Tôhoku Math. Journ.
33 (1981), 263-288.

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

KENKICHI IWASAWA

(Received July 29, 1980)

Let $f: R' \to R$ be an n-fold covering of compact, connected Riemann surfaces and let g and g' denote the genara of R and 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 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 forumla 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 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 $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, and $\boldsymbol{C}$ 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 $\boldsymbol{Q}$ in $\boldsymbol{C}$, not necessarily finite over $\boldsymbol{Q}$. For such a field K, let $\mathfrak{o}_K$ denote the ring of all algebraic integers in K. The invertible $\mathfrak{o}_K$-submodules of K are called the ideals of K, and they form a multiplicative group I_K, the ideal group of K. Let P_K denote the subgroup of principal ideals (α), $\alpha \in K^\times$. The ideal-class group $C_K = I_K/P_K$ is then a torsion abelian group so that

$$C_K = \bigoplus_q C_K(q)$$

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

$$I_v = \varinjlim \langle \mathfrak{p}_{v_i} \rangle .$$

It is isomorphic to a subgroup of the additive group of $\boldsymbol{Q}$, containing $\boldsymbol{Z}$. In particular, if there exists a subfield k such that v is unramified for the extension K/k, then $\mathfrak{p}_v$ belongs to I_K and $I_v = \langle \mathfrak{p}_v \rangle \cong \boldsymbol{Z}$. 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 $\boldsymbol{Q}$; 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 $K \subseteqq L \subseteqq M$.

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

[3] For $\boldsymbol{Z}_p$-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 $\boldsymbol{Z}_p$-field K, i.e., a finite place on K with $v|\boldsymbol{Q} = q$. From $K = k_\infty = k\boldsymbol{Q}_\infty$, we then see easily that the subgroup I_v of I_K is defined as explained above and that if $q \neq p$, then $I_v = \langle \mathfrak{p}_v \rangle \cong \boldsymbol{Z}$, and if $q = p$, then I_v is isomorphic to the union $\bigcup_{n\geqq 0} p^{-n}\boldsymbol{Z}$. Furthermore, for each prime number q, there exist only a finite number of q-places on K, and

$$I_K = \bigoplus_v I_v$$

where v ranges over all finite places on K.

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

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

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

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

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

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

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., $v|\boldsymbol{Q} = q \neq p$. 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 $T \subseteqq Z \subseteqq G$. 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,

$$I_{L,v} \xrightarrow{\sim} \boldsymbol{Z}[G/Z]$$

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

$$H^n(L/K, I_{L,v}) \xrightarrow{\sim} H^n(G, \boldsymbol{Z}[G/Z]) \xrightarrow{\sim} H^n(Z, \boldsymbol{Z}) , \quad n \geqq 0$$

with trivial Z-action on $\boldsymbol{Z}$.[4]

[4] See [7], Chap. II, Théorème 6.

(b) Let $w_1, \cdots, w_g$ be the distinct extensions of v on L. Then, in the ideal group I_L,

$$\mathfrak{p}_v = \prod_{\sigma} \sigma(\mathfrak{p}_w) = \left(\prod_{i=1}^{g} \mathfrak{p}_{w_i}\right)^{e}, \quad \sigma \in G .$$

Hence

$$I^G_{L\ v} = H^0(L/K, I_{L,v}) = \langle \mathfrak{p}_v^{1/e} \rangle \cong \boldsymbol{Z} .$$

(c) T is a normal subgroup of Z and

$$Z/T \xrightarrow{\sim} \mathrm{Gal}\,(\mathfrak{k}_w/\mathfrak{k}_v)$$

where $\mathfrak{k}_v = \mathfrak{o}_K/\mathfrak{p}_v$ and $\mathfrak{k}_w = \mathfrak{o}_L/\mathfrak{p}_w$ are the residue fields of v and w respectively. In particular, $f = [\mathfrak{k}_w : \mathfrak{k}_v]$. Note that both $\mathfrak{k}_v$ and $\mathfrak{k}_w$ are algebraic extensions of the finite field $\boldsymbol{F}_q$ with q elements and that $[\mathfrak{k}_v : \boldsymbol{F}_q]$ is divisible by p^∞ because $K = k_\infty$.

Assume now that L/K is a p-extension. Then Z/T is a p-group, and the remark just mensioned above implies that $f = [\mathfrak{k}_w : \mathfrak{k}_v] = 1$, $Z = T$. However, since $v\,|\,\boldsymbol{Q} \neq p$, 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

$$\begin{aligned} H^n(L/K, I_{L,v}) &\cong \boldsymbol{Z}/e\boldsymbol{Z}\,, \quad \text{for all even} \quad n \geqq 2\,, \\ &= 0\,, \qquad\quad \text{for all odd} \quad n \geqq 1\,, \end{aligned}$$

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

$$\begin{aligned} I^G_{L,v} &= H^0(L/K, I_{L,v}) = I_v\,, \\ &= H^n(L/K, I_{L,v}) = 0\,, \quad \text{for} \quad n \geqq 1\,. \end{aligned}$$

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

$$L = \varinjlim L_i\,.$$

For a finite place v on K, let

$$I_{L,v} = \varinjlim I_{L}^{i}{}_{,v}$$

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

$$I_L = \bigoplus_{v} I_{L,v}\,.$$

Hence

$$H^n(L/K, I_L) = \bigoplus_v H^n(L/K, I_{L,v}) ,$$
$$H^n(L/K, I_{L,v}) = \varinjlim H^n(L_i/K, I_{L_i,v}) , \quad n \geqq 0 .$$

LEMMA 1. *Let $v|\boldsymbol{Q} = p$. Then*

$$I^G_{L,v} = H^0(L/K, I_{L,v}) = I_v ,$$
$$H^n(L/K, I_{L,v}) = 0 , \quad \textit{for} \quad n \geqq 1 .$$

Let $v|\boldsymbol{Q} \neq p$. 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 $T(w/v) \cong \boldsymbol{Z}/e\boldsymbol{Z}$ and

$$I^G_{L,v} = H^0(L/K, I_{L,v}) = \langle \mathfrak{p}_v^{1/e} \rangle \cong \boldsymbol{Z} ,$$
$$H^n(L/K, I_{L,v}) \cong \boldsymbol{Z}/e\boldsymbol{Z} , \quad \textit{for even} \quad n \geqq 2 ,$$
$$= 0 , \quad \textit{for odd} \quad n \geqq 1 .$$

On the other hand, if e is infinite, then $T(w/v) \cong \boldsymbol{Z}_p$ and

$$I^G_{L\cdot v} = H^0(L/K, I_{L,v}) = \{\mathfrak{p}_v^r \,|\, r \in R\} \cong R = \bigcup_{n \geqq 0} p^{-n}\boldsymbol{Z} ,$$
$$H^n(L/K, I_{L,v}) = 0 , \quad \textit{for} \quad n \geqq 1 .$$

PROOF. The first part is an immediate consequence of the results for $H^n(L_i/K, I_{L_i,v})$ mentioned in § 1. Let $v|\boldsymbol{Q} \neq p$ and let $w_i = w|L_i$, $e_i = e(w_i/v)$, $T_i = T(w_i/v) = Z(w_i/v)$ for each i. Then $T = T(w/v) = \varprojlim T_i$, and the argument in § 1 shows that the following diagram is commutative for $L_i \subseteqq L_j$:

$$\begin{tikzcd}
H^n(L_i/K, I_{L_i,v}) \arrow[r, "\sim"] \arrow[d] & H^n(T_i, \boldsymbol{Z}) \arrow[d] \\
H^n(L_j/K, I_{L_j,v}) \arrow[r, "\sim"] & H^n(T_j, \boldsymbol{Z}) .
\end{tikzcd}$$

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 $\boldsymbol{Z}$. Hence it follows that

$$H^n(L/K, I_{L,v}) \xrightarrow{\sim} H^n(T, \varinjlim \boldsymbol{Z}) , \quad n \geqq 0 .$$

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 $T(w/v) \cong \boldsymbol{Z}_p$, 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 $\boldsymbol{Z}_p$-field K with $G = \mathrm{Gal}(L/K)$. Suppose that each finite non-p-place on K is either unramified in L or infinitely ramified in L. Then*

$$H^n(L/K, I_L) = 0\ , \quad \textit{for all} \quad n \geqq 1\ ,$$

and

$$I_L^G/I_K = \bigoplus_v A_v$$

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

$$A_v = \mathfrak{p}_v^R/\mathfrak{p}_v \cong R/\boldsymbol{Z} \cong \boldsymbol{Q}_p/\boldsymbol{Z}_p$$

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

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

LEMMA 3. *Let the order of $\mathfrak{k}_v^\times$ 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 $\mathfrak{k}_{v_0}^\times$ 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 $\mathfrak{k}_v^\times$ be divisible by p^∞ 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

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

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, $n \geqq 0$, be the intermediate fields of the $\boldsymbol{Z}_p$-extension K/k:

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

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_n, unramified outside S_n. Then $k_n \subseteqq K \subseteqq F_n \subseteqq L$ so that we put $w_n = w|F_n$. As v_n is unramified in K and $e(v/v_n) = 1$, we have

$$e(w_n/v_n) = e(w_n/v) \leqq e(w/v) = p^a .$$

For each place z in S_n, let $k_{n,z}$ denote the z-completion of k_n, 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 $U_{n,z}$, $z \in S_n$, and let E_n be the group of global units in k_n. 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_n}. Since $v|\boldsymbol{Q} \neq p$, V_n is isomorphic to the Sylow p-subgroup of $\mathfrak{k}_{v_n}^\times$, and since the order of $\mathfrak{k}_v^\times$ is divisible by p^∞, V_n is a finite cyclic group with order divisible by p^{n+1}.

Now, applying class field theory for F_n/k_n, one sees that $e(w_n/v_n)$ 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 $V_n \to U_n/E_n U_n^{p^{n+1}}$ is at most equal to $e(w/v) = p^a$, and it follows that

$$V_n^{p^a} \times 1 \times \cdots \times 1 \subseteqq E_n U_n^{p^{n+1}} \subseteqq U_n = \prod_z U_{n,z} .$$

Consequently, if $n \geqq a$, then there exists a unit ε in E_n such that ε is a p^{n+1}-th power in $k_{n,z}$ for every p-place z on k_n, but is at most a p^a-th power in k_{n,v_n}. Let ζ be a primitive $2p$-th root of unity in $\boldsymbol{C}$ and let

$$k' = k(\zeta) , \qquad K' = k'_\infty = K(\zeta) .$$

Replacing k by $K \cap k'$ if necessary, we may assume that $K \cap k' = k$ so that $k_n(\zeta)$ is the n-th intermediate field of the $\boldsymbol{Z}_p$-extension K'/k' for all $n \geqq 0$: $k'_n = k_n(\zeta)$. Let v' be an extension of v on K', let $v'_n = v'|k'_n$, and let V'_n be the group defined for the local field $k'_{n,v'}$ similarly as V_n for k_n. Since the degree $[\mathfrak{k}_{v'_n}: \mathfrak{k}_{v_n}]$ is a factor of $b = [k': k] = [k'_n: k_n]$ and since $b|p-1$ if $p > 2$ and $b = 1$ or 2 if $p = 2$, it follows that $V'_n = V_n$ for $p > 2$ and $[V'_n: V_n] = 1$ or 2 for $p = 2$, $n \geqq 1$. Consequently, we see that ε is at most a p^{a+1}-th power in the local field k'_{n,v'_n}, for $n > a$. Let ε_n denote a p^{n+1}-th root of ε in $\boldsymbol{C}$. As k'_n contains primitive p^{n+1}-th roots of unity, it follows from the above that $k'_n(\varepsilon_n)/k'_n$ is an unramified cyclic p-extension, of which the local degree at v'_n is divisible by $p^{n+1}p^{-a-1} = p^{n-a}$. Therefore, by class field theory, the order of the ideal-class of $\mathfrak{p}_{v'_n}$ in k'_n 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 $p_{v'_n}$ in k'_n is equal to the order of the ideal-class of $\mathfrak{p}_{v'}$ 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 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 $\mathfrak{k}_v^\times$ is divisible by p^∞. 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: $K \subseteqq L_0 \subseteqq L$. 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 $v \notin S_0$ or $v \in S_0$. Hence we may apply Lemma 2 for such an extension L/K.

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

$$W(p) = \bigcup_{n \geqq 0} W_{p^n} .$$

Then a Z_p-field K contains $W(p)$ if and only if it contains W_{2p}. When this happens, we shall call K a cyclotomic Z_p-field. Let v be any finite non-p-place on such a cyclotomic Z_p-field K. It is clear that the order of $\mathfrak{k}_v^\times$ is then divisible by p^∞. Let $\mathfrak{p}_v^a = (\alpha)$ with $\alpha \in K^\times$, $a \geqq 1$, and let α_n be a p^n-th root of α in C for $n \geqq 1$. Then one sees easily that the field L in Lemma 4 contains all α_n, $n \geqq 1$, 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_∞ (e.g., a Z_p-field) and let L/K be a p-extension, unramified at every infinite, i.e., archimedean, place on K. Then*

$$H^n(L/K, L^\times) = 0 , \quad \textit{for all} \quad n \geqq 1 .$$

PROOF. We may assume that L/K is finite. Since $H^1(L/K, L^\times) = 0$, it is sufficient to prove $H^2(L/K, L^\times) = 0$.[5] Let $K = \varinjlim k_n$, $L = \varinjlim k'_n$ where for each $n \geqq 0$, 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_∞, the local degree of the extension K/Q at each finite place of K is divisible by p^∞. 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,

[5] See [8], Chap. IX, Théorème 8.

respectively. Let M/K be an arbitrary Galois extension of number fields and let $G = \mathrm{Gal}(M/K)$. Then we have short exact sequences

$$\begin{aligned} &0 \to P_M \to I_M \to C_M \to 0 , \\ &0 \to E_M \to M^{\times} \to P_M \to 0 , \end{aligned} \tag{1}$$

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

Theorem 1. *Let K be a $\boldsymbol{Z}_p$-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*

$$H^n(M/K, E_M) = 0 , \quad \textit{for all} \quad n \geqq 2 ,$$

and there exists an exact sequence

$$0 \to C_K(p) \to H^1(M/K, E_M) \to \bigoplus_v A_v \to 0$$

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

$$A_v = \mathfrak{p}_v^R/\mathfrak{p}_v^{\boldsymbol{Z}} \cong \boldsymbol{Q}_p/\boldsymbol{Z}_p , \quad R = \bigcup_{n \geqq 0} p^{-n}\boldsymbol{Z} .$$

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

$$H^n(M/K, C_M) = H^n(M/K, C_M(p)) = 0 , \quad \text{for} \quad n \geqq 1 .$$

By Lemmas 2, 5, we also have

$$H^n(M/K, I_M) = 0 , \qquad H^n(M/K, M^{\times}) = 0 , \quad \text{for} \quad n \geqq 1 .$$

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

$$I_M^G \to C_M^G \to H^1(M/K, P_M) \to 0 , \qquad H^n(M/K, P_M) = 0 , \quad n \geqq 2 ,$$
$$K^{\times} \to P_M^G \to H^1(M/K, E_M) \to 0 , \qquad H^n(M/K, P_M) \xrightarrow{\sim} H^{n+1}(M/K, E_M) , \quad n \geqq 1 .$$

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

$$H^n(M/K, E_M) = 0 , \quad \text{for all} \quad n \geqq 2 .$$

We also obtain from the second exact sequence that

$$H^1(M/K, E_M) \cong P_M^G/P_K = (I_M^G \cap P_M)/P_K . \tag{2}$$

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

$$0 \to I_K \cap P_M/P_K \to I_K/P_K \to I_K/I_K \cap P_M \to 0 ,$$

we have $I_K/I_K \cap P_M = I_K P_M/P_M \subseteqq I_M/P_M$. Hence we obtain an exact sequence

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

On the other hand, we also have the exact sequence

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

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

$$I_M^G/I_M^G \cap P_M = I_M^G P_M/P_M \subseteqq I_M/P_M ,$$

we know that $I_M^G/(I_M^G \cap P_M)I_K$ is a factor group of a subgroup of $C_M(p)$. The assumption $C_M(p) = 0$ then implies

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

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 $H^1(L/K, L^\times) = 0$, it follows from (1) that

$$H^1(L/K, E_L) \cong P_L^G/P_K ,$$
$$\operatorname{Ker}(H^2(L/K, E_L) \to H^2(L/K, L^\times)) \cong \operatorname{Coker}(I_L^G \to C_L^G) .$$

When both K and L are finite over $\boldsymbol{Q}$, 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 $\boldsymbol{Z}_p$-module. For a $\boldsymbol{Z}_p$-field K, the following facts are known on the structure of the $\boldsymbol{Z}_p$-module A_K.[6] Namely, let $K = k_\infty = k\boldsymbol{Q}_\infty$ with k finite over $\boldsymbol{Q}$ and let $\lambda = \lambda(K/k)$ and $\mu = \mu(K/k)$ denote respectively the so-called λ- and μ-invariant of the $\boldsymbol{Z}_p$-extension K/k. Then

$$A_K \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^\lambda \oplus A'$$

with A' a $\boldsymbol{Z}_p$-module of bounded exponent: $p^a A' = 0$, $a \geqq 0$. Furthermore, if $\mu = 0$, then $A' = 0$ so that

$$A_K \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^\lambda , \qquad A_K/pA_K = 0 ;$$

and if $\mu > 0$, then A' is infinite so that A_K/pA_K is an infinite $\boldsymbol{Z}_p$-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 $\boldsymbol{Z}_p$-module A_K and is independent of the choice of k such that $K = k_\infty$. Hence it may be denoted by λ_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, λ_K an analogue of twice the genus of that curve.

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

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

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

$$V_K = V(A_K) .$$

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

$$V_K \cong \boldsymbol{Q}_p^\lambda , \qquad \lambda_K = \dim_{\boldsymbol{Q}_p} V_K .$$

Now, it has been conjectured for some time that $\mu_K = 0$ for all $\boldsymbol{Z}_p$-fields K. The conjecture was proved by Ferrero-Washington [3] in the case where K is an abelian extension over the rational field $\boldsymbol{Q}$, 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 $\boldsymbol{Z}_p$-field.

THEOREM 2. *Let K be a cyclotomic $\boldsymbol{Z}_p$-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* Gal (M/K) *is a free pro-p-group.*

PROOF.[7] Since there is no non-trivial unramified abelian p-extension over M, we see easily that $A_M = C_M(p) = 0$. 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. On the

[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 ε in E_M defines an exact sequence

$$0 \to W_p \to E_M \xrightarrow{p} E_M \to 0 \ ,$$

and this induces the exact sequence

$$H^1(M/K, E_M) \xrightarrow{p} H^1(M/K, E_M) \to H^2(M/K, W_p) \to H^2(M/K, E_M)$$

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

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

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

$$0 \to A_K \to H^1(M/K, E_M) \to \bigoplus_v A_v \to 0$$

where v ranges over a finite set and $A_v \cong \boldsymbol{Q}_p/\boldsymbol{Z}_p$ 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., $H^2(\mathrm{Gal}\,(M/K), \boldsymbol{Z}/p\boldsymbol{Z}) = 0$. As $\mathrm{Gal}\,(M/K)$ is a pro-p-group, the last equality means that $\mathrm{Gal}\,(M/K)$ is a free pro-p-group.[8] 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 $\boldsymbol{C}$. When a number field K is invariant under the automorphism J of $\boldsymbol{C}$, 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

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

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

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

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

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

It is also known that for such K,

$$(3) \qquad E_K^+ = E_{K^+} \ , \qquad E_K^- = W_K \ , \qquad [E_K\colon W_K E_{K^+}] = 1 \ \text{ or } \ 2 \ .$$

[8] See [9], Chap. I, § 4.

We now assume that $p > 2$ and K is a $\boldsymbol{Z}_p$-field of C-M type. We can then fined a number field k of C-M type, finite over $\boldsymbol{Q}$, such that $K = k_\infty$, $K^+ = k_\infty^+$. For such K/k, we can define four invariants $\lambda(K/k)^\pm$, $\mu(K/k)^\pm$ which have similar properties as explained in § 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 $\lambda_K^\pm$. In fact, we have

$$A_K = A_K^+ \oplus A_K^- , \qquad A_K^+ = A_{K^+} ,$$
$$V_K = V_K^+ \oplus V_K^- , \qquad V_K^\pm = V(A_K^\pm) , \quad \dim_{\boldsymbol{Q}_p} V_K^\pm = \lambda_K^\pm .$$

Furthermore, if $\mu_K^- = 0$, then

$$A_K^- \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{\lambda_K^-} ;$$

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 $\boldsymbol{Z}_p$-field, i.e., $W(p) \subseteqq K$. Let S^+ be a set of finite places on $K^+ = K \cap \boldsymbol{R}$, 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 $M^+ = M \cap \boldsymbol{R}$, justifying the notation M^+. It is easy to see that M/K^+ is a Galois extension, that $K \cap M^+ = K^+$, and that

$$\text{(4)} \qquad \begin{aligned} &\operatorname{Gal}(M/K^+) = \operatorname{Gal}(M/K) \times \operatorname{Gal}(M/M^+) , \\ &\operatorname{Gal}(M/K) = \operatorname{Gal}(M^+/K^+) . \end{aligned}$$

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 $H^n(M/K, E_M)$, $n \geqq 1$, 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 $\mathfrak{a}$ be an ideal of I_M in the ideal-class c and let $\mathfrak{a}^p = (\alpha)$, $\alpha \in M^\times$. Then $\mathfrak{b}^p = (\beta)$ with $\mathfrak{b} = \mathfrak{a}^{1-J}$, $\beta = \alpha^{1-J}$. 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 $M(\sqrt[p]{\beta}) = MM'$. It then follows from the definition of M^+ that $M' = M^+$, $M(\sqrt[p]{\beta}) = M$ so that $\mathfrak{b} = (\sqrt[p]{\beta})$ with $\sqrt[p]{\beta} \in M^\times$. Thus $(1 - J)c = 0$, $c \in A_M^- = 0$, and consequently $c = 0$. Therefere $A_M^- = 0$, $A_M = A_M^+ \oplus A_M^- = 0$, 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 $K^+ = k_\infty^+$ is a $\boldsymbol{Z}_p$-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 $\mathrm{Gal}(M^+/K^+)$ 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 $H^1(M/K, E_M)$ in Theorem 1 is a finite sum.

THEOREM 3. *Let K be a cyclotomic $\boldsymbol{Z}_p$-field of* C-M *type for $p > 2$ and let S^+ be a finite set of finite places on $K^+ = K \cap \boldsymbol{R}$, 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* $\mathrm{Gal}(M^+/K^+)$ *is a free pro-p-group, and if this is the case, then the minimal number of generators for* $\mathrm{Gal}(M^+/K^+)$ *is $\lambda_K^- + s$.*

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

$$H^n(M/K, E_M)^- = H^n(M/K, W_M) = H^n(M/K, W(p)), \quad \text{for} \quad n \geqq 1 .$$

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

$$H^n(M/K, W(p)) = 0, \quad \text{for} \quad n \geqq 2 .$$

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

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

where, as easily seen from the definition of A_v,

$$(\bigoplus_v A_v)^- \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^s .$$

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 $H^2(M/K, W_p) = 0$, namely, that $\mu_K = 0$ if and only if $\mathrm{Gal}\,(M^+/K^+) = \mathrm{Gal}\,(M/K)$ is a free pro-p-group. Furthermore, when this is the case, then $A_K^- \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{\lambda^-}$ so that

$$H^1(M/K, W(p)) \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{\lambda^- + s} .$$

However, since $W(p) \subseteq K$, $H^1(M/K, W(p))$ is the Pontrjagin dual of the factor commutator group of $\mathrm{Gal}\,(M/K)$. Therefore the above isomorphism indicates that $\lambda_K^- + s$ is the minimal number of generators for the free pro-p-group $\mathrm{Gal}\,(M^+/K^+)$.

We note here that an essential difference between Theorem 2 and Theorem 3 lies in that the free pro-p-group $\mathrm{Gal}\,(M^+/K^+)$ in Theorem 3 is finitely generated while this is not so for the free pro-p-group $\mathrm{Gal}\,(M/K)$ in Theorem 2.

We shall next also briefly explain a generalization of Theorem 3. Let K' be a totally real $\boldsymbol{Z}_p$-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 $\boldsymbol{Z}_p$-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

$$\chi : \mathrm{Gal}\,(K/K') \to \boldsymbol{Z}_p^\times$$

such that $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for all $\sigma \in \mathrm{Gal}\,(K/K')$ and $\zeta \in W(p) \subseteq K$. Let $A_K^{(1)}$ 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 σ in $\mathrm{Gal}\,(K/K')$. The $\boldsymbol{Z}_p$-module $A_K^{(1)}$ is then a direct summand of A_K and it has similar properties as mentioned earlier for A_K and $A_K^\pm$; for example, if $A_K^{(1)} = pA_K^{(1)}$, then

$$A_K^{(1)} \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^\lambda$$

with an integer $\lambda = \lambda_K^{(1)} \geqq 0$. Let s be the number of finite non-p-places on K' which are ramified in M' and which split completely in K.

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

7. In general, let K be a Z_p-field, and L/K a finite Galois extension with $G = \text{Gal}(L/K)$. Then L is again a 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 λ_L-dimensional p-adic representation

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

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

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

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

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

where

$$\pi_{L/K}^\pm \colon G \to GL(V_L^\pm) .$$

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 Z_p-field, i.e., $W(p) \subseteqq K$. 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 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^+:

$$K^+ \subseteqq L^+ \subseteqq M^+ .$$

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

$$K \subseteqq L \subseteqq M .$$

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

$$0 \to A_L \to H^1(M/L, E_M) \to \bigoplus_w A_w \to 0$$

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 $\mathrm{Gal}(L/K^+)$. Hence it induces an exact sequence of G-modules:

$$0 \to A_L^- \to H^1(M/L, E_M)^- \to (\bigoplus_w A_w)^- \to 0 ,$$

where $H^1(M/L, E_M)^- = H^1(M/L, W(p))$ 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 alse true. In general, for each finite non-p-place v^+ on K^+, define a module B_{v^+} over $G = \mathrm{Gal}(L^+/K^+)$ 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

$$(5) \qquad \pi_0 = \pi_{L/K}^- \oplus (\bigoplus_{v^+} \pi_{v^+})$$

with π_0 and π_{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 $T = T(w^+/v^+)$. Then $T = Z(w^+/v^+)$ by § 1 so that as G-modules,

$$B_{v^+} \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)[G/T]$$

where the right hand side denotes the linear combinations of the left cosets of G modulo T with coefficients in $\boldsymbol{Q}_p/\boldsymbol{Z}_p$. Consequently

$$V(B_{v^+}) \cong \boldsymbol{Q}_p[G/T] ,$$

and we see that π_{v^+} is isomorphic to the representation of G over the field $\boldsymbol{Q}_p$, 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 π_0 of G on the space $V_0 = V(H^1(M/L, W(p))$.

Let

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

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

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

As explained in the proof of Theorem 3, $H^1(M/L, W(p))$ is the Pontrjagin dual of Y^{ab}, the factor commutator group of Y. Since $W(p) \subseteqq K$, we see that as G-modules,

$$V_0 \cong Y^{ab} \otimes_{\boldsymbol{Z}_p} \boldsymbol{Q}_p\ ,$$

where the action of $G = X/Y$ on the right is given by conjugations in X. Let us now assume that $\mu_K = 0$. 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 π_0 can be described by the following purely group-theoretical lemma:

LEMMA 7. *Let X be a free pro-p-group with m generators, $m \geqq 1$, and let Y be a closed normal subgroup with finite index in X. Then the representation π_0 of the finite group $G = X/Y$ on the vector space $Y^{ab} \otimes_{\boldsymbol{Z}_p} \boldsymbol{Q}_p$ is given by*

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

where π_1 denotes the one-dimensional trivial representation of G over $\boldsymbol{Q}_p$, and π_G the regular representation of G over $\boldsymbol{Q}_p$.

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

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

is exact. Then there exists[10] an exact sequence of $\boldsymbol{Z}_p[G]$-modules:

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

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

We now consider again the case where $X = \mathrm{Gal}\,(M/K)$, $Y = \mathrm{Gal}\,(M/L)$,

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

and $G = X/Y = \mathrm{Gal}(L/K)$. 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 $X \neq 1$, $m \geqq 1$ so that we obtain from (5) and Lemma 7 that

$$\pi_1 \oplus (\lambda_K^- + s - 1)\pi_G = \pi_{L/K}^- \oplus (\bigoplus_{v^+} \pi_{v^+}) ,$$

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

$$\pi_G = \pi_{v^+} \oplus \pi'_{v^+}$$

where π'_{v^+} is the representation of G over $\boldsymbol{Q}_p$, induced by the representation $\pi_T - \pi_1 | T$ for T. Note that when we change the extension w^+ of v^+ on L^+, the inertia group $T(w^+/v^+)$ is relaced by its conjugate in G so that π_{v^+} and π'_{v^+} are unchanged (up to isomorphisms). We now obtain from the above that

$$(6) \qquad \pi_{L/K}^- = \pi_1 \oplus (\lambda_K^- - 1)\pi_G \oplus (\bigoplus_{v^+} \pi'_{v^+})$$

where v^+ ranges over all finite non-p-places on K^+ which are ramified in M^+ and split in K. However, if v^+ is unramified in M^+, then $T(w^+/v^+) = 1$ so that $\pi_{v^+} = \pi_G$, $\pi'_{v^+} = 0$. Hence the sum in (6) may be taken over all v^+ 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 v^+ and the representation $\pi_G - \pi_1$.

Finally, if $G = 1$, then $K = L$, $V_K^- = V_L^-$, and $\pi_{L/K}^- = \lambda_K^- \pi_1$. Since $\pi'_{v^+} = 0$ for all v^+, 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 cyclotonic $\boldsymbol{Z}_p$-fields of* C-M *type. Let $\pi_{L/K}^-: G \rightarrow GL(V_L^-)$ be the representation of $G = \mathrm{Gal}(L/K)$ on the vector space $V_L^- = V(A_L^-)$ over $\boldsymbol{Q}_p$. Assume that $\mu_K = 0$. Then*

$$\pi_{L/K}^- = \pi_1 \oplus (\lambda_K^- - 1)\pi_G \oplus (\bigoplus_{v^+} \pi'_{v^+}) .$$

Here π_1 is the one-dimensional trivial representation of G over $\boldsymbol{Q}_p$, π_G is the regular representation of G over $\boldsymbol{Q}_p$, v^+ ranges over all finite non-p-places on $K^+ = K \cap \boldsymbol{R}$ which split in K, and π'_{v^+} denotes the complement in π_G of the representation π_{v^+} of $G = \mathrm{Gal}(L^+/K^+)$, induced by the one-dimensional trivial representation, over $\boldsymbol{Q}_p$, of the inertia group $T(w^+/v^+)$ of v^+ 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 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: $K \subseteqq L \subseteqq M$. 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 M/L 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

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

Therefore the Hochschild-Serre spectral sequence for $K \subseteqq L \subseteqq M$ induces[11] an exact sequence

$$\begin{aligned} 0 &\to H^1(L/K, E_L) \to H^1(M/K, E_M) \to H^0(L/K, H^1(M/L, E_M)) \\ &\to H^2(L/K, E_L) \to H^2(M/K, E_M) \to H^1(L/K, H^1(M/L, E_M)) \\ &\to \cdots\,. \end{aligned}$$

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 relaced by $H^n(\ ,\ )^\pm$. By Theorem 1,

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

Since W_p is not contained in W_L,

$$H^n(L/K, E_L)^- = H^n(L/K, W_L) = 0\,, \quad \text{for} \quad n \geqq 1\,.$$

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

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

where we put

$$G = \mathrm{Gal}\,(L/K)\,, \qquad A = H^1(M/L, E_M)^-\,.$$

[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 s 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

$$\begin{aligned} &0 \to A_K^- \to H^1(M/K, E_M)^- \to \bigoplus_{v^+} A_{v^+} \to 0 \,, \\ (7) \qquad &0 \to A_L^- \longrightarrow A \longrightarrow \bigoplus_{v^+} B_{v^+} \to 0 \,, \end{aligned}$$

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

$$A_K^- \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{\lambda_K^-} \,, \qquad A_L^- \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{\lambda_L^-} \,,$$

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

$$(8) \qquad A^G \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{\lambda_K^- + s} \qquad A \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^t$$

with s defined above and with a certain integer $t \geqq \lambda_L^-$. Let

$$A_p = \operatorname{Ker}(p\colon A \to A)$$

so that $0 \to A_p \to A \xrightarrow{p} A \to 0$ is exact. Then $H^n(G, A) = 0$, for $n \geqq 1$, imply

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

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

$$A \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)[G]^{\lambda_K^- + s} \,.$$

Let π_0 denote as before the representation of G on the vector space $V_0 = V(A)$ over $\boldsymbol{Q}_p$. Then the above isomorphism implies

$$V_0 \cong \boldsymbol{Q}_p[G]^{\lambda_K^- + s} \,, \qquad \pi_0 = (\lambda_K^- + s)\pi_G$$

with π_G denoting again the regular representation of G over $\boldsymbol{Q}_p$. From the exact sequence (7), we again obtain the equality (5) in § 7, but with the representation π_0 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 $\boldsymbol{Z}_p$-fields of* C-M *type. Let $\pi_{L/K}^-\colon G \to GL(V_L^-)$ be the representation of $G =$* Gal (L/K) *on the vector space $V_L^- = V(A_L^-)$ over $\boldsymbol{Q}_p$. Assume that $\mu_K = 0$. Then*

$$\pi_{L/K}^- = \lambda_K^- \pi_G \oplus \Big(\bigoplus_{v^+} \pi'_{v^+}\Big)$$

[12] See [8], Chap. IX, Théorème 5.

where π_G and the sum over v^+ are defined in the same manner as in Theorem 4.

Note that in both Theorem 4 and Theorem 5, $\pi'_{v^+} = 0$ 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 Z_p-field K, let

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

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

$$\pi^-_{L/K} = \delta_K \pi_1 \oplus (\lambda^-_K - \delta_K)\pi_G \oplus (\bigoplus_{v^+} \pi'_{v^+}) \ . \tag{9}$$

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

$$\deg(\pi^-_{L/K}) = \lambda^-_L \ , \qquad \deg(\pi_1) = 1 \ , \qquad \deg(\pi_G) = n = [L : K] \ .$$

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

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

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

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

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

$$2(\lambda^-_L - \delta_L) = 2(\lambda^-_K - \delta_K)[L : K] + \sum_{w} (e(w/v) - 1) \tag{10}$$

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 λ^-_L does not work to obtain similar results for $\pi^+_{L/K}$ and λ^+_L. 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 $\boldsymbol{Z}_p$-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.[13] Then we have exact sequences of modules over $G = \mathrm{Gal}\,(L/K)$:

$$0 \to P_{L,S} \to I_{L,S} \to G_{L,S} \to 0 \ ,$$
$$0 \to E_{L,S} \to L^{\times} \to P_{L,S} \to 0 \ ,$$

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

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

Hence the above exact sequences imply that for $n \geqq 1$,

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

As G is cyclic, we then obtain

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

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

$$A_{L,S} \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{\lambda_L} \ .$$

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

$$X_p = \boldsymbol{Z}_p[G] \ , \qquad X_{p-1} = (1-\sigma)X_p \ , \qquad X_1 = X_p/X_{p-1} = \boldsymbol{Z}_p \ ,$$
$$A_i = \mathrm{Hom}_{\boldsymbol{Z}_p}(X_i, \boldsymbol{Q}_p/\boldsymbol{Z}_p) \ , \qquad \text{for} \quad i = 1,\ p-1,\ p \ .$$

Then

$$A_{L,S} = A_1^{a_1} \oplus A_{p-1}^{a_{p-1}} \oplus A_p^{a_p} \tag{11}$$

with some integers a_1, a_{p-1}, $a_p \geqq 0$[14]. With the functor V defined in § 5, let

$$V_i = V(A_i) \ , \quad \pi_i \colon G \to GL(V_i) \ , \quad \text{for} \quad i = 1,\ p-1,\ p \ .$$

[13] Cf. [1].

[14] This is a well-known result on the integral representations of G over the ring $\boldsymbol{Z}_p$.

Then π_1 is the trivial representation of G over $\boldsymbol{Q}_p$, π_{p-1} is the unique faithful irreducible representation of G over $\boldsymbol{Q}_p$, 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 $G = \mathrm{Gal}\,(L/K)$ 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

$$\begin{aligned} &r(H^1(G, A_1)) = 1 , \quad &&r(H^1(G, A_{p-1})) = 0 , \quad &&r(H^1(G, A_p)) = 0 , \\ &r(H^2(G, A_1)) = 0 , \quad &&r(H^2(G, A_{p-1})) = 1 , \quad &&r(H^2(G, A_p)) = 0 \end{aligned}$$

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

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

Then it follows from (11) that

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

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

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

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 defind 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 $\mu_K = 0$ implies

$$A_{K,S} = C_{K,S}(p) \cong (\boldsymbol{Q}_p/\boldsymbol{Z}_p)^{\lambda_K} .$$

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

$$H^1(L/K, E_{L,S}) \cong P^G_{L,S}/P_{K,S} ,$$
$$H^2(L/K, E_{L,S}) \cong \text{Coker}\,(I^G_{L,S} \to C^G_{L,S}) .$$

As the cohomology groups on the left are finite, it follows that both the kernel and the cokernel of $A_{K,S} \to A^G_{L,S}$ are finite groups. Hence we see from (11) that

$$\lambda_K = a_1 + a_p .$$

Therefore

$$\begin{aligned} \pi_{L/K} &= a_1\pi_1 \oplus a_{p-1}\pi_{p-1} \oplus a_p\pi_p \\ &= (a_1 + a_p)\pi_p \oplus (a_{p-1} - a_1)\pi_{p-1} \\ &= \lambda_K\pi_G \oplus d\pi_{p-1} \oplus (h_2 - h_1)\pi_{p-1} . \end{aligned}$$

For each non-p-place v on K, let the representations π_v and π'_v be defined similarly as π_{v^+} and π'_{v^+} in § 7. Then for the cyclic extension L/K of degree p,

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

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

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

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

for the representation $\pi_{L/K}$ of $G = \text{Gal}\,(L/K)$ on the vector space V_L over $\boldsymbol{Q}_p$. Here, h_i denotes the rank of the abelian group $H^i(L/K, E_L)$ for $i = 1, 2$, π_G is the regular representation of G over $\boldsymbol{Q}_p$, π_{p-1} the unique faithful irreducible representation of G over $\boldsymbol{Q}_p$ with degree $p - 1$, and v ranges over all non-p-places of K, with π'_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 λ_L and λ_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 $\boldsymbol{Z}_p$-fields of C-M type, similar results can be proved for $\pi^-_{L/K}$ and λ^-_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

[1] A. BRUMER, Galois groups of extensions of algebraic number fields with given ramification, Mich. Jour. Math. 13 (1966), 33-40.

[2] C. CHEVALLEY AND A. WEIL, Über das Verhalten der Integrale erster Gattung bei Automorphismen des Funktionenkörpers, Hamb. Abh. 10 (1934), 358-361.

[3] B. FERRERO AND L. WASHINGTON, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. Math. 109 (1979), 377-395.

[4] K. Iwasawa, On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc. 65 (1959), 183-226.

[5] K. Iwasawa, On $\boldsymbol{Z}_l$-extensions of algebraic number fields, Ann. Math. 98 (1973), 246-326.

[6] Y. KIDA, l-extensions of CM-fields and cyclotomic invariants, J. Number Theory 12 (1980), 519-528.

[7] S. LANG, Rapport sur la Cohomologie des Groupes, W. A. Benjamin, Inc., New York-Amsterdam, 1966.

[8] J.-P. SERRE, Corps Locaux, Hermann, Paris, 1962.

[9] J.-P. SERRE, Cohomologie Galoisienne, Lecture Notes in Math. 5, Springer-Verlag, Berlin-Heidelberg-New York, 1964.

[10] K. WINGBERG, Die Einheitengruppe von p-Erweiterungen regulär p-adischer Zahlkörper als Galoismodul, Jour. für die reine u. angew. Math. 305 (1979), 206-214.

DEPARTMENT OF MATHEMATICS
PRINCETON UNIVERSITY
PRINCETON, NEW JERSEY 08544
U.S.A.