CHAPTER IV

THEOREM 1: PROOF FOR CYCLIC EXTENSIONS

Non-degeneracy of the trace in separable extensions. In this section, $\mathbf{k}$ may be either a finite field or an algebraic number field. (The result for finite fields is needed in the proof of proposition 4.7.) $\mathbf{S}_{\mathbf{K}/\mathbf{k}}(xy)$ is a $\mathbf{k}$-bilinear form of $\mathbf{K}$ represented by matrix $\mathbf{S}_{ij} = \mathbf{S}_{\mathbf{K}/\mathbf{k}}(\alpha_i\alpha_j)$ with respect to basis $\alpha_1, \dots, \alpha_n$ of $\mathbf{K}$ over $\mathbf{k}$. If $x = a_1\alpha_1 + \cdots + a_n\alpha_n$ and $y = b_1\alpha_1 + \cdots + b_n\alpha_n$, then

$$\begin{aligned}\mathbf{S}_{\mathbf{K}/\mathbf{k}}(xy) &= \mathbf{S}_{\mathbf{K}/\mathbf{k}}(\sum_{i=1}^{n}\sum_{j=1}^{n} a_i\alpha_i\alpha_j b_j) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i \mathbf{S}_{\mathbf{K}/\mathbf{k}}(\alpha_i\alpha_j) b_j = \sum_{i=1}^{n}\sum_{j=1}^{n} a_i \mathbf{S}_{ij} b_j = (\mathbf{X}^t)\mathbf{S}\mathbf{Y}.\end{aligned}$$

LEMMA 4.1. *If $\mathbf{K}/\mathbf{k}$ is a finite normal separable extension with Galois group $G = G(\mathbf{K} : \mathbf{k})$ then*

$$\mathbf{N}_{\mathbf{K}/\mathbf{k}}\alpha = \prod_{\sigma\in G} \alpha^\sigma \quad \textit{and} \quad \mathbf{S}_{\mathbf{K}/\mathbf{k}}\alpha = \sum_{\sigma\in G} \alpha^\sigma.$$

PROOF. Let $[\mathbf{k}(\alpha) : \mathbf{k}] = n$ and $[\mathbf{K} : \mathbf{k}(\alpha)] = m$. Let G be the Galois group of $\mathbf{K}$ over $\mathbf{k}$ and H be the subgroup of G that fixes $\mathbf{k}(\alpha)$. Let $\{\rho_1, \dots, \rho_n\}$ be a set of representatives for the distinct right cosets of H in G. The minimum polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ of α over $\mathbf{k}$ has factorization $(x - \alpha^{\rho_1})\dots(x - \alpha^{\rho_n})$, so $a_1 = -\sum_{k=1}^{n} \alpha^{\rho_k}$ and $a_n = (-1)^n \prod_{k=1}^{n} \alpha^{\rho_k}$. The matrix representing T_α as a linear transformation of $\mathbf{k}(\alpha)$ with respect to basis $1, \alpha, \dots, \alpha^{n-1}$ is

$$\mathbf{T} = \begin{pmatrix} 0 & 0 & \dots & 0 & -a^n \\ 1 & 0 & \dots & 0 & -a_{n-1} \\ 0 & 1 & \dots & 0 & -a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_1 \end{pmatrix}$$

Then $\mathbf{N}_{\mathbf{k}(\alpha)/\mathbf{k}}\alpha = \det(\mathbf{T}) = (-1)^{n+1}(-a_n) = \prod_{k=1}^{n} \alpha^{\rho_k}$ and $\mathbf{S}_{\mathbf{k}(\alpha)/\mathbf{k}}\alpha = \mathrm{trace}(\mathbf{T}) = -a_1 = \sum_{k=1}^{n} \alpha^{\rho_k}$. We have

$$\mathbf{N}_{\mathbf{K}/\mathbf{k}}\alpha = \mathbf{N}_{\mathbf{k}(\alpha)/\mathbf{k}}\mathbf{N}_{\mathbf{K}/\mathbf{k}(\alpha)}\alpha = \mathbf{N}_{\mathbf{k}(\alpha)/\mathbf{k}}\alpha^m,$$
$$\mathbf{S}_{\mathbf{K}/\mathbf{k}}\alpha = \mathbf{S}_{\mathbf{k}(\alpha)/\mathbf{k}}\mathbf{S}_{\mathbf{K}/\mathbf{k}(\alpha)}\alpha = m\mathbf{S}_{\mathbf{k}(\alpha)/\mathbf{k}}\alpha.$$

Let $H = \{\tau_1, \ldots, \tau^m\}$. Then the nm products $\tau_j\rho_k$ run over G. We have

$$\prod_{\sigma\in G} \alpha^{\sigma} = \prod_{j=1}^{m}\prod_{k=1}^{n} \alpha^{\tau_j\rho_k} = \left(\prod_{k=1}^{n} \alpha^{\rho_k}\right)^m = \mathbf{N}_{\mathbf{K}/\mathbf{k}}\alpha$$
$$\sum_{\sigma\in G} \alpha^{\sigma} = \sum_{j=1}^{m}\sum_{k=1}^{n} \alpha^{\tau_j\rho_k} = m\sum_{k=1}^{n} \alpha^{\rho_k} = \mathbf{S}_{\mathbf{K}/\mathbf{k}}\alpha.$$

Lemma 4.2. *If $\mathbf{K}/\mathbf{k}$ is a finite normal separable extension then matrix $\mathbf{S}$ is non-singular.*

Proof. Let $\{\sigma_1, \ldots, \sigma_n\}$ be the automorphisms in Galois group $G(\mathbf{K} : \mathbf{k})$. By lemma 4.1, $\mathbf{S}_{ij} = \sum_{k=1}^{n} \alpha_i^{\sigma_k}\alpha_j^{\sigma_k}$, so $\mathbf{S}_{ij} = \mathbf{A}\mathbf{A}^t$ where $\mathbf{A}_{ik} = \alpha_i^{\sigma_k}$. With respect to a simple basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, $\mathbf{A}$ has the form $\mathbf{A}_{ik} = (\alpha^{\sigma_k})^{i-1}$, which is a Vandermonde matrix $V(\alpha^{\sigma_1}, \ldots, \alpha^{\sigma_n})$. There are n distinct conjugates of generator α, so $\mathbf{A}$ is non-singular and so is $\mathbf{S}$.

Lemma 4.3. *Let $\mathbf{K}$ be a finite normal extension $\mathbf{k}$. Matrix $(\mathbf{S}_{ij})$ is non-singular if and only if for every non-zero element y of $\mathbf{K}$ there exists an element x of $\mathbf{K}$ so that $\mathbf{S}_{\mathbf{K}/\mathbf{k}}(xy) \neq 0$.*

Proof. $\mathbf{S}_{\mathbf{K}/\mathbf{k}}(xy) = (\mathbf{X}^t)\mathbf{S}\mathbf{Y}$. Suppose $\mathbf{S}$ non-singular. If $y \neq 0$ then $\mathbf{S}\mathbf{Y} \neq 0$, so there is a vector $\mathbf{X}$ so that $(\mathbf{X}^t)\mathbf{S}\mathbf{Y} \neq 0$. conversely, if $\mathbf{S}$ is singular then $\mathbf{S}\mathbf{Y} = 0$ for some non-zero y, and $\mathbf{S}_{\mathbf{K}/\mathbf{k}}(xy) = 0$ for every x in $\mathbf{K}$.

Proposition 4.4. *Let $\mathbf{L}$ be a finite separable (not necessarily normal) extension of $\mathbf{k}$. Then the trace $\mathbf{S}_{\mathbf{L}/\mathbf{k}}(xy)$ is non-degenerate: for every non-zero y in $\mathbf{L}$ there is an x in $\mathbf{L}$ so that $\mathbf{S}_{\mathbf{L}/\mathbf{k}}(xy) \neq 0$.*

Proof. Let y be a non-zero element of $\mathbf{L}$. Then $\mathbf{L}$ is contained in a finite normal extension $\mathbf{K}$, and

$$\mathbf{S}_{\mathbf{K}/\mathbf{k}}(xy) = \mathbf{S}_{\mathbf{L}/\mathbf{k}}\big(\mathbf{S}_{\mathbf{K}/\mathbf{L}}(xy)\big) = \mathbf{S}_{\mathbf{L}/\mathbf{k}}\big(\mathbf{S}_{\mathbf{K}/\mathbf{L}}(x)y\big).$$

Choose x in $\mathbf{K}$ so that $\mathbf{S}_{\mathbf{K}/\mathbf{k}}(xy) \neq 0$. Then $\mathbf{S}_{\mathbf{K}/\mathbf{L}}(x)$ is the desired element of $\mathbf{L}$.

Remark. In lemma 4.5, let the images modulo $\wp$ and p of elements β in $\mathbf{O}_\wp$ and b in $\mathbf{o}_p$ be denoted by $\overline{\beta}$ and $\overline{b}$, respectively.

LEMMA 4.5. *Suppose that p-adic extension $\mathbf{K}_\wp/\mathbf{k}_p$ is not ramified. Let $F(q)$ denote finite field $\mathbf{o}_p/p$ where $q = Np$; let $F(q^f)$ denote finite field $\mathbf{O}_\wp/\wp$ where $q^f = N\wp$. Then*

$$\overline{\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha} = \mathbf{N}_{F(q^f)/F(q)}\overline{\alpha} \quad \textit{and} \quad \overline{\mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha} = \mathbf{S}_{F(q^f)/F(q)}\overline{\alpha}.$$

PROOF. Choose $w_1, \dots, w_f$ in $\mathbf{O}_\wp$ so that $\overline{w_1}, \dots, \overline{w_f}$ is a basis for $F(q^f)$ over $F(q)$. Let $p = (\pi)$ for $\pi \in \mathbf{o}_p$. Suppose $a_1w_1 + \cdots + a_nw_n = 0$ with $a_i \in \mathbf{k}_p$. After multiplying by a power of π, we may take the coefficients a_i in $\mathbf{o}_p$. Then each coefficient a_i is 0 modulo p, so $a_i = \pi a_i'$ with a_i' in $\mathbf{o}_p$. Dividing by π, we have $a_1'w_1 + \cdots + a_n'w_n = 0$. In this fashion we can show that each a_i is divisible by an arbitrarily large power of π, so each $a_i = 0$ and $w_1, \dots, w_f$ must be linearly independent over $\mathbf{k}_p$. We have $[\mathbf{K}_\wp/\mathbf{k}_p] = f$, so $w_1, \dots, w_f$ is a basis of $\mathbf{K}_\wp$ over $\mathbf{k}_p$. With respect basis $w_1, \dots, w_f$, let the matrix representing T_α be $(\, a_{ij}\,)$. With respect to basis $\overline{w_1}, \dots, \overline{w_f}$, the matrix representing $T_{\overline{\alpha}}$ as a linear transformation of $\mathbf{O}\wp/\wp$ over $\mathbf{o}_p/p$ will be $(\, \overline{a_{ij}}\,)$. We have $\overline{\det(\, a_{ij}\,)} = \det(\, \overline{a_{ij}}\,)$ and $\overline{\operatorname{trace}(\, a_{ij}\,)} = \operatorname{trace}(\, \overline{a_{ij}}\,)$, which proves the lemma.

Every unit is a norm in unramified p-adic extensions. If $\mathbf{K}/\mathbf{k}$ is a finite extension of algebraic numbers then $\mathbf{O}_\wp/\wp$ is a finite field containing $\mathrm{N}\wp$ elements; $\mathbf{o}_p/p$ is finite field containing $\mathrm{N}p$ elements. Let these finite fields be denoted by $F(q^f)$ and $F(q)$, where $q = \mathrm{N}p$ and $q^f = \mathrm{N}\wp$.

LEMMA 4.6. *Every element in $F(q)$ is the norm of an element in $F(q^f)$.*

PROOF. The Galois group of $F(q^f)$ over $F(q)$ is generated by σ where $\alpha^\sigma = \alpha^q$. Then

$$\mathbf{N}_{F(q^f)/F(q)}(\alpha) = \alpha\alpha^q \dots \alpha^{q^{n-1}} = \alpha^{1+q+\cdots+q^{n-1}} = \alpha^{\left(\frac{q^n-1}{q-1}\right)}.$$

$\mathbf{N}_{F(q^f)/F(q)}(0) = 0$, so we have to show that the $q-1$ non-zero elements of $F(q)$ are norms. Take α to be a generator of $F(q^f)^*$. Then

$$\mathbf{N}_{F(q^f)/F(q)}(\alpha^u) = \alpha^{u\left(\frac{q^{n-1}}{q-1}\right)}.$$

For $u = 0, 1, \dots, q-2$ we have $0 \le u(q^n-1)/(q-1) < q^n - 1$. Since α has order $q^n - 1$, there are $q-1$ distinct values of $\mathbf{N}_{F(q^f)/F(q)}(\alpha^u)$.

PROPOSITION 4.7. *If $\mathbf{K}_\wp$ is an finite unramified extension of p-adic field $\mathbf{k}_p$, then every unit in $\mathbf{k}_p$ is the norm of an element in $\mathbf{K}_\wp$.*

PROOF. Let β be a unit in $\mathbf{k}_p$. By lemma 4.6, there is an α_1 in $\mathbf{K}_\wp$ so that $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha_1 = \beta (\mathrm{mod}\ p)$. Suppose that we have already found α_n in $\mathbf{K}_\wp$ so that

$\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha_n = \beta(\text{mod } p^n)$. Let $p = (\pi)$. The extension $\mathbf{K}_\wp/\mathbf{k}_p$ is not ramified, so $p\mathbf{O}_\wp = \wp$, and $\wp^n = \pi^n\mathbf{O}_\wp$ for $n \geq 0$. Then $\left(\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha_n\right)^{-1}\beta = 1+\delta\pi^n(\text{mod } p^{n+1})$. Put $\alpha_{n+1} = \alpha_n(1 + x\pi^n)$. The condition $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha_{n+1} = \beta(\text{mod } p^{n+1})$ will be satisfied if we can find x in $\mathbf{K}_\wp$ so that

$$\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}(1 + x\pi^n) = 1 + \delta\pi^n(\text{mod } p^{n+1}). \tag{4.1}$$

Let (x_{ij}) be the matrix representing T_x in $\mathbf{K}_\wp$ over $\mathbf{k}_p$ with respect to some basis. then the matrix representing $T_{1+x\pi^n}$ is

$$\begin{pmatrix} 1 + x_{11}\pi^n & x_{12}\pi^n & \dots & x_{1f}\pi^n \\ x_{21}\pi^n & 1 + x_{22}\pi^n & \dots & x_{2f}\pi^n \\ \vdots & \vdots & \ddots & \vdots \\ x_{f1}\pi^n & x_{f2}\pi^n & \dots & 1 + x_{ff}\pi^n \end{pmatrix}.$$

We therefore have

$$\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}(1 + x\pi^n) = 1 + (x_{11} + \dots + x_{ff})\pi^n = 1 + \pi^n\mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p}x(\text{mod } p^{n+1}).$$

Condition (4.1) is therefore

$$1 + \pi^n\mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p}x = 1 + \delta\pi^n(\text{mod } p^{n+1}),$$

or

$$\mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p}x = \delta(\text{mod } p).$$

By lemma 4.3, the trace $\mathbf{S} : \mathbf{O}_\wp/\wp \to \mathbf{o}_p/p$ is non-degenerate; there exists an element $\gamma \in \mathbf{O}_\wp$ so that $\mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p}\gamma = \epsilon \neq 0(\text{mod } p)$. Then $\mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p}\gamma\epsilon^{-1} = 1(\text{mod } p)$, and $\mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p}\gamma\epsilon^{-1}\delta = \delta(\text{mod } p)$. Therefore $\alpha_{n+1} = \alpha_n(1 + \gamma\epsilon^{-1}\delta\pi^n)$ satisfies (4.1). The sequence $\{\alpha_n\}$ converges to a limit α in $\mathbf{K}_\wp$ satisfying $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha = \beta$.

Exponential and logarithm functions. In the following discussion of exponential and logarithm functions, let $\wp$ denote a prime of $\mathbf{k}$ and $(p) = \wp \cap \mathbf{Z}$ the rational prime that $\wp$ divides, with $p > 0$.

LEMMA 4.8. *Let $\wp$ be a finite prime of $\mathbf{k}$. The series*

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \dots + \frac{x^k}{k!} + \dots \tag{4.2}$$

converges for x in $\mathbf{k}_\wp$ if $\operatorname{ord}_\wp(x) > \frac{b}{p-1}$ where $b = \operatorname{ord}_\wp(p)$.

PROOF. The series converges if and only if $\lim_{k\to\infty}\left|x^k/k!\right|_\wp = 0$. The exact power to which rational prime p divides $k!$ is

$$\operatorname{ord}_p(k!) = \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \left[\frac{k}{p^3}\right] + \dots.$$

Let $k = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$ where $0 \le a_i < p$. Then

$$\begin{array}{lcccccccc} \left[\frac{k}{p}\right] & = & a_1 & + & a_2 p & + & \dots & + & a_r p^{r-1} \\ \left[\frac{k}{p^2}\right] & = & & & a_2 & + & \dots & + & a_r p^{r-2} \\ \vdots & & & & & & & & \end{array}$$

Summing each column, we have

$$\mathrm{ord}_p(k!) = a_0 \frac{p^0 - 1}{p-1} + a_1 \frac{p^1 - 1}{p-1} + a_2 \frac{p^2-1}{p-1} + \cdots + a_r \frac{p^r - 1}{p-1},$$

or

$$\mathrm{ord}_p(k!) = \frac{k - (a_0 + a_1 + \cdots + a_r)}{p-1} \le \frac{k-1}{p-1}.$$

Since $b = \mathrm{ord}_\wp(p)$, we have

$$\mathrm{ord}_\wp(k!) = b\left(\frac{k - (a_0 + a_1 + \cdots + a_r)}{p-1}\right) \le b\left(\frac{k-1}{p-1}\right). \tag{4.3}$$

Then

$$\begin{aligned} \mathrm{ord}_\wp(x^k/k!) &= k\,\mathrm{ord}_\wp(x) - \mathrm{ord}_\wp(k!) \\ &\ge k\,\mathrm{ord}_\wp(x) - b\left(\frac{k-1}{p-1}\right) = k\left(\mathrm{ord}_\wp(x) - \frac{b}{p-1}\right) + \frac{b}{p-1}, \end{aligned}$$

so $\mathrm{ord}_\wp(x^k/k!) \to \infty$ if $\mathrm{ord}_\wp(x) - b/(p-1) > 0$.

Lemma 4.9. *If* $\mathrm{ord}_\wp(x) > \frac{b}{p-1}$ *then* $\mathrm{ord}_\wp\big(\exp(x) - 1\big) = \mathrm{ord}_\wp(x)$.

Proof. We have

$$\exp(x) - 1 = x + \frac{x^2}{2!} + \cdots + \frac{x^k}{k!} + \dots.$$

We need to show $|x^k/k!|_\wp < |x|_\wp$, or $|x^{k-1}/k!|_\wp < 1$ for $k \ge 2$. We have $\mathrm{ord}_\wp(k!) \le b\left(\frac{k-1}{p-1}\right)$, so if $\mathrm{ord}_\wp(x) > \frac{b}{p-1}$ and $k \ge 2$ then

$$\mathrm{ord}_\wp\left(\frac{x^{k-1}}{k!}\right) = (k-1)\mathrm{ord}_\wp(x) - \mathrm{ord}_\wp(k!) > (k-1)\frac{b}{p-1} - b\frac{k-1}{p-1} = 0.$$

LEMMA 4.10. *Let $\wp$ be a finite prime of* $\mathbf{k}$. *The infinite series*

$$\log(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - \cdots - \frac{x^k}{k} - \ldots$$

converges for x in $\mathbf{k}_\wp$ if $|x|_\wp < 1$.

PROOF. If $\operatorname{ord}_\wp(x) > 0$ we show that $\left|x^k/k\right|_\wp \to 0$, or $k\operatorname{ord}_\wp(x) - \operatorname{ord}_\wp(k) \to \infty$. Let $k = up^v$ where $(u,p) = 1$. Then $k = p^{\log_p(k)}$, so $\operatorname{ord}_\wp(k) = bv \le b\log_p(k)$. If $\operatorname{ord}(x) > 0$ then for large k we have $\frac{\log_p(k)}{k} < \frac{1}{2b}\operatorname{ord}_\wp(x)$, and

$$\begin{aligned} k\operatorname{ord}_\wp(x) - \operatorname{ord}_\wp(k) &= k\left(\operatorname{ord}_\wp(x) - \frac{\operatorname{ord}_\wp(k)}{k}\right) \\ &\ge k\left(\operatorname{ord}_\wp(x) - \frac{b\log_p(k)}{k}\right) > \frac{k}{2}\operatorname{ord}_\wp(x) \to \infty. \end{aligned}$$

LEMMA 4.11. *If $\operatorname{ord}_\wp(x) > \frac{b}{p-1}$ then $\operatorname{ord}_\wp\big(\log(1-x)\big) = \operatorname{ord}_\wp(x)$.*

PROOF. If $\operatorname{ord}_\wp(x) > \frac{b}{p-1}$, we need to show

$$\left|\frac{x^2}{2} + \frac{x^3}{3} + \cdots + \frac{x^k}{k} + \ldots\right|_\wp < |x|_\wp.$$

It is enough to show $|x^k/k|_\wp < |x|_\wp$, or

$$k\operatorname{ord}_\wp(x) - \operatorname{ord}_\wp(k) > \operatorname{ord}_\wp(x) \qquad \text{for } k \ge 2.$$

Put $k = up^v$, where $(u,p) = 1$. We need $up^v\operatorname{ord}_\wp(x) - bv > \operatorname{ord}_\wp(x)$, or

$$(up^v - 1)\operatorname{ord}_\wp(x) - bv > 0$$

Since $u \ge 1$, we need $(p^v - 1)\operatorname{ord}_\wp(x) - bv > 0$, or

$$\left(\frac{p^v-1}{p-1}\right)\operatorname{ord}_\wp(x) - \frac{bv}{p-1} > 0.$$

If $\operatorname{ord}_\wp(x) > \frac{b}{p-1}$ then we need

$$\left(\frac{p^v-1}{p-1}\right)\left(\frac{b}{p-1}\right) - \frac{bv}{p-1} \ge 0,$$

or

$$\frac{p^v-1}{p-1} - v = (1 + p + \cdots + p^{v-1}) - v \ge 0.$$

The last inequality is certainly valid, since $p \ge 2$ and $v \ge 0$.

LEMMA 4.12. *For s and t in $\mathbf{k}_\wp$, if $\operatorname{ord}_\wp(s) > \frac{b}{p-1}$ and $\operatorname{ord}_\wp(t) > \frac{b}{p-1}$ then*

$$\begin{aligned} \log\big((1-s)(1-t)\big) &= \log(1-s) + \log(1-t) \\ \exp\big(\log(1-s)\big) &= 1-s \\ \exp(s)\exp(t) &= \exp(s+t) \\ \log\big(\exp(s)\big) &= s \end{aligned}$$

PROOF. That each of the above series converges follows from the four previous lemmas.

LEMMA 4.13. *If $n > 0$ and $\operatorname{ord}_\wp(n) = a$, then every element in the set*

$$\left\{ y \in \mathbf{k}_\wp^* \mid \operatorname{ord}_\wp(y-1) > \frac{b}{p-1} + a \right\}$$

is the n-th power of an element in $\left\{ x \in \mathbf{k}_\wp^* \mid \operatorname{ord}_\wp(x-1) > \frac{b}{p-1} \right\}$.

PROOF. If $\operatorname{ord}_\wp(y-1) > b/(p-1) + a$ then $\log\big(1-(y-1)\big) = \log(y)$ is defined, and $\operatorname{ord}_\wp\big(\log(y)\big) = \operatorname{ord}_\wp(y-1)$. Then $\operatorname{ord}_\wp(\log(y)/n) > b/(p-1)$, so $x = \exp\big(\log(y)/n\big)$ and $\exp\big(\log(y)\big)$ are defined. We have

$$x^n = \left(\exp\left(\frac{\log(y)}{n}\right)\right)^n = \exp\big(\log(y)\big) = y,$$

and

$$\operatorname{ord}_\wp(x-1) = \operatorname{ord}_\wp\left(\exp\left(\frac{\log(y)}{n}\right) - 1\right) = \operatorname{ord}_\wp\left(\frac{\log(y)}{n}\right) > \frac{b}{p-1}.$$

REMARK. We revert to the usual notation: p is a prime of $\mathbf{k}$ and $\wp$ a prime of finite extension field $\mathbf{K}$.

LEMMA 4.14. *$\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$ is an open subgroup of $\mathbf{k}_p^*$.*

PROOF. Let $[\mathbf{K}_\wp : \mathbf{k}_p] = n$. If α is in $\mathbf{k}_p^*$ then $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha = \alpha^n$, so Every n-th power of an element in $\mathbf{k}_p^*$ is in $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$. If $\operatorname{ord}_p(n) = a$ then every element in open set $\{\alpha \mid \operatorname{ord}_p(\alpha - 1) > \frac{b}{p-1} + a\}$ is an n-th power by lemma 4.13. Subgroup $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$ contains an open set, so $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$ is open.

PROPOSITION 4.15. *If E is a finite set of primes of $\mathbf{k}$ containing all infinite primes and all primes that are ramified in $\mathbf{K}$, then*

$$\mathbf{I_k}\{E\}\mathbf{k}^*\mathbf{N_{K/k}I_K} = \mathbf{I_k}.$$

PROOF. Given $\mathbf{i}$ in $\mathbf{I_k}$, let F be the set of prime for which $|\mathbf{i}_p|_p \neq 1$. By lemma 2.4, there exists an element α in $\mathbf{k}_p^*$ so that $\alpha^{-1}\mathbf{i}_p$ is arbitrarily close to 1 at primes p in $E \cup F$. In particular, we want $\alpha^{-1}\mathbf{i}_p \in \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\mathbf{K}_\wp^*$ for the finite primes in $E \cup F$ and $\alpha^{-1}\mathbf{i}_p \in \mathbf{R}^+$ for the real infinite primes of $\mathbf{k}$. Define $\mathbf{i}_1$ and $\mathbf{i}_2$ so that

$$\mathbf{i}_1 = \begin{cases} 1 & \text{for } p \notin E \cup F \\ \alpha^{-1}\mathbf{i}_p & \text{for } p \in E \cup F \end{cases} \qquad \mathbf{i}_2 = \begin{cases} \alpha^{-1}\mathbf{i}_p & \text{for } p \notin E \cup F \\ 1 & \text{for } p \in E \cup F \end{cases}.$$

Then $\mathbf{i} = \alpha\mathbf{i}_1\mathbf{i}_2$ where $\alpha \in \mathbf{k}^*$, $\mathbf{i}_1 \in \mathbf{N_{K/k}I_K}$, and $\mathbf{i}_2 \in \mathbf{I_k}\{E \cup F\} \subset \mathbf{I_k}\{E\}$.

Two number-theoretic lemmas. Put $T_r = \big(a^{v^r} - 1\big)/\big(a^{v^{r-1}} - 1\big)$, where $r > 0$, $a > 1$, $v > 1$. We have

$$\begin{aligned} a^{v^r} - 1 &= \left(\left(a^{v^{r-1}} - 1\right) + 1\right)^v - 1 \\ &= \left(a^{v^{r-1}} - 1\right)^v + \cdots + \binom{k}{v}\left(a^{v^{r-1}} - 1\right)^k + \cdots + v\left(a^{v^{r-1}} - 1\right) \end{aligned}$$

$$T_r = \left(a^{v^{r-1}} - 1\right)^{v-1} + v\left(a^{v^{r-1}} - 1\right)^{v-2} + \cdots + v \tag{4.4}$$

LEMMA 4.16. *If $r > 0$, $a > 1$, and v is prime then*
(1) *if q is a prime so that $q|T_r$ and $q|(a^{v^{r-1}} - 1)$ then $q = v$,*
(2) *if $v|T_r$ then $v|(a^{v^{r-1}} - 1)$,*
(3) *if $v > 2$ or $r > 1$ then $T_r \neq 0(\text{mod } v^2)$.*

PROOF. (1) If $q|T_r$ and $q|(a^{v^{r-1}} - 1)$ then by (4.4), q must divided v, so $q = v$. (2) If $v|T_r$ then v divides every term of (4.4) except possibly $(a^{v^{r-1}} - 1)^{v-1}$, so v divides that term too. Therefore v divides $a^{v^{r-1}} - 1$.
(3) Assume $T_r = 0(\text{mod } v^2)$. Then v divides $a^{v^{r-1}} - 1$ by (2). If $v > 2$ then v^2 divides every term of (4.4) except v; then v^2 cannot divide T_r, so $v > 2$ is impossible. If $r > 1$ then (since $v = 2$) we have $T_r = (a^{2^{r-1}} - 1) + 2$. If a is even then T_r is odd (impossible), so a is odd. $a^{2^{r-1}}$ is a square so $a^{2^{r-1}} = 1(\text{mod } 4)$ and $T_r = 2(\text{mod } 4)$ (impossible). It must be that $r = 1$.

LEMMA 4.17. *Given positive integers m, a, and prime power $v^h > 1$, we can find prime q not dividing am so that the order of a modulo q is v^l where $l \geq h$.*

PROOF. Let $q_1, \ldots, q_s$ be the primes dividing m. If q_i divides some $a^{v^r} - 1$ then let q_i divide $a^{v^{r_i}} - 1$. Take r_0 greater than h and also greater than any of the r_i that are defined. We claim that there is a prime q dividing T_{r_0} so that q is not equal to v or any of the q_i. Then q also divides $a^{v^{r_0}} - 1$, so $a^{v^{r_0}} = 1 (\mathrm{mod}\ q)$. If $a^{v^{r_0 - 1}} = 1 (\mathrm{mod}\ q)$ then by (4.4) we would have $T_{r_0} = v (\mathrm{mod}\ q)$ (impossible). Therefore the order of a modulo q is v^{r_0}, which is greater than v^h.

We need to show how to find q. By (4.4) we must have $T_{r_0} > v$. If T_{r_0} were a power of v then by (3) of lemma 4.16 we would have $r_0 = 1$. But r_0 was chosen greater than 1, so T_{r_0} has some prime divisor q that is not v. Then q divides $a^{v^{r_0}} - 1$. Suppose that $q = q_i$. Since q_i divides $a^{v^{r_i}} - 1$ and $r_i < r_0$, then q_i would divide $a^{v^{r_0 - 1}} - 1$. By (1) of lemma 4.16, $q_i = v$ (impossible). Therefore $q \neq q_i$.

Existence of cyclic extensions with given properties.

PROPOSITION 4.18. *Let finite prime p of $\mathbf{Q}$, finite extension $\mathbf{T}$ of $\mathbf{Q}$, and prime power $v^h > 1$ be given. Then there exists a cyclic extension $\mathbf{Z}$ of $\mathbf{Q}$ so that*
(1) *$\mathbf{Z}$ is contained in a cyclotomic extension of $\mathbf{Q}$,*
(2) *p is not ramified in $\mathbf{Z}$,*
(3) *Artin symbol $\left(\frac{\mathbf{Z}:\mathbf{Q}}{p}\right)$ has order v^h,*
(4) *$\mathbf{Z} \cap \mathbf{T} = \mathbf{Q}$, and*
(5) *$[\mathbf{Z} : \mathbf{Q}]$ is a power of v and $[\mathbf{Z} : \mathbf{Q}] \geq v^h$.*

PROOF. Look at all of the fields $\mathbf{Q}(\zeta_m) \cap \mathbf{T}$; choose m_0 so that $[\mathbf{Q}(\zeta_{m_0}) \cap \mathbf{T} : \mathbf{Q}]$ is maximum. We first want to show that if m is relatively prime to m_0 then $\mathbf{Q}(\zeta_m) \cap \mathbf{T} = \mathbf{Q}$. We have $\mathbf{Q}(\zeta_m) \cap \mathbf{T} \subset \mathbf{Q}(\zeta_{mm_0}) \cap \mathbf{T}$. Also, $\mathbf{Q}(\zeta_{m_0}) \cap \mathbf{T} \subset \mathbf{Q}(\zeta_{mm_0}) \cap \mathbf{T}$, but by the choice of m_0, we must have $\mathbf{Q}(\zeta_{m_0}) \cap \mathbf{T} = \mathbf{Q}(\zeta_{mm_0}) \cap \mathbf{T}$. Therefore $\mathbf{Q}(\zeta_m) \cap \mathbf{T} \subset \mathbf{Q}(\zeta_m) \cap \mathbf{Q}(\zeta_{m_0}) = \mathbf{Q}$ as claimed.

By lemma 4.17, given m_0, p, and v^h, we can find prime q relatively prime to p and m_0 so that the order of p modulo q is v^l and $l \geq h$. Let $\mathbf{k} = \mathbf{Q}(\zeta_q)$, a cyclic extension with Galois group isomorphic to $\mathbf{Z}_q^*$. By lemma 3.2 we have $\left(\frac{\mathbf{k}:\mathbf{Q}}{p}\right) \zeta = \zeta^p$. The order of $\left(\frac{\mathbf{k}:\mathbf{Q}}{p}\right)$ is the order of p modulo q, which is v^l. Let σ be a generator of $G = G(\mathbf{k} : \mathbf{Q})$; the order of σ is $q - 1$. Then $\left(\frac{\mathbf{k}:\mathbf{Q}}{p}\right) = \sigma^{rv^k}$, where v does not divide r. Since $\sigma^{rv^{k+l}} = \left(\frac{\mathbf{k}:\mathbf{Q}}{p}\right)^{v^l} = 1$, and v^{k+l} is the smallest power for which this is true, it follows that v^{k+l} is the exact power of v dividing $q - 1$.

Take $\mathbf{Z}$ to be the fixed field of the subgroup H generated by $\sigma^{v^{k+h}}$. By lemma 2.13, $\left(\frac{\mathbf{Z}:\mathbf{Q}}{p}\right) = \sigma^{rv^k}$. Then $\left(\frac{\mathbf{Z}:\mathbf{Q}}{p}\right)^{v^h} = \sigma^{rv^{k+h}} \in H$. Therefore $\left(\frac{\mathbf{Z}:\mathbf{Q}}{p}\right)^{v^h} = 1$. If

$j < h$ then $\left(\frac{\mathbf{Z:Q}}{p}\right)^{v^j} = \sigma^{rv^{k+j}} \notin \langle \sigma^{v^{k+h}} \rangle$, so $\left(\frac{\mathbf{Z:Q}}{p}\right)^{v^j} \neq 1$; therefore $\left(\frac{\mathbf{Z:Q}}{p}\right)$ is order v^h.

We have (1) $\mathbf{Z}$ is contained in $\mathbf{Q}(\zeta_q)$, (2) p does not divide q and so is not ramified in $\mathbf{Z}$, (3) Artin symbol $\left(\frac{\mathbf{Z:Q}}{p}\right)$ has order v^h, (4) $\mathbf{Z} \cap \mathbf{T} \subset \mathbf{Q}(\zeta_q) \cap T \subset \mathbf{Q}$, and (5) $[\mathbf{Z} : \mathbf{Q}] = [G : H] = [< \sigma >:< \sigma^{v^{k+h}} >] = v^{k+h}$.

Remark. It is possible to choose the roots of unity so that $\zeta_{mn}^n = \zeta_m$. (Choose an embedding of the algebraic closure of $\mathbf{Q}$ into the complex field such that ζ_n is mapped to $e^{2\pi i/n}$ for each $n > 1$.) This relation will simplify the proof of proposition 4.19.

Lemma 4.19. *If (n, m) is the greatest common divisor of n and m then*

$$\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m) = \mathbf{Q}(\zeta_{nm/(n,m)}).$$

Proof. There exists integers u and v so that $un + vm = (n, m)$, and we have $\zeta_m^u \zeta_n^v = \zeta_{nm}^{un+mv} = \zeta_{nm}^{(n,m)} = \zeta_{nm/(n,m)}$, so $\mathbf{Q}(\zeta_{nm/(n,m)})$ is contained in $\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m)$. Since $\zeta_{mn/(n,m)}^{n/(n,m)} = \zeta_m$ and $\zeta_{mn/(n,m)}^{m/(n,m)} = \zeta_n$ we also have $\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m)$ contained in $\mathbf{Q}(\zeta_{nm/(n,m)})$. Therefore $\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m) = \mathbf{Q}(\zeta_{nm/(n,m)})$.

Proposition 4.20. *Let finite prime p of $\mathbf{Q}$, finite extension $\mathbf{T}$ of $\mathbf{Q}$, and positive integer n be given. Then there exists a cyclic extension $\mathbf{Z}$ of $\mathbf{Q}$ so that*
(1) *$\mathbf{Z}$ is contained in a cyclotomic extension of $\mathbf{Q}$.*
(2) *p is not ramified in $\mathbf{Z}$,*
(3) *Artin symbol $\left(\frac{\mathbf{Z:Q}}{p}\right)$ has order n,*
(4) *$\mathbf{Z} \cap \mathbf{T} = \mathbf{Q}$,*
(5) *n divides $[\mathbf{Z} : \mathbf{Q}]$, and the only primes dividing $[\mathbf{Z} : \mathbf{Q}]$ are those dividing n.*

Proof. If n is a prime power then proposition 4.20 reduces to proposition 4.18. Suppose that the conclusion of Proposition 4.20 holds for relatively prime n_1 and n_2. We must show that the conclusion holds for $n_1 n_2$. Let $\mathbf{Z}_1 = \mathbf{Z}(p, n_1, \mathbf{T})$ satisfy the conclusion for n_1, and let $\mathbf{Z}_2 = \mathbf{Z}(p, n_2, \mathbf{Z}_1\mathbf{T})$ satisfy the conclusion for n_2.

Choose $\mathbf{Z}$ to be $\mathbf{Z}_1\mathbf{Z}_2$. Then $\mathbf{Z}_1$ is contained in $\mathbf{Q}(\zeta_{m_1})$ and $\mathbf{Z}_2$ is contained in $\mathbf{Q}(\zeta_{m_2})$. By lemma 4.19, $\mathbf{Z}$ is contained in $\mathbf{Q}(\zeta_m)$, where m is the least common multiple of m_1 and m_2, showing (1). p is not ramified in $\mathbf{Z}_1$, so any prime of $\mathbf{Z}_2$ dividing p is not ramified in $\mathbf{Z}_1\mathbf{Z}_2/\mathbf{Z}_2$ by lemma 2.16. Since p is not ramified in $\mathbf{Z}_2/\mathbf{Q}$ then p is not ramified in $\mathbf{Z}_1\mathbf{Z}_2/\mathbf{Q}$, showing (2).

We must that $\mathbf{Z}/\mathbf{Q}$ is cyclic. We have $\mathbf{Z}_1 \cap \mathbf{Z}_2 \subset \mathbf{Z}_1\mathbf{T} \cap \mathbf{Z}_2 = \mathbf{Q}$. Therefore by lemmas 2.10 and 2.11, we have $G(\mathbf{Z}_1\mathbf{Z}_2 : \mathbf{Q}) = \mathbf{G}(\mathbf{Z}_1 : \mathbf{Q}) \times \mathbf{G}(\mathbf{Z}_2 : \mathbf{Q})$. Let cyclic group $\mathbf{G}(\mathbf{Z}_1 : \mathbf{Q})$ of order r_1 be generated by σ_1, and let cyclic group $\mathbf{G}(\mathbf{Z}_2 : \mathbf{Q})$

of order r_2 be generated by σ_2. The only primes dividing r_1 are those dividing n_1, and the only primes dividing r_2 are those dividing n_2. Then r_1 and r_2 are relatively prime, and the order of (σ_1, σ_2) must be $r_1 r_2$. The isomorphism corresponding to (σ_1, σ_2) generates $G(\mathbf{Z}_1\mathbf{Z}_2 : \mathbf{Q})$, so $\mathbf{Z}/\mathbf{Q}$ is cyclic of degree $r_1 r_2$, and the only primes dividing $[\mathbf{Z} : \mathbf{Q}]$ are those dividing $n_1 n_2$ showing (5).

Artin symbol $\left(\frac{\mathbf{Z}:\mathbf{Q}}{p}\right)$ corresponds to the pair $\left(\left(\frac{\mathbf{Z}_1:\mathbf{Q}}{p}\right), \left(\frac{\mathbf{Z}_2:\mathbf{Q}}{p}\right)\right)$ by the corollary to lemma 2.13. These Artin symbols for $\mathbf{Z}_1$ and $\mathbf{Z}_2$ have orders n_1 and n_2, respectively. Therefore $\left(\frac{\mathbf{Z}:\mathbf{Q}}{p}\right)$ has order $n_1 n_2$, showing (3). Finally, $[\mathbf{Z}_1\mathbf{Z}_2\mathbf{T} : \mathbf{Z}_2] = [\mathbf{Z}_1\mathbf{T} : \mathbf{Z}_2 \cap \mathbf{Z}_1\mathbf{T}] = [\mathbf{Z}_1\mathbf{T} : \mathbf{Q}]$, so $[\mathbf{Z}_1\mathbf{Z}_2\mathbf{T} : \mathbf{Z}_2][\mathbf{Z}_2 : \mathbf{Q}] = [\mathbf{Z}_1\mathbf{T} : \mathbf{Q}][\mathbf{Z}_2 : \mathbf{Q}]$. Therefore $[\mathbf{Z}_1\mathbf{Z}_2\mathbf{T} : \mathbf{Q}] = [\mathbf{Z}_1\mathbf{T} : \mathbf{Q}][\mathbf{Z}_2 : \mathbf{Q}]$. By lemma 2.10, it follow that $\mathbf{Z}_1\mathbf{Z}_2 \cap \mathbf{T} = \mathbf{Q}$, showing (4).

PROPOSITION 4.21. *Let* $\mathbf{k}$ *be a finite extension of* $\mathbf{Q}$. *Let finite prime* $\wp$ *of* $\mathbf{k}$, *finite extension* $\mathbf{T}$ *of* $\mathbf{k}$, *and positive integer* n *be given. Then there exists a cyclic extension* $\mathbf{Z}$ *of* $\mathbf{k}$ *so that*
(1) $\mathbf{Z}$ *is contained in a cyclotomic extension of* $\mathbf{k}$.
(2) $\wp$ *is not ramified in* $\mathbf{Z}$,
(3) *Artin symbol* $\left(\frac{\mathbf{Z}:\mathbf{k}}{\wp}\right)$ *has order* n,
(4) $\mathbf{Z} \cap \mathbf{T} = \mathbf{k}$,
(5) n *divides* $[\mathbf{Z} : \mathbf{k}]$.

PROOF. Let (p) be the prime of $\mathbf{Q}$ that $\wp$ divides; let $\mathrm{N}\wp = p^f$. Let $\mathbf{Z}'$ be the cyclic extension of $\mathbf{Q}$ satisfying the conclusion of proposition 4.20 for p, nf and $\mathbf{T}$. Take $\mathbf{Z} = \mathbf{Z}'\mathbf{k}$. Since $\mathbf{Z}' \subset \mathbf{Q}(\zeta_m)$, we have $\mathbf{Z} \subset \mathbf{k}(\zeta_m)$, showing (1). Since p is not ramified in $\mathbf{Z}'$ then $\wp$ is not ramified in $\mathbf{Z}$ by lemma 2.16, showing (2). Artin symbol $\left(\frac{\mathbf{Z}':\mathbf{Q}}{p}\right)$ has order nf, and by lemma 2.16 we have $\left(\frac{\mathbf{Z}:\mathbf{k}}{\wp}\right) = \left(\frac{\mathbf{Z}':\mathbf{Q}}{p}\right)^f$. Therefore $\left(\frac{\mathbf{Z}:\mathbf{k}}{\wp}\right)$ has order n, showing (3).

We want to show $\mathbf{Z} \cap \mathbf{T} = \mathbf{k}$. We have

$$[\mathbf{ZT} : \mathbf{T}] = [\mathbf{Z}'\mathbf{T} : \mathbf{T}] = [\mathbf{Z}' : \mathbf{Z}' \cap \mathbf{T}] = [\mathbf{Z}' : \mathbf{Q}] \geq [\mathbf{Z}'\mathbf{k} : \mathbf{k}] = [\mathbf{Z} : \mathbf{k}] \geq [\mathbf{ZT} : \mathbf{T}].$$

Therefore $[\mathbf{Z} : \mathbf{k}] = [\mathbf{ZT} : \mathbf{T}] = [\mathbf{Z} : \mathbf{Z} \cap \mathbf{T}]$ so $\mathbf{k} = \mathbf{T} \cap \mathbf{Z}$, showing (4). Finally, $G(\mathbf{Z} : \mathbf{k})$ contains an element of order n by (3), so n divides $[\mathbf{Z} : \mathbf{k}]$, showing (5).

PROPOSITION 4.22. *If* $\mathbf{K}_1\mathbf{k}$ *is a finite abelian extension and Theorem 1 holds for* $\mathbf{K}_1/\mathbf{k}$, *then Theorem 1 holds for any extension* $\mathbf{K}_2/\mathbf{k}$ *such that* $\mathbf{K}_1 \supset \mathbf{K}_2 \supset \mathbf{k}$.

PROOF. Theorem 1 holds for $\mathbf{K}_2/\mathbf{k}$ if and only $\phi_{\mathbf{K}_2/\mathbf{k}}$ of (2.1) can be extended onto $\mathbf{I}_\mathbf{k}$ so that the kernel contains $\mathbf{k}^*$. The restriction of $\phi_{\mathbf{K}_1/\mathbf{k}}(\mathbf{i})$ as defined by (2.1) to $\mathbf{K}_2$ coincides with $\phi_{\mathbf{K}_2/\mathbf{k}}(\mathbf{i})$ for $\mathbf{i} \in \mathbf{I}_\mathbf{k}\{E\}$. Since $\phi_{\mathbf{K}_1/\mathbf{k}}$ can be extended to all of $\mathbf{I_k}$ so that the kernel contains $\mathbf{k}^*$, we may define $\phi_{\mathbf{K}_2/\mathbf{k}}(\mathbf{i})$ for $\mathbf{I} \in \mathbf{I_k}$ to be the restriction of $\phi_{\mathbf{K}_1/\mathbf{k}}(\mathbf{i})$ to $\mathbf{K}_2$.

Remark. The cyclic extension $\mathbf{Z}/\mathbf{k}$ guaranteed by proposition 4.21 is contained in a cyclotomic extension of $\mathbf{k}$. Since we have proved Theorem 1 for cyclotomic extensions, then Theorem 1 holds for the extensions $\mathbf{Z} = \mathbf{Z}(p, n, \mathbf{T})/\mathbf{k}$.

Proof of theorem 1 for cyclic extensions. Let $\mathbf{K}/\mathbf{k}$ be a cyclic extension of degree n, and let σ_0 be a generator of $G(\mathbf{K} : \mathbf{k})$. There is an isomorphism $\chi : G(\mathbf{K} : \mathbf{k}) \longrightarrow \mathbf{C}$ to n-th roots of unity in defined by

$$\chi(\sigma_0^x) = \exp\left(\frac{2\pi i x}{n}\right).$$

By the first and second fundamental inequalities (to be proved in chapters 7 and 8), we have $[\mathbf{I_k} : \mathbf{k}^*\mathbf{N_{K/k}I_K}] = n$. Finite abelian group $\mathbf{I_k}/(\mathbf{k}^*\mathbf{N_{K/k}I_K})$ is a direct product of cyclic groups

$$\frac{\mathbf{I_k}}{\mathbf{k}^*\mathbf{N_{K/k}I_K}} = \mathbf{H}_1 \times \cdots \times \mathbf{H}_r,$$

where $\mathbf{H}_k$ is a cyclic group of order n_k generated by h_k. Every element of the quotient group can be written as a product

$$h_1^{x_1} \dots h_r^{x_r} \text{ where } 0 \leq x_k < n_k.$$

For each r-tuple $\omega = (\omega_1, \dots, \omega_r)$ with $0 \leq \omega_k < n_k$, there is a homomorphism $\chi_\omega : \mathbf{H}_1 \times \cdots \times \mathbf{H}_r \to \mathbf{C}$ defined by

$$\chi_\omega\left(h_1^{x_1} \dots h_r^{s_r}\right) = \exp\left(\frac{2\pi i \omega_1 x_1}{n_1}\right) \dots \exp\left(\frac{2\pi i \omega_1 x_1}{n_1}\right).$$

The number of homomorphisms χ_ω is n. Each homomorphism uniquely determines the r-tuple ω because the image $\exp(2\pi i \omega_k/n_k)$ of h_k determines ω_k.

Choose a prime p of $\mathbf{k}$. By proposition 4.21, there is a cyclic extension $\mathbf{Z} = \mathbf{Z}(p, n, \mathbf{K})$ contained in a cyclotomic extension of $\mathbf{k}$ such that $[\mathbf{Z} : \mathbf{k}]$ is divisible by n, prime p is not ramified in $\mathbf{Z}$, Artin symbol $\left(\frac{\mathbf{Z}:\mathbf{k}}{p}\right)$ has order exactly n, and $\mathbf{Z} \cap \mathbf{K} = \mathbf{k}$. Let ρ_0 generate the Galois group $G(\mathbf{Z} : \mathbf{k})$, and let $rn = [\mathbf{Z} : \mathbf{k}]$. There is an isomorphism $\Theta : G(\mathbf{Z} : \mathbf{k}) \to \mathbf{C}$ defined by

$$\Theta(\rho_0^x) = \exp\left(\frac{2\pi i x}{rn}\right).$$

Since $\mathbf{Z} \cap \mathbf{K} = \mathbf{k}$, we have

$$G(\mathbf{ZK} : \mathbf{k}) = G(\mathbf{Z} : \mathbf{k}) \times G(\mathbf{K} : \mathbf{k}) = \left\{(\rho_0^x, \sigma_0^y) \;\middle|\; 0 \leq x < rn, 0 \leq y < n\right\}.$$

Let $\mathbf{S} = \mathbf{S}(a)$ be the fixed field of $\left\{(\rho_0^x, \sigma_0^y) \;\middle|\; xa - yr = 0(\mathrm{mod}\ rn\right\}$. Then $\mathbf{ZS} \subset \mathbf{ZK}$. If (ρ_0^x, σ_0^y) fixes $\mathbf{Z}$ then $x = 0(\mathrm{mod}\ rn)$, and if (ρ_0^x, σ_0^y) fixes $\mathbf{S}$ then $xa - yr = 0(\mathrm{mod}\ rn)$. If $\mathbf{ZS}$ is fixed then $yr = 0(\mathrm{mod}\ rn)$, or $y = 0(\mathrm{mod}\ n)$, so only the identity of $G(\mathbf{ZK} : \mathbf{k})$ fixes $\mathbf{ZS}$. Therefore $\mathbf{ZS} = \mathbf{ZK}$.

$\mathbf{Z}$ is contained in a cyclotomic extension of $\mathbf{k}$, so $\mathbf{ZS}$ is contained in a cyclotomic extension of $\mathbf{S}$. Therefore Theorem 1 holds for $\mathbf{ZS}/\mathbf{S}$. $G(\mathbf{ZS} : \mathbf{S})$ is isomorphic to a subgroup of $G(\mathbf{Z} : \mathbf{k})$. Let ρ^{x_0} generate $G(\mathbf{ZS} : \mathbf{S})$, and we can take x_0 to be the least positive power of ρ that is in $G(\mathbf{ZS} : \mathbf{S})$ (*i.e.,* that fixes $\mathbf{S}$), so x_0 divides rn.

Since $\mathbf{N}_{\mathbf{S}/\mathbf{k}}$ maps $\ker(\phi_{\mathbf{ZS}/\mathbf{S}}) = \mathbf{S}^*\mathbf{N}_{\mathbf{ZS}/\mathbf{S}}\mathbf{I}_{\mathbf{ZS}}$ to $\ker(\chi_\omega) = \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}$, there is an induced homomorphism $f : G(\mathbf{ZS} : \mathbf{S}) \to \mathbf{C}$ so that $f\phi_{\mathbf{ZS}/\mathbf{S}} = \chi_\omega \mathbf{N}_{\mathbf{S}/\mathbf{K}}$. (See diagram (4.7), noting that $\mathbf{N}_{\mathbf{S}/\mathbf{k}}\mathbf{N}_{\mathbf{ZS}/\mathbf{S}} = \mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{N}_{\mathbf{ZK}/\mathbf{K}}$ because $\mathbf{ZS} = \mathbf{ZK}$.) The image of $\rho_0^{x_0}$ must be an (rn/x_0)-th root of unity, so there is an integer u so that $f(\rho_0^{x_0}) = \Theta(\rho_0)^{ux_0} = \Theta(\rho_0^{x_0})^u$. Since $\rho_0^{x_0}$ generates the image of $\phi_{\mathbf{ZS}/\mathbf{S}}$, we have $f\left(\phi_{\mathbf{ZS}/\mathbf{S}}(\mathbf{i})\right) = \Theta\left(\phi_{\mathbf{ZS}/\mathbf{S}}(\mathbf{i})|_{\mathbf{Z}}\right)^u$. The restriction $\phi_{\mathbf{ZS}/\mathbf{S}}(\mathbf{i})|_{\mathbf{Z}}$ of $\phi_{\mathbf{ZS}/\mathbf{S}}(\mathbf{i})$ to $\mathbf{Z}$ is $\phi_{\mathbf{Z}/\mathbf{k}}(\mathbf{N}_{\mathbf{S}/\mathbf{k}}\mathbf{i})$ (proposition 2.19). Therefore there is an integer $u = u(a, p, \mathbf{Z})$ depending on the choices of a, p and $\mathbf{Z}$ so that

$$\chi_\omega\left(\mathbf{N}_{\mathbf{S}/\mathbf{k}}\mathbf{i}\right) = \Theta\left(\phi_{\mathbf{Z}/\mathbf{k}}\left(\mathbf{N}_{\mathbf{S}/\mathbf{k}}\mathbf{i}\right)\right)^u \qquad \text{for } \mathbf{i} \in \mathbf{I}_{\mathbf{S}}. \tag{4.5}$$

Diagram (4.7)

$$\begin{tikzcd}
\mathbf{I}_{\mathbf{ZK}} \arrow[r, equal] \arrow[d, "\mathbf{N}_{\mathbf{ZK}/\mathbf{K}}"] & \mathbf{I}_{\mathbf{ZS}} \arrow[d, "\mathbf{N}_{\mathbf{ZS}/\mathbf{S}}"] & & & \\
\mathbf{I}_{\mathbf{K}} \arrow[d, "\mathbf{N}_{\mathbf{K}/\mathbf{k}}"] & \mathbf{I}_{\mathbf{S}} \arrow[r] \arrow[d, "\mathbf{N}_{\mathbf{S}/\mathbf{k}}"] & \frac{\mathbf{I}_{\mathbf{S}}}{\mathbf{S}^*\mathbf{N}_{\mathbf{ZS}/\mathbf{S}}\mathbf{I}_{\mathbf{ZS}}} \arrow[r, "\phi_{\mathbf{ZS}/\mathbf{S}}"] & G(\mathbf{ZS} : \mathbf{S}) \arrow[r, equal] \arrow[d, "f"] & \langle \rho_0^{x_0} \rangle \\
\mathbf{I}_{\mathbf{k}} \arrow[r, equal] & \mathbf{I}_{\mathbf{k}} \arrow[r] & \frac{\mathbf{I}_{\mathbf{k}}}{\mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}} \arrow[r, "\chi_\omega"] & \mathbf{C} & G(\mathbf{Z} : \mathbf{k}) \arrow[l, "\Theta"']
\end{tikzcd}$$

Let $\mathbf{Z}' = \mathbf{Z}'(p', n, \mathbf{K})$ be another cyclic extension satisfying the conclusion of proposition 4.21, where p' is a prime of $\mathbf{k}$. (Note: $\mathbf{Z}'$ will be used to show that certain later results are independent of p and of $\mathbf{Z}$.) Now let $\mathbf{W} = \mathbf{W}(p, n, \mathbf{ZZ}'\mathbf{K})$ be a cyclic extension of $\mathbf{k}$ satisfying the conclusion of proposition 4.21. Then $\mathbf{W}$ is a cyclic extension contained in a cyclotomic extension of $\mathbf{k}$, $[\mathbf{W} : \mathbf{k}]$ is divisible by n, Artin symbol $\left(\frac{\mathbf{W}:\mathbf{k}}{p}\right)$ has order n, and $\mathbf{W} \cap \mathbf{ZZ}'\mathbf{K} = \mathbf{k}$. Let $[\mathbf{W} : \mathbf{k}] = sn$, and let τ_0 be a generator of cyclic group $G(\mathbf{W} : \mathbf{k})$. There is an isomorphism $\Xi : G(\mathbf{W} : \mathbf{k}) \to \mathbf{C}$ defined by

$$\Xi(\tau_0^z) = \exp\left(\frac{2\pi i}{sn}\right).$$

We repeat the previous argument, with $\mathbf{W}$ in place of $\mathbf{Z}$. Since $\mathbf{W} \cap \mathbf{ZZ'K} = \mathbf{k}$, we have

$$G(\mathbf{KW} : \mathbf{k}) = G(\mathbf{K} : \mathbf{k}) \times G(\mathbf{W} : \mathbf{k}) = \left\{ (\sigma_0^y, \tau_0^z) \;\middle|\; 0 \le y < n, 0 \le z < sn \right\}.$$

Let $\mathbf{T}$ be the fixed field of $\left\{ (\sigma_0^y, \tau_0^z) \;\middle|\; ys - z = 0(\mathrm{mod}\ sn \right\}$. Then $\mathbf{WT} \subset \mathbf{KW}$. If (σ_0^y, τ_0^z) fixes $\mathbf{W}$ then $z = 0(\mathrm{mod}\ sn)$, and if (ρ_0^x, σ_0^y) fixes $\mathbf{T}$ then $ys - z = 0(\mathrm{mod}\ sn)$. If $\mathbf{TW}$ is fixed then $ys = 0(\mathrm{mod}\ sn)$, or $y = 0(\mathrm{mod}\ n)$, so only the identity of $G(\mathbf{KW} : \mathbf{k})$ fixes $\mathbf{TW}$. Therefore $\mathbf{TW} = \mathbf{KW}$.

Since $\mathbf{W}$ is contained in a cyclotomic extension of $\mathbf{k}$ then $\mathbf{TW}$ is contained in a cyclotomic extension of $\mathbf{T}$. Therefore Theorem 1 holds for $\mathbf{TW}/\mathbf{T}$. $G(\mathbf{TW} : \mathbf{T})$ is isomorphic to a subgroup of $G(\mathbf{W} : \mathbf{k})$. Let τ^{z_0} generate $G(\mathbf{TW} : \mathbf{T})$, and we can take z_0 to be the least positive power of τ that is in $G(\mathbf{TW} : \mathbf{T})$ (*i.e.,* that fixes $\mathbf{T}$), so z_0 divides sn.

Since $\mathbf{N}_{\mathbf{T}/\mathbf{k}}$ maps $\ker(\phi_{\mathbf{TW}/\mathbf{W}}) = \mathbf{T}^*\mathbf{N}_{\mathbf{TW}/\mathbf{W}}\mathbf{I}_{\mathbf{TW}}$ to $\ker(\chi_\omega) = \mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}$, there is an induced homomorphism $g : G(\mathbf{TW} : \mathbf{T}) \to \mathbf{C}$ so that $g\phi_{\mathbf{TW}/\mathbf{W}} = \chi_\omega \mathbf{N}_{\mathbf{T}/\mathbf{k}}$. (See diagram (4.8), noting that $\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{N}_{\mathbf{TW}/\mathbf{T}} = \mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{N}_{\mathbf{KW}/\mathbf{K}}$ because $\mathbf{TW} = \mathbf{KW}$.) The image of $\tau_0^{z_0}$ must be an (sn/z_0)-th root of unity, so there is an integer v so that $g(\tau_0^{z_0}) = \Xi(\tau_0)^{vz_0} = \Xi(\tau_0^{z_0})^v$. Since $\tau_0^{z_0}$ generates the image of $\phi_{\mathbf{TW}/\mathbf{W}}$, we have $g\left(\phi_{\mathbf{TW}/\mathbf{W}}(\mathbf{i})\right) = \Xi\left(\phi_{\mathbf{TW}/\mathbf{W}}(\mathbf{i})|_{\mathbf{W}}\right)^u$. The restriction $\phi_{\mathbf{TW}/\mathbf{W}}(\mathbf{i})|_{\mathbf{W}}$ of $\phi_{\mathbf{TW}/\mathbf{T}}(\mathbf{i})$ to $\mathbf{W}$ is $\phi_{\mathbf{W}/\mathbf{k}}(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i})$ (proposition 2.19). Therefore there is an integer $v = v(p, p', \mathbf{Z}, \mathbf{Z}')$ depending on the choices of p, p', $\mathbf{Z}$ and $\mathbf{Z}'$ so that

$$\chi_\omega\left(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i}\right) = \Xi\left(\phi_{\mathbf{T}/\mathbf{k}}\left(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i}\right)\right)^v \qquad \text{for } \mathbf{i} \in \mathbf{I}_{\mathbf{T}}. \tag{4.6}$$

Diagram (4.8)

$$\begin{tikzcd}
\mathbf{I}_{\mathbf{KW}} \arrow[r, equal] \arrow[d, "\mathbf{N}_{\mathbf{KW}/\mathbf{K}}"] & \mathbf{I}_{\mathbf{TW}} \arrow[d, "\mathbf{N}_{\mathbf{TW}/\mathbf{T}}"] & & & \\
\mathbf{I}_{\mathbf{K}} \arrow[d, "\mathbf{N}_{\mathbf{K}/\mathbf{k}}"] & \mathbf{I}_{\mathbf{T}} \arrow[r] \arrow[d, "\mathbf{N}_{\mathbf{T}/\mathbf{k}}"] & \frac{\mathbf{I}_{\mathbf{T}}}{\mathbf{T}^*\mathbf{N}_{\mathbf{TW}/\mathbf{W}}\mathbf{I}_{\mathbf{TW}}} \arrow[r, "\phi_{\mathbf{TW}/\mathbf{T}}"] & G(\mathbf{TW} : \mathbf{T}) \arrow[r, equal] \arrow[d, "g"] & \langle \tau_0^{z_0} \rangle \\
\mathbf{I}_{\mathbf{k}} \arrow[r, equal] & \mathbf{I}_{\mathbf{k}} \arrow[r] & \frac{\mathbf{I}_{\mathbf{k}}}{\mathbf{k}^*\mathbf{N}_{\mathbf{K}/\mathbf{k}}\mathbf{I}_{\mathbf{K}}} \arrow[r, "\chi_\omega"] & \mathbf{C} & G(\mathbf{W} : \mathbf{k}) \arrow[l, "\Xi"']
\end{tikzcd}$$

Multiply both sides of (4.6) by $\Theta\left(\phi_{\mathbf{Z}/\mathbf{k}}(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i})\right)^{-u}$ to obtain

$$\begin{aligned} \chi_\omega(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i})\Theta\left(\phi_{\mathbf{Z}/\mathbf{k}}(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i})\right)^{-u} \\ = \Theta\left(\phi_{\mathbf{Z}/\mathbf{k}}(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i})\right)^{-u} \Xi\left(\phi_{\mathbf{T}/\mathbf{k}}\left(\mathbf{N}_{\mathbf{T}/\mathbf{k}}\mathbf{i}\right)\right)^v \qquad \text{for } \mathbf{i} \in \mathbf{I}_{\mathbf{T}}. \end{aligned} \tag{4.9}$$

Given $\mathbf{j} \in \mathbf{I_{ST}}$, if $\mathbf{i} = \mathbf{N_{ST/T}}\,\mathbf{j}$ then $\mathbf{N_{T/k}}\mathbf{i} = \mathbf{N_{S/k}}(\mathbf{N_{ST/S}}\,\mathbf{j}) = \mathbf{N_{ST/k}}\,\mathbf{j}$. The kernel of the mapping $\mathbf{I_k} \to \mathbf{C}$ by $\mathbf{i} \to \chi_\omega(\mathbf{i})\Theta(\phi_{\mathbf{Z/k}}\mathbf{i})^{-u}$ contains $\mathbf{N_{S/k}}\mathbf{I_S}$ by (4.5). If we evaluate (4.9) at $\mathbf{i} = \mathbf{N_{ST/T}}\,\mathbf{j}$, we obtain

$$(4.10) \qquad 1 = \Theta\left(\phi_{\mathbf{Z/k}}(\mathbf{N_{ST/k}}\,\mathbf{j})\right)^{-u} \Xi\left(\phi_{\mathbf{W/k}}(\mathbf{N_{ST/k}}\,\mathbf{j})\right)^{v} \qquad \text{for } \mathbf{j} \in \mathbf{I_{ST}}.$$

We have $\mathbf{ZS} = \mathbf{ZK}$ contained in a cyclotomic extension of $\mathbf{S}$ and $\mathbf{TW} = \mathbf{KW}$ contained in a cyclotomic extension of $\mathbf{T}$, so $\mathbf{ZKW} = \mathbf{ZSW} = \mathbf{ZTW}$ is contained in a cyclotomic extension of $\mathbf{TS}$. Therefore Theorem 1 holds for $\mathbf{ZKW/TS}$. The restriction of $\phi_{\mathbf{ZKW/TS}}$ to $\mathbf{ZST}$ is $\phi_{\mathbf{ZST/TS}}(\mathbf{i}) = \phi_{\mathbf{Z/k}}(\mathbf{N_{ST/k}}(\mathbf{i}))$, and the restriction of $\phi_{\mathbf{ZKW/TS}}$ to $\mathbf{STW}$ is $\phi_{\mathbf{STW/TS}}(\mathbf{i}) = \phi_{\mathbf{W/k}}(\mathbf{N_{ST/k}}(\mathbf{i}))$. (Let σ_1 denote the restriction of $\phi_{\mathbf{ZKW/TS}}$ to $\mathbf{K}$.) The mapping $(\rho, \sigma, \tau) \to \Theta(\rho)^{-u}\Xi(\tau)^v$ is a homomorphism $G(\mathbf{ZKW} : \mathbf{k}) \to \mathbf{C}$ which maps $\phi_{\mathbf{ZKW/ST}}(\mathbf{i}) = \left(\phi_{\mathbf{Z/k}}(\mathbf{N_{ST/k}}\mathbf{i}), \sigma_1, \phi_{\mathbf{W/k}}(\mathbf{N_{ST/k}}\mathbf{i})\right)$ to 1 by (4.10). The homomorphism $\phi_{\mathbf{ZKW/ST}}$ maps $\mathbf{I_{ST}}$ onto $G(\mathbf{ZKW} : \mathbf{ST})$. Therefore

$$\Theta(\rho)^{-u}\Xi(\tau)^v = 1 \qquad \text{for any } (\rho, \sigma, \tau) \in G(\mathbf{ZKW} : \mathbf{k}) \text{ leaving } \mathbf{ST} \text{ fixed.}$$

In particular, the automorphism $(\rho_0^r, \sigma_0^a, \tau_0^{as})$ leaves both $\mathbf{S}$ and $\mathbf{T}$ fixed. Therefore

$$\Theta\left(\rho_0^r\right)^{-u} \Xi\left(\tau_0^{as}\right)^v = 1.$$

We have $\exp\bigl(2\pi i r/(rn)\bigr)^{-u} \exp\bigl(2\pi i a s/(sn)\bigr)^{v} = \exp\bigl(2\pi i(-u/n + av/n)\bigr) = 1$, or

$$(4.11) \qquad u = av (\operatorname{mod} n).$$

We show that v is independent of $\mathbf{Z}$ and $\mathbf{Z}'$. The construction leading from $\mathbf{W}$ to v is symmetric in $\mathbf{Z}$ and $\mathbf{Z}'$. We can reverse the roles of $\mathbf{Z}$ and $\mathbf{Z}'$, and the $v(\mathbf{Z}, \mathbf{Z}')$ that satisfies (4.11) for $u(\mathbf{Z})$ also satisfies (4.11) for $u(\mathbf{Z}')$.

$$v(\mathbf{W}, \mathbf{Z}, \mathbf{Z}')a = u(a, \mathbf{Z})(\operatorname{mod} n)$$
$$v(\mathbf{W}, \mathbf{Z}, \mathbf{Z}')a = u(a, \mathbf{Z}')(\operatorname{mod} n)$$

We can also start from either $\mathbf{Z}'$ or $\mathbf{Z}''$, obtaining

$$v(\mathbf{W}, \mathbf{Z}', \mathbf{Z}'')a = u(a, \mathbf{Z}')(\operatorname{mod} n)$$
$$v(\mathbf{W}, \mathbf{Z}', \mathbf{Z}'')a = u(a, \mathbf{Z}'')(\operatorname{mod} n)$$

We choose $a = 1$ to conclude that $v(\mathbf{W}, \mathbf{Z}, \mathbf{Z}') = u(1, \mathbf{Z}) = u(1, \mathbf{Z}') = v(\mathbf{W}, \mathbf{Z}', \mathbf{Z}'')$. In like manner we have $v(\mathbf{W}, \mathbf{Z}', \mathbf{Z}'') = v(\mathbf{W}, \mathbf{Z}'', \mathbf{Z}''')$. Therefore $v_{\mathbf{W}}$ is independent of $\mathbf{Z}$ and $\mathbf{Z}'$.

v is independent of $\mathbf{W}$. If $\mathbf{W}'$ is chosen then, since u is independent of $\mathbf{W}$, we have

$$v(\mathbf{W})a = u(a, \mathbf{Z}) = v(\mathbf{W}')a(\text{mod } n).$$

Choose $a = 1$ to conclude that $v(\mathbf{W}) = u(1, \mathbf{Z}) = v(\mathbf{W}')1(\text{mod } n)$.

v is independent of p and p'. The construction leading from $\mathbf{W}$ to v is symmetric in p and p'. We can start from either $\mathbf{Z} = \mathbf{Z}(p, n, \mathbf{K})$ or $\mathbf{Z}' = \mathbf{Z}'(p', n, \mathbf{K})$, concluding that

$$\begin{aligned} v(p, p')a &= u(p, \mathbf{Z})(\text{mod } n) \\ v(p, p')a &= u(p', \mathbf{Z}')(\text{mod } n) \end{aligned}$$

We can start from $\mathbf{Z}' = \mathbf{Z}(p', n, \mathbf{K})$ or $\mathbf{Z}'' = \mathbf{Z}''(p'', n, \mathbf{K})$, concluding that

$$\begin{aligned} v(p', p'')a &= u(p', \mathbf{Z}')(\text{mod } n) \\ v(p', p'')a &= u(p'', \mathbf{Z}'')(\text{mod } n) \end{aligned}$$

Choose $a = 1$ to conclude that $v(p, p') = v(p', p'')(\text{mod } n)$. Likewise, $v(p', p'') = v(p'', p''')(\text{mod } n)$. Therefore v is independent of p. We have shown the independence of u and v from p, $\mathbf{Z}$ and $\mathbf{W}$.

Now let p be a prime not ramified in $\mathbf{K}$. Choose $\mathbf{Z} = \mathbf{Z}(p, n, \mathbf{K})$. Artin symbol $\left(\frac{\mathbf{Z}:\mathbf{k}}{p}\right)$ has order n. Since $[\mathbf{Z} : \mathbf{k}] = rn$, we have

$$\left(\frac{\mathbf{Z} : \mathbf{k}}{p}\right) = \rho_0^{x_1 r} \qquad \text{where } (x_1, n) = 1. \tag{4.12}$$

Artin symbol $\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)$ is some power of σ_0, so let

$$\left(\frac{\mathbf{K} : \mathbf{k}}{p}\right) = \sigma_0^{y_1}. \tag{4.13}$$

$\mathbf{S}$ is the fixed field of $\left\{(\rho_0^x, \sigma_0^y) \mid xa - yr = 0(\text{mod } n)\right\}$. $\left(\frac{\mathbf{S}:\mathbf{k}}{p}\right)$ and $\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)$ are the restrictions of $\left(\frac{\mathbf{ZK}:\mathbf{k}}{p}\right)$ to $\mathbf{S}$ and $\mathbf{K}$, respectively, so

$$\left(\frac{\mathbf{ZK} : \mathbf{k}}{p}\right) = \left(\left(\frac{\mathbf{Z} : \mathbf{k}}{p}\right), \left(\frac{\mathbf{K} : \mathbf{k}}{p}\right)\right) = \left(\rho_0^{x_1 r}, \sigma_0^{y_1}\right).$$

Choose a so that $x_1 a - y_1 = 0(\text{mod } n)$. Then

$$r x_1 a - r y_1 = 0(\text{mod } n),$$

so $\left(\frac{\mathbf{ZK}:\mathbf{k}}{p}\right)$ fixes $\mathbf{S}$, so $\left(\frac{\mathbf{S}:\mathbf{k}}{p}\right) = 1$. If $\wp$ is a prime of $\mathbf{S}$ dividing p then $\left(\frac{\mathbf{S}:\mathbf{k}}{p}\right)$ generates $G(\mathbf{S}_\wp/\mathbf{k}_p)$, so $\mathbf{S}_\wp = \mathbf{k}_p$.

For $\alpha \in \mathbf{k}_p$, let $\mathbf{i} = \mathbf{i}(\alpha, p)$ be the idele in $\mathbf{I}_k$ so that

$$\mathbf{i}_q = \begin{cases} \alpha \text{ at } q = p \\ 1 \text{ at } q \neq p \end{cases}$$

Since $\mathbf{S}_\wp = \mathbf{k}_p$, choose $\mathbf{j} = \mathbf{j}(\alpha, \wp)$ for a prime $\wp$ of $\mathbf{K}$ dividing p. Then

$$\mathbf{N}_{\mathbf{S}/\mathbf{k}}\,\mathbf{j}(\alpha, \wp) = \mathbf{i}(\alpha, p)$$

and by (4.5) we have

$$\begin{aligned} \chi_\omega\big(\mathbf{i}(\alpha, p)\big) &= \chi_\omega\big(\mathbf{N}_{\mathbf{S}/\mathbf{k}}\,\mathbf{j}(\alpha, \wp)\big) \\ &= \Theta\big(\phi_{\mathbf{Z}/\mathbf{k}}(\mathbf{N}_{\mathbf{S}/\mathbf{k}}\,\mathbf{j}(\alpha, \wp))\big)^u = \Theta\big(\phi_{\mathbf{Z}/\mathbf{k}}\,\mathbf{i}(\alpha, p))\big)^u \end{aligned} \tag{4.14}$$

Prime p is not ramified in $\mathbf{Z}$, so

$$\phi_{\mathbf{Z}/\mathbf{k}}\big(\mathbf{i}(\alpha, p)\big) = \left(\frac{\mathbf{Z}:\mathbf{k}}{p}\right)^b \qquad \text{where } |\alpha|_p = \mathrm{N}p^{-b}. \tag{4.15}$$

By (4.14), (4.15), and (4.12) we have

$$\begin{aligned} \chi_\omega\big(\mathbf{i}(\alpha, p)\big) &= \Theta\left(\left(\frac{\mathbf{Z}:\mathbf{k}}{p}\right)\right)^{bu} = \Theta\left(\rho_0^{rx_1bu}\right) \\ &= \exp\left(\frac{2\pi irx_1bu}{rn}\right) = \exp\left(\frac{2\pi ix_1bu}{n}\right) \end{aligned}$$

Since $va = u(\mathrm{mod}\ n)$, and since a was chosen so that $x_1a = y_1(\mathrm{mod}\ n)$, we have $x_1bu = x_1bva = y_1bv(\mathrm{mod}\ n)$. By 4.13, we have

$$\chi_\omega\big(\mathbf{i}(\alpha, p)\big) = \exp\left(\frac{2\pi iy_1bv}{n}\right) = \chi\left(\sigma_0^{y_1bv}\right) = \chi\left(\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)\right)^{bv}.$$

To summarize, suppose that p is not ramified in $\mathbf{K}$, α is an element of $\mathbf{k}_p$, and $\mathbf{i} = \mathbf{i}(\alpha, p)$ is an idele in $\mathbf{I}_\mathbf{k}$ with components $\mathbf{i}_q = \alpha$ at prime $q = p$ and $\mathbf{i}_q = 1$ at primes $q \neq p$. Then there is an integer v independent of p so that $0 < v < n$ and

$$\chi_\omega\big(\mathbf{i}(\alpha, p)\big) = \chi\left(\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)\right)^{bv} \qquad \text{where } |\alpha|_p = \mathrm{N}p^{-b} \tag{4.16}$$

If $\mathbf{i} \in \mathbf{I_k}\{E\}$, then (2.1) defines $\phi_{\mathbf{K/k}}$ by

$$\phi_{\mathbf{K/k}}(\mathbf{i}) = \prod_{p \neq E} \left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{b_p} \qquad \text{where } \mathbf{I}_p = \mathrm{N}p^{-b_p}.$$

The only non-trivial terms of the product over E are for primes in $F = \{p \mid |\mathbf{i}_p| \neq 1\}$, so

$$\chi\big(\phi_{\mathbf{K/k}}(\mathbf{i})\big)^v = \prod_{p \notin F} \chi\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)^{b_p v} = \prod_{p \notin F} \chi_\omega\big(\mathbf{i}(\mathbf{i}_p, p)\big).$$

Idele $\mathbf{i}$ in $\mathbf{I_k}\{E\}$ as a direct product is

$$\mathbf{i} = \prod_{\mathbf{p} \in F} \mathbf{i}(\mathbf{i}_p, p) \times \prod_{\mathbf{p} \notin F} \mathbf{i}(\mathbf{i}_p, p)$$

For a prime p not in F, each component $\mathbf{i}_p$ is the norm of an $\beta_\wp$ element in $\mathbf{K}_\wp$ for prime $\wp$ of $\mathbf{K}$ dividing p, by proposition 4.7. By setting $\mathbf{j}_\wp = \beta$ at one prime $\wp$ dividing each prime p not in F and $\mathbf{j}_\wp = 1$ otherwise, we have

$$\prod_{p \notin F} \mathbf{i}(\mathbf{i}_p, p) \in \mathbf{N_{K/k}}\,\mathbf{I_K} \subset \ker(\chi_\omega)$$

therefore

$$\chi\big(\phi_{\mathbf{K/k}}(\mathbf{i})\big)^v = \chi_\omega\left(\prod_{p \in F} \mathbf{i}(\mathbf{i}_p, p)\right) = \chi_\omega(\mathbf{i}) \qquad \text{for } \mathbf{i} \in \mathbf{I_k}\{E\}. \tag{4.17}$$

Since $\mathbf{I_k} = \mathbf{I_k}\{E\}\mathbf{k}^*\mathbf{N_{K/k}}\mathbf{I_K}$, then $\chi_\omega(\mathbf{i})$ is completely determined by its values at $\mathbf{i}$ in $\mathbf{I_k}\{E\}$. The n functions χ_ω are all distinct because if $\chi_{\omega_1} = \chi_{\omega_2}$ then $1 = \chi_{\omega_1}(\mathbf{i})\chi_{\omega_2}(\mathbf{i})^{-1} = \chi_{(\omega_1-\omega_2)}(\mathbf{i})$. But if $\omega_1 - \omega_2 \neq (0)$ then $\chi_{(\omega_1-\omega_2)}(\mathbf{i}) \neq 1$ for some $\mathbf{i}$ in $\mathbf{I_k}\{E\}$, so we must have $\omega_1 = \omega_2$. There are n homomorphisms χ_ω corresponding to n values of v, so the correspondence is one-to-one. There is therefore some ω_0 that corresponds to $v = 1$, and we have

$$\chi\big(\phi_{\mathbf{K/k}}(\mathbf{i})\big) = \chi_{\omega_0}(\mathbf{i}) \qquad \text{for } \mathbf{i} \in \mathbf{I_k}\{E\}. \tag{4.18}$$

The right side of (4.18) is defined for all $\mathbf{i}$ in $\mathbf{I_k}$. χ is an isomorphism from $G[\mathbf{K}:\mathbf{k}]$ to the n-th roots of unity. Define

$$\phi_{\mathbf{K/k}}(\mathbf{i}) = \chi^{-1}\big(\chi_{\omega_0}(\mathbf{i})\big) \qquad \text{for } \mathbf{i} \in \mathbf{I_k}. \tag{4.19}$$

This definition agrees with (2.1) for $\mathbf{i}$ in $\mathbf{I_k}\{E\}$ and the kernel contains $\mathbf{k}^*$. This completes the proof of theorem 1 for cyclic extensions.