\sigma^{-i}}} = \left|\lambda_p^{\sigma^{-i}}\right|_{\wp_i} = |\lambda_p|_{\wp_i}.$$

Let idele $\mathbf{i} \in \mathbf{I_p}$ have component $\mathbf{i}_p = \lambda_p$ for $p \notin E$, and $\mathbf{i}_p = 1$ for $p \in E$. If $\wp \notin E'$ then $|\beta\mathbf{i}^{-1}|_{\wp_i} = 1$, so $\beta\mathbf{i}^{-1} \in \mathbf{I_K}(E')$. Using the imbedding $\mathbf{I_k} \to \mathbf{I_K}$, we have $\mathbf{I_k}(E) \subset \mathbf{I_K}(E')$, so

$$\mathbf{I}_k = \mathbf{k}^*\mathbf{I}_k(E) \subset \mathbf{k}^*\mathbf{I_K}(E').$$

Put $\mathbf{i} = \delta\mathbf{j}$ with $\delta \in \mathbf{k}^*$ and $\mathbf{j} \in \mathbf{I_K}(E')$. Then $\beta\mathbf{i}^{-1} = \beta\delta^{-1}\mathbf{j}^{-1}$. Since $\beta\mathbf{i}^{-1}$ and $\mathbf{j}^{-1}$ are in $\mathbf{I_K}(E')$, then so is $\beta\delta^{-1}$ in $\mathbf{I_K}(E')$. Therefore $\beta\delta^{-1} \in \mathbf{K}^*(E')$, so $\gamma = \delta^{-1}$ is the required element.

The subgroup L. If $p_0, \dots, p_s$ are the primes in E, each p_i in E splits into g_i primes in $\mathbf{K}$. We claim that there exist elements in $J = \mathbf{K}^*(E')$ as follows.

(1) Elements $\eta_1, \dots \eta_s$ so that $\eta_i^{1-\sigma} = 1$.

(2) Elements $H_0, \dots, H_s$ so that $H_i^{\sigma^{g_i}} = H_i$ and $H_i^{1+\sigma+\cdots+\sigma^{g_i-1}} = 1$.

(3) The elements $\eta_1, \dots, \eta_s, H_0, H_0^{\sigma}, \dots, H_0^{\sigma^{g_0-2}}, \dots, H_s, H_s^{\sigma}, \dots, H_s^{\sigma^{g_s-2}}$ are independent and generate a subgroup L of finite index in $J = \mathbf{K}^*(E')$. (If $g_i = 1$ then H_i is omitted.)

We will now apply Herbrand's lemma using the subgroup above L to compute $[\ker(g_1) : \mathrm{Im}(f_1)]$ and $[\ker(f_1) : \mathrm{Im}(g_1)]$, after which we will show that L is a subgroup of finite index in J.

Computation of $[\ker(g_1) : \mathit{Im}(f_1)]$ *and* $[\ker(f_1) : \mathit{Im}(g_1)]$. A typical element of L has the form

$$\Delta = \prod_{i=1}^{s} \eta^{u_i} \prod_{i=0}^{s} H_i^{v_i(\sigma)}$$

where $v_i(\sigma)$ is a polynomial with rational integer coefficients of degree at most $g_i - 2$. Note that $\mathbf{N}_{\mathbf{K}/\mathbf{k}} H_i = 1$, because if $\mathbf{Z}_i$ is the subfield of $\mathbf{K}$ fixed by the subgroup $< \sigma^{g_i} >$ then $H_i \in \mathbf{Z}_i$ and

$$\mathbf{N}_{\mathbf{Z}_i/\mathbf{k}} H_i = H_i^{1+\sigma+\cdots+\sigma^{g_i-1}} = 1,$$

so $\mathbf{N}_{\mathbf{K}/\mathbf{k}} H_i = \mathbf{N}_{\mathbf{Z}_i/\mathbf{k}} \mathbf{N}_{\mathbf{K}/\mathbf{Z}_i} H_i = \mathbf{N}_{\mathbf{Z}_i/\mathbf{k}} (H_i)^{n/g_i} = 1$. Therefore,

$$f(\Delta) = \prod_{i=1}^{s} \eta^{n u_i} \prod_{i=0}^{s} \mathbf{N}_{\mathbf{K}/\mathbf{k}} H_i^{v_i(\sigma)} = \prod_{i=1}^{s} \eta^{n u_i}.$$

The right side is an element of L, so $f(L) \subset L$, and we have

$$\mathrm{Im}(f_1) = \left\{ \prod_{i=1}^{s} \eta^{n u_i} \;\middle|\; u_i \in \mathbf{Z} \right\} \tag{7.20}$$

Since the η_i are independent, the kernel of f_1 is

$$\ker(f_1) = \left\{ \prod_{i=0}^{s} H_i^{v_i(\sigma)} \;\middle|\; v_i(\sigma) \in \mathbf{Z}[\sigma] \text{ and } \deg(v_i) \le g_i - 2 \right\}. \tag{7.21}$$

Next, we find the kernel and image of g_1. We have

$$g_1(\Delta) = \prod_{i=0}^{s} H_i^{v_i(\sigma)(1-\sigma)}. \tag{7.22}$$

Let m_i be the coefficient of σ^{g_i-2} in $v_i(\sigma)$. Since $H_i^{1+\sigma+\cdots+\sigma^{g_i-1}} = 1$, we have

$$H_i^{v_i(\sigma)(1-\sigma)} = H_i^{v_i(\sigma)(1-\sigma)+m_i(1+\sigma+\cdots+\sigma^{g_i-1})},$$

and $v_i(\sigma)(1-\sigma)+m_i(1+\sigma+\cdots+\sigma^{g_i-1})$ is a polynomial of degree at most g_i-2. Therefore $\ker(g_1)$ is the set

$$\ker(g_1) = \left\{ \prod_{i=1}^{s} \eta^{u_i} \prod_{i=0}^{s} H_i^{v_i(\sigma)} \;\middle|\; v_i(\sigma)(1-\sigma)+m_i(1+\sigma+\cdots+\sigma^{g_i-1}) = 0 \right\}.$$

There exist polynomials $a(x)$ and $b(x)$ so that $(1-x)a(x)+(1+x+\cdots+x^{g_i-1})b(x) = 1$. If $v_i(\sigma)(1-\sigma)+m_i(1+\sigma+\cdots+\sigma^{g_i-1}) = 0$, then $v_i(\sigma) = (1+\sigma+\cdots+\sigma^{g_i-1})\big(v_i(\sigma)b(\sigma)-m_ia(\sigma)\big)$. Since the degree of $v_i(\sigma)$ is at most g_i-2 then we must have $v_i(\sigma)=0$. Therefore

$$\ker(g_1) = \left\{ \prod_{i=1}^{s} \eta^{u_i} \right\}. \tag{7.23}$$

For the computation of $\mathrm{Im}(g_1)$, we have the following lemma.

Lemma 7.14. *A necessary and sufficient condition for polynomial $h(x)$ of degree at most $g-2$ to be of the form*

$$h(x) = v(x)(1-x)+m(1+x+\cdots+x^{g-1})$$

where m is a rational integer and $v(x)$ is a polynomial of degree at most $g-2$ is

$$h(1) = 0 (\mathrm{mod}\ g).$$

Proof. If $h(x) = v(x)(1-x)+m(1+x+\cdots+x^{g-1})$ then $h(1)=mg$. Conversely, suppose $h(1)=mg$ for some integer m. Let $v(x)$ be the quotient of the division of $h(x)-m(1+x+\cdots+x^{g-1})$ by $1-x$. Then we have

$$h(x)-m(1+x+\cdots+x^{g-1}) = v(x)(1-x)+r \quad \text{where } \deg\big(v(x)\big) \le g-2, \text{ and } r \in \mathbf{Z}.$$

Setting $x=1$, we conclude that $r=0$, so $h(x) = v(x)(1-x)+m(1+x+\cdots+x^{g-1})$.

Applying lemma 7.14, we see that (7.22) is equivalent to

$$\mathrm{Im}(g_1) = \left\{ \prod_{i=0}^{s} H_i^{h_i(\sigma)} \;\middle|\; h_i(1) = 0 (\mathrm{mod}\ g_i) \text{ and } \deg\big(h_i\big) \le g_i-2 \right\} \tag{7.24}$$

By (7.22) and (7.19), we have

$$[\ker(g_1) : \mathrm{Im}(f_1)] = \left[\prod_{i=1}^{s} \eta^{u_i} : \prod_{i=1}^{s} \eta^{nu_i}\right] = n^s. \tag{7.25}$$

By (7.21) and (7.24), we have

$$[\ker(f_1) : \mathrm{Im}(g_1)] = \left[\prod_{i=0}^{s} H_i^{v_i(\sigma)} : \prod_{i=0}^{s} H_i^{h_i(\sigma)}\right] \qquad \begin{cases} \deg(v_i) \le g_i - 2, \\ \deg(h_i) \le g_i - 2, \\ \quad h_i(1) = 0 (\mathrm{mod}\ g_i) \end{cases}$$

In the homomorphism $H_i^{v_i(\sigma)} \to \mathbf{Z}/(g)$ by $H_i^{v_i(\sigma)} \to v_i(1)(\mathrm{mod}\ g)$, the kernel consists of those $h_i(\sigma)$ such that $h_i(\sigma) = 1(\mathrm{mod}\ g_i)$, so $H_i^{v_i(\sigma)}/H_i^{h_i(\sigma)}$ is isomorphic to $\mathbf{Z}/(g_i)$. therefore

$$[\ker(f_1) : \mathrm{Im}(g_1)] = \prod_{i=0}^{s} g_i. \tag{7.26}$$

From (7.25) and (7.26), we have

$$\frac{[\ker(g_1) : \mathrm{Im}(f_1)]}{[\ker(f_1) : \mathrm{Im}(g_1)]} = \frac{n^s}{\prod_{i=0}^{s} g_i} = \frac{1}{n} \prod_{i=0}^{s} \left(\frac{n}{g_i}\right) = \frac{1}{n} \prod_{i=0}^{s} n_i = \frac{1}{n} \prod_{p \in E} n_p. \tag{7.27}$$

From (7.27) and (7.18), and recalling that $[\ker(f) : \mathrm{Im}(g)] = 1$, we have

$$\left[\mathbf{k}^*(E) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{K}(E')\big)\right] = \frac{1}{n} \prod_{p \in E} n_p = \frac{1}{[\mathbf{K} : \mathbf{k}]} \prod_{p \in E} n_p. \tag{7.28}$$

Substituting the right side of (7.28) into (7.16), we obtain

$$\left[\mathbf{I_k} : \mathbf{k}^* \mathbf{N}_{\mathbf{K}/\mathbf{k}} \mathbf{I_K}\right] = [\mathbf{K} : \mathbf{k}] \left[\mathbf{k}^*(E) \cap \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{I_K}(E')\big) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{K}(E')\big)\right]. \tag{7.29}$$

Except for constructing generators for subgroup L, we have finished the proof of the first fundamental inequality.

First fundamental inequality. *If* $\mathbf{K}$ *is a cyclic extension of* $\mathbf{k}$ *then* $\left[\mathbf{I_k} : \mathbf{k}^* \mathbf{N}_{\mathbf{K}/\mathbf{k}} \mathbf{I_K}\right]$ *is divisible by* $[\mathbf{K} : \mathbf{k}]$.

Proof. The term $\left[\mathbf{k}^*(E) \cap \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{I_K}(E')\big) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{K}(E')\big)\right]$ in (7.29) is finite because it divides $\left[\mathbf{k}^*(E) : \mathbf{N}_{\mathbf{K}/\mathbf{k}}\big(\mathbf{K}(E')\big)\right]$, which has been shown in (7.28) to be finite.

Construction of generators for subgroup L. For each prime $p = p_i$, $0 \leq i \leq s$, in E, there are $g = g_i$ primes of $\mathbf{K}$ dividing p; their splitting groups coincide and so may all be denoted by $S_p(\mathbf{K}/\mathbf{k})$. Since $[G(\mathbf{K}/\mathbf{k}) : S_p(\mathbf{K}/\mathbf{k})] = g$ then $S_p(\mathbf{K}/\mathbf{k})$ is generated by σ^g. Let $\mathbf{Z}$ be the subfield of $\mathbf{K}$ fixed by $S_p(\mathbf{K}/\mathbf{k})$. Then $G(\mathbf{K} : \mathbf{Z}) = S_p(\mathbf{K}/\mathbf{k})$. To determine $S_p(\mathbf{K}/\mathbf{Z})$, for prime $\wp$ in E' dividing p we have

$$S_\wp(\mathbf{K}/\mathbf{Z}) = \left\{\tau \in G(\mathbf{K} : \mathbf{Z}) \;\middle|\; \wp^\tau = \wp\right\}$$
$$= \left\{\tau \in S_p(\mathbf{K}/\mathbf{k}) \;\middle|\; \wp^\tau = \wp\right\} = S_p(\mathbf{K}/\mathbf{k}) = G(\mathbf{K} : \mathbf{Z}).$$

Then $[G(\mathbf{K} : \mathbf{Z}) : S_\wp(\mathbf{K}/\mathbf{Z})] = 1$, so each prime $\wp$ of $\mathbf{K}$ divides exactly one prime $\wp'$ of $\mathbf{Z}$. The subgroups $S_\wp(\mathbf{K}/\mathbf{Z})$ all coincide with $S_p(\mathbf{K}/\mathbf{k})$. We next determine the splitting groups $S_{\wp'}(\mathbf{Z}/\mathbf{k})$. We have the exact sequence

$$1 \to S_p(\mathbf{K}/\mathbf{k}) \to G(\mathbf{K} : \mathbf{k}) \to G(\mathbf{Z} : \mathbf{k}) \to 1.$$

Let $\overline{\tau}$ be the image of τ in $G(\mathbf{Z} : \mathbf{k})$. Then

$$S_{\wp'}(\mathbf{Z}/\mathbf{k}) = \left\{\overline{\tau} \in G(\mathbf{Z} : \mathbf{k}) \;\middle|\; {\wp'}^{\overline{\tau}} = \wp'\right\}.$$

We have ${\wp'}^{\overline{\tau}} = (\wp \cap \mathbf{O_Z})^\tau = \wp^\tau \cap \mathbf{O_Z} = {\wp^\tau}'$, so ${\wp'}^{\overline{\tau}} = \wp'$ if and only if ${\wp^\tau}' = \wp'$ if and only if $\wp^\tau = \wp$. Therefore $\overline{\tau} \in S_{\wp'}(\mathbf{Z}/\mathbf{k})$ if and only if $\tau \in S_\wp(\mathbf{K}/\mathbf{k})$ if and only if $\overline{\tau} = 1$. This show that $S_{\wp'}(\mathbf{Z}/\mathbf{k}) = 1$ so

$$\mathbf{Z}_{\wp'} = \mathbf{k}_p.$$

To determine the parameters e' and f' for the splitting of prime $\wp_i'$ in $\mathbf{K}$, the extension $\mathbf{K}_\wp$ of $\mathbf{Z}_{\wp'}$ is identical to extension $\mathbf{K}_\wp$ of $\mathbf{k}_p$, so we have $e' = e$ and $f' = f$.

Lemma 7.15. *Let $\wp$ be a prime of abelian extension $\mathbf{K}$ of $\mathbf{k}$, and let $\mathbf{Z}$ the subfield fixed by the splitting group $S_\wp(\mathbf{K}/\mathbf{k})$. If α is in $\mathbf{K}^*$, we have $\left|\mathbf{N}_{\mathbf{K}/\mathbf{Z}}\alpha\right|_\wp$ is greater than 1, equal to 1, or less than 1, if and only if $|\alpha|_\wp$ is greater than 1, equal to 1, or less than 1, respectively.*

Proof. The proof depends on the fact that $\wp$ is the only prime of $\mathbf{K}$ dividing prime $\wp' = \wp \cap \mathbf{O_Z}$ of $\mathbf{Z}$. For α in $\mathbf{K}^*$ the formula expressing $\mathbf{N}_{\mathbf{K}/\mathbf{Z}}\alpha$ as the product of local norms reduces to

$$\mathbf{N}_{\mathbf{K}/\mathbf{Z}}\alpha = \mathbf{N}_{\mathbf{K}_\wp/\mathbf{Z}_{\wp'}}\alpha.$$

Therefore

$$\left|\mathbf{N}_{\mathbf{K}/\mathbf{Z}}\alpha\right|_{\wp'} = \left|\mathbf{N}_{\mathbf{K}_\wp/\mathbf{Z}_{\wp'}}\alpha\right|_{\wp'} = |\alpha|_\wp.$$

Applying the above formula (twice!) to the element $\mathbf{N}_{\mathbf{K}/\mathbf{Z}}\alpha$, we have

$$\left|\mathbf{N}_{\mathbf{K}/\mathbf{Z}}\alpha\right|_{\wp} = \left|\mathbf{N}_{\mathbf{K}/\mathbf{Z}}\left(\mathbf{N}_{\mathbf{K}/\mathbf{Z}}\alpha\right)\right|_{\wp'} = \left|\left(\mathbf{N}_{\mathbf{K}/\mathbf{Z}}\alpha\right)^{ef}\right|_{\wp'} = |\alpha|_{\wp}^{ef},$$

from which the conclusion follows immediately.

REMARK. The primes of E are $p_0, \ldots, p_s$. For each p_i in E, choose one prime $\wp_i$ in E' which divides p_i. Prime p_i splits into g_i primes in $\mathbf{K}$. Splitting group $S_{p_i}(\mathbf{K}/\mathbf{k})$ is generated by σ^{g_i}, and $\wp_i, \wp_i^{\sigma}, \ldots, \wp_i^{\sigma^{g_i-1}}$ is the complete list of distinct primes of $\mathbf{K}$ dividing p_i. The number of primes in E' is $s'+1 = \sum_{i=0}^{s} g_i$.

LEMMA 7.16. *If a single prime $\wp_i$ is selected then there exists an element α in $\mathbf{K}^*$ so that*

$$|\alpha|_{\wp_i} > 1 \qquad \text{and} \qquad |\alpha|_{\wp} < 1 \quad \text{for } \wp \in E', \wp \neq \wp_i.$$

PROOF. E contains at least one infinite prime, so we take p_s to be infinite. Then $\wp_s$ is also infinite. Let ν be a positive real constant so that $\nu > \max(\mu, 1)$ where constant mu is defined below. If $s = 0$ then there is nothing to prove. We construct idele $\mathbf{j} \in \mathbf{I_K}$ by choosing components $\mathbf{j}_{\wp}$ in the following order.

If $i = 1\ldots, s-1$, choose components as follows:
(1) At $\wp \notin E'$, choose $\mathbf{j}_{\wp} = 1$.
(2) At $\wp \in E'$, $\wp \neq \wp_i$ and $\wp \neq \wp_s$, choose $\mathbf{j}_{\wp} \in \mathbf{K}_{\wp}^*$ so that $|\mathbf{j}|_{\wp} < \frac{1}{\nu}$.
(3) At $\wp_i$, choose $\mathbf{j}_{\wp_i} \in \mathbf{K}_{\wp}^*$ large enough so that $|\mathbf{j}|_{\wp_i} > \nu \prod_{\wp \in E', \wp \neq \wp_i, \wp \neq \wp_s} |\mathbf{j}|_{\wp}^{-1}$.
(4) At $\wp_s$, choose $\mathbf{j}_{\wp_s} \in \mathbf{K}_{\wp}^*$ so that $|\mathbf{j}| = 1$.

From (3) we have $\prod_{\wp \in E', \wp \neq \wp_s} |\mathbf{j}|_{\wp} > \nu$. Then from (4), we have

$$|\mathbf{j}|_{\wp_s} = \prod_{\wp \in E', \wp \neq \wp_s} |\mathbf{j}|_{\wp}^{-1} < \frac{1}{\nu}.$$

If $i = s$, choose components of $\mathbf{j}$ as follows:
(1_s) At $\wp \notin E'$, choose $\mathbf{j}_{\wp} = 1$.
(2_s) At $\wp \in E', \wp \neq \wp_s$, choose $\mathbf{j}_{\wp} \in \mathbf{K}_{\wp}^*$ so that $|\mathbf{j}|_{\wp} < \frac{1}{\nu}$.
(3_s) At $\wp_s$, choose $\mathbf{j} \in \mathbf{K}_{\wp_s}^*$ so that $|\mathbf{j}| = 1$.

From (3_s) and (2_s), we have $|\mathbf{j}|_{\wp_s} = \prod_{\wp \in E', \wp \notin \wp_s} |\mathbf{j}|_{\wp}^{-1} > (\nu)^{s'} > \nu$.

By our construction, $\mathbf{j}$ is in $\mathbf{I_K}(E') \cap \mathbf{I_K^0}$. By lemma 6.10, there exists a constant μ so that

$$\mathbf{I_K}(E') \cap \mathbf{I_K^0} = \mathbf{K}^*(E) \left\{ \mathbf{i} \in \mathbf{I_K}(E') \;\Big|\; \frac{1}{\mu} \leq |\mathbf{i}|_{\wp} \leq \mu \text{ for } \wp \in E' \right\}.$$

Therefore there exist element $\alpha \in \mathbf{K}^*(E')$ and idele $\mathbf{i} \in \mathbf{I_K}(E')$ so that $\mathbf{j} = \alpha\mathbf{i}$ and $\mathbf{i}$ satisfies the condition $\frac{1}{\mu} \leq |\mathbf{i}|_\wp \leq \mu$ for $\wp \in E'$. For $\wp_i$ we have

$$|\alpha|_{\wp_i} = |\mathbf{j}|_{\wp_i}|\mathbf{i}|_{\wp_i}^{-1} > \frac{\nu}{\mu} > 1$$

and for $\wp \in E'$, $\wp \neq \wp_i$ we have

$$|\alpha|_\wp = |\mathbf{j}|_\wp|\mathbf{i}|_\wp^{-1} < \frac{\mu}{\nu} < 1.$$

Lemma 7.17. *There exist elements $H_0^{**}, \ldots, H_s^{**}$ in $\mathbf{K}^*$ so that*

$$|H_i^{**}|_{\wp_i} > 1 \qquad \text{and} \qquad |H_i^{**}|_\wp < 1 \quad \text{for } \wp \in E', \wp \neq \wp_i.$$

Proof. Apply Lemma 7.16 for $i = 1, \ldots, s$.

Lemma 7.18. *Let $H_0^{**}, \ldots, H_s^{**}$ in $\mathbf{K}^*(E')$ satisfy the conclusion of lemma 7.16. Let $\mathbf{Z}_i$ be the subfield fixed by splitting group $S_{p_i}(\mathbf{K}/\mathbf{k}) =< \sigma^{g_i} >$. Put $H_i^* = \mathbf{N}_{\mathbf{K}/\mathbf{Z}_i} H_i^{**}$. Then elements*

$$(H_0^*), \ldots, (H_0^*)^{\sigma^{g_i-1}}, \ldots, (H_s^*), \ldots, (H_s^*)^{\sigma^{g_s-1}}$$

satisfy the condition

$$\left|(H_i^*)^{\sigma^j}\right|_{\wp_i^{\sigma^j}} > 1 \qquad \text{and} \qquad \left|(H_i^*)^{\sigma^j}\right|_\wp < 1 \quad \text{if} \quad \wp \in E' \text{ and } \wp \neq \wp_i^{\sigma^j}$$

Proof. The primes of E' are $\wp_i^{\sigma^j}$ for $0 \leq i \leq s$, $0 \leq j < g_i$. Suppose that $\wp$ in E' does not divide p_i. Then $\wp = \wp_{i'}^{\sigma^j}$ with $i' \neq i$. We have $[\mathbf{K} : \mathbf{Z}_i] = n_i$ where $n = n_i g_i$. Then

$$|H_i^*|_\wp = \left|\mathbf{N}_{\mathbf{K}/\mathbf{Z}_i} H_i^{**}\right|_\wp = \left|\prod_{k=0}^{n_i-1} (H_i^{**})^{\sigma^{kg_i}}\right|_\wp = \prod_{k=0}^{n_i-1} |H_i^{**}|_{\wp^{\sigma^{-kg_i}}} < 1,$$

because none of the $\wp^{\sigma^{-kg_i}}$ coincide with $\wp_i$, so all of the terms $|H_i^{**}|_{\wp^{\sigma^{-kg_i}}}$ are less than 1.

We also have to check $(H_i^*)^{\sigma^j}$ at $\wp_i, \wp_i^\sigma, \ldots, \wp_i^{\sigma^{g_i-1}}$. Since $H_i^* = \mathbf{N}_{\mathbf{K}/\mathbf{Z}_i} H_i^{**}$ and $|H_i^{**}|_{\wp_i} > 1$, then by lemma 7.15 we have

$$\left|(H_i^*)^{\sigma^j}\right|_{\wp_i^{\sigma^j}} = |H_i^*|_{\wp_i} > 1.$$

For $\wp = \wp_i^{\sigma^{j'}} \neq \wp_i^{\sigma^j}$, we have $\wp^{\sigma^{-j}} \neq \wp_i$ so

$$\left|(H_i^*)^{\sigma^j}\right|_\wp = |H_i^*|_{\wp^{\sigma^{-j}}} < 1,$$

showing that the $(H_i^*)^{\sigma^j}$ satisfy the required conditions.

Lemma 7.19. *Put* $U_{ij} = (H_i^*)^{\sigma^j}$, $0 \leq i \leq s$, $0 \leq j < g_i$. *There are* $s' + 1$ *pairs* (i, j). *If we exclude* $U_{i_0 j_0}$ *for one pair* (i_0, j_0), *then the remaining* s' *elements* U_{ij} *are independent.*

Proof. Suppose that $\prod_{(i,j)\neq(i_0,j_0)} U_{ij}^{a_{ij}} = 1$. Let

$$F' = \left\{(i,j) \;\middle|\; a_{ij} > 0\right\} \qquad \text{and} \qquad F'' = \left\{(i,j) \;\middle|\; a_{ij} < 0\right\},$$

so $F' \cap F'' = \emptyset$. Suppose that F' is not empty. Then

$$\prod_{(i,j)\in F'} U_{ij}^{b_{ij}} = \prod_{(i,j)\in F''} U_{ij}^{b_{ij}}$$

where $b_{ij} > 0$. Let $\wp_i^{\sigma^j}$ be denoted by $\wp_{ij}$. Since $(i_0, j_0) \notin F' \cup F''$ we have

$$\prod_{(i,j)\in F'} \left|U_{ij}^{a_{ij}}\right|_{\wp_{i_0 j_0}} = \prod_{(i,j)\in F''} \left|U_{ij}^{b_{ij}}\right|_{\wp_{i_0 j_0}} < 1.$$

This show that F'' cannot be empty. By the product formula, we have

$$\prod_{\wp} \left| \prod_{(i,j)\in F'} U_{ij}^{b_{ij}} \right|_{\wp} = \prod_{\wp\in E'} \left| \prod_{(i,j)\in F'} U_{ij}^{b_{ij}} \right|_{\wp} = \prod_{\wp\in E'} \prod_{(i,j)\in F'} \left|U_{ij}^{b_{ij}}\right|_{\wp} = 1.$$

Since $\wp_{i_0 j_0} \in E'$, there exists (i_i, j_1) so that

$$\prod_{(i,j)\in F'} \left|U_{ij}^{b_{ij}}\right|_{\wp_{i_1 j_1}} > 1.$$

and (i_1, j_1) must be in F'. We have a contradiction since (i_1, j_1) is not in F'', but

$$\prod_{(i,j)\in F''} \left|U_{ij}^{b_{ij}}\right|_{\wp_{i_1 j_1}} = \prod_{(i,j)\in F'} \left|U_{ij}^{b_{ij}}\right|_{\wp_{i_1 j_1}} > 1.$$

Lemma 7.20. *Suppose that* A *is an abelian group containing a subgroup* A_0 *of finite index in* A, *and* A_0 *is free abelian on* s' *generators. Let* B *be a subgroup of* A *containing* s' *independent elements. Then* B *has finite index in* A.

Proof. Take B' to a subgroup of B generated by s' independent elements. Then $B' \subset B \subset A$. Let $[A : A_0] = m$. Replace B' by $B_0 = mB'$. Then $B_0 \subset A_0$ and B_0 has s' independent elements. Let $x_1, \ldots, x_{s'}$ be a basis for A_0; let $y_1, \ldots, y_{s'}$

be independent in B_0. Let $y_i = \sum_{j=1}^{s'} a_{ij}x_j$. Matrix (a_{ij}) is non-singular, because otherwise there exist integers $b_1, \ldots, b_{s'}$, not all zero, so that $\sum_{i=0}^{s'} b_i a_{ij} = 0$. Then $\sum_{i=0}^{s'} b_i y_i = \sum_{i=0}^{s'} \sum_{j=0}^{s'} b_i a_{ij} x_j = \sum_{j=0}^{s'} \sum_{i=0}^{s'} b_i a_{ij} x_j = 0$, which is impossible. There exists an integer matrix (c_{ik}) so that $(c_{ik})(a_{kj}) = aI$, where $a = \det(a_{ij})$. Then

$$\sum_{k=0}^{s'} c_{ik} y_k = \sum_{k=0}^{s'} \sum_{j=0}^{s'} c_{ik} a_{kj} x_j = a x_i \in B_0.$$

Therefore $aA_0 \subset B_0$, so $[A_0 : B_0] < [A_0 : aA_0] = a^{s'}$, so $[A : B] < [A : B_0] = [A : A_0][A_0 : B_0] < ma^{s'}$, which proves the lemma.

We now define the elements $\eta_0, \ldots, \eta_s$ and $H_0, \ldots, H_s$ as follows.

$$\eta_i = \mathbf{N}_{\mathbf{Z}_i/\mathbf{k}} H_i^* \qquad \text{and} \quad H_i = \eta_i^{-1} (H_i^*)^{g_i} \quad \text{for } 0 \le i \le s$$

These satisfy the first two of three required conditions.
(1) η_i is in $\mathbf{k}^*(E)$, so $\eta_i^{1-\sigma} = 1$.
(2) $\mathbf{N}_{\mathbf{Z}_i/\mathbf{k}} H_i = \mathbf{N}_{\mathbf{Z}_i/\mathbf{k}} \left(\eta_i^{-1} (H_i^*)^{g_i}\right) = \eta_i^{-g_i} \eta_i^{g_i} = 1$.

Let L be the subgroup generated by the following elements (This is one more than we need, but we will show that η_0 may be discarded.)

$$\eta_0, \ldots, \eta_s, H_0, \ldots, H_0^{\sigma^{g_0-2}}, \ldots, H_s, \ldots, H_0^{\sigma^{g_s-2}}.$$

Since $\mathbf{N}_{\mathbf{Z}_i/\mathbf{k}} H_i = 1$, then $H_i^{1+\sigma+\cdots+\sigma^{g_i-1}} = 1$, or $H_i^{\sigma^{g_i-1}} = \left(H_i^{1+\sigma+\cdots+\sigma^{g_i-2}}\right)^{-1}$, so $H_i^{\sigma^{g_i-1}}$ is in L. We have $H_i^{\sigma^j} = \eta_i^{-1}\left(H_i^{*\sigma^j}\right)^{g_i}$, so $\left(H_i^{*\sigma^j}\right)^{g_i} = \eta_i H_i^{\sigma^j}$ is in L for $0 \le j \le g_i - 1$. By lemma 7.19, we know that L contains s' independent elements, so by lemma 7.20 subgroup L has finite index in $\mathbf{K}^*(E')$. We still need to discard one element. If we could discard one of the $H_i^{\sigma^j}$ leaving s' independent elements, then $\eta_0, \ldots, \eta_s$ would be a set of $s+1$ independent units in $k^*(E)$, but this would be a violation of unit theorem 6.13. Therefore we must discard one of the η_i. After relabeling the η_i, we obtain the following set of s' independent generators for L.

$$\eta_1, \ldots, \eta_s, H_0, \ldots, H_0^{\sigma^{g_0-2}}, \ldots, H_s, \ldots, H_0^{\sigma^{g_s-2}}. \tag{7.29}$$

Condition (3) is now satisfied: elements (7.29) are independent and generate a subgroup of finite index in $\mathbf{K}^*(E')$. The completes the proof of the first fundamental inequality.