PROOF OF THEOREM 2 (EXISTENCE THEOREM)

Let $\mathbf{k}$ be a finite extension of the rational field $\mathbf{Q}$ and let $\mathbf{K}$ be an abelian extension of $\mathbf{k}$. In this section, p will denote a rational prime and $\wp$ will denote a prime of $\mathbf{k}$.

LEMMA 12.1. *Let H be a closed subgroup of finite index in $\mathbf{I_k}$ containing $\mathbf{k}^*$. If there exists an abelian extension $\mathbf{L}/\mathbf{k}$ such that $\ker(\phi_{\mathbf{L}/\mathbf{k}}) \subset H$, then there exists an abelian extension $\mathbf{K}/\mathbf{k}$ such that $\ker(\phi_{\mathbf{K}/\mathbf{k}}) = H$.*

PROOF. Let $\mathbf{K}$ be the fixed field of the image of H in $G(\mathbf{L} : \mathbf{k})$ under the homomorphism $\phi_{\mathbf{L}/\mathbf{k}}$. Then $\phi_{\mathbf{K}/\mathbf{k}}$ is the restriction of $\phi_{\mathbf{L}/\mathbf{k}}$ to $\mathbf{K}$. The kernel of $\phi_{\mathbf{K}/\mathbf{k}}$ is precisely H.

LEMMA 12.2. *Let H be a closed subgroup of finite index in $\mathbf{I_k}$ containing $\mathbf{k}^*$, and let $\mathbf{Z}/\mathbf{k}$ be a cyclic extension. Let H' be the inverse image of H under the homomorphism $\mathbf{N}_{\mathbf{Z}/\mathbf{k}} : \mathbf{I_Z} \to \mathbf{I_k}$. If Theorem 2 holds for subgroup H' of $\mathbf{I_Z}$, then there exists an abelian extension $\mathbf{K}$ of $\mathbf{k}$ such that $\ker(\phi_{\mathbf{K}/\mathbf{k}}) = H$.*

PROOF. Let us check that H' has the required properties. We have $\mathbf{Z}^*$ contained in H', and H' is closed because $\mathbf{N}_{\mathbf{Z}/\mathbf{k}}$ is continuous. We need to show that $[\mathbf{I_Z} : H']$ is finite. Since $H' = \mathbf{N}_{\mathbf{Z}/\mathbf{k}}^{-1} H$ then $\mathbf{N}_{\mathbf{Z}/\mathbf{k}} H' = H \cap \mathbf{N}_{\mathbf{Z}/\mathbf{k}} \mathbf{I_Z}$, so

$$\frac{\mathbf{I_Z}}{H'} \simeq \frac{\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I_Z}}{H \cap \mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I_Z}} \simeq \frac{H\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I_Z}}{H} \subset \frac{\mathbf{I_k}}{H}.$$

Therefore $[\mathbf{I_Z} : H']$ is finite. By the hypothesis, there exists an abelian extension $\mathbf{T}$ of $\mathbf{Z}$ so that $\ker(\phi_{\mathbf{T}/\mathbf{Z}}) = H'$. We want to show that $\mathbf{T}/\mathbf{k}$ is abelian. First, we show that $\mathbf{T}/\mathbf{k}$ is normal. Let σ be a generator of $G(\mathbf{Z} : \mathbf{k})$. The automorphism σ can be extended to an isomorphism (also denoted σ) of $\mathbf{T}$ to a conjugate field $\mathbf{T}'$. By lemma 10.42, for $\mathbf{i}$ in $\mathbf{I_Z}$ we have

$$\phi_{\mathbf{T}'/\mathbf{Z}}(\sigma\mathbf{i}) = \sigma\big(\phi_{\mathbf{T}/\mathbf{Z}}(\mathbf{i})\big)\sigma^{-1}.$$

We have $\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\sigma(\mathbf{i}) = \mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{i}$, so $\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\big(\mathbf{i}^{-1}\sigma(\mathbf{i})\big) = 1$, so $\mathbf{i}^{-1}\sigma(\mathbf{i})$ is in H'. Therefore $\mathbf{i}$ is in H' if and only if $\sigma(\mathbf{i})$ is in H', which is the same as $\sigma^{-1}(\mathbf{j})$ is in H' if and only if $\mathbf{j}$ is in H'. Putting $\mathbf{i} = \sigma^{-1}(\mathbf{j})$, we have

$$\phi_{\mathbf{T}'/\mathbf{Z}}(\mathbf{j}) = \sigma\big(\phi_{\mathbf{T}/\mathbf{Z}}(\sigma^{-1}(\mathbf{j})\big)\sigma^{-1}.$$

This shows that $\ker(\phi_{\mathbf{T}'/\mathbf{Z}}) = H'$, and therefore $\mathbf{T}' = \mathbf{T}$. Since $\sigma(\mathbf{T}) = \mathbf{T}$ and σ generates $G(\mathbf{Z} : \mathbf{k})$, then $\mathbf{T}$ is invariant under every extension of every automorphism in $G(\mathbf{Z} : \mathbf{k})$. This shows that $\mathbf{T}$ is normal over $\mathbf{k}$.

To show that $\mathbf{T}/\mathbf{k}$ is abelian, we have $\phi_{\mathbf{T}/\mathbf{Z}}\big(\mathbf{i}^{-1}\sigma(\mathbf{i})\big) = 1$ since $\mathbf{i}^{-1}\sigma(\mathbf{i})$ is in H'. Then $\phi_{\mathbf{T}/\mathbf{Z}}\big(\sigma(\mathbf{i})\big) = \phi_{\mathbf{T}/\mathbf{Z}}\big(\mathbf{i}\big)$, so $\sigma\big(\phi_{\mathbf{T}/\mathbf{k}}(\mathbf{i})\big)\sigma^{-1} = \phi_{\mathbf{T}/\mathbf{Z}}(\mathbf{i})$. Since $\phi_{\mathbf{T}/\mathbf{Z}}$ is onto $G(\mathbf{T} : \mathbf{Z})$ then σ commutes with every automorphism in $G(\mathbf{T} : \mathbf{Z})$. Every element of $G(\mathbf{T} : \mathbf{k})$ is of the form $\sigma^a\tau$ with τ in $G(\mathbf{T} : \mathbf{Z})$, so $G(\mathbf{T} : \mathbf{k})$ is abelian.

We now know that $\phi_{\mathbf{T}/\mathbf{k}}$ is defined. The kernel of $\phi_{\mathbf{T}/\mathbf{k}}$ is $\mathbf{k}^*\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{I}_{\mathbf{T}}$. Then

$$\mathbf{k}^*\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{I}_{\mathbf{T}} = \mathbf{k}^*\mathbf{N}_{\mathbf{Z}/\mathbf{k}}(\mathbf{N}_{\mathbf{T}/\mathbf{Z}}\mathbf{I}_{\mathbf{T}}) \subset \mathbf{k}^*\mathbf{N}_{\mathbf{Z}/\mathbf{k}}(H') \subset H.$$

Since $\ker(\phi_{\mathbf{T}/\mathbf{k}})$ is contained in H, then by lemma 12.1 there exists an abelian extension $\mathbf{K}/\mathbf{k}$ such that $\ker(\phi_{\mathbf{K}/\mathbf{k}}) = H$. This completes the proof.

LEMMA 12.3. *Suppose that p is a prime number, $\mathbf{k}$ contains the p-th roots of unity, H is a closed subgroup of finite index in $\mathbf{I}_{\mathbf{k}}$ containing $\mathbf{k}^*$ and $[\mathbf{I}_{\mathbf{k}} : H] = p$. Then there exists an abelian extension $\mathbf{K}/\mathbf{k}$ such that $\ker(\phi_{\mathbf{K}/\mathbf{k}}) = H$.*

PROOF. Let E be a set of primes of $\mathbf{k}$ containing all infinite primes, all primes dividing p, all primes dividing the conductor of H, and so that $\mathbf{I}_{\mathbf{k}} = \mathbf{k}^*\mathbf{I}_k(E)$. By corollary 8.20, there exists an abelian extension $\mathbf{L}/\mathbf{k}$ such that the kernel of $\phi_{\mathbf{L}/\mathbf{k}}$ is $\mathbf{k}^*\mathbf{I}_{\mathbf{k}}^p(E)$. Since $[\mathbf{I}_{\mathbf{k}} : H] = p$ then we have

$$\prod_{\wp \in E} (\mathbf{k}_\wp^*)^p \prod_{\wp \notin E} \{1\} \subset H$$

and since E contains all primes dividing the conductor of H then

$$\prod_{\wp \in E} \{1\} \prod_{\wp \notin E} \mathbf{u}_\wp \subset H.$$

Therefore $\mathbf{I}_{\mathbf{k}}^p(E)$ is contained in H, so the kernel of $\phi_{\mathbf{L}/\mathbf{k}}$ is contained in H. By lemma 12.1, there exists an abelian extension $\mathbf{K}/\mathbf{k}$ such that $\ker(\phi_{\mathbf{K}/\mathbf{k}}) = H$.

LEMMA 12.4. *Suppose that* p *is a prime number,* H *is a closed subgroup of finite index in* $\mathbf{I_k}$ *containing* $\mathbf{k}^*$ *and* $[\mathbf{I_k} : H] = p$*. Then there exists an abelian extension* $\mathbf{K}/\mathbf{k}$ *such that* $\ker(\phi_{\mathbf{K}/\mathbf{k}}) = H$*.*

PROOF. Let $\mathbf{Z}$ be the field obtained by adjoining the p-th roots of unity to $\mathbf{k}$. Then $\mathbf{Z}/\mathbf{k}$ is a cyclic extension. Define H' to be the inverse image of H as in the hypothesis of lemma 12.2. As in the proof of lemma 12.2, we have that $[\mathbf{I_Z} : H']$ is a divisor of $[\mathbf{I_k} : H]$. Since p is prime, then $[\mathbf{I_Z} : H']$ is 1 or p. In the former case, take $\mathbf{T} = \mathbf{Z}$. In the latter case, we apply lemma 12.3 to $\mathbf{Z}$ and H'. There exists an abelian extension $\mathbf{T}/\mathbf{Z}$ such that $\ker(\phi_{\mathbf{T}/\mathbf{Z}}) = H'$. By lemma 12.2, there exists an abelian extension $\mathbf{K}/\mathbf{k}$ such that $\ker(\phi_{\mathbf{K}/\mathbf{k}}) = H$.

PROPOSITION 12.5. *If* H *is a closed subgroup of finite index in* $\mathbf{I_k}$ *and contains* $\mathbf{k}^*$*, then there is an abelian extension* $\mathbf{K}$ *of* $\mathbf{k}$ *such that* H *is the kernel of* $\phi_{\mathbf{K}/\mathbf{k}}$*.*

PROOF. We proceed by induction on the number of (not distinct) prime divisors of $[\mathbf{I_k} : H] = n$. Choose a subgroup H_1 so that $H \subset H_1 \subset \mathbf{I_k}$ and $[\mathbf{I_k} : H_1] = p$ where p is prime. By lemma 12.4, there exists an abelian extension $\mathbf{Z}/\mathbf{k}$ such that $\ker(\phi_{\mathbf{Z}/\mathbf{k}}) = H_1$. Let H' be the inverse image of H under the homomorphism $\mathbf{N}_{\mathbf{Z}/\mathbf{k}} : \mathbf{I_Z} \to \mathbf{I_k}$. We have

$$\frac{\mathbf{I_Z}}{H'} \simeq \frac{H\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I_Z}}{H} \subset \frac{H_1 H}{H} = \frac{H_1}{H}.$$

Therefore $[\mathbf{I_Z} : H']$ divides n/p and so has fewer prime divisors than n. By induction there exists an abelian extension $\mathbf{T}/\mathbf{Z}$ such that $\ker(\phi_{\mathbf{T}/\mathbf{Z}}) = H'$. By lemma 12.2, there exists an abelian extension $\mathbf{K}/\mathbf{k}$ such that $\phi_{\mathbf{K}/\mathbf{k}} = H$.

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

PROOF. Proposition 12.5 shows that $\mathbf{K}$ exists, and proposition 2.15 shows that $\mathbf{K}$ is uniquely determined by H.

Existence theorem for local fields. In this section, p denotes a prime of $\mathbf{k}$ and $\wp$ denotes a prime of $\mathbf{K}$. Primes of other extensions of $\mathbf{k}_p$ may be denoted by $\wp'$, or by q, q', *etc.* The norm residue symbol will be denoted by $(\alpha, \mathbf{K}_\wp/\mathbf{k}_p)$. The lemmas and proofs for local fields are essentially line-for-line translations of their counterparts for global fields.

LEMMA 12.6. *If $\mathbf{K}_\wp$ and $\mathbf{L}_{\wp'}$ are abelian extensions of $\mathbf{k}_p$, then $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = \mathbf{N}_{\mathbf{L}_{\wp'}/\mathbf{k}_p}\mathbf{L}_{\wp'}^*$ if and only if $\mathbf{K}_\wp = \mathbf{L}_{\wp'}$.*

PROOF. By proposition 2.11, the natural homomorphism

$$G(\mathbf{K}_\wp\mathbf{L}_{\wp'} : \mathbf{k}_p) \to G(\mathbf{K}_\wp : \mathbf{k}_p) \times G(\mathbf{L}_{\wp'} : \mathbf{k}_p)$$

is an injection and the image of $(\alpha, \mathbf{K}_\wp\mathbf{L}_{\wp'}/\mathbf{k}_p)$ is $\big((\alpha, \mathbf{K}_\wp/\mathbf{k}_p), (\alpha, \mathbf{L}_{\wp'}/\mathbf{k}_p)\big)$. If α is in $\mathbf{N}_{\mathbf{K}_\wp\mathbf{L}_{\wp'}/\mathbf{k}_p}(\mathbf{K}_\wp\mathbf{L}_{\wp'})^*$ then $(\alpha, \mathbf{K}_\wp\mathbf{L}_{\wp'}/\mathbf{k}_p) = 1$, so $(\alpha, \mathbf{K}_\wp/\mathbf{k}_p) = 1$ and $(\alpha, \mathbf{L}_{\wp'}/\mathbf{k}_p) = 1$, and therefore α is in $\mathbf{N}_{\mathbf{K}_\wp}\mathbf{K}_\wp^*$ and in $\mathbf{N}_{\mathbf{L}_{\wp'}}\mathbf{L}_{\wp'}^*$. Suppose that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = \mathbf{N}_{\mathbf{L}_{\wp'}/\mathbf{k}_p}\mathbf{L}_{\wp'}^*$. If α is in $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$, then both symbols $(\alpha, \mathbf{K}_\wp/\mathbf{k}_p)$ and $(\alpha, \mathbf{L}_{\wp'}/\mathbf{k}_p)$ are trivial, so $(\alpha, \mathbf{K}_\wp\mathbf{L}_{\wp'}/\mathbf{k}_p)$ is trivial, so α is in $\mathbf{N}_{\mathbf{K}_\wp\mathbf{L}_{\wp'}}(\mathbf{K}_\wp\mathbf{L}_{\wp'})^*$, and therefore $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = \mathbf{N}_{\mathbf{K}_\wp\mathbf{L}_{\wp'}}(\mathbf{K}_\wp\mathbf{L}_{\wp'})^* = \mathbf{N}_{\mathbf{L}_{\wp'}/\mathbf{k}_p}\mathbf{L}_{\wp'}^*$. This implies that $[\mathbf{K}_\wp : \mathbf{k}_p] = [\mathbf{K}_\wp\mathbf{L}_{\wp'} : \mathbf{k}_p] = [\mathbf{L}_{\wp'} : \mathbf{k}_p]$, so $\mathbf{K}_\wp = \mathbf{K}_\wp\mathbf{L}_{\wp'} = \mathbf{L}_{\wp'}$.

LEMMA 12.7. *If n is prime and $\mathbf{k}_p$ contains the n-th roots of unity, then there exists an abelian extension $\mathbf{K}_\wp/\mathbf{k}_p$ such that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = (\mathbf{k}_p^*)^n$.*

PROOF. By proposition 8.12, if p does not divide n, then $[\mathbf{k}_p^* : (\mathbf{k}_p^*)^n] = n^2$. If p divides n, then $[\mathbf{k}_p^* : (\mathbf{k}_p^*)^n] = n^2(\mathrm{N}p)^a$ where $n\mathbf{o}_p = p^a$, and since n is prime then $\mathrm{N}p = n^f$ so $n^2(\mathrm{N}p)^a = n^{2+af}$. Put $m = 2$ in the former case and $m = 2 + af$ in the latter. Then $\mathbf{k}_p^*/\left(\mathbf{k}_p^*\right)^n$ must be the product of m cyclic groups order n, so let $\beta_1, \ldots, \beta_m$ generate $\mathbf{k}_p^*$ modulo $(\mathbf{k}_p^*)^n$. By lemma 8.5 (which applies to any field containing the n-th roots of units), $\mathbf{K}_\wp = \mathbf{k}_p\left(\sqrt[n]{\beta_1}, \ldots, \sqrt[n]{\beta_m}\right)$ has degree n^m over $\mathbf{k}_p$ with Galois group isomorphic to the product of m cyclic groups order n. Therefore $\mathbf{k}_p^*/\left(\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*\right)$ is also isomorphic to the product of m cyclic groups of order n, so $(\mathbf{k}_p^*)^n$ is contained in $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$ Both of these subgroups have index n^m in $\mathbf{k}_p^*$, so they must coincide. This completes the proof.

LEMMA 12.8. *Let H be a closed subgroup of finite index in $\mathbf{k}_p^*$. If there exists an abelian extension $\mathbf{L}_{\wp'}/\mathbf{k}_p$ such that $\mathbf{N}_{\mathbf{L}_{\wp'}/\mathbf{k}_p}\mathbf{L}_{\wp'}^* \subset H$, then there exists an abelian extension $\mathbf{K}_\wp/\mathbf{k}_p$ such that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$.*

PROOF. Let $\mathbf{K}_\wp$ be the fixed field of the image of H under the mapping $\alpha \to (\alpha, \mathbf{L}_{\wp'}/\mathbf{k}_p)$. Since $(\alpha, \mathbf{K}_\wp/\mathbf{k}_p)$ coincides with the restriction to $\mathbf{K}_\wp$ of $(\alpha, \mathbf{L}_{\wp'}/\mathbf{k}_p)$ then $(\alpha, \mathbf{K}_\wp/\mathbf{k}_p)$ is trivial if and only if α is in H. Therefore H is the kernel of $(\alpha, \mathbf{K}_\wp/\mathbf{k}_p)$, so $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$.

LEMMA 12.9. *Let H be a closed subgroup of finite index in $\mathbf{k}_p^*$, and let $\mathbf{Z}_{\wp'}/\mathbf{k}_p$ be a cyclic extension. Let H' be the inverse image of H under the homomorphism $\mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p} : \mathbf{Z}_{\wp'}^* \to \mathbf{k}_p^*$. Then H' is a closed subgroup of finite index in $\mathbf{Z}_{\wp'}^*$. If there* *exists an abelian extension* $\mathbf{T}_q$ *of* $\mathbf{Z}_{\wp'}$ *such that* $\mathbf{N}_{\mathbf{T}_q/\mathbf{Z}_{\wp'}}\mathbf{T}_q^* = H'$, *then there exists an abelian extension* $\mathbf{K}_\wp$ *of* $\mathbf{k}_p$ *such that* $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$.

Proof. H' is closed because $\mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}$ is continuous, so we need to show that $[\mathbf{Z}_{\wp'}^* : H']$ is finite. Since $H' = \mathbf{N}^{-1}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}H$ then $\mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}H' = H \cap \mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}\mathbf{Z}_{\wp'}^*$, so

$$\frac{\mathbf{Z}_{\wp'}^*}{H'} \simeq \frac{\mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}\mathbf{Z}_{\wp'}^*}{H \cap \mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}\mathbf{Z}_{\wp'}^*} \simeq \frac{H\mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}\mathbf{Z}_{\wp'}^*}{H} \subset \frac{\mathbf{k}_p^*}{H}.$$

Therefore $[\mathbf{Z}_{\wp'}^* : H']$ is finite. By the hypothesis, there exists an abelian extension $\mathbf{T}_q$ of $\mathbf{Z}$ so that $\mathbf{N}_{\mathbf{T}_q/\mathbf{Z}_{\wp'}}\mathbf{T}_q^* = H'$. We want to show that $\mathbf{T}_q/\mathbf{k}_p$ is abelian. First, we show that $\mathbf{T}_q/\mathbf{k}_p$ is normal. Let σ be a generator of $G(\mathbf{Z}_{\wp'} : \mathbf{k}_p)$. The automorphism σ can be extended to an isomorphism (also denoted σ) of $\mathbf{T}_q$ to a conjugate field $\mathbf{T}'_{q'}$. By lemma 10.42, for α in $\mathbf{Z}_{\wp'}$ we have

$$(\alpha, \mathbf{T}'_{q'}/\mathbf{Z}_{\wp'}) = \sigma\big(\sigma^{-1}(\alpha), \mathbf{T}_q/\mathbf{Z}_{\wp'}\big)\sigma^{-1}.$$

We have $\mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}\sigma^{-1}(\alpha) = \mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}\alpha$, so $\mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}\big(\alpha^{-1}\sigma^{-1}(\alpha)\big) = 1$, so $\alpha^{-1}\sigma^{-1}(\alpha)$ is in H'. Therefore $\sigma^{-1}(\alpha)$ is in H' if and only if α is in H'. This shows that $(\alpha, \mathbf{T}'_{q'}/\mathbf{Z}_{\wp'}) = 1$ if and only if α is in H', so $\mathbf{N}_{\mathbf{T}_{q'}/\mathbf{Z}_{\wp'}}\mathbf{T}_{q'} = H'$ and therefore $\mathbf{T}'_{q'} = \mathbf{T}_q$. Since $\sigma(\mathbf{T}_q) = \mathbf{T}_q$ and σ generates $G(\mathbf{Z}_{\wp'} : \mathbf{k}_p)$, then $\mathbf{T}_q$ is invariant under every extension of every automorphism in $G(\mathbf{Z}_{\wp'} : \mathbf{k}_p)$. This shows that $\mathbf{T}_q$ is normal over $\mathbf{k}_p$.

To show that $\mathbf{T}_q/\mathbf{k}_p$ is abelian, we have $\big(\alpha^{-1}\sigma(\alpha), \mathbf{T}_q/\mathbf{Z}_{\wp'}\big) = 1$, since $\alpha^{-1}\sigma(\alpha)$ is in H'. Then $\big(\sigma(\alpha), \mathbf{T}_q/\mathbf{Z}_{\wp'}\big) = \big(\alpha, \mathbf{T}_q/\mathbf{Z}_{\wp'}\big)$, so $\big(\alpha, \mathbf{T}_q/\mathbf{Z}_{\wp'}\big) = \sigma\big(\alpha, \mathbf{T}_q/\mathbf{Z}_{\wp'}\big)\sigma^{-1}$. Since the norm residue symbol maps $\mathbf{Z}_{\wp'}^*$ onto $G(\mathbf{T}_q : \mathbf{Z}_{\wp'})$ then σ commutes with every automorphism in $G(\mathbf{T}_q : \mathbf{Z}_{\wp'})$. Every element of $G(\mathbf{T}_q : \mathbf{k}_p)$ is of the form $\sigma^a\tau$ with τ in $G(\mathbf{T}_q : \mathbf{Z}_{\wp'})$, so $G(\mathbf{T}_q : \mathbf{k}_p)$ is abelian.

We now know that the norm residue symbol is defined for $\mathbf{T}_q/\mathbf{k}_p$ is defined, and the kernel is $\mathbf{N}_{\mathbf{T}_q/\mathbf{k}_p}\mathbf{T}_q^*$. Then

$$\mathbf{N}_{\mathbf{T}_q/\mathbf{k}_p}\mathbf{T}_q^* = \mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}(\mathbf{N}_{\mathbf{T}_q/\mathbf{Z}_{\wp'}}\mathbf{T}_q^*) = \mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}(H') \subset H.$$

Since $\mathbf{N}_{\mathbf{T}_q/\mathbf{k}_p}\mathbf{T}_q^*$ is contained in H, then by lemma 12.8 there exists an abelian extension $\mathbf{K}_\wp/\mathbf{k}_p$ such that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$. This completes the proof.

Lemma 12.10. *Suppose that* n *is a prime number,* $\mathbf{k}_p$ *contains the* n*-th roots of unity,* H *is a closed subgroup of finite index in* $\mathbf{k}_p^*$ *and* $[\mathbf{k}_p^* : H] = n$. *Then there exists an abelian extension* $\mathbf{K}_\wp/\mathbf{k}_p$ *such that* $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$.

Proof. By lemma 12.7, there exists an abelian extension corresponding to the subgroup $(\mathbf{k}_p^*)^n$. Since $[\mathbf{k}_p^* : H] = n$ then $(\mathbf{k}_p^*)^n \subset H$. By lemma 12.8, there exists an abelian extension $\mathbf{K}_\wp/\mathbf{k}_p$ such that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$.

LEMMA 12.11. *Suppose that n is a prime number, H is a closed subgroup of finite index in $\mathbf{k}_p^*$ and $[\mathbf{k}_p^* : H] = n$. Then there exists an abelian extension $\mathbf{K}_\wp/\mathbf{k}_p$ such that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$.*

PROOF. Let $\mathbf{Z}_{\wp'}$ be the field obtained by adjoining the n-th roots of unity to $\mathbf{k}_p$. Then $\mathbf{Z}_{\wp'}/\mathbf{k}_p$ is a cyclic extension since $G(\mathbf{Z}_{\wp'} : \mathbf{k}_p) \subset G(\mathbf{Z} : \mathbf{k})$. Define H' to be the inverse image of H as in the hypothesis of lemma 12.9. As in the proof of lemma 12.9, we have that $[\mathbf{Z}_{\wp'} : \mathbf{k}_p]$ is a divisor of $[\mathbf{k}_p^* : H]$. Since n is prime, then $[\mathbf{Z}_{\wp'} : \mathbf{k}_p]$ is 1 or n. In the former case, take $\mathbf{T}_q = \mathbf{Z}_{\wp'}$. In the latter case, we apply lemma 12.10 to $\mathbf{Z}_{\wp'}$ and H'. There exists an abelian extension $\mathbf{T}_q/\mathbf{Z}_{\wp'}$ such that $\mathbf{N}_{\mathbf{T}_q/\mathbf{Z}_{\wp'}}\mathbf{T}_q^* = H'$. By lemma 12.8, there exists an abelian extension $\mathbf{K}_\wp/\mathbf{k}_p$ such that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$.

PROPOSITION 12.12. *If H is a closed subgroup of finite index in $\mathbf{k}_p^*$, then there is an abelian extension $\mathbf{K}_\wp$ of $\mathbf{k}_p$ such that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$.*

PROOF. We proceed by induction on the number of (not distinct) prime divisors of $[\mathbf{k}_p^* : H] = m$. Choose a subgroup H_1 so that $H \subset H_1 \subset \mathbf{k}_p^*$ and $[\mathbf{k}_p^* : H_1] = n$ where n is prime. By lemma 12.4, there exists an abelian extension $\mathbf{Z}_{\wp'}/\mathbf{k}_p$ such that $\mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p}\mathbf{Z}_{\wp'}^* = H_1$. Let H' be the inverse image of H under the homomorphism $\mathbf{N}_{\mathbf{Z}_{\wp'}/\mathbf{k}_p} : \mathbf{Z}_{\wp'}^* \to \mathbf{k}_p^*$. We have

$$\frac{\mathbf{I_Z}}{H'} \simeq \frac{H\mathbf{N}_{\mathbf{Z}/\mathbf{k}}\mathbf{I_Z}}{H} \subset \frac{H_1 H}{H} = \frac{H_1}{H}.$$

Therefore $[\mathbf{I_Z} : H']$ divides m/n and so has fewer prime divisors than m. By induction there exists an abelian extension $\mathbf{T}_q/\mathbf{Z}_{\wp'}$ such that $\mathbf{N}_{\mathbf{T}_q/\mathbf{Z}_{\wp'}}\mathbf{Z}_{\wp'}^* = H'$. By lemma 12.9, there exists an abelian extension $\mathbf{K}_\wp/\mathbf{k}_p$ such that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$.

PROPOSITION 12.13 - EXISTENCE THEOREM FOR LOCAL FIELDS. *The abelian extension $\mathbf{K}_\wp$ of $\mathbf{k}_p$ is uniquely determined by the kernel of $(\alpha, \mathbf{K}_\wp/\mathbf{k}_p)$. If H is a closed subgroup of finite index in $\mathbf{k}_p^*$, then there is a unique abelian extension $\mathbf{K}_\wp$ of $\mathbf{k}_p$ such that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^* = H$*

PROOF. Lemma 12.13 shows that $\mathbf{K}_\wp$ exists, and lemma 12.6 shows that $\mathbf{K}_\wp$ is uniquely determined by H.