CHAPTER X

NORM RESIDUE SYMBOL

Let $\mathbf{k}$ be an algebraic number field and let p be a prime of $\mathbf{k}$. We can embed $\mathbf{k}_p^*$ in $\mathbf{I_k}$ by $\alpha \to \mathbf{i}(\alpha, p, \mathbf{k})$, where

$$\mathbf{i}(\alpha, p, \mathbf{k}) = \begin{cases} \alpha & \text{at prime } p \text{ of } \mathbf{k} \\ 1 & \text{at other primes of } \mathbf{k}. \end{cases}$$

Note that if $\wp$ is a prime of $\mathbf{K}$ that divides p and α is in $\mathbf{K}_\wp^*$, then

$$\mathbf{N_{K/k}}\big(\mathbf{i}(\alpha, \wp, \mathbf{K})\big) = \mathbf{i}\left(\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha, p, \mathbf{k}\right) \tag{10.1}$$

If $\mathbf{K/k}$ is an abelian extension then $\alpha \to \phi_{\mathbf{K/k}}\big(\mathbf{i}(\alpha, p, \mathbf{k})\big)$ is a homomorphism of $\mathbf{k}_p^*$ to $G(\mathbf{K} : \mathbf{k})$. Define the *norm residue symbol* by

$$\left(\frac{\alpha, \mathbf{K/k}}{p}\right) = \phi_{\mathbf{K/k}}\big(\mathbf{i}(\alpha, p, \mathbf{k})\big).$$

If p is finite and not ramified in $\mathbf{K}$, then the norm residue and Artin symbols are related by

$$\left(\frac{\alpha, \mathbf{K/k}}{p}\right) = \left(\frac{\mathbf{K} : \mathbf{k}}{p}\right)^a \qquad \text{if } (\alpha) = p^a. \tag{10.2}$$

If $\mathbf{i}$ is an idele in $\mathbf{I_k}$ then $\phi_{\mathbf{K/k}}\big(\mathbf{i}(\alpha, p, \mathbf{k})\big)$ can be non-trivial only at the finite number of primes that are infinite or ramified or for which $|\mathbf{i}|_p \neq 1$, so we may write

$$\phi_{\mathbf{K/k}}(\mathbf{i}) = \prod_p \phi_{\mathbf{K/k}}\mathbf{i}(\mathbf{i}_p, p, \mathbf{k}) = \prod_p \left(\frac{\mathbf{i}_p, \mathbf{K/k}}{p}\right)$$

Since α in $\mathbf{k}^*$ is in the kernel of $\phi_{\mathbf{K/k}}$, we have the *general reciprocity law.*

$$\prod_p \left(\frac{\alpha, \mathbf{K/k}}{p}\right) = 1 \qquad \text{for } \alpha \in \mathbf{k}^* \tag{10.3}$$

Lemma 10.1. *If $\wp$ is a prime of $\mathbf{K}$ dividing p then $\left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right)$ is in the splitting group of $\wp$. Therefore, the norm residue symbol maps $\mathbf{k}_p^*$ to $G(\mathbf{K}_\wp : \mathbf{k}_p)$.*

Proof. Let S be the splitting group of $\wp$. let $\mathbf{Z}$ be the fixed field of S, and let q be the prime of $\mathbf{Z}$ which $\wp$ divides. We have $\mathbf{K}_\wp \supset \mathbf{Z}_q \supset \mathbf{k}_p$. Since $S = G(\mathbf{K}_\wp : \mathbf{k}_p)$ then $\mathbf{Z}_q = \mathbf{k}_p$. Let $\mathbf{i} = \mathbf{i}(\alpha, q, \mathbf{Z})$ in $\mathbf{I}_\mathbf{Z}$. By (10.1) we have $\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\,\mathbf{i}(\alpha, q, \mathbf{Z}) = \mathbf{i}(\alpha, p, \mathbf{k})$, so

$$\left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right) = \phi_{\mathbf{K}/\mathbf{k}}\big(\mathbf{i}(\alpha, p, \mathbf{k})\big) = \phi_{\mathbf{K}/\mathbf{k}}\big(\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\,\mathbf{i}(\alpha, q, \mathbf{Z})\big).$$

According to proposition 2.19, we have

$$\phi_{\mathbf{K}/\mathbf{k}}\big(\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\,\mathbf{i}(\alpha, q, \mathbf{Z})\big) = \phi_{\mathbf{K}/\mathbf{Z}}\big(\mathbf{i}(\alpha, q, \mathbf{Z})\big).$$

This shows that $\left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right)$ in the image of $\phi_{\mathbf{K}/\mathbf{Z}}$ and thus leaves $\mathbf{Z}$ fixed. Therefore $\left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right)$ is in the splitting group of $\wp$.

Lemma 10.2. *If $\mathbf{T}'$ is a complete field such that $\mathbf{k}_p \subset \mathbf{T}' \subset \mathbf{K}_\wp$ then there exists a field $\mathbf{T}$ such that $\mathbf{k} \subset \mathbf{T} \subset \mathbf{K}$, and if p' is the prime of $\mathbf{T}$ which $\wp$ divides then $\mathbf{T}_{p'} = \mathbf{T}'$.*

Proof. Let S be the splitting group of $\wp$ and H the subgroup of S leaving $\mathbf{T}'$ fixed. Let $\mathbf{T} = \mathbf{T}' \cap \mathbf{K}$ be the subfield of $\mathbf{K}$ fixed by H, and let p' be the prime of $\mathbf{T}$ which $\wp$ divides. Then $\mathbf{T}_{p'} \subset \mathbf{T}'$, since $\mathbf{T}'$ is complete. On the other hand $[\mathbf{K}_\wp : \mathbf{T}_{p'}]$ divides $[\mathbf{K} : \mathbf{T}]$, and $[\mathbf{K} : \mathbf{T}] = [H : 1] = [\mathbf{K}_\wp : \mathbf{T}']$. Therefore $[\mathbf{K}_\wp : \mathbf{T}_{p'}] = [\mathbf{K}_\wp : \mathbf{T}']$, so $\mathbf{T}_{p'} = \mathbf{T}'$.

Lemma 10.3. *Let $\mathbf{T}$ be any finite extension of $\mathbf{k}$, and let $\mathbf{K}$ be an abelian extension of $\mathbf{k}$. If p is a prime of $\mathbf{k}$, let $\wp'$ be a prime of $\mathbf{KT}$ dividing p, and let $\wp'$ divide primes $\wp$ of $\mathbf{k}$ and p' of $\mathbf{T}$, respectively. Then*

$$\left(\frac{\beta,\mathbf{KT}/\mathbf{T}}{p'}\right) = \left(\frac{\mathbf{N}_{\mathbf{T}_{p'}/\mathbf{k}_p}\beta,\mathbf{K}/\mathbf{k}}{p}\right) \qquad \textit{for } \beta \in \mathbf{T}_{p'}.$$

Proof. By proposition 2.19 and (10.1), we have

$$\begin{aligned}\left(\frac{\beta,\mathbf{KT}/\mathbf{T}}{p'}\right) &= \phi_{\mathbf{KT}/\mathbf{T}}\big(\mathbf{i}(\beta, p', \mathbf{T})\big) = \phi_{\mathbf{K}/\mathbf{k}}\big(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i}(\beta, p', \mathbf{T})\big)\\ &= \phi_{\mathbf{K}/\mathbf{k}}\big(\mathbf{i}(\mathbf{N}_{\mathbf{T}_{p'}/\mathbf{k}_p}\beta, p, \mathbf{k})\big) = \left(\frac{\mathbf{N}_{\mathbf{T}_{p'}/\mathbf{k}_p}\beta,\mathbf{K}/\mathbf{k}}{p}\right).\end{aligned}$$

Corollary 10.4. *If* $\mathbf{T} \subset \mathbf{K}$ *in lemma 10.3 then* $\mathbf{KT} = \mathbf{K}$, *so*

$$\left(\frac{\beta, \mathbf{K}/\mathbf{T}}{p'}\right) = \left(\frac{\mathbf{N}_{\mathbf{T}_{p'}/\mathbf{k}_p}\beta, \mathbf{K}/\mathbf{k}}{p}\right) \qquad \textit{for } \beta \in \mathbf{T}_{p'}.$$

Lemma 10.5. *The kernel of* $\alpha \to \left(\frac{\alpha, \mathbf{K}/\mathbf{k}}{p}\right)$ *contains* $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$.

Proof. If $\alpha = \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\beta$ then by corollary 10.4 we have

$$\left(\frac{\alpha, \mathbf{K}/\mathbf{k}}{p}\right) = \left(\frac{\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\beta, \mathbf{K}/\mathbf{k}}{p}\right) = \left(\frac{\beta, \mathbf{K}/\mathbf{K}}{\wp}\right) = 1.$$

Kummer extensions. Let $\mathbf{k}$ contain the n-th roots of unity, where n is not necessarily prime, and let p be a prime of $\mathbf{k}$. If β is in $\mathbf{k}_p^*$ then consider $\mathbf{k}_p(\sqrt[n]{\beta})/\mathbf{k}_p$. By lemma 4.13, if we choose β_0 in $\mathbf{k}^*$ so that $|\beta\beta_0^{-1} - 1|_p$ is sufficiently small then $\beta\beta_0^{-1} = \gamma^n$ where γ is in $\mathbf{k}_p^*$, so $\mathbf{k}_p(\sqrt[n]{\beta}) = \mathbf{k}_p(\sqrt[n]{\beta_0})$. Put $\mathbf{K} = \mathbf{k}(\sqrt[n]{\beta_0})$. The valuation on $\mathbf{k}_p(\sqrt[n]{\beta_0})$ restricted to $\mathbf{k}(\sqrt[n]{\beta_0})$ determines a prime $\wp$ of $\mathbf{K}$ which divides p. Then $\mathbf{K}_\wp = \mathbf{k}_p(\sqrt[n]{\beta_0})$. If α is in $\mathbf{k}_p^*$ then $\left(\frac{\alpha, \mathbf{K}/\mathbf{k}}{p}\right)$ is in $G(\mathbf{K}_\wp : \mathbf{k}_p)$ by lemma 10.1. The Galois group $G(\mathbf{K}_\wp : \mathbf{k}_p)$ is isomorphic to a subgroup of the cyclic group containing the n-roots of unity. There exists an n-root of unity ζ depending on α and β so that

$$\left(\frac{\alpha, \mathbf{K}/\mathbf{k}}{p}\right) \sqrt[n]{\beta} = \zeta \sqrt[n]{\beta}$$

Setting $\left(\frac{\alpha,\beta}{p}\right) = \zeta$, we have a map from $\mathbf{k}_p^* \times \mathbf{k}_p^*$ to n-th roots of unity defined by

$$\left(\frac{\alpha, \mathbf{K}/\mathbf{k}}{p}\right) \sqrt[n]{\beta} = \left(\frac{\alpha, \beta}{p}\right) \sqrt[n]{\beta}$$

We may write $\left(\frac{\alpha,\beta}{p}\right)_n$ whenever it is necessary to make n explicit.

Lemma 10.6. *Symbol* $\left(\frac{\alpha,\beta}{p}\right)$ *has the following properties.*

(a) $\left(\frac{\alpha\beta, \gamma}{p}\right) = \left(\frac{\alpha, \gamma}{p}\right)\left(\frac{\beta, \gamma}{p}\right)$ (d) $\left(\frac{\alpha, \beta\gamma}{p}\right) = \left(\frac{\alpha, \beta}{p}\right)\left(\frac{\alpha, \gamma}{p}\right)$

(b) $\left(\frac{-\alpha, \alpha}{p}\right) = 1$ (e) $\left(\frac{\alpha, \beta}{p}\right) = \left(\frac{\beta, \alpha}{p}\right)^{-1}$

(c) $\left(\frac{\alpha, \beta\gamma^n}{p}\right) = \left(\frac{\alpha\gamma^n, \beta}{p}\right) = \left(\frac{\alpha, \beta}{p}\right)$ (f) $\left(\frac{1-\alpha, \alpha}{p}\right) = 1$ *if* $\alpha \neq 0, 1$

Proof. (a) is obvious. To prove (b), take $\mathbf{K}_\wp = \mathbf{k}_p(\sqrt[n]{\alpha})$. Let $[\mathbf{K}_\wp : \mathbf{k}_p] = m$ and $d = n/m$. Let ζ be a primitive m-th root of unity. Write $\mathbf{N}$ for $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}$. We would like to show that $-\alpha = \mathbf{N}\beta$ for some element β in $\mathbf{K}_\wp^*$. We have

$$\mathbf{N}\left(\sqrt[n]{\alpha}\right)^d = \left(\zeta\sqrt[n]{\alpha}\right)^d\left(\zeta^2\sqrt[n]{\alpha}\right)^d\dots\left(\zeta^m\sqrt[n]{\alpha}\right)^d = \zeta^{(1+2+\cdots+m)d}\alpha = \zeta^{\frac{1}{2}m(m+1)d}\alpha$$

There are three cases to consider. First, suppose that m is odd. Then $\frac{1}{2}m(m+1)d$ is divisible by m, so $\mathbf{N}\left(\sqrt[n]{\alpha}\right)^d = \alpha$. We have $\mathbf{N}(-1) = (-1)^m = -1$, so

$$\mathbf{N}\left(-(\sqrt[n]{\alpha})^d\right) = \mathbf{N}(-1)\mathbf{N}(\sqrt[n]{\alpha})^d = -\alpha.$$

Next suppose that m is even and d is odd. Then $\zeta^{\frac{1}{2}m(m+1)d} = (-1)^{(m+1)d} = -1$, so

$$\mathbf{N}\left((\sqrt[n]{\alpha})^d\right) = -\alpha.$$

Finally, suppose that m and d are both even. Then $\zeta^{\frac{1}{2}m(m+1)d} = 1$. If ζ_1 be a primitive n-th root of unity then $\mathbf{N}(\zeta_1)^{d/2} = \zeta_1^{md/2} = -1$, so

$$\mathbf{N}\left(\zeta_1^{d/2}\left(\sqrt[n]{\alpha}\right)^d\right) = (-1)\alpha = -\alpha.$$

We have found β so that $-\alpha = \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\beta$ in all three cases.

To prove (c), choose β_0 in $\mathbf{k}^*$ so that $\beta \simeq_n \beta_0$. Then $\mathbf{k}\left(\sqrt[n]{\beta_0}\right) = \mathbf{k}\left(\sqrt[n]{\beta}\right) = \mathbf{k}\left(\sqrt[n]{\beta\gamma^n}\right)$. Then $\left(\frac{\alpha,\beta}{p}\right)$ and $\left(\frac{\alpha,\beta\gamma^n}{p}\right)$ are both determined by norm residue symbol $\sigma = \left(\frac{\alpha,\mathbf{k}\left(\sqrt[n]{\beta_0}\right)/\mathbf{k}}{p}\right)$.

$$\left(\frac{\alpha,\beta}{p}\right)\sqrt[n]{\beta} = \sigma\left(\sqrt[n]{\beta}\right) \quad \text{and} \quad \left(\frac{\alpha,\beta\gamma^n}{p}\right)\sqrt[n]{\beta}\gamma = \sigma\left(\sqrt[n]{\beta}\gamma\right) = \gamma\sigma\left(\sqrt[n]{\beta}\right)$$

Therefore

$$\left(\frac{\alpha,\beta}{p}\right) = \frac{\sigma\left(\sqrt[n]{\beta}\right)}{\sqrt[n]{\beta}} = \left(\frac{\alpha,\beta\gamma^n}{p}\right)$$

To prove (d), choose β_0 and γ_0 in $\mathbf{k}_p^*$ so that $\beta \simeq_n \beta_0$ and $\gamma \simeq_n \gamma_0$. Then $\beta\gamma \simeq_n \beta_0\gamma_0$. By (c), we have $\left(\frac{\alpha,\beta\gamma}{p}\right) = \left(\frac{\alpha,\beta_0\gamma_0}{p}\right)$, so we may suppose β and γ are in $\mathbf{k}_p^*$. Since $\left(\frac{\alpha,\mathbf{k}(\sqrt[n]{\beta\gamma})/\mathbf{k}}{p}\right)$ is the restriction to $\mathbf{k}(\sqrt[n]{\beta\gamma})$ of $\left(\frac{\alpha,\mathbf{k}(\sqrt[n]{\beta},\sqrt[n]{\gamma})/\mathbf{k}}{p}\right)$, then

$$\begin{aligned}\left(\frac{\alpha,\beta\gamma}{p}\right)\sqrt[n]{\beta\gamma} &= \left(\frac{\alpha,\mathbf{k}(\sqrt[n]{\beta\gamma})/\mathbf{k}}{p}\right)\sqrt[n]{\beta\gamma} = \left(\frac{\alpha,\mathbf{k}(\sqrt[n]{\beta},\sqrt[n]{\gamma})/\mathbf{k}}{p}\right)\sqrt[n]{\beta\gamma}\\ &= \left(\left(\frac{\alpha,\mathbf{k}(\sqrt[n]{\beta})/\mathbf{k}}{p}\right)\sqrt[n]{\beta}\right)\left(\left(\frac{\alpha,\mathbf{k}(\sqrt[n]{\gamma})/\mathbf{k}}{p}\right)\sqrt[n]{\gamma}\right).\end{aligned}$$

By Lemma 8.5, we have

$$\left(\frac{\alpha,\beta\gamma}{p}\right)\sqrt[n]{\beta\gamma}=\left(\left(\frac{\alpha,\beta}{p}\right)\sqrt[n]{\beta}\right)\left(\left(\frac{\alpha,\gamma}{p}\right)\sqrt[n]{\gamma}\right)=\left(\frac{\alpha,\beta}{p}\right)\left(\frac{\alpha,\gamma}{p}\right)\sqrt[n]{\beta\gamma}.$$

To prove (e), apply (b) to obtain

$$1=\left(\frac{-\alpha\beta,\alpha\beta}{p}\right)=\left(\frac{-\alpha,\alpha}{p}\right)\left(\frac{\beta,\alpha}{p}\right)\left(\frac{\alpha,\beta}{p}\right)\left(\frac{-\beta,\beta}{p}\right)=\left(\frac{\beta,\alpha}{p}\right)\left(\frac{\alpha,\beta}{p}\right).$$

To prove (f), suppose that $[\mathbf{k}_p\,(\sqrt[n]{\alpha}) : \mathbf{k}_p] = m$, and put $d = n/m$. Let ζ be a primitive n-th root of unity. The conjugates of $\sqrt[n]{\alpha}$ are $\zeta^{kd}\sqrt[n]{\alpha}$ for $0 \leq k < m$. Substitute $x = 1$ in

$$x^n-\alpha=\left(x-\sqrt[n]{\alpha}\right)\left(x-\zeta\sqrt[n]{\alpha}\right)\ldots\left(x-\zeta^{n-1}\sqrt[n]{\alpha}\right)$$

to obtain

$$\begin{aligned}1-\alpha=\prod_{i=0}^{n-1}\left(1-\zeta^i\sqrt[n]{\alpha}\right)&=\prod_{j=0}^{d-1}\prod_{k=0}^{m-1}\left(1-\zeta^{kd+j}\sqrt[n]{\alpha}\right)\\&=\prod_{j=0}^{d-1}\prod_{k=0}^{m-1}\left(1-\zeta^j\zeta^{kd}\sqrt[n]{\alpha}\right)=\prod_{j=0}^{d-1}\mathbf{N}_{\mathbf{k}_p(\sqrt[n]{\alpha})/\mathbf{k}_p}\left(1-\zeta^j\sqrt[n]{\alpha}\right).\end{aligned}$$

Legendre symbol. If prime p of $\mathbf{k}$ does not divide n and ζ_1 and ζ_2 are two distinct n-th roots of unity in $\mathbf{k}$, then $\zeta_1 \neq \zeta_2 (\text{mod } n)$ by lemma 8.8. The multiplicative group of $\mathbf{o}/p$ therefore contains a subgroup of order n, so n divides $\mathrm{N}p-1$. If $\alpha \in \mathbf{k}^*$ and $\alpha \neq 0(\text{mod } p)$, then $\alpha^{\mathrm{N}p-1} = 1(\text{mod } p)$, so $\alpha^{(\mathrm{N}p-1)/n}$ is an n-root of unity modulo p. There is a unique n-root of unity ζ in $\mathbf{k}$ so that $\alpha^{(\mathrm{N}p-1)/n} = \zeta(\text{mod } p)$.

The *Legendre symbol* $\left(\frac{\alpha}{p}\right)$ is defined to be the n-root of unity satisfying

$$\alpha^{\frac{\mathrm{N}p-1}{n}}=\left(\frac{\alpha}{p}\right)(\text{mod } p).$$

In any finite abelian group having order $\mathrm{N}p-1$ divisible by n, an element x is an n-th power if and only if $x^{(\mathrm{N}p-1)/n} = 1$. Therefore α is an n-th power modulo p if and only if $\left(\frac{\alpha}{p}\right) = 1$. By lemma 8.11, $[\mathbf{u}_p : \mathbf{u}_p^n] = n$ when p does not divide n. Therefore the homomorphism $\mathbf{u}_p/\mathbf{u}_p^n \to \mathbf{o}_p/\mathbf{o}_p^n$ is an isomorphism. This shows that α is an n-th power in $\mathbf{u}_p$ if and only if $\left(\frac{\alpha}{p}\right) = 1$.

Lemma 10.7. *Let* $\mathbf{k}$ *contain the* n*-th roots of unity and let* $\alpha \neq 0$ *be an element of* $\mathbf{k}$. *Let* p *be a prime of* $\mathbf{k}$ *which does not divide* n *or* α. *The Artin and Legendre symbols are related by*

$$\left(\frac{\mathbf{k}(\sqrt[n]{\alpha}) : \mathbf{k}}{p}\right) \sqrt[n]{\alpha} = \left(\frac{\alpha}{p}\right) \sqrt[n]{\alpha}$$

Proof. The Artin symbol satisfies

$$\left(\frac{\mathbf{k}(\sqrt[n]{\alpha}) : \mathbf{k}}{p}\right) \sqrt[n]{\alpha} = (\sqrt[n]{\alpha})^{\mathrm{N}p} (\mathrm{mod}\ \wp),$$

where prime $\wp$ of $\mathbf{k}(\sqrt[n]{\alpha})$ divides p. There is an n-th root of unity ζ such that

$$\left(\frac{\mathbf{k}(\sqrt[n]{\alpha}) : \mathbf{k}}{p}\right) \sqrt[n]{\alpha} = \zeta(\sqrt[n]{\alpha}).$$

Then $\zeta(\sqrt[n]{\alpha}) = (\sqrt[n]{\alpha})^{\mathrm{N}p} (\mathrm{mod}\ \wp)$. Since $(\sqrt[n]{\alpha})$ is a unit in $\mathbf{O}_{\wp}$, we have

$$\zeta = (\sqrt[n]{\alpha})^{\mathrm{N}p-1} = (\sqrt[n]{\alpha})^{n\frac{\mathrm{N}p-1}{n}} = \alpha^{\frac{\mathrm{N}p-1}{n}} (\mathrm{mod}\ \wp).$$

This show that $\zeta = \left(\frac{\alpha}{p}\right)$, which completes the proof.

If β is a unit in $\mathbf{k}_p^*$, take β_0 in $\mathbf{k}$ sufficiently close to β so that $\beta\beta_0^{-1}$ is an n-th power in $\mathbf{k}_p^*$, and we also want $\beta = \beta_0 (\mathrm{mod}\ p)$. Then

$$\left(\frac{\mathbf{k}\left(\sqrt[n]{\beta_0}\right) : \mathbf{k}}{p}\right) \sqrt[n]{\beta_0} = \left(\frac{\beta_0}{p}\right) \sqrt[n]{\beta_0},$$

and, by (10.2), for α in $\mathbf{k}_p^*$ we have

$$\left(\frac{\alpha, \mathbf{k}\left(\sqrt[n]{\beta_0}\right)/\mathbf{k}}{p}\right) = \left(\frac{\mathbf{k}\left(\sqrt[n]{\beta_0}\right) : \mathbf{k}}{p}\right)^a \qquad \text{where } (\alpha) = p^a,$$

so

$$\left(\frac{\alpha, \mathbf{k}\left(\sqrt[n]{\beta_0}\right)/\mathbf{k}}{p}\right) \sqrt[n]{\beta_0} = \left(\frac{\beta_0}{p}\right)^a \sqrt[n]{\beta_0}.$$

Since $\beta_0 = \beta(\mathrm{mod}\ p)$ and $\mathbf{k}_p(\sqrt[n]{\beta_0}) = \mathbf{k}_p(\sqrt[n]{\beta})$, we have

$$\left(\frac{\alpha, \beta}{p}\right) = \left(\frac{\beta}{p}\right)^a. \tag{10.4}$$

Lemma 10.8. *If* $\mathbf{k}$ *contains the* n*-th roots of unity,* α *and* β *are in* $\mathbf{k}_p^*$*, and* p *is a prime of* $\mathbf{k}$ *that does not divide* n*, then*

$$\left(\frac{\alpha,\beta}{p}\right)=\left(\frac{\beta}{p}\right)^a \qquad \textit{if } (\alpha)=p^a \textit{ and } \beta\in\mathbf{u}_p.$$
$$\left(\frac{\alpha,\beta}{p}\right)=\left(\frac{\alpha}{p}\right)^{-b} \qquad \textit{if } (\beta)=p^b \textit{ and } \alpha\in\mathbf{u}_p.$$

Proof. The first formula is (10.4), and the second follows from the first by lemma 10.6(e).

Lemma 10.9. *If* $\mathbf{k}$ *contains the* n*-th roots of unity,* α *and* β *are in* $\mathbf{k}_p^*$*, and* p *is a prime of* $\mathbf{k}$ *that does not divide* n*, then*

$$\left(\frac{\alpha,\beta}{p}\right)=\left(\frac{(-1)^{ab}\beta^a/\alpha^b}{p}\right) \qquad \textit{if } (\alpha)=p^a \textit{ and } (\beta)=p^b.$$

Proof. Choose π so that $p=(\pi)$. Let $\alpha=\pi^a\alpha'$ and $\beta=\pi^b\beta'$. Then α' and β' are in $\mathbf{u}_p$, and by lemma 10.6a and 10.6d we have

$$\left(\frac{\alpha,\beta}{p}\right)=\left(\frac{\pi^a\alpha',\pi^b\beta'}{p}\right)=\left(\frac{\pi^a,\pi^b}{p}\right)\left(\frac{\pi^a,\beta'}{p}\right)\left(\frac{\alpha',\pi^b}{p}\right)\left(\frac{\alpha',\beta'}{p}\right).$$

Applying lemma 10.8, we have $\left(\frac{\alpha',\beta'}{p}\right)=1$, so

$$\left(\frac{\alpha,\beta}{p}\right)=\left(\frac{\pi,\pi}{p}\right)^{ab}\left(\frac{\beta'}{p}\right)^a\left(\frac{\alpha'}{p}\right)^{-b}.$$

By (b) and (d) of lemma 10.6, we have $\left(\frac{\pi,\pi}{p}\right)=\left(\frac{\pi,-1}{p}\right)\left(\frac{\pi,-\pi}{p}\right)=\left(\frac{\pi,-1}{p}\right)$, and $\left(\frac{\pi,-1}{p}\right)=\left(\frac{-1}{p}\right)$ by lemma 10.8, so

$$\left(\frac{\alpha,\beta}{p}\right)=\left(\frac{-1}{p}\right)^{ab}\left(\frac{\beta'}{p}\right)^a\left(\frac{\alpha'}{p}\right)^{-b}=\left(\frac{(-1)^{ab}(\beta')^a/(\alpha')^b}{p}\right).$$

Since $\beta^a/\alpha^b=(\beta')^a/(\alpha')^b$, the conclusion follows.

Jacobi symbol; reciprocity law for n-th powers. If $\mathbf{k}$ contains the n-th roots of unity, suppose that the factorization of principal ideals generated by α and β in $\mathbf{k}^*$ be $(\alpha) = \prod p^{a_p}$ and $(\beta) = \prod p^{b_p}$, where p runs over finite primes of $\mathbf{k}$. Suppose also that α and β have no common prime divisor, and that β is relatively prime to n. Then $a_p b_p = 0$ for every finite prime p, and $b_p = 0$ if p divides n. Define the Jacobi symbol to be the product of Legendre symbols.

$$\left(\frac{\alpha}{\beta}\right) = \prod_{b_p \neq 0} \left(\frac{\alpha}{p}\right)^{b_p}.$$

Note that legendre symbol $\left(\frac{\alpha}{p}\right)$ is defined when $b_p \neq 0$.

Proposition 10.10 (Reciprocity law for n-th powers). *If $\mathbf{k}$ contains the n-th roots of unity, and elements α and β of $\mathbf{k}^*$ are relatively prime and are divisible by no finite prime of $\mathbf{k}$ dividing n, then*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \prod_{p \in E} \left(\frac{\alpha, \beta}{p}\right)$$

where E consists of primes of $\mathbf{k}$ that are either infinite or divide n.

Proof. Applying the general reciprocity (10.3) to $\mathbf{k}(\sqrt[n]{\beta})/\mathbf{k}$, we have

$$\prod_p \left(\frac{\alpha, \beta}{p}\right) = 1 \qquad \text{for } \alpha \text{ and } \beta \text{ in } \mathbf{k}^*.$$

The primes of $\mathbf{k}$ for which $\left(\frac{\alpha,\beta}{p}\right)$ may be nontrivial belong to four disjoint sets: primes dividing α, primes dividing β, primes dividing n, and infinite primes.

$$1 = \prod_{a_p \neq 0} \left(\frac{\alpha, \beta}{p}\right) \prod_{b_p \neq 0} \left(\frac{\alpha, \beta}{p}\right) \prod_{p|(n)} \left(\frac{\alpha, \beta}{p}\right) \prod_{\text{infinite } p} \left(\frac{\alpha, \beta}{p}\right)$$

Applying lemma 10.8, we have

$$1 = \prod_{a_p \neq 0} \left(\frac{\beta}{p}\right)^{a_p} \prod_{b_p \neq 0} \left(\frac{\alpha}{p}\right)^{-b_p} \prod_{p \in E} \left(\frac{\alpha, \beta}{p}\right),$$

and apply the definition of the Jacobi symbol to obtain

$$1 = \left(\frac{\beta}{\alpha}\right)\left(\frac{\alpha}{\beta}\right)^{-1} \prod_{p \in E} \left(\frac{\alpha, \beta}{p}\right).$$

Quadratic reciprocity laws. If p is a complex infinite prime then all extensions of $\mathbf{k}_p$ are trivial, so $\left(\frac{\alpha,\beta}{p}\right)_2$ is always trivial. Real infinite primes may occur only when $n = 2$, since $\mathbf{k}$ must contain the n-th roots of unity. If $n = 2$ then $\mathbf{k}_p(\sqrt{\beta})$ is nontrivial if and only if $b < 0$, and in that case α is not a norm if and only if $\alpha < 0$, so $\left(\frac{\alpha,\beta}{p}\right)_2 \neq 1$ for real infinite primes if and only if α and β are both negative, and we have the following corollary.

Corollary 10.11 (General quadratic reciprocity law). *Let $n = 2$, and suppose that $\mathbf{k}$ has r real infinite primes. Let $\sigma_i, \ldots, \sigma_r$ be the distinct isomorphisms of $\mathbf{k}$ to the real numbers. Put $\alpha_i = \sigma_i(\alpha)$ and $\beta_i = \sigma_i(\beta)$. If α and β in $\mathbf{k}^*$ are relatively prime and are not divisible by any prime dividing* (2)*, then*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = \prod_{p|(2)} \left(\frac{\alpha,\beta}{p}\right)_2 \prod_{i=1}^{r} (-1)^{s(\alpha_i,\beta_i)}, \qquad s(\alpha_i,\beta_i) = \begin{cases} 1 & \text{if } \alpha_i < 0,\ \beta_i < 0 \\ 0 & \text{otherwise} \end{cases}$$

Lemma 10.12. *Suppose that p is a prime of $\mathbf{k}$ dividing (2) and β is an element of $\mathbf{k}_p^*$ satisfying $\beta = 1\big(\mathrm{mod}\ (4)\big)$. Then p is unramified in $\mathbf{k}_p(\sqrt{\beta})$.*

Proof. There is nothing to prove if $[\mathbf{k}_p(\sqrt{\beta}) : \mathbf{k}_p] = 1$, so consider the case that $[\mathbf{k}_p(\sqrt{\beta}) : \mathbf{k}_p] = 2$. Let x_1, x_2 form a basis for the ring of integers in $\mathbf{k}_p(\sqrt{\beta})$. Write $\mathbf{S}$ for $\mathbf{S}_{\mathbf{k}_p(\sqrt{\beta})/\mathbf{k}_p}$, and put $D = \det\big(\mathbf{S}(x_i x_j)\big)$. To show that p is unramified, we need to show that p does not divide the local discriminant $\mathbf{D}_{\mathbf{k}_p(\sqrt{\beta})/\mathbf{k}_p} = (D)$ (chapter 1, p. 6). Let $y_1 = 1$ and $y_2 = (1 + \sqrt{\beta})/2$. We have

$$\det \begin{pmatrix} \mathbf{S}(y_1 y_1) & \mathbf{S}(y_1 y_2) \\ \mathbf{S}(y_2 y_1) & \mathbf{S}(y_2 y_2) \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+\beta}{2} \end{pmatrix} = \beta$$

Also, y_2 is an integer in $\mathbf{k}_p(\sqrt{\beta})$ since it is a root of $x^2 - x + (1-\beta)/4$, a polynomial with coefficients in $\mathbf{o}_p$ because $\beta = 1\big(\mathrm{mod}\ (4)\big)$. There are elements a_{ij} in $\mathbf{o}_p$ such that $y_i = \sum_{j=1}^{2} a_{ij} x_j$. Then

$$\big(\mathbf{S}(y_i y_j)\big) = \big(a_{ij}\big)\big(\mathbf{S}(x_i x_j)\big)\big(a_{ij}\big)^t$$

Putting $A = \det(a_{ij})$, then A is an element of $\mathbf{o}_p$, and $\beta = DA^2$. Since p divides (2), we have $\beta = 1(\mathrm{mod}\ p)$, so $DA^2 = 1(\mathrm{mod}\ p)$. Thus p cannot divide the discriminant.

The following special cases of the quadratic reciprocity law are due to Hilbert and Hecke.

Corollary 10.13 (Quadratic reciprocity law — Hecke). *Suppose that α and β in $\mathbf{k}^*$ are relatively prime and prime to (2). If either α or β is congruent to a square modulo* (4)*, then*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)=\prod_{i=1}^{r}(-1)^{s(\alpha_i,\beta_i)}$$

Proof. Let p be a prime of $\mathbf{k}$ dividing (2). If $\beta=\gamma^2\big(\text{mod }(4)\big)$ with γ in $\mathbf{u}_p$, then $\beta_1=\beta/\gamma^2=1\big(\text{mod }(4)\big)$, and $\mathbf{k}_p(\sqrt{\beta_1})=\mathbf{k}_p(\sqrt{\beta})$, so $\mathbf{k}_p(\sqrt{\beta})$ is unramified by lemma 10.12. Since α is a unit in $\mathbf{k}_p$, it is a norm from $\mathbf{k}_p(\sqrt{\beta})$, so $\left(\frac{\alpha,\beta}{p}\right)_2=1$. The case for α follows by symmetry (Lemma 10.6e).

Corollary 10.14 (Quadratic reciprocity law—Hilbert). *Suppose that $\mathbf{k}$ has no real primes, and suppose the class number h is odd. Let p and q are two distinct prime ideals which do not divide* (2)*. Then $p^h=(x)$ and $q^h=(y)$ are principal, and*

$$\left(\frac{x}{q}\right)\left(\frac{y}{p}\right)=\prod_{\ell|(2)}\left(\frac{x,y}{\ell}\right)$$

Proof. We have $\left(\frac{x}{y}\right)=\left(\frac{x}{q}\right)^h=\left(\frac{x}{q}\right)$, and $\left(\frac{y}{x}\right)=\left(\frac{y}{p}\right)^h=\left(\frac{y}{p}\right)$. The result now follows from corollary 10.11 with $r=0$.

Corollary 10.15 (Quadratic reciprocity law for rational numbers). *Suppose that positive integers a and b are relatively prime and both odd. Then*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$

Proof. Since a and b are positive, we only need to consider $p=2$. By lemma 10.12, if $b=1(\text{mod }4)$ then $\mathbf{Q}_{(2)}(\sqrt{b})/\mathbf{Q}_{(2)}$ is unramified. Then a is a norm, so $\left(\frac{a,b}{(2)}\right)=1$. The same holds if $a=1(\text{mod }4)$by lemma 10.6e. Suppose that $a=b=3(\text{mod }4)$. Every integer that is a norm from $\mathbf{Q}_{(2)}(\sqrt{b})$ has the form x^2-by^2 where x and y are in integers of that field. But $x^2-3y^2=x^2+y^2(\text{mod }4)$, so norms can take only the values 0, 1, or 2 (mod 4). Therefore a cannot be a norm, so $\left(\frac{a,b}{(2)}\right)=-1$.

Quadratic reciprocity law for Gaussian integers. We need a few preliminary results. Let i represent$\sqrt{-1}$, and let $\mathbf{k}=\mathbf{Q}(i)$, and let $\mathbf{o}$ be the ring of integers of $\mathbf{k}$.

Lemma 10.18. *The integers of* $\mathbf{k}$ *are the Gaussian integers, that is,* $\mathbf{o} = \mathbf{Z} + \mathbf{Z}i$.

Proof. Since every element of $\mathbf{k}$ satisfies a 2-nd degree equation over $\mathbf{Q}$, if element $\alpha = (a/b) + (c/d)i$ of $\mathbf{k}$ is integral over $\mathbf{Q}$ then both $\mathbf{S}_{\mathbf{k}/\mathbf{Q}}\alpha = -2a/b$ and $\mathbf{N}_{\mathbf{k}/\mathbf{Q}}\alpha = (a^2/b^2) + (c^2/d^2) = (a^2d^2 + b^2c^2)/(b^2d^2)$ are integers. Then b must divide a^2d^2. We may take a and b to be relatively prime, so b divides d. Likewise, d must divide b^2c^2; we may take c and d to be relatively prime, so d divides b. Since $d = \pm b$, we have $a^2d^2 + b^2c^2 = a^2b^2 + b^2c^2$ is divisible by b^4, so $a^2 + c^2$ is divisible by b^2. Since $-2a/b$ is an integer then b divides 2. If $b = \pm 2$ then $a^2 + c^2$ would be divisible by 4, but that is impossible because a and c must both be odd if $b = \pm d$ is even. Therefore we must have $b = \pm 1$, and $\alpha = \pm a \pm ci$, so $\mathbf{o} \subset \mathbf{Z} + \mathbf{Z}i$.

Lemma 10.19. *(2) is ramified in* $\mathbf{k}$. $p = (1+i)$ *is the prime of* $\mathbf{k}$ *dividing (2) and* $\left[\mathbf{k}_p : \mathbf{Q}_{(2)}\right] = 2$.

Proof. In the field $\mathbf{Q}(i)$, we have $(1+i)^2 = (2i) = (2)$. Since $efg = 2$, it must be that $p = (1+i)$ is prime, (2) is ramified with ramification index $e = 2$, and $f = 1$, $g = 1$. Finally, $[\mathbf{k}_p : \mathbf{Q}_{(2)}] = ef = 2$.

Lemma 10.20. $p = (1+i)$ *is ramified in* $\mathbf{k}\left(\sqrt{i}\right)$, *and* $\left[\mathbf{k}_p\left(\sqrt{i}\right) : \mathbf{k}_p\right] = 2$.

Proof. First, suppose that there exist a and b in $\mathbf{Q}_{(2)}$ so that $(a + b\,i)^2 = i$. Then $a^2 - b^2 + 2abi = i$, so $a^2 = b^2$ and $2ab = 1$. That would mean $\operatorname{ord}_2(a) = \operatorname{ord}_2(b)$ and $1 + 2\operatorname{ord}_2(a) = 0$ which is impossible. Therefore $x^2 - i$ is irreducible over $\mathbf{k}_p$, so $\left[\mathbf{k}_p\left(\sqrt{i}\right) : \mathbf{k}_p\right] = 2$. Next, we have

$$\mathbf{N}_{\mathbf{k}_p(\sqrt{i})/\mathbf{k}_p}\left(1 + \sqrt{i}\right) = \left(1 + \sqrt{i}\right)\left(1 - \sqrt{i}\right) = 1 - i.$$

We have $1 - i = -i(1+i)$, so $\operatorname{ord}_p(1-i) = 1$. Let $\wp$ be the prime of $\mathbf{k}_p\left(\sqrt{i}\right)$ dividing p, and let $\operatorname{ord}_\wp(1 + \sqrt{i}) = a$. Then

$$\mathrm{N}\wp^{-a} = \left|1 + \sqrt{i}\right|_\wp = \left|\mathbf{N}_{\mathbf{k}_p(\sqrt{i})/\mathbf{k}_p}\left(1 + \sqrt{i}\right)\right|_p = |1 - i|_p = \mathrm{N}p^{-1}.$$

But $\mathrm{N}\wp = \mathrm{N}p^f$, so $af = 1$. We must have $a = f = 1$, so $e = 2$. We have shown that p is ramified and also that $\wp = \left(1 + \sqrt{i}\right)$ in $\mathbf{k}_p\left(\sqrt{i}\right)$.

Lemma 10.21. *Let* p *be the prime of* $\mathbf{k}$ *dividing* (2). *If* α *and* β *are units then* $\left(\frac{\alpha,\beta}{p}\right)$ *only depends on* α *and* β *modulo* (4).

Proof. If β is a unit of $\mathbf{o}_p$ and $\beta = \beta'\big(\text{mod } (4)\big)$ then $\beta^{-1}\beta' = 1\big(\text{mod } (4)\big)$. Therefore $\mathbf{k}_p\left(\sqrt{\beta^{-1}\beta'}\right)/\mathbf{k}_p$ is unramified by lemma 10.12, so $\left(\frac{\alpha,\beta^{-1}\beta'}{p}\right) = 1$ if α is a unit of $\mathbf{o}_p$. This shows that $\left(\frac{\alpha,\beta}{p}\right) = \left(\frac{\alpha,\beta'}{p}\right)$, and the case for α follows by symmetry using lemma 10.6e.

Lemma 10.22. *In $\mathbf{k}_p$, every unit in $\mathbf{o}_p$ is congruent modulo* (4) *to exactly one of the following set of eight elements*

$$\left\{\pm i^a(3+2i)^{a'} \mid \quad a = 0,1; \quad a' = 0,1\right\}.$$

Proof. Since $p = (1+i)$ it follows that an integer $a+bi$ is in p if and only if $a = b(\mathrm{mod}\ 2)$. We have $(4) = p^4$, so the sixteen elements $a+bi$ such that $0 \leq a < 4$ and $0 \leq b < 4$ form a complete set of residues modulo (4). Every element of $\mathbf{o}$ not divisible by p is congruent modulo (4) to exactly one of the set of eight elements

$$\{a+bi \mid \quad 0 \leq a < 4,\ 0 \leq b < 4, \text{ and } a \neq b(\mathrm{mod}\ 2)\}. \tag{10.5}$$

The eight elements $\pm i^a(3i+b)^{a'}$ for $a = 0,1$ and $b = 0,1$ are

$$\pm 1, \quad \pm i, \quad \pm(3+2i), \quad \text{and } \pm(2-3i).$$

These coincide modulo (4) with the eight elements in (10.5).

Proposition 10.23 (quadratic reciprocity law—Gaussian integers). *Let $\alpha = \pm i^a(3+2i)^{a'}$ modulo* (4)*, and $\beta = \pm i^b(3+2i)^{b'}$ modulo* (4)*. Then*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = (-1)^{ba'+ab'}$$

Proof. There are no real infinite primes of $\mathbf{k}$, and $p = (i+i)$ is the only prime dividing (2), so

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = \left(\frac{\pm i^a(3+2i)^{a'}, \pm i^b(3+2i)^{b'}}{p}\right).$$

We have $\left(\frac{\gamma,-1}{p}\right) = \left(\frac{-1,\gamma}{p}\right) = 1$ and also $\left(\frac{\gamma,\gamma}{p}\right) = \left(\frac{\gamma,-\gamma}{p}\right)\left(\frac{\gamma,-1}{p}\right) = 1$ for every unit γ of $\mathbf{k}_p$, since -1 is a square in $\mathbf{k}$. Therefore

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = \left(\frac{(3+2i),i}{p}\right)^{ba'}\left(\frac{i,(3+2i)}{p}\right)^{ab'} = \left(\frac{(3+2i),i}{p}\right)^{ba'-ab'}.$$

We need to show that $\left(\frac{(3+2i),i}{p}\right) = -1$. If $\left(\frac{(3+2i),i}{p}\right) = 1$, then we would have $\left(\frac{\alpha,\beta}{p}\right) = 1$ for all units α and β in $\mathbf{o}_p$. However $\mathbf{k}_p(\sqrt{i})/\mathbf{k}_p$ is ramified, so there exists a unit of $\mathbf{o}_p$ which is not a norm by lemma 7.6. This shows that $\left(\frac{(3+2i),i}{p}\right)$ cannot be 1.

Remark. The quadratic reciprocity law for the rational number field may restated in a form that is analogous to proposition 10.13. If $\alpha = (-1)^a(\mathrm{mod}\ 4)$ and $\beta = (-1)^b(\mathrm{mod}\ 4)$, then

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = (-1)^{ab}$$

Local class field theory. It will be shown that the norm residue symbol maps $\mathbf{k}_p^*$ onto $G(\mathbf{K}_\wp : \mathbf{k}_p)$ with kernel $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$. First, we show that the following assertion holds for abelian extensions by reducing the abelian case to the case of cyclic extensions of prime degree (lemma 11.24), then to the case Kummer extensions (lemma 10.25), then by proving the assertion for Kummer extensions (lemmas 10.26—10.30). We then prove that the kernel is $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$.

Assertion. *If $\wp$ is a prime of $\mathbf{K}$ dividing p then homomorphism*

$$\alpha \to \left(\frac{\alpha, \mathbf{K}/\mathbf{k}}{p}\right)$$

maps $\mathbf{k}_p^*$ onto $G(\mathbf{K}_\wp : \mathbf{k}_p)$.

Because $\mathbf{K}/\mathbf{k}$ is abelian, if $\wp_1, \ldots, \wp_g$ are the primes of $\mathbf{K}$ dividing p then the Galois groups $G(\mathbf{K}_{\wp_i} : \mathbf{k}_p)$ all coincide and the norm groups $\mathbf{N}_{\mathbf{K}_{\wp_i}/\mathbf{k}_p}\mathbf{K}_\wp^*$ all coincide.

Lemma 10.24. *If Assertion holds for cyclic extensions of prime degree, then Assertion holds for abelian extensions in general.*

Proof. Suppose Assertion is false for some abelian extension $\mathbf{K}/\mathbf{k}$ and prime $\wp$ dividing p. Let S be the splitting group of $\wp$, and let $\mathbf{Z}$ be the fixed field of S. Then $S_\wp(\mathbf{K} : \mathbf{Z}) = S_\wp(\mathbf{K} : \mathbf{k})$. Let q be the prime of $\mathbf{Z}$ divisible by $\wp$. Then $\mathbf{k}_p \subset \mathbf{Z}_q \subset \mathbf{K}_\wp$. Every element of $\mathbf{Z}_q$ is fixed by $S = G(\mathbf{K}_\wp : \mathbf{k}_p)$, so $\mathbf{Z}_q = \mathbf{k}_p$, and

$$\alpha \in \mathbf{Z}_q^* = \mathbf{k}_p^* \Longrightarrow \left(\frac{\alpha, \mathbf{K}/\mathbf{Z}}{q}\right) = \left(\frac{\mathbf{N}_{\mathbf{Z}_q/\mathbf{k}_p}\alpha, \mathbf{K}/\mathbf{k}}{p}\right) = \left(\frac{\alpha, \mathbf{K}/\mathbf{k}}{p}\right).$$

Let σ be an automorphism in $S_\wp(\mathbf{K}/\mathbf{k})$ that is not in the image of $\mathbf{k}_p^*$. Then σ is also an automorphism in $S_\wp(\mathbf{K}/\mathbf{Z})$ that is not in the image of $\mathbf{Z}_q^*$. Therefore the Assertion is false for $\mathbf{K}/\mathbf{Z}$ and prime $\wp$ dividing q. We need to show that Assertion is false of a cyclic extension of prime degree. We have

$$S = S_\wp(\mathbf{K} : \mathbf{k}) = S_\wp(\mathbf{K} : \mathbf{Z}) = G(\mathbf{K} : \mathbf{Z}) \quad \text{and} \quad S = G(\mathbf{K}_\wp : \mathbf{k}_p) = G(\mathbf{K}_\wp : \mathbf{Z}_q).$$

Let H the image of $\mathbf{Z}_q^*$. Then H is a proper subgroup of $G(\mathbf{K}_\wp/\mathbf{Z}_q)$. Let $\mathbf{L}$ be the fixed field of H. There exists a subgroup H' such that $H \subset H' \subset S$ and S/H' is cyclic of prime degree. Let $\mathbf{L}'$ be the fixed field of H', and let q' be the prime of $\mathbf{L}'$ which $\wp$ divides. We will show that the Assertion if false for $\mathbf{L}'/\mathbf{Z}$.

$$\begin{array}{ccccccc}
\mathbf{K} & \supset & \mathbf{L} & \supset & \mathbf{L}' & \supset & \mathbf{Z}_q \\
| & & | & & | & & | \\
\{1\} & \subset & H & \subset & H' & \subset & S
\end{array}$$

The number of primes of $\mathbf{K}$ dividing q is equal to the index of $S_\wp(\mathbf{K} : \mathbf{Z})$ in $G(\mathbf{K} : \mathbf{Z})$. It follows that $\wp$ is the only prime of $\mathbf{K}$ which divides q, so q' is the only prime of $\mathbf{L}'$ which divides q. We conclude that $S_{q'}(\mathbf{L}' : \mathbf{Z}) = G(\mathbf{L}' : \mathbf{Z})$, so $S_{q'}(\mathbf{L}' : \mathbf{Z})$ is a non-trivial cyclic group of prime degree. On the other hand, if α is in $\mathbf{Z}_q$ then $\left(\frac{\alpha,\mathbf{L}'/\mathbf{Z}}{q}\right)$ is the restriction of $\left(\frac{\alpha,\mathbf{K}/\mathbf{Z}}{q}\right)$ (which is in H) to $\mathbf{L}'$ (which is contained in the fixed field of H), and is therefore always trivial. This shows that Assertion is false for cyclic extension $\mathbf{L}'$ of $\mathbf{Z}$ and prime q' dividing q.

Lemma 10.25. *If Assertion holds for cyclic extensions of prime degree n where the base field contains the n-th roots of unity, then the assertion holds for all cyclic extensions of prime degree.*

Proof. Let $\mathbf{K}/\mathbf{k}$ be a cyclic extension of prime degree n, and let $\wp$ be a prime of $\mathbf{K}$ dividing prime p of $\mathbf{k}$. If $[\mathbf{K}_\wp/\mathbf{k}_p] = 1$ then Assertion holds trivially for $\mathbf{K}/\mathbf{k}$, so let us suppose that $[\mathbf{K}_\wp/\mathbf{k}_p] = n$. We only have to show the existence of some element of $\mathbf{k}_p^*$ with non-trivial norm residue symbol. Let $\mathbf{Z} = \mathbf{k}(\zeta)$, where ζ is a primitive n-th root of unity. Let $\wp'$ be a prime of $\mathbf{KZ}$ dividing $\wp$, and let p' be a prime of $\mathbf{Z}$ which $\wp'$ divides. $\mathbf{KZ}$ is a abelian extension of $\mathbf{k}$ (lemma 2.12) and $[\mathbf{Z} : \mathbf{k}]$ divides $n-1$, so $\mathbf{Z} \cap \mathbf{K} = \mathbf{k}$ and therefore $[\mathbf{KZ} : \mathbf{Z}] = [\mathbf{K} : \mathbf{k}] = n$.

Since $[\mathbf{Z}_{p'} : \mathbf{k}_p]$ divides $n-1$ then $[(\mathbf{KZ})_{\wp'} : \mathbf{Z}_{p'}] = [\mathbf{K}_\wp : \mathbf{k}_p] = n$. The hypothesis is that Assertion holds for $\mathbf{KZ}/\mathbf{Z}$, so there is an element α in $\mathbf{Z}_{p'}^*$ so that the norm residue symbol $\left(\frac{\alpha,\mathbf{KZ}/\mathbf{Z}}{p'}\right)$ is not trivial, and by lemma 10.3, its restriction to $\mathbf{K}$ is $\left(\frac{\mathbf{N}_{\mathbf{Z}_{p'}/\mathbf{k}p}\alpha,\mathbf{K}/\mathbf{k}}{p}\right)$. If $\left(\frac{\alpha,\mathbf{KZ}/\mathbf{Z}}{p'}\right)$ were trivial on $\mathbf{K}$ then it would be trivial on all of $\mathbf{KZ}$, which is impossible, so we conclude that $\left(\frac{\mathbf{N}_{\mathbf{Z}_{p'}/\mathbf{k}p}\alpha,\mathbf{K}/\mathbf{k}}{p}\right)$ is a non-trivial norm residue symbol for $\mathbf{K}/\mathbf{k}$.

Proof of Assertion for Kummer extensions. Let n be prime, let $\mathbf{k}$ contain the n-th roots of unity, and let $\mathbf{K}/\mathbf{k}$ be a cyclic extension of degree n. By lemma 8.7, there exists an element γ of $\mathbf{k}^*$ so that $\mathbf{K} = \mathbf{k}\left(\sqrt[n]{\gamma}\right)$. Let q be a prime of $\mathbf{k}$. The Galois group $G\big(\mathbf{k}_q\big(\sqrt[n]{\gamma}\big) : \mathbf{k}_q\big)$ does not depend on the choice of the prime of $\mathbf{K}$ dividing q.

Let E be a set of primes of $\mathbf{k}$ containing q, primes dividing (n) or (γ), all infinite primes, and primes such that $\mathbf{I_k} = \mathbf{k}^*\mathbf{I_k}(E)$. Suppose that E contains $s+1$ primes. By the unit theorem (6.13), $\mathbf{k}^*(E)/\mathbf{k}^*(E)^n$ is the direct product of $s+1$ cyclic groups of order n. Let $\beta_0, \ldots, \beta_s$ be a set of generators. In the proof of Lemma 8.18, it was established that there exist primes $p_0, \ldots, p_s$ not in E such that

$$\mathbf{k}_{p_i}\left(\sqrt[n]{\beta_j}\right) = \mathbf{k}_{p_i} \quad \text{if } i \neq j$$

$$\mathbf{k}_{p_j}\left(\sqrt[n]{\beta_j}\right) \neq \mathbf{k}_{p_j} \quad \text{and the extension is not ramified.}$$

For $j = 0, \dots, s$, choose an element π_j in $\mathbf{k}_{p_j}$ so that $p_j = (\pi_j)$ and put

$$\mathbf{i}_j = \mathbf{i}(\pi_j, p_j, \mathbf{k}).$$

Choose α_j in $\mathbf{k}^*$ so that $\mathbf{i}_j \alpha_j^{-1}$ is in $\mathbf{I}_k(E)$. Note that if $p \notin E$ then α_j is in $\mathbf{u}_p$ except at $p = p_j$, and at $p = p_j$, we have $(\alpha_j) = (\pi_j)$.

Lemma 10.26. *If $p \notin E \cup \{p_0, \dots, p_s\}$ then $\left(\frac{\alpha_j, \beta_i}{p}\right) = 1$ for $0 \le i, j \le s$.*

Proof. The only primes of $\mathbf{k}$ which can ramify in $\mathbf{k}_p\left(\sqrt[n]{\beta_i}\right)$ are those dividing n or β_i, all of which are in E, so if p is not in E then $\mathbf{k}_p\left(\sqrt[n]{\beta_i}\right)$ is unramified. If p is not in E and not in $\{p_0, \dots, p_s\}$ then α_j is a unit, so the norm residue symbol $\left(\frac{\alpha_j, \beta_i}{p}\right)$ is trivial for $0 \le i, j \le s$.

Lemma 10.27. *For the primes $p_0, \dots, p_s$ and $0 \le i, j, k \le s$, we have*

$$\left(\frac{\alpha_j, \beta_i}{p_k}\right) = \begin{cases} 1 & \textit{unless } i = j = k \\ \left(\dfrac{\beta_k}{p_k}\right) & \textit{if } i = j = k, \end{cases}$$

and Legendre symbol $\left(\frac{\beta_k}{p_k}\right)$ is a primitive n-th root of unity.

Proof. If $i \ne k$ then $\mathbf{k}_{p_k}\left(\sqrt[n]{\beta_i}\right) = \mathbf{k}_{p_k}$ so $\left(\frac{\alpha_j, \beta_i}{p_k}\right) = 1$ for every j. Suppose $i = k$. If $0 \le j \le s$ and $j \ne k$, then α_j is in $\mathbf{u}_{p_k}$. Since $\mathbf{k}_{p_k}\left(\sqrt[n]{\beta_k}\right)/\mathbf{k}_{p_k}$ is unramified then $\left(\frac{\alpha_j, \beta_k}{p_k}\right) = 1$. Finally, if $j = k$, then since $(\alpha_k) = (\pi_k)$ we have $\left(\frac{\alpha_k, \beta_k}{p_k}\right) = \left(\frac{\beta_k}{p_k}\right)$ by lemma 10.8.

Lemma 10.28. *$\left(\mathbf{k}^*(E)\mathbf{I}_{\mathbf{k}}^n(E)\right)/\mathbf{I}_{\mathbf{k}}^n(E)$ is the direct product of $s+1$ cyclic groups of order n, and the elements $\beta_0, \dots, \beta_s$ generate $\mathbf{k}^*(E)\mathbf{I}_{\mathbf{k}}^n(E)$ modulo $\mathbf{I}_{\mathbf{k}}^n(E)$.*

Proof. We have

$$\frac{\mathbf{k}^*(E)\mathbf{I}_{\mathbf{k}}^n(E)}{\mathbf{I}_{\mathbf{k}}^n(E)} \simeq \frac{\mathbf{k}^*(E)}{\mathbf{k}^*(E) \cap \mathbf{I}_{\mathbf{k}}^n(E)} = \frac{\mathbf{k}^*(E)}{\mathbf{k}^*(E)^n},$$

since, by (8.19a), we have $\mathbf{k}^*(E) \cap \mathbf{I}_{\mathbf{k}}^n(E) = \mathbf{k}^*(E)^n$.

If $\mathbf{i}$ is in $\mathbf{I}_{\mathbf{k}}$, let $\mathbf{i}^E$ denote the projection of $\mathbf{i}$ onto $\prod_{p \in E} \mathbf{k}_p^*$, that is

$$(\mathbf{i}^E)_p = \begin{cases} \mathbf{i}_p & \text{if } p \in E \\ 1 & \text{if } p \notin E. \end{cases}$$

For each of the elements $\alpha_0, \dots, \alpha_s$ we have the projections $\alpha_0^E, \dots, \alpha_s^E$.

Lemma 10.29. *$\mathbf{I}_{\mathbf{k}}(E)/\big(\mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E)\big)$ is the direct product of n^{s+1} cyclic groups of order n, and the projections $\alpha_0^E, \dots, \alpha_s^E$ generate $\mathbf{I}_{\mathbf{k}}(E)$ over $\mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E)$.*

Proof. We found $[\mathbf{I}_{\mathbf{k}}(E) : \mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E)] = n^{s+1}$ at formula (8.18) in the proof of lemma 8.16. Since n is prime and the order of every element of $\mathbf{I}_{\mathbf{k}}(E)/\big(\mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E)\big)$ divides n, then the group must be the product of n^{s+1} cyclic groups of order n.

Let $\alpha = \alpha_0^{a_0} \dots \alpha_s^{a_s}$. Then $\alpha = \alpha^E \prod_{p \notin E} \alpha_p$, and $\alpha^E = (\alpha_0^E)^{a_0} \dots (\alpha_s^E)^{a_s}$. We want to show that the n^{s+1} products

$$(\alpha_0^E)^{a_0} \dots (\alpha_s^E)^{a_s} \qquad 0 \le a_j < n, \quad 0 \le j \le s$$

all lie in different cosets modulo $\mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E)$. Suppose that α^E is in $\mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E)$. If we can show that $a_j = 0 (\text{mod } n)$ for $0 \le j \le s$, then we will be done.

For $i = 0, \dots, s$, the only primes of $\mathbf{k}$ which can ramify in $\mathbf{k}\left(\sqrt[n]{\beta_i}\right)$ are those dividing n or β_i (lemma 8.9), and β_i is in $\mathbf{k}^*(E)$. Therefore all primes which can ramify in $\mathbf{k}\left(\sqrt[n]{\beta_i}\right)$ are in E. This shows that

$$\mathbf{I}^n_{\mathbf{k}}(E) \subset \mathbf{N}_{\mathbf{k}\left(\sqrt[n]{\beta_i}\right)/\mathbf{k}} \mathbf{I}_{\mathbf{k}\left(\sqrt[n]{\beta_i}\right)},$$

so

$$\mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E) \subset \mathbf{k}^*\mathbf{N}_{\mathbf{k}\left(\sqrt[n]{\beta_i}\right)/\mathbf{k}} \mathbf{I}_{\mathbf{k}\left(\sqrt[n]{\beta_i}\right)} \subset \ker\Big(\phi_{\mathbf{k}\left(\sqrt[n]{\beta_i}\right)/\mathbf{k}}\Big).$$

Therefore, if α^E is in $\mathbf{k}^*(E)\mathbf{I}^n_{\mathbf{k}}(E)$, then $\phi_{\mathbf{k}\left(\sqrt[n]{\beta_i}\right)/\mathbf{k}}(\alpha^E) = 1$, so we have

$$1 = \phi_{\mathbf{k}\left(\sqrt[n]{\beta_i}\right)/\mathbf{k}}(\alpha) = \phi_{\mathbf{k}\left(\sqrt[n]{\beta_i}\right)/\mathbf{k}}(\alpha^E) \prod_{p \notin E} \phi_{\mathbf{k}\left(\sqrt[n]{\beta_i}\right)/\mathbf{k}}(\alpha_p) = \prod_{p \notin E} \left(\frac{\alpha, \mathbf{k}\left(\sqrt[n]{\beta_i}\right)/\mathbf{k}}{p}\right).$$

Since $\alpha = \alpha_0^{a_0} \dots \alpha_s^{a_s}$, then by lemma 11.4 the only primes for which the norm residue symbols in the above formula can be non-trivial are $p_0, \dots, p_s$, so we have

$$1 = \prod_{k=0}^{s} \left(\frac{\alpha, \mathbf{k}\left(\sqrt[n]{\beta_i}\right)/\mathbf{k}}{p_k}\right) = \prod_{k=0}^{s} \prod_{j=0}^{s} \left(\frac{\alpha_j, \beta_i}{p_k}\right)^{a_j} \qquad \text{for } i = 0, \dots s.$$

By lemma 10.27, all terms of the product are trivial except when $i = j = k$, so

$$1 = \left(\frac{\alpha_i, \beta_i}{p_i}\right)^{a_i} = \left(\frac{\alpha_i}{p_i}\right)^{a_i} \qquad \text{for } i = 0, \dots, s.$$

The symbols $\left(\frac{\alpha_i}{p_i}\right)$ are primitive n-th roots of unity (lemma 10.27), so

$$a_i = 0 (\text{mod } n) \qquad \text{for } i = 0, \dots, s.$$

This completes the proof of the lemma.

Lemma 10.30. *Let $\mathbf{K} = \mathbf{k}(\sqrt[n]{\gamma})$ be a cyclic extension of prime degree n over field $\mathbf{k}$ containing the n roots of unity, and let prime $\wp$ of $\mathbf{K}$ divide prime q of $\mathbf{k}$. Then Assertion holds for $\mathbf{K}/\mathbf{k}$.*

Proof. The Galois group $G(\mathbf{K}_\wp : \mathbf{k}_p)$ does not depend on the choice of $\wp$ dividing q. Since $\mathbf{k}(\sqrt[n]{\gamma})/\mathbf{k}$ is cyclic of prime degree, then $\mathbf{k}_q(\sqrt[n]{\gamma})/\mathbf{k}_q$ is either trivial or cyclic of degree n. If $\mathbf{k}_q(\sqrt[n]{\gamma}) = \mathbf{k}_q$ then there is nothing to prove, so suppose that $\mathbf{k}_q(\sqrt[n]{\gamma}) \neq \mathbf{k}_q$. We need to show that there exists an element α in $\mathbf{k}_q^*$ for which the norm residue symbol for q is not trivial. Let us make the hypothesis that all norm residue symbols for $\mathbf{k}(\sqrt[n]{\gamma})/\mathbf{k}$ are trivial at the prime q. We will show this to be impossible.

Consider the idele $\mathbf{i}(\gamma, q, \mathbf{k})$ in $\mathbf{I_k}(E)$. By lemmas 10.28 and 10.29, we have

$$\mathbf{i}(\gamma, q, \mathbf{k}) = \alpha^E \beta \mathbf{i}$$

where

$$\alpha = \alpha_0^{a_0} \dots \alpha_s^{a_s}, \quad \beta = \beta_0^{b_0} \dots \beta_s^{b_s}, \quad \mathbf{i} \in \mathbf{I}_\mathbf{k}^n(E).$$

At prime q, we have $\gamma = \alpha^E \beta \mathbf{i}_q$. Since q is in E, we therefore have $\gamma \simeq_n \alpha\beta$, and $\mathbf{k}_q(\sqrt[n]{\alpha\beta}) = \mathbf{k}_q(\sqrt[n]{\gamma})$. But $\mathbf{k}_q(\sqrt[n]{\gamma}) \neq \mathbf{k}_q$, so $\alpha\beta \neq 1$.

For any δ in $\mathbf{k}^*$, we have

$$1 = \prod_p \left(\frac{\delta, \alpha\beta}{p}\right) = \prod_{p \notin E} \left(\frac{\delta, \alpha\beta}{p}\right) \prod_{p \in E} \left(\frac{\delta, \alpha\beta}{p}\right).$$

Consider the product over primes p in E. If $p \neq q$ then we have $1 = \alpha\beta \mathbf{i}_p$ with $\mathbf{i}_p \in (k_p^*)^n$, so $\alpha\beta \simeq_n 1$ in $\mathbf{k}_p^*$, and therefore $\left(\frac{\delta,\alpha\beta}{p}\right) = 1$; if $p = q$, then $\left(\frac{\delta,\gamma}{q}\right) = 1$ by our hypothesis. Therefore all terms of the product over E vanish, and we have

$$1 = \prod_{p \notin E} \left(\frac{\delta, \alpha\beta}{p}\right) \qquad \text{for } \delta \in \mathbf{k}^*. \tag{10.6}$$

Since $\alpha\beta \neq 1$ then either $\alpha \neq 1$ or $\beta \neq 1$. Suppose that $\alpha \neq 1$. Then $a_k \neq 0(\text{mod } n)$ for some k. In this case, take $\delta = \beta_k$. Then (10.6) becomes

$$1 = \prod_{p \notin E} \left(\frac{\beta_k, \alpha\beta}{p}\right) = \prod_{p \notin E} \left(\frac{\beta_k, \alpha}{p}\right) \prod_{p \notin E} \left(\frac{\beta_k, \beta}{p}\right).$$

If p is not in E then $\left(\frac{\beta_k,\beta}{p}\right) = 1$ because $\mathbf{k}_p(\sqrt[n]{\beta_k})/\mathbf{k}_p$ is unramified and β is in $\mathbf{k}^*(E)$; also, $\left(\frac{\beta_k,\alpha}{p}\right) = 1$ unless p is one of $p_0, \dots, p_s$ by lemma 10.26. Then, by lemma 10.27, we have

$$1 = \prod_{j=0}^{s}\left(\frac{\beta_k,\alpha}{p_j}\right) = \prod_{j=0}^{s}\left(\frac{\alpha,\beta_k}{p_j}\right)^{-1} = \left(\frac{\alpha,\beta_k}{p_k}\right)^{-1}$$
$$= \prod_{i=0}^{s}\left(\frac{\alpha_i,\beta_k}{p_k}\right)^{-a_i} = \left(\frac{\alpha_k,\beta_k}{p_k}\right)^{-a_k} = \left(\frac{\beta_k}{p_k}\right)^{-a_k}$$

But this is impossible since $\left(\frac{\beta_k}{p_k}\right)^{-a_k}$ is a primitive n-root of unity by lemma 10.27. Therefore $\alpha = 1$. The other possibility is that $\beta \neq 1$, and we have $b_k \neq 0 (\text{mod } n)$ for some k. In this case, take $\delta = \alpha_k$. Applying lemma 10.26 to (10.6), we obtain

$$1 = \prod_{p\notin E}\left(\frac{\alpha_k,\alpha\beta}{p}\right) = \prod_{p\notin E}\left(\frac{\alpha_k,\beta}{p}\right) = \prod_{j=0}^{s}\left(\frac{\alpha_k,\beta}{p_j}\right).$$

By lemma 10.27, we have

$$1 = \prod_{j=0}^{s}\prod_{i=0}^{s}\left(\frac{\alpha_k,\beta_i}{p_j}\right)^{b_i} = \left(\frac{\alpha_k,\beta_k}{p_k}\right)^{b_k} = \left(\frac{\beta_k}{p_k}\right)^{b_k}.$$

But this is also impossible since $\left(\frac{\beta_k}{p_k}\right)^{b_k}$ is a primitive n-root of unity. Since both cases are impossible, the hypothesis that $\left(\frac{\delta,\gamma}{q}\right) = 1$ for all δ in $\mathbf{k}_q^*$ has led to a contradiction. This concludes the proof.

Proposition 10.31. *Let $\mathbf{K}/\mathbf{k}$ be an abelian extension and let prime $\wp$ of $\mathbf{K}$ divide prime p of $\mathbf{k}$. Then homomorphism*

$$\alpha \to \left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right)$$

maps $\mathbf{k}_p^*$ onto $G(\mathbf{K}_\wp : \mathbf{k}_p)$.

Proof. The proposition follows from lemma 10.24, 10.25 and 10.30.

Second inequality for local extensions. The assertion that $[\mathbf{k}^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*]$ divides $[\mathbf{K}_\wp : \mathbf{k}_p]$ is the *second inequality for local extensions.* We will show that if $\mathbf{K}/\mathbf{k}$ is abelian then the second inequality holds for the completions $\mathbf{K}_\wp/\mathbf{k}_p$.

Proposition 10.32. *Suppose that* $\mathbf{K}/\mathbf{k}$ *is an abelian extension and* $\mathbf{L}_1$, $\mathbf{L}_2$, $\mathbf{L}_3$ *are subfields of* $\mathbf{K}_\wp$ *such that* $\mathbf{K}_\wp \supset \mathbf{L}_1 \supset \mathbf{L}_2 \supset \mathbf{L}_3 \supset \mathbf{k}_p$. *If the second inequality holds for both* $\mathbf{L}_1/\mathbf{L}_2$ *and* $\mathbf{L}_2/\mathbf{L}_3$*, then the second inequality holds for* $\mathbf{L}_1/\mathbf{L}_3$.

Proof. (By lemma 10.2, local fields $\mathbf{L}_1$, $\mathbf{L}_2$, $\mathbf{L}_3$ are the completions of subfields of $\mathbf{K}$ containing $\mathbf{k}$, but the primes of these three intermediate fields are not explicitly needed.) In the following diagram, homomorphism $\mathbf{N}_{\mathbf{L}_2/\mathbf{L}_3}$ is onto, so $\iota\mathbf{N}_{\mathbf{L}_2/\mathbf{L}_3}$ is onto and the kernel contains $\mathbf{N}_{\mathbf{L}_1/\mathbf{L}_2}\mathbf{L}_1^*$.

$$\begin{tikzcd}
\mathbf{L}_2^* \arrow[r, "\mathbf{N}_{\mathbf{L}_2/\mathbf{L}_3}"] \arrow[d] & \mathbf{N}_{\mathbf{L}_2/\mathbf{L}_3}\mathbf{L}_2^* \arrow[d, "\iota"] \\
\frac{\mathbf{L}_2^*}{\mathbf{N}_{\mathbf{L}_1/\mathbf{L}_2}\mathbf{L}_1^*} \arrow[r, "\overline{\mathbf{N}_{\mathbf{L}_2/\mathbf{L}_3}}"] & \frac{\mathbf{N}_{\mathbf{L}_2/\mathbf{L}_3}\mathbf{L}_2^*}{\mathbf{N}_{\mathbf{L}_1/\mathbf{L}_3}\mathbf{L}_1^*}
\end{tikzcd}$$

The induced homomorphism $\overline{\mathbf{N}_{\mathbf{L}_2/\mathbf{L}_3}}$ is onto, so $[\mathbf{N}_{\mathbf{L}_2/\mathbf{L}_3}\mathbf{L}_2^* : \mathbf{N}_{\mathbf{L}_1/\mathbf{L}_3}\mathbf{L}_1^*]$ divides $[\mathbf{L}_2^* : \mathbf{N}_{\mathbf{L}_1/\mathbf{L}_2}\mathbf{L}_1^*]$. We have

$$[\mathbf{L}_3^* : \mathbf{N}_{\mathbf{L}_1/\mathbf{L}_3}\mathbf{L}_1^*] = [\mathbf{L}_3^* : \mathbf{N}_{\mathbf{L}_2/\mathbf{L}_3}\mathbf{L}_2^*][\mathbf{N}_{\mathbf{L}_2/\mathbf{L}_3}\mathbf{L}_2^* : \mathbf{N}_{\mathbf{L}_1/\mathbf{L}_3}\mathbf{L}_1^*].$$

Therefore $[\mathbf{L}_3^* : \mathbf{N}_{\mathbf{L}_1/\mathbf{L}_3}\mathbf{L}_1^*]$ divides $[\mathbf{L}_3^* : \mathbf{N}_{\mathbf{L}_2/\mathbf{L}_3}\mathbf{L}_2^*][\mathbf{L}_2^* : \mathbf{N}_{\mathbf{L}_1/\mathbf{L}_2}\mathbf{L}_1^*]$. By the hypothesis, $[\mathbf{L}_3^* : \mathbf{N}_{\mathbf{L}_1/\mathbf{L}_3}\mathbf{L}_1^*]$ must divide $[\mathbf{L}_3 : \mathbf{L}_2][\mathbf{L}_1 : \mathbf{L}_2] = [\mathbf{L}_1 : \mathbf{L}_3]$, as claimed.

Lemma 10.33. *If* $\mathbf{K}_\wp/\mathbf{k}_p$ *is abelian then* $[\mathbf{k}_p^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$ *divides* $[\mathbf{K}_\wp : \mathbf{k}_p]$.

Proof. The abelian group $G(\mathbf{K}_\wp : \mathbf{k}_p)$ has subgroups G_i for $0 \leq i \leq s$ such that

$$G(\mathbf{K}_\wp : \mathbf{k}_p) = G_0 \supset G_1 \supset \cdots \supset G_s = \{1\}$$

and G_i/G_{i+1} is cyclic. Let $\mathbf{K}_i$ be the fixed field of G_i. The second inequality holds for the cyclic extensions $\mathbf{K}_{i+1}/\mathbf{K}_i$ (proposition 7.4). If the second inequality holds for $\mathbf{K}_i/\mathbf{K}_0$ then it holds for $\mathbf{K}_{i+1}/\mathbf{K}_0$ by lemma 10.32. By induction, the second inequality holds for $\mathbf{K}_s/\mathbf{K}_0 = \mathbf{K}_\wp/\mathbf{k}_p$, and the conclusion follows.

Theorem 10.34. *If* $\mathbf{K}/\mathbf{k}$ *is abelian then* $\alpha \to \left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right)$ *maps* $\mathbf{k}_p^*$ *onto* $G(\mathbf{K}_\wp : \mathbf{k}_p)$ *and the kernel is* $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$.

Proof. If H is the kernel of $\alpha \to \left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right)$, then we know that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$ is contained in H (lemma 10.5), so $[\mathbf{k}_p^* : H]$ divides $[\mathbf{k}^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*]$. We know that $[\mathbf{k}_p^* : H] = [\mathbf{K}_\wp : \mathbf{k}_p]$ (proposition 10.31), and that $[\mathbf{k}^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*]$ divides $[\mathbf{K}_\wp : \mathbf{k}_p]$ (lemma 10.33). Therefore $[\mathbf{k}^* : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*] = [\mathbf{K}_\wp : \mathbf{k}_p]$. Finally, since $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* \subset H$, then we have $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$.

Ramification and the conductor. If $\mathbf{K}/\mathbf{k}$ is abelian, let H be the kernel of $\phi_{\mathbf{K}/\mathbf{k}} \to G(\mathbf{K} : \mathbf{k})$, and let modulus n be the conductor of H. Then $W(n) \subset H$ and if n' is a modulus such that $W(n') \subset H$ then n divides n'.

Let m_p be the conductor of $\left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right)$, that is, let m_p be the smallest non-negative integer such that $W_p(m_p)$ is contained in the kernel of $\alpha \to \left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right)$.

Lemma 10.35. $n = \prod_p m_p$.

Proof. Let $m = \prod_p m_p$. We first want to show that $W(m) \subset H$. Let E contain all infinite primes of $\mathbf{k}$ and all primes that ramify in $\mathbf{K}$. Let E_1 contain all primes of $\mathbf{k}$ not in E such that $m_p = 0$, and let E_2 contain all primes not in E such that $m_p > 0$. E and E_2 contain only finitely many primes. If $\mathbf{i}$ is in $\mathbf{I_k}$ then $\mathbf{i} = \mathbf{i}_1\mathbf{i}_2$ where

$$\mathbf{i}_1 = \prod_{p \in E_1} \mathbf{i}(\mathbf{i}_p, p, \mathbf{k}),$$
$$\mathbf{i}_2 = \prod_{p \in E_2 \cup E} \mathbf{i}(\mathbf{i}_p, p, \mathbf{k}).$$

Since $\mathbf{i}_1 \in \mathbf{I}_k\{E\}$ then $\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i}_1)$ may be computed from definition (2.1). Since $|\mathbf{i}_1|_p = 1$ at every prime p then $\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i}_1) = 1$. At each coordinate of $\mathbf{i}_2$ we have $(\mathbf{i}_2)_p \in W_p(m_p)$, so

$$\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i}_2) = \prod_p \phi_{\mathbf{K}/\mathbf{k}}\big(\mathbf{i}(\mathbf{i}_p, p, \mathbf{k})\big) = \prod_p \left(\frac{\mathbf{i}_p, \mathbf{K}/\mathbf{k}}{p}\right) = 1.$$

Therefore $\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i}) = \phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i}_1)\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i}_2) = 1$. This shows that $W(m) \subset H$, so n divides m.

We next show that n cannot be a proper divisor of m. Suppose that $n_p < m_p$ for some p. Then there exists an element α in $W_p(n_p) \subset \mathbf{k}_p^*$ such that $\left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right) \neq 1$. Put $\mathbf{i} = \mathbf{i}(\alpha, p, \mathbf{k})$. Then $\mathbf{i}$ is in $W(n) \subset \ker\left(\phi_{\mathbf{K}/\mathbf{k}}\right)$, so $\left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right) = \phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i}) = 1$, a contradiction.

Proposition 10.36. *If $\mathbf{K}/\mathbf{k}$ is an abelian extension, then a prime of $\mathbf{k}$ is ramified in $\mathbf{K}$ if and only if it divides the conductor of the kernel of $\phi_{\mathbf{K}/\mathbf{k}}$.*

Proof. Let m be the conductor of the kernel of $\phi_{\mathbf{K}/\mathbf{k}}$. Let p be a prime of $\mathbf{k}$ and let e be the ramification index of p. We want to show that $e > 1$ if and only if $m_p > 0$ or, equivalently, that $e = 1$ if and only if $m_p = 0$.

Suppose that p is finite and not ramified in $\mathbf{K}$. Since every unit of an unramified extension is a norm then $W_p(0)$ is contained in the kernel of $\left(\frac{\alpha,\mathbf{K}/\mathbf{k}}{p}\right)$. Therefore

$m_p = 0$ if p is finite. Suppose that p is infinite and not ramified in $\mathbf{K}$. This means $\mathbf{K}_\wp = \mathbf{k}_p$, so every element of $\mathbf{k}_p^*$ is a norm. This shows that $W_p(0) = \mathbf{k}_p^*$ is contained in the kernel of the norm residue symbol, so $m_p = 0$ if p is infinite. In both case, if $e = 1$ then $m_p = 0$.

Conversely, suppose that p is ramified. If p is infinite then $\mathbf{k}_p$ is real and $\mathbf{K}_\wp$ is complex. Not every element of $\mathbf{k}_p^*$ is a norm, so we must have $m_p = 1$. Now suppose that p is a finite prime of $\mathbf{k}$ with ramification index $e > 1$ in $\mathbf{K}$. To show that $m_p > 0$, we need to show that not every unit (element of $W_p(0)$) has a trivial norm residue symbol. Let $I = I_\wp$ be the inertial subgroup of the splitting group $S = S_\wp$. Let $\mathbf{T}$ be the fixed field of I and let q be the prime of $\mathbf{T}$ which $\wp$ divides. I has order e, and q is completely ramified in $\mathbf{K}/\mathbf{T}$ with degree and ramification index both equal to e. I has a subgroup I' so that I/I' is cyclic of order $e' > 1$. Let $\mathbf{T}'$ be the fixed field of I' and let q' be the prime of $\mathbf{T}'$ which $\wp$ divides.

$$\begin{array}{ccccccc}
\{1\} & \subset & I' & \subset & I & \subset & G \\
\mathbf{K} & \supset & \mathbf{T}' & \supset & \mathbf{T} & \supset & \mathbf{k} \\
\mathbf{K}_\wp & \supset & \mathbf{T}'_q & \supset & \mathbf{T}_q & \supset & \mathbf{k}_p
\end{array}$$

Then $\mathbf{T}'/\mathbf{T}$ is a cyclic extension of degree e', and q is completely ramified in $\mathbf{T}'/\mathbf{T}$ with ramification index e'. By proposition 7.3, we have

$$\left[\mathbf{u}_q : \mathbf{N}_{\mathbf{T}_{q'}/\mathbf{T}_q} \mathbf{U}_{q'}\right] = e' > 1$$

Let α be an element of $\mathbf{u}_q$ that is not in $\mathbf{N}_{\mathbf{T}_{q'}/\mathbf{T}_q} \mathbf{U}_{q'}$. Then $\left(\frac{\alpha, \mathbf{T}'/\mathbf{T}}{q}\right)$ is not trivial on $\mathbf{T}'$, so $\left(\frac{\alpha, \mathbf{K}/\mathbf{T}}{q}\right)$ is not trivial. By corollary 10.4, we have

$$\left(\frac{\alpha, \mathbf{K}/\mathbf{T}}{q}\right) = \left(\frac{\mathbf{N}_{\mathbf{T}_q/\mathbf{k}_p} \alpha, \mathbf{K}/\mathbf{k}}{p}\right).$$

Then $\mathbf{N}_{\mathbf{T}_q/\mathbf{k}_p} \alpha$ is an element of $\mathbf{u}_p = W_p(0)$ with non-trivial norm residue symbol. This shows that $m_p > 0$.

Remark. We have not determined the precise value of $[\mathbf{u}_p : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}} \mathbf{U}_\wp]$ except in the cyclic case, but we have at least shown that $[\mathbf{u}_p : \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}} \mathbf{U}_\wp] > 1$ if $e > 1$.

Behavior under isomorphisms. Suppose that $\mathbf{K}$ and $\mathbf{K}'$ are two finite extensions of the rational number field and let $\tau : \mathbf{K} \to \mathbf{K}'$ be an isomorphism. Let $\mathbf{k}$ be a subfield of $\mathbf{K}$ and let $\mathbf{k}'$ be the image of $\mathbf{k}$ under τ.

Lemma 10.37. *If* $\mathbf{K}/\mathbf{k}$ *is a normal extension then* $\mathbf{K}'/\mathbf{k}'$ *is also normal and* $G(\mathbf{K}' : \mathbf{k}') = \tau G(\mathbf{K} : \mathbf{k}) \tau^{-1}$.

Proof. We first show that $\mathbf{K}'/\mathbf{k}'$ is normal. Any element $\tau\alpha$ in $\mathbf{K}'$ is a root of an irreducible polynomial $g(x)$ over $\mathbf{k}'$, and $g(x) = \tau\big(f(x)\big)$ for some irreducible polynomial $f(x)$ over $\mathbf{k}$. We have $\tau\bigl(f(\alpha)\bigr) = g(\tau\alpha) = 0$, so α is a root of $f(x)$. If $\mathbf{K}/\mathbf{k}$ is normal then $f(x)$ splits completely over $\mathbf{k}$, so $g(x)$ splits completely over $\mathbf{k}'$, and therefore $\mathbf{K}'/\mathbf{k}'$ is normal. We have $\tau G(\mathbf{K} : \mathbf{k})\tau^{-1} \subset G(\mathbf{K}' : \mathbf{k}')$. Apply this result to the inverse isomorphism $\tau^{-1} : \mathbf{K}' \to \mathbf{K}$ to obtain $\tau^{-1}G(\mathbf{K}' : \mathbf{k}')\tau \subset G(\mathbf{K} : \mathbf{k})$, so the groups are identical.

Lemma 10.38. *For each prime p of $\mathbf{k}$ we can define a valuation p' of $\mathbf{k}'$ by $|\alpha'|_{p'} = |\tau^{-1}\alpha'|_p$. If p is a prime ideal of $\mathbf{k}$ then p' is a prime ideal of $\mathbf{k}'$ and $\tau(p) = p'$. (Note: if p is an infinite prime then set $\tau(p) = p'$ by formal definition.)*

Proof. If p is a prime ideal then we have $\alpha' \in p'$ if and only if $|\alpha'|_{p'} < 1$ if and only if $|\tau^{-1}\alpha'|_p < 1$ if and only if $\tau^{-1}\alpha' \in p$ if and only if $\alpha' \in \tau(p)$.

Lemma 10.39. *Let $\wp_1, \ldots, \wp_g$ be the primes of $\mathbf{K}$ dividing p. Then the primes of $\mathbf{K}'$ dividing $\tau(p)$ are $\tau(\wp_1), \ldots, \tau(\wp_g)$.*

Proof. Certainly $|\tau^{-1}\alpha'|_{\wp_i}$ is a valuation of $\mathbf{K}'$ extending $\tau(p)$, so $\tau(\wp_i)$ is a prime dividing $\tau(p)$. Conversely, if $\wp'$ is a prime of $\mathbf{K}'$ dividing $\tau(p)$ then $\tau^{-1}(\wp')$ is a prime of $\mathbf{K}$ dividing p, so $\tau^{-1}(\wp') = \wp_i$ for some i, and $\wp' = \tau(\wp_i)$.

Lemma 10.40. *If $\wp$ is unramified in a normal extension $\mathbf{K}/\mathbf{k}$ the $\tau(\wp)$ is unramified in $\mathbf{K}'/\mathbf{k}'$.*

Proof. If α is an integral element in $\mathbf{k}$ then $\tau(\alpha)$ is integral in $\mathbf{k}'$ and vice versa. If $\sigma(\wp) = \wp$ then $\tau\sigma\tau^{-1}\tau(\wp) = \tau\wp$, so σ is in the splitting group of $\wp$ if and only if $\tau\sigma\tau^{-1}$ is in the splitting group of $\tau(\wp)$. We have

$$\sigma(\alpha) - \alpha \in \wp \Longleftrightarrow \tau\sigma\tau^{-1}(\tau\alpha) - \tau(\alpha) \in \tau(\wp).$$

so σ is in the inertial group of $\wp$ if and only if $\tau\sigma\tau^{-1}$ is in the inertial group of $\tau(\wp)$.

Lemma 10.41. *If $\mathbf{K}/\mathbf{k}$ is an abelian extension and $\tau : \mathbf{K} \to \mathbf{K}'$ is an ismorphism with $\mathbf{k}' = \tau(\mathbf{k})$ and $p' = \tau(p)$ then*

$$\tau \left(\frac{\mathbf{K}/\mathbf{k}}{p}\right) \tau^{-1} = \left(\frac{\mathbf{K}'/\mathbf{k}'}{p'}\right).$$

Proof. The isomorphism τ mapping $\mathbf{o}$ to $\mathbf{o}'$ and p to p' determines an isomorphism of the finite field $\mathbf{o}/p$ onto $\mathbf{o}'/p'$, so we have $\mathrm{N}p = \mathrm{N}p'$. If α' is in $\mathbf{o}'$ then

$$\left(\frac{\mathbf{K}/\mathbf{k}}{p}\right) \tau^{-1}(\alpha') = \bigl(\tau^{-1}(\alpha')\bigr)^{\mathrm{N}p} (\mathrm{mod}\ \wp)$$

so

$$\tau \left(\frac{\mathbf{K}/\mathbf{k}}{p}\right) \tau^{-1}(\alpha') = (\alpha')^{\mathrm{N}p'} \bigl(\mathrm{mod}\ \tau(\wp)\bigr),$$

and this is the defining property of the Artin symbol for p' in $\mathbf{K}'/\mathbf{k}$.

Lemma 10.42. *Let $\mathbf{K}/\mathbf{k}$ be an abelian extension. The isomorphism τ determines an isomorphism $\mathbf{I_k} \to \mathbf{I_{k'}}$ of idele groups by $\big(\tau(\mathbf{i})\big)_{\tau(p)} = \mathbf{i}_p$, and we have $\tau\phi_{\mathbf{K}/\mathbf{k}}(\mathbf{i})\tau^{-1} = \phi_{\mathbf{K}'/\mathbf{k}'}\big(\tau(\mathbf{i})\big)$, so the following diagram is commutative.*

$$\begin{tikzcd}
\mathbf{I_k} \arrow[r, "\phi_{\mathbf{K}/\mathbf{k}}"] \arrow[d, "\tau"] & G(\mathbf{K}:\mathbf{k}) \arrow[d, "\tau(\cdot)\tau^{-1}"] \\
\mathbf{I_{k'}} \arrow[r, "\phi_{\mathbf{K}'/\mathbf{k}'}"] & G(\mathbf{K}':\mathbf{k}')
\end{tikzcd}$$

Proof. Let E and E' contain the infinite and ramified primes of $\mathbf{k}$ and $\mathbf{k}'$, respectively. There is a one-to-one correspondence between primes in E and E'. Putting $\mathbf{i}' = \tau(\mathbf{i})$, we need to show that $\tau\phi_{\mathbf{K}/\mathbf{k}}\big(\tau^{-1}(\mathbf{i}')\big)\tau^{-1} = \phi_{\mathbf{K}'/\mathbf{k}'}(\mathbf{i}')$ for any idele $\mathbf{i}'$ in $\mathbf{I_{k'}}$. Certainly $\tau\phi_{\mathbf{K}/\mathbf{k}}\big(\tau^{-1}(\mathbf{i}')\big)\tau^{-1}$ is a homomorphism of $\mathbf{I_{k'}}$ onto $G(\mathbf{K}':\mathbf{k}')$, and the kernel contains ${\mathbf{k}'}^*$. We need to show that it agrees with $\phi_{\mathbf{K}'\mathbf{k}'}(\mathbf{i}')$ on $\mathbf{I_{k'}}\{E'\}$. Note that since $\tau(\mathbf{i})_{\tau(p)} = \mathbf{i}_p$ then $\operatorname{ord}_{\tau(p)}\big(\tau(\mathbf{i})\big) = \operatorname{ord}_p(\mathbf{i})$, or $\operatorname{ord}_{p'}(\mathbf{i}') = \operatorname{ord}_p(\mathbf{i})$ where $\mathbf{i}' = \tau(\mathbf{i})$ and $p' = \tau(p)$. Then

$$\begin{aligned}
\phi_{\mathbf{K}'/\mathbf{k}'}(\mathbf{i}') = \prod_{p'\notin E'} \left(\frac{\mathbf{K}'/\mathbf{k}'}{p'}\right)^{\operatorname{ord}_{p'}(\mathbf{i}')} &= \prod_{p\notin E} \left(\tau\left(\frac{\mathbf{K}/\mathbf{k}}{p}\right)\tau^{-1}\right)^{\operatorname{ord}_p(\mathbf{i})} \\
&= \tau\left(\prod_{p\notin E}\left(\frac{\mathbf{K}/\mathbf{k}}{p}\right)^{\operatorname{ord}_p(\mathbf{i})}\right)\tau^{-1} = \tau\phi_{\mathbf{K}/\mathbf{k}}\big(\tau^{-1}(\mathbf{i}')\big)\tau^{-1}.
\end{aligned}$$

Since $\phi_{\mathbf{K}'/\mathbf{k}'}(\mathbf{i}')$ and $\tau\phi_{\mathbf{K}/\mathbf{k}}\big(\tau^{-1}(\mathbf{i}')\big)\tau^{-1}$ agree on $\mathbf{I_{k'}}\{E'\}$ then they agree on all of $\mathbf{I_{k'}}$, which completes the proof.

Lemma 10.43. *If $\mathbf{K}/\mathbf{k}$ is an abelian extension and $\tau : \mathbf{K} \to \mathbf{k}'$ is an isomorphism with $\mathbf{k}' = \tau(\mathbf{k})$, $\alpha' = \tau(\alpha)$ and $p' = \tau(p)$, then we have*

$$\left(\frac{\alpha', \mathbf{K}'/\mathbf{k}'}{p'}\right) = \tau\left(\frac{\alpha, \mathbf{K}/\mathbf{k}}{p}\right)\tau^{-1}.$$

Proof. Under the isomorphism $\tau : \mathbf{I_k} \to \mathbf{I_{k'}}$, we have $\tau\big(\mathbf{i}(\alpha, p, \mathbf{k})\big) = \mathbf{i}(\alpha', p', \mathbf{k}')$, so the conclusion follows by Lemma 10.42.