

A CLASS NUMBER FORMULA OF IWASAWA'S MODULES

BY TAKASHI FUKUDA

§ 0. Introduction.

Let p be an odd prime number which will be fixed throughout the following. Let k be a finite extension of \mathbf{Q} and k_∞ be the cyclotomic \mathbf{Z}_p -extension $k\mathbf{Q}_\infty$ of k , where \mathbf{Q}_∞ is the unique \mathbf{Z}_p -extension of \mathbf{Q} (c.f. [6]). For any $n \geq 0$, let k_n be the unique extension of k in k_∞ of degree p^n over k : $k = k_0 \subset k_1 \subset \dots \subset k_\infty$, and let $\Gamma_n = \text{Gal}(k_\infty/k_n)$. Let A_n be the p -Sylow subgroup of the ideal class group of k_n and D_n be the subgroup of A_n consisting of ideal classes containing ideals $\prod \mathfrak{P}^{m(\mathfrak{P})}$, where \mathfrak{P} runs over all primes of k_n lying over p and $m(\mathfrak{P}) \in \mathbf{Z}$. Let A'_n be the factor group A_n/D_n (c.f. [6]).

We assume that k is a *CM* field. Then k_∞ is also a *CM* field. Let j denote the complex conjugation of k_∞ . For any $\mathbf{Z}[\{1, j\}]$ -module M , let

$$M^- = \{a \in M \mid (1+j)a = 0\}.$$

(0.1) DEFINITION. Let $A_\infty^- = \varprojlim A_n^-$ and $A_\infty'^- = \varprojlim A_n'^-$, with respect to the natural maps induced from inclusion maps $k_n \rightarrow k_m$ for $m \geq n \geq 0$.

In [3] Greenberg, and in [2] Ferrero and Greenberg have proved that, if k is abelian over \mathbf{Q} , then the order of $(A_\infty'^-)^{I_n}$ is finite for any $n \geq 0$. We shall compute its order by using p -adic L -functions associated to k when the degree of k over \mathbf{Q} is prime to p .

In the following, we assume that k is a finite imaginary abelian extension of \mathbf{Q} whose degree is prime to p . Let G denote the Galois group $\text{Gal}(k/\mathbf{Q})$ and \hat{G} be its character group $\text{Hom}(G, \bar{\mathbf{Q}}_p^\times)$, where $\bar{\mathbf{Q}}_p$ is a fixed algebraic closure of \mathbf{Q}_p . We also consider \hat{G} as the set of primitive Dirichlet characters with values in $\bar{\mathbf{Q}}_p$ which are associated to the extension k/\mathbf{Q} by class field theory. Let ω be the Teichmüller character module p . Take $\phi \in \hat{G}$ with $\phi \neq \omega$ and $\phi(j) = -1$. Let $L_p(s; \omega\phi^{-1})$ be the p -adic L -function attached to $\omega\phi^{-1}$. For $\kappa \in 1 + p\mathbf{Z}_p$ with $\kappa \in 1 + p^2\mathbf{Z}_p$, using Iwasawa's construction of p -adic L -functions, we have the unique power series $f(T; \omega\phi^{-1}) \in A_\phi$ such that

$$f(\kappa^{s-1}; \omega\phi^{-1}) = L_p(s; \omega\phi^{-1}),$$

where $\mathbf{Z}_p[\phi] = \mathbf{Z}_p[\{\text{all values of } \phi\}]$ and $A_\phi = \mathbf{Z}_p[\phi][[T]]$. We note that

Received February 25, 1982

$$f(0; \omega\phi^{-1}) = L_p(0; \omega\phi^{-1}) = (1 - \phi^{-1}(p))L(0; \phi^{-1}).$$

(0.2) DEFINITION. We define $\hat{f}(T; \omega\phi^{-1}) \in A_\phi$ by

$$\hat{f}(T; \omega\phi^{-1}) = \begin{cases} f(T; \omega\phi^{-1})/T & \text{if } \phi(p)=1, \\ f(T; \omega\phi^{-1}) & \text{otherwise.} \end{cases}$$

Ferrero and Greenberg [2] have proved that $\hat{f}(0; \omega\phi^{-1}) \neq 0$. Then we see that

$$\hat{f}(\zeta - 1; \omega\phi^{-1}) \neq 0 \quad \text{for all } \zeta \text{ with } \zeta^{p^n} = 1 \text{ and } n \geq 0.$$

Hence the order of

$$A_\phi / (\hat{f}(T; \omega\phi^{-1}), \omega_n)$$

is finite, where $\omega_n = (1+T)^{p^n} - 1$.

For a finite set A , let $\#A$ denote the cardinality of A . A representation of a group G will be called \mathbf{Q}_p -irreducible if it is defined over \mathbf{Q}_p and irreducible over \mathbf{Q}_p . A character of G will be called \mathbf{Q}_p -irreducible if it is the character of some \mathbf{Q}_p -irreducible representation of G .

(0.3) THEOREM. Assume that

- (1) k/\mathbf{Q} is a finite abelian extension,
- (2) k is imaginary, and
- (3) the degree $[k:\mathbf{Q}]$ is prime to p .

Then we have

$$\#(A_{\infty}^{\prime})^{\Gamma_n} = \# \bigoplus_{\phi} A_{\phi} / (\hat{f}(T; \omega\phi^{-1}), \omega_n) \quad \text{for all } n \geq 0,$$

where Φ runs over all \mathbf{Q}_p -irreducible characters of $G = \text{Gal}(k/\mathbf{Q})$ such that $\Phi \neq \omega$, $\Phi(j) \neq \mathbf{Q}(1)$ and ϕ is an absolutely irreducible component of Φ .

For $a, b \in \mathbf{Q}_p^{\times}$, we write $a \sim_p b$ if $\text{ord}_p(a) = \text{ord}_p(b)$. Note that

$$\#A_{\phi} / (\hat{f}(T; \omega\phi^{-1}), \omega_n) \sim_p \prod_{\phi} \prod_{\zeta^{p^n}=1} \hat{f}(\zeta - 1; \omega\phi^{-1}), \quad (0.4)$$

where ϕ runs over all "conjugates" of ϕ over \mathbf{Q}_p .

(0.5) Remark. When no prime of the maximal real subfield k^+ of k lying over p splits in k , our formula in Theorem (0.3) is a direct consequence of the analytic class number formula for k (c.f. [1]). But, if there exist some primes of k^+ lying over p which split in k , then $(A_{\infty}^{\prime})^{\Gamma_n}$ is an infinite group and $f(0; \omega\phi^{-1})$ vanishes for some ϕ .

(0.6) Remark. To prove Theorem (0.3), we use essentially Gauss sums, Gross-Koblitz formula concerning a relation between Gauss sums and special values of Morita's p -adic Γ -function in [4], and Ferrero-Greenberg formula concerning

$L'_p(0; \chi)$ in [2].

(0.7) *Remark.* The assumption (3) is not essential. In fact, to prove Theorem (2.1), we need not assume that the degree of k over \mathbf{Q} is prime to p .

(0.8) *Remark.* In [2], Ferrero and Greenberg proved Theorem (0.3) when k is imaginary quadratic and $n=0$.

We define fundamental Iwasawa's modules in §1. In §2, we reduce Theorem (0.3) to Theorem (2.1). In §3, we introduce an essential exact sequences of Iwasawa's modules following [3]. And in §4, p -adic regulators are defined. In §5, following [4], we define Gauss sums, which we use to combine orders of two modules in Theorem (2.1). And the group of Gauss sums is introduced. In §6, we prove Theorem (2.1). In §7, some examples are given.

The author had studied some parts of the content of this paper from December 1980 till July 1981 with H. Nakazato. The author expresses his gratitude to Mr. H. Nakazato for his allowance of publishing this paper.

Notations.

As usual, $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$, and \mathbf{C} denote the ring of rational integers, the field of rational numbers, the field of real numbers, and the field of complex numbers, respectively. For a prime number p , \mathbf{Z}_p and \mathbf{Q}_p denote the ring of p -adic integers and the field of p -adic numbers, respectively. Let $\bar{\mathbf{Q}}$ (resp. $\bar{\mathbf{Q}}_p$) be an fixed algebraic closures of \mathbf{Q} (resp. \mathbf{Q}_p). We also fix embeddings $\bar{\mathbf{Q}} \subset \mathbf{C}$ and $\rho: \bar{\mathbf{Q}} \subset \bar{\mathbf{Q}}_p$.

§1. Iwasawa's modules.

Let k/\mathbf{Q} be as in Theorem (0.3). Since the degree of k over \mathbf{Q} is prime to p , all primes of k lying over p are totally ramified in k . Since $(A'_{\infty})^{\Gamma_n}$ is finite for $n \geq 0$, and the natural maps $A'_m \rightarrow A'_m$ are injective for $m \geq n \geq 0$, we have

(1.1) LEMMA. *For any integer $n \geq 0$, there exists an integer m_0 such that $(A'_{\infty})^{\Gamma_n} = (A'_m)^{\Gamma_n}$ for all $m \geq m_0$.*

Let Z be the decomposition group of p for k/\mathbf{Q} . Recall that $G = \text{Gal}(k/\mathbf{Q})$ and $\hat{G} = \text{Hom}(G, \bar{\mathbf{Q}}_p^{\times})$. For any $\phi \in \hat{G}$, $\text{Tr } \phi$ denotes the \mathbf{Q}_p -irreducible character of G which contains ϕ as an absolutely irreducible component, and $e(\text{Tr } \phi)$ denotes the orthogonal idempotent in $\mathbf{Z}_p[G]$ associated to $\text{Tr } \phi$. We consider A_n, D_n , and A'_n as $\mathbf{Z}_p[G]$ -modules in the natural way. Since all primes of k lying over p are totally ramified in k_n , we have

(1.2.) LEMMA. *If the restriction $\phi|_Z$ is not trivial, then $e(\text{Tr } \phi)D_n = 0$ for all $n \geq 0$.*

Following [3], we have

(1.3) LEMMA. For $m \geq n \geq 0$, we have

$$D_m^-/D_n^- \cong ((\mathbf{Z}_p/p^{m-n}\mathbf{Z}_p)[G/Z])^- \quad \text{as } \mathbf{Z}_p[G]\text{-modules.}$$

(1.4) LEMMA. For $m \geq n \geq 0$,

$$0 \longrightarrow D_n^- \longrightarrow A_n^- \xrightarrow{\alpha} (A_m^-)^{G_n}/D_m^- \longrightarrow 0$$

is an exact sequence of $\mathbf{Z}_p[G]$ -modules, where α is induced by the canonical inclusion $A_n^- \rightarrow A_m^-$.

For $m \geq n \geq 0$, put

$$M_n^{(m)} = \{a \in A_m^- \mid (s-1)a \in D_m^-\},$$

where s is a generator of $\text{Gal}(k_m/k_n)$ (c.f. [3]). Define a homomorphism $\beta : M_n^{(m)} \rightarrow D_m^-$ by $\beta(a) = (s-1)a$. Then $D_m^- \subset \text{Ker } \beta = (A_m^-)^{G_n}$. We have an exact sequence of $\mathbf{Z}_p[G]$ -modules:

$$0 \longrightarrow (A_m^-)^{G_n}/D_m^- \longrightarrow M_n^{(m)}/D_m^- \longrightarrow D_m^-. \tag{1.5}$$

From Lemma (1.4) and since $M_n^{(m)}/D_m^- = (A_m^-)^{G_n}$, we have an exact sequence of $\mathbf{Z}_p[G]$ -modules:

$$0 \longrightarrow A_n^- \longrightarrow (A_m^-)^{G_n} \longrightarrow D_m^-. \tag{1.6}$$

§ 2. Reduction.

In this section, we reduce Theorem (0.3) to the following theorem.

(2.1) THEOREM. Suppose that

- (1) k/\mathbf{Q} is a finite abelian extension,
- (2) k is imaginary, and
- (3) p is totally decomposed in k/\mathbf{Q} .

Then we have

$$\#(A_\infty^-)^{G_n} = \# \bigoplus_{\phi} A_{\phi} / (\hat{f}(T; \omega\phi^{-1}), \omega_n) \quad \text{for } n \geq 0,$$

where Φ and ϕ are as in Theorem (0.3).

In Theorem (2.1), we need not assume that the degree $[k:\mathbf{Q}]$ is prime to p , and it is essential that p is totally decomposed in k/\mathbf{Q} .

Let k/\mathbf{Q} satisfy the conditions (1), (2), and (3) in Theorem (0.3). For $n \geq 0$, let \mathbf{Q}_n be the n -th layer of the unique \mathbf{Z}_p -extension of \mathbf{Q} (c.f. [6]). Since $[k:\mathbf{Q}]$ is prime to p , we see that $k_n = k\mathbf{Q}_n$.

(2.2) LEMMA. $\#A_n^- \sim \prod_p \prod_{\phi} \prod_{\eta} L(0; \phi^{-1}\eta^{-1}) \quad \text{for } n \geq 0,$

where ϕ runs over all characters of $\text{Gal}(k/\mathbf{Q})$ such that $\phi(j) = -1$ and $\phi \neq \omega$, and η runs over all characters of $\text{Gal}(\mathbf{Q}_n/\mathbf{Q})$.

As in §1, let Z be the decomposition group of p for k/\mathbf{Q} . Let X_1 (resp. X_2) be the set of all \mathbf{Q}_p -irreducible characters $\text{Tr } \phi$ of $G = \text{Gal}(k/\mathbf{Q})$ such that $\phi(j) = -1$ and $\phi(p) = 1$ (resp. $\phi(p) \neq 1$). Let $m \geq n \geq 0$. Put $A'_{m,i} = \bigoplus_{\phi \in X_i} e(\phi)A'_m$, and $A_{m,i} = \bigoplus_{\phi \in X_i} e(\phi)A_m$ for $i = 1$ and 2 . Then $A'_m = A'_{m,1} \oplus A'_{m,2}$, and $A_m = A_{m,1} \oplus A_{m,2}$.

From Lemma (1.2) and (1.6), we see that

$$(A'_{m,2})^{\Gamma n} = A'_{n,2} = A_{n,2}. \tag{2.3}$$

Let $A(k^Z)_n$ denote the p -Sylow subgroup of the ideal class group of $(k^Z)_n$, where $(k^Z)_n$ is the n -th layer of the cyclotomic \mathbf{Z}_p -extension of the fixed field k^Z of Z . Then

$$A(k^Z)_n \cong A_{n,1} \quad \text{and} \quad A(k^Z)'_m \cong A'_{m,1}. \tag{2.4}$$

By Lemma (2.2) for k^Z , we have

$$\#A(k^Z)_n \sim \prod_p \prod_{\phi} \prod_{\eta} L(0; \phi^{-1}\eta^{-1}), \tag{2.5}$$

where ϕ runs over all characters of $\text{Gal}(k/\mathbf{Q})$ such that $\phi(j) = -1$, $\phi \neq \omega$, and $\phi|Z = 1$, and η runs over all characters of $\text{Gal}(\mathbf{Q}_n/\mathbf{Q})$.

In the rest of this section, we shall prove the following lemma.

(2.6) LEMMA. *Theorem (0.3) follows from Theorem (2.1).*

Proof. Assume that k satisfies the conditions (1), (2), and (3) in Theorem (0.3). For any $n \geq 0$, there exists an integer $m \geq n$ such that

$$(A(k^Z)'_{\infty})^{\Gamma n} = (A(k^Z)'_m)^{\Gamma n} \quad \text{and} \quad (A'_{\infty})^{\Gamma n} = (A'_m)^{\Gamma n}.$$

Hence, by (2.3) and (2.4), we have

$$(A'_{\infty})^{\Gamma n} = (A'_{m,1})^{\Gamma n} \oplus (A'_{m,2})^{\Gamma n} \cong (A(k^Z)'_{\infty})^{\Gamma n} \oplus A_{n,2}. \tag{2.7}$$

By Theorem (2.1) for k^Z , we have

$$\begin{aligned} \#(A(k^Z)'_{\infty})^{\Gamma n} &= \# \bigoplus_{\psi} A_{\psi} / (\hat{f}(T; \omega\phi^{-1}), \omega_n) \\ &= \# \bigoplus_{\phi \in X_1} A_{\phi} / (\hat{f}(T; \omega\phi^{-1}), \omega_n), \end{aligned} \tag{2.8}$$

where ψ and ϕ are as in Theorem (2.1) with respect to k^Z . On the other hand, since $A_n = A_{n,1} \oplus A_{n,2} \cong A(k^Z)_n \oplus A_{n,2}$, from (2.2) and (2.5), we see that

$$\#A_{n,2} \sim \prod_p \prod_{\phi|Z \neq 1} \prod_{\eta} L(0; \phi^{-1}\eta^{-1}) \sim \prod_p \prod_{\phi|Z \neq 1} \prod_{\zeta^{p^n}=1} \hat{f}(\zeta - 1; \omega\phi^{-1}). \tag{2.9}$$

Combining (2.7), (2.8), and (2.9), we obtain Lemma (2.6).

§3 The group of imaginary p -units.

In the following, we assume that k satisfies the conditions (1)-(3) in Theorem (2.1). For $n \geq 0$, let H_n be the group of p -units of k_n :

$$H_n = \{\alpha \in k_n^\times \mid (\alpha) = \text{product of primes of } k_n \text{ lying over } p\}.$$

Let $m \geq n \geq 0$. Let $N_{m,n} : k_m \rightarrow k_n$ be the norm map. Recall that

$$M_n^{(m)} = \{a \in A_m^- \mid (s-1)a \in D_m^-\},$$

where s is a generator of $\text{Gal}(k_m/k_n)$.

(3.1) DEFINITION. We define a homomorphism

$$\varphi_n^{(m)} : M_n^{(m)} \longrightarrow H_n^{1-j}/N_{m,n}(H_m^{1-j})$$

in the following way (c.f. [1, 3]). Let $c \in M_n^{(m)}$ and let $\mathfrak{A} \in c$. Then $\mathfrak{A}^{1-s} = (\alpha)\mathfrak{B}$ for some $\alpha \in k_m^\times$ and some ideal \mathfrak{B} which is a product of primes of k_m lying over p . Define

$$\varphi_n^{(m)}(c) = N_{m,n}(\alpha^{1-j}) \bmod N_{m,n}(H_m^{1-j}).$$

This is well-defined (c.f. [3]), and we have

- (3.2) LEMMA ([3]). (1) $\text{Ker } \varphi_n^{(m)} = (A_m^-)^{\Gamma_n}$, and
 (2) $\text{Im } \varphi_n^{(m)} = (H_n^{1-j} \cap N_{m,n}(k_m^\times)^{1-j})/N_{m,n}(H_m^{1-j})$.

Proof. (1) See [3],

(2) By definition of $\varphi_n^{(m)}$, $\text{Im } \varphi_n^{(m)} \subset (H_n^{1-j} \cap N_{m,n}(k_m^\times)^{1-j})/N_{m,n}(H_m^{1-j})$. Take any $\alpha \in k_m^\times$ such that $N_{m,n}(\alpha) \in H_n^{1-j}$. Then $(N_{m,n}(\alpha))$ is an ideal of k_n which is a product of primes of k_n lying over p . Since each prime of k_n lying over p is totally ramified in k_m/k_n , there exists an ideal \mathfrak{B} of k_m which is a product of primes of k_m lying over p such that $(N_{m,n}(\alpha)) = N_{m,n}(\mathfrak{B})$. Then $N_{m,n}(\alpha\mathfrak{B}^{-1}) = (1)$. Thus there exists an ideal \mathfrak{A} of k_m such that $(\alpha)\mathfrak{B}^{-1} = \mathfrak{A}^{1-s}$. Let r be an integer prime to p such that the class of $\mathfrak{A}^{r(1-j)}$ is contained in A_m^- . Put $a = \text{class of } \mathfrak{A}^{r(1-j)}$. Then $a \in M_n^{(m)}$ and $\varphi_n^{(m)}(a) = N_{m,n}(\alpha^{2r(1-j)}) \bmod N_{m,n}(H_m^{1-j})$. Since $(H_n^{1-j} \cap N_{m,n}(k_m^\times)^{1-j})/N_{m,n}(H_m^{1-j})$ is a finite abelian p -group, $\text{Im } \varphi_n^{(m)} = (H_n^{1-j} \cap N_{m,n}(k_m^\times)^{1-j})/N_{m,n}(H_m^{1-j})$.

(3.3) COROLLARY.

$$0 \longrightarrow A_n'^- \longrightarrow (A_m'^-)^{\Gamma_n} \xrightarrow{\tilde{\varphi}} \text{Im } \varphi_n^{(m)} \longrightarrow 0$$

is an exact sequence of $\mathbf{Z}_p[G]$ -modules, where $\tilde{\varphi}$ is induced from $\varphi_n^{(m)}$ since $\varphi_n^{(m)}(D_m^-) = 0$ (c.f. (1.5) and (1.6)).

§ 4. *p*-adic regurators.

In this section, we shall define *p*-adic regurators for certain subgroups of H_0^{1-j} . Assume that k satisfies the conditions (1)-(3) in Theorem (2.1). For $n \geq 0$, let E_n be the unit group of k_n and let \mathbf{P}_n be the subgroup $\{(\alpha) | \alpha \in H_n\}$ of the ideal group of k_n . From a natural exact sequence $0 \rightarrow E_n \rightarrow H_n \rightarrow \mathbf{P}_n \rightarrow 0$, we have an exact sequence $0 \rightarrow E_n \cap H_n^{1-j} \rightarrow H_n^{1-j} \rightarrow \mathbf{P}_n^{1-j} \rightarrow 0$. Let $\mu(k_n)$ denote the group of all roots of unity in k_n , then we have $E_n \cap H_n^{1-j} = \mu(k_n) \cap H_n^{1-j}$. Hence, we have (letting $n=0$)

$$\mu(k)H_0^{1-j} / \mu(k) \cong \mathbf{P}_0^{1-j}. \tag{4.1}$$

We note that \mathbf{P}_0^{1-j} is a free \mathbf{Z} -module of rank $g = [k : \mathbf{Q}] / 2$. Assume that M is a submodule of $\mu(k)H_0^{1-j}$ such that $\mu(k)M / \mu(k)$ has rank g . Let m_1, m_2, \dots, m_g be a system of elements of $\mu(k)M$ such that $m_1 \bmod \mu(k), \dots, m_g \bmod \mu(k)$ are \mathbf{Z} -basis of $\mu(k)M / \mu(k)$. Let s_1, s_2, \dots, s_g be a system of representatives of $G / \{1, j\}$. Let \log_p denote the *p*-adic logarithm from \mathbf{Q}_p^\times into \mathbf{Q}_p normalized by $\log_p p = 0$ and $\log_p \zeta = 0$ for $\zeta^{p-1} = 1$ (c.f. [5]). Recall that $\rho : \bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_p$ is the fixed embedding. Then $\rho(k) \subset \mathbf{Q}_p$ by the assumption (3) in Theorem (2.1).

(4.2) DEFINITION. We define the *p*-adic regurator of M by

$$R_p(M) = \det \begin{pmatrix} \log_p \rho(s_1 m_1), & \dots, & \log_p \rho(s_1 m_g) \\ \vdots & & \vdots \\ \log_p \rho(s_g m_1), & \dots, & \log_p \rho(s_g m_g) \end{pmatrix} \quad \text{up to } \pm 1.$$

This definition is independent of the choices of (s_1, \dots, s_g) and (m_1, \dots, m_g) .

(4.3) LEMMA. Let $M_1 \subset M_2$ be submodules of $\mu(k)H_0^{1-j}$ such that $R_p(M_1) \neq 0$. Then, $R_p(M_2) \neq 0$, and

$$\frac{R_p(M_1)}{R_p(M_2)} = (\mu(k)M_2 : \mu(k)M_1) \quad \text{up to } \pm 1.$$

§ 5. Gauss sums.

In this section, we recall Gauss sums in [4]. Assume that k satisfies the conditions (1)-(3) in Theorem (2.1). Let N be the conductor of k/\mathbf{Q} . Since p is totally decomposed in k , N is prime to p . Let $K = \mathbf{Q}(\mu_N)$, $G_N = \text{Gal}(K/\mathbf{Q})$, $H = \text{Gal}(K/k)$, and let D be the decomposition group of p for K/\mathbf{Q} , where μ_N denote the group of all N -th roots of unity in $\bar{\mathbf{Q}}$. For any $t \in \mathbf{Z}$ such that $(t, N) = 1$, define $s_t \in G_N$ by $s_t(\zeta) = \zeta^t$ for all $\zeta \in \mu_N$. Then $D = \langle s_p \rangle$. Let v be the place of $\bar{\mathbf{Q}}$ corresponding to the fixed embedding $\rho : \bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_p$. Let \mathfrak{p} (resp. \mathfrak{p}_N) be the prime of k (resp. K) which is the restriction of v to k (resp. K).

(5.1) DEFINITION. Put

$$\mathcal{A}_N = \frac{1}{N} \mathbf{Z}/\mathbf{Z} - \{0 \bmod \mathbf{Z}\} \quad \text{and} \quad \mathbf{A}_N = \text{Map}(\mathcal{A}_N, \mathbf{Z}).$$

For $a = (t/N \bmod \mathbf{Z}) \in \mathcal{A}_N$, let $\delta_{t/N} = \delta_a \in \mathbf{A}_N$ be the map defined by $\delta_a(a) = 1$ and $\delta_a(b) = 0$ for $b \in \mathcal{A}_N$ with $b \neq a$. The group G_N acts on \mathcal{A}_N and \mathbf{A}_N by

$$s_t(t'/N \bmod \mathbf{Z}) = tt'/N \bmod \mathbf{Z} \quad \text{for } s_t \in G_N, \quad t'/N \bmod \mathbf{Z} \in \mathcal{A}_N$$

and

$$(s\alpha)(a) = \alpha(s^{-1}a) \quad \text{for } s \in G_N, \quad \alpha \in \mathbf{A}_N, \quad a \in \mathcal{A}_N.$$

We define the Gauss sum $g(\alpha, \mathfrak{p}_N, \Psi \circ \text{Tr}) = g(\alpha, \mathfrak{p}_N)$ as in (1.3) and (1.4) of [4].

(5.2) *Note.* Let $\alpha \in N\mathbf{A}_N$. Then $g(\alpha, \mathfrak{p}_N)$ is contained in K^p . The action of G_N on $g(\alpha, \mathfrak{p}_N)$ is given by

$$g(\alpha, \mathfrak{p}_N)^s = g(s\alpha, \mathfrak{p}_N) \quad \text{for } s \in G_N.$$

For $x \in \mathbf{R}$, let $\langle x \rangle$ be the unique real number such that $0 \leq \langle x \rangle < 1$ and $x - \langle x \rangle \in \mathbf{Z}$. For $a = (t/N \bmod \mathbf{Z}) \in \mathcal{A}_N$, let $\langle a \rangle = \langle t/N \rangle$, and for $\alpha \in \mathbf{A}_N$, let $n(\alpha) = \sum_{a \in \mathcal{A}_N} \alpha(a) \langle a \rangle$.

Let Γ_p be the p -adic Γ -function defined by Morita. As in [4], we define $\Gamma_p: \mathbf{A}_N \rightarrow \mathbf{Z}_p$ by

$$\Gamma_p(\alpha) = \prod_{a \in \mathcal{A}_N} \Gamma_p(\langle a \rangle)^{\alpha(a)} \quad \text{for } \alpha \in \mathbf{A}_N.$$

The following theorem was proved by Gross and Koblitz [4].

(5.3) **THEOREM.** *If $n(\alpha) \in \mathbf{Z}$, then*

$$\rho(g(\alpha, \mathfrak{p}_N)) = (-p)^{n(\sum_{s \in D} s\alpha)} \Gamma_p(\sum_{s \in D} s\alpha) \quad \text{in } \mathbf{Q}_p.$$

(5.4) **COROLLARY.** *Let $\alpha \in N\mathbf{A}_N$. Then*

$$\log_p \rho(g(\alpha, \mathfrak{p}_N)) = \sum_{s \in D} \log_p \Gamma_p(s\alpha).$$

Let $X^- = \{\phi \in \hat{G} \mid \phi(j) = -1\}$. Let M be a divisor of N . We put $X_M = \{\phi \in X^- \mid \text{conductor of } \phi = M\}$ and $H_M = \text{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q}(\mu_M)) \subset G_N$. Recall that $2g = [k: \mathbf{Q}] = \#G = \#(G_N/H)$. Fix a system of representatives $\{s_1, \dots, s_{2g}\}$ of G_N/H ($s_i \in G_N$, $1 \leq i \leq 2g$). For $\phi \in X^-$, let

$$e(\phi) = \frac{1}{\#G} \sum_{s \in G} \phi(s^{-1})s \in \bar{\mathbf{Q}}_p[G]$$

and

$$\check{e}(\phi) = \frac{1}{\#G} \sum_{i=1}^{2g} \phi((s_i H)^{-1})s_i \in \bar{\mathbf{Q}}_p[G_N].$$

Then we see that $\#G \sum_{\phi \in X_M^-} e(\phi) \in \mathbf{Z}[G]$ and $\#G \sum_{\phi \in X_M^-} \tilde{e}(\phi) \in \mathbf{Z}[G_N]$.

(5.5) DEFINITION. Let \mathbf{A}_k be the submodule of $N\mathbf{A}_N$ generated by

$$\left\{ \#G \sum_{\phi \in X_M^-} e(\phi) N\delta_{1/M} | M | N \right\}.$$

(5.6) DEFINITION. We define the Gauss sum $g_k(\alpha)$ of k associated to $\alpha \in N\mathbf{A}_N$ by

$$g_k(\alpha) = N_{K^D/k}(g(\alpha, \mathfrak{p}_N))$$

and the group \mathcal{G}_k of Gauss sums of k by

$$\mathcal{G}_k = \{g_k(\alpha) | \alpha \in \mathbf{A}_k\}.$$

We define a $\mathbf{Z}[G_N]$ -homomorphism $S_k : N\mathbf{A}_N \rightarrow \mathbf{Z}[G]$ by

$$S_k(\alpha) = \sum_{s \in G_N} n(s\alpha)(sH)^{-1} \quad \text{for } \alpha \in N\mathbf{A}_N.$$

We have Stickelberger relations for k .

(5.7) If $\alpha \in N\mathbf{A}_N$, then

$$(g_k(\alpha)) = \mathfrak{p}^{S_k(\alpha)} \quad \text{in } k.$$

For $n \geq 0$, let \mathbf{D}_n be the subgroup of the ideal group of k_n generated by primes of k_n lying over p , and let $\mathbf{G}_k = \{(g_k(\alpha)) | \alpha \in \mathbf{A}_k\}$. From (5.7), \mathbf{G}_k is a $\mathbf{Z}[G]$ -submodule of \mathbf{D}_0 .

(5.8) PROPOSITION.

$$(\mathbf{D}_0^{1-j} : \mathbf{G}_k^{1-j}) = (2gN)^g \prod_{M|N} (\#H_M)^{\#X_M^-} \prod_{\phi \in X^-} L(0; \phi^{-1}).$$

Proof. Since p is totally decomposed in k , we have

$$\mathbf{D}_0^{1-j} = (1-j)\mathbf{Z}[G] \cdot \mathfrak{p} \cong (1-j)\mathbf{Z}[G].$$

We compute the index $(\mathbf{D}_0^{1-j} : \mathbf{G}_k^{1-j})$ in $(1-j)\mathbf{Z}[G] \otimes \bar{\mathbf{Q}}_p = (1-j)\bar{\mathbf{Q}}_p[G]$ and in $e(\phi)\bar{\mathbf{Q}}_p[G] = e(\phi)\bar{\mathbf{Q}}_p$ for $\phi \in X^-$, because $(1-j)\bar{\mathbf{Q}}_p[G] = \bigoplus_{\phi \in X^-} e(\phi)\bar{\mathbf{Q}}_p$. Let $M|N$ and let $\phi \in X_M^-$. For $L|N$, we have

$$\begin{aligned} e(\phi)S_k(\#G \sum_{\phi \in X_L^-} \tilde{e}(\phi)N\delta_{1/L}) \\ = \begin{cases} e(\phi)\#GN \sum_{s_t \in G_N} \langle t/M \rangle \phi^{-1}(s_t H) & \text{if } L=M, \\ 0 & \text{if } L \neq M. \end{cases} \end{aligned}$$

Futhermore we have

$$\sum_{s_t \in G_N} \langle t/M \rangle \phi^{-1}(s_t H) = \#H_M \sum_{\bar{s}_t \in G_M} \langle t/M \rangle \phi_M^{-1}(\bar{s}_t \bar{H}),$$

where $\bar{s}_t = s_t H_M$, $G_M = G_N / H_M$, $\bar{H} = H H_M / H_M$, and ϕ_M is the character of G_M / \bar{H} induced from ϕ . Hence

$$e(\phi) S_k({}^*G \sum_{\phi \in X_{\bar{L}}} \tilde{\rho}(\phi) N \delta_{1/L}) = \begin{cases} e(\phi) {}^*G N {}^*H_M L(0; \phi^{-1}) & \text{if } L = M, \\ 0 & \text{if } L \neq M. \end{cases}$$

Since $(1-j)e(\phi) = 2e(\phi)$, we have

$$(\mathbf{D}_0^{1-j} : \mathbf{G}_k^{1-j}) = (2gN)^g \prod_{M|N} ({}^*H_M)^{\#X_M^-} \prod_{\phi \in X^-} L(0; \phi^{-1}).$$

We shall compute the p -adic regulator of \mathcal{G}_k^{1-j} by using p -adic L -functions.

(5.9) THEOREM.

$$R_p(\mathcal{G}_k^{1-j}) = (4gN)^g \prod_{M|N} ({}^*H_M)^{\#X_M^-} \prod_{\phi \in X^-} L'_p(0; \omega\phi^{-1}) \quad \text{up to } \pm 1.$$

We recall a result of Ferrero and Greenberg [2].

(5.10) THEOREM. *Let $M|N$ and let $\phi \in X_{\bar{M}}$. Then*

$$L'_p(0; \omega\phi^{-1}) = \sum_{\bar{s}_t \in G_M} \phi^{-1}(\bar{s}_t) \log_p \Gamma_p(s_t \delta_{1/M}).$$

By (5.10) and (5.4),

$$L'_p(0; \omega\phi^{-1}) = \frac{1}{N^{\#H_M}} \sum_{s \in G} \phi^{-1}(s) \log_p \rho(g_k(N\delta_{1/M})^s). \tag{5.11}$$

Put $g_{k,M} = g_k(N\delta_{1/M})$. We have, for $s_t \in G_N$ with $s_t H = s$,

$$\begin{aligned} & \log_p \rho(g_k(N^{\#G} \sum_{\phi \in X_{\bar{M}}} \tilde{\rho}(\phi) s_t \delta_{1/M})) \\ &= \log_p \rho\left((g_{k,M}) \sum_{\phi \in X_{\bar{M}}} e(\phi) s \right) \end{aligned}$$

(5.12) Claim. Let $L|N$ and let $\phi \in X_{\bar{L}}$. Then

$$\begin{aligned} & \sum_{s \in G} \phi^{-1}(s) \log_p \rho\left((g_{k,M}) \sum_{\phi \in X_{\bar{M}}} e(\phi) s \right) \\ &= \begin{cases} \sum_{s \in G} \phi^{-1}(s) \log_p \rho((g_{k,M})^s) & \text{if } L = M, \\ 0 & \text{if } L \neq M. \end{cases} \end{aligned}$$

In fact, computing in $\bar{\mathbf{Q}}_p[G] \otimes \log_p \rho(\mathcal{G}_k^{1-j}) = \bar{\mathbf{Q}}_p[G] = \sum_{\phi} e(\phi) \bar{\mathbf{Q}}_p$, because $\log_p \rho(\mathcal{G}_k^{1-j}) \subset \bar{\mathbf{Q}}_p$, we have

$$e(\phi) \sum_{s \in G} s^{-1} \log_p \rho\left((g_{k,M}) \sum_{\phi \in X_{\bar{M}}} e(\phi) s \right)$$

$$\begin{aligned}
 &= e(\phi)^{\#G} \sum_{\phi \in X_M^-} e(\phi) \sum_{s \in G} s^{-1} \log_p \rho((g_{k, M})^s) \\
 &= \begin{cases} e(\phi)^{\#G} \sum_{s \in G} \phi^{-1}(s) \log_p \rho((g_{k, M})^s) & \text{if } L=M, \\ 0 & \text{if } L \neq M. \end{cases}
 \end{aligned}$$

Proof of Theorem (5.9)

Define the map $\log_p: H_0^{1-j} \rightarrow (1-j)Q_p[G]$ by

$$\log_p(x) = (1-j) \sum_{s \in G/(1, j)} \log_p \rho(x^s) s^{-1} \quad \text{for } x \in H_0^{1-j}.$$

Since $\log_p(\mathcal{G}_k^{1-j}) \subset (1-j)Q_p[G]$, we compute $R_p(\mathcal{G}_k^{1-j})$ in $(1-j)Q_p[G] \otimes \bar{Q}_p = (1-j)\bar{Q}_p[G] = \bigoplus_{\phi \in X^-} e(\phi)\bar{Q}_p$. Since \mathcal{G}_k^{1-j} is generated by

$$(g_{k, M}^{1-j})_{\phi \in X_L^-}^{\#G \sum e(\phi)} \quad \text{for all } M|N, L|N,$$

we have from (5.12)

$$\begin{aligned}
 \pm R_p(\mathcal{G}_k^{1-j}) &= \prod_{M|N} \prod_{\phi \in X_M^-} 2^{\#G} \sum_{s \in G} \phi^{-1}(s) \log_p \rho((g_{k, M})^s) \\
 &= (2^{\#G})^{\#X^-} \prod_{M|N} \prod_{\phi \in X_M^-} N^{\#} H_M L'_p(0; \omega\phi^{-1}). \quad \text{Q. E. D.}
 \end{aligned}$$

Ferrero and Greenberg [2] have proved that $L'_p(0; \omega\phi^{-1}) \neq 0$. Then we see that $R_p(\mathcal{G}_k^{1-j}) \neq 0$. Hence, by Lemma (4.3),

$$R_p(H_0^{1-j}) \neq 0 \quad (\text{c.f. [3]}). \tag{5.13}$$

§ 6. Proof of Theorem (2.1).

In this section, we shall prove Theorem (2.1). Let $n \geq 0$. Recall that $\mathbf{D}_n = \{\prod \mathfrak{P}^{m(\mathfrak{P})} | \mathfrak{P} | p \text{ in } k_n, m(\mathfrak{P}) \in \mathbf{Z}\}$. Let \mathcal{P}_n be the principal ideal group of k_n . Put $\mathbf{P}_n = \mathcal{P}_n \cap \mathbf{D}_n$ and $\mathcal{D}_n = \mathbf{D}_n / \mathbf{P}_n$. Then

$$(\mathbf{D}_0^{1-j}; \mathbf{P}_0^{1-j}) = \# \mathcal{D}_0^{1-j} \quad (\text{up to a 2-factor}) \underset{p}{\sim} \# D_0^-.$$

From Lemma (4.3) and (5.13), we have

$$\pm \frac{R_p(\mathcal{G}_k^{1-j})}{R_p(H_0^{1-j})} = (\mathbf{P}_0^{1-j}; \mathbf{G}_k^{1-j}) = \frac{(\mathbf{D}_0^{1-j}; \mathbf{G}_k^{1-j})}{(\mathbf{D}_0^{1-j}; \mathbf{P}_0^{1-j})} \quad (\text{up to a 2-factor}).$$

Thus, from Proposition (5.8) and Theorem (5.9), we have

$$\pm \frac{\prod_{\phi \in X^-} L'_p(0; \omega\phi^{-1})}{R_p(H_0^{1-j})} = \frac{\prod_{\phi \in X^-} L(0; \phi^{-1})}{\# \mathcal{D}_0^{1-j}} \quad (\text{up to a 2-factor}) \tag{6.1}$$

(6.2) LEMMA. For $m \geq 0$,

$$\#(H_0^{1-j}/(H_0^{1-j} \cap N_{m,0}(k_m^\times)^{1-j})) \sim \frac{p^{(m+1)g}}{R_p(H_0^{1-j})}.$$

Proof. Recall the map \log_p in §5. Since k_m/k is totally ramified at p , by Hasse's norm theorem following [3], we have

$$x \in N_{m,0}(k_m^\times)^{1-j} \Leftrightarrow \log_p(x) \in (1-j)p^{m+1}\mathbf{Z}_p[G], \quad \text{for } x \in H_0^{1-j}. \quad \text{Q. E. D.}$$

(6.3) For $n \geq 0$ and for a sufficiently large $m \geq n$,

$$\mathbf{Z}_p \otimes (H_0^{1-j} \cap N_{m,0}(k_m^\times)^{1-j}) = \mathbf{Z}_p \otimes (N_{n,0}(H_n^{1-j} \cap N_{m,n}(k_m^\times)^{1-j})).$$

In fact, by Lemma (6.2), there exists a sufficiently large $m \geq n$, such that

$$\mathbf{Z}_p \otimes N_{n,0}(H_n^{1-j}) \subset \mathbf{Z}_p \otimes (H_0^{1-j} \cap N_{m,0}(k_m^\times)^{1-j}).$$

(6.4) For $m \geq n \geq 0$, we have

$$\begin{aligned} & (\mathbf{Z}_p \otimes H_0^{1-j} : \mathbf{Z}_p \otimes (H_0^{1-j} \cap N_{m,0}(k_m^\times)^{1-j})) \\ &= (\mathbf{Z}_p \otimes \mathbf{P}_0^{1-j} : \mathbf{Z}_p \otimes (\mathbf{P}_0^{1-j} \cap N_{m,0}(\mathcal{P}_m^{1-j}))) \end{aligned}$$

and

$$\begin{aligned} & (\mathbf{Z}_p \otimes (H_n^{1-j} \cap N_{m,n}(k_m^\times)^{1-j}) : \mathbf{Z}_p \otimes N_{m,n}(H_m^{1-j})) \\ &= (\mathbf{Z}_p \otimes (\mathbf{P}_n^{1-j} \cap N_{m,n}(\mathcal{P}_m^{1-j})) : \mathbf{Z}_p \otimes N_{m,n}(\mathbf{P}_m^{1-j})). \end{aligned}$$

For any $n \geq 0$, let m be an integer satisfying (6.3). Since the norm maps $N_{m,n} : \mathbf{D}_m^{1-j} \rightarrow \mathbf{D}_n^{1-j}$ and $N_{n,0} : \mathbf{D}_n^{1-j} \rightarrow \mathbf{D}_0^{1-j}$ are bijective, we have the following diagram :

$$\begin{array}{ccc} \mathbf{D}_m^{1-j} & \supset & \mathbf{P}_m^{1-j} \\ \wr \downarrow N_{m,n} & & \wr \downarrow \\ \mathbf{D}_n^{1-j} & \supset \mathbf{P}_n^{1-j} \cap N_{m,n}(\mathcal{P}_m^{1-j}) \supset N_{m,n}(\mathbf{P}_m^{1-j}) & \\ \wr \downarrow N_{n,0} & \wr \downarrow & \wr \downarrow \\ \mathbf{D}_0^{1-j} \supset \mathbf{P}_0^{1-j} \supset \mathbf{P}_0^{1-j} \cap N_{m,0}(\mathcal{P}_m^{1-j}) \supset N_{m,0}(\mathbf{P}_m^{1-j}). & & \end{array} \quad (6.5)$$

We have, by (6.5),

$$\begin{aligned} & (\mathbf{Z}_p \otimes (\mathbf{P}_n^{1-j} \cap N_{m,n}(\mathcal{P}_m^{1-j})) : \mathbf{Z}_p \otimes N_{m,n}(\mathbf{P}_m^{1-j})) \\ &= \frac{(\mathbf{Z}_p \otimes \mathbf{D}_m^{1-j} : \mathbf{Z}_p \otimes \mathbf{P}_m^{1-j})}{(\mathbf{Z}_p \otimes \mathbf{D}_0^{1-j} : \mathbf{Z}_p \otimes \mathbf{P}_0^{1-j})(\mathbf{Z}_p \otimes \mathbf{P}_0^{1-j} : \mathbf{Z}_p \otimes (\mathbf{P}_0^{1-j} \cap N_{m,0}(\mathcal{P}_m^{1-j})))}. \end{aligned}$$

Hence, by Lemma (3.2) and (6.4), we have

$$\# \text{Im } \varphi_n^{(m)} = \frac{\#(D_m^-/D_0^-)}{(\mathbf{Z}_p \otimes H_0^{1-j} : \mathbf{Z}_p \otimes (H_0^{1-j} \cap N_{m,0}(k_m^\times)^{1-j}))}.$$

Thus, by Lemma (6.2) and Lemma (1.3), we have

$$* \text{Im } \varphi_n^{(m)} \underset{p}{\sim} p^{-s} R_p(H_0^{1-j}). \tag{6.6}$$

Note that

$$L'_p(0; \omega\phi^{-1}) \underset{p}{\sim} p \hat{f}(0; \omega\phi^{-1}). \tag{6.7}$$

Proof of Theorem (2.1)

For a given n , take an integer $m \geq n$ such that $(A'_\infty)^{I^n} = (A'_m)^{I^n}$ and (6.3) holds. By using (3.3), (6.1), (6.6) and (6.7), we have

$$*(A'_m)^{I^n} \underset{p}{\sim} \prod_{\phi \in X^-} \prod_{\zeta^{p^n=1}} \tilde{f}(\zeta-1; \omega\phi^{-1}),$$

because

$$*(A'_n/A'_0) \underset{p}{\sim} \prod_{\phi \in X^-} \prod_{\substack{\zeta^{p^n=1} \\ \zeta \neq 1}} \tilde{f}(\zeta-1; \omega\phi^{-1}).$$

Hence, we complete the proof of Theorem (2.1).

§ 7. Examples.

1. Let $p=5$, and k be the unique subfield of $\mathbf{Q}(\exp(2\pi i/1949))$ of degree 4 over \mathbf{Q} . Then 5 splits completely in k/\mathbf{Q} . There are two imaginary \mathbf{Q}_5 -irreducible characters of $\text{Gal}(k/\mathbf{Q})$. We have $*A_0^- = 5^3$ and $D_0^- \cong \mathbf{Z}/5\mathbf{Z} \oplus \mathbf{Z}/5\mathbf{Z}$, by an easy computation. Hence $*A_0^- = 5$. By a computation (modulo congruence) of the coefficients of $f(T; \omega\phi^{-1})$, we have

$$*\bigoplus_{\phi} A_{\phi} / (\hat{f}(T; \omega\phi^{-1}), \omega_0) = 5^3.$$

Using Theorem (0.3) we have $*(A'_\infty)^{I^0} = 5^3$. Hence $A_0^- \cong (A'_\infty)^{I^0}$. Moreover, we see that $*A_1^- = 5^3$, $*D_1^- = 5^4$, and $*A_1^- = 5^5$. Note that λ^- -invariant of k (for $p=5$) is 6.

2. Let $p=5$, and k be the unique subfield of $\mathbf{Q}(\exp(2\pi i/2269))$ of degree 4 over \mathbf{Q} . We have

$$\bigoplus_{\phi} A_{\phi} / (\hat{f}(T; \omega\phi^{-1}), \omega_0) = \{0\}.$$

By using Theorem (0.3), we have $(A'_\infty)^{I^0} = \{0\}$. Hence $*D_0^- = *A_0^- = 5^3$. Note that λ^- -invariant of k is 2. We have $A_0^- = (A'_\infty)^{I^0} = \{0\}$.

REFERENCES

[1] COATES, J., LICHTENBAUM, S., On l -adic zeta functions. Ann. Math. **98** (1973), 498-550.
 [2] FERRERO, B., GREENBERG, R., On the behavior of p -adic L -functions at $s=0$. Inv. Math. **50** (1978), 91-102.
 [3] GREENBERG, R., On a certain l -adic representation. Inv. Math. **21** (1973), 117-124.

- [4] GROSS, B., KOBLITZ, N., Gauss sums and the p -adic Γ -function. Ann. Math. **109** (1979), 569-581.
- [5] IWASAWA, K., Lectures on p -adic L -functions. Ann. Math. Studies **74**, Princeton University Press, 1972.
- [6] IWASAWA, K., On Z_l -extensions of algebraic number fields. Ann. Math. **98** (1973), 246-326.
- [7] FEDERER, L., GROSS, B., Regulators and Iwasawa modules. Inv. Math. **62** (1981), 443-457.
- [8] GROSS, B., p -adic L -series at $s=0$. (to appear)

DEPARTMENT OF MATHEMATICS
TOKYO INSTITUTE OF TECHNOLOGY
OH-OKAYAMA, MEGURO-KU, TOKYO
JAPAN

Addendum in proof

We received from Gross the preprint of [8] after we had sent him the preprint of this paper. There is a partial overlap between the content of [8] and that of this paper. Assuming Conjecture (5.3) of the paper of Federer and Gross [7] and combining their Proposition (3.9) [7], one will get Theorem (0.3) in this paper in the case of $n=0$. In [7], they announced that Conjecture (5.3) of abelian case was proved in [8]. In this paper, without assuming Conjecture (5.3) [7], we prove Theorem (0.3) for all $n \geq 0$ by using Theorem (5.9).