CHAPTER VIII

SECOND FUNDAMENTAL INEQUALITY

Kummer extensions. Let $\mathbf{k}$ contain the n-th roots of unity, and let ζ be a primitive n-root of unity. A *Kummer extension* is an extension of $\mathbf{k}$ generated by the roots of $x^n - \alpha$ where α is a non-zero element of $\mathbf{k}$. If one root is denoted $\sqrt[n]{\alpha}$ then the other roots are $\zeta \sqrt[n]{\alpha}, \zeta^2 \sqrt[n]{\alpha}, \ldots, \zeta^{n-1} \sqrt[n]{\alpha}$. If α and β are elements of $\mathbf{k}^*$, then we write $\alpha \simeq_n \beta$ if $\alpha = \beta\gamma^n$ for some $\gamma \in \mathbf{k}^*$. Elements $\alpha_1, \ldots, \alpha_r$ of $\mathbf{k}$ are *independent modulo* $(\mathbf{k}^*)^n$ means $\alpha_1^{a_1} \ldots \alpha_r^{a_r} \simeq_n 1$ only if $a_1 = \cdots = a_r = 0(\text{mod } n)$.

Lemma 8.1. *Let n_0 be the smallest positive power of α so that $\alpha^{n_0} \simeq_n 1$. Then n_0 divides n. There is an element α_0 so that $\alpha = \alpha_0^d$, where $n = n_0 d$, and $\mathbf{k}\left(\sqrt[n]{\alpha}\right) = \mathbf{k}\left(\sqrt[n_0]{\alpha_0}\right)$.*

Proof. The set of integers a such that $\alpha^a \simeq_n 1$ is an ideal, so take n_0 to be the positive integer which generates the ideal. Since $\alpha^n \simeq_n 1$ then n is in the ideal, so $n = n_0 d$ for some positive integer d. We have $\alpha^{n_0} = \gamma^n = \gamma^{n_0 d}$ for some γ in $\mathbf{k}^*$. If ζ is a primitive n-th root of unity, then

$$0 = \alpha^{n_0} - \gamma^{n_0 d} = \prod_{i=0}^{n_0 - 1} \left(\alpha - \zeta^{id}\gamma^d\right).$$

For some $0 \le i < n_0$, we have $\alpha = \zeta^{id}\gamma^d = \left(\zeta^i\gamma\right)^d$, so take $\alpha_0 = \zeta^i\gamma$. Then $\alpha = \alpha_o^d = \alpha_0^{n/n_0} = \left(\sqrt[n_0]{\alpha_0}\right)^n$. This show $\sqrt[n_0]{\alpha_0}$ is a root of $x^n - \alpha$, so $\mathbf{k}\left(\sqrt[n]{\alpha}\right) = \mathbf{k}\left(\sqrt[n_0]{\alpha_0}\right)$.

Lemma 8.2. *Let n_0 be the smallest positive power of α so that $\alpha^{n_0} \simeq_n 1$. Then $\left[\mathbf{k}\left(\sqrt[n]{\alpha}\right) : \mathbf{k}\right] = n_0$. For $\sigma \in G\left(\mathbf{k}\left(\sqrt[n]{\alpha}\right) : \mathbf{k}\right)$, let ζ_σ be the n-root of unity so that $\sigma\left(\sqrt[n]{\alpha}\right) = \zeta_\sigma\left(\sqrt[n]{\alpha}\right)$. Then $\sigma \to \zeta_\sigma$ defines an isomorphism of $G\left(\mathbf{k}\left(\sqrt[n]{\alpha}\right) : \mathbf{k}\right)$ onto the n_0-th roots of unity.*

Proof. (Galois automorphisms will applied on the left when radical notation is used.) By lemma 8.1, $\alpha = \alpha_0^d$ where $n = n_0 d$, and $\mathbf{k}\left(\sqrt[n]{\alpha}\right) = \mathbf{k}\left(\sqrt[n_0]{\alpha_0}\right)$. We need to show that $x^{n_0} - \alpha_0$ is irreducible over $\mathbf{k}$. The factorization of $x^{n_0} - \alpha_0$ into linear factors over $\mathbf{k}\left(\sqrt[n]{\alpha}\right)$ is

$$x^{n_0} - \alpha_0 = \prod_{i=0}^{n_0-1} \left(x - \zeta^{id} \sqrt[n_0]{\alpha_0}\right). \tag{8.1}$$

Any non-trivial factor of $x^{n_0} - \alpha_0$ over $\mathbf{k}$ would be a product of ν linear factors with $0 < \nu \leq n_0$, and the constant term would be $\pm\zeta_0 \left(\sqrt[n_0]{\alpha_0}\right)^\nu$, where $\zeta_0^{n_0} = 1$. Since $\mathbf{k}$ contains the n-th roots of unity then $\left(\sqrt[n_0]{\alpha_0}\right)^\nu$ is in $\mathbf{k}$. Let c be the greatest common divisor of ν and n_0, and put $c = an_0 + b\nu$. Then

$$\left(\sqrt[n_0]{\alpha_0}\right)^c = \left(\sqrt[n_0]{\alpha_0}\right)^{an_0+b\nu} = \alpha_0^a \left(\left(\sqrt[n_0]{\alpha_0}\right)^\nu\right)^b.$$

Therefore $\left(\sqrt[n_0]{\alpha_0}\right)^c$ is in $\mathbf{k}$, and

$$\alpha^c = \alpha^{n_0(c/n_0)} = \alpha_0^{n(c/n_0)} = \left(\left(\sqrt[n_0]{\alpha_0}\right)^c\right)^n,$$

so $\alpha^c \simeq_n 1$. But this is impossible if $0 < c < n_0$, so we must have $\nu = n_0$. This shows that $x^{n_0} - \alpha_0$ is irreducible over $\mathbf{k}$ and $[\mathbf{k}\left(\sqrt[n]{\alpha}\right) : \mathbf{k}] = n_0$.

If $\sigma\left(\sqrt[n]{\alpha}\right) = \zeta_\sigma \left(\sqrt[n]{\alpha}\right)$ then ζ_σ does not depend on $\sqrt[n]{\alpha}$ because if $\zeta^i \sqrt[n]{\alpha}$ is another root of $x^n - \alpha$ then

$$\sigma\left(\zeta^i \sqrt[n]{\alpha}\right) = \zeta^i \sigma\left(\sqrt[n]{\alpha}\right) = \zeta^i \zeta_\sigma \left(\sqrt[n]{\alpha}\right) = \zeta_\sigma \left(\zeta^i \sqrt[n]{\alpha}\right).$$

Therefore we may take $\sqrt[n]{\alpha} = \sqrt[n_0]{\alpha_0}$. The map $\sigma \to \zeta_\sigma$ is certainly a homomorphism. Since $[\mathbf{k}\left(\sqrt[n]{\alpha}\right) : \mathbf{k}] = n_0$ then $\sqrt[n]{\alpha}$ has n_0 distinct conjugates over $\mathbf{k}$. This shows that the image of $G\big(\mathbf{k}\left(\sqrt[n]{\alpha}\right) : \mathbf{k}\big)$ is the group of n_0-th roots of unity.

Lemma 8.3. $\mathbf{k}\left(\sqrt[n]{\beta}\right) \subset \mathbf{k}\left(\sqrt[n]{\alpha}\right)$ *if and only if* $\beta \simeq_n \alpha^\nu$ *for some* ν, $0 \leq \nu < n_0$.

Proof. If $\beta = \alpha^\nu \gamma^n$ then $\left(\sqrt[n]{\alpha}\right)^\nu$ is an n-th root of β, so $\mathbf{k}\left(\sqrt[n]{\beta}\right) \subset \mathbf{k}\left(\sqrt[n]{\alpha}\right)$. Conversely, suppose $\mathbf{k}\left(\sqrt[n]{\beta}\right) \subset \mathbf{k}\left(\sqrt[n]{\alpha}\right)$. Let $\alpha = \alpha_0^d$ so that $\mathbf{k}\left(\sqrt[n]{\alpha}\right) = \mathbf{k}\left(\sqrt[n_0]{\alpha_0}\right)$ and $[\mathbf{k}\left(\sqrt[n]{\alpha}\right) : \mathbf{k}] = n_0$. There exist $\gamma_0, \ldots, \gamma_{n_0-1}$ in $\mathbf{k}$ so that

$$\sqrt[n]{\beta} = \sum_{i=0}^{n_0-1} \gamma_i \left(\sqrt[n_0]{\alpha_0}\right)^i. \tag{8.2}$$

Choose σ in $G\big(\mathbf{k}\left(\sqrt[n]{\alpha}\right) : \mathbf{k}\big)$ so that ζ_σ is a primitive n_0-th root of unity. Let ζ be an n-th root of unity so that $\sigma(\sqrt[n]{\beta}) = \zeta \sqrt[n]{\beta}$. Applying σ to both sides of (8.2) gives

$$\zeta \sqrt[n]{\beta} = \sum_{i=0}^{n_0-1} \gamma_i \left(\zeta_\sigma \sqrt[n_0]{\alpha_0}\right)^i,$$

or

$$\sqrt[n]{\beta} = \sum_{i=0}^{n_0-1} \gamma_i \zeta^{-1} \zeta_\sigma^i \left(\sqrt[n_0]{\alpha_0} \right)^i . \tag{8.3}$$

The coefficients in (8.2) and (8.3) must coincide, so if $\gamma_i \neq 0$ then $\zeta^{-1}\zeta_\sigma^i = 1$. The values of the $\zeta^{-1}\zeta_\sigma^i = 1$ are all different, so γ_i cannot be non-zero for two different value of i. Therefore

$$\sqrt[n]{\beta} = \gamma_{i_0} \left(\sqrt[n_0]{\alpha_0} \right)^{i_0} ,$$

so we have $\beta = \gamma_{i_0}^n {\alpha_0^{i_0}}^d = \gamma_{i_0}^n \alpha^{i_0}$, or $\beta \simeq_n \alpha^{i_0}$ where $\nu = i_0$ satisfies $0 \leq \nu < n_0$.

Lemma 8.4. *Every extension of* $\mathbf{k}$ *contained in* $\mathbf{k}(\sqrt[n]{\alpha})$ *is of the form* $\mathbf{k}(\sqrt[n]{\beta})$ *where* $\beta = \alpha^y$ *for some* y.

Proof. Suppose $\mathbf{k} \subset \mathbf{K} \subset \mathbf{k}(\sqrt[n]{\alpha})$. Let σ generate $G(\mathbf{k}(\sqrt[n]{\alpha}) : \mathbf{k})$. Let the subgroup fixing $\mathbf{K}$ be generated by σ^x where x divides $n_0 = [\mathbf{k}(\sqrt[n]{\alpha}) : \mathbf{k}]$. Let $\sqrt[n]{\alpha} = \sqrt[n_0]{\alpha_0}$. A typical element of $\mathbf{k}(\sqrt[n]{\alpha})$ is

$$\sum_{i=0}^{n_0-1} \gamma_i \left(\sqrt[n_0]{\alpha_0} \right)^i . \tag{8.4}$$

Applying σ^x to (8.4) yields

$$\sum_{i=0}^{n_0-1} \gamma_i \zeta_\sigma^{xi} \left(\sqrt[n_0]{\alpha_0} \right)^i . \tag{8.5}$$

An element is in $\mathbf{K}$ if and only if (8.4) and (8.5) coincide, which is equivalent to $\gamma_i = \gamma_i \zeta_\sigma^{xi}$ for $0 \leq i < n_0$. Therefore an element of $\mathbf{k}(\sqrt[n]{\alpha})$ is in $\mathbf{K}$ if and only if either $\gamma_i = 0$ or xi is divisible by n_0 for $0 \leq i < n_0$. Since x divides n_0 then γ_i may be non-zero only for $i = jn_0/x$, $0 \leq j < x$, so elements of $\mathbf{K}$ are of the form

$$\sum_{j=0}^{x-1} \gamma_{jn_0/x} \zeta_\sigma^{jn_0} \left(\sqrt[n_0]{\alpha_0} \right)^{jn_0/x} = \sum_{j=0}^{x-1} \gamma_{jn_0/x} \zeta_\sigma^{jn_0} \left(\sqrt[x]{\alpha_0} \right)^j .$$

Then $\mathbf{K} = \mathbf{k}(\sqrt[x]{\alpha_0})$. Putting $n_0 = xy$ then $\sqrt[x]{\alpha_0} = \sqrt[n_0]{\alpha_0^y} = \sqrt[n]{\alpha^y}$, so $\mathbf{K} = \mathbf{k}(\sqrt[n]{\alpha^y})$.

Lemma 8.5. *Suppose that* $\alpha_1, \ldots, \alpha_r$ *are independent elements modulo* $(\mathbf{k}^*)^n$. *Then* $\mathbf{K} = \mathbf{k}\left(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_r}\right)$ *has degree* n^r *over* $\mathbf{k}$. *Every cyclic subfield is of the form* $\mathbf{k}\left(\sqrt[n]{\alpha_1^{x_1} \ldots \alpha_r^{x_r}}\right)$. *Galois group* $G(\mathbf{K} : \mathbf{k})$ *is canonically isomorphic to the product of the* n*-th roots of unity with itself* r *times, where* $\sigma \in G$ *corresponds to* $(\zeta_1, \ldots, \zeta_r)$ *if* $\sigma\left(\sqrt[n]{\alpha_i}\right) = \zeta_i\left(\sqrt[n]{\alpha_i}\right)$.

Proof. The case for $r = 1$ is established by lemma 8.2 and lemma 8.4. The general case will be proved by induction. Suppose that the conclusion holds for $r-1$. Then $[\mathbf{k}\left(\sqrt[n]{\alpha_2}, \ldots, \sqrt[n]{\alpha_r}\right) : \mathbf{k}] = n^{r-1}$, and every subfield of $\mathbf{k}\left(\sqrt[n]{\alpha_2}, \ldots, \sqrt[n]{\alpha_r}\right)$ is of the form $\mathbf{k}\left(\sqrt[n]{\alpha_2^{x_2} \ldots \alpha_r^{x_r}}\right)$. Let $\mathbf{L} = \mathbf{k}\left(\sqrt[n]{\alpha_2}, \ldots, \sqrt[n]{\alpha_r}\right) \cap \mathbf{k}(\sqrt[n]{\alpha_1})$. Then

$$\mathbf{L} = \mathbf{k}\left(\sqrt[n]{\alpha_2^{x_2} \ldots \alpha_r^{x_r}}\right) = \mathbf{k}\left(\sqrt[n]{\alpha_1^{x_1}}\right).$$

By lemma 8.3 we have $\alpha_2^{x_2} \ldots \alpha_r^{x_r} \simeq_n \alpha_1^{x x_1}$, or $\alpha_1^{-x x_1} \alpha_2^{x_2} \ldots \alpha_r^{x_r} \simeq_n 1$. Since $\alpha_1, \ldots, \alpha_r$ are independent modulo $(\mathbf{k}^*)^n$, we have

$$-x x_1 = x_2 = \cdots = x_r = 0 (\bmod n).$$

This shows $\alpha_2^{x_2} \ldots \alpha_r^{x_r} \simeq_n 1$, so $\mathbf{k}\left(\sqrt[n]{\alpha_2^{x_2} \ldots \alpha_r^{x_r}}\right) = \mathbf{k}$. By lemma 2.10, we have $[\mathbf{K} : \mathbf{k}] = n^r$, establishing the first claim. By lemma 2.11, there is an isomorphism $\sigma \to (\sigma_1, \sigma')$ of Galois groups

$$G\big(\mathbf{k}\left(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_r}\right) : \mathbf{k}\big) \simeq G\big(\mathbf{k}\left(\sqrt[n]{\alpha_1}\right) : \mathbf{k}\big) \times G\big(\mathbf{k}\left(\sqrt[n]{\alpha_2}, \ldots, \sqrt[n]{\alpha_r}\right) : \mathbf{k}\big).$$

By lemma 8.2, $G(\mathbf{k}\left(\sqrt[n]{\alpha_1}\right) : \mathbf{k})$ is isomorphic to the group of n-th roots of unity with $\sigma_1 \to \zeta_1$ if $\sigma_1\left(\sqrt[n]{\alpha_1}\right) = \zeta_1\left(\sqrt[n]{\alpha_1}\right)$. By the induction hypothesis, Galois group $G\big(\mathbf{k}\left(\sqrt[n]{\alpha_2}, \ldots, \sqrt[n]{\alpha_r}\right) : \mathbf{k}\big)$ is isomorphic to the product of $r-1$ copies of the n-th roots of unity with $\sigma' \to (\zeta_2, \ldots, \zeta_r)$ if $\sigma'\left(\sqrt[n]{\alpha_i}\right) = \zeta_i\left(\sqrt[n]{\alpha_i}\right)$. The composite map $\sigma \to (\zeta_1, \zeta_2, \ldots, \zeta_r)$ is an isomorphism between $G\big(\mathbf{k}\left(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_r}\right) : \mathbf{k}\big)$ and the product of r copies of the n-th roots of unity.

It remains to prove the claim about cyclic subfields. Suppose that $\mathbf{k} \subset \mathbf{L} \subset \mathbf{k}\left(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_r}\right)$ and $G(\mathbf{L} : \mathbf{k})$ is cyclic. Let τ generate $G(\mathbf{L} : \mathbf{k})$. Choose ζ to be some primitive n-th root of unity. For each $i = 1, \ldots, r$, let σ_i be the element of $G\big(\mathbf{k}\left(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_r}\right) : \mathbf{k}\big)$ corresponding to $(1, \ldots, \zeta, \ldots, 1)$. Every element of $G\big(\mathbf{k}\left(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_r}\right) : \mathbf{k}\big)$ is of the form $\prod_{i=1}^{r} \sigma_i^{y_i}$. Let the restriction of σ_i to $\mathbf{L}$ be τ^{x_i}. Then $\prod_{i=1}^{r} \sigma_i^{y_i}$ leaves elements of $\mathbf{L}$ fixed if and only if $\prod_{i=1}^{r} \tau^{x_i y_i} = 1$, or

$$\sum_{i=1}^{r} x_i y_i = 0 (\bmod m) \quad \text{where } m = [\mathbf{L} : \mathbf{k}]. \tag{8.6}$$

Every element α of $\mathbf{k}\left(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_r}\right)$ may be uniquely represented as

$$\alpha = \sum_{k_1=1}^{n-1} \cdots \sum_{k_r=1}^{n-1} \gamma_{k_1 \ldots k_r} \left(\sqrt[n]{\alpha_1}\right)^{k_1} \ldots \left(\sqrt[n]{\alpha_r}\right)^{k_r}. \tag{8.7}$$

The result of applying $\sigma = \prod_{i=1}^{r} \sigma_i^{y_i}$ to α is

$$\sigma(\alpha) = \sum_{k_1=1}^{n-1} \cdots \sum_{k_r=1}^{n-1} \gamma_{k_1 \ldots k_r} \zeta^{y_1 k_1 + \cdots + y_r k_r} \left(\sqrt[n]{\alpha_1}\right)^{k_1} \ldots \left(\sqrt[n]{\alpha_r}\right)^{k_r}.$$

Then α is in $\mathbf{L}$ if and only if $\gamma_{k_1 \ldots k_r} = \gamma_{k_1 \ldots k_r} \zeta^{y_1 k_1 + \cdots + y_r k_r}$ for all $(y_1, \ldots, y_r)$ satisfying (8.6), which is equivalent to

$$\textit{either } \gamma_{k_1 \ldots k_r} = 0, \textit{ or } \sum_{i=1}^{r} x_i y_i = 0 (\operatorname{mod} m) \Longrightarrow \sum_{i=1}^{r} y_i k_i = 0 (\operatorname{mod} n).$$

Therefore elements of $\mathbf{L}$ have the form

$$\alpha = \sum_{(k_1, \ldots, k_r) \in S} \gamma_{k_1 \ldots k_r} \left(\sqrt[n]{\alpha_1}\right)^{k_1} \ldots \left(\sqrt[n]{\alpha_r}\right)^{k_r} \tag{8.8}$$

where

$$S = \left\{ (k_1, \ldots, k_r) \;\middle|\; \sum_{i=1}^{r} x_i y_i = 0 (\operatorname{mod} m) \Longrightarrow \sum_{i=1}^{r} y_i k_i = 0 (\operatorname{mod} n) \right\}.$$

Since $G(\mathbf{L} : \mathbf{k})$ is cyclic of order m and $G[\mathbf{K} : \mathbf{k}]$ is the product of r copies of cyclic groups of order n, it follows that m must divide n. Let $md = n$. Since $\sum_{i=1}^{r} x_i y_i = 0 (\operatorname{mod} m)$ if and only if $\sum_{i=1}^{r} d x_i y_i = 0 (\operatorname{mod} n)$, the condition for set S is

$$S = \left\{ (k_1, \ldots, k_r) \;\middle|\; \sum_{i=1}^{r} d x_i y_i = 0 (\operatorname{mod} n) \Longrightarrow \sum_{i=1}^{r} y_i k_i = 0 (\operatorname{mod} n) \right\}.$$

We claim that if $(k_1, \ldots, k_r)$ is in S then there is an integer a so that $k_i = a d x_i (\operatorname{mod} n)$ for $1 \leq i \leq n$. Assuming this for the moment, then for $(k_1, \ldots, k_r)$ in S we have

$$\begin{aligned} \left(\sqrt[n]{\alpha_1}\right)^{k_1} \ldots \left(\sqrt[n]{\alpha_r}\right)^{k_r} &= \left(\left(\sqrt[n]{\alpha_1}\right)^{d x_1} \ldots \left(\sqrt[n]{\alpha_r}\right)^{d x_r} \right)^a \alpha_1^{b_1} \ldots \alpha_r^{b_r} \\ &= \left(\sqrt[n]{\alpha_1^{d x_1} \ldots \alpha_r^{d x_r}} \right)^a \alpha_1^{b_1} \ldots \alpha_r^{b_r}. \end{aligned}$$

We therefore have

$$\mathbf{L} \subset \mathbf{k}\left(\sqrt[n]{\alpha_1^{dx_1} \dots \alpha_r^{dx_r}}\right).$$

Note that $(dx_1, \dots, dx_r)$ is in the set S, so $\alpha = \sqrt[n]{\alpha_1^{dx_1} \dots \alpha_r^{dx_r}}$ is an element of $\mathbf{L}$, and we have

$$\mathbf{L} = \mathbf{k}\left(\sqrt[n]{\alpha_1^{dx_1} \dots \alpha_r^{dx_r}}\right).$$

We still need to establish the claim about the existence of integer a, which is established by the following lemma.

LEMMA 8.6. *If $(dx_1, \dots, dx_r)$ and $(k_1, \dots, k_r)$ satisfy the condition*

$$\sum_{i=1}^{r} dx_i y_i = 0(\text{mod } n) \Longrightarrow \sum_{i=1}^{r} y_i k_i = 0(\text{mod } n),$$

then there exists an integer a so that $k_i = a dx_i(\text{mod } n)$ for $1 \leq i \leq r$.

PROOF. The proof is by induction. Take $r = 1$. The hypothesis is that given dx_1 and k_1, if $dx_1 y_1 = 0(\text{mod } n)$ then $y_1 k_1 = 0(\text{mod } n)$. Let c be the greatest common divisor of dx_1 and n. Then $(n/c)dx_1 = 0(\text{mod } n)$, so $(n/c)k_1 = 0(\text{mod } n)$. Therefore c divides k_1. Since dx_1/c and n/c are relatively prime, then dx_1/c has an inverse modulo n/c, so there exists an integer a such that $a(dx_1/c) = (k_1/c)(\text{mod } n/c)$, or $a dx_1 = k_1(\text{mod } n)$.

Suppose that the lemma holds for the case $r-1$. If $(dx_2, \dots, dx_r)$ and $(k_2', \dots, k_r')$ satisfy the condition that if $\sum_{i=2}^{r} dx_i y_i = 0(\text{mod } n)$ implies $\sum_{i=2}^{r} y_i k_i' = 0(\text{mod } n)$, then there exists an integer a_2 so that $k_i' = a_2 dx_i(\text{mod } n)$ for $2 \leq i \leq r$. Now suppose that $(dx_1, \dots, dx_r)$ and $(k_1, \dots, k_r)$ satisfy the condition that $\sum_{i=1}^{r} dx_i y_i = 0(\text{mod } n)$ implies $\sum_{i=1}^{r} y_i k_i = 0(\text{mod } n)$.

Let y_1 be such that $dx_1 y_1 = 0(\text{mod } n)$. Take $(y_1, \dots, y_r) = (y_1, 0, \dots, 0)$. Then $\sum_{i=1}^{r} dx_i y_i = 0(\text{mod } n)$, so $\sum_{i=1}^{r} y_i k_i = y_1 k_1 = 0(\text{mod } n)$. Since dx_1 and k_1 satisfy the hypothesis for $r = 1$, then there exists an integer a_1 so that $k_1 = a_1 dx_1(\text{mod } n)$. Put

$$\begin{aligned} k_1' &= k_1 - a_1 dx_1 \\ k_2' &= k_2 - a_1 dx_2 \\ &\vdots \\ k_r' &= k_r - a_1 dx_r \end{aligned} \tag{8.8}$$

Let c be the greatest common divisor of dx_1 and n. We want to show that $\big((nd/c)x_2, \ldots, (nd/c)x_r\big)$ and $(k_2', \ldots, k_r')$ satisfy the hypothesis for the case $r-1$. Suppose that $\sum_{i=2}^{r}(nd/c)x_iy_i = 0(\mathrm{mod}\ n)$. Then $\sum_{i=2}^{r} dx_iy_i = 0(\mathrm{mod}\ c)$. Put $c = \lambda_1 dx_1 + \lambda_2 n$. Then

$$\sum_{i=2}^{r} dx_iy_i = c\lambda_3 = \lambda_1\lambda_3 dx_1 + \lambda_2\lambda_3 n,$$

or

$$-\lambda_1\lambda_3 dx_1 + \sum_{i=2}^{r} dx_iy_i = 0(\mathrm{mod}\ n).$$

Putting $y_1 = -\lambda_1\lambda_3$, we have

$$\sum_{i=1}^{r} dx_iy_i = 0(\mathrm{mod}\ n).$$

Then

$$\sum_{i=1}^{r} y_ik_i' = \sum_{i=1}^{r} y_i(k_i - a_1dx_i) = \sum_{i=1}^{r} y_ik_i - a_1\sum_{i=1}^{r} dx_iy_i = 0 - 0 = 0(\mathrm{mod}\ n).$$

We have $k_1' = 0(\mathrm{mod}\ n)$ by (8.8), so the term $i = 1$ may be deleted to obtain

$$\sum_{i=2}^{r} k_i'y_i = 0(\mathrm{mod}\ n).$$

The hypothesis for the case $r-1$ is satisfied, so there exists an integer a_2 so that $k_i' = a_2(nd/c)x_i(\mathrm{mod}\ n)$ for $2 \le i \le r$. For $i = 1$, we have $k_1' = 0 = a_2(nd/c)x_1(\mathrm{mod}\ n)$ because c divides dx_1, so

$$k_i' = a_2\frac{n}{c}dx_i(\mathrm{mod}\ n) \text{ for } 1 \le i \le r.$$

Finally, we have

$$k_i = k_i' + a_1dx_i = a_2\frac{n}{c}dx_i + a_1dx_i = \left(a_2\frac{n}{c} + a_1\right)dx_i(\mathrm{mod}\ n) \text{ for } 1 \le i \le r.$$

Put $a = a_2n/c + a_1$. Then $k_i = adx_i(\mathrm{mod}\ n)$ for $1 \le i \le n$. This completes the proof of lemma 8.6 and also of lemma 8.5.

LEMMA 8.7. *Suppose that n is prime and $\mathbf{k}$ contains the n-th roots of unity. If $\mathbf{K}/\mathbf{k}$ is an extension of degree n, then there is an element α in $\mathbf{k}$ so that $\mathbf{K} = \mathbf{k}(\sqrt[n]{\alpha})$.*

PROOF. Let θ be an element of $\mathbf{K}$ that is not in $\mathbf{k}$. Then $\mathbf{K} = \mathbf{k}(\theta)$ since there are no intermediate subfields. Let σ be a generator of $G(\mathbf{K} : \mathbf{k})$, which is cyclic of order n. Then $\theta, \theta^{\sigma}, \dots, \theta^{\sigma^{n-1}}$ are all distinct. The matrix

$$\Theta = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \theta & \theta^{\sigma} & \dots & \theta^{\sigma^{n-1}} \\ \vdots & & & \vdots \\ \theta^{n-1} & (\theta^{\sigma})^{n-1} & \dots & \left(\theta^{\sigma^{n-1}}\right)^{n-1} \end{pmatrix}$$

is a non-singular Vandermonde matrix. Let $\zeta \neq 1$ be an n-th root of unity. Θ does not annihilate column vector $Z = (1, \zeta, \dots, \zeta^{n-1})^t$, so if $(\beta_0, \dots, \beta_{n-1})^t = \Theta Z$ then not all of the β_j are zero. Choosing j so that $\beta_j \neq 0$, we have

$$\beta_j = \theta^j + \dots + \left(\theta^{\sigma^i}\right)^j \zeta^i + \dots + \left(\theta^{\sigma^{n-1}}\right)^j \zeta^{n-1} \neq 0.$$

Apply σ to both sides to obtain

$$\begin{aligned} \beta_j^{\sigma} &= (\theta^{\sigma})^j + \dots + \left(\theta^{\sigma^{i+1}}\right)^j \zeta^i + \dots + \left(\theta^{\sigma^n}\right)^j \zeta^{n-1} \\ &= \left(\theta^j\right) \zeta^{-1} + \dots + \left(\theta^{\sigma^i}\right)^j \zeta^{i-1} + \dots + \left(\theta^{\sigma^{n-1}}\right)^j \zeta^{n-2} \\ &= \beta_j \zeta^{-1}. \end{aligned}$$

Therefore $\beta_j \notin \mathbf{k}$ and $(\beta_j^n)^{\sigma} = (\beta_j^{\sigma})^n = \beta_j^n$, so β_j^n is in $\mathbf{k}$. Take $\alpha = \beta_j^n$. Then $\mathbf{K} = \mathbf{k}(\sqrt[n]{\alpha})$.

LEMMA 8.8. *Suppose that $\mathbf{k}$ contain the n-th roots of unity, and let $\zeta \neq 1$ be an n-th root of unity. If $\zeta = 1 (\mathrm{mod}\ p)$ then p must divide (n).*

PROOF. If $\zeta \neq 1$ then ζ is a root of $x^{n-1} + \dots + x + 1$, so

$$\zeta^{n-1} + \dots + \zeta + 1 = 0.$$

If $\zeta = 1 (\mathrm{mod}\ p)$ then $n = 0 (\mathrm{mod}\ p)$.

LEMMA 8.9. *Let p be a prime of $\mathbf{k}$ such that p does not divide n and p does not divide element α of $\mathbf{k}$. Then p does not ramify in $\mathbf{k}(\sqrt[n]{\alpha})$.*

PROOF. Let $\mathbf{K} = \mathbf{k}(\sqrt[n]{\alpha})$. Let $\wp$ be a prime of $\mathbf{K}$ dividing p. Element α is not divisible by p, so α is a unit in $\mathbf{o}_p$. We have $|\sqrt[n]{\alpha}|_{\wp}^n = |\alpha|_{\wp} = |\alpha|_p^{ef} = 1$, so $\sqrt[n]{\alpha}$

is a unit in $\mathbf{O}_\wp$. If σ is in $G(\mathbf{K} : \mathbf{k})$ then there is an n-root of unity ζ so that $\sigma(\sqrt[n]{\alpha}) = \zeta\sqrt[n]{\alpha}$. Suppose that σ is in the inertial group of $\wp$. Then

$$\sigma\left(\sqrt[n]{\alpha}\right) = \sqrt[n]{\alpha}(\text{mod } \wp).$$

Then $\zeta\sqrt[n]{\alpha} = \sqrt[n]{\alpha}(\text{mod } \wp)$. Since $\sqrt[n]{\alpha}$ is a unit in $\mathbf{O}_\wp$, we have $\zeta = 1(\text{mod } \wp)$. Then $\zeta = 1$ by lemma 8.8, which shows that the inertial group is trivial. Therefore p does not ramify in $\mathbf{k}(\sqrt[n]{\alpha})$.

LEMMA 8.10. *The p-adic field $\mathbf{k}_p$ contains only a finite number of roots of unity.*

PROOF. If $N > b/(p-1)$ as defined in lemma 4.12 then there is an isomorphism between subgroups $W = \{\alpha \in \mathbf{k}^* \mid \text{ord}_p(\alpha - 1) > N\}$ and $\{y \in \mathbf{o}_p \mid \text{ord}_p(y) > N\}$. W contains no root of unity other than $\alpha = 1$. Therefore the only root of unity in the kernel of the homomorphism $\mathbf{o}_p^* \to \mathbf{o}_p^*/W$ is $\alpha = 1$. The number of roots of unity in $\mathbf{o}_p^*$ cannot be greater than $[\mathbf{o}_p^* : W] < \mathrm{N}p^{N+1}$.

LEMMA 8.11. *If the p-adic field contains the n-th roots of unity then*

$$[\mathbf{k}_p^* : (\mathbf{k}_p^*)^n] = n^2(\mathrm{N}p)^a \textit{ and } [\mathbf{u}_p : \mathbf{u}_p^n] = n(\mathrm{N}p)^a$$

where $n\mathbf{o}_p = p^a$.

PROOF. If $p = (\pi)$ then $\mathbf{k}_p^*$ is the direct product $\langle\pi\rangle\mathbf{u}_p$, so

$$[\mathbf{k}_p^* : (\mathbf{k}^*)^n] = n[\mathbf{u}_p : (\mathbf{u}_p)^n].$$

Let V be the group of roots of unity in $\mathbf{k}_p$. Then V is a cyclic group of order divisible by n. Then

$$[\mathbf{u}_p : (\mathbf{u}_p)^n] = [\mathbf{u}_p : V(\mathbf{u}_p)^n][V(\mathbf{u}_p)^n : (\mathbf{u}_p)^n]$$

and

$$[V(\mathbf{u}_p)^n : (\mathbf{u}_p)^n] = [V : V \cap (\mathbf{u}_p)^n] = [V : V^n] = n,$$

so

$$[\mathbf{k}_p^* : (\mathbf{k}^*)^n] = n^2[\mathbf{u}_p : V(\mathbf{u}_p)^n]. \tag{8.9}$$

Suppose N is sufficiently large so that $\log(x)$ is defined on $W = 1 + p^N$. Then $[\mathbf{u}_p : W]$ is finite. Let m be an integer divisible by $[\mathbf{u}_p : W]$ and by the order of V. Consider the map $\alpha \to \alpha^m \to \alpha^m\mathbf{u}_p^{nm}$.

$$\mathbf{u}_p \to (\mathbf{u}_p)^m \to (\mathbf{u}_p)^m/(\mathbf{u}_p)^{nm}.$$

The kernel contains $V\mathbf{u}_p^n$. Also, suppose α is in the kernel. Then $\alpha^m \in \mathbf{u}_p^{nm}$, so $\alpha^m = \beta^{nm}$, or $(\alpha\beta^{-n})^m = 1$. We have $\alpha\beta^{-n} = \zeta \in V$, or $\alpha = \zeta\beta^n \in V\mathbf{u}_p^n$, so the kernel is exactly $V\mathbf{u}_p^n$. This shows

$$[\mathbf{u}_p : V\mathbf{u}_p^n] = [\mathbf{u}_p^m : \mathbf{u}_p^{mn}]. \tag{8.10}$$

The map $x \to \log(x)$ maps W isomorphically onto p^N. Let M be the image of $\mathbf{u}_p^m$. (We have $\mathbf{u}_p^m \subset W$ since m is divisible by $[\mathbf{u}_p : W]$.) We claim that M is a $\mathbf{Z}_q$ module where $q = \mathbf{Z} \cap p$ is the rational prime which p divides. Let $A = \sum_{i=0}^{\infty} a_i q^i$ be an element of $\mathbf{Z}_q$, and put

$$A_k = a_0 + a_1 q + \cdots + a_k q^k, \quad 0 \le a_i < q.$$

If $y \in M$, let $y = \log(x)$ where $x \in \mathbf{u}_p^m$. The $x = x_1^m$ where $x \in \mathbf{u}_p$. Since $x \in W = 1 + p^N$ then $x = 1 + \beta_0 \pi^N$ with $b \in \mathbf{u}_p$. Let $(q) = p^e$ in $\mathbf{o}_p$. Then

$$\begin{aligned} x^q &= (1+\beta_0\pi^N)^q = 1 + q\beta_0\pi^N + \ldots = 1 + \beta_1\pi^{N+1} \\ x^{q^2} &= (1+\beta_1\pi^{N+1})^q = 1 + q\beta_1\pi^{N+1} + \ldots = 1 + \beta_2\pi^{N+2} \end{aligned}$$

There exist elements $\beta_0, \beta_1, \beta_2, \ldots,$ in $\mathbf{u}_p$ depending only on x so that

$$x^{A_k} = \prod_{i=0}^{k} \left(1 + a_i\beta_i\pi^{N+i}\right).$$

This shows that the sequence x^{A_k} converges to an element X of $\mathbf{u}_p$. We have $\log(\lim_{i\to\infty} x^{A_k}) = \lim_{i\to\infty} \log(x^{A_k}) = \lim_{i\to\infty} A_k \log(x)$, so $\log(X) = A\log(x)$. We need to show that X is an m-th power. Let z be an element in $\mathbf{u}_p$ so that $z^m = x$. Then $\left(z^{A_k}\right)^m = x^{A_k}$. There exists a convergent subsequence $z^{A_{k_j}}$ since $\mathbf{u}_p$ is compact. Then

$$\left(\lim_{j\to\infty} z^{A_{k_j}}\right)^m = \lim_{j\to\infty} \left(z^{A_{k_j}}\right)^m = \lim_{j\to\infty} x^{A_{k_j}} = X.$$

This shows that Ay is the image of an m-power, so Ay is in M. This shows M is an $\mathbf{Z}_q$-module.

Next, by lemma 4.13, if $a = \mathrm{ord}_p(n)$ then every element x in $1 + p^{N+a}$ is the n-th power of an element in $1 + p^N$. Therefore, $p^{N+a} \subset M$. This shows that M contains $[\mathbf{k}_p : \mathbf{Q}_q]$ independent elements, i.e., M is a free $\mathbf{Z}_p$ module of the same dimension as $\mathbf{o}_p$. Therefore $M \simeq \mathbf{o}_p$, and $nM \simeq n\mathbf{o}_p$. Then

$$[\mathbf{u}_p^m : \mathbf{u}_p^{nm}] = [M : nM] = [\mathbf{o}_p : n\mathbf{o}_p] = [\mathbf{o}_p : p^a] = (\mathrm{N}p)^a.$$

Using the above formula in (8.9) and (8.10) completes the proof of the lemma.

Lemma 8.12. *Let* $\mathbf{k}$ *be an algebraic number field containing the* n*-th roots of unity. Let* E *be a finite set of primes containing all infinite primes and all primes dividing* n*, and let* $\mathbf{I}_{\mathbf{k}}^n(E) = \prod_{p\in E}(\mathbf{k}_p^*)^n \times \prod_{p\notin E} \mathbf{u}_p$*. If* E *contains* $s+1$ *primes then*

$$[\mathbf{I}_{\mathbf{k}}(E) : \mathbf{I}_{\mathbf{k}}^n(E)] = n^{2(s+1)}.$$

Proof. We have $\mathbf{I}_{\mathbf{k}}(E) = \prod_{p\in E} \mathbf{k}_p^* \times \prod_{p\notin E} \mathbf{u}_p$,so

$$[\mathbf{I}_{\mathbf{k}}(E) : \mathbf{I}_{\mathbf{k}}^n(E)] = \prod_{p\in E} \left[\mathbf{k}_p^* : \left(\mathbf{k}_p^*\right)^n\right].$$

If p is a complex infinite prime of $\mathbf{k}$ then $[\mathbf{k}_p^* : (\mathbf{k}_p^*)^n] = 1$; if p is a real infinite prime then $n = 1$ or $n = 2$, so $[\mathbf{k}_p^* : (\mathbf{k}_p^*)^n] = n$. If p is a finite prime then by lemma 8.11 we have $[\mathbf{k}_p^* : (\mathbf{k}_p^*)^n] = n^2 \mathrm{N}p^{\mathrm{ord}_p(n)}$. Let E contain r_0 finite primes, r_1 real primes and r_2 complex primes. Let E_0 be the set of finite primes in E. We have

$$[\mathbf{I}_{\mathbf{k}}(E) : \mathbf{I}_{\mathbf{k}}^n(E)] = \left(n^{2r_0} \prod_{p\in E_0} \mathrm{N}p^{\mathrm{ord}_p(n)}\right) n^{r_1}. \tag{8.11}$$

Each prime p in E_0 divides some rational prime q, and we have $\mathrm{N}p = \mathrm{N}q^f$ and $\mathrm{ord}_p(n) = e\,\mathrm{ord}_q(n)$. Since E_0 contains all primes dividing n, and $efg = [\mathbf{k} : \mathbf{Q}] = r_1 + 2r_2$, we have

$$\prod_{p\in E_0} \mathrm{N}p^{\mathrm{ord}_p(n)} = \prod_{q|n}\prod_{p|q} \mathrm{N}p^{\mathrm{ord}_p(n)} = \prod_{q|n}\prod_{p|q} \mathrm{N}q^{ef\,\mathrm{ord}_q(n)} = \prod_{q|n} \mathrm{N}q^{efg\,\mathrm{ord}_q(n)} = n^{r_1+2r_2}$$

Using this result in (8.11) produces $n^{2r_0+2r_1+2r_2} = n^{2(s+1)}$.

Reduction to the case of extensions of prime degree n. Every finite abelian group G contains a decomposition $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$ such that G_i/G_{i+1} is cyclic of prime index, so if $\mathbf{K}$ is an abelian extension of $\mathbf{k}$ then there exist extensions $\mathbf{k} = \mathbf{k}_0 \subset \mathbf{k}_1 \subset \cdots \subset \mathbf{k}_r = \mathbf{K}$ such that $\mathbf{k}_{i+1}/\mathbf{k}_i$ is cyclic of prime degree. Lemma 8.14 will show that if the second inequality holds for each extension $\mathbf{k}_{i+1}/\mathbf{k}$ then it will hold for $\mathbf{K}/\mathbf{k}$, after which it will be enough to prove the second inequality for cyclic extensions of prime degree.

Lemma 8.13. *Suppose that* $\mathbf{K}$ *is a finite abelian extension of* $\mathbf{K}_1$ *and* $\mathbf{K}_1$ *is a finite abelian extension of* $\mathbf{k}$*. Then*

$$\left[\mathbf{k}^*\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}\right] \text{ divides } \left[\mathbf{I}_{\mathbf{K}_1} : \mathbf{K}_1^*\mathbf{N}_{\mathbf{K}/\mathbf{K}_1}\mathbf{I}_{\mathbf{K}}\right].$$

PROOF. We have We have

$$\begin{aligned}(8.12)\quad \left[\mathbf{k}^*\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}\right] &= \left[\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{k}} \cap \mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1}\right] \\ &= \left[\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\left(\mathbf{N}_{\mathbf{K}/\mathbf{K}_1}\mathbf{I}_{\mathbf{k}}\right) \cap \mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1}\right] \\ &= \left[\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1} : \left(\mathbf{k}^* \cap \mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1}\right)\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\left(\mathbf{N}_{\mathbf{K}/\mathbf{K}_1}\mathbf{I}_{\mathbf{K}}\right)\right].\end{aligned}$$

Since $\mathbf{k}^* \cap \mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1} \supset \mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{K}_1^*$, the rightmost term of (8.12) divides (8.13).

$$(8.13)\qquad \left[\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1} : \mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\left(\mathbf{K}_1^*\mathbf{N}_{\mathbf{K}/\mathbf{K}_1}\mathbf{I}_{\mathbf{K}}\right)\right]$$

The kernel of the homomorphism in (8.14) contains $\mathbf{K}_1^*\mathbf{N}_{\mathbf{K}/\mathbf{K}_1}\mathbf{I}_{\mathbf{K}}$.

$$(8.14)\qquad \mathbf{I}_{\mathbf{K}_1} \xrightarrow{\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}} \mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{K}_1 \longrightarrow \frac{\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{K}_1}{\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\left(\mathbf{K}_1^*\mathbf{N}_{\mathbf{K}/\mathbf{K}_1}\mathbf{I}_{\mathbf{K}}\right)}$$

Therefore the homomorphism

$$\frac{\mathbf{I}_{\mathbf{K}_1}}{\mathbf{K}_1^*\mathbf{N}_{\mathbf{K}/\mathbf{K}_1}\mathbf{I}_{\mathbf{K}}} \longrightarrow \frac{\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{K}_1}{\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\left(\mathbf{K}_1^*\mathbf{N}_{\mathbf{K}/\mathbf{K}_1}\mathbf{I}_{\mathbf{K}}\right)}$$

is a surjection, so (8.13) must divide $\left[\mathbf{I}_{\mathbf{K}_1} : \mathbf{K}_1^*\mathbf{N}_{\mathbf{K}/\mathbf{K}_1}\mathbf{I}_{\mathbf{K}}\right]$ proving the lemma.

LEMMA 8.14. *Suppose that* $\mathbf{K}$ *is a finite abelian extension of* $\mathbf{K}_1$ *and* $\mathbf{K}_1$ *is a finite abelian extension of* $\mathbf{k}$ *such that the second inequality is valid for* $\mathbf{K}/\mathbf{K}_1$ *and* $\mathbf{K}_1/\mathbf{k}$. *Then the second inequality is valid for* $\mathbf{K}/\mathbf{k}$.

PROOF. We have

$$(8.15)\qquad \left[\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}\right] = \left[\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1}\right]\left[\mathbf{k}^*\mathbf{N}_{\mathbf{K}_1/\mathbf{k}}\mathbf{I}_{\mathbf{K}_1} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}\right].$$

If the second fundamental inequality holds for $\mathbf{K}_1/\mathbf{k}$ then first factor of (8.12) divides $[\mathbf{K}_1 : \mathbf{k}]$, By lemma 8.13, the second factor divides $\left[\mathbf{I}_{\mathbf{K}_1} : \mathbf{K}_1^*\mathbf{N}_{\mathbf{K}/\mathbf{K}_1}\mathbf{I}_{\mathbf{K}}\right]$, which divides $[\mathbf{K} : \mathbf{K}_1]$ if the second fundamental inequality holds for $\mathbf{K}/\mathbf{K}_1$. This shows that the right side of (8.15) divides $[\mathbf{K} : \mathbf{K}_1][\mathbf{K}_1 : \mathbf{k}]$, so $\left[\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}\right]$ divides $[\mathbf{K} : \mathbf{k}]$, proving the second inequality for $\mathbf{K}/\mathbf{k}$.

Reduction to extensions of fields containing n-th roots of unity.

LEMMA 8.15. *If the second fundamental inequality holds for abelian extensions of prime degree n where the ground field contains the n-th roots of unity, then it also holds for any abelian extension of degree n.*

PROOF. Put $\mathbf{Z} = \mathbf{k}(\zeta)$, where ζ is a primitive n-th root of unity. Let $\mathbf{K}/\mathbf{k}$ be an abelian extension of degree n. Since $\mathbf{N}_{\mathbf{KZ}/\mathbf{k}}\mathbf{I}_{\mathbf{KZ}}$ is a subgroup of $\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}$ then $\left[\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}\right]$ divides $\left[\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{N}_{\mathbf{KZ}/\mathbf{k}}\mathbf{I}_{\mathbf{KZ}}\right]$, and for that term we have

$$(8.16)\qquad \left[\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{N}_{\mathbf{KZ}/\mathbf{k}}\mathbf{I}_{\mathbf{KZ}}\right] = \left[\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I}_{\mathbf{Z}}\right]\left[\mathbf{k}^*\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I}_{\mathbf{Z}} : \mathbf{k}^*\mathbf{N}_{\mathbf{KZ}/\mathbf{k}}\mathbf{I}_{\mathbf{KZ}}\right].$$

By lemma 8.13, the second factor on the right side divides $\left[\mathbf{I_Z} : \mathbf{Z}^*\mathbf{N_{KZ/Z}}\mathbf{I_{KZ}}\right]$. Therefore $\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}}\mathbf{I_K}\right]$ divides $\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{Z/k}}\mathbf{I_Z}\right]\left[\mathbf{I_Z} : \mathbf{Z}^*\mathbf{N_{KZ/Z}}\mathbf{I_{KZ}}\right]$. We have $[\mathbf{KZ} : \mathbf{Z}] = [\mathbf{K} : \mathbf{Z} \cap \mathbf{K}]$, and the later divides $[\mathbf{K} : \mathbf{k}] = n$, so $[\mathbf{KZ} : \mathbf{Z}]$ is either 1 or n. By hypothesis, the second inequality holds for $\mathbf{KZ}/\mathbf{Z}$, so $\left[\mathbf{I_Z} : \mathbf{Z}^*\mathbf{N_{KZ/Z}}\mathbf{I_{KZ}}\right]$ divides $[\mathbf{KZ} : \mathbf{Z}]$, which divides n.

If we can show that $\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}}\mathbf{I_K}\right]$ and $\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{Z/k}}\mathbf{I_Z}\right]$ are relatively prime, then $\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}}\mathbf{I_K}\right]$ must divide $\left[\mathbf{I_Z} : \mathbf{Z}^*\mathbf{N_{KZ/Z}}\mathbf{I_{KZ}}\right]$. If p is a prime of $\mathbf{k}$ and $\wp$ a prime of $\mathbf{K}$ dividing p, then every element of $(\mathbf{k}_p^*)^n$ is in $\mathbf{N}_{\mathbf{K}_\wp^*/\mathbf{k}_p^*}\mathbf{K}_\wp^*$. By lemma 7.5, every element of $(\mathbf{I_k})^n$ is in $\mathbf{N_{K/k}}\mathbf{I_K}$. Therefore every element in $\mathbf{I_k}/\mathbf{k}^*\mathbf{N_{K/k}}\mathbf{I_K}$ has order dividing n, so n is the only prime dividing $[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}}\mathbf{I_K}]$. We apply the same argument to $\mathbf{Z}/\mathbf{k}$. The degree of $\mathbf{Z} = \mathbf{k}(\zeta)$ over $\mathbf{k}$ is a divisor of $n-1$, so every element of $(\mathbf{I_k})^{n-1}$ is in $\mathbf{N_{Z/k}}\mathbf{I_Z}$. Therefore only primes dividing $n-1$ can divide $[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{Z/k}}\mathbf{I_Z}]$. This show $\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}}\mathbf{I_K}\right]$ and $\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{Z/k}}\mathbf{I_Z}\right]$ are relatively prime, which completes the proof.

Proof for extensions of prime degree n containing the n-th roots of unity. Suppose that $\mathbf{K}/\mathbf{k}$ is an extension of prime degree n, and $\mathbf{k}$ contains the n-th roots of unity. By lemma 8.7, $\mathbf{K} = \mathbf{k}(\sqrt[n]{\beta_0})$ where β_0 is in $\mathbf{K}$ but not in $(\mathbf{k}^*)^n$. Let E be a finite set of primes of $\mathbf{k}$ containing all primes dividing β_0, all primes dividing n, all infinite primes, and such that $\mathbf{I_k} = \mathbf{k}^*\mathbf{I_k}(E)$ (lemma 7.11). Let $\mathbf{I}^n_{\mathbf{k}}(E)$ be the set

$$\mathbf{I}^n_{\mathbf{k}}(E) = \left\{\mathbf{i} \in \mathbf{I_k} \mid \mathbf{i}_p \in \mathbf{u}_p \text{ if } p \notin E;\ \mathbf{i}_p \in \left(\mathbf{k}_p^*\right)^n \text{ if } p \in E\right\}.$$

By lemma 4.7 (every unit in an unramified extension is a norm) and lemma 7.5 (an idele is a norm if every coordinate is a local norm), we have $\mathbf{I}^n_{\mathbf{k}}(E) \subset \mathbf{N_{K/k}}\mathbf{I_K}$. Therefore

$$\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}}\mathbf{I_K}\right] = \frac{[\mathbf{I_k} : \mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E)]}{\left[\mathbf{k}^*\mathbf{N_{K/k}}\mathbf{I_K} : \mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E)\right]}. \tag{8.17}$$

The next two lemmas compute the right side of (8.17).

Lemma 8.16. $[\mathbf{I_k} : \mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E)] = n^{s+1}$.

Proof. We have

$$\begin{aligned}
(8.18)\quad [\mathbf{I_k} : \mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E)] &= [\mathbf{k}^*\mathbf{I_k}(E) : \mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E)] = [\mathbf{I_k}(E) : \mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E) \cap \mathbf{I}_k(E)] \\
&= [\mathbf{I_k}(E) : \mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E)] = \frac{[\mathbf{I_k}(E) : \mathbf{I}^n_{\mathbf{k}}(E)]}{[\mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E) : \mathbf{I}^n_{\mathbf{k}}(E)]} = \frac{[\mathbf{I_k}(E) : \mathbf{I}^n_{\mathbf{k}}(E)]}{[\mathbf{k}^*(E) : \mathbf{k}^*(E) \cap \mathbf{I}^n_{\mathbf{k}}(E)]} \\
&= \frac{[\mathbf{I_k}(E) : \mathbf{I}^n_{\mathbf{k}}(E)]}{[\mathbf{k}^*(E) : \mathbf{k}^*(E)^n]}\,[\mathbf{k}^*(E) \cap \mathbf{I}^n_{\mathbf{k}}(E) : \mathbf{k}^*(E)^n]\,.
\end{aligned}$$

The rightmost expression in (8.18) contains three subexpressions. As to the first, by lemma 8.13 we have

$$[\mathbf{I_k}(E) : \mathbf{I_k}^n(E)] = n^{2(s+1)}.$$

As to the second, by the unit theorem $\mathbf{k}^*(E)$ is the direct product of a finite group (order divisible by n) and s infinite cyclic groups, so $\mathbf{k}(E)/\mathbf{k}^n(E)$ is the direct product of $s+1$ cyclic groups of order n. Therefore the index is

$$[\mathbf{k}(E) : \mathbf{k}^n(E)] = n^{s+1}.$$

Finally, we consider the third subexpression. Let θ be an element of $\mathbf{k}^*(E) \cap \mathbf{I_k}^n(E)$. We will show that θ is in $\mathbf{k}^*(E)^n$. Suppose that $\mathbf{i}$ is in $\mathbf{I_k}(E)$. Let p be any prime of $\mathbf{k}$ and $\wp$ any prime of $\mathbf{K}' = \mathbf{k}(\sqrt[n]{\theta})$ dividing p. If p is in E then θ is an n-th power in $\mathbf{k}_p^*$ so $\mathbf{K}'_\wp = \mathbf{k}_p$, and if p is not in E then $\mathbf{K}'_\wp/\mathbf{k}_p$ is unramified so $\mathbf{i}_p$ is in $\mathbf{N}_{\mathbf{K}'_\wp/\mathbf{k}_p}(K'_\wp)^*$ by lemma 4.7. Since $\mathbf{i}$ is a norm everywhere locally then, by lemma 7.5, $\mathbf{i}$ is in $\mathbf{N}_{\mathbf{k}(\sqrt[n]{\theta})/\mathbf{k}}\mathbf{I}_{\mathbf{k}(\sqrt[n]{\theta})}$. This show that $\mathbf{I_k}(E)$ is contained in $\mathbf{N}_{\mathbf{k}(\sqrt[n]{\theta})/\mathbf{k}}\mathbf{I}_{\mathbf{k}(\sqrt[n]{\theta})}$. Since $\mathbf{I_k} = \mathbf{k}^*\mathbf{I_k}(E)$ then $\mathbf{I_k}$ is contained in $\mathbf{k}^*\mathbf{N}_{\mathbf{k}(\sqrt[n]{\theta})/\mathbf{k}}\mathbf{I}_{\mathbf{k}(\sqrt[n]{\theta})}$, so

$$\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N}_{\mathbf{k}(\sqrt[n]{\theta})/\mathbf{k}}\mathbf{I}_{\mathbf{k}(\sqrt[n]{\theta})}\right] = 1. \tag{8.19}$$

Extension $\mathbf{k}(\sqrt[n]{\theta})/\mathbf{k}$ is cyclic so the first fundamental inequality applies, and we conclude that $[\mathbf{k}(\sqrt[n]{\theta}) : \mathbf{k}] = 1$ because of (8.19). We have $\mathbf{k}(\sqrt[n]{\theta}) = \mathbf{k}$, so θ is in $\mathbf{k}^*(E)^n$. This proves that $\mathbf{k}^*(E) \cap \mathbf{I_k}^n(E) \subset \mathbf{k}^*(E)^n$, so

$$[\mathbf{k}^*(E) \cap \mathbf{I_k}^n(E) : \mathbf{k}^*(E)^n] = 1. \tag{8.19a}$$

Applying these three results to (8.18), we obtain the desired result

$$[\mathbf{I_k} : \mathbf{k}^*\mathbf{I_k}^n(E)] = \frac{n^{2(s+1)}}{n^{s+1}} = n^{s+1}.$$

Remark. By formula (8.17) and lemma 8.16, we know $\left[\mathbf{k}^*\mathbf{N_{K/k}I_K} : \mathbf{k}^*\mathbf{I_k}^n(E)\right]$ divides n^{s+1}. If we can find ideles $\mathbf{i}_1, \ldots, \mathbf{i}_s$ in $\mathbf{N_{K/k}I_K}$ so that $\mathbf{i}_1^{a_1} \ldots \mathbf{i}_s^{a_s}$ is in $\mathbf{k}^*\mathbf{I_k}^n(E)$ only if the exponents a_i all satisfy $a_i = 0 (\mathrm{mod}\ n)$, this would show that there are at least n^s distinct cosets of $\mathbf{k}^*\mathbf{I_k}^n(E)$ in $\mathbf{k}^*\mathbf{N_{k/k}I_K}$, which would show that $[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}I_k}]$ is either n or 1, proving the second fundamental inequality.

Remark. The following two observations will be needed in chapter 11. First, we have

$$\begin{aligned}[\mathbf{k}^*(E)\mathbf{I_k}^n(E) : \mathbf{I_k}^n(E)] &= [\mathbf{k}^*(E) : \mathbf{k}^*(E) \cap \mathbf{I_k}^n(E)] \\ &= \frac{[\mathbf{k}^*(E) : \mathbf{k}^*(E)^n]}{[\mathbf{k}^*(E) \cap \mathbf{I_k}^n(E) : \mathbf{k}^*(E)^n]} = \frac{n^{s+1}}{1} = n^{s+1}\end{aligned}$$

Also, the kernel of the map $\mathbf{k}^*(E) \to \frac{\mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E)}{\mathbf{I}^n_{\mathbf{k}}(E)}$ is $\mathbf{k}^*(E) \cap \mathbf{I}^n_{\mathbf{k}}(E) = \mathbf{k}^*(E)^n$, so

$$\frac{\mathbf{k}^*(E)}{\mathbf{k}^*(E)^n} \simeq \frac{\mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E)}{\mathbf{I}^n_{\mathbf{k}}(E)}.$$

Lemma 8.17. $\left[\mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}} : \mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E)\right]$ *is either* n^s *or* n^{s+1}.

Proof. As stated in the proof of lemma 8.17, $\mathbf{k}^*(E)/\mathbf{k}^*(E)^n$ is the direct product of $s+1$ cyclic groups of order n, so the group is a vector space of dimension $s+1$ over finite field $\mathbf{Z}_n$. Element β_0 is in $\mathbf{k}^*(E)$ but not in $\mathbf{k}^*(E)^n$, so the element β_0 can be extended to a basis $\beta_0, \beta_1, \ldots, \beta_s$ of $\mathbf{k}^*(E)/\mathbf{k}^*(E)^n$. These elements are independent modulo $(\mathbf{k}^*)^n$ because if $\beta_0^{a_0} \ldots \beta_s^{a_s} = \gamma^n$ with γ in $(\mathbf{k}^*)^n$, then γ must be in $\mathbf{k}^*(E)$, so the exponents a_i must all be divisible by n. Put

$$\begin{aligned} \mathbf{T} &= \mathbf{k}\left(\sqrt[n]{\beta_0}, \ldots, \sqrt[n]{\beta_s}\right) \\ \mathbf{T}^{(j)} &= \mathbf{k}\left(\sqrt[n]{\beta_0}, \ldots, \sqrt[n]{\beta_{j-1}}, \sqrt[n]{\beta_{j+1}} \ldots, \sqrt[n]{\beta_s}\right) \qquad 0 < j \le s \end{aligned}$$

By lemma 8.5, we have $[\mathbf{T} : \mathbf{k}] = n^{s+1}$ and $[\mathbf{T}^{(j)} : \mathbf{k}] = n^s$.

There exist infinitely many primes of $\mathbf{T}^{(j)}$ which do not split completely in $\mathbf{T}$, because otherwise the Artin symbols for extension $\mathbf{T}/\mathbf{T}^{(j)}$ would be trivial except for a finite set of primes, so the trivial homomorphism would serve to extend $\phi_{\mathbf{T}/\mathbf{T}^{(j)}}$ By the corollary to the first fundamental inequality (Proposition 2.21), homomorphism $\phi_{\mathbf{T}/\mathbf{T}^{(j)}}$ maps onto $G(\mathbf{T} : \mathbf{T}^{(j)})$, so we would have $[\mathbf{T} : \mathbf{T}^{(j)}] = 1$, which is impossible.

For $1 \le j \le s$, choose a prime $q^{(j)}$ in $\mathbf{T}^{(j)}$ which does not split completely in $\mathbf{T}$, divides no prime in E and is not ramified in $\mathbf{T}$. Let $\wp_j$ be a prime of $\mathbf{T}$ dividing $q^{(j)}$, and let p_j be the prime of $\mathbf{k}$ which $q^{(j)}$ divides. For prime $q^{(j)}$ we have $[\mathbf{T} : \mathbf{T}^{(j)}] = n = efg$ with $e = 1$ and $g < n$. Therefore $g = 1$ and $f = n$, so $[\mathbf{T}_{\wp_j} : \mathbf{T}^{(j)}_{q^{(j)}}] = ef = n$. Since $\mathbf{T} = \mathbf{T}^{(j)}(\sqrt[n]{\beta_j})$, this means β_j cannot be in $\mathbf{u}^n_{p_j}$. We have $[\mathbf{u}_{p_j} : \mathbf{u}^n_{p_j}] = n$ by lemma 8.11 (since all the primes of $\mathbf{k}$ dividing n are in E and p_j is not in E), so β_j generates $\mathbf{u}_{p_j}/\mathbf{u}^n_{p_j}$.

For the β_ℓ with $\ell \ne j$, $(0 \le \ell \le s)$, we must have $\beta_\ell \in \mathbf{u}^n_{p_j}$ because otherwise β_ℓ would also generate $\mathbf{u}_{p_j}/\mathbf{u}^n_{p_j}$ and we would have $\beta_j = \beta_\ell^x\gamma^n$ where γ is in $\mathbf{u}_{p_j}$, which would mean $\mathbf{T}_{\wp_j} = \mathbf{T}^{(j)}_{q_j}(\sqrt[n]{\beta_j})$ would be contained in $\mathbf{T}^{(j)}_{q_j}$, which is a contradiction. Therefore for $1 \le j \le s$, we have

$$\beta_j \notin \mathbf{u}^n_{p_j} \text{ and } \beta_\ell \in \mathbf{u}^n_{p_j} \text{ if } \ell \ne j, \qquad 0 \le \ell \le s$$

and

$$\mathbf{T}^{(j)}_{q_j} = \mathbf{k}_{p_j}(\sqrt[n]{\beta_0}, \sqrt[n]{\beta_1}, \ldots, \sqrt[n]{\beta_{j-1}}, \sqrt[n]{\beta_{j+1}}, \ldots, \sqrt[n]{\beta_s}) = \mathbf{k}_{p_j}.$$

The sets $\mathbf{u}_{p_1}^n, \dots, \mathbf{u}_{p_s}^n$ are all distinct, so the primes $p_1, \dots, p_s$ are distinct. Choose a generator π_j in $\mathbf{o}_{p_j}$ so that $p_j = (\pi_j)$. Define ideles $\mathbf{i}_1, \dots, \mathbf{i}_s$ in $\mathbf{I_k}(E)$ by

$$(\mathbf{i}_j)_p = \begin{cases} \pi_j & \text{if } p = p_j \\ 1 & \text{otherwise} \end{cases} \tag{8.20}$$

Since $\mathbf{T}_{q_j}^{(j)} = \mathbf{k}_{p_j}$ then $\mathbf{i}_j$ is a norm from $\mathbf{I}_{\mathbf{T}^{(j)}}$ locally everywhere so $\mathbf{i}_j \in \mathbf{N}_{\mathbf{T}^{(j)}/\mathbf{k}}\mathbf{I}_{\mathbf{T}^{(j)}}$ by lemma 7.5. Since $\mathbf{k} \subset \mathbf{K} \subset \mathbf{T}^{(j)}$ we have $\mathbf{i}_j \in \mathbf{N_{K/k}I_K}$. We will show that $\mathbf{i}_1, \dots, \mathbf{i}_s$ satisfy the condition of the remark preceeding lemma 8.17. Suppose that $\mathbf{i}_1^{a_1} \dots \mathbf{i}_s^{a_s}$ is in $\mathbf{k}^*\mathbf{I}_\mathbf{k}^n(E)$. Then we have

$$\mathbf{i}_1^{a_1} \dots \mathbf{i}_s^{a_s} = \alpha \mathbf{i} \quad \text{where } \alpha \in \mathbf{k}^* \text{ and } \mathbf{i} \in \mathbf{I}_\mathbf{k}^n(E). \tag{8.21}$$

With α defined by (8.21), we would like to compute $\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N}_{\mathbf{k}(\sqrt[n]{\alpha})/\mathbf{k}}\mathbf{I}_{\mathbf{k}(\sqrt[n]{\alpha})}\right]$. For a prime p of $\mathbf{k}$ we consider the following three cases. First, suppose that $p \notin E$ and $p \neq p_j$ for $1 \le j \le s$. Evaluating (8.21) at component (p), we have $1 = \alpha \mathbf{i}_p$ with $\mathbf{i}_p$ in $\mathbf{u}_p$. Therefore α is in $\mathbf{u}_p$ so p does not divide α, and p does not divide n since E contains all primes dividing n. Therefore p does not ramify in $\mathbf{k}(\sqrt[n]{\alpha})/\mathbf{k}$, so every element of $\mathbf{u}_p$ is in $\mathbf{N}_{\mathbf{k}_p(\sqrt[n]{\alpha})/\mathbf{k}}\mathbf{k}_p(\sqrt[n]{\alpha})$.

Second, suppose that $p = p_j$ where $1 \le j \le s$. Every element of $\mathbf{u}_p^n$ is in $\mathbf{N}_{\mathbf{k}_p(\sqrt[n]{\alpha})/\mathbf{k}}\mathbf{k}_p(\sqrt[n]{\alpha})$.

Third, suppose that p is in E. Evaluating (8.21) at component (p), we have $1 = \alpha \mathbf{i}_p$ with $\mathbf{i}_p$ in $\mathbf{u}_p^n$, so α is in $\mathbf{u}_p^n$. Then $\mathbf{k}_p(\sqrt[n]{\alpha}) = \mathbf{k}_p$, so every element of $\mathbf{k}_p^*$ is in $\mathbf{N}_{\mathbf{k}_p(\sqrt[n]{\alpha})/\mathbf{k}}\mathbf{k}_p(\sqrt[n]{\alpha})$.

Let F be the set of primes of the first case ($p \notin E$ and $p \neq p_j$ for $1 \le j \le s$). Combining the three cases and using lemma 7.5, we have

$$\prod_{p \in F} \mathbf{u}_p \prod_{j=1}^{s} \mathbf{u}_p^n \prod_{p \in E} \mathbf{k}_p^* \subset \mathbf{N}_{\mathbf{k}(\sqrt[n]{\alpha})/\mathbf{k}}\mathbf{I}_{\mathbf{k}(\sqrt[n]{\alpha})}. \tag{8.22}$$

We already know that β_j generates $\mathbf{u}_{p_j}/\mathbf{u}_{p_j}^n$ for $1 \le j \le s$, so

$$\mathbf{u}_{p_j} = \left\{\beta_j^r \mathbf{u}_{p_j}^n \;\middle|\; 0 \le r < n\right\} \subset \mathbf{k}^*(E)\mathbf{u}_{p_j}^n,$$

and therefore

$$\prod_{j=1}^{s} \mathbf{u}_{p_j} \subset \mathbf{k}^*(E) \prod_{j=1}^{s} \mathbf{u}_{p_j}^n. \tag{8.22a}$$

Applying (8.22a), we obtain

$$\mathbf{I_k}(E) = \prod_{p\in F} \mathbf{u}_p \prod_{j=1}^{s} \mathbf{u}_{p_j} \prod_{p\in E} \mathbf{k}_p^* \subset \mathbf{k}^*(E) \prod_{p\in F} \mathbf{u}_p \prod_{j=1}^{s} \mathbf{u}_{p_j}^n \prod_{p\in E} \mathbf{k}_p^* \tag{8.22b}$$

Using the (8.22b) and (8.22), we have

$$\mathbf{I_k} = \mathbf{k}^*\mathbf{I_k}(E) \subset \mathbf{k}^* \prod_{p\in F} \mathbf{u}_p \prod_{j=1}^{s} \mathbf{u}_{p_j}^n \prod_{p\in E} \mathbf{k}_p^* \subset \mathbf{k}^*\mathbf{N}_{\mathbf{k}(\sqrt[n]{\alpha})/\mathbf{k}}\mathbf{I}_{\mathbf{k}(\sqrt[n]{\alpha})}.$$

This shows that

$$\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N}_{\mathbf{k}(\sqrt[n]{\alpha})/\mathbf{k}}\mathbf{I}_{\mathbf{k}(\sqrt[n]{\alpha})}\right] = 1. \tag{8.23}$$

Since $\mathbf{k}(\sqrt[n]{\alpha})/\mathbf{k}$ is cyclic, the first fundamental inequality applies, so $[\mathbf{k}(\sqrt[n]{\alpha}) : \mathbf{k}]$ divides $\left[\mathbf{I_k} : \mathbf{k}^*\mathbf{N}_{\mathbf{k}(\sqrt[n]{\alpha})/\mathbf{k}}\mathbf{I}_{\mathbf{k}(\sqrt[n]{\alpha})}\right]$, and then by (8.23) we have $[\mathbf{k}(\sqrt[n]{\alpha}) : \mathbf{k}] = 1$. Then $\mathbf{k}(\sqrt[n]{\alpha}) = \mathbf{k}$, so α is in $(\mathbf{k}^*)^n$. Taking components of (8.21) at p_j for $1 \le j \le s$, we obtain

$$\pi_j^{a_j} = \alpha \mathbf{i}_{p_j} \quad \text{where } \alpha \in (\mathbf{k}_p^*)^n, \text{ and } \mathbf{i}_{p_j} \in \mathbf{u}_{p_j}.$$

Then $p_j^{a_j} = \left(\pi_j^{a_j}\right) = (\beta)^n$ in $\mathbf{o}_{p_j}$, so $a_j = 0(\text{mod } n)$ for $1 \le j \le s$. This proves that there are at least n^s distinct cosets of $\mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E)$ in $\mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I_K}$, which proves the lemma.

Proposition 8.18. $[\mathbf{I_k} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I_K}]$ *divides* $[\mathbf{K} : \mathbf{k}]$.

Proof. By (8.17) and lemmas 8.16 and 8.17, $[\mathbf{I_k} : \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I_K}]$ is 1 or n.

Proposition 8.19. *The second fundamental inequality holds for any abelian extension.*

Proof. By Proposition 8.18, the second fundamental inequality holds for extensions of prime degree n where the ground field contains the n-th roots of unity. Lemma 8.15 removes the requirement that the ground field contain the n-th roots of unity. Lemma 8.14 and the remark preceeding it show that the second fundamental inequality holds for any abelian extension.

Corollary to theorem 1. Now that theorem 1 has been established, the following corollary will be of use in proving theorem 2. Let $\mathbf{k}$ be an algebraic number field containing the n-th roots of unity where n is prime. Let E be a finite set of primes of $\mathbf{k}$ containing the infinite primes, primes dividing n, and so that $\mathbf{I_k} = \mathbf{k}^*\mathbf{I_k}(E)$. If E contains $s+1$ primes then $\mathbf{k}^*(E)/\left(\mathbf{k}^*(E)\right)^n$ is the direct product of $s+1$ cyclic groups of order n. Let $\beta_0, \dots, \beta_s$ be such that the cosets of $\left(\mathbf{k}^*(E)\right)^n$ generate $\mathbf{k}^*(E)$.

Corollary 8.20. *The kernel of* $\phi_{\mathbf{k}(\sqrt[n]{\beta_0},\ldots,\sqrt[n]{\beta_s})/\mathbf{k}}$ *is* $\mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E)$.

Proof. Since the $s+1$ elements $\beta_0,\ldots,\beta_s$ are independent modulo $(\mathbf{k}^*)^n$ then $[\mathbf{k}(\sqrt[n]{\beta_0},\ldots,\sqrt[n]{\beta_s}) : \mathbf{k}] = n^{s+1}$. For $0 \le j \le s$, let H_j be the kernel of $\phi_{\mathbf{k}(\sqrt[n]{\beta_0})\mathbf{k}}$. Since β_j is in $\mathbf{k}^*(E)$ then

$$\mathbf{I}^n_{\mathbf{k}}(E) \subset \mathbf{N}_{\mathbf{k}(\sqrt[n]{\beta_j})\mathbf{k}}\mathbf{I}_{\mathbf{k}(\sqrt[n]{\beta_j})}.$$

By Theorem I, we have

$$\mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E) \subset \mathbf{k}^*\mathbf{N}_{\mathbf{k}(\sqrt[n]{\beta_j})\mathbf{k}}\mathbf{I}_{\mathbf{k}(\sqrt[n]{\theta})} = \ker\left(\phi_{\mathbf{k}(\sqrt[n]{\beta_j})/\mathbf{k}}\right) = H_j,$$

so

$$\mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E) \subset H_0 \cap \cdots \cap H_s. \tag{8.24}$$

By lemma 8.5 and formula (5.1), for $\mathbf{i}$ in $\mathbf{I}_{\mathbf{k}}$, we have

$$\phi_{\mathbf{k}\left(\sqrt[n]{\beta_0},\ldots,\sqrt[n]{\beta_s}\right)/\mathbf{k}}(\mathbf{i}) = \left(\phi_{\mathbf{k}\left(\sqrt[n]{\beta_0}\right)/\mathbf{k}}(\mathbf{i}),\ldots,\phi_{\mathbf{k}\left(\sqrt[n]{\beta_s}\right)/\mathbf{k}}(\mathbf{i})\right).$$

The right side is 1 if and only if $\phi_{\mathbf{k}(\sqrt[n]{\beta_j})/\mathbf{k}}(\mathbf{i}) = 1$ for $0 \le j \le s$, that is, if and only if $\mathbf{i}$ is in $H_0 \cap \cdots \cap H_s$. Therefore

$$\ker\left(\phi_{\mathbf{k}\left(\sqrt[n]{\beta_0},\ldots,\sqrt[n]{\beta_s}\right)/\mathbf{k}}\right) = H_0 \cap \cdots \cap H_s. \tag{8.25}$$

By theorem I, we have

$$\begin{aligned}[\mathbf{I}_{\mathbf{k}} : H_0 \cap \cdots \cap H_s] &= \left[\mathbf{I}_{\mathbf{k}} : \ker\left(\phi_{\mathbf{k}\left(\sqrt[n]{\beta_0},\ldots,\sqrt[n]{\beta_s}\right)/\mathbf{k}}\right)\right] \\ &= \left[\mathbf{k}\left(\sqrt[n]{\beta_0},\ldots,\sqrt[n]{\beta_s}\right) : \mathbf{k}\right] = n^{s+1}\end{aligned} \tag{8.26}$$

By lemma 8.16, we have $[\mathbf{I}_{\mathbf{k}} : \mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E)] = n^{s+1}$. By (8.24) and (8.26), we conclude that $H_0 \cap \cdots \cap H_s = \mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E)$. Then by (8.25), we conclude

$$\ker\left(\phi_{\mathbf{k}\left(\sqrt[n]{\beta_0},\ldots,\sqrt[n]{\beta_s}\right)/\mathbf{k}}\right) = \mathbf{k}^*\mathbf{I}^n_{\mathbf{k}}(E).$$