RIEMANN-HURWITZ FORMULA AND p-ADIC GALOIS REPRESENTATIONS FOR NUMBER FIELDS

KENKICHI IWASAWA

(Received July 29, 1980)

Let \( f: \mathbb{R}' \rightarrow \mathbb{R} \) be an \( n \)-fold covering of compact, connected Riemann surfaces and let \( g \) and \( g' \) denote the genera of \( \mathbb{R} \) and \( \mathbb{R}' \) respectively. The classical formula of Riemann-Hurwitz then states that
\[
2g' - 2 = (2g - 2)n + \sum (e(P') - 1)
\]
where the sum is taken over all points \( P' \) on \( \mathbb{R}' \) and \( e(P') \) denotes the ramification index of \( P' \) for the covering \( f \). In a recent paper [6], Kida proved a highly interesting analogue of the above formula for algebraic number fields.\(^1\) In the present paper, we shall give an alternate proof for the theorem of Kida from a different point of view. Namely, assuming that the covering \( f \) is regular, let \( G \) denote the group of all covering transformations for \( f \). Then the finite group \( G \) acts naturally on the space of all differentials of the first kind on \( \mathbb{R}' \), and the representation of \( G \) thus defined was completely determined by Chevalley-Weil [2]. In the following, we shall study certain \( p \)-adic representations of Galois groups which may be regarded as analogues, for algebraic number fields, of the representation of \( G \) mentioned above, and we shall prove a result for such \( p \)-adic representations, quite similar to the theorem of Chevalley-Weil for the representation of \( G \). The formula of Kida will then follow from this by comparing the degrees of the representations. Our proof is based essentially upon Galois cohomology theory for algebraic number fields which are not necessarily finite over the rational field. Hence some preliminary results in that theory will be discussed in the earlier part of the paper.\(^2\) In the last section of the paper, we shall also indicate briefly another approach to Kida's formula which is slightly different from what is described above; this might be of some interest because it applies also for, e.g., totally real algebraic number fields.

1. Throughout the following, let \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \) denote the ring of rational integers, the field of rational numbers, the field of real numbers, and that of complex numbers, respectively. By a number field \( K \), we

\(^1\) See the formula (10) in § 9 below.
\(^2\) See also [1], [9] for Galois cohomology theory.
shall mean any algebraic extension of $\mathcal{O}$ in $\mathcal{C}$, not necessarily finite over $\mathcal{Q}$. For such a field $\mathcal{K}$, let $\mathcal{O}_\mathcal{K}$ denote the ring of all algebraic integers in $\mathcal{K}$. The invertible $\mathcal{O}_\mathcal{K}$-submodules of $\mathcal{K}$ are called the ideals of $\mathcal{K}$, and they form a multiplicative group $I_\mathcal{K}$, the ideal group of $\mathcal{K}$. Let $P_\mathcal{K}$ denote the subgroup of principal ideals $(\alpha)$, $\alpha \in \mathcal{K}^\times$. The ideal-class group $C_\mathcal{K} = I_\mathcal{K}/P_\mathcal{K}$ is then a torsion abelian group so that

$$C_\mathcal{K} = \bigoplus q C_\mathcal{K}(q)$$

where $q$ ranges over all prime numbers and $C_\mathcal{K}(q)$ denotes the $q$-primary component of $C_\mathcal{K}$. If $\mathcal{K}$ is a subfield of a number field $\mathcal{L}$, there is a natural imbedding $I_\mathcal{K} \to I_\mathcal{L}$, and it induces homomorphisms $C_\mathcal{K} \to C_\mathcal{L}$, $C_\mathcal{K}(q) \to C_\mathcal{L}(q)$. Let $\mathcal{v}$ be a finite, i.e., non-archimedean, place on $\mathcal{K}$ and let $p_\mathcal{v}$ denote the associated maximal ideal of $\mathcal{O}_\mathcal{K}$. If $\mathcal{K}/\mathcal{Q}$ is finite, then $p_\mathcal{v}$ belongs to $I_\mathcal{K}$ and generates a cyclic subgroup $\langle p_\mathcal{v} \rangle$ of $I_\mathcal{K}$. For infinite $\mathcal{K}/\mathcal{Q}$, this is not true in general. However, in some special cases, we can still define a subgroup $I_\mathcal{v}$ of $I_\mathcal{K}$, similar to $\langle p_\mathcal{v} \rangle$ mentioned above. Namely, assume that $\mathcal{K}$ has a subfield $\mathcal{K}$, finite over $\mathcal{Q}$, such that $\mathcal{v}$ is the unique extension of $\mathcal{v}|\mathcal{K}$ on $\mathcal{K}$, $\mathcal{v}|\mathcal{K}$ being the restriction (projection) of $\mathcal{v}$ on the subfield $\mathcal{K}$. Let $\mathcal{K} = \lim k_i$ where $k \subseteq k_i \subseteq \mathcal{K}$ and $k_i/\mathcal{Q}$ is finite, and let $v_i = v|k_i$. Then $\langle p_{v_i} \rangle$ is contained in $\langle p_{v_j} \rangle$ for $k_i \subseteq k_j$, so that a subgroup $I_\mathcal{v}$ of $I_\mathcal{K} = \lim I_{k_i}$ is defined by

$$I_\mathcal{v} = \lim \langle p_{v_i} \rangle$$

It is isomorphic to a subgroup of the additive group of $\mathcal{Q}$, containing $\mathcal{Z}$. In particular, if there exists a subfield $k$ such that $\mathcal{v}$ is unramified for the extension $\mathcal{K}/k$, then $p_\mathcal{v}$ belongs to $I_\mathcal{K}$ and $I_\mathcal{v} = \langle p_\mathcal{v} \rangle \cong \mathcal{Z}$. We note here in passing that the ramification theory can be reasonably extended to places on extensions of number fields which are not necessarily finite over $\mathcal{Q}$; for example, the ramification indices are defined for such places so that they agree with the classical definition for finite algebraic number fields and satisfy the chain rule for $\mathcal{K} \subseteq \mathcal{L} \subseteq \mathcal{M}$.

Let $\mathcal{p}$ be a fixed prime number and let $\mathcal{Z}_\mathcal{p}$ and $\mathcal{Q}_\mathcal{p}$ denote the ring of $\mathcal{p}$-adic integers and the field of $\mathcal{p}$-adic numbers respectively. Let $\mathcal{Q}_\mathcal{Q}$ be the unique $\mathcal{Z}_\mathcal{p}$-extension over $\mathcal{Q}$ in $\mathcal{C}$.\(^3\) For each number field $\mathcal{k}$, finite over $\mathcal{Q}$, the composite $\mathcal{k}_\mathcal{Q} = \mathcal{k}\mathcal{Q}_\mathcal{Q}$ is then a $\mathcal{Z}_\mathcal{p}$-extension over $\mathcal{k}$, and it is clearly a finite extension of $\mathcal{Q}_\mathcal{Q}$. Conversely, if $\mathcal{K}$ is a finite extension over $\mathcal{Q}_\mathcal{Q}$ in $\mathcal{C}$, then there exists $\mathcal{k}$, finite over $\mathcal{Q}$, such that $\mathcal{K} = \mathcal{k}_\mathcal{Q}$. In the following, we shall call such a number field $\mathcal{K}$ simply a $\mathcal{Z}_\mathcal{p}$-field.

\(^3\) For $\mathcal{Z}_\mathcal{p}$-extensions of algebraic number fields, see [5] and the papers in the bibliography of [5].
Let $q$ be any prime number and let $v$ be a $q$-place on a $\mathbb{Z}_p$-field $K$, i.e., a finite place on $K$ with $v|\mathbb{Q} = q$. From $K = k_v = k\mathbb{Q}_v$, we then see easily that the subgroup $I_v$ of $I_K$ is defined as explained above and that if $q \neq p$, then $I_v = \langle \mathfrak{p}_v \rangle \cong \mathbb{Z}$, and if $q = p$, then $I_v$ is isomorphic to the union $\bigcup_{n \geq 0} p^{-n}\mathbb{Z}$. Furthermore, for each prime number $q$, there exist only a finite number of $q$-places on $K$, and

$$I_K = \bigoplus I_v$$

where $v$ ranges over all finite places on $K$.

Now, let $L$ be a finite Galois extension of a $\mathbb{Z}_p$-field $K$ with $G = \text{Gal}(L/K)$; $L$ itself is then a $\mathbb{Z}_p$-field. For each finite place $v$ on $K$, let

$$I_{L,v} = \bigoplus I_w$$

where $w$ runs over all extensions of $v$ on $L$ and where $I_w$ denotes the subgroup of $I_L$ defined similarly as $I_v$ for $K$. Clearly $I_{L,v}$ is a subgroup of $I_L$, invariant under $G$, and

$$I_L = \bigoplus I_{L,v}$$

with $v$ ranging over all finite places of $K$. Writing $H^n(L/K, I_L)$ for the cohomology group $H^n(G, I_L)$, we then have

$$H^n(L/K, I_L) = \bigoplus H^n(L/K, I_{L,v}), \quad \text{for } n \geq 0.$$ 

We shall next consider $H^n(L/K, I_{L,v})$ for each finite place $v$ on $K$.

First, let $v$ be a non-$p$-place, i.e., $v|\mathbb{Q} = q \neq p$. For an extension $w$ of $v$ on $L$, we can define the decomposition group $Z = Z(w/v)$ and the inertia group $T = T(w/v)$ as usual so that $T \subseteq Z \subseteq G$. Let $e = e(w/v) = [T:1]$, $f = f(w/v) = [Z:T]$, $g = g(w/v) = [G:Z]$ so that $efg = [G:1] = [L:K]$. Then, as in the classical theory for finite algebraic number fields, one proves the following:

(a) All extensions of $v$ on $L$ are given by $\sigma(w)$, $\sigma \in G$, so that $g$ is the number of distinct extensions of $v$ on $L$. Hence, as $G$-modules,

$$I_{L,v} \cong Z[G/Z]$$

where $Z[G/Z]$ denotes the module of all linear combinations of the left cosets of $G$ modulo $Z$ with coefficients in $Z$ and where the isomorphism is defined by $\sigma(v_w) \mapsto \sigma Z$, for $\sigma \in G$. Consequently

$$H^n(L/K, I_{L,v}) \cong H^n(G, Z[G/Z]) \cong H^n(Z, Z), \quad n \geq 0$$

with trivial $Z$-action on $Z$.\(^4\)

\(^4\) See [7], Chap. II, Théorème 6.
(b) Let $w_1, \ldots, w_g$ be the distinct extensions of $v$ on $L$. Then, in the ideal group $I_L$,

$$p_v = \prod \sigma(p_w) = \left(\prod_{i=1}^g p_{w_i}\right)^\sigma, \quad \sigma \in G.$$  

Hence

$$I_{L,v}^0 = H^0(L/K, I_{L,v}) = \langle p_v^e \rangle \cong \mathbb{Z}.$$  

(c) $T$ is a normal subgroup of $Z$ and

$$Z/T \cong \text{Gal} \left( t_w/t_v \right)$$

where $t_v = o_K/p_v$ and $t_w = o_L/p_w$ are the residue fields of $v$ and $w$ respectively. In particular, $f = [t_w : t_v]$. Note that both $t_v$ and $t_w$ are algebraic extensions of the finite field $F_q$ with $q$ elements and that $[t_v : F_q]$ is divisible by $p^e$ because $K = k_w$.

Assume now that $L/K$ is a $p$-extension. Then $Z/T$ is a $p$-group, and the remark just mentioned above implies that $f = [t_w : t_v] = 1$, $Z = T$. However, since $v|Q \neq p$, $v$ is tamely ramified in $L$ so that $T$ is a cyclic group of order $e$. Hence, in this case, we obtain from (a) above that

$$H^n(L/K, I_{L,v}) \cong Z/eZ, \quad \text{for all even } n \geq 2,$$

$$= 0, \quad \text{for all odd } n \geq 1,$$

while $H^n(L/K, I_{L,v})$ is given in general by (b).

Next, let $v$ be a $p$-place on $K$. Then $I_{L,v}$ is uniquely divisible by $p$ as mentioned earlier. Hence, for a $p$-extension $L/K$, we see easily that

$$I_{L,v}^0 = H^0(L/K, I_{L,v}) = I_v,$$

$$= H^0(L/K, I_{L,v}) = 0, \quad \text{for } n \geq 1.$$  

2. Let $K$ be again a $\mathbb{Z}_p$-field and let $L/K$ be a $p$-extension with $G = \text{Gal} \left( L/K \right)$. We do not assume here that $L/K$ is a finite extension. Hence $L$ is not necessarily a $\mathbb{Z}_p$-field. However, if $\{L_i\}$ denotes the family of all finite Galois extensions of $K$ contained in $L$, then each $L_i$ is a $\mathbb{Z}_p$-field and

$$L = \lim_{\rightarrow} L_i.$$  

For a finite place $v$ on $K$, let

$$I_{L,v} = \lim_{\rightarrow} I_{L,v}^i,$$  

where $I_{L_i,v}$ is defined as in § 1 and where the limit is taken with respect to $I_{L_i,v} \rightarrow I_{L_j,v}$ for $L_i \subseteq L_j$. Then $I_{L,v}$ is a subgroup of $I_L$, invariant under $G$, and

$$I_L = \bigoplus_v I_{L,v}.$$
Hence
\[ H^n(L/K, I_L) = \bigoplus_v H^n(L/K, I_{L,v}) , \]
\[ H^n(L/K, I_{L,v}) = \lim_{\to} H^n(L_i/K, I_{L_i,v}) , \quad n \geq 0 . \]

**Lemma 1.** Let \( v \mid \mathbb{Q} = p \). Then
\[ I_{L,v} = H^0(L/K, I_{L,v}) = I_v , \]
\[ H^n(L/K, I_{L,v}) = 0 , \quad \text{for} \quad n \geq 1 . \]

Let \( v \mid \mathbb{Q} \neq p \). Let \( w \) be an extension of \( v \) on \( L \) and let \( e = e(w/v) \) denote the ramification index of \( w/v \), i.e., the order of the inertia group \( T(w/v) \).

If \( e \) is finite, then \( T(w/v) \cong \mathbb{Z}/e\mathbb{Z} \) and
\[ I_{L,v} = H^0(L/K, I_{L,v}) = \langle \psi^{1/e} \rangle \cong \mathbb{Z} , \]
\[ H^n(L/K, I_{L,v}) \cong \mathbb{Z}/e\mathbb{Z} , \quad \text{for even} \quad n \geq 2 , \]
\[ = 0 , \quad \text{for odd} \quad n \geq 1 . \]

On the other hand, if \( e \) is infinite, then \( T(w/v) \cong \mathbb{Z}_p \) and
\[ I_{L,v} = H^0(L/K, I_{L,v}) = \{ p^r | r \in \mathbb{R} \} \cong \mathbb{R} = \bigcup_{n \geq 0} p^{-n}\mathbb{Z} , \]
\[ H^n(L/K, I_{L,v}) = 0 , \quad \text{for} \quad n \geq 1 . \]

**Proof.** The first part is an immediate consequence of the results for \( H^*(L_i/K, I_{L_i,v}) \) mentioned in §1. Let \( v \mid \mathbb{Q} \neq p \) and let \( w_i = w \mid L_i \), \( e_i = e(w_i/v) \), \( T_i = T(w_i/v) = \mathbb{Z}(w_i/v) \) for each \( i \). Then \( T = T(w/v) = \lim T_i \), and the argument in §1 shows that the following diagram is commutative for \( L_i \subseteq L_j \):
\[ H^*(L_i/K, I_{L_i,v}) \cong H^*(T_i, \mathbb{Z}) \]
\[ H^*(L_j/K, I_{L_j,v}) \cong H^*(T_j, \mathbb{Z}) . \]

Here the vertical map on the right is defined by the natural homomorphism \( T_j \to T_i \) and by the endomorphism \( a \mapsto (e_j/e_i)a \) of \( \mathbb{Z} \). Hence it follows that
\[ H^*(L/K, I_{L,v}) \cong H^*(T, \lim \mathbb{Z}) , \quad n \geq 0 . \]

As each \( T_i \) is a cyclic group of order \( e_i \), the statements in the second part are consequences of the above remarks and of the results in §1.

When \( e(w/v) \) is infinite and \( T(w/v) \cong \mathbb{Z}_p \), we shall say that the finite non-\( p \)-place \( v \) is infinitely ramified in \( L \); note that if \( w' \) is another extension of \( v \) on \( L \), then \( e(w'/v) = e(w/v) \), \( T(w'/v) \cong T(w/v) \) so that the definition is in fact independent of the choice of \( w \). The following result is then an immediate consequence of Lemma 1:
LEMMA 2. Let $L$ be a $p$-extension over a $\mathbb{Z}_p$-field $K$ with $G = \text{Gal}(L/K)$. Suppose that each finite non-$p$-place on $K$ is either unramified in $L$ or infinitely ramified in $L$. Then

$$H^n(L/K, I_L) = 0, \text{ for all } n \geq 1,$$

and

$$I^n_I = \bigoplus_v A_v$$

where $v$ ranges over all finite non-$p$-places on $K$, ramified in $L$ and where, for each $v$,

$$A_v = \mathbb{P}^v/\mathbb{P}_v \cong R/Z \cong \mathbb{Q}_p/Z_p$$

with $R = \bigcup_{n \geq 0} p^{-n} \mathbb{Z}$ in $\mathbb{Q}$.

LEMMA 3. Let $K$ be a $\mathbb{Z}_p$-field, $v$ a finite non-$p$-place on $K$, and $\mathfrak{t}_v$ the residue field of $v$: $\mathfrak{t}_v = o_K/p_v$. Since $\mathfrak{t}_v$ is an algebraic extension of a finite field and $K = k_\infty = k\mathbb{Q}_\infty$ with $k$ finite over $\mathbb{Q}$, we see easily that the multiplicative group $\mathfrak{t}_v^\times$ is a torsion abelian group and that the order of $\mathfrak{t}_v^\times$ is either divisible by $p^a$ or prime to $p$, i.e., the $p$-primary component of $\mathfrak{t}_v^\times$ is either infinite or the identity group.

LEMMA 3. Let the order of $\mathfrak{t}_v^\times$ be prime to $p$ and let $L/K$ be a $p$-extension. Then $v$ is unramified in $L$.

PROOF. We may assume that $L/K$ is finite. Then we can find a $p$-extension of finite algebraic number fields, $k'/k$, such that $K = k_\infty$, $L = k_\infty'$. Let $v_0 = v|_k$. Then $v_0$ is a non-$p$-place on $k$ and the order of $\mathfrak{t}_v^\times$ is prime to $p$. Since $k'/k$ is a $p$-extension, it follows that $v_0$ is unramified in $k'$. Hence $v$ also is unramified in $L$.

LEMMA 4. Let the order of $\mathfrak{t}_v^\times$ be divisible by $p^a$ and let $S$ be a set of places on $K$, including $v$ and all $p$-places of $K$. Let $L$ denote the maximal abelian $p$-extension over $K$, unramified outside $S$. Then $v$ is infinitely ramified in $L$.

PROOF. Let $w$ be an extension of $v$ on $L$ and assume that

$$e(w/v) = p^a < \infty, \quad a \geq 0.$$  

Let $k$ be a finite algebraic number field such that $K = k_\infty$ and that $v$ is the unique extension of $v|k$ on $K$, and let $k_n$, $n \geq 0$, be the intermediate fields of the $\mathbb{Z}_p$-extension $K/k$:

$$k = k_0 \subset \cdots \subset k_n \subset \cdots \subset k_\infty = K, \quad K = \bigcup_{n \geq 0} k_n.$$  

Let $S_n$ denote the union of $v_n = v|k_n$ and all $p$-places on $k_n$, and $F_n$ the
maximal abelian $p$-extension over $k_\alpha$, unramified outside $S_\alpha$. Then $k_\alpha \subseteq K \subseteq F_\alpha \subseteq L$ so that we put $w_\alpha = w|F_\alpha$. As $v_\alpha$ is unramified in $K$ and $e(v/v_\alpha) = 1$, we have

$$e(w_\alpha/v_\alpha) = e(w/v) \leq e(w/v) = p^\alpha.$$  

For each place $z$ in $S_\alpha$, let $k_{n,z}$ denote the $z$-completion of $k_\alpha$, and $U_{n,z}$ the multiplicative group of the local units in $k_{n,z}$. Let $U_n$ be the direct product of all such $U_{n,z}$, $z \in S_\alpha$, and let $E_n$ be the group of global units in $k_\alpha$. Then there is a natural imbedding $E_n \to U_n$, and we shall denote by $\bar{E}_n$ the closure of $E_n$ in the compact group $U_n$. On the other hand, let $V_n$ denote the Sylow $p$-subgroup of the profinite abelian group $U_{n,v_\alpha}$. Since $v|Q \neq p$, $V_n$ is isomorphic to the Sylow $p$-subgroup of $\mathbb{T}_n$, and since the order of $\mathbb{T}_n$ is divisible by $p^{n+1}$, $V_n$ is a finite cyclic group with order divisible by $p^{n+1}$.

Now, applying class field theory for $F_\alpha/k_\alpha$, one sees that $e(w_\alpha/v_\alpha)$ is the order of the image of the product of maps $V_n \to U_n \to U_n/\bar{E}_n$. Hence the order of the image of $V_n \to U_n/E_nU_{n,p^{n+1}}$ is at most equal to $e(w/v) = p^\alpha$, and it follows that

$$V_n^\times \times 1 \times \cdots \times 1 \subseteq E_nU_{n,p^{n+1}} \subseteq U_n = \prod_z U_{n,z}.$$  

Consequently, if $n \geq a$, then there exists a unit $\varepsilon$ in $E_n$ such that $\varepsilon$ is a $p^{n+1}$-th power in $k_{n,z}$ for every $p$-place $z$ on $k_\alpha$, but is at most a $p^\alpha$-th power in $k_{n,v_\alpha}$. Let $\zeta$ be a primitive $2p$-th root of unity in $C$ and let $k' = k(\zeta)$, $K' = k'_\alpha = \mathbb{K}(\zeta)$. Replacing $k$ by $K \cap k'$ if necessary, we may assume that $K \cap k' = k$ so that $k_{\alpha}(\zeta)$ is the $n$-th intermediate field of the $\mathbb{Z}_p$-extension $K'/k'$ for all $n \geq 0$: $k_n = k_{\alpha}(\zeta)$. Let $v'$ be an extension of $v$ on $K'$, let $v'_z = v'|k'_z$, and let $V_z'$ be the group defined for the local field $k'_z, v'_z$, similarly as $V_n$ for $k_\alpha$. Since the degree $[t_{n,v}: t_{n,v_\alpha}]$ is a factor of $b = [k': k] = [k'_z: k_z]$ and since $b|p - 1$ if $p > 2$ and $b = 1$ or 2 if $p = 2$, it follows that $V'_z = V_z$ for $p > 2$ and $[V'_z: V_z] = 1$ or 2 for $p = 2$, $n \geq 1$. Consequently, we see that $\varepsilon$ is at most a $p^{n+1}$-th power in the local field $k'_z, v'_z$, for $n > a$. Let $\varepsilon_\alpha$ denote a $p^{n+1}$-th root of $\varepsilon$ in $C$. As $k'_\alpha$ contains primitive $p^{n+1}$-th roots of unity, it follows from the above that $k'_\alpha(\varepsilon_\alpha)/k'_\alpha$ is an unramified cyclic $p$-extension, of which the local degree at $v'_z$ is divisible by $p^{n+1}p^{a-1}p^{n-a}$. Therefore, by class field theory, the order of the ideal-class of $p_{v'_z}$ in $k'_\alpha$ is divisible by $p^{n-a}$ for all $n > a$. However, this is impossible because, for a non-$p$-place $v'$, the order of the ideal-class of $p_{v'}$ in $k'_\alpha$ is equal to the order of the ideal-class of $p_{v'}$ in $K'$ whenever $n$ is large enough.
The contradiction proves that \(e(w/v)\) is infinite, namely, that \(v\) is infinitely ramified in \(L\).

Now, let \(S\) be any set of places on a \(\mathbb{Z}_p\)-field \(K\), containing all \(p\)-places of \(K\), and let \(S_0\) denote the subset of all finite non-\(p\)-places \(v\) in \(S\) such that the order of \(t_v\) is divisible by \(p^\alpha\). Let \(L_0\) denote the maximal abelian \(p\)-extension over \(K\), unramified outside \(S\), and let \(L\) be any \(p\)-extension over \(K\), containing \(L_0\) and unramified outside \(S\): \(K \subseteq L_0 \subseteq L\). Let \(v\) be a finite non-\(p\)-place on \(K\). Then it follows from Lemmas 3, 4 that \(v\) is unramified in \(L\) or infinitely ramified in \(L\) according as \(v \in S_0\) or \(v \not\in S_0\). Hence we may apply Lemma 2 for such an extension \(L/K\).

For each integer \(n \geq 1\), let \(W_n\) denote the group of all \(n\)-th roots of unity in \(C\), and let

\[
W(p) = \bigcup_{n \geq 0} W_{p^n}.
\]

Then a \(\mathbb{Z}_p\)-field \(K\) contains \(W(p)\) if and only if it contains \(W_{2p}\). When this happens, we shall call \(K\) a cyclotomic \(\mathbb{Z}_p\)-field. Let \(v\) be any finite non-\(p\)-place on such a cyclotomic \(\mathbb{Z}_p\)-field \(K\). It is clear that the order of \(t_v\) is then divisible by \(p^\alpha\). Let \(\psi_v = (\alpha)\) with \(\alpha \in K^\times\), \(a \geq 1\), and let \(\alpha_n\) be a \(p^\alpha\)-th root of \(\alpha\) in \(C\) for \(n \geq 1\). Then one sees easily that the field \(L\) in Lemma 4 contains all \(\alpha_n\), \(n \geq 1\), so that \(v\) is infinitely ramified in \(L\). Thus the proof of Lemma 4 is much simpler in this case.

4. We need another lemma as follows:

**Lemma 5.** Let \(K\) be a number field containing \(Q_\infty\) (e.g., a \(\mathbb{Z}_p\)-field) and let \(L/K\) be a \(p\)-extension, unramified at every infinite, i.e., archimedean, place on \(K\). Then

\[
H^n(L/K, L^\times) = 0, \quad \text{for all} \quad n \geq 1.
\]

**Proof.** We may assume that \(L/K\) is finite. Since \(H^1(L/K, L^\times) = 0\), it is sufficient to prove \(H^2(L/K, L^\times) = 0\). Let \(K = \lim_{\rightarrow} k_n\), \(L = \lim_{\rightarrow} k_n'\) where for each \(n \geq 0\), \(k_n'/k_n\) is a Galois extension of finite algebraic number fields such that \(k_n'K = L\), \(k_n' \cap K = k_n\). Then it follows from the assumption that whenever \(n\) is large enough, \(k_n'/k_n\) is unramified at every infinite place of \(k_n\). On the other hand, since \(K\) contains \(Q_\infty\), the local degree of the extension \(K/Q\) at each finite place of \(K\) is divisible by \(p^\alpha\). Hence we obtain \(H^2(L/K, L^\times) = 0\) by the same argument as in the proof of [9], Chap. II, Proposition 9.

Now, in general, for each number field \(K\), let \(E_K\) and \(W_K\) denote the group of all units of \(K\) and the group of all roots of unity in \(K\),

\[3\text{) See [8], Chap. IX, Théorème 8.}\]
respectively. Let $M/K$ be an arbitrary Galois extension of number fields and let $G = \text{Gal}(M/K)$. Then we have short exact sequences

\begin{align*}
0 &\rightarrow P_M \rightarrow I_M \rightarrow C_M \rightarrow 0, \\
0 &\rightarrow E_M \rightarrow M^\times \rightarrow P_M \rightarrow 0,
\end{align*}

and they induce long exact sequences for the cohomology groups $H^n(M/K, \_ ) = H^n(G, \_ )$, $n \geq 0$.

**Theorem 1.** Let $K$ be a $\mathbb{Z}_p$-field and let $M$ be a $p$-extension over $K$ with the following properties: (i) $C_M(p) = 0$ and $M/K$ is unramified at every infinite place of $K$, (ii) each finite non-$p$-place on $K$ is either unramified in $M$ or infinitely ramified in $M$. Then

\[ H^n(M/K, E_M) = 0, \text{ for all } n \geq 2, \]

and there exists an exact sequence

\[ 0 \rightarrow C_K(p) \rightarrow H^1(M/K, E_M) \rightarrow \bigoplus_v A_v \rightarrow 0 \]

where $v$ ranges over all non-$p$-places $v$ on $K$, ramified in $M$, and where, for each $v$,

\[ A_v = p_v^C/p_v^C \cong \mathbb{Q}_p/\mathbb{Z}_p, \quad R = \bigcup_{n>0} p^{-n}\mathbb{Z}. \]

**Proof.** Since $G = \text{Gal}(M/K)$ is a pro-$p$-group,

\[ H^n(M/K, C_M) = H^n(M/K, C_M(p)) = 0, \text{ for } n \geq 1. \]

By Lemmas 2, 5, we also have

\[ H^n(M/K, I_M) = 0, \quad H^n(M/K, M^\times) = 0, \text{ for } n \geq 1. \]

Therefore (1) induces exact sequences and isomorphisms as follows:

\begin{align*}
I^0_M &\rightarrow C_M^0 \rightarrow H^1(M/K, P_M) \rightarrow 0, \quad H^n(M/K, P_M) = 0, \quad n \geq 2, \\
K^\times &\rightarrow P_M^0 \rightarrow H^1(M/K, E_M) \rightarrow 0, \quad H^n(M/K, P_M) \cong H^{n+1}(M/K, E_M), \quad n \geq 1.
\end{align*}

However, since $H^1(M/K, P_M)$ is a $p$-primary abelian group, the first exact sequence and $C_M(p) = 0$ induce $H^1(M/K, P_M) = 0$. Hence

\[ H^n(M/K, E_M) = 0, \text{ for all } n \geq 2. \]

We also obtain from the second exact sequence that

\[ H^1(M/K, E_M) \cong P_M^0/P_K = (I^0_M \cap P_M)/P_K. \]

From $P_K \subseteq I_K \cap P_M \subseteq I^0_M \cap P_M$, we then see that both $I_K \cap P_M/P_K$ and $I^0_M \cap P_M/I_K \cap P_M$ are $p$-primary abelian groups. Now, in the exact sequence

\[ 0 \rightarrow I_K \cap P_M/P_K \rightarrow I_K/P_K \rightarrow I_K/I_K \cap P_M \rightarrow 0, \]

we have

\[ H^n(M/K, C_M(p)) = 0, \text{ for all } n \geq 1. \]

By the universal cohomology sequence, we have the long exact sequence

\[ \cdots \rightarrow H^n(M/K, C_M(p)) \rightarrow H^n(M/K, E_M) \rightarrow H^{n+1}(M/K, P_M) \rightarrow \cdots \]

and since $H^n(M/K, C_M(p)) = 0$, we get

\[ H^n(M/K, E_M) \cong \bigoplus_{v} A_v. \]
we have $I_K/I_K \cap P_M = I_KP_M/P_M \subseteq I_M/P_M$. Hence we obtain an exact sequence

$$0 \to I_K \cap P_M/P_K \to C_K(p) \to C_M(p) \to 0.$$ 

On the other hand, we also have the exact sequence

$$0 \to I_M^0 \cap P_M/I_K \cap P_M \to I_M^0/I_K \to I_M^0/(I_M^0 \cap P_M)I_K \to 0.$$ 

Since $I_M^0/I_K$ is easily seen to be $p$-primary and since

$I_M^0/(I_M^0 \cap P_M)I_K$ is a factor group of a subgroup of $C_M(p)$.

The assumption $C_M(p) = 0$ then implies

$$I_K \cap P_M/P_K \cong C_K(p), \quad I_M^0 \cap P_M/I_K \cap P_M \cong I_M^0/I_K.$$ 

Therefore, by Lemma 2 and the isomorphism (2) above, one obtains the exact sequence for $H^1(M/K, E_M)$ stated in the theorem.

REMARK. For any Galois extension $L/K$ of number fields, we see easily that $H^1(L/K, I_L) = 0$. Since $H^1(L/K, L^\sim) = 0$, it follows from (1) that

$$H^1(L/K, E_L) \cong P_L^0/P_K, \quad \text{Ker}(H^2(L/K, E_L) \to H^2(L/K, L^\sim)) \cong \text{Coker}(I_L^0 \to C_L^0).$$

When both $K$ and $L$ are finite over $Q$, these isomorphisms are well known in the classical literature.

5. Let $K$ be a number field. In the following, we shall denote the $p$-primary part $C_K(p)$ of the ideal-class group $C_K$ simply by $A_K$:

$$A_K = C_K(p).$$

As a $p$-primary abelian group, $A_K$ is a torsion $Z_p$-module. For a $Z_p$-field $K$, the following facts are known on the structure of the $Z_p$-module $A_K$.\(^6\)

Namely, let $K = k_\infty = kQ_\infty$ with $k$ finite over $Q$ and let $\lambda = \lambda(K/k)$ and $\mu = \mu(K/k)$ denote respectively the so-called $\lambda$- and $\mu$-invariant of the $Z_p$-extension $K/k$. Then

$$A_K \cong (Q_p/Z_p)^{\lambda} \oplus A'$$

with $A'$ a $Z_p$-module of bounded exponent: $p^aA' = 0$, $a \geq 0$. Furthermore, if $\mu = 0$, then $A' = 0$ so that

$$A_K \cong (Q_p/Z_p)^{\lambda}, \quad A_K/pA_K = 0;$$

and if $\mu > 0$, then $A'$ is infinite so that $A_K/pA_K$ is an infinite $Z_p$-module.

\(^6\) For the results stated below, see [4], [5].
Now, it follows from the above that $\lambda = \lambda(K/k)$ depends only upon the structure of the $\mathbb{Z}_p$-module $A_K$ and is independent of the choice of $k$ such that $K = k_\omega$. Hence it may be denoted by $\lambda_K$; $\lambda_K = \lambda(K/k)$. Similarly, since $A_K/pA_K$ is zero or infinite according as $\mu = 0$ or $\mu > 0$, the fact that $\mu(K/k) = 0$ is actually a property of $K$ so that it may be simply written as

$$\mu_K = 0.$$

The isomorphism for $A_k$ shows that in the case $\mu_k = 0$, $A_K$ gives us a good analogue of the $p$-power division points of the Jacobian variety of an algebraic curve and, hence, $\lambda_K$ an analogue of twice the genus of that curve.

In general, for each torsion $\mathbb{Z}_p$-module $A$, let

$$V(A) = \text{Hom}_{\mathbb{Z}_p}(A, \mathbb{Q}_p/A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$  

Then $A \mapsto V(A)$ defines an exact contravariant functor from torsion $\mathbb{Z}_p$-modules into vector spaces over $\mathbb{Q}_p$. For $A = A_K$, let

$$V_K = V(A_K).$$

Since $V(A') = 0$ for the above $\mathbb{Z}_p$-module $A'$, we then have

$$V_K \cong \mathbb{Q}_p^\omega, \quad \lambda_K = \dim_{\mathbb{Q}_p} V_K.$$

Now, it has been conjectured for some time that $\mu_K = 0$ for all $\mathbb{Z}_p$-fields $K$. The conjecture was proved by Ferrero-Washington [3] in the case where $K$ is an abelian extension over the rational field $\mathbb{Q}$, but the problem is yet unsolved in the general case. As an application of Theorem 1, we shall next give a necessary and sufficient condition for $\mu_k = 0$ when $K$ is a cyclotomic $\mathbb{Z}_p$-field.

**Theorem 2.** Let $K$ be a cyclotomic $\mathbb{Z}_p$-field, $S$ a finite set of places on $K$, including all $p$-places of $K$, and $M$ the maximal $p$-extension over $K$, unramified outside $S$. Then $\mu_K = 0$ if and only if $\text{Gal}(M/K)$ is a free pro-$p$-group.

**Proof.** Since there is no non-trivial unramified abelian $p$-extension over $M$, we see easily that $A_M = C_p(p) = 0$. As $K$ contains $W(p)$, it is a totally imaginary field so that $M/K$ is unramified at every infinite place of $K$. By the remark after Lemma 4, each finite non-$p$-place on $K$ is either unramified or infinitely ramified in $M$. Therefore both conditions (i) and (ii) in Theorem 1 are satisfied for the extension $M/K$.

---

7) This is essentially a known result. Cf. [1], Corollary 2.5. A proof is included here to clarify, in this simpler case, the main idea of arguments which will again be applied later to prove more elaborate results.
other hand, we also see from the definition of $M$ that the map $\varepsilon \mapsto \varepsilon^p$ for $\varepsilon$ in $E_M$ defines an exact sequence

$$0 \rightarrow W_p \rightarrow E_M \rightarrow E_M^p \rightarrow 0,$$

and this induces the exact sequence

$$H^1(M/K, EM) \rightarrow H^1(M/K, EM)^p \rightarrow H^2(M/K, W_p) \rightarrow H^2(M/K, EM),$$

where $H^2(M/K, EM) = 0$ by Theorem 1. Hence

$$H^2(M/K, W_p) \cong H^1(M/K, EM)/pH^1(M/K, EM).$$

However, by the same theorem, there exists an exact sequence

$$0 \rightarrow A_K \rightarrow H^1(M/K, EM) \rightarrow \bigoplus_v A_v \rightarrow 0$$

where $v$ ranges over a finite set and $A_v \cong \mathbb{Q}_p/\mathbb{Z}_p$ for every such $v$. Since $A_K/pA_K$ is zero or infinite according as $\mu_K = 0$ or $\mu_K > 0$, it follows from the above exact sequence that $\mu_K = 0$ if and only if $H^2(M/K, W_p) = 0$, i.e., $H^2(\text{Gal}(M/K), \mathbb{Z}/p\mathbb{Z}) = 0$. As $\text{Gal}(M/K)$ is a pro-$p$-group, the last equality means that $\text{Gal}(M/K)$ is a free pro-$p$-group. Hence the theorem is proved. Note that the finiteness of the set $S$ is used only to deduce $\mu_K = 0$ from $H^2(M/K, W_p) = 0$, and not in the opposite deduction.

6. Let $J$ denote the complex-conjugation of the complex field $C$. When a number field $K$ is invariant under the automorphism $J$ of $C$, the restriction of $J$ on the subfield $K$ will be simply denoted again by $J$. In such a case, $J$ acts on various abelian groups canonically associated with $K$, e.g., $K^\times$, $I_K$, $C_K$, etc. In general, when $J$ acts on an abelian group $A$, we define the subgroups $A^+$ and $A^-$ by

$$A^\pm = \{a \in A, J(a) = \pm a\}.$$

One sees immediately that if $A$ is uniquely divisible by 2, e.g., a $\mathbb{Z}_p$-module with $p > 2$, then

$$A = A^+ \oplus A^-.$$

For each number field $K$, let $K^+$ denote the maximal real subfield of $K$: $K^+ = K \cap R$. $K$ is called a number field of C-M type if $K^+$ is totally real, $K$ is totally imaginary, and $[K: K^+] = 2$. $K$ is then invariant under $J$, and

$$\text{Gal}(K/K^+) = \{1, J\}.$$

It is also known that for such $K$,

$$E_K^+ = E_K^+, \quad E_K^- = W_K, \quad [E_K: W_K E_K^+] = 1 \text{ or } 2.$$

---

\(^5\) See [9], Chap. I, §4.
We now assume that \( p > 2 \) and \( K \) is a \( \mathbb{Z}_p \)-field of C-M type. We can then fined a number field \( k \) of C-M type, finite over \( \mathbb{Q} \), such that \( K = k_m, K^+ = k_m^+ \). For such \( K/k \), we can define four invariants \( \lambda(K/k)^\pm, \mu(K/k)^\pm \) which have similar properties as explained in \( \S \) 5 for \( \lambda(K/k) \) and \( \mu(K/k) \).\(^9\) For example, \( \lambda(K/k)^\pm \) depend only upon \( K \) so that they may be denoted by \( \lambda_k \). In fact, we have

\[
A_K = A_K^+ \oplus A_K^-, \quad A_K^+ = A_{K^+},
\]

\[
V_K = V_K^+ \oplus V_K^-, \quad V_K^+ = V(A_K^-), \quad \dim_{\mathbb{Q}_p} V_K^\pm = \lambda_k^\pm.
\]

Furthermore, if \( \mu_k = 0 \), then

\[
A_K^- \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_k^-};
\]

and \( A_{K^+}/pA_{K^+} \) is zero or infinite according as \( \mu_k = 0 \) or \( \mu_k > 0 \).

In addition to the above, let us now also assume that \( K \) is a cyclotomic \( \mathbb{Z}_p \)-field, i.e., \( W(p) \subseteq K \). Let \( S^+ \) be a set of finite places on \( K^+ = K \cap \mathbb{R} \), containing all \( p \)-places of \( K^+ \), and let \( M^+ \) denote the maximal \( p \)-extension over \( K^+ \), unramified outside \( S^+ \). Let

\[
M = KM^+.
\]

Since \( M^+/K^+ \) is unramified at every infinite place on \( K^+ \), \( M^+ \) is totally real, and it follows that \( M \) is a number field of C-M type and that \( M = M \cap \mathbb{R} \), justifying the notation \( M^+ \). It is easy to see that \( M/K^+ \) is a Galois extension, that \( K \cap M^+ = K^+ \), and that

\[
\text{Gal}(M/K^+) = \text{Gal}(M/K) \times \text{Gal}(M/M^+),
\]

(4)

\[
\text{Gal}(M/K) = \text{Gal}(M^+/K^+).
\]

It is also known that \( \mu_K = 0 \) if and only if \( \mu_k = 0 \).

**Lemma 6.** The extension \( M/K \) has the properties (i), (ii) stated in Theorem 1 so that the cohomology groups \( H^n(M/K, E_\omega) \), \( n \geq 1 \), are given by that theorem.

**Proof.** As in the proof of Theorem 2, \( A_M = A_{M^+} = 0 \) for the maximal \( p \)-extension over \( K^+ \), unramified outside \( S^+ \). Since \( K \) is totally imaginary, \( M/K \) is unramified at every infinite place of \( K \). (This follows also from the fact that \( M/K \) is a \( p \)-extension with \( p > 2 \).) Let \( c \in A_M, pc = 0 \). Let \( a \) be an ideal of \( I_M \) in the ideal-class \( c \) and let \( a^\omega = (\alpha), \alpha \in M^\times \). Then \( b^\omega = (\beta) \) with \( b = a^{\omega-j}, \beta = \alpha^{\omega-j} \). Since \( M \) contains \( W_p \), \( M(\sqrt[p]{\beta})/M \) is a cyclic extension of degree 1 or \( p \). However, \( \beta^{1+j} = 1 \) implies that \( M(\sqrt[p]{\beta})/M^+ \) is abelian. Hence there exists a cyclic extension \( M^+ / M^+ \) which is of degree 1 or \( p \), unramified outside \( p \)-places of \( M^+ \),

\(^9\) See [5].
and satisfies $M(\sqrt[3]{\beta}) = MM'$. It then follows from the definition of $M'$ that $M' = M^+, M(\sqrt[3]{\beta}) = M$ so that $b = (\sqrt[3]{\beta})$ with $\sqrt[3]{\beta} \in M^\times$. Thus $(1 - J)c = 0$, $c \in A_\nu = 0$, and consequently $c = 0$. Therefore $A_\nu = 0$, $A_M = A_M' \oplus A_M'' = 0$, and the property (i) of Theorem 1 is verified for $M/K$. Next, let $v$ be a non-$p$-place on $K$ and let $v' = v|K^+$. Since $K^+ = k^+_\nu$ is a $\mathbb{Z}_p$-field, it follows from the remark after Lemma 4 that $v'$ is either unramified in $M^+$ or infinitely ramified in $M^+$. Using the fact that $\text{Gal}(M^+/K^+)$ is a pro-$p$-group with $p > 2$, we then see from (4) that $v$ is unramified or infinitely ramified in $M$ according as $v'$ is unramified or infinitely ramified in $M^+$. Hence $M/K$ has also the property (ii) of Theorem 1.

Let $v^+$ be any place on $K^+$ and let $v$ be an extension of $v^+$ on $K$. Then $v$ and $\bar{v} = J(v)$ are the only extensions of $v^+$ on $K$. As usual, we shall say that $v^+$ splits in $K$ if $v \neq \bar{v}$. Since each place on $K^+$ has at most two extensions on $K$, the above proof shows that if $S^+$ is a finite set, then there exist only a finite number of finite non-$p$-places $v$ on $K$ which are ramified in $M$; namely, the direct sum $\bigoplus_v A_v$ in the exact sequence for $H^1(M/K, E_n)$ in Theorem 1 is a finite sum.

**Theorem 3.** Let $K$ be a cyclotomic $\mathbb{Z}_p$-field of $\text{C-M type for } p > 2$ and let $S^+$ be a finite set of finite places on $K^+ = K \cap R$, including all $p$-places of $K^+$. Let $M^+$ be the maximal $p$-extension over $K^+$, unramified outside $S^+$, and let $s$ denote the number of finite non-$p$-places on $K^+$ which split in $K$ and are ramified in $M^+$. Then $\mu_K = 0$ if and only if $\text{Gal}(M^+/K^+)$ is a free pro-$p$-group, and if this is the case, then the minimal number of generators for $\text{Gal}(M^+/K^+)$ is $\lambda_K + s$.

**Proof.** As stated above, let $M = KM^+$. Then $\text{Gal}(M/K^+)$ acts on $E_M$ so that $J$ also acts on $H^*(M/K, E_M)$. Hence $H^*(M/K, E_M)^\times$ are defined. Since $p > 2$, it follows from (3), (4) and $W(p) \subseteq W_M$ that

$$H^*(M/K, E_M)^- = H^*(M/K, W_M) = H^*(M/K, W(p)),$$

for $n \geq 1$.

Therefore, by Theorem 1 and Lemma 6, we see that

$$H^*(M/K, W(p)) = 0,$$

for $n \geq 2$.

Furthermore, the exact sequence in Theorem 1 also implies an exact sequence

$$0 \to A_\kappa \to H^1(M/K, W(p)) \to (\bigoplus_v A_v)^- \to 0$$

where, as easily seen from the definition of $A_v$,

$$(\bigoplus_v A_v)^- \cong (Q_p/Z_p)'_\nu.$$
Now, from $H^2(M/K, W(p)) = 0$ and from the exact sequence
\[ 0 \to W_p \to W(p) \xrightarrow{p} W(p) \to 0, \]
one obtains
\[ H^2(M/K, W_p) \cong H^1(M/K, W(p))/pH^1(M/K, W(p)). \]
On the other hand, $A_{K}/pA_{K}$ is zero or infinite according as $\mu_{K} = 0$ or $\mu_{K} > 0$. Therefore, similarly as in the proof of Theorem 2, we conclude from the above exact sequence for $H^1(M/K, W(p))$ that $\mu_{K} = 0$ if and only if $H^1(M/K, W_p) = 0$, namely, that $\mu_{K} = 0$ if and only if $\text{Gal}(M^+/K^+) = \text{Gal}(M/K)$ is a free pro-$p$-group. Furthermore, when this is the case, then $A_{K} \cong (Q_p/Z_p)^{\lambda}$ so that
\[ H^1(M/K, W(p)) \cong (Q_p/Z_p)^{\lambda+s}. \]
However, since $W(p) \subseteq K$, $H^1(M/K, W(p))$ is the Pontrjagin dual of the factor commutator group of $\text{Gal}(M/K)$. Therefore the above isomorphism indicates that $\lambda + s$ is the minimal number of generators for the free pro-$p$-group $\text{Gal}(M^+/K^+)$. We note here that an essential difference between Theorem 2 and Theorem 3 lies in that the free pro-$p$-group $\text{Gal}(M^+/K^+)$ in Theorem 3 is finitely generated while this is not so for the free pro-$p$-group $\text{Gal}(M/K)$ in Theorem 2.

We shall next also briefly explain a generalization of Theorem 3. Let $K'$ be a totally real $\mathbb{Z}_p$-field with $p > 2$. Let $S'$ be a finite set of finite places on $K'$, including all $p$-places of $K'$, and let $M'$ denote the maximal $p$-extension over $K'$, unramified outside $S'$. Let $K = K'(W_p)$. Then $K$ is a cyclotomic $\mathbb{Z}_p$-field of C-M type and $K/K'$ is a cyclic extension with degree a factor of $p - 1$. In fact, there exists a monomorphism $\chi : \text{Gal}(K/K') \to \mathbb{Z}_p^\times$ such that $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for all $\sigma \in \text{Gal}(K/K')$ and $\zeta \in W(p) \subseteq K$. Let $A_{K}^{(p)}$ denote the submodule of $A_{K} = C_{K}(p)$, consisting of all $a$ in $A_{K}$ such that $\sigma(a) = \chi(\sigma)a$ for every $\sigma$ in $\text{Gal}(K/K')$. The $\mathbb{Z}_p$-module $A_{K}^{(p)}$ is then a direct summand of $A_{K}$ and it has similar properties as mentioned earlier for $A_{K}$ and $A_{K}^\times$; for example, if $A_{K}^{(p)} = pA_{K}^{(p)}$, then
\[ A_{K}^{(p)} \cong (Q_p/Z_p)^{\lambda} \]
with an integer $\lambda = \lambda_{K}^{(p)} \geq 0$. Let $s$ be the number of finite non-$p$-places on $K'$ which are ramified in $M'$ and which split completely in $K$. 

\[ \text{RIEMANN-HURWITZ FORMULA} \]
Now, it can be proved that the Galois group $\text{Gal}(M'/K')$ is a free pro-$p$-group if and only if $A(1)_K = pA(1)_K$, and if this is the case, then the minimal number of generators for $\text{Gal}(M'/K')$ is $\lambda(1)_K + s$. The proof is similar to that of Theorem 3, the key fact in this case being $C_n(p)^{(i)} = 0$ for $M = KM'$. However, we omit the detail. It is clear that $A(1)_K = pA(1)_K$ follows from $A_K = pA_K$, namely, from $\mu_K = 0$. Therefore $\mu_K = 0$ for $K = K'(W'_p)$ implies that $\text{Gal}(M'/K')$ is a free pro-$p$-group. Hence it follows from the theorem of Ferrero-Washington [3] that for any $\mathbb{Z}_p$-field $K'$, $p > 2$, which is real and abelian over $\mathbb{Q}$, the Galois group $\text{Gal}(M'/K')$ is always a free pro-$p$-group with a finite number of generators.

7. In general, let $K$ be a $\mathbb{Z}_p$-field, and $L/K$ a finite Galois extension with $G = \text{Gal}(L/K)$. Then $L$ is again a $\mathbb{Z}_p$-field and $G$ acts on $A_L = C_L(p)$ in the natural manner. Therefore $G$ acts also on the vector space $V_L = V(A_L)$ defined in §5 and we obtain a $\lambda_L$-dimensional $p$-adic representation

$$\pi_{L/K} : G = \text{Gal}(L/K) \rightarrow GL(V_L).$$

Let $p > 2$ and assume that both $K$ and $L$ are number fields of C-M type. Then $L/K^+$ is a Galois extension and

$$\text{Gal}(L/K^+) = \text{Gal}(L/K) \times \text{Gal}(L/L^+), \quad \text{Gal}(L/K) = \text{Gal}(L^+/K^+).$$

Consequently, we have the decomposition for $\pi_{L/K}$:

$$\pi_{L/K} = \pi_{L/K}^+ \oplus \pi_{L/K}^-$$

where

$$\pi_{L/K}^- : G \rightarrow GL(V_L^-).$$

Let us next investigate the above representation $\pi_{L/K}^-$ in the case where $L/K$ is a finite $p$-extension and $K$ is a cyclotomic $\mathbb{Z}_p$-field, i.e., $W(p) \subseteq K$. We first note that there exist only a finite number of finite places on $K^+$ which are ramified in $L^+$; in fact, this is true in general for any finite extension of $\mathbb{Z}_p$-fields. Since $L^+/K^+$ is unramified at every infinite place of $K^+$, there exists a finite set $S^+$ of finite places on $K^+$, including all $p$-places of $K^+$, such that $L^+$ is contained in the maximal $p$-extension $M^+$ over $K^+$, unramified outside $S^+$:

$$K^+ \subseteq L^+ \subseteq M^+.\notag$$

For $M = KM^+$, we then have

$$K \subseteq L \subseteq M.\notag$$

It is clear that $M^+$ is the maximal $p$-extension over $L^+$, unramified outside the set of extensions, on $L^+$, of all $v^+$ in $S^+$. Thus $M^+/L^+$ is the same kind of extension as $M^+/K^+$ in Lemma 6 so that there exists an
exact sequence

\[ 0 \to A_L \to H^1(M/L, E_w) \to \bigoplus_w A_w \to 0 \]

where \( w \) ranges over all finite non-\( p \)-places on \( L \), ramified in \( M \). Furthermore, in this case, the maps in the exact sequence are homomorphisms over \( \text{Gal}(L/K^+) \). Hence it induces an exact sequence of \( G \)-modules:

\[ 0 \to A_L^- \to H^1(M/L, E_w^-) \to \bigoplus_w A_w^- \to 0, \]

where \( H^i(M/L, E_w^-) = H^i(M/L, W(p)) \) as explained in the proof of Theorem 3. Let \( v^+ = w|K^+ \). By the remark after Lemma 4, \( v^+ \) is either unramified in \( M^+ \) or infinitely ramified in \( M^+ \). Therefore, if \( w \) is ramified in \( M \), then \( v^+ \) is ramified in \( M^+ \), and the converse is also true. In general, for each finite non-\( p \)-place \( v^+ \) on \( K^+ \), define a module \( B_{v^+} \) over \( G = \text{Gal}(L^+/K^+) \) by

\[ B_{v^+} = \bigoplus_{w^+} A_{w^+}, \]

with \( w^+ \) ranging over all extensions of \( v^+ \) on \( L^+ \). Then we obtain from the above an exact sequence of \( G \)-modules:

\[ 0 \to A_L^- \to H^1(M/L, W(p)) \to \bigoplus_{v^+} B_{v^+} \to 0, \]

where \( v^+ \) now runs over all finite non-\( p \)-places on \( K^+ \), ramified in \( M^+ \) and split in \( K \). Let

\[ V_0 = V(H^1(M/L, W(p))) \]

with the functor \( V \) defined in §5. Since \( V \) is exact, it follows from the above that

\[ V_0 \cong V_L^- \oplus \bigoplus_{v^+} V(B_{v^+}) \]

as representation spaces for the finite group \( G \). Thus

(5)

\[ \pi_0 = \pi_{L/K} \oplus \bigoplus_{v^+} \pi_{v^+} \]

with \( \pi_0 \) and \( \pi_{v^+} \) denoting the representations of \( G \) on the spaces \( V_0 \) and \( V(B_{v^+}) \) respectively. Now, for each \( v^+ \), fix an extension \( w^+ \) of \( v^+ \) on \( L^+ \), and let \( T = T(w^+/v^+) \) by §1 so that as \( G \)-modules,

\[ B_{v^+} \cong (Q_p/Z_p)[G/T] \]

where the right hand side denotes the linear combinations of the left cosets of \( G \) modulo \( T \) with coefficients in \( Q_p/Z_p \). Consequently

\[ V(B_{v^+}) \cong Q_p[G/T], \]

and we see that \( \pi_{v^+} \) is isomorphic to the representation of \( G \) over the
field $Q_p$, induced by the trivial one-dimensional representation of the subgroup $T = T(w^+/v^+)$. It is then clear from (5) that the representation $\pi_{L/K}$ is completely determined if we know the representation $\pi_0$ of $G$ on the space $V_0 = V(H'(M/L, W(p))$.

Let

$$X = \text{Gal}(M^+/K^+) = \text{Gal}(M/K), \quad Y = \text{Gal}(M^+/L^+) = \text{Gal}(M/L).$$

Then $Y$ is a closed normal subgroup of the pro-$p$-group $X$ and

$$X/Y = \text{Gal}(L^+/K^+) = \text{Gal}(L/K) = G.$$ 

As explained in the proof of Theorem 3, $H'(M/L, W(p))$ is the Pontrjagin dual of $Y^{ab}$, the factor commutator group of $Y$. Since $W(p) \subseteq K$, we see that as $G$-modules,

$$V_0 \cong Y^{ab} \otimes_{\mathbb{Z}_p} Q_p,$$

where the action of $G = X/Y$ on the right is given by conjugations in $X$. Let us now assume that $\ell_K = 0$. Then it follows from Theorem 3 that $X$ is a free pro-$p$-group with $\lambda_K + s$ generators, where $s$ denotes the number of places $v^+$ in the direct sum in (5). Therefore the representation $\pi_0$ can be described by the following purely group-theoretical lemma:

**LEMMA 7.** Let $X$ be a free pro-$p$-group with $m$ generators, $m \geq 1$, and let $Y$ be a closed normal subgroup with finite index in $X$. Then the representation $\pi_0$ of the finite group $G = X/Y$ on the vector space $Y^{ab} \otimes_{\mathbb{Z}_p} Q_p$ is given by

$$\pi_0 = \pi_1 \oplus (m - 1)\pi_G,$$

where $\pi_1$ denotes the one-dimensional trivial representation of $G$ over $Q_p$, and $\pi_G$ the regular representation of $G$ over $Q_p$.

**PROOF.** Let $I_G$ denote the augmentation ideal of the group ring $\mathbb{Z}_p[G]$ so that

$$0 \to I_G \to \mathbb{Z}_p[G] \to \mathbb{Z}_p \to 0$$

is exact. Then there exists an exact sequence of $\mathbb{Z}_p[G]$-modules:

$$0 \to Y^{ab} \to \mathbb{Z}_p[G]^m \to I_G \to 0.$$

The lemma follows from this by replacing each term of the above by its tensor product with $Q_p$ over $\mathbb{Z}_p$.

We now consider again the case where $X = \text{Gal}(M/K)$, $Y = \text{Gal}(M/L)$, and $W(p) \subseteq K$, where $m$ need not be the minimal number of generators for $G$. 

---

10) See [10]. Note that $m$ need not be the minimal number of generators for $G$. 

---
RIEMANN-HURWITZ FORMULA

and \( G = X/Y = \text{Gal}(L/K) \). We know that \( X \) is a free pro-p-group with \( m = \lambda_K + s \) generators. Assume that \( G \neq 1 \), i.e., \( K \neq L \). Then \( X \neq 1 \), \( m \geq 1 \) so that we obtain from (5) and Lemma 7 that

\[
\pi_1 \bigoplus (\lambda_K + s - 1)\pi_0 = \pi_{L/K} \bigoplus \bigoplus_{\nu^+} \pi'_{\nu^+},
\]

where \( s \) is exactly the number of places \( \nu^+ \) which appear on the right. For such a place \( \nu^+ \), let \( w^+ \) denote an extension of \( \nu^+ \) on \( L^+ \) and let \( T = T(w^+/\nu^+) \). Then \( \pi_{\nu^+} \) is the representation of \( G \) over \( Q_p \), induced by the trivial representation \( \pi_1 | T \) of the subgroup \( T \). Therefore

\[
\pi_G = \pi_{\nu^+} \bigoplus \pi'_{\nu^+}
\]

where \( \pi'_{\nu^+} \) is the representation of \( G \) over \( Q_p \), induced by the representation \( \pi_1 - \pi_1 | T \) for \( T \). Note that when we change the extension \( w^+ \) of \( \nu^+ \) on \( L^+ \), the inertia group \( T(w^+/\nu^+) \) is replaced by its conjugate in \( G \) so that \( \pi_{\nu^+} \) and \( \pi'_{\nu^+} \) are unchanged (up to isomorphisms). We now obtain from the above that

(6) \[
\pi_{L/K} = \pi_1 \bigoplus (\lambda_K - 1)\pi_0 \bigoplus \bigoplus_{\nu^+} \pi'_{\nu^+}
\]

where \( \nu^+ \) ranges over all finite non-p-places on \( K^+ \) which are ramified in \( M^+ \) and split in \( K \). However, if \( \nu^+ \) is unramified in \( M^+ \), then \( T(w^+/\nu^+) = 1 \) so that \( \pi_{\nu^+} = \pi_G, \pi'_{\nu^+} = 0 \). Hence the sum in (6) may be taken over all \( \nu^+ \) which split in \( K \). Note also that if \( \lambda_K = 0 \), then the right-hand side of (6) should be interpreted as the difference of the sum over \( \nu^+ \) and the representation \( \pi_0 - \pi_1 \).

Finally, if \( G = 1 \), then \( K = L, V_K = V_L, \) and \( \pi_{L/K} = \lambda_K \pi_1 \). Since \( \pi'_{\nu^+} = 0 \) for all \( \nu^+ \), the equality (6) still holds in this case. Thus we have proved the following

**THEOREM 4.** Let \( p > 2 \) and let \( L/K \) be a finite p-extension of cyclotomic \( \mathbb{Z}_p \)-fields of C-M type. Let \( \pi_{L/K}: G \to \text{GL}(V_L) \) be the representation of \( G = \text{Gal}(L/K) \) on the vector space \( V_L = V(A_L) \) over \( Q_p \). Assume that \( \pi_K = 0 \). Then

\[
\pi_{L/K} = \pi_1 \bigoplus (\lambda_K - 1)\pi_0 \bigoplus \bigoplus_{\nu^+} \pi'_{\nu^+}.
\]

Here \( \pi_1 \) is the one-dimensional trivial representation of \( G \) over \( Q_p \), \( \pi_0 \) is the regular representation of \( G \) over \( Q_p \), \( \nu^+ \) ranges over all finite non-p-places on \( K^+ = K \cap R \) which split in \( K \), and \( \pi'_{\nu^+} \) denotes the complement in \( \pi_0 \) of the representation \( \pi_{\nu^+} \) of \( G = \text{Gal}(L^+/K^+) \), induced by the one-dimensional trivial representation, over \( Q_p \), of the inertia group \( T(w^+/\nu^+) \) of \( \nu^+ \) for the Galois extension \( L^+/K^+ \).
As mentioned above, when $\lambda_K = 0$, the right hand side of the formula should be interpreted as the difference of the sum over $v^+$ and $\pi_G - \pi_1$.

8. Again, let $p > 2$ and let $L/K$ be a finite $p$-extension of $\mathbb{Z}_p$-fields of C-M type. We shall next study the representation $\pi_{L/K}$ in the case where $K$ is not cyclotomic. Since $p > 2$, $[Q(W_p):Q] = p - 1$, $L$ also is then non-cyclotomic and $W_p$ is not contained in $W_L$. We can find a finite set $S$ of finite places on $K$, including all $p$-places of $K$, such that $L$ is contained in the maximal $p$-extension $M$ over $K$, unramified outside $S$: $K \subseteq L \subseteq M$. Furthermore, we may choose $S$ so that it is invariant under the automorphism $J$ of $K/K^+$. Then $M/K^+$ is a Galois extension. Clearly, if $S'$ denotes the set of all extensions, on $L$, of the places in $S$, then $M$ is the maximal $p$-extension over $L$, unramified outside $S'$. Therefore, as in the proof of Theorem 2, we can see that both extensions $M/K$ and $L/K$ satisfy the conditions (i), (ii) of Theorem 1; here one has only to note that both $K$ and $L$ are totally imaginary because they are number fields of C-M type. It then follows from Theorem 1 that

$$H^n(M/L, E_u) = 0, \text{ for all } n \geq 2.$$

Therefore the Hochschild-Serre spectral sequence for $K \subseteq L \subseteq M$ induces\textsuperscript{11) an exact sequence

$$0 \to H^1(L/K, E_u) \to H^1(M/K, E_u) \to H^1(L/K, H^1(M/L, E_u)),$$

$$H^2(L/K, E_u) \to H^2(M/K, E_u) \to H^1(L/K, H^1(M/L, E_u)),$$

$\cdots$.

Since $M/K^+$ and $M/L^+$ are Galois extensions, the automorphism $J$ acts on each term of the above exact sequence, and we obtain similar exact sequences where $H^n(\ , )$ are replaced by $H^n(\ , )^\pm$. By Theorem 1,

$$H^n(M/K, E_u) = H^n(M/K, E_u)^\pm = 0, \text{ for } n \geq 2.$$

Since $W_p$ is not contained in $W_L$,

$$H^n(L/K, E_u) = H^n(L/K, W_L) = 0, \text{ for } n \geq 1.$$

Therefore it follows from the exact sequence for $H^n(\ , )^-$ that

$$A^0 \cong H^1(M/K, E_u)^-, \quad H^n(G, A) = 0, \text{ for } n \geq 1$$

where we put

$$G = \text{Gal} (L/K), \quad A = H^1(M/L, E_u)^-.$$

\textsuperscript{11) See [7], Chap. VI, Théorème 4.} Of course, one has to consider here Galois cohomology groups instead of cohomology groups of discrete groups.
Let now denote the number of finite non-$p$-places $v^+$ on $K^+$ which split in $K$ and are ramified in $M$. Similarly as in §7, Theorem 1 for $M/K$ and $M/L$ then give us the exact sequences

$$0 \to A_{K}^{-} \to H^1(M/K, E_n^{-}) \to \bigoplus_{v^+} A_{v^+} \to 0,$$

(7)

$$0 \to A_{L}^{-} \to A \to \bigoplus_{v^+} B_{v^+} \to 0,$$

where $v^+$ ranges over the places on $K^+$ as mentioned above and where $A_{v^+}$ and $B_{v^+}$ are defined in the same manner as in §7.

Assume now that $\mu_K = 0$. It is known in general that this induces $\mu_L = 0$ for a finite $p$-extension $L/K$. Therefore $\mu_K = \mu_L = 0$ so that

$$A_{K}^{-} \cong (Q_p/Z_p)^{\lambda_K}, \quad A_{L}^{-} \cong (Q_p/Z_p)^{\lambda_L},$$

as explained in §6. Hence we obtain from the above that

$$A^g \cong (Q_p/Z_p)^{\lambda_K+s}, \quad A \cong (Q_p/Z_p)^t,$$

with $s$ defined above and with a certain integer $t \geq \lambda_L$. Let

$$A_p = \ker (p: A \to A)$$

so that $0 \to A_p \to A \to 0$ is exact. Then $H^n(G, A) = 0$, for $n \geq 1$, imply

$$H^n(G, A_p) = 0, \quad \text{for all } n \geq 2.$$

Since $G$ is a finite $p$-group, it follows that $A_p$ is free over $(Z/pZ)[G]^{12}).$ From (8), we then see that

$$A \cong (Q_p/Z_p)[G]^{12+s}.$$ 

Let $\pi_o$ denote as before the representation of $G$ on the vector space $V_o = V(A)$ over $Q_p$. Then the above isomorphism implies

$$V_0 \cong Q_p[G]^{12+s}, \quad \pi_o = (\lambda_K + s)\pi_o$$

with $\pi_o$ denoting again the regular representation of $G$ over $Q_p$. From the exact sequence (7), we again obtain the equality (5) in §7, but with the representation $\pi_o$ as mentioned above. Therefore, just as in §7, we can prove the following result:

**Theorem 5.** Let $p > 2$ and let $L/K$ be a finite $p$-extension of non-cyclotomic $Z_p$-fields of C-M type. Let $\pi_{L/K}^{-}: G \to GL(V_L^{-})$ be the representation of $G = \text{Gal}(L/K)$ on the vector space $V_L^{-} = V(A_L^{-})$ over $Q_p$. Assume that $\mu_K = 0$. Then

$$\pi_{L/K}^{-} = \lambda_K \pi_o \bigoplus \bigoplus_{v^+} (\bigoplus_{v^+} \pi_{v^+}^o)$$

12) See [8], Chap. IX, Théorème 5.
where $\pi_\phi$ and the sum over $v^+$ are defined in the same manner as in Theorem 4.

Note that in both Theorem 4 and Theorem 5, $\pi_\phi' = 0$ if $v^+$ is unramified in $L^+$. Hence the sum over $v^+$ is actually a finite sum and it is zero if and only if $L^+/K^+$ is unramified outside the $p$-places of $K^+$.

9. In general, for each $\mathbb{Z}_p$-field $K$, let

$$\delta_K = 1 \text{ or } 0$$

according as $K$ is cyclotomic or not. As in Theorems 4, 5, let $L/K$ be a finite $p$-extension of $\mathbb{Z}_p$-fields of C-M type. Then the formulae in those theorems can be uniformly written as

$$\pi_{L/K} = \delta_K \pi_1 \oplus (\lambda_K - \delta_K) \pi_G \oplus \bigoplus_{v^+} (\pi_\phi')^+.$$  

We shall next compare the degrees of the representations on the both sides. It is clear that

$$\deg(\pi_{L/K}) = \lambda_K, \quad \deg(\pi_1) = 1, \quad \deg(\pi_G) = n = [L:K].$$

Since $\pi_{v^+}$ is induced by the trivial representation of the inertia group $T(w^+/v^+) = Z(w^+/v^+)$, we have

$$\deg(\pi_{v^+}) = n/e = g, \quad \deg(\pi_\phi') = n - g = g(e - 1)$$

where $e = e(w^+/v^+) = [T(w^+/v^+):1]$ is the ramification index of $w^+$ for the extension $L^+/K^+$ and where $g = g(w^+/v^+)$ is the number of the extensions $w^+$ of $v^+$ on $L^+$. Hence it follows from (9) that

$$\lambda_K = \delta_K + (\lambda_K - \delta_K)[L:K] + \sum_{w^+} (e(w^+/v^+) - 1),$$

where the sum on the right is now taken over all finite non-$p$-places $w^+$ on $L^+$, split in $L$. The same formula may be also written as

$$2(\lambda_K - \delta_K) = 2(\lambda_K - \delta_K)[L:K] + \sum_w (e(w/v) - 1)$$

with $w$ ranging over all finite non-$p$-places on $L$, split for the extension $L/L^+$. This is the formula of Kida [6], mentioned in the introduction. We note that it is easy to deduce from (9) a similar formula for $L'/K$ where $L'$ is an arbitrary intermediate field of $K$ and $L$, not necessarily a Galois extension over $K$.

The proof of the above formulae for $\pi_{L/K}$ and $\lambda_K$ does not work to obtain similar results for $\pi_{L/K}^+$ and $\lambda_K^+$. The main reason is that while Galois cohomology groups with values in $E_L^- = W_L$ can be quite simply calculated, it is not so for $E_L^+ = E_{L^+}$. However, less explicit formulae
involving some cohomological invariants still can be proved by similar arguments in certain cases. We shall next explain it briefly. In what follows, let \( p \) denote an arbitrary prime number, possibly 2, and let \( L \) be a cyclic extension of degree \( p \) over a \( \mathbb{Z}_p \)-field \( K \), unramified at every infinite place on \( K \). Let \( S \) be the set of all finite non-\( p \)-places on \( K \), ramified in \( L \), and let \( I_{L,S} \) and \( P_{L,S} \) denote the group of all \( S \)-ideals of \( L \) and the subgroup of principal ideals in \( I_{L,S} \), respectively. Then we have exact sequences of modules over \( G = \text{Gal}(L/K) \):

\[
0 \to P_{L,S} \to I_{L,S} \to G_{L,S} \to 0,
\]

\[
0 \to E_{L,S} \to L^* \to P_{L,S} \to 0,
\]

where \( C_{L,S} \) is the ideal-class group of \( S \)-ideals of \( L \), and \( E_{L,S} \) the group of \( S \)-units in \( L \). It follows from Lemmas 1, 5 that

\[
H^n(L/K, I_{L,S}) = 0, \quad H^n(L/K, L^*) = 0, \quad \text{for } n \geq 1.
\]

Hence the above exact sequences imply that for \( n \geq 1 \),

\[
H^n(L/K, C_{L,S}) \cong H^{n+1}(L/K, P_{L,S}), \quad H^n(L/K, P_{L,S}) \cong H^{n+1}(L/K, E_{L,S}).
\]

As \( G \) is cyclic, we then obtain

\[
H^n(L/K, A_{L,S}) \cong H^n(L/K, E_{L,S}), \quad \text{for } n \geq 1,
\]

where we put

\[
A_{L,S} = C_{L,S}(p).
\]

We now assume that \( \mu_K = 0 \) so that \( \mu_L = 0 \). Since \( A_{L,S} \) is a factor group of \( A_L = C_L(p) \) modulo a finite subgroup, it follows from the remark in §5 that

\[
A_{L,S} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^L.
\]

The structure of such a \( G \)-module \( A_{L,S} \) can be described as follows. Namely, let \( \sigma \) be a generator of \( G \) and let

\[
X_p = \mathbb{Z}_p[G], \quad X_{p-1} = (1 - \sigma)X_p, \quad X_i = X_p/X_{p-1} = \mathbb{Z}_p, \quad A_i = \text{Hom}_{\mathbb{Z}_p}(X_i, \mathbb{Q}_p/\mathbb{Z}_p), \quad \text{for } i = 1, p - 1, p.
\]

Then

\[
A_{L,S} = A_1^{a_1} \oplus A_{p-1}^{a_{p-1}} \oplus A_p^{a_p}
\]

with some integers \( a_i, a_{p-1}, a_p \geq 0 \). With the functor \( V \) defined in §5, let

\[
V_\ell = V(A_i), \quad \pi_i : G \to GL(V_\ell), \quad \text{for } i = 1, p - 1, p.
\]

13) Cf. [1].

14) This is a well-known result on the integral representations of \( G \) over the ring \( \mathbb{Z}_p \).
Then $\pi_1$ is the trivial representation of $G$ over $Q_p$, $\pi_{p-1}$ is the unique faithful irreducible representation of $G$ over $Q_p$, and

$$\pi_p = \pi_1 \oplus \pi_{p-1} = \pi_G.$$ 

Since

$$V_L = V(A_L) = V(A_{L,S}),$$

it follows from the above that

$$\pi_L/K = a_1 \pi_1 \oplus a_{p-1} \pi_{p-1} \oplus a_p \pi_p$$

for the representation $\pi_{L/K}$ of $G = \text{Gal}(L/K)$ on the space $V_L$. We shall next compute the integers $a_1$, $a_{p-1}$, and $a_p$.

Since $G$ is a cyclic group of order $p$, the cohomology groups of $G$ are abelian groups of exponent $p$. One checks easily that

$$r(H_1(G, A_1)) = 1, \quad r(H_1(G, A_{p-1})) = 0, \quad r(H_1(G, A_p)) = 0,$$

$$r(H_2(G, A_1)) = 0, \quad r(H_2(G, A_{p-1})) = 1, \quad r(H_2(G, A_p)) = 0$$

for the ranks of the abelian groups $H^n(G, A_i)$. Let

$$r_n = r(H^n(L/K, A_L, S)) = r(H^n(L/K, E_{L,S})), \quad n \geq 1.$$ 

Then it follows from (11) that

$$r_1 = a_1, \quad r_2 = a_{p-1}.$$ 

In particular, we see that both $H^1(L/K, E_{L,S})$ and $H^2(L/K, E_{L,S})$ are finite groups so that the Herbrand quotient $q(E_{L,S})$ of the $G$-module $E_{L,S}$ is defined. Let $d$ denote the number of places on $K$ in the finite set $S$ and let

$$h_n = r(H^n(L/K, E_L)), \quad n \geq 1$$

for the $G$-submodule $E_L$ of $E_{L,S}$. Then it can be seen easily that

$$q(E_{L,S}/E_L) = p^d.$$ 

Hence, by Herbrand’s lemma, $q(E_L)$ is defined and

$$q(E_{L,S}) = q(E_L)p^d.$$ 

Thus both $h_1$ and $h_2$ are finite and they satisfy

$$a_{p-1} - a_1 = h_2 - h_1 + d.$$ 

Now, the assumption $\mu(n) = 0$ implies

$$A_{K,S} = C_{K,S}(p) \cong (Q_p/Z_p)^{rk}.$$ 

On the other hand, since $H^2(L/K, L^\times) = 0$ by Lemma 5, the remark at the end of §4, applied for $E_{L,S}$, gives us
As the cohomology groups on the left are finite, it follows that both
the kernel and the cokernel of $A_{k,s} \to A_{y,s}$ are finite groups. Hence we see from (11) that

$$\lambda_K = a_1 + a_p .$$

Therefore

$$\pi_{L/K} = a_1 \pi_1 \oplus a_{p-1} \pi_{p-1} \oplus a_p \pi_p$$

$$= (a_1 + a_p) \pi_p \oplus (a_{p-1} - a_1) \pi_{p-1}$$

$$= \lambda_K \pi_G \oplus d \pi_{p-1} \oplus (h_2 - h_1) \pi_{p-1} .$$

For each non-$p$-place $v$ on $K$, let the representations $\pi_v$ and $\pi'_v$ be defined similarly as $\pi_v^+$ and $\pi'_v^+$ in §7. Then for the cyclic extension $L/K$ of degree $p$,

$$\pi'_v = \pi_{p-1} \text{ or } 0$$

according as $v$ is ramified or unramified in $L$. Hence the following theorem is proved:

**Theorem 6.** Let $p \geq 2$ and let $L$ be a cyclic extension of degree $p$ over a $\mathbb{Z}_p$-field $K$, unramified at every infinite place of $K$. Assume that $\mu_K = 0$. Then

$$\pi_{L/K} = \lambda_K \pi_G \oplus (\bigoplus \pi'_v) \oplus (h_2 - h_1) \pi_{p-1}$$

for the representation $\pi_{L/K}$ of $G = \text{Gal}(L/K)$ on the vector space $V_L$ over $\mathbb{Q}_p$. Here, $h_i$ denotes the rank of the abelian group $H^i(L/K, E_L)$ for $i = 1, 2$, $\pi_G$ is the regular representation of $G$ over $\mathbb{Q}_p$, $\pi_{p-1}$ the unique faithful irreducible representation of $G$ over $\mathbb{Q}_p$ with degree $p - 1$, and $v$ ranges over all non-$p$-places of $K$, with $\pi'_v$ as mentioned above.

Of course, if $h_2 - h_1$ is negative, the right hand side of the formula should be interpreted as a difference of two representations.

Now, comparing the degrees of the representations in Theorem 6, we immediately obtain the following formula for $\lambda_L$ and $\lambda_K$:

$$\lambda_L = p\lambda_K + \sum_w (e(w/v) - 1) + (p - 1)(h_2 - h_1) ,$$

where $w$ ranges over all non-$p$-places on $L$. Checking the proof of Theorem 6, one also finds that in the case where $p > 2$ and $L/K$ is an extension of $\mathbb{Z}_p$-fields of C-M type, similar results can be proved for $\pi_{L/K}$ and $\lambda_L$ by the same method. These are of course the special cases of the formulae (9) and (10) for a cyclic extension $L/K$ of degree $p$. However, as Kida [6] pointed out, his formula in the general case is actually an
easy consequence of the special case mentioned above. Thus the above method provides another proof of Kida's formula (10).

BIBLIOGRAPHY