CHAPTER XI

NORM RESIDUE SYMBOL FOR KUMMER EXTENSIONS

Throughout this chapter, \( p \) will denote a rational prime number; \( \wp \) will denote a prime of \( k \), and \( \wp' \) will denote a prime of an extension \( K \) of \( k \). Let \( m \) be a positive integer and let \( k \) contain the \( m \)-th roots of unity. The general \( m \)-power reciprocity law for elements in \( k \) has been found to be

\[
\left( \frac{\alpha}{\beta} \right)_m \left( \frac{\beta}{\alpha} \right)_m^{-1} = \prod_{\wp \in E} \left( \frac{\alpha, \beta}{\wp} \right)_m
\]

where \( E \) contains all primes of \( k \) dividing \( m \) and all infinite primes, and elements \( \alpha \) and \( \beta \) of \( k \) are relatively prime to each other and to \( m \). Our main objective will be to compute the symbol \( \left( \frac{\alpha, \beta}{\wp} \right)_p \) for odd primes \( p \) in the case \( k = \mathbb{Q}(\zeta) \) where \( \zeta \) is a primitive \( p \)-th root of unity, obtaining the \( p \)-th power reciprocity law in the process.

**Lemma 11.1.** Suppose that \( k \) contains the \( m \)-th roots of unity and \( \wp \) is an infinite prime of \( k \). Non-trivial norm residue symbols occur only if \( m = 2 \) and \( \wp \) is real, in which case we have

\[
\left( \frac{\alpha, \beta}{\wp} \right)_m = \begin{cases} 
1 & \text{if } \alpha > 0 \text{ or } \beta > 0, \\
-1 & \text{if } \alpha < 0 \text{ and } \beta < 0.
\end{cases}
\]

**Proof.** If \( m > 2 \) then all infinite primes of \( k \) are complex because \( k \) contains the \( m \)-th roots of unity.

**Norm residue symbol for composite powers.**

**Lemma 11.2.** Suppose that \( k \) contains the \( mn \)-th roots of unity, \( \wp \) is a finite prime of \( k \) and \( \alpha \) and \( \beta \) are elements of \( k^*_\wp \). Let \( m \) and \( n \) be relatively prime. If \( ma + nb = 1 \) then

\[
\left( \frac{\alpha, \beta}{\wp} \right)_{mn} = \left( \frac{\alpha, \beta}{\wp} \right)_m^b \left( \frac{\alpha}{\wp} \right)_n^a
\]

(11.1)
Proof. We can choose $\beta_0$ in $k^*$ sufficiently close to $\beta$ so that $\beta_0 \simeq_{\text{mn}} \beta$. Then $\beta$ may be replaced by $\beta_0$ in all norm residue symbol expressions, so we may as well suppose that $\beta$ is in $k^*$. For an integer $s$ dividing $mn$, let $\sigma_s$ be the norm residue symbol automorphism.

$$\sigma_s = \left( \frac{\alpha, k(\sqrt[\beta]{\beta})/k}{\varphi} \right)$$

We have $1/mn = a/n + b/m$, so $m^{\sqrt[\beta]{\beta}} = (\sqrt[\beta]{\beta})^b (\sqrt[\beta]{\beta})^a$. Since $\sigma_m$ and $\sigma_n$ are restrictions of $\sigma_{mn}$ to their respective subfields, then

$$\sigma_{mn} \left( m^{\sqrt[\beta]{\beta}} \right) = \sigma_{mn} \left( (\sqrt[\beta]{\beta})^b (\sqrt[\beta]{\beta})^a \right) = \left( \sigma_m (\sqrt[\beta]{\beta}) \right)^b \left( \sigma_n (\sqrt[\beta]{\beta}) \right)^a.$$ 

Therefore

$$\frac{\sigma_{mn} \left( m^{\sqrt[\beta]{\beta}} \right)}{m^{\sqrt[\beta]{\beta}}} = \left( \frac{\sigma_m (\sqrt[\beta]{\beta})}{\sqrt[\beta]{\beta}} \right)^b \left( \frac{\sigma_n (\sqrt[\beta]{\beta})}{\sqrt[\beta]{\beta}} \right)^a,$$

so

$$\left( \frac{\alpha, \beta}{\varphi} \right)_{mn} = \left( \frac{\alpha, \beta}{\varphi} \right)_m^b \left( \frac{\alpha, \beta}{\varphi} \right)_n^a.$$

Lemma 11.3. $k_\varphi$ contains the $(N\varphi - 1)$-th roots of unity.

Proof. Let $\zeta$ be a primitive $(N\varphi - 1)$-th root of unity. Then $k_\varphi(\zeta)/k_\varphi$ is unramified since $\varphi$ does not divide $N\varphi - 1$. Let $\varphi'$ be the prime of $k_\varphi(\zeta)$. In the map $O_{\varphi'} \to O_{\varphi'}/\varphi'$, element $\zeta$ maps to an element of $O_{\varphi'}/\varphi$ since $O_{\varphi'}/\varphi$ is the splitting field of $x^{N\varphi - 1} - 1$. This shows that $O_{\varphi'}/\varphi' = O_{\varphi}/\varphi$. Therefore $f = 1$, so $[k_\varphi(\zeta) : k_\varphi] = ef = 1$, and we have $k_\varphi(\zeta) = k_\varphi$.

Lemma 11.4. Let $V$ be the group of $(N\varphi - 1)$-th roots of unity in $k_\varphi$. Then the image of $V$ in $O_{\varphi}/\varphi$ is all of $(O_{\varphi}/\varphi)^*$.

Proof. If $v$ is in $V$ and $v \neq 1$, then $v$ is a root of $x^{N\varphi - 2} + \cdots + x + x = 0$. If $v = 1 \mod \varphi$ then we would have $N\varphi - 1 = 0 \mod \varphi$, which is impossible. Therefore the kernel of $V \to (O_{\varphi}/\varphi)^*$ is trivial, so the map is an isomorphism since both $V$ and $(O_{\varphi}/\varphi)^*$ have $(N\varphi - 1)$ elements.

Lemma 11.5. Let $\pi$ be an element of $k_\varphi^*$ such that $\varphi = (\pi)$. For fixed $\pi$, every element $\alpha$ of $k_\varphi^*$ has a unique representation as

$$\alpha = \pi^{a} v u \quad \text{where } v \in V \text{ and } u \in W_\varphi(1).$$

Therefore $k_\varphi^*$ is a direct product $\langle \pi \rangle V W_\varphi(1)$.

Proof. Exponent $a$ is determined by $a = \ord_\varphi(\alpha)$. Put $\alpha' = \alpha/\pi^a$. Then $\alpha'$ is in $u_\varphi$. By lemma 11.4, there is a unique element $v$ in $V$ so that $\alpha' = v(\mod \varphi)$. Then $u = \alpha'/v$ is in $W_\varphi(1)$. Since $\alpha'$ and $v$ are uniquely determined then so is $u$. 
Lemma 11.6. If $n$ is relatively prime to $N\varphi - 1$ then $V = V^n$ and the map $x \to x^n$ is an isomorphism of $(\mathcal{O}_\varphi/\varphi)^*$.

Proof. Let $a$ and $b$ be integers such that $na + (N\varphi - 1)b = 1$. Then $y \to y^a$ is inverse to $x \to x^n$, and we have $V \supset V^n \supset V^{na} = V$, so $V = V^n$.

The case of powers relatively prime to $\varphi$. Suppose that $n = p^r$ where $(p)$ is the rational prime divisible by $\varphi$ and $m$ is relatively prime to $p$. Lemma 11.2 shows how computation of the norm residue symbol for $mn$-th powers is reduced to separate computations for $m$-th powers and $p^r$-th powers. Lemma 11.7 gives an explicit formula for the former case.

Lemma 11.7. Let $\pi$ be an element of $k_\varphi^*$ such that $\varphi = (\pi)$. Suppose that $m$ is relatively prime to $\varphi$. If $\alpha = \pi^a v u$ and $\beta = \pi^b v' u'$ as in lemma 11.5, then

$$
\left( \frac{\alpha, \beta}{\varphi} \right)_m = \left( \frac{-1}{\varphi} \right)_m^{ab} (v)^{-b} \frac{N\varphi - 1}{m} (v')^a \frac{N\varphi - 1}{m}.
$$

Proof. Since $\varphi$ does not divide $m$ then we can apply lemma 10.9.

$$
\left( \frac{\alpha, \beta}{\varphi} \right)_m = \left( \frac{-1}{\varphi} \right)_m^{ab} \left( \frac{\beta^a/\alpha^b}{\varphi} \right)_m = \left( \frac{-1}{\varphi} \right)_m^{ab} \left( \frac{(v'u')^a / (vu)^b}{\varphi} \right)_m.
$$

We have $u = 1 \pmod{\varphi}$ and $u' = 1 \pmod{\varphi}$, so both $\left( \frac{u}{\varphi} \right)_m$ and $\left( \frac{u'}{\varphi} \right)_m$ are trivial. $\left( \frac{v}{\varphi} \right)_m$ is the unique $(N\varphi - 1)$-th root of unity such that $\left( \frac{v}{\varphi} \right)_m = v \frac{N\varphi - 1}{m} \pmod{\varphi}$. But $v$ is an $(N\varphi - 1)$-th root of unity, so $\left( \frac{v}{\varphi} \right)_m = (v)^{\frac{N\varphi - 1}{m}}$, and likewise $\left( \frac{v'}{\varphi} \right)_m = (v')^{\frac{N\varphi - 1}{m}}$.

The case of $p^r$-th powers where $\varphi$ divides $(p)$. Take $n = p^r$ where $\varphi$ divides $(p)$. Then $n$ is relatively prime to $N\varphi - 1$. Group $V$ is cyclic of order $N\varphi - 1$, so $V^n = V$, and every element of $V$ is a $n$-th power. Since every $n$-th power norm residue symbol involving an element $v$ in $V$ is trivial, we have

$$
(11.2) \quad \left( \frac{\alpha, \beta}{\varphi} \right)_n = \left( \frac{\pi^a v u, \pi^b v' u'}{\varphi} \right)_n = \left( \frac{\pi^a u, \pi^b u}{\varphi} \right)_n.
$$

To compute (11.2), it is only necessary to assume that $k$ contains the $n$-th roots of unity.
Lemma 11.8. Suppose that \( \wp \) is a prime of \( k \) and \( (p) \) is the rational prime that \( \wp \) divides. Let \( n = p^a \), and suppose that \( k \) contains the \( n \)-th roots of unity. Then \( W_\wp(1)/W_\wp(1)^n \) is the direct sum of \( d + 1 \) cyclic groups of order \( n \), where \( d = [k_\wp : Q_{(p)}] \).

Proof. Every element of \( W_\wp(1)/W_\wp(1)^n \) has order dividing \( n \), so the group is the direct product of cyclic subgroups each having order dividing \( n \). Let \( \alpha \) map to a generator of any one of these cyclic subgroups having order \( n' = p^b \). Then \( y \leq x \), and \( \alpha^{n'} \) is in \( W_\wp(1)^n \), so \( \alpha^{n'} = \beta^n \) for some element \( \beta \) in \( W_\wp(1) \). Suppose that \( y < x \). Then \( \alpha^{n'} = (\beta^{p^{x-y}})^p \), so \( \alpha = \beta^{p^{x-y}} \zeta' \), where \( \zeta' \) is a \( p^y \)-th root of unity. Since \( k \) contains the \( p^x \)-th roots of unity then \( \zeta' = \zeta^{p^{x-y}} \) where \( \zeta \) is some \( p^x \)-th root of unity, and we have \( \alpha = (\beta \zeta)^{p^{x-y}} \). But \( \alpha \) cannot be a \( p \)-th power, so it impossible to have \( y < x \). Therefore each cyclic subgroup in the direct product has order exactly \( p^x \). By lemma 11.5, \( u_\wp \) is a direct product \( VW_\wp(1) \). Since \( N_\wp - 1 \) and \( n = p^x \) are relatively prime then \( V^n = V \). We therefore have

\[
\frac{u_\wp}{u_\wp^n} = \frac{VW_\wp(1)}{VW_\wp(1)^n} = \frac{W_\wp(1)}{W_\wp(1)^n} = \frac{W_\wp(1)}{W_\wp(1)^n}.
\]

Since \( [k_\wp : Q_{(p)}] = d \) and \( n = p^x \), we have \( |n|_\wp = \left| N_{k_\wp/Q_{(p)}} n \right|_p = |n|^d = n^{-d} \). By lemma 8.11, we have \( [u_\wp : u_\wp^n] = n|n|^{-1} \), so

\[
[W_\wp(1) : W_\wp(1)^n] = [u_\wp : u_\wp^n] = n(n^d) = n^{d+1}.
\]

Therefore \( W_\wp(1)/W_\wp(1)^n \) must be the product of \( d + 1 \) cyclic groups of order \( n \).

Definition. An element \( \alpha \) in \( W_\wp(1) \) is \( n \)-primary if \( k_\wp(\sqrt[\wp]{\alpha})/k_\wp \) is unramified.

Lemma 11.9. With the hypothesis of lemma 11.8, the image in \( W_\wp(1)/W_\wp(1)^n \) of the set of \( n \)-primary elements is a cyclic group of order \( n \).

Proof. Since \( k_\wp^n \) is a direct product \( \langle \pi \rangle VW_\wp(1) \) and \( V = V^n \) we have

\[
\frac{k_\wp^n}{(k_\wp^n)^n} = \frac{\langle \pi \rangle VW_\wp(1)}{\langle \pi^n \rangle VW_\wp(1)^n} = \frac{\langle \pi \rangle}{\langle \pi^n \rangle} \times \frac{W_\wp(1)}{W_\wp(1)^n}.
\]

By lemma 11.8, \( k_\wp^n/(k_\wp^n)^n \) is the direct sum of \( d + 2 \) cyclic groups of order \( n \), where \( d = [k_\wp : Q_{(p)}] \). Let \( \beta_1, \ldots, \beta_{d+2} \) be a set of generators for \( k_\wp/(k_\wp^n)^n \), and the \( \beta_i \) may be chosen to be elements of \( k^* \). The \( \beta_i \) are independent modulo \( n \), so by lemma 8.5 the extension \( k_\wp(\sqrt[\wp]{\beta_1}, \ldots, \sqrt[\wp]{\beta_{d+2}}) \) of \( k_\wp \) has degree \( n^{d+2} \), with Galois
group isomorphic to the direct sum of the $d + 2$ Galois groups $G(k_\wp(\sqrt[d] x) : k_\wp)$, where $1 \leq i \leq d + 2$. Every extension of the form $k_\wp(\sqrt[d] x)$ where $\beta$ is in $k_\wp^*$ is a subfield of $k_\wp(\sqrt[x]{\beta}, \ldots, \sqrt[x]{\beta_{d+2}})$. Put $K = k(\sqrt[x]1, \ldots, \sqrt[x]{\beta_{d+2}})$. The kernel of $\alpha \to (\alpha_1/k_\wp) = n^{d+2}$ in $K$ and contains $(k_\wp^*)^n$. Since $[k_\wp^* : (k_\wp^*)^n] = n^{d+2}$, then the kernel is exactly $(k_\wp^*)^n$.

Let $H$ be the image in $G = G(k_\wp(\sqrt[x]1, \ldots, \sqrt[x]{\beta_{d+2}}) : k_\wp)$ of the units $u_\wp$ of $k_\wp$. An element $\beta$ of $k_\wp^*$ is in the fixed field of $H$ if and only if $(\alpha_1/k_\wp)_n = \sqrt[x]1$ for every $\alpha$ in $u_\wp$, which is if and only if $\sqrt[x]1$ is in $k_\wp(\sqrt[x]1)$, so $\sqrt[x]1$ is the smallest positive value of $x$ such that $\gamma_2 \simeq 1$. Let $\gamma_2 = c/nq + r$ and $0 \leq r < n$. Put $\gamma_1 = \gamma_2 / \pi^n$. Then $\gamma_2 = \gamma_1$, so the fixed field of $H$ is $k_\wp(\sqrt[x]1)$, and $(\gamma_1) = \varphi^r$. The map $\alpha \to (\alpha_1/k_\wp)_n$ is a homomorphism $k_\wp^* \to G(k_\wp(\sqrt[x]1) : k_\wp)$. The kernel has index $n$ in $W_\wp$ and contains $u_\wp(k_\wp^*)^n$, so the kernel is exactly $u_\wp(k_\wp^*)^n$.

Since $-1$ is in $u_\wp$, we have

$$(\gamma_1, \gamma_1) = (\gamma_2, 1) = (\gamma_2, \gamma_1) = (1, 1) = 1.$$
Lemma 11.10. With the hypothesis of lemma 11.8, choose a fixed element \( \pi \) so that \( \varphi = (\pi) \). Put

\[
W_\pi = \left\{ \alpha \in W_\varphi(1) \mid \left( \frac{\pi, \alpha}{\varphi} \right)_n = 1 \right\}.
\]

Let \( \gamma_0 \) in \( W_\varphi(1) \) be a generator of group the \( n \)-primary elements modulo \( W_\varphi(1)^n \) and let \( \gamma_0 \) be the coset \( \gamma_0 W_\varphi(1)^n \). Then \( W_\varphi(1)/W_\varphi(1)^n \) is a direct product

\[
\frac{W_\varphi(1)}{W_\varphi(1)^n} = \frac{W_\pi}{W_\pi(1)^n} \times \langle \gamma_0 \rangle.
\]

Proof. Suppose that \( \alpha \) is \( n \)-primary and in \( W_\pi \). Then \( \left( \frac{\beta, \alpha}{\varphi} \right)_n = 1 \) for every element \( \beta \) of \( k^*_\varphi \), and in particular for a set of generators \( \beta_1, \ldots, \beta_{d+2} \) generators of \( k^*_\varphi/k^*_\varphi \). Therefore for \( 1 \leq i \leq d+2 \), the norm residue symbols \( \left( \frac{\alpha, k_\varphi(\sqrt{\beta_i})/k_\varphi}{\varphi} \right)_n \) are trivial, so \( \left( \frac{\alpha, k_\varphi(\sqrt{\beta_1}, \ldots, \sqrt{\beta_{d+2}})/k_\varphi}{\varphi} \right)_n \) is trivial by lemma 8.5, and therefore \( \alpha \) is in \( (k^*_\varphi)^n \cap W_\varphi(1) \). Then \( \alpha = v^n w^n \) with \( v \) in \( V_\varphi \) and \( u \) in \( W_\varphi(1) \). We have \( v^n = 1 \mod \varphi \), so \( v = 1 \), and therefore \( \alpha \) is in \( W_\varphi(1)^n \). We have shown that \( W_\varphi(1)/W_\varphi(1)^n \cap \langle \gamma_0 \rangle \) is a trivial group.

Now suppose that \( \alpha \) is an arbitrary element of \( W_\varphi(1) \). It remains to show that \( W_\pi \) and \( \gamma_0 \) generate \( W_\varphi(1) \) modulo \( W_\varphi(1)^n \). Since \( k_\varphi(\sqrt{\gamma_0}) \) has degree \( n \) over \( k_\varphi \), then there exists an element \( \beta \) in \( k^*_\varphi \) such that \( \left( \frac{\beta, \gamma_0}{\varphi} \right)_n \) is a primitive \( n \)-th root of unity. Let \( \beta = \pi^b v \). Then \( \left( \frac{\beta, \gamma_0}{\varphi} \right)_n = \left( \frac{\pi^b, \gamma_0}{\varphi} \right)_n \), so \( \pi \gamma_0 \) must be a primitive \( n \)-th root of unity. There exists an \( a \) so that \( \left( \frac{\pi, \alpha}{\varphi} \right)_n = \left( \frac{\pi, \gamma_0}{\varphi} \right)_n \). We have \( \alpha = (\alpha \gamma_0^{-a}) \gamma_0^a \). Then \( \alpha \gamma_0^{-a} \) is in \( W_\pi \) because \( \left( \frac{\pi, \alpha \gamma_0^{-a}}{\varphi} \right)_n = \left( \frac{\pi, \alpha}{\varphi} \right)_n \left( \frac{\pi, \gamma_0}{\varphi} \right)_n^{-a} = 1 \). This completes the proof of the lemma.

The computation of the norm residue symbol for \( p^2 \)-th powers has been reduced to the following. An element \( \alpha \) of \( k^*_\varphi \) may be expressed as \( x = \pi^a v w \) where \( v \) is in \( V_\varphi \) and \( w \) is in \( W_\varphi(1) \). Let \( w \simeq_n u_0 \gamma_0^{a'} \) with \( u \) in \( W_\pi \). Likewise, let \( \beta \) in \( k^*_\varphi \) be expressed as \( \beta = \pi^b v' w' \) where \( v' \) is in \( V_\varphi \) and \( w' \simeq_n u'_0 \gamma_0^{b'} \) with \( u' \) in \( W_\pi \). Then

\[
\left( \frac{x, y}{\varphi} \right)_n = \left( \frac{\pi^a v u_0 \gamma_0^{a'}, \pi^b v' u'_0 \gamma_0^{b'}}{\varphi} \right)_n = \left( \frac{\pi, \pi}{\varphi} \right)_n \left( \frac{\pi, \gamma_0}{\varphi} \right)_n \left( \frac{u, u'}{\varphi} \right)_n \left( \frac{\gamma_0, \pi}{\varphi} \right)_n \left( \frac{\beta a'}{\varphi} \right)_n.
\]
Therefore

\[ \left( \frac{x, y}{\wp} \right)_n = \left( \frac{\pi, -1}{\wp} \right)_n^{ab} \left( \frac{\pi, \gamma_0}{\wp} \right)_n^{ab' - ba'} \left( \frac{u, u'}{\wp} \right)_n \]

The problems that remain are essentially two.

1. Find a generator \( \gamma_0 \) for the \( n \)-primary elements and calculate \( \left( \frac{\pi, \gamma_0}{\wp} \right)_n \).

2. Find a basis \( v_1, \ldots, v_d \) of \( W_\wp \mod W_\wp(1)^n \) and calculate \( \left( \frac{v_i, v_j}{\wp} \right)_n \).

**The \( p \)-primary elements for odd primes.** We specialize to the case \( n = p \) and \( p > 2 \). Let \( k = \mathbb{Q}(\zeta) \) where \( \zeta \) is a primitive \( p \)-th root of unity. Then \( [k : \mathbb{Q}] = p - 1 \). The prime \( (p) \) is completely ramified in \( k \); if \( \pi = 1 - \zeta \) then \( (p) = \wp^{p-1} \) where \( \wp = (\pi) \). We have \( [k_\wp : \mathbb{Q}(p)] = p - 1 \) with ramification index \( e = p - 1 \); since \( f = 1 \) then the rational integers \( 0, 1, \ldots, p - 1 \) are a complete residue system for \( \mathfrak{o}_\wp / \wp \).

**Lemma 11.11.** \( [W_\wp(1) : W_\wp(k + 1)] = p^k \)

**Proof.** Every element of \( W_\wp(1) \) may be uniquely represented modulo \( \pi^{k+1} \) by \( 1 + a_1\pi + a_2\pi^2 + \cdots + a_k\pi^k \) with coefficients \( a_i \) belonging to a complete residue system for \( \mathfrak{o}_\wp / \wp \). There are \( p^k \) choices for the coefficients \( a_1, \ldots, a_k \).

**Lemma 11.12.** \( W_\wp(1)^p = W_\wp(p + 1) \)

**Proof.** Let \( b = \text{ord}_\wp(p) \). By lemma 4.13, every element \( x \) of \( k_\wp \) such that \( \text{ord}_\wp(x) > b/(p - 1) \) + \( \text{ord}_\wp(p) \) is the \( p \)-th power of some element \( y \) in \( k_\wp \) such that \( \text{ord}_\wp(y) > b/(p - 1) \). Since \( \text{ord}_\wp(p) = p - 1 \), then every \( x \) such that \( \text{ord}_\wp(x) > p \) is the \( p \)-th power of some \( y \) such that \( \text{ord}_\wp(y) > 1 \), that is \( W_\wp(p + 1) \subset W_\wp(2)^p \). Let \( V_\wp = \langle \zeta \rangle \) be the group of \( p \)-power roots of unity. Since \( \zeta = 1(\mod \wp) \) then

\[ W_\wp(p + 1) \subset W_\wp(2)^p \subset (W_\wp(2)V_\wp)^p \subset W_\wp(1)^p \subset W_\wp(1) \]

By lemma 11.8 and lemma 11.11, subgroups \( W_\wp(p + 1) \) and \( W_\wp(1)^p \) both have index \( p^p \) in \( W_\wp(1) \), so the two must coincide.

**Lemma 11.13.** If element \( \alpha \) of \( k_\wp \) is in \( W_\wp(p) \) then \( \frac{\sqrt[p]{\pi - 1}}{\pi} \) is integral over \( \mathfrak{o}_\wp \).

**Proof.** The element in question is a root of polynomial \( (p\pi)^{-1}((\pi x + 1)^p - \alpha) \) having coefficients in \( k_\wp \), and

\[ \frac{(\pi x + 1)^p - \alpha}{p\pi} = \frac{p\pi}{p\pi} x^p + \frac{(p)^p}{p\pi} x^{p-1} + \cdots + \frac{(p-1)^p}{p\pi} \pi x + \frac{1 - \alpha}{p\pi} \]

The leading coefficient is a unit and the other coefficients except possibly the constant term are elements of \( \mathfrak{o}_\wp \). If \( \alpha = 1(\mod \wp^p) \) then the constant term is also in \( \mathfrak{o}_\wp \).
Lemma 11.14. Let \( \alpha \) of \( k_{\wp} \) be in \( W_{\wp}(1) \). Then \( \alpha \) is \( p \)-primary if and only if \( \alpha \) is in \( W_{\wp}(p) \).

Proof. Let \( P \) be the group of \( p \)-primary elements in \( W_{\wp}(1) \). Then we have \([W_{\wp}(1) : W_{\wp}(1)^p] = p^p\) and \([P : W_{\wp}(1)^p] = p\) by lemma 11.8 and lemma 11.9, so \([W_{\wp}(1) : P] = p^{p-1}\). Also we have \([W_{\wp}(1) : W_{\wp}(p)] = p^p\) by lemma 11.11, so it will be enough to show that \( W_{\wp}(p) \) is contained in \( P \), i.e. \( k_{\wp}(\sqrt[p]{\alpha})/k_{\wp} \) is unramified if \( \alpha \equiv 1 \pmod{\wp} \). Let \( \tau \) be an automorphism in the inertial subgroup of \( G(k_{\wp}(\sqrt[p]{\alpha}) : k_{\wp}) \), and let \( \tau(\sqrt[p]{\alpha}) = \zeta'\sqrt[p]{\alpha} \) where \( \zeta' \) is a \( p \)-th root of unity. (We need to show that \( \zeta' \) must be 1.) Let \( \wp' \) be the prime of \( k_{\wp}(\sqrt[p]{\alpha}) \) dividing \( \wp \). Then \( \tau(\gamma) = \gamma \pmod{\wp'} \) for every \( \gamma \) that is integral over \( o_{\wp} \). The element \((\sqrt[p]{\alpha} - 1)/\pi\) is integral over \( o_{\wp} \) by lemma 11.13, so we have

\[
\frac{\zeta'\sqrt[p]{\alpha} - 1}{\pi} = \frac{\sqrt[p]{\alpha} - 1}{\pi} \pmod{\wp'}.
\]

Therefore

\[
\frac{(\zeta' - 1)\sqrt[p]{\alpha}}{\pi} = 0 \pmod{\wp'}.
\]

If \( \zeta' \neq 1 \) then \((\zeta' - 1)/\pi\) is a unit, but that is impossible since \( \sqrt[p]{\alpha} \) is also a unit. This shows that \( \zeta' = 1 \), the inertial group is trivial, and \( k_{\wp}(\sqrt[p]{\alpha})/k_{\wp} \) is unramified, which concludes the proof.

Lemma 11.15. With \( \pi = 1 - \zeta \) we have

\[
\zeta^i = 1 - i\pi \pmod{\wp^2} \quad \text{and} \quad \frac{\pi^{p-1}}{p} = -1 \pmod{\wp}.
\]

Proof. Since \( \zeta \equiv 1 \pmod{\wp} \) then, for \( 1 \leq i < p \), we have

\[
\frac{1 - \zeta^i}{1 - \zeta} = 1 + \zeta + \cdots + \zeta^{i-1} = i \pmod{\wp},
\]

so \( 1 - \zeta^i = i\pi \pmod{\wp^2} \), which establishes the first conclusion. For the second, substitute \( x = 1 \) in \( x^{p-1} + \cdots + x + 1 = (x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{p-1}) \) to obtain

(11.3)

\[
p = (1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{p-1}).
\]

Therefore

\[
\frac{\pi^{p-1}}{p} = \frac{(1 - \zeta)(1 - \zeta) \cdots (1 - \zeta)}{(1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{p-1})} = \frac{1}{(p-1)!} \pmod{\wp}.
\]

Since \((p-1)! = -1 \pmod{p}\) then the second conclusion follows.
Lemma 11.16. If $\alpha$ in $k_\varphi$ is a $p$-primary element, there is a rational integer $a$ such that $0 \leq a < p$ and $\alpha = 1 + ap\pi \pmod{\varphi^{p+1}}$. With $\pi = 1 - \zeta$, we have

\[
\left( \frac{\pi, \alpha}{\varphi} \right)_p = \zeta^a.
\]

Proof. Let $\alpha$ be $p$-primary. There is an integer $a$ so that $\alpha = 1 + ap\pi$ modulo $\varphi^{p+1}$ since the integers $0, 1, \ldots, p - 1$ are a complete residue system for $\mathcal{O}_\varphi/\varphi$. We can choose an element $\alpha'$ in $k$ that is sufficiently close to $\alpha$ so that $\alpha' \simeq_p \alpha$ and $\alpha' = \alpha \pmod{\varphi^{p+1}}$, so we may assume that $\alpha$ is in $k$. In that case, put $K = k(\sqrt[p]{\alpha})$ and let $\varphi'$ be a prime of $K$ dividing $\varphi$. If $\alpha$ is $p$-primary then $\varphi$ is unramified in $K$ so in the completion we have $\varphi' = \varphi \mathcal{O}_{\varphi'}$ and therefore $\varphi' = (\varphi)$. Put

\[
\sqrt[p]{\alpha} = 1 + b\pi \quad \text{where } b \in \mathcal{O}_{\varphi'}.
\]

Then

\[
\alpha = (1 + b\pi)^p = 1 + pb\pi + b^p\pi^p \pmod{\varphi^{p+1}}.
\]

By lemma 11.15, $\pi^p = -p\pi \pmod{\varphi^{p+1}}$, so $\pi^p = -p\pi \pmod{\varphi^{p+1}}$, and

\[
\alpha = 1 + pb\pi - b^p\pi^p \pmod{\varphi^{p+1}}.
\]

Therefore we have

\[(11.4) \quad a = b - b^p \pmod{\varphi'}.
\]

Let $\left( \frac{\pi, \alpha}{\varphi} \right)_p \sqrt[p]{\alpha} = \zeta^a \sqrt[p]{\alpha}$. Since $K/k$ is unramified then we have

\[
\left( \frac{\pi, K/k}{\varphi} \right) = \phi_{K/k}(i(\pi, \varphi, k)) = \left( \frac{K/k}{\varphi} \right).
\]

and therefore for any $\beta$ in $\mathcal{O}_{\varphi'}$ we have

\[
\left( \frac{\pi, K/k}{\varphi} \right) \beta = \beta^{N\varphi} = \beta^p \pmod{\varphi'}.
\]

Choose $\beta = (\sqrt[p]{\alpha} - 1)/\pi$, which is in $\mathcal{O}_{\varphi'}$ by lemma 11.13. Then

\[
\left( \frac{\pi, K/k}{\varphi} \right) \beta = \frac{\zeta^a \sqrt[p]{\alpha} - 1}{\pi},
\]
so
\[ \frac{\zeta^a \sqrt[p]{\alpha} - 1}{\pi} = \left( \frac{\sqrt[p]{\alpha} - 1}{\pi} \right)^p = \beta^p (\text{mod } \wp'). \]

We have \( \zeta^a = 1 - a'\pi (\text{mod } \wp^2) \) by lemma 11.15, so
\[ \frac{(1 - a'\pi)(1 + b\pi) - 1}{\pi} = b^p (\text{mod } \wp'). \]

This shows that \( -a' + b = b^p (\text{mod } \wp') \), or \( a' = b - b^p (\text{mod } \wp') \). Comparison with (11.4) shows \( a = a' (\text{mod } \wp') \). Both \( a \) and \( a' \) are rational integers, so have
\[ a = a' (\text{mod } p), \]
which completes the proof of the lemma.

We have solved the first basic problem for prime \( p \). The generator of the \( p \)-primary elements modulo \( W_\wp W(p + 1) = \gamma_0 = 1 + p\pi \), and
\[ \left( \frac{\pi, \gamma_0}{\wp} \right)_p = \zeta \quad \text{where } \pi = 1 - \zeta. \]

**Generators of \( W_\wp W(1)^p \) and the \( p \)-th power reciprocity law.** If we can find a set of generators \( u_1, \ldots, u_{p-1} \) for \( W_\wp(1)/W_\wp(p) \), then every element \( \alpha \) of \( W_\wp(1) \) will be expressible as \( \alpha = u_1^{t_1} \ldots u_{p-1}^{t_{p-1}} \gamma_0 (\text{mod } \wp^{p+1}) \), so if \( \left( \frac{\pi, u_i}{\wp} \right) = \zeta^{c_i} \) then we will have
\[ W_\wp = \{ \alpha \in W_\wp(1) \mid c_1 t_1 + \ldots + c_{p-1} t_{p-1} + t_0 = 0 (\text{mod } p) \}. \]

The constants \( c_i \) will be determined in the last section.

**Lemma 11.17.** If \( r \) is a primitive root modulo \( p \) then
\[ r^i \prod_{k=1, k \neq i}^{p-1} (r^i - r^k) = -1 (\text{mod } p). \]

**Proof.** Since \( r, r^2, \ldots, r^{p-1} \) form a reduced residue system modulo \( p \), then
\[ \prod_{k=1}^{p-1} (x - r^k) = x^{p-1} - 1 (\text{mod } p). \]
Then
\[
\frac{d}{dx} \prod_{k=1}^{p-1} (x - r^k) = \frac{d}{dx} (x^{p-1} - 1) \pmod{p},
\]
or
\[
\sum_{i=1}^{p-1} \prod_{k \neq i} (x - r^k) = (p-1)x^{p-2} \pmod{p}.
\]

Set \( x = r^i \) and multiply both sides by \( r^i \) to obtain the desired result.
\[
r^i \prod_{k \neq i}^{p-1} (r^i - r^k) = (p-1)r^i(p-1) = -1 \pmod{p}.
\]

**Lemma 11.18.** Let \( \sigma \) be a generator of \( G(K_p : Q(p)) \) and let \( \zeta^\sigma = \zeta^r. \) Then \( r \) is a primitive root modulo \( p. \) For \( i = 1, \ldots, p-1, \) set
\[
u_i = (1 - \pi^i)r^i(\sigma - r)(\sigma - r^2) \cdots (\sigma - r^{i-1})(\sigma - r^{i+1}) \cdots (\sigma - r^{p-1})
\]

Then
\[
u_i^\sigma \equiv_p u_i r_i \quad \text{and} \quad \nu_i = 1 - \pi^i \pmod{\wp^{i+1}}.
\]

**Proof.** If \( f(x) \) and \( g(x) \) are polynomials in \( \mathbb{Z}[x] \) and \( f(x) = g(x) \pmod{p} \) then \( \alpha^f(\sigma) \equiv_p \alpha^g(\sigma) \) for \( \alpha \) in \( K^*. \) Since \( f(x) = (x-r)(x-r^2) \cdots (x-r^{p-1}) \) is a polynomial of degree \( p-1 \) having roots \( 1, 2, \ldots, p-1, \pmod{p}, \) then \( f(x) = x^{p-1} - 1 \pmod{p}. \) Therefore \( \alpha^f(\sigma) \equiv_p 1. \) We have \( \nu_i^\sigma - r^i = (1 - \pi^i)^{-r^i}f(\sigma) \equiv_p 1, \) so \( \nu_i^\sigma \equiv_p u_i r_i, \) which is the first part of the lemma. For the second part, we have \( \pi = 1 - \zeta, \) so
\[
\pi^\sigma = 1 - \zeta^\sigma = 1 - \zeta^r = (1 - (1 - \pi)^r) = r\pi \pmod{\wp^2}.
\]

Put \( \pi^\sigma = r\pi + \beta \pi^2. \) Then \( (\pi^\sigma)^i = (r\pi + \beta \pi^2)^i = r^i\pi^i \pmod{\wp^{i+1}}, \) so
\[
(\pi^i)^\sigma = r^i\pi^i \pmod{\wp^{i+1}}.
\]

Before proceeding further, we make the following observation. If \( j_1, \ldots, j_{s+1} \) are any given integers, then we have
\[
(1 + r^i(r^i - r^{j_1}) \cdots (r^i - r^{j_s})\pi^i)^{\sigma - r^{j_{s+1}}}
\]
\[
= (1 + r^i(r^i - r^{j_1}) \cdots (r^i - r^{j_s})\pi^i)^\sigma (1 + r^i(r^i - r^{j_1}) \cdots (r^i - r^{j_s})\pi^i)^{-r^{j_{s+1}}}
\]
\[
= (1 + r^i(r^i - r^{j_1}) \cdots (r^i - r^{j_s})r^i\pi^i) \quad (1 - r^i(r^i - r^{j_1}) \cdots (r^i - r^{j_s})r^{j_{s+1}}\pi^i)^{-1} \pmod{\wp^{i+1}}
\]
\[
= (1 + r^i(r^i - r^{j_1}) \cdots (r^i - r^{j_s})(r^i - r^{j_{s+1}})\pi^i) \pmod{\wp^{i+1}}
\]
To compute $u_i$, we start from $(1 - \pi^i)^{-r^i} = 1 + r^i\pi^i(\text{mod } \wp^{i+1})$, then successively apply $\sigma - r$, $\sigma - r^2$, up to $\sigma - r^{p-1}$, but omit $\sigma - r^i$. By applying the above observation at each step, we arrive at

$$u_i = (1 + r^i(r^i - r) \ldots (r^i - r^{i-1})(r^i - r^{i+1}) \ldots (r^i - r^{p-1})\pi^i)(\text{mod } \wp^{i+1}).$$

By lemma 11.17, we obtain $u_i = 1 - \pi^i(\text{mod } \wp^{i+1})$, which completes the proof.

**Lemma 11.19.** For $1 \leq i \leq p - 1$ and $1 \leq j \leq p - 1$, we have

$$(u_i, u_j)_{\wp^p} = \begin{cases} \zeta^{-i} & \text{if } i + j = p \\ 0 & \text{if } i + j \neq p \end{cases}$$

**Proof.** We apply automorphisms on the left in this proof, so we have $\sigma\zeta = \zeta r$ and $\sigma u_i \simeq p u_i^r$. First, we have

$$(11.5) \quad (\frac{\sigma u_i, \sigma u_j}{\wp})_{\wp^p} = (\frac{u_i^r, u_j^r}{\wp})_{\wp^p} = (\frac{u_i, u_j}{\wp})_{\wp^p}^{r^{-i+j}}.$$  

We also have

$$\left(\frac{\sigma u_i, \sigma u_j}{\wp}\right)_{\wp^{\sqrt{\wp}}} = \left(\frac{\sigma u_i, k(\sqrt{\wp}u_j)/k}{\wp}\right)_{\wp^{\sqrt{\wp}}}.$$  

Automorphism $\sigma : k \to k$ may be extended to an isomorphism $\sigma : k(\wp^{\sqrt{\wp}}) \to k(\wp^{\sqrt{\wp}})$. (In the notation of lemma 10.43, we have $K = k(\sqrt{\wp})$, $K' = k(\wp^{\sqrt{\wp}})$, $k' = k$, and $\wp' = \wp$.) Since $(\sigma \sqrt{u_j})^p = \sigma u_j$, then $\sigma \sqrt{u_j}$ is a root of $x^p - \sigma u_j$, and we may write $\sigma \sqrt{u_j} = \sqrt{\wp}u_j$. (The particular choice of $\sqrt{\wp}u_j$ determines the extension of $\sigma$.) Using the notation of lemma 10.43, we have

$$\left(\frac{\sigma u_i, k(\wp^{\sqrt{\wp}})/k}{\wp}\right) = \left(\frac{u_i, K'/k'}{\wp'}\right) = \sigma \left(\frac{u_i, K/k}{\wp}\right)^{-1} = \sigma \left(\frac{u_i, k(\sqrt{u_j})/\wp}{\wp}\right)^{-1}.$$  

Therefore

$$\left(\frac{\sigma u_i, k(\sqrt{\wp}u_j)/\wp}{\wp}\right)_{\wp^{\sqrt{\wp}}} = \sigma \left(\frac{u_i, k(\sqrt{\wp}u_j)/\wp}{\wp}\right)^{-1} = \sigma \left(\frac{u_i, u_j}{\wp}\right)^{r} \sqrt{\wp}u_j.$$
or

\[ \left( \frac{\sigma u_i, \sigma u_j}{\wp} \right)_p = \left( \frac{u_i, u_j}{\wp} \right)_p^r \]

Comparison with (11.5) shows that

\[ \left( \frac{u_i, u_j}{\wp} \right)_p^r \frac{1}{\wp} = \left( \frac{u_i, u_j}{\wp} \right)_p^{r+i+j} \]

If \( \left( \frac{u_i, u_j}{\wp} \right)_p \neq 1 \), then we must have \( r = i+j (\mod p) \), so \( 1 = i + j (\mod p - 1) \). For \( i \) and \( j \) in the range \( 1 \leq i \leq p-1 \) and \( 1 \leq j \leq p-1 \), the only value of \( i + j \) which satisfies the condition \( 1 = i + j (\mod p - 1) \) is \( i + j = p \). So far, we have established that

\[ \left( \frac{u_i, u_j}{\wp} \right)_p = 0 \quad \text{if } i + j \neq p. \]

We need to compute \( \left( \frac{u_i, u_{p-i}}{\wp} \right)_p \). Since \( u_k = 1 - \pi^k (\mod \wp^{k+1}) \) for \( 1 \leq k < p \), and \( \gamma_0 = 1 + p\pi \), then we can find integers \( a_k \) for \( i + 1 \leq k \leq p \) such that \( 0 \leq a_k < p \) and

\[ 1 - \pi^i = u_i u_{i+1}^{a_{i+1}} \ldots u_{p-1}^{a_{p-1}} \gamma_0^{a_p} (\mod \wp^{p+1}). \]

Likewise, we can find integers \( b_\ell \) for \( p-i + 1 \leq \ell \leq p \) such that \( 0 \leq b_\ell < p \) and

\[ 1 - \pi^{p-i} = u_{p-i} u_{p-i+1}^{b_{p-i+1}} \ldots u_{p-1}^{b_{p-1}} \gamma_0^b (\mod \wp^{p+1}). \]

Since \( \left( \frac{u_i, u_j}{\wp} \right)_p = 0 \) unless \( i + j = p \), and since \( \gamma_0 \) is \( p \)-primary, we have

\[ (11.6) \quad \left( \frac{1 - \pi^i, 1 - \pi^{p-i}}{\wp} \right)_p = \left( \frac{u_i u_{i+1}^{a_{i+1}} \ldots u_{p-1}^{a_{p-1}} \gamma_0^{a_p} u_{p-i} u_{p-i+1}^{b_{p-i+1}} \ldots u_{p-1}^{b_{p-1}} \gamma_0^b}{\wp} \right)_p = \left( \frac{u_i, u_{p-i}}{\wp} \right)_p. \]

The problem now is to compute \( \left( \frac{1 - \pi^i, 1 - \pi^{p-i}}{\wp} \right)_p \). Suppose that \( \alpha + \beta = \gamma \), and put \( \mu = \alpha / \gamma \). Then \( 1 - \mu = \beta / \gamma \). By lemma 10.6(f), we have

\[ 1 = \left( \frac{1 - \mu, \mu}{\wp} \right)_p = \left( \frac{\beta, \alpha}{\wp} \right)_p \left( \frac{\beta, \gamma}{\wp} \right)^{-1} \left( \frac{\gamma, \alpha}{\wp} \right)^{-1} \left( \frac{\gamma, \gamma}{\wp} \right)_p. \]
Since \( \left( \frac{\alpha \gamma}{\psi} \right)_p = 1 \) for \( p > 2 \), we have

\[
\left( \frac{\beta, \alpha}{\varphi} \right)_p = \left( \frac{\beta, \gamma}{\varphi} \right)_p \left( \frac{\gamma, \alpha}{\varphi} \right)_p.
\]

Choose \( \alpha = \pi^{p-i}(1 - \pi^i) \) and \( \beta = 1 - \pi^p \). Then \( \gamma = 1 - \pi^p \), and we have

\[
\left( \frac{1 - \pi^{p-i}, \pi^{p-i}(1 - \pi^i)}{\varphi} \right)_p = \left( \frac{1 - \pi^{p-i}, 1 - \pi^p}{\varphi} \right)_p \left( \frac{1 - \pi^p, \pi^{p-i}(1 - \pi^i)}{\varphi} \right)_p.
\]

Apply lemma 10.6(f) to the left side, and apply the fact that \( 1 - \pi^p \) is \( p \)-primary (annihilates units) to the right to obtain

\[
\left( \frac{1 - \pi^{p-i}, 1 - \pi^i}{\varphi} \right)_p = \left( \frac{1 - \pi^p, \pi^{p-i}}{\varphi} \right)_p.
\]

We have \( 1 - \pi^p = 1 + p\pi \pmod{\varphi^{p+1}} \) by lemma 11.15, so

\[
\left( \frac{1 - \pi^i, 1 - \pi^{p-i}}{\varphi} \right)_p = \left( \frac{\pi^{p-i}, 1 + p\pi}{\varphi} \right)_p.
\]

Apply (11.6) on the left side, and apply lemma 11.16 on the right to obtain

\[
\left( \frac{u_i, u_{p-i}}{\varphi} \right)_p = \zeta^{p-i} = \zeta^{-i}.
\]

The completes the proof of lemma 11.19.

**Theorem 11.20 - Reciprocity Law for Odd Prime Powers.** If \( \alpha \) and \( \beta \) are elements of \( \mathcal{W}_{\varphi}(1) \), then let \( a_i \) and \( b_i \) \( (1 \leq i < p) \) be integers such that \( 0 \leq a_i < p \) and \( 0 \leq b_i < p \) and

\[
\alpha = u_1^{a_1} \ldots u_{p-1}^{a_{p-1}} \pmod{\varphi^p} \quad \text{and} \quad \beta = u_1^{b_1} \ldots u_{p-1}^{b_{p-1}} \pmod{\varphi^p}.
\]

Then

\[
\left( \frac{\alpha}{\beta} \right)_p \left( \frac{\beta}{\alpha} \right)_p^{-1} = \zeta^{-\sum_{i=1}^{p-1} ia_i b_{p-i}}.
\]

**Proof.** Since \( \alpha \) and \( u_1^{a_1} \ldots u_{p-1}^{a_{p-1}} \) differ only by a factor that is \( p \)-primary, and likewise for \( \beta \) and \( u_1^{b_1} \ldots u_{p-1}^{b_{p-1}} \), then we have

\[
\left( \frac{\alpha}{\beta} \right)_p \left( \frac{\beta}{\alpha} \right)_p^{-1} = \left( \frac{\alpha, \beta}{\varphi} \right)_p = \prod_{i=1}^{p-1} \prod_{j=1}^{p-1} \left( \frac{u_i, u_j}{\varphi} \right)_p^{a_i b_j} = \prod_{i=1}^{p-1} \left( \frac{u_i, u_{p-i}}{\varphi} \right)_p^{a_i b_{p-i}} = \prod_{i=1}^{p-1} \zeta^{-i a_i b_{p-i}} = \zeta^{-\sum_{i=1}^{p-1} i a_i b_{p-i}}.
\]
Computation of symbols \( \left( \frac{\pi u_i}{\wp} \right)_p \).

**Lemma 11.21.**

\[
\left( \frac{p, u_i}{\wp} \right)_p = 1 \quad \text{for } i = 1, \ldots, p - 1
\]

**Proof.** By lemma 11.18, we have

\[
\left( \frac{p, \sigma u_i}{\wp} \right)_p = \left( \frac{p, u_i^{r_i}}{\wp} \right)_p = \left( \frac{p, u_i}{\wp} \right)_p^{r_i}.
\]

We can compute \( \left( \frac{p, \sigma u_i}{\wp} \right)_p \) in another way using lemma 10.43. Proceeding as in the proof of lemma 11.19, we have

\[
\sqrt{\sigma u_i} = \sigma \sqrt{u_i}
\]

so

\[
\left( \frac{p, \sigma u_i}{\wp} \right)_p = \sigma \left( \frac{p, u_i^{r_i}}{\wp} \right)_p = \sigma \left( \frac{p, u_i}{\wp} \right)_p^{r_i}.
\]

Therefore

\[
\left( \frac{p, \sigma u_i}{\wp} \right)_p \sigma \sqrt{u_i} = \sigma \left( \frac{p, u_i^{r_i}}{\wp} \right)_p \sqrt{u_i}.
\]

Comparison with (10.7) shows that \( \left( \frac{p, u_i}{\wp} \right)_p^{r_i} \). If \( \left( \frac{p, u_i}{\wp} \right)_p \neq 1 \) then we must have \( r = r'(\mod p) \), or \( i = 1 \).

It remains to prove the lemma in the case \( i = 1 \). We have \( 1 - \pi = \zeta \), and by lemma 11.17 with \( i = 1 \) we have \( r(r - r^2) \ldots (r - r^{p-1}) = -1(\mod p) \), so

\[
(10.8) \quad u_1 = \zeta^{-r(r-2)\ldots(r-p+2)} = \zeta^{-r(r-2)\ldots(r-p+2)} = \zeta.
\]

We have \( p = (1 - \zeta)(1 - \zeta^2) \ldots (1 - \zeta^{p-1}) \), so the lemma is proved if \( \left( \frac{1 - \zeta^i}{\wp} \right)_p = 1 \) for \( 1 \leq j < p \). For each \( j \) there is a \( j' \) so that \( jj' = 1(\mod p) \), and

\[
\left( \frac{1 - \zeta^i}{\wp} \right)_p = \left( \frac{1 - \zeta^j}{\wp} \right)_p = \left( \frac{1 - \zeta^j}{\wp} \right)_p^{j'} = 1.
\]

This completes the proof of the lemma.
Lemma 11.22. Put $\xi = -\frac{\pi^{p-1}}{p}$. Then

$$\left(\frac{\pi, u_i}{\varphi}\right)_p = \left(\frac{\xi, u_i}{\varphi}\right)_p$$

for $1 \leq i < p$.

Proof. Since $p$ is odd then $-1 = (-1)^p$, so by lemma 11.21 we have

$$\left(\frac{\pi, u_i}{\varphi}\right)_p = \left(\frac{\pi^{p-1}, u_i}{\varphi}\right)_p^{-1} = \left(\frac{-\pi^{p-1}/p, u_i}{\varphi}\right)_p^{-1} = \left(\frac{\xi, u_i}{\varphi}\right)_p^{-1},$$

which proves the lemma.

For any $\alpha$ in $W_\pi(1)$, let $t_1(\alpha), \ldots, t_{p-1}(\alpha)$ be the unique integers satisfying

$$\alpha = u_1^{t_1(\alpha)} \cdot u_{p-1}^{t_{p-1}(\alpha)}(\mod \varphi^p) \quad \text{and} \quad 0 \leq t_i(\alpha) < p$$

Then

$$\left(\frac{\xi, u_i}{\varphi}\right)_p = \left(\frac{u_{p-i}^{t_{p-i}(\xi)} u_i}{\varphi}\right)_p = \xi^{it_{p-i}(\xi)}.$$  

The problem is to compute $t_1(\xi), \ldots, t_{p-1}(\xi)$ for $1 \leq i \leq p-2$, since the next lemma shows that $t_{p-1}(\xi) = 1$.

Lemma 11.23.

$$\left(\frac{\xi, u_1}{\varphi}\right)_p = 1, \quad \text{or} \quad t_{p-1}(\xi) = 0.$$  

Proof. By (11.3) and (11.8) we have

$$\left(\frac{\xi, u_i}{\varphi}\right)_p = \left(\frac{-\pi^{p-1}, u_i}{\varphi\varphi}\right)_p = \left(\frac{-1, \xi}{\varphi}\right)_p \left(\frac{1 - \xi}{\varphi}\right)_p^{p-1} \prod_{j=1}^{p-1} \left(\frac{1 - \xi^j, \xi}{\varphi}\right)_p.$$

We have $-1 = (-1)^p$, and $\left(\frac{1 - \xi^j, \xi}{\varphi}\right)_p = 1$ was shown in the proof of lemma 11.21.
Kummer’s logarithmic differential quotient for \( p > 2 \). Every element \( \alpha \) in \( \mathfrak{o}_p \) is a linear combination of \( 1, \zeta, \ldots, \zeta^{p-2} \) with coefficients in \( \mathbb{Z}(p) \). Suppose that \( \phi(x) \) and \( \psi(x) \) are polynomials over \( \mathbb{Z}(p) \) such that \( \alpha = \phi(\zeta) = \psi(\zeta) \). Then \( \zeta \) is a root of \( \phi(x) - \psi(x) \), so \( \phi(x) - \psi(x) \) is divisible by the minimal polynomial of \( \zeta \) over \( \mathbb{Z}(p) \), which is \( f_0(x) = x^{p-1} + \cdots + x + 1 \) because \([\mathbb{Q}(\zeta) : \mathbb{Q}(2)] = p - 1\). Let \( \eta(x) \) be a polynomial with coefficients in \( \mathbb{Z}(p) \) such that

\[
\phi(x) - \psi(x) = f_0(x)\eta(x).
\]

Applying formal differentiation, we obtain

\[
(11.11) \quad \phi^{(n)}(x) - \psi^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f_0^{(k)}(x)\eta^{(n-k)}(x) \quad \text{for} \ 0 \leq n \leq p - 1
\]
as an identity of polynomials over \( \mathbb{Z}(p) \).

**Lemma 11.24.** Let \( f_0(x) = x^{p-1} + \cdots + x + 1 \). Then

\[
f_0^{(k)}(1) = 0 \pmod{p} \quad \text{for} \ 0 \leq k \leq p - 2
\]
together with

\[
f_0^{(p-1)}(1) = -1 \pmod{p}.
\]

**Proof.** Both sides of the identity

\[
(p - 1)!f_0(x) = \sum_{k=0}^{p-1} f_0^{(k)}(1) \frac{(p - 1)!}{k!} (x - 1)^k
\]
are polynomials with integer coefficients, and \( f_0^{(k)}(1) \) and \( (p - 1)!/k! \) are integers. We have \((x - 1)f_0(x) = x^p - 1 = (x - 1)^p \pmod{p} \), so \( f_0(x) = (x - 1)^{p-1} \pmod{p} \). Therefore

\[
(p - 1)!(x - 1)^{p-1} = \sum_{k=0}^{p-1} f_0^{(k)}(1) \frac{(p - 1)!}{k!} (x - 1)^k \pmod{p}
\]
The coefficients of \( (x - 1)^k \) for \( 0 \leq k \leq p - 1 \) must be identical on both sides, so

\[
f_0^{(k)}(1) = 0 \pmod{p} \quad \text{for} \ 0 \leq k \leq p - 2,
\]
and

\[
f_0^{(p-1)}(1) = (p - 1)! = -1 \pmod{p}.
\]
**Lemma 11.25.** If $\alpha$ is an element of $\mathbb{Q}_p(\zeta)$ and $\alpha = \phi(\zeta) = \psi(\zeta)$ where $\phi(x)$ and $\psi(x)$ are polynomials with coefficients in $\mathbb{Z}_p$, then

$$\phi^{(n)}(1) - \psi^{(n)}(1) = 0 \pmod{p} \text{ for } 0 \leq n \leq p - 2$$

and

$$\phi^{(p-1)}(1) - \psi^{(p-1)}(1) = -\frac{\phi(1) - \psi(1)}{p} \pmod{p}$$

**Proof.** The result for $0 \leq n \leq p - 2$ is obtained by setting $x = 1$ in (11.11) and applying lemma 11.24. For $n = p - 1$ we have

$$\phi^{(p-1)}(1) - \psi^{(p-1)}(1) = f_0^{(p-1)}(1)\eta(1) = -\eta(1) \pmod{p}.$$ 

We have $\phi(1) - \psi(1) = f_0(1)\eta(1)$. Since $f_0(1) = p$ then $\phi(1) - \psi(1)$ is divisible by $p$ and $\eta(1) = (\phi(1) - \psi(1))/p$, which gives the desired result for $n = p - 1$.

**Lemma 11.26.** Suppose that $\alpha$ is in $W_{\psi}(1)$ and $\alpha = \phi(\zeta) = \psi(\zeta)$. Then we have $1 = \phi(1) = \psi(1) \pmod{0}$, and

$$\phi^{(n)}(1) = \psi^{(n)}(1) \pmod{p} \text{ for } 0 \leq n < p - 1$$

and

$$\phi^{(p-1)}(1) + \frac{\phi(1) - 1}{p} = \psi^{(p-1)}(1) + \frac{\psi(1) - 1}{p} \pmod{p}$$

**Proof.** Since $\alpha = 1 \pmod{\phi}$ and $\zeta = 1 \pmod{\phi}$ then we have $1 = \phi(1) = \psi(1) \pmod{\phi}$. Therefore $1 = \phi(1) = \psi(1) \pmod{p}$, so $\phi(1) - 1$ and $\psi(1) - 1$ are divisible by $p$. The results now follow immediately from lemma 11.25.

We consider the formal power series $F(z) = \log (\phi(e^z))$.

$$F(z) = \log (\phi(1)) + \frac{\phi'(1)}{\phi(1)}z + \frac{(\phi''(1) + \phi'(1))^2}{\phi(1)^2}z^2 + \ldots$$

If $\phi(1)$ is in $W_{\psi}(1)$ then $\log (\phi(1))$ is defined, but we are actually interested only in coefficients of $z^n$ for $1 \leq n \leq p - 1$. 

Lemma 11.27.

\[
\frac{d^n}{dz^n} F(z) = \frac{\phi^{(n)}(e^z) e^{nz}}{\phi(e^z)} + R_n(z)
\]

where \(R_n(z)\) is a rational expression in \(e^z, \phi(e^z), \phi'(e^z), \ldots, \phi^{(n-1)}(e^z)\). The numerator of \(R_n(z)\) is a sum of terms each of which is divisible by at least one of \(\phi'(e^z), \ldots, \phi^{(n-1)}(e^z)\), and the denominator is a power of \(\phi(e^z)\).

Proof. Put \(w = e^z\), \(u_0 = \phi(e^z)\), and \(u_i = \phi^{(i)}(e^z)\) for \(i \geq 0\). Then \(w' = w\) and \(u'_i = u_{i+1}w\) for \(i \geq 0\). We have \(F(z) = \log(u_0)\), so \(dF(z)/dz = u_1w/u_0\). Therefore \(R_1(z) = 0\), so the conclusion holds for \(n = 1\). For \(n = 2\), we have

\[
\frac{d^2}{dz^2} F(z) = \frac{u_2w^2}{u_0} + \frac{u_1w}{u_0} - \frac{u_2w^2}{u_0^2} = \frac{u_2w^2}{u_0} + \frac{u_1u_0w - u_2u_1w^2}{u_0^2}
\]

so every term of the numerator of \(R_2(z)\) is divisible by \(u_1\).

Assume that the lemma is true for \(n\). Then

\[
\frac{d^n}{dz^n} F(z) = \frac{u_nw^n}{u_0} + R_n(z)
\]

and

\[
R_n(z) = \frac{S_1u_1 + \cdots + S_{n-1}u_{n-1}}{u_0^{k_n}}
\]

where \(S_1(z), \ldots, S_{n-1}(z)\) are polynomials in \(w, u_0, \ldots, u_{n-1}\). We have

\[
\frac{d}{dz} R_n(z) = \frac{\sum_{j=1}^{n-1} \left( (S'_j u_j + S_j u_{j+1}w) u_0^{k_n} - k_n S_j u_j u_0^{k_n-1} u_1 w \right) u_0^{2k_n}}{u_0^{2k_n}}
\]

and every term of the numerator is divisible by at least one of \(u_1, \ldots, u_n\). Then

\[
\frac{d^{n+1}}{dz^{n+1}} F(z) = \\
= \frac{u_{n+1}w^{n+1}}{u_0} + \frac{nu_nw^n}{u_0} - \frac{u_{n+1}w^{n+1}}{u_0^2} + \frac{d}{dz} R_n(z) = \frac{u_{n+1}w^{n+1}}{u_0} + R_{n+1}(z)
\]

We see that \(R_{n+1}(z)\) is a rational expression in \(w, u_0, u_1, \ldots, u_n\) with denominator \(u_0^{2k_n}\), and every term of the numerator contains at least one factor from the list \(u_1, \ldots, u_n\), and the conclusion therefore follows.
Lemma 11.28. If $\alpha = \phi(\zeta)$ is in $W_{p}(1)$, define $\ell_n(\alpha)$ by

$$
\ell_n(\alpha) = \begin{cases} 
\frac{d^n}{dz^n} F(0) & \text{for } 1 \leq n \leq p - 2 \\
\frac{d^{(p-1)}}{dz^{(p-1)}} F(0) + \frac{\phi(1) - 1}{p} & \text{for } n = p - 1.
\end{cases}
$$

Then $\ell_n(\alpha)$ depends only on $\alpha$ and not on $\phi(x)$ for $1 \leq n \leq p - 1$.

Proof. By lemma 11.27, $\frac{d^n}{dz^n} F(0) = \frac{\phi^{(n)}(1)}{\phi(1)} + R_n(0)$, where $R_n(0)$ is a rational expression in $1, \phi(1), \ldots, \phi^{n-1}(1)$ with denominator a power of $\phi(1)$. By lemma 11.26, $\phi(1) \equiv 1 \pmod{p}$ and $\ell_1(\alpha), \ldots, \ell_{p-2}(\alpha)$ depend modulo $p$ only on $\alpha$ and not on $\phi(x)$. For $n = p - 1$, we have

$$
\ell_{p-1}(\alpha) = \phi^{(p-1)}(1) + \frac{\phi(1) - 1}{p} + R_{p-1}(0)(\text{mod } p).
$$

By lemma 11.26, this expression depends modulo $p$ only on $\alpha$ and not on $\phi(x)$.

Lemma 11.29. For $\alpha_1$ and $\alpha_2$ in $W_{p}(1)$, we have

(1) $\ell_j(\alpha_1\alpha_2) = \ell_j(\alpha_1) + \ell_j(\alpha_2)(\text{mod } p)$,

(2) $\ell_j(\alpha_1\alpha_2^{-1}) = \ell_j(\alpha_1) - \ell_j(\alpha_2)(\text{mod } p)$.

If $\alpha_1 = \alpha_2(\text{mod } \wp^{p-1})$ then

(3) $\ell_j(\alpha_1) = \ell_j(\alpha_2)(\text{mod } p)$ for $1 \leq j \leq p - 2$.

If $\alpha_1 = \alpha_2(\text{mod } \wp^p)$ then

(4) $\ell_{p-1}(\alpha_1) = \ell_{p-1}(\alpha_2)(\text{mod } p)$.

If $\sigma$ generates $G(\mathbb{Q}_{(p)}(\zeta) : \mathbb{Q}_{(p)})$ and $\zeta^\sigma = \zeta^r$ then

(5) $\ell_j(\alpha^\sigma) = r^j \ell_j(\alpha)(\text{mod } p)$ for $1 \leq j \leq p - 1$.

Proof. If $\alpha_1 = \phi_1(\zeta)$ and $\alpha_2 = \phi_2(\zeta)$ then $\alpha_1\alpha_2 = \phi_1(\zeta)\phi_2(\zeta)$, and (1) follows from the identity of formal power series

$$
\log(\phi_1(e^z)\phi_2(e^z)) = \log(\phi_1(e^z)) + \log(\phi_2(e^z)).
$$
Then (2) follows from
\[ \ell_j((\alpha_1\alpha_2^{-1})\alpha_2) = \ell_j(\alpha_1\alpha_2^{-1}) + \ell_j(\alpha_2)(\mod p). \]

As to (3), it is enough to show that if \( \alpha = 1(\mod \wp^{p-1}) \) then \( \ell_j(\alpha) = 0(\mod p) \) for \( 1 \leq j \leq p - 2 \). Put
\[ \alpha = a_0 + \sum_{k=0}^{p-2} a_k \pi^k. \]

Then \( a_0 = 1(\mod p) \), and \( a_k = 0(\mod p) \) for \( 1 \leq k \leq p - 2 \). We have \( \alpha = a_0 + \sum_{k=0}^{p-2} a_k(1 - \zeta)^k \), so \( \alpha = \phi(\zeta) \) with
\[ \phi(x) = a_0 + \sum_{k=0}^{p-2} a_k(1 - x)^k \]

We have \( \phi(x) = 1(\mod p) \), and \( \phi^{(n)}(x) = 0(\mod p) \) for \( n \geq 1 \). By lemma 11.27 we have
\[ \ell_1(\alpha) = \cdots = \ell_{p-2}(\alpha) = 0(\mod p). \]

As to (4), since all derivatives of \( \phi(x) \) vanish modulo \( p \) then all derivatives of \( \log(\phi(e^z)) \) vanish modulo \( p \) at \( z = 0 \). If \( \alpha = 1(\mod \wp^p) \) then \( a_0 = 1(\mod p^2) \), so we have
\[ \ell_{p-1}(\alpha) = \phi(1) - \frac{1}{p}a_0 = \frac{a_0 - 1}{p} = 0(\mod p). \]

As to (5), if \( \alpha = \sum_{k=0}^{p-2} b_k \xi^k = \phi(\zeta) \) and \( \zeta^\sigma = \zeta^r \) then \( \alpha^\sigma = \sum_{k=0}^{p-2} b_k \xi^{rk} = \phi(\zeta^r) = \psi(\zeta) \) where \( \psi(x) = \phi(x^r) \). If \( \log(\phi(e^z)) = \sum_{n=0}^{\infty} c_n z^n \), then \( \log(\psi(e^z)) = \log(\phi(e^{rz})) = \sum_{n=0}^{\infty} c_n r^n z^n \). Therefore
\[ \ell_j(\alpha^\sigma) = r^j \ell_j(\alpha) \quad \text{for } 1 \leq j \leq p - 2. \]

For \( j = p - 1 \), we have \( r^{p-1} = 1(\mod p) \) so we are claiming that \( \ell_{p-1}(\alpha^\sigma) = \ell_{p-1}(\alpha)(\mod p) \). Since all derivatives of \( \log(\phi(e^z)) \) vanish modulo \( p \) at \( z = 0 \), this reduces to
\[ \frac{\phi(x) - 1}{x} \bigg|_{x=1} = \frac{\phi(x^r) - 1}{x} \bigg|_{x=1} (\mod p). \]

This completes the proof of lemma 11.29.
Lemma 11.30. If $\alpha$ is in $W_p(1)$ and $t_1(\alpha), \ldots t_{p-1}(\alpha)$ are as in (11.9), then

$$t_j(\alpha) = \frac{(-1)^{j-1}}{j!} \ell_j(\alpha) \pmod{p} \quad \text{for } 1 \leq j \leq p-1.$$ 

Proof. We have $\ell_j(u_i^a) = r^i \ell_j(u_i)(\mod p)$ for $1 \leq j \leq p-1$ by lemma 11.29(5). Also, we have $u_i^a = u_i^r \pmod{\wp^p}$ by lemma 11.18, so $\ell_j(u_i^a) = \ell_j(u_i^r)(\mod p)$ for $1 \leq j \leq p-2$ by lemma 11.29(3) and for $j = p-1$ by lemma 11.29(4). Therefore, if $\ell_j(u_i) \neq 0(\mod p)$ then $r^i = r^j(\mod p)$, or $i = j$. Since $u_i = 1 - \pi^i(\mod \wp^{i+1})$ by lemma 11.18, we have

$$u_j = (1 - \pi^j)u_{j+1}^{a_{j+1}} \ldots u_{p-1}^{a_{p-1}}(\mod p),$$

so $\ell_j(u_j) = \ell_j(1 - \pi^j)(\mod p)$. Since $1 - \pi^j = 1 - (1 - \zeta)^j$, then we take $\phi(x) = 1 - (1 - x)^j$. Then

$$\phi(e^z) = 1 - (1 - e^z)^j = 1 + (-1)^{j-1}z^j + \ldots$$

so

$$\log(\phi(e^z)) = (-1)^j z^j + \ldots$$

In this case we have $\phi(1) = 1$, so $(\phi(1) - 1)/p = 0$, and therefore

$$\ell_j(u_j) = \ell_j(1 - \pi^j) = \left. \frac{d^j}{dz^j} \log(\phi(e^z)) \right|_{z=0} = (-1)^j j!(\mod p).$$

Putting $\alpha = u_1^{t_1(\alpha)} \ldots u_{p-1}^{t_{p-1}(\alpha)}(\mod \wp^p)$, we have

$$\ell_j(\alpha) = t_j(\alpha) \ell_j(u_j) = (-1)^j j! t_j(\alpha)(\mod p),$$

which proves the lemma.

We will be completely finished if we can compute $\ell_j(\xi)$ for $1 \leq j \leq p-2$, since we have already established that $t_{p-1}(\xi) = 0$ (lemma 11.23). The Bernoulli numbers $B_a$ are defined by

$$\log \left( \frac{e^z - 1}{z} \right) = \sum_{a=1}^{\infty} \frac{B_a}{a} \frac{z^a}{a!}$$

The denominators of $B_1, \ldots, B_{p-2}$ cannot be divisible by $p$. 
Lemma 11.31. For $1 \leq j \leq p - 2$ we have
\[ \ell_j(\xi) = -\frac{B_j}{j} (\mod p) \]

Proof. We have
\[
\xi^{-1} = -\frac{p}{\pi^{p-1}} = -\prod_{k=1}^{p-1} \frac{1 - \zeta^k}{1 - \zeta} = -(p - 1)! \prod_{k=1}^{p-1} \frac{1}{1 - \frac{\zeta^k}{1 - \zeta}} = -(p - 1)! \prod_{k=1}^{p-1} \gamma_k
\]
where $\gamma_k = (1 + \zeta + \cdots + \zeta^{k-1})/k$ is in $W_\varphi(1)$. Since $-(p - 1)! = 1 (\mod \varphi^{p-1})$, then by lemma 11.29(3) we have $\ell_j(-(p - 1)!)/ \ell_j(1) = 0$, so
\[
\ell_j(\xi^{-1}) = \sum_{k=1}^{p-1} \ell_j(\gamma_k) \quad \text{for } 1 \leq j \leq p - 2.
\]
To compute $\ell_j(\gamma_k)$, we use $\phi_k(x) = (1 + x + \cdots + x^{k-1})/k = \frac{x^{k-1}}{k(x-1)}$.
\[
\log (\phi_k(e^z)) = \log \left( \frac{e^{kz} - 1}{kz} \right) \frac{z}{e^z - 1}
\]
\[
= \log \frac{e^{kz} - 1}{kz} - \log \frac{e^z - 1}{z} = \sum_{a=1}^\infty \frac{B_a}{a} (k^a - 1) \frac{z^a}{a!}
\]
Therefore for $1 \leq j \leq p - 2$ we have
\[
\ell_j(\gamma_k) = \frac{d^j}{dz^j} \log (\phi_k(e^z)) \bigg|_{z=0} = \frac{B_j}{j} (k^j - 1) \quad \text{for } 1 \leq j \leq p - 2,
\]
so
\[
\ell_j(\xi^{-1}) = \sum_{k=1}^{p-1} \frac{B_j}{j} (k^j - 1).
\]
If $r$ is a primitive root modulo $p$ and $1 \leq j \leq p - 2$, then
\[
\sum_{\nu=1}^{p-1} k^j = \sum_{\nu=1}^{p-1} r^{\nu j} = \frac{r^{pj} - 1}{r^j - 1} = 0 (\mod p),
\]
so
\[
\ell_j(\xi^{-1}) = -(p - 1) \frac{B_j}{j} = \frac{B_j}{j} (\mod p),
\]
which proves the lemma.