J. Math. Soc. Japan
Vol. 16, No. 1, 1964

On some modules in the theory of cyclotomic fields

by Kenkichi IWASAWA*

(Received Oct. 3, 1963)

Let p be a fixed odd prime, and let $q_n=p^{n+1}$ for any integer $n\geqq 0$. Let F_n denote the cyclotomic field of q_n-th roots of unity over the rational field; and Φ_n, the local cyclotomic field of q_n-th roots of unity over the p-adic number field. The main purpose of the present paper is to introduce three compact modules $\mathfrak{X}$, $\mathfrak{Y}$, and $\mathfrak{Z}$ into the theory of cyclotomic fields F_n and Φ_n, $n\geqq 0$. They are defined as inverse limits of certain subgroups $\mathfrak{X}_n$, $\mathfrak{Y}_n$, and $\mathfrak{Z}_n$ respectively, of the additive group of Φ_n, $n\geqq 0$, and $\mathfrak{Y}$ is a submodule of $\mathfrak{X}$; $\mathfrak{Z}$, a submodule of $\mathfrak{Y}$. We shall determine the algebraic structure of $\mathfrak{X}/\mathfrak{Z}$ by direct computation, and we shall also show by class field theory how $\mathfrak{X}/\mathfrak{Y}$ and $\mathfrak{Y}/\mathfrak{Z}$ are related respectively to the ideal class groups and the unit groups of the fields F_n, $n\geqq 0$. Using these results, we shall then study the group-theoretical meaning of the classical class number formula for F_n as noted in a previous paper [**10**].

§1.

1.1. Let $\boldsymbol{Z}$, $\boldsymbol{Z}_p$, $\boldsymbol{Q}$ and $\boldsymbol{Q}_p$ denote the ring of rational integers, the ring of p-adic integers, the rational field, and the p-adic number field respectively. We shall fix an algebraic closure Ω of $\boldsymbol{Q}_p$, and consider all algebraic extensions of $\boldsymbol{Q}$ and $\boldsymbol{Q}_p$ as subfields of Ω.

Let F denote the union of all F_n, $n\geqq 0$; and Φ, the union of all Φ_n, $n\geqq 0$. Then both $F/\boldsymbol{Q}$ and $\Phi/\boldsymbol{Q}_p$ are abelian extensions, and their Galois groups are identified in a natural way. Put

$$G=G(F/\boldsymbol{Q})=G(\Phi/\boldsymbol{Q}_p)^{1)},$$
$$G_n=G(F_n/\boldsymbol{Q})=G(\Phi_n/\boldsymbol{Q}_p),$$
$$\Gamma=G(F/F_0)=G(\Phi/\Phi_0),$$
$$\Gamma_n=G(F/F_n)=G(\Phi/\Phi_n), \qquad n\geqq 0,$$

* The present research was supported in part by the National Science Foundation grant NSF-GP-379.

1) $G(\ /\ )$ shall denote the Galois group of the Galois extension in the parenthesis.

so that $\Gamma=\Gamma_0, G_n=G/\Gamma_n$.

Let W_n $(n\geqq 0)$ denote the group of all q_n-th roots of unity in F_n (in Φ_n), and let W be the union of all $W_n, n\geqq 0$. Let $\boldsymbol{U}$ be the multiplicative group of all p-adic units in $\boldsymbol{Q}_p$. Then there exists an isomorphism

$$\kappa: G\to \boldsymbol{U}$$

such that

$$\zeta^{\sigma}=\zeta^{\kappa(\sigma)},$$

for any σ in G and ζ in W. The image of Γ under κ is the subgroup $\boldsymbol{U}_0$ of all u in $\boldsymbol{U}$ such that $u\equiv 1 \bmod p$. Let $\boldsymbol{V}$ denote the subgroup of all $(p-1)$-st roots of unity in $\boldsymbol{U}$; $\boldsymbol{V}$ is a cyclic group of order $p-1$, and

$$\boldsymbol{U}=\boldsymbol{U}_0\times \boldsymbol{V}.$$

Let Δ denote the subgroup of G, corresponding to $\boldsymbol{V}$ under κ. Then

$$G=\Gamma\times\Delta,$$

and Δ is canonically isomorphic to G_0.

For any u in $\boldsymbol{U}$, let $\sigma(u)$ denote the inverse image of u under κ; $\sigma(u)$ is the element of G such that $\zeta^{\sigma(u)}=\zeta^u$ for any ζ in W. We denote by $\sigma(u)_n$ the image of $\sigma(u)$ under the natural homomorphism $G\to G_n$ $(n\geqq 0)$. Clearly $\sigma(u)_n$ depends only upon the residue class of $u \bmod q_n$.

In general, for any group $\mathfrak{G}$ and any additive abelian group A, let $A[\mathfrak{G}]$ denote the set of all maps $f:\mathfrak{G}\to A$ such that $f(x)=0$ except for a finite number of x's in $\mathfrak{G}$. Defining $f+g$ by

$$(f+g)(x)=f(x)+g(x),$$

we make $A[\mathfrak{G}]$ into a module. If A is a ring, $A[\mathfrak{G}]$ is nothing but the additive group of the group ring of $\mathfrak{G}$ over A. If there is a homomorphism $G\to\mathfrak{G}$, we can also make $A[\mathfrak{G}]$ into a G-module, by defining σf as

$$(\sigma f)(x)=f(s^{-1}x), \qquad x\in\mathfrak{G},$$

where s denotes the image of σ under $G\to\mathfrak{G}$.

For any integer i, we define an element ${}^i\varepsilon$ of the group ring $\boldsymbol{Z}_p[G]$ by

$${}^i\varepsilon=(p-1)^{-1}\sum_v v^{-i}\sigma(v), \qquad v\in\boldsymbol{V}.$$

The elements ${}^0\varepsilon, {}^1\varepsilon, \cdots, {}^{p-2}\varepsilon$ form a system of orthogonal idempotents in $\boldsymbol{Z}_p[G]$ with $\sum_i {}^i\varepsilon=1$. We also put

$${}^+\varepsilon=\sum_{i\ \text{even}} {}^i\varepsilon, \qquad {}^-\varepsilon=\sum_{i\ \text{odd}} {}^i\varepsilon.$$

Then ${}^+\varepsilon+{}^-\varepsilon=1$, ${}^+\varepsilon{}^-\varepsilon=0$. If A is a $\boldsymbol{Z}_p[G]$-module, we define submodules of A by

$${}^+A={}^+\varepsilon A, \qquad {}^-A={}^-\varepsilon A, \qquad {}^iA={}^i\varepsilon A, \qquad 0\leqq i\leqq p-2.$$

Then we obtain the direct decompositions

$$A = {}^{+}A \oplus {}^{-}A = {}^{0}A \oplus {}^{1}A \oplus \cdots \oplus {}^{p-2}A .$$

1.2. Let

$$\mathfrak{R}_n = \boldsymbol{Z}_p[G_n], \qquad \mathfrak{S}_n = \boldsymbol{Q}_p[G_n], \qquad n \geqq 0 .$$

By means of the natural homomorphism $G \to G_n$, both $\mathfrak{R}_n$ and $\mathfrak{S}_n$ become G-modules and hence, also $\boldsymbol{Z}_p[G]$-modules. Let $\mathfrak{R}_n^0$ denote the submodule of all $\sum_\rho a_\rho \rho$ ($\rho \in G_n$, $a_\rho \in \boldsymbol{Z}_p$) in $\mathfrak{R}_n$ such that $\sum_\rho a_\rho = 0$, and let

$$\mathfrak{A}_n = \mathfrak{B}_n + \mathfrak{R}_n^0, \qquad \mathfrak{B}_n = \mathfrak{R}_n \xi_n ,$$

where

$$\xi_n = q_n^{-1} \sum_a \left(a - \frac{q_n - p}{2}\right)\sigma(a)_n , \qquad 0 \leqq a < q_n, (a, p) = 1 .$$

Clearly $\mathfrak{A}_n$ and $\mathfrak{B}_n$ are $\boldsymbol{Z}_p[G]$-submodules of $\mathfrak{S}_n$.

Let $m \geqq n \geqq 0$. Then the natural homomorphism $G_m \to G_n$ defines a $\boldsymbol{Z}_p[G]$-homomorphism

$$t_{n,m} : \mathfrak{S}_m \to \mathfrak{S}_n$$

in the obvious manner. There also exists an injective $\boldsymbol{Z}_p[G]$-homomorphism

$$t'_{m,n} : \mathfrak{S}_n \to \mathfrak{S}_m$$

such that

$$t'_{m,n} \circ t_{n,m}(\alpha) = \nu_{n,m}\alpha , \qquad \alpha \in \mathfrak{S}_m ,$$

where

$$\nu_{n,m} = \sum_{i=0}^{p^{m-n-1}} \sigma(1+p)^{ip^n} .$$

Since $t_{n,m}(\sigma(a)_m) = \sigma(a)_n$, we see easily that $t_{n,m}(\mathfrak{R}_m) = \mathfrak{R}_n$, $t_{n,m}(\mathfrak{R}_m^0) = \mathfrak{R}_n^0$, and

$$t_{n,m}(\xi_m) = \xi_n .$$

Hence

$$t_{n,m}(\mathfrak{A}_m) = \mathfrak{A}_n, \qquad t_{n,m}(\mathfrak{B}_m) = \mathfrak{B}_n .$$

Let $\mathfrak{A}$ and $\mathfrak{B}$ denote the inverse limits of $\mathfrak{A}_n$ and $\mathfrak{B}_n$, $n \geqq 0$, respectively, relative to the maps $t_{n,m}$, $m \geqq n$:

$$\mathfrak{A} = \lim \mathfrak{A}_n, \qquad \mathfrak{B} = \lim \mathfrak{B}_n .$$

$\mathfrak{A}_n$ is a compact submodule of $\mathfrak{S}_n$ in the natural topology of $\mathfrak{S}_n$ defined by the p-adic topology of $\boldsymbol{Q}_p$. Hence $\mathfrak{A}$ is a compact $\boldsymbol{Z}_p[G]$-module, and $\mathfrak{B}$ is a closed submodule of $\mathfrak{A}$. Since $\mathfrak{B}_n$, $n \geqq 0$, is compact, the compact $\boldsymbol{Z}_p[G]$-module $\mathfrak{A}/\mathfrak{B}$ is the inverse limit of $\mathfrak{A}_n/\mathfrak{B}_n$, $n \geqq 0$:

$$\mathfrak{A}/\mathfrak{B} = \lim \mathfrak{A}_n/\mathfrak{B}_n .$$

Hence

$${}^{\pm}(\mathfrak{A}/\mathfrak{B}) = \lim {}^{\pm}\mathfrak{A}_n/{}^{\pm}\mathfrak{B}_n, \quad {}^{i}(\mathfrak{A}/\mathfrak{B}) = \lim {}^{i}\mathfrak{A}_n/{}^{i}\mathfrak{B}_n , \qquad 0 \leqq i \leqq p-2 ,$$

where ${}^{\pm}(\mathfrak{A}/\mathfrak{B})$ etc. denote the components of the decompositions of respective modules defined in 1.1.

Let

$$ {}^{\pm}\xi_n = {}^{\pm}\varepsilon\xi_n, \qquad {}^{i}\xi_n = {}^{i}\varepsilon\xi_n, \qquad 0 \leqq i \leqq p-2. $$

Then

$$ {}^{+}\xi_n = (2p^n)^{-1} \sum_{\rho} \rho, \qquad \rho \in G_n, $$

(1)

$$ {}^{-}\xi_n = (2q_n)^{-1} \sum_{a} (2a - q_n)\sigma(a)_n, \qquad 0 \leqq a < q_n, (a, p) = 1, $$

and

(2) $$ \kappa(\sigma)\sigma^{-}\xi_n \equiv {}^{-}\xi_n \bmod \mathfrak{R}_n^0, \qquad \sigma \in G. $$

PROPOSITION 1.

$$ {}^{0}\mathfrak{A}_n = {}^{0}\mathfrak{B}_n \oplus {}^{0}\mathfrak{R}_n^0, \qquad {}^{0}\mathfrak{B}_n = \boldsymbol{Z}_p{}^{+}\xi_n, $$

$$ {}^{i}\mathfrak{A}_n = {}^{i}\mathfrak{R}_n, \qquad {}^{i}\mathfrak{B}_n = 0, \qquad i \text{ even}, \ i \neq 0, $$

$$ {}^{i}\mathfrak{A}_n = {}^{i}\mathfrak{R}_n, \qquad {}^{i}\mathfrak{B}_n = \mathfrak{R}_n{}^{i}\xi_n = {}^{i}\mathfrak{R}_n{}^{i}\xi_n, \qquad i \text{ odd}, \ i \neq p-2, $$

$$ {}^{p-2}\mathfrak{A}_n = {}^{p-2}\mathfrak{B}_n. $$

PROOF. It is clear that ${}^{i}\mathfrak{A}_n = {}^{i}\mathfrak{B}_n + {}^{i}\mathfrak{R}_n^0$ and ${}^{i}\mathfrak{B}_n = \mathfrak{R}_n{}^{i}\xi_n = {}^{i}\mathfrak{R}_n{}^{i}\xi_n$ for every i. Let i be even. It follows from (1) that ${}^{i}\xi_n = {}^{i}\varepsilon{}^{+}\xi_n = {}^{+}\xi_n$ or ${}^{i}\xi_n = 0$ according as $i = 0$ or $i \neq 0$. Since ${}^{0}\mathfrak{B}_n = \mathfrak{R}_n{}^{+}\xi_n = \boldsymbol{Z}_p{}^{+}\xi_n$ and $\boldsymbol{Z}_p{}^{+}\xi_n \cap {}^{0}\mathfrak{R}_n^0 = 0$, we obtain ${}^{0}\mathfrak{A}_n = {}^{0}\mathfrak{B}_n \oplus {}^{0}\mathfrak{R}_n^0$. We also see from the above that ${}^{i}\mathfrak{B}_n = \mathfrak{R}_n{}^{i}\xi_n = 0$ and ${}^{i}\mathfrak{A}_n = {}^{i}\mathfrak{R}_n^0 = {}^{i}\mathfrak{R}_n$ for $i \neq 0$.

Next, let i be odd and $i \neq p-2$. It then follows from (2) that ${}^{i}\xi_n = {}^{i}\varepsilon{}^{-}\xi_n$ is contained in ${}^{i}\mathfrak{R}_n^0 = {}^{i}\varepsilon\mathfrak{R}_n^0$. Hence ${}^{i}\mathfrak{A}_n = \mathfrak{R}_n{}^{i}\xi_n + {}^{i}\mathfrak{R}_n^0 = {}^{i}\mathfrak{R}_n^0 = {}^{i}\mathfrak{R}_n$.

To prove the last equality, we consider cohomology groups of Γ/Γ_n. It follows from (2) that

$$ \kappa(\sigma)\sigma^{p-2}\xi_n \equiv {}^{p-2}\xi_n \quad \bmod {}^{p-2}\mathfrak{R}_n^0 = {}^{p-2}\mathfrak{R}_n, \qquad \sigma \in G, $$

and that ${}^{p-2}\mathfrak{A}_n / {}^{p-2}\mathfrak{R}_n$ is a cyclic group of order q_n generated by the coset of ${}^{p-2}\xi_n$. The above congruence then shows that $H^k(\Gamma/\Gamma_n, {}^{p-2}\mathfrak{A}_n/{}^{p-2}\mathfrak{R}_n) = 0$ for every k. Since ${}^{p-2}\mathfrak{R}_n \cong \boldsymbol{Z}_p[\Gamma/\Gamma_n]$ as (Γ/Γ_n)-modules, we also have $H^k(\Gamma/\Gamma_n, {}^{p-2}\mathfrak{R}_n) = 0$. Hence $H^k(\Gamma/\Gamma_n, {}^{p-2}\mathfrak{A}_n) = 0$. However, as ${}^{p-2}\mathfrak{A}_n$ is a free $\boldsymbol{Z}_p$-module of rank p^n, ${}^{p-2}\mathfrak{A}_n$ is isomorphic to $p({}^{p-2}\mathfrak{A}_n)$, and $H^k(\Gamma/\Gamma_n, p({}^{p-2}\mathfrak{A}_n)) = 0$. Therefore, $H^k(\Gamma/\Gamma_n, {}^{p-2}\mathfrak{A}_n/p({}^{p-2}\mathfrak{A}_n)) = 0$ for every k, and we see that ${}^{p-2}\mathfrak{A}_n/p({}^{p-2}\mathfrak{A}_n) \cong (\boldsymbol{Z}/p\boldsymbol{Z})[\Gamma/\Gamma_n]$ as (Γ/Γ_n)-modules. On the other hand, since ${}^{p-2}\xi_n$ generates ${}^{p-2}\mathfrak{A}_n/{}^{p-2}\mathfrak{R}_n$, it is not contained in the submoduie $p({}^{p-2}\mathfrak{A}_n) + {}^{p-2}\mathfrak{R}_n$ of index p in ${}^{p-2}\mathfrak{A}_n$. Hence the cosets of $\rho^{p-2}\xi_n$, $\rho \in \Gamma/\Gamma_n$, form a basis of the abelian group ${}^{p-2}\mathfrak{A}_n/p({}^{p-2}\mathfrak{A}_n)$. It follows that ${}^{p-2}\mathfrak{A}_n = {}^{p-2}\mathfrak{B}_n + p({}^{p-2}\mathfrak{A}_n)$, and hence that ${}^{p-2}\mathfrak{A}_n = {}^{p-2}\mathfrak{B}_n$.

It also follows from the above proof that

$$\mathfrak{A}_n \cap \mathfrak{R}_n = p^n({}^0\mathfrak{B}_n) \oplus \mathfrak{R}_n^0 ,$$

$$\mathfrak{A}_n/(\mathfrak{A}_n \cap \mathfrak{R}_n) = ({}^0\mathfrak{B}_n/p^n({}^0\mathfrak{B}_n)) \oplus ({}^{p-2}\mathfrak{A}_n/{}^{p-2}\mathfrak{R}_n) .$$

Since $[{}^{p-2}\mathfrak{A}_n : {}^{p-2}\mathfrak{R}_n] = q_n$, we obtain

$$(3) \qquad \begin{aligned} [\mathfrak{R}_n : \mathfrak{A}_n \cap \mathfrak{R}_n] &= p^n , \\ [\mathfrak{A}_n : \mathfrak{A}_n \cap \mathfrak{R}_n] &= p^{2n+1} . \end{aligned}$$

Now, let $\mathfrak{R}$ be the inverse limit of $\mathfrak{R}_n$, $n \geqq 0$, relative to $t_{n,m} : \mathfrak{R}_m \to \mathfrak{R}_n$, $m \geqq n$, and let $\mathfrak{R}^0$ be defined similarly. $\mathfrak{R}$ is a compact $\boldsymbol{Z}_p[G]$-module, and $\mathfrak{R}^0$ is a closed submodule of $\mathfrak{R}$. Since $t_{n,m}({}^i\xi_m) = {}^i\xi_n$, $m \geqq n$, the elements ${}^i\xi_n$, $n \geqq 0$, determine an element ${}^i\xi$ in ${}^i\mathfrak{A}$. It then follows immediately from the above proposition that

$$\begin{aligned} &{}^0(\mathfrak{A}/\mathfrak{B}) = {}^0\mathfrak{R}^0 , \\ &{}^i(\mathfrak{A}/\mathfrak{B}) = {}^i\mathfrak{R} , && i \text{ even}, \ i \neq 0 , \\ &{}^i(\mathfrak{A}/\mathfrak{B}) = {}^i\mathfrak{R}/{}^i\mathfrak{R}\,{}^i\xi , && i \text{ odd}, \ i \neq p-2 , \\ &{}^{p-2}(\mathfrak{A}/\mathfrak{B}) = 0 . \end{aligned}$$

In general, for any compact $\boldsymbol{Z}_p[\Gamma]$-module A, we put

$$A^{(n)} = A/\omega_n A , \qquad n \geqq 0 ,$$

where

$$\omega_n = 1 - \sigma(1+p)^{p^n} . \qquad n \geqq 0 .$$

PROPOSITION 2. *The natural homomorphisms* ${}^-(\mathfrak{A}/\mathfrak{B}) \to {}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n$ *and* ${}^i(\mathfrak{A}/\mathfrak{B}) \to {}^i\mathfrak{A}_n/{}^i\mathfrak{B}_n$, $i \neq 0$, *induce isomorphisms*

$$\begin{aligned} &{}^-(\mathfrak{A}/\mathfrak{B})^{(n)} \cong {}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n , \\ &{}^i(\mathfrak{A}/\mathfrak{B})^{(n)} \cong {}^i\mathfrak{A}_n/{}^i\mathfrak{B}_n , && i \neq 0, n \geqq 0 . \end{aligned}$$

PROOF. Let $i \neq 0$ and $m \geqq n \geqq 0$. We first notice that $H^k(\Gamma_n/\Gamma_m, {}^i\mathfrak{A}_m) = 0$ for every k. For $i = p-2$, this can be shown similarly as in the proof of the previous proposition. For $i \neq p-2$, it follows from ${}^i\mathfrak{A}_m = {}^i\mathfrak{R}_m$.

Since $t'_{m,n} \circ t_{n,m}(\alpha) = \nu_{n,m}\alpha$, $\alpha \in {}^i\mathfrak{A}_m$, and since $t'_{m,n}$ is injective, we see from $H^1(\Gamma_n/\Gamma_m, {}^i\mathfrak{A}_m) = 0$ that the kernel of $t_{n,m} : {}^i\mathfrak{A}_m \to {}^i\mathfrak{A}_n$ is $\omega_n {}^i\mathfrak{A}_m$. Therefore, the kernel of ${}^i\mathfrak{A}_m/{}^i\mathfrak{B}_m \to {}^i\mathfrak{A}_n/{}^i\mathfrak{B}_n$ is $\omega_n({}^i\mathfrak{A}_m/{}^i\mathfrak{B}_m)$. Since this holds for every $m \geqq n$, the kernel of ${}^i(\mathfrak{A}/\mathfrak{B}) \to {}^i\mathfrak{A}_n/{}^i\mathfrak{B}_n$ is $\omega_n {}^i(\mathfrak{A}/\mathfrak{B})$. As ${}^i(\mathfrak{A}/\mathfrak{B}) \to {}^i\mathfrak{A}_n/{}^i\mathfrak{B}_n$ is surjective, we obtain an isomorphism ${}^i(\mathfrak{A}/\mathfrak{B})^{(n)} \to {}^i\mathfrak{A}_n/{}^i\mathfrak{B}_n$. The isomorphism ${}^-(\mathfrak{A}/\mathfrak{B})^{(n)} \cong {}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n$ is a consequence of what has just been proved.

1.3. Let Λ denote the local ring of formal power series in an indeterminate T with coefficients in $\boldsymbol{Z}_p$:

$$\Lambda = \boldsymbol{Z}_p[[T]] .$$

Since ${}^{i}\mathfrak{R}_n = {}^{i}\varepsilon\mathfrak{R}_n$ is isomorphic to $\boldsymbol{Z}_p[\Gamma/\Gamma_n]$ as algebras over $\boldsymbol{Z}_p$, there exists a ring isomorphism over $\boldsymbol{Z}_p$:

$$ {}^{i}\mathfrak{R}_n \to \Lambda/(1-(1+T)^{p^n}), $$

which maps ${}^{i}\varepsilon\sigma(1+p)_n$ to the coset of $1+T \bmod (1-(1+T)^{p^n})$; here $(1-(1+T)^{p^n})$ denotes the principal ideal of Λ generated by $1-(1+T)^{p^n}$. These isomorphisms, for $n \geqq 0$, then define a topological ring isomorphism over $\boldsymbol{Z}_p$:

$$ {}^{i}\mathfrak{R} \to \Lambda, $$

mapping ${}^{i}\varepsilon\sigma(1+p)$ to $1+T$. We see easily that ${}^{i}\mathfrak{R}_n^0$ corresponds to $(T)/(1-(1+T)^{p^n})$ so that ${}^{i}\mathfrak{R}^0 \to (T)$ under the above isomorphism. For odd $i \neq p-2$, let

$$ {}^{i}\xi \to {}^{i}g $$

under the same isomorphism. We shall next describe the power series ${}^{i}g$.

For any a in $\boldsymbol{Q}_p$, there exist a rational integer b and a power of p, p^m $(m \geqq 0)$, such that $p^m a \equiv b \bmod p^m$, $0 \leqq b < p^m$. The rational number b/p^m is then uniquely determined by a, and hence will be denoted by $\langle a \rangle$. If a is a rational number with its denominator a power of p, then $\langle a \rangle$ is nothing but the fractional part of a: $\langle a \rangle = a - [a]$. With this notation, we may write ${}^{-}\xi_n$ in the form

$$ {}^{-}\xi_n = {}^{-}\varepsilon\Big(\sum_a \Big\langle \frac{a}{q_n} \Big\rangle \sigma(a)_n\Big), $$

where a ranges over any system of representatives of $\boldsymbol{U}/(1+q_n\boldsymbol{Z}_p)$. Since

$$ v(1+p)^e, \qquad 0 \leqq e < p^n, v \in \boldsymbol{V}, $$

form such a system of representatives, we obtain

$$ \begin{aligned} {}^{i}\xi_n = {}^{i}\varepsilon{}^{-}\xi_n &= {}^{i}\varepsilon\Big(\sum_v \sum \Big\langle \frac{v(1+p)^e}{q_n} \Big\rangle \sigma(v)_n \sigma(1+p)_n^e\Big) \\ &= {}^{i}\varepsilon\Big(\sum_v \sum \Big\langle \frac{v(1+p)^e}{q_n} \Big\rangle v^i \sigma(1+p)_n^e\Big), \end{aligned} $$

for any odd $i \neq p-2$. Hence we see that

$$ {}^{i}g(T) = \lim_{n\to\infty} {}^{i}g_n(T), $$

where ${}^{i}g_n(T)$ denotes the polynomial of degree at most p^n defined by

$$ {}^{i}g_n(T) = \sum_{e=0}^{p^n-1} \sum_v \Big\langle \frac{v(1+p)^e}{q_n} \Big\rangle v^i (1+T)^e. $$

We notice that

$$ {}^{i}g(T) \equiv {}^{i}g_m(T) \equiv {}^{i}g_n(T) \mod (1-(1+T)^{p^n}), \qquad m \geqq n. $$

Hence

$$ {}^{i}g(0) = {}^{i}g_0(0) = \frac{1}{p} \sum_{a=1}^{p-1} a v(a)^i, $$

where $v(a)$ denotes the element of V such that $v(a)\equiv a \bmod p$.

Now the following proposition is an immediate consequence of what is stated in the above:

PROPOSITION 3. *Let $\Lambda=\boldsymbol{Z}_p[[T]]$ be made into a $\boldsymbol{Z}_p[\Gamma]$-module so that*

$$\sigma(1+p)x=(1+T)x$$

for any x in Λ. Then, as $\boldsymbol{Z}_p[\Gamma]$-modules,

$$\begin{aligned}
&{}^0(\mathfrak{A}/\mathfrak{B})\cong(T)=T\Lambda\ (\cong\Lambda),\\
&{}^i(\mathfrak{A}/\mathfrak{B})\cong\Lambda, && i \text{ even},\ i\neq 0,\\
&{}^i(\mathfrak{A}/\mathfrak{B})\cong\Lambda/({}^ig), && i \text{ odd},\ i\neq p-2,\\
&{}^{p-2}(\mathfrak{A}/\mathfrak{B})=0,
\end{aligned}$$

where $({}^ig)$ denotes the principal ideal of Λ generated by the ${}^ig$ defined in the above.

Let χ be any character of $\boldsymbol{U}/(1+q_n\boldsymbol{Z}_p)$ with values in Ω. Then there exists an integer i such that $\chi(v)=v^i$ for every v in $\boldsymbol{V}$. With i fixed, let

$${}^iD_n=\prod_{\chi}\Big(\frac{1}{q_n}\sum_a a\chi(a)\Big),$$

where $0\leqq a<q_n,(a,p)=1$, and where χ ranges over all characters of $\boldsymbol{U}/(1+q_n\boldsymbol{Z}_p)$ satisfying $\chi(v)=v^i, v\in\boldsymbol{V}$. Then the classical formula for the first factor ${}^-h_n$ of the class number of F_n states that

$$\text{(I)}\qquad {}^-h_n=2q_n\prod_i\Big(-\frac{1}{2}{}^iD_n\Big),\qquad 0\leqq i\leqq p-2,(i,2)=1^{2)}.$$

Hence ${}^iD_n\neq 0$ for every odd index i $(0\leqq i\leqq p-2)$. Furthermore, it is easy to see that ${}^iD_n$ is a p-adic integer for $i\neq p-2$ and $q_n{}^{p-2}D_n$ is a p-adic unit[3].

PROPOSITION 4. *The compact Γ-module ${}^-(\mathfrak{A}/\mathfrak{B})$ is strictly Γ-finite[4], and the order of ${}^-(\mathfrak{A}/\mathfrak{B})^{(n)}={}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n$ is equal to the exact power of p dividing the first factor ${}^-h_n$ of the class number of F_n $(n\geqq 0)$. For any odd i, the Γ-module ${}^i(\mathfrak{A}/\mathfrak{B})$ is also strictly Γ-finite, and if $i\neq p-2$, the order of ${}^i(\mathfrak{A}/\mathfrak{B})^{(n)}={}^i\mathfrak{A}_n/{}^i\mathfrak{B}_n$ is equal to the exact power of p dividing the p-adic integer ${}^iD_n\neq 0$.*

PROOF. We may write ${}^iD_n$ in the form:

$${}^iD_n=\prod_{\zeta}\Big(\sum_{e=0}^{p^n-1}\sum_v\Big\langle\frac{v(1+p)^e}{q_n}\Big\rangle v^i\zeta^e\Big),$$

where ζ ranges over all p^n-th roots of unity in Ω. Hence we see that ${}^iD_n$ is equal to the determinant of the circulant matrix whose first row is

2) See [5], § 5.

3) See [10], § 2.

4) For the theory of Γ-finite modules which will be used throughout the paper, see [8] and [11].

$\left(\cdots, \sum_v \left\langle \frac{v(1+p)^e}{q_n} \right\rangle v^i, \cdots\right)$, $e=0,1,\cdots,p^n-1$. On the other hand, it follows from Proposition 3 that for odd $i \neq p-2$, we have

$$\begin{aligned} {}^i(\mathfrak{A}/\mathfrak{B})^{(n)} &\cong \Lambda/({}^ig, 1-(1+T)^{p^n}) \\ &= \Lambda^{(n)}/({}^ig_n), \qquad n \geqq 0, \end{aligned}$$

where

$$\Lambda^{(n)} = \Lambda/\omega_n\Lambda = \sum_{e=0}^{p^n-1} \boldsymbol{Z}_p(1+T)^e.$$

Since $(1+T)^{p^n}=1$ on $\Lambda^{(n)}$, we see from the above that ${}^i(\mathfrak{A}/\mathfrak{B})^{(n)}$ is finite, and its order is equal to the exact power of p dividing ${}^iD_n \neq 0$. On the other hand, we know that $q_n{}^{p-2}D_n$ is a p-adic unit, that ${}^-(\mathfrak{A}/\mathfrak{B})^{(n)}$ is the direct sum of ${}^i(\mathfrak{A}/\mathfrak{B})^{(n)}$ with odd i, and that ${}^{p-2}(\mathfrak{A}/\mathfrak{B})^{(n)} = {}^{p-2}\mathfrak{A}_n/{}^{p-2}\mathfrak{B}_n = 0$. Hence it follows from (I) that the order of ${}^-(\mathfrak{A}/\mathfrak{B})^{(n)}$ is equal to the exact power of p dividing ${}^-h_n$.

For odd $i \neq p-2$, let $p^{e(n;i)}$ denote the order of ${}^i(\mathfrak{A}/\mathfrak{B})^{(n)}$. Using ${}^i(\mathfrak{A}/\mathfrak{B}) \cong \Lambda/({}^ig)$, we may express the characteristic function $e(n;i)$ of the Γ-module ${}^i(\mathfrak{A}/\mathfrak{B})$ as follows[5]: By Weierstrass' preparation theorem, there exist an integer $e_i \geqq 0$, a unit ${}^iu(T)$ in $\Lambda = \boldsymbol{Z}_p[[T]]$, and a polynomial ${}^im(T)$ of the form:

$${}^im(T) = {}^ia_0 + \cdots + {}^ia_{d_i-1}T^{d_i-1} + T^{d_i}, \qquad {}^ia_k \in p\boldsymbol{Z}_p.$$

such that

$${}^ig(T) = p^{e_i}{}^iu(T){}^im(T).$$

The integers $d_i \geqq 0$ and $e_i \geqq 0$ then give the *invariants* of ${}^i(\mathfrak{A}/\mathfrak{B})$; namely, for all sufficiently large n, we have

$$e(n;i) = d_in + e_ip^n + r_i,$$

with an integer r_i independent of n. It follows in particular that the invariant e_i is positive if and only if ${}^ig(T)$ is divisible by p in $\Lambda = \boldsymbol{Z}_p[[T]]$, namely, if and only if for every $n \geqq 0$,

$$\sum_v \left\langle \frac{v(1+p)^e}{q_n} \right\rangle v^i \equiv 0 \mod p, \qquad 0 \leqq e < p^n,$$

or equivalently

$$\sum_v \left\langle \frac{av}{q_n} \right\rangle v^i \equiv 0 \mod p,$$

for any a in $\boldsymbol{U}$[6].

1.4. The algebra $\mathfrak{S}_n = \boldsymbol{Q}_p[G_n]$ has an involution $\alpha \to \alpha^*$ such that $\rho^* = \rho^{-1}$ for any ρ in G_n. We see easily that $\mathfrak{R}_n^* = \mathfrak{R}_n$, $(\mathfrak{R}_n^0)^* = \mathfrak{R}_n^0$, and

5) See [11]. The ring Λ was first introduced by Serre into the theory of Γ-finite modules.

6) See [7].

$$\mathfrak{A}_n^* = \mathfrak{B}_n^* + \mathfrak{R}_n^0, \quad \mathfrak{B}_n^* = \mathfrak{R}_n \xi_n^*,$$

where

$$\xi_n^* = q_n^{-1} \sum_a \left(a - \frac{q_n - p}{2}\right) \sigma(a)_n^{-1}, \qquad 0 \leqq a < q_n, (a, p) = 1.$$

The homomorphism $t_{n,m}: \mathfrak{S}_m \to \mathfrak{S}_n$, $m \geqq n$, commutes with the involutions on $\mathfrak{S}_m$ and $\mathfrak{S}_n$, and maps $\mathfrak{A}_m^*$ onto $\mathfrak{A}_n^*$. Hence if we denote by $\mathfrak{A}^*$ the inverse limit of $\mathfrak{A}_n^*$, $n \geqq 0$, relative to $t_{n,m}$, then the maps $\mathfrak{A}_n \to \mathfrak{A}_n^*$, $n \geqq 0$, define a topological $\boldsymbol{Z}_p$-isomorphism

$$\mathfrak{A} \to \mathfrak{A}^*$$

such that

$$(\sigma\alpha)^* = \sigma^{-1}\alpha^*, \qquad \sigma \in G.$$

The inverse limit of $\mathfrak{B}_n^*$, $n \geqq 0$, gives a closed submodule $\mathfrak{B}^*$ of $\mathfrak{A}^*$, and the above isomorphism induces similar isomorphisms $\mathfrak{B} \to \mathfrak{B}^*$ and $\mathfrak{A}/\mathfrak{B} \to \mathfrak{A}^*/\mathfrak{B}^*$. Since

$$({}^{\pm}\varepsilon)^* = {}^{\pm}\varepsilon, \quad ({}^{j}\varepsilon)^* = {}^{i}\varepsilon, \qquad 0 \leqq i \leqq p-2, i+j = p-1,$$

we have

$${}^{\pm}(\mathfrak{A}^*) = ({}^{\pm}\mathfrak{A})^*, \qquad {}^{i}(\mathfrak{A}^*) = ({}^{j}\mathfrak{A})^*, \qquad i+j = p-1.$$

These modules will be denoted simply by ${}^{\pm}\mathfrak{A}^*$ and ${}^{i}\mathfrak{A}^*$ respectively, and similarly for the submodules of $\mathfrak{B}^*$ and $\mathfrak{A}^*/\mathfrak{B}^*$.

Let

$$\mathrm{Res}: \boldsymbol{Q}_p \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$$

be the natural homomorphism of the additive group $\boldsymbol{Q}_p$ so that $\mathrm{Res}(a)$, $a \in \boldsymbol{Q}_p$, denotes the residue class of a mod $\boldsymbol{Z}_p$. For each $n \geqq 0$, we define a non-degenerate symmetric pairing $\mathfrak{S}_n \times \mathfrak{S}_n \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ by

$$(\alpha, \beta)_n = \mathrm{Res}\left(\sum_\rho a_\rho b_\rho\right),$$

for any $\alpha = \sum_\rho a_\rho \rho$ and $\beta = \sum_\rho b_\rho \rho$ ($\rho \in G_n$) in $\mathfrak{S}_n$. Then we see easily that

$$(\sigma\alpha, \sigma\beta)_n = (\alpha, \beta)_n, \qquad \alpha, \beta \in \mathfrak{S}_n, \sigma \in G,$$

$$(\alpha\gamma, \beta)_n = (\alpha, \beta\gamma^*)_n, \qquad \alpha, \beta, \gamma \in \mathfrak{S}_n,$$

$$(t_{n,m}(\alpha), \beta)_n = (\alpha, t'_{m,n}(\beta))_m, \qquad \alpha \in \mathfrak{S}_m, \beta \in \mathfrak{S}_n, m \geqq n.$$

PROPOSITION 5. *For each $n \geqq 0$, there exists a non-degenerate pairing $(x, y^*)_n$:*

$$^{-}(\mathfrak{A}_n/\mathfrak{B}_n) \times {}^{-}(\mathfrak{A}_n^*/\mathfrak{B}_n^*) \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$$

such that

$$(\sigma x, \sigma y^*)_n = (x, y^*)_n, \qquad \sigma \in G,$$

$$(t_{n,m}(x), y^*)_n = (x, t'_{m,n}(y^*))_m, \qquad m \geqq n,$$

for x in ${}^{-}(\mathfrak{A}_n/\mathfrak{B}_n)$ and y^* in ${}^{-}(\mathfrak{A}_n^*/\mathfrak{B}_n^*)$ or in ${}^{-}(\mathfrak{A}_m^*/\mathfrak{B}_m^*)$.

PROOF. We first notice that since $t'_{m,n}(\mathfrak{A}_n^*)=t'_{m,n}\circ t_{n,m}(\mathfrak{A}_m^*)=\nu_{n,m}\mathfrak{A}_m^*$ and similarly $t'_{m,n}(\mathfrak{B}_n^*)=\nu_{n,m}\mathfrak{B}_m^*$, $t'_{m,n}$ induces homomorphisms $\mathfrak{A}_n^*/\mathfrak{B}_n^*\to\mathfrak{A}_m^*/\mathfrak{B}_m^*$ and ${}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*\to{}^-\mathfrak{A}_m^*/{}^-\mathfrak{B}_m^*$, $m\geqq n$.

Now the pairing $(\alpha,\beta)_n$ on $\mathfrak{S}_n$ induces a non-degenerate pairing ${}^-\mathfrak{S}_n\times{}^-\mathfrak{S}_n\to\boldsymbol{Q}_p/\boldsymbol{Z}_p$. For any subgroup A of ${}^-\mathfrak{S}_n$, let $A^\perp$ denote the annihilator of A in ${}^-\mathfrak{S}_n$. Since ${}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n$ is finite, it follows from ${}^-\mathfrak{B}_n={}^-\mathfrak{R}_n{}^-\xi_n$ that ${}^-\xi_n$ has an inverse in the algebra ${}^-\mathfrak{S}_n$. Therefore, ${}^-\xi_n^*=({}^-\xi_n)^*$ also has an inverse in ${}^-\mathfrak{S}_n$. As $({}^-\mathfrak{R}_n)^\perp={}^-\mathfrak{R}_n$, it follows from $({}^-\mathfrak{R}_n{}^-\xi_n,\beta)_n=({}^-\mathfrak{R}_n,\beta({}^-\xi_n)^*)_n$ that

$$({}^-\mathfrak{B}_n)^\perp=({}^-\mathfrak{R}_n)^\perp({}^-\xi_n^*)^{-1}={}^-\mathfrak{R}_n({}^-\xi_n^*)^{-1}.$$

Since ${}^-\mathfrak{A}_n={}^-\mathfrak{B}_n+{}^-\mathfrak{R}_n^0={}^-\mathfrak{B}_n+{}^-\mathfrak{R}_n$, we have

$$({}^-\mathfrak{A}_n)^\perp=({}^-\mathfrak{B}_n)^\perp\cap({}^-\mathfrak{R}_n)^\perp={}^-\mathfrak{R}_n({}^-\xi_n^*)^{-1}\cap{}^-\mathfrak{R}_n,$$

and

$$\begin{aligned}({}^-\mathfrak{B}_n)^\perp/({}^-\mathfrak{A}_n)^\perp&={}^-\mathfrak{R}_n({}^-\xi_n^*)^{-1}/({}^-\mathfrak{R}_n({}^-\xi_n^*)^{-1}\cap{}^-\mathfrak{R}_n)\\&\cong{}^-\mathfrak{R}_n/({}^-\mathfrak{R}_n\cap{}^-\mathfrak{R}_n{}^-\xi_n^*)\\&\cong({}^-\mathfrak{R}_n{}^-\xi_n^*+{}^-\mathfrak{R}_n)/{}^-\mathfrak{R}_n{}^-\xi_n^*\\&={}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*.\end{aligned}$$

Clearly the pairing on ${}^-\mathfrak{S}_n$ induces a non-degenerate pairing of ${}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n$ and $({}^-\mathfrak{B}_n)^\perp/({}^-\mathfrak{A}_n)^\perp$ into $\boldsymbol{Q}_p/\boldsymbol{Z}_p$. Using the above isomorphisms, we then obtain a pairing $(x,y^*)_n:({}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n)\times({}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*)\to\boldsymbol{Q}_p/\boldsymbol{Z}_p$.

Let α be an element of ${}^-\mathfrak{A}_n$ representing x in ${}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n$, and let β be an element of ${}^-\mathfrak{R}_n$ representing y^* in ${}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*$, where ${}^-\mathfrak{A}_n^*={}^-\mathfrak{B}_n^*+{}^-\mathfrak{R}_n$. Then, by the definition,

$$(x,y^*)_n=(\alpha,\beta({}^-\xi_n^*)^{-1})_n=(\alpha{}^-\xi_n^{-1},\beta)_n.$$

Hence it is clear that $(\sigma x,\sigma y^*)_n=(x,y^*)_n$ for any σ in G. Next, let x be in ${}^-\mathfrak{A}_m/{}^-\mathfrak{B}_m$, and let α be an element of ${}^-\mathfrak{A}_m$ representing x. Using the fact that $t_{n,m}$ is a ring homomorphism mapping ${}^-\xi_m$ to ${}^-\xi_n$, $m\geqq n$, we have

$$\begin{aligned}(t_{n,m}(x),y^*)_n&=(t_{n,m}(\alpha){}^-\xi_n^{-1},\beta)_n=(t_{n,m}(\alpha{}^-\xi_m^{-1}),\beta)_n\\&=(\alpha{}^-\xi_m^{-1},t'_{m,n}(\beta))_m\\&=(x,t'_{m,n}(y^*))_m.\end{aligned}$$

Hence the proposition is proved.

PROPOSITION 6. *The Γ-modules ${}^-(\mathfrak{A}/\mathfrak{B})$ and ${}^i(\mathfrak{A}/\mathfrak{B})$, with odd i, are regular and self-adjoint*[7].

PROOF. For each $n\geqq 0$, we define a pairing ${}^-(\mathfrak{A}_n/\mathfrak{B}_n)\times{}^-(\mathfrak{A}_n/\mathfrak{B}_n)\to\boldsymbol{Q}_p/\boldsymbol{Z}_p$ by

$$(x,y)_n=(x,y^*)_n,\qquad x,y\in{}^-(\mathfrak{A}_n/\mathfrak{B}_n),$$

where the right-hand side denotes the pairing of ${}^-(\mathfrak{A}_n/\mathfrak{B}_n)$ and ${}^-(\mathfrak{A}_n^*/\mathfrak{B}_n^*)$ given

7) See [8], §5.

in Proposition 5. It is clear that $(x,y)_n$ is non-degenerate and satisfies

$$(\sigma x, y)_n = (x, \sigma y)_n, \qquad \sigma \in G,$$

$$(t_{n,m}(x), y)_n = (x, t'_{m,n}(y))_m, \qquad m \geqq n,$$

for x in $^-(\mathfrak{A}_n/\mathfrak{B}_n)$ and y in $^-(\mathfrak{A}_n/\mathfrak{B}_n)$ or in $^-(\mathfrak{A}_m/\mathfrak{B}_m)$. Since $^-(\mathfrak{A}/\mathfrak{B})^{(n)} = {}^-(\mathfrak{A}_n/\mathfrak{B}_n)$, the existence of $(x,y)_n$ shows that $^-(\mathfrak{A}/\mathfrak{B})$ is self-adjoint. It is easy to see that for each odd i, $(x,y)_n$ induces a pairing ${}^i(\mathfrak{A}_n/\mathfrak{B}_n) \times {}^i(\mathfrak{A}_n/\mathfrak{B}_n) \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ with similar properties. Hence ${}^i(\mathfrak{A}/\mathfrak{B})$ is also self-adjoint. Since every self-adjoint Γ-module is regular, the proposition is completely proved.

We note that we can obtain a similar result for any strictly Γ-finite Γ-module of the type $\Lambda/(g), g \in \Lambda$.

1.5. The group W, which is the union of all $W_n, n \geqq 0$, the group of q_n-th roots of unity in F_n, is isomorphic to the additive group $\boldsymbol{Q}_p/\boldsymbol{Z}_p$. In the following, we shall fix an isomorphism

$$\iota : W \to \boldsymbol{Q}_p/\boldsymbol{Z}_p,$$

and denote by ζ_n the q_n-th root of unity in W_n such that

$$\iota(\zeta_n) = \mathrm{Res}\left(\frac{1}{q_n}\right), \qquad n \geqq 0.$$

Let $\mathfrak{o}_n$ denote the ring of all integers in the local cyclotomic field Φ_n, and let $\mathfrak{p}_n$ be the unique prime ideal of $\mathfrak{o}_n$; $\mathfrak{p}_n$ is the principal ideal generated by

$$\pi_n = 1 - \zeta_n.$$

The additive group of the field Φ_n, which we shall denote again by Φ_n, is a locally compact abelian group in its natural $\mathfrak{p}_n$-adic topology. Let T_n and $T_{n,m}$ $(m \geqq n \geqq 0)$ denote the trace map from Φ_n to $\boldsymbol{Q}_p$ and that from Φ_m to Φ_n respectively, and let

$$\langle \alpha, \beta \rangle_n = \mathrm{Res}\,(T_n(\alpha\beta))$$

for any α, β in Φ_n. Then we have a non-degenerate, symmetric pairing $\Phi_n \times \Phi_n \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ such that

$$\langle \alpha, \beta \rangle_n = \langle \alpha^\sigma, \beta^\sigma \rangle_n, \qquad \alpha, \beta \in \Phi_n, \sigma \in G,$$

$$\langle \alpha, \beta \rangle_m = \langle T_{n,m}(\alpha), \beta \rangle_n. \qquad \alpha \in \Phi_m, \beta \in \Phi_n, m \geqq n.$$

For any closed subgroup A of Φ_n, we denote by $A^\perp$ the annihilator of A in Φ_n relative to this pairing. Then $A^\perp$ is a closed subgroup of Φ_n such that $(A^\perp)^\perp = A$, and A and $\Phi_n/A^\perp$, as well as $A^\perp$ and Φ_n/A, form a pair of mutually dual locally compact abelian groups in the sense of Pontrjagin. If A is in particular a non-zero ideal of Φ_n, then $A^\perp = A^{-1}\mathfrak{d}_n^{-1}$, where

$$\mathfrak{d}_n = q_n \mathfrak{p}_n^{-p^n}$$

is the different of $\Phi_n/\boldsymbol{Q}_p$. In the following, any pairing of locally compact abelian groups with similar properties will be simply called a dual pairing.

Let Φ_n^* denote the multiplicative group of Φ_n; Φ_n^* is also a locally compact group in the $\mathfrak{p}_n$-adic topology. Let U_n denote the subgroup of all local units in Φ_n^*, and let

$$U_{n,0}=1+\mathfrak{p}_n .$$

Then U_n is an open, compact subgroup of Φ_n^*, and

$$\Phi_n^*=\Pi_n\times U_n , \qquad U_n=U_{n,0}\times \boldsymbol{V} ,$$

where Π_n denotes the cyclic subgroup of Φ_n^* generated by π_n.

Let $\mathfrak{L}_n$ be the set of all elements of the form $\log\alpha$ with α in $U_{n,0}$:

$$\mathfrak{L}_n=\log U_{n,0} .$$

$\mathfrak{L}_n$ is an open, compact $\boldsymbol{Z}_p$-submodule of Φ_n, invariant under G. Let

$$\mathfrak{X}_n=\mathfrak{L}_n^{\perp} ;$$

$\mathfrak{X}_n$ is the set of all α in Φ_n such that $T_n(\alpha\log\beta)$ is contained in $\boldsymbol{Z}_p$ for any β in $U_{n,0}$. By the duality, $\mathfrak{X}_n$ is also an open, compact $\boldsymbol{Z}_p$-submodule of Φ_n, invariant under G.

Let

$$\theta_n=q_n^{-1}\sum_{s=0}^{n}\zeta_s^{-1}=q_n^{-1}\sum_{s=0}^{n}\zeta_n^{-p^s} , \qquad n\geqq 0 .$$

PROPOSITION 7. *The $(p-1)p^n$ elements θ_n^{ρ}, $\rho\in G_n$, form a normal basis of $\Phi_n/\boldsymbol{Q}_p$ (as well as that of $F_n/\boldsymbol{Q}$), and they generate over $\boldsymbol{Z}_p$ a submodule $\mathfrak{M}_n$ of index $p^{p^{n-1}}$ in $q_n^{-1}\mathfrak{o}_n$:*

$$[q_n^{-1}\mathfrak{o}_n : \mathfrak{M}_n]=p^{p^{n-1}} .$$

PROOF. We use induction on n. Since $\theta_0=p^{-1}\zeta_0^{-1}$, the lemma is obvious for $n=0$. Let $n>0$. It follows from the induction assumption that $q_{n-1}\mathfrak{M}_{n-1}$ is a free $\boldsymbol{Z}_p$-module of rank $(p-1)p^{n-1}$, with index $p^{p^{n-1}-1}$ in $\mathfrak{o}_{n-1}$. On the other hand, it is easy to see that $\mathfrak{o}_n=\mathfrak{o}_{n-1}+q_n\mathfrak{M}_n$ and that $q_n\mathfrak{M}_{n-1}$ is contained in $\mathfrak{o}_{n-1}\cap q_n\mathfrak{M}_n$. Hence we obtain from $\mathfrak{o}_n/q_n\mathfrak{M}_n=\mathfrak{o}_{n-1}/(\mathfrak{o}_{n-1}\cap q_n\mathfrak{M}_n)$ that

$$\begin{aligned}[\mathfrak{o}_n : q_n\mathfrak{M}_n] &\leqq [\mathfrak{o}_{n-1} : q_n\mathfrak{M}_{n-1}]\\ &=[\mathfrak{o}_{n-1} : q_{n-1}\mathfrak{M}_{n-1}][q_{n-1}\mathfrak{M}_{n-1} : q_n\mathfrak{M}_{n-1}]\\ &=p^{p^{n-1}-1}p^{(p-1)p^{n-1}}\\ &=p^{p^n-1} .\end{aligned}$$

It follows that $(p-1)p^n$ elements θ_n^{ρ} are linearly independent over $\boldsymbol{Q}_p$ and form a normal basis of $\Phi_n/\boldsymbol{Q}_p$. Considering the action of the Galois group of Φ_n/Φ_{n-1} on $q_n\mathfrak{M}_n$, we then see that $q_n\mathfrak{M}_{n-1}=\mathfrak{o}_{n-1}\cap q_n\mathfrak{M}_n$. Hence we obtain

from the above that $[\mathfrak{o}_n : q_n\mathfrak{M}_n] = p^{p^{n-1}}$, q.e.d.

LEMMA. *Let*

$$\alpha = \sum_{\rho} c_\rho \theta_n^\rho , \qquad \rho \in G_n ,$$

with c_ρ *in* $\boldsymbol{Z}_p$ *satisfying* $\sum_{\rho} c_\rho = 0$. *Then* α *is contained in* $\mathfrak{X}_n$.

PROOF. Let $\mu(m)$ $(m \geqq 1)$ be the Möbius' function, and let

$$\tau_n^{(a)} = \prod_{\substack{m=1 \\ (m,p)=1}}^{\infty} (1-\pi_n^{am})^{\frac{\mu(m)}{m}} ,$$

for any integer $a \geqq 1$[8]. Then these elements $\tau_n^{(a)}$ generate the group $U_{n,0} = 1+\mathfrak{p}_n$ topologically. Hence an element α in Φ_n belongs to $\mathfrak{X}_n$ if and only if $\langle \alpha, \log \tau_n^{(a)} \rangle_n = 0$ for every $a \geqq 1$.

Since

$$T_n(\zeta_n^j) = \begin{cases} (p-1)p^n , & \text{if} \quad p^{n+1} \mid j , \\ -p^n , & \text{if} \quad p^{n+1} \nmid j , \quad p^n \mid j , \\ 0 , & \text{if} \quad p^n \nmid j , \end{cases}$$

we have

$$\begin{aligned} T_n(\zeta_n^{-ip^s}\pi_n^{ap^e}) &= \sum_{t=0}^{ap^e} (-1)^t \binom{ap^e}{t} T_n(\zeta_n^{t-ip^s}) \\ &= p^{n+1} \sum_{\substack{t \equiv ip^s (p^{n+1}) \\ 0 \leqq t \leqq ap^e}} (-1)^t \binom{ap^e}{t} - p^n \sum_{\substack{t \equiv ip^s (p^n) \\ 0 \leqq t \leqq ap^e}} (-1)^t \binom{ap^e}{t} , \end{aligned}$$

for any i prime to p. Using

$$\log \tau_n^{(a)} = -\sum_{e=0}^{\infty} p^{-e} \pi_n^{ap^e} ,$$

we obtain

$$\begin{aligned} T_n(q_n^{-1}\zeta_n^{-ip^s} \log \tau_n^{(a)}) = -\sum_{e=0}^{\infty} p^{-e} \Big\{ & \sum_{\substack{t \equiv ip^s (p^{n+1}) \\ 0 \leqq t \leqq ap^e}} (-1)^t \binom{ap^e}{t} \\ & - p^{-1} \sum_{\substack{t \equiv ip^s (p^n) \\ 0 \leqq t \leqq ap^e}} (-1)^t \binom{ap^e}{t} \Big\} . \end{aligned} \tag{4}$$

The series

$$\sum_{e=0}^{\infty} p^{-e} \Big\{ \sum_{\substack{t \equiv ip^s (p^m) \\ 0 \leqq t \leqq ap^e}} (-1)^t \binom{ap^e}{t} \Big\} \tag{5}$$

converges for $m = 0$, because $\sum_{0 \leqq t \leqq ap^e} (-1)^t \binom{ap^e}{t} = (1-1)^{ap^e} = 0$. Since the series on the right-hand side of (4) converges, we see by induction on m that the series (5) converges for every $m \geqq 0$. Hence

8) See [2], § 7.

$$T_n(q_n^{-1}\zeta_n^{-ip^s}\log\tau_n^{(a)}) = -\sum_{e=0}^{\infty} p^{-e}\Big\{\sum_{\substack{t\equiv ip^s(p^{n+1})\\ 0\leqq t\leqq ap^e}}(-1)^t\binom{ap^e}{t}\Big\}$$

$$+\sum_{e=0}^{\infty} p^{-(e+1)}\Big\{\sum_{\substack{t\equiv ip^s(p^n)\\ 0\leqq t\leqq ap^e}}(-1)^t\binom{ap^e}{t}\Big\}.$$

Using

$$\binom{ap^e}{t}\equiv\binom{ap^{e+1}}{tp} \mod p^{2e+2}\ ^{9)},$$

we have

$$\sum_{\substack{t\equiv ip^s(p^n)\\ 0\leqq t\leqq ap^e}}(-1)^t\binom{ap^e}{t} = \sum_{\substack{tp\equiv ip^{s+1}(p^{n+1})\\ 0\leqq tp\leqq ap^{e+1}}}(-1)^t\Big[\binom{ap^{e+1}}{tp}+\Big\{\binom{ap^e}{tp}-\binom{ap^{e+1}}{tp}\Big\}\Big]$$

$$= \sum_{\substack{t\equiv ip^{s+1}(p^{n+1})\\ 0\leqq t\leqq ap^{e+1}}}(-1)^t\binom{ap^{e+1}}{t}+r_e,$$

where $r_e\equiv 0 \mod p^{2e+2}$. It follows that

$$T_n(q_n^{-1}\zeta_n^{-ip^s}\log\tau_n^{(a)}) = -\sum_{e=0}^{\infty} p^{-e}\Big\{\sum_{\substack{t\equiv ip^s(p^{n+1})\\ 0\leqq t\leqq ap^e}}(-1)^t\binom{ap^e}{t}\Big\}$$

$$+\sum_{e=0}^{\infty} p^{-(e+1)}\Big\{\sum_{\substack{t\equiv ip^{s+1}(p^{n+1})\\ 0\leqq t\leqq ap^{e+1}}}(-1)^t\binom{ap^{e+1}}{t}\Big\}$$

$$+\sum_{e=0}^{\infty} p^{-(e+1)}r_e$$

$$\equiv -\sum_{e=0}^{\infty} p^{-e}\Big\{\sum_{\substack{t\equiv ip^s(p^{n+1})\\ 0\leqq t\leqq ap^e}}(-1)^t\binom{ap^e}{t}\Big\}$$

$$+\sum_{e=0}^{\infty} p^{-e}\Big\{\sum_{\substack{t\equiv ip^{s+1}(p^{n+1})\\ 0\leqq t\leqq ap^e}}(-1)^t\binom{ap^e}{t}\Big\} \mod \boldsymbol{Z}_p.$$

Taking the sum over $s=0,1,\cdots,n$, we obtain for $\rho=\sigma(i)_n$ that

$$T_n(\theta_n^{\rho}\log\tau_n^{(a)}) \equiv -\sum_{e=0}^{\infty} p^{-e}\Big\{\sum_{\substack{t\equiv i(p^{n+1})\\ 0\leqq t\leqq ap^e}}(-1)^t\binom{ap^e}{t}\Big\}$$

$$+\sum_{e=0}^{\infty} p^{-e}\Big\{\sum_{\substack{t\equiv 0(p^{n+1})\\ 0\leqq t\leqq ap^e}}(-1)^t\binom{ap^e}{t}\Big\} \mod \boldsymbol{Z}_p.$$

However, if $t\equiv i \mod p^{n+1}$, then t is prime to p, and

$$\binom{ap^e}{t} = \frac{ap^e}{t}\binom{ap^e-1}{t-1}\equiv 0 \mod p^e.$$

9) See [2], Hilfssatz 2.

Hence the first sum on the right-hand side of the above is contained in $\boldsymbol{Z}_p$. Therefore,

$$T_n(\theta_n^{\gamma} \log \tau_n^{(a)}) \equiv u_n^{(a)} \mod \boldsymbol{Z}_p,$$

where

$$u_n^{(a)} = \sum_{e=0}^{\infty} p^{-e}\Big\{ \sum_{\substack{t \equiv 0 (p^{n+1}) \\ 0 \leqq t \leqq ap^e}} (-1)^t \binom{ap^e}{t} \Big\}.$$

It then follows that

$$T_n(\alpha \log \tau_n^{(a)}) \equiv (\sum_{\rho} c_\rho) u_n^{(a)} \equiv 0 \mod \boldsymbol{Z}_p.$$

Hence α is contained in $\mathfrak{X}_n$.

1.6. Now, by Proposition 7, there exists a $\boldsymbol{Z}_p[G]$-isomorphism

$$\varphi_n : \mathfrak{S}_n = \mathfrak{Q}_p[G_n] \to \Phi_n \qquad n \geqq 0,$$

such that

$$\varphi_n(\rho) = \theta_n^{\gamma}$$

for any ρ in G_n. Since

$$\sum_{\rho} \theta_n^{\gamma} = T_n(\theta) = -\frac{1}{p}, \qquad \rho \in G_n,$$

we have

$$\varphi_n(-p \sum_{\rho} \rho) = 1, \qquad \rho \in G_n.$$

Let

$$\mu_n = \frac{1}{q_n} \frac{\zeta_n}{\pi_n} \qquad n \geqq 0.$$

Then

$$\begin{aligned}
\sum_{\substack{0 \leqq a < q_n \\ (a,p)=1}} a\theta_n^{\sigma(a)} &= q_n^{-1} \sum_{s=0}^{n} \sum_{a} a\zeta_s^{-a} \\
&= q_n^{-1} \sum_{s=0}^{n} \sum_{\substack{0 \leqq a < q_s \\ (a,p)=1}} \Big(\sum_{k=0}^{p^{n-s-1}} (a + kq_s) \Big) \zeta_s^{-a} \\
&= q_n^{-1} \sum_{s=0}^{n} \sum_{\substack{0 \leqq a < q_s \\ (a,p)=1}} p^{n-s} a \zeta_n^{-p^{n-s}a} \\
&\quad + q_n^{-1} \sum_{s=0}^{n} \frac{(p^{n-s}-1)p^{n-s}}{2} q_s \sum_{\substack{0 \leqq a < q_s \\ (a,p)=1}} \zeta_s^{-a} \\
&= q_n^{-1} \sum_{a=0}^{q_n - 1} a\zeta_n^{-a} - q_n^{-1} \frac{(p^n-1)p^{n+1}}{2} \\
&= \frac{\zeta_n}{\pi_n} - \frac{p^n - 1}{2}.
\end{aligned}$$

Hence

$$\mu_n = q_n^{-1} \sum_a \left(a - \frac{q_n - p}{2}\right) \theta_n^{\sigma(a)}, \qquad 0 \leqq a < q_n, (a, p) = 1,$$

and we have

$$\varphi_n(\xi_n) = \mu_n .$$

Since

$$T_{n,m}(\theta_m) = \theta_n, \qquad m \geqq n \geqq 0,$$

we also see that the following diagram is commutative:

$$\begin{array}{ccc} \mathfrak{S}_m & \xrightarrow{\varphi_m} & \Phi_m \\ \downarrow t_{n,m} & & \downarrow T_{n,m} \\ \mathfrak{S}_n & \xrightarrow{\varphi_n} & \Phi_n \end{array} .$$

THEOREM 1. *The map* $\varphi_n : \mathfrak{S}_n \to \Phi_n$ *defines a* $\boldsymbol{Z}_p[G]$*-isomorphism*

$$\mathfrak{A}_n \to \mathfrak{X}_n, \qquad n \geqq 0 .$$

PROOF. It follows from the lemma in 1.5 that $\varphi_n(\mathfrak{R}_n^0)$ is contained in $\mathfrak{X}_n$. It also follows from Artin-Hasse's explicit formula for Hilbert's norm residue symbol in Φ_n that $\mu_n = \varphi_n(\xi_n)$ is contained in $\mathfrak{X}_n$[10]. Hence $\varphi_n(\mathfrak{A}_n) = \varphi_n(\mathfrak{R}_n \xi_n + \mathfrak{R}_n^0)$ is a submodule of $\mathfrak{X}_n$.

The annihilator of $\mathfrak{p}_n^{p^{n+1}} = \log(1+\mathfrak{p}_n^{p^{n+1}})$ relative to the pairing $\langle \alpha, \beta \rangle_n$ is $\mathfrak{p}_n^{-p^{n-1}} \mathfrak{d}_n^{-1} = q_n^{-1} \mathfrak{p}_n^{-1}$. Hence $\mathfrak{X}_n = (\log(1+\mathfrak{p}_n))^{\perp}$ is contained in $q_n^{-1}\mathfrak{p}_n^{-1}$, and $[q_n^{-1}\mathfrak{p}_n^{-1} : \mathfrak{X}_n] = [\log(1+\mathfrak{p}_n) : \log(1+\mathfrak{p}_n^{p^{n+1}})]$. However, the kernel of the log map: $1+\mathfrak{p}_n \to \log(1+\mathfrak{p}_n)$ is W_n, and $W_n \cap (1+\mathfrak{p}_n^{p^{n+1}}) = 1$. Hence $[\log(1+\mathfrak{p}_n) : \log(1+\mathfrak{p}_n^{p^{n+1}})] = q_n^{-1}[1+\mathfrak{p}_n : 1+\mathfrak{p}_n^{p^{n+1}}] = q_n^{-1} p^{p^n}$, and

$$[q_n^{-1}\mathfrak{p}_n^{-1} : \mathfrak{X}_n] = p^{p^n - n - 1} .$$

On the other hand, it follows from (3) that $[\varphi_n(\mathfrak{R}_n) : \varphi_n(\mathfrak{A}_n \cap \mathfrak{R}_n)] = p^n$, $[\varphi_n(\mathfrak{A}_n) : \varphi_n(\mathfrak{A}_n \cap \mathfrak{R}_n)] = p^{2n+1}$. By Proposition 7, $\mathfrak{M}_n = \varphi_n(\mathfrak{R}_n)$ has index $p^{p^n - 1}$ in $q_n^{-1}\mathfrak{o}_n$. Hence $[q_n^{-1}\mathfrak{p}_n^{-1} : \varphi_n(\mathfrak{R}_n)] = p^{p^n}$, and we obtain from the above that

$$[q_n^{-1}\mathfrak{p}_n^{-1} : \varphi_n(\mathfrak{A}_n)] = p^{p^n - n - 1} .$$

Since $\varphi_n(\mathfrak{A}_n)$ is contained in $\mathfrak{X}_n$, we see that $\varphi_n(\mathfrak{A}_n) = \mathfrak{X}_n$, q. e. d.

Let

$$\mathfrak{Z}_n = \varphi_n(\mathfrak{B}_n), \qquad n \geqq 0 .$$

$\mathfrak{Z}_n$ is the submodule of $\mathfrak{X}_n$ generated over $\boldsymbol{Z}_p$ by the conjugates $\mu_n^{\rho}, \rho \in G_n$, of μ_n. Clearly we have $\boldsymbol{Z}_p[G]$-isomorphisms

$$\mathfrak{B}_n \to \mathfrak{Z}_n, \qquad \mathfrak{A}_n / \mathfrak{B}_n \to \mathfrak{X}_n / \mathfrak{Z}_n .$$

Since the diagram

10) See [2] and 3.1 below.

$$\begin{array}{ccc} \mathfrak{A}_m & \xrightarrow{\varphi_m} & \mathfrak{X}_m \\ \downarrow{\scriptstyle t_{n,m}} & & \downarrow{\scriptstyle T_{n,m}} \\ \mathfrak{A}_n & \xrightarrow{\varphi_n} & \mathfrak{X}_n \end{array}, \qquad m \geqq n \geqq 0,$$

is commutative, we obtain $T_{n,m}(\mathfrak{X}_m)=\mathfrak{X}_n$, and similarly $T_{n,m}(\mathfrak{Z}_m)=\mathfrak{Z}_n$. Hence, let $\mathfrak{X}$ and $\mathfrak{Z}$ denote the inverse limits of $\mathfrak{X}_n$ and $\mathfrak{Z}_n$, $n \geqq 0$, relative to $T_{n,m}: \mathfrak{X}_m \to \mathfrak{X}_n$ and $T_{n,m}: \mathfrak{Z}_m \to \mathfrak{Z}_n$, $m \geqq n$, respectively:

$$\mathfrak{X} = \varprojlim \mathfrak{X}_n, \qquad \mathfrak{Z} = \varprojlim \mathfrak{Z}_n .$$

$\mathfrak{X}$ is a compact $\boldsymbol{Z}_p[G]$-module, and $\mathfrak{Z}$ is a closed submodule of $\mathfrak{X}$. From the above, we obtain immediately the following

THEOREM 2. *The maps* $\varphi_n: \mathfrak{S}_n \to \Phi_n$, $n \geqq 0$, *induce* $\boldsymbol{Z}_p[G]$*-isomorphisms:*

$$\mathfrak{A} \to \mathfrak{X}, \qquad \mathfrak{B} \to \mathfrak{Z}, \qquad \mathfrak{A}/\mathfrak{B} \to \mathfrak{X}/\mathfrak{Z} .$$

We now see the structure of the compact $\boldsymbol{Z}_p[G]$-modules $\mathfrak{X}$, $\mathfrak{Z}$ and $\mathfrak{X}/\mathfrak{Z}$ from the propositions in 1.2-1.4. We note in particular that ${}^-(\mathfrak{X}/\mathfrak{Z})$ is a regular strictly Γ-finite Γ-module such that

$${}^-(\mathfrak{X}/\mathfrak{Z})^{(n)} = {}^-\mathfrak{X}_n/{}^-\mathfrak{Z}_n \cong {}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n , \qquad n \geqq 0 ,$$

and that the order of ${}^-(\mathfrak{X}/\mathfrak{Z})^{(n)}$ is equal to the exact power of p dividing the first factor ${}^-h_n$ of the class number of F_n.

§ 2.

2.1. For $m \geqq n \geqq 0$, let N_n and $N_{n,m}$ denote the norm map from Φ_n to $\boldsymbol{Q}_p$ and that from Φ_m to Φ_n respectively. The restriction of N_n on F_n obviously gives the norm map from F_n to $\boldsymbol{Q}$, and similarly for the restriction of $N_{n,m}$ on F_m.

Let P_n be the set of all α in F_n such that the principal ideal (α) in F_n is a power of the prime ideal (π_n). P_n is a subgroup of the multiplicative group F_n^* of the field F_n, and

$$P_n = \Pi_n \times E_n ,$$

where E_n is the group of all units of F_n.

Let ${}^+F_n$ denote the maximal real subfield of F_n, and let ${}^+F_n^*$ be its multiplicative group. Put

$${}^+P_n = {}^+F_n^* \cap P_n , \qquad {}^+E_n = {}^+F_n^* \cap E_n .$$

Then ${}^+E_n$ is the group of all units of ${}^+F_n$, and

$${}^+P_n = {}^+\Pi_n \times {}^+E_n , \qquad E_n = {}^+E_n \times W_n ,$$

where ${}^+\Pi_n$ denotes the cyclic subgroup of ${}^+F_n^*$ generated by ${}^+\pi_n = \pi_n^{1+\delta}$, $\delta = \sigma(-1)$. It follows immediately from the definition that

$$P_n = F_n^* \cap P_m, \qquad m \geqq n \geqq 0,$$

and similarly for ${}^+P_n$, E_n, and ${}^+E_n$.

For any $m \geqq n$, $N_{n,m}(P_m)$ is a subgroup of P_n. Let

$$P'_n = \bigcap_{m \geqq n} N_{n,m}(P_m).$$

Since $N_{n,m}(\pi_m) = \pi_n$, π_n is contained in P'_n, and

$$P'_n = \Pi_n \times E'_n,$$

with

$$E'_n = P'_n \cap E_n = \bigcap_{m \geqq n} N_{n,m}(E_m).$$

Since $N_{n,m}({}^+\pi_m) = {}^+\pi_n$, $N_{n,m}(\zeta_m) = \zeta_n$, we also have

$${}^+P'_n = {}^+\Pi_n \times {}^+E'_n, \qquad E'_n = {}^+E'_n \times W_n,$$

where

$${}^+P'_n = {}^+F_n^* \cap P'_n = \bigcap_{m \geqq n} N_{n,m}({}^+P_m), \qquad {}^+E'_n = {}^+F_n^* \cap E'_n = \bigcap_{m \geqq n} N_{n,m}({}^+E_m).$$

It follows that

$$P_n/P'_n = {}^+P_n/{}^+P'_n = E_n/E'_n = {}^+E_n/{}^+E'_n, \qquad n \geqq 0.$$

Let Q_n denote the subgroup of F_n^* generated by π_n and its conjugates π_n^ρ, $\rho \in G_n$. Since P'_n is invariant under G, Q_n is contained in P'_n. Let

$$C_n = E_n \cap Q_n = E'_n \cap Q_n.$$

Then

$$Q_n = \Pi_n \times C_n.$$

Since $\pi_n^{1-\delta} = -\zeta_n$, $\pm W_n$ is contained in Q_n. It follows that

$$C_n = {}^+C_n \times W_n, \qquad {}^+Q_n = {}^+\Pi_n \times {}^+C_n,$$

where ${}^+Q_n = Q_n \cap {}^+F_n^*$ and ${}^+C_n = C_n \cap {}^+F_n^*$. Hence

$$P_n/Q_n = {}^+P_n/{}^+Q_n = E_n/C_n = {}^+E_n/{}^+C_n,$$
$$P'_n/Q_n = {}^+P'_n/{}^+Q_n = E'_n/C_n = {}^+E'_n/{}^+C_n, \qquad n \geqq 0.$$

Let r be a fixed primitive root mod p^2, and let

$$\varepsilon_n = \zeta_n^{-\frac{r-1}{2}} \frac{1-\zeta_n^r}{1-\zeta_n} = \frac{\zeta_n^{\frac{r}{2}} - \zeta_n^{-\frac{r}{2}}}{\zeta_n - \zeta_n^{-1}}, \qquad n \geqq 0.$$

ε_n is a so-called circular unit of the cyclotomic field F_n, and we see readily that ${}^+C_n$ is generated by $\pm\varepsilon_n^\rho$, $\rho \in G_n$. Hence the classical formula for the second factor ${}^+h_n$ of the class number of F_n states that

(II) $$ {}^+h_n = [{}^+E_n : {}^+C_n]^{11}.$$

11) See [5], § 11.

It follows in particular that ${}^+E_n/{}^+C_n$ is a finite group.

Let ${}^+G_n$ denote the Galois group of ${}^+F_n/\boldsymbol{Q}$. Since ${}^+P_n/{}^+Q_n$ is finite and since

$$\varepsilon_n^2 = \varepsilon_n^{1+\delta} = \frac{(1-\zeta_n^r)(1-\zeta_n^{-r})}{(1-\zeta_n)(1-\zeta_n^{-1})} = {}^+\pi_n^{\tau-1}, \qquad \sigma = \sigma(r)_n,$$

we see that the subgroup of ${}^+Q_n$ generated by ${}^+\pi_n^\rho, \rho \in {}^+G_n$, is G-isomorphic to $\boldsymbol{Z}[{}^+G_n]$ and has a finite index in ${}^+Q_n$ which is a power of 2. Hence the cohomology groups

$$H^k(\Gamma_n/\Gamma_m, {}^+Q_m) = 0,$$

for any k and $m \geqq n \geqq 0$.

PROPOSITION 8. *The group ${}^+P_n'$ has a G-subgroup P_n'' such that $P_n'' \cong \boldsymbol{Z}[{}^+G_n]$ as G-groups and such that the index $[{}^+P_n' : P_n'']$ is finite and prime to p.*

PROOF. For any $m \geqq 0$, let M_m' denote the extension of F_m obtained by adjoining all q_m-th roots of elements in ${}^+P_m$, and let M be the union of the increasing sequence of subfields $M_m', m \geqq 0$, in Ω. Since $E_m = {}^+E_m \times W_m$ and since ${}^+\pi_l^{p^{l-m}}/{}^+\pi_m$ belongs to ${}^+E_l$ for any $l \geqq m$, M is nothing but the abelian extension of F obtained by adjoining p^l-th roots of elements in E_m for all l and $m \geqq 0$. Let M_m be the maximal abelian extension of F_m contained in M. Clearly F is a subfield of M_m. Let A_m denote the character group of the compact abelian Galois group $G(M_m/F)$. For any χ in A_m and σ in G, we define χ^σ by

$$\chi^\sigma(u) = \chi(u^{\sigma^{-1}}), \qquad u \in G(M_m/F),$$

where $u^{\sigma^{-1}} = s^{-1}us$ with an element s in $G(M_m/\boldsymbol{Q})$ which induces σ on F. We then have

$$\chi^{\sigma\tau} = (\chi^\tau)^\sigma, \qquad \chi \in A_m, \sigma, \tau \in G,$$

and A_m becomes a $\boldsymbol{Z}_p[G]$-module. For the structure of A_m, we know the following[12]: Let $J_m = {}^-((\boldsymbol{Q}_p/\boldsymbol{Z}_p)[G_m])$. Then there exist an integer $n_1 \geqq 0$ and a fixed finite p-primary $\boldsymbol{Z}_p[G]$-module D such that whenever $m \geqq n_1$, the $\boldsymbol{Z}_p[G]$-modules A_m and J_m have submodules B_m and D_m respectively, with the property

$$A_m/B_m \cong D, \qquad B_m \cong J_m/D_m, \qquad D_m \cong D.$$

Since D is finite, $p^eD = 0$ for some $e \geqq 0$.

Now, given $n \geqq 0$, we choose an m such that $m \geqq n, n_1, 2e$. It is easy to see that $F \cap M_m' = F_m$ and $G(FM_m'/F) = G(M_m'/F_m)$. Let A_m' be the submodule of A_m corresponding to the sub-extension FM_m'/F of M/F. Then by the theory of Kummer extensions, there exists an isomorphism $f: {}^+P_m/({}^+P_m)^{q_m} \to A_m'$ such that

12) See [9], § 10, Theorem 17.

$$f(x^\sigma)=\kappa(\sigma)f(x)^\sigma\,,\qquad \sigma\in G\,,$$

for any x in ${}^+P_m/({}^+P_m)^{q_m}$. Such an isomorphism or homomorphism of $\boldsymbol{Z}_p[G]$-modules will be called in general a κ-isomorphism or κ-homomorphism[13].

As an abelian group, ${}^+P_m/\{\pm1\}$ is isomorphic to $\boldsymbol{Z}^s$, $s=\frac{1}{2}(p-1)p^m$. Hence $A'_m\cong{}^+P_m/({}^+P_m)^{q_m}\cong(\boldsymbol{Z}/q_m\boldsymbol{Z})^s$. Let $A''_m=p^eA'_m$. Since $A_m/B_m\cong D$ and $p^eD=0$, A''_m is a submodule of B_m, isomorphic to $(\boldsymbol{Z}/q_{m-e}\boldsymbol{Z})^s$. Let J'_m be the submodule of all x in J_m such that $q_{m-e}x=0$. Since $p^eD_m=0$ and $m\geqq 2e$, D_m is contained in pJ'_m. Identifying B_m with J_m/D_m, put $B'_m=J'_m/D_m$. Then B'_m is contained in A''_m, and $A''_m/B'_m\cong D$, $B'_m/pB'_m\cong J'_m/pJ'_m\cong{}^-((\boldsymbol{Z}/p\boldsymbol{Z})[G_m])$. Clearly f induces a κ-isomorphism $g:{}^+P_m/({}^+P_m)^{q_{m-e}}\to A''_m=p^eA'_m$. Let S_m be the subgroup of ${}^+P_m$ containing $({}^+P_m)^{q_{m-e}}$ such that $S_m/({}^+P_m)^{q_{m-e}}\to B'_m$ under g. Then g defines κ-isomorphisms ${}^+P_m/S_m\to D$ and $S_m/S_m^p\to{}^-((\boldsymbol{Z}/p\boldsymbol{Z})[G_m])$. It follows that S_m/S_m^p is $\boldsymbol{Z}_p[G]$-isomorphic to ${}^+((\boldsymbol{Z}/p\boldsymbol{Z})[G_m])=(\boldsymbol{Z}/p\boldsymbol{Z})[{}^+G_m]$. Let α'_m be an element of S_m such that the cosets of $(\alpha'_m)^\rho$, $\rho\in{}^+G_m$, form a basis of S_m/S_m^p, and let S'_m be the subgroup of S_m generated by these $(\alpha'_m)^\rho$. We then see easily that $S'_m\cong\boldsymbol{Z}[{}^+G_m]$ as G-groups and that the index of S'_m in S_m is finite and prime to p. It follows that $H^k(\Gamma_n/\Gamma_m,S_m)=0$ for every k. Hence $N_{n,m}(S_m)=F_n\cap S_m={}^+P_n\cap S_m$.

Since ${}^+P_m/S_m$ is κ-isomorphic to a fixed finite module D, $N_{n,m}({}^+P_m)$ is contained in S_m whenever m is sufficiently large. $N_{n,m}({}^+P_m)$ is then contained in $F_n\cap S_m=N_{n,m}(S_m)$, and we see that $N_{n,m}({}^+P_m)=F_n\cap S_m={}^+P_n\cap S_m=N_{n,m}(S_m)$. Hence ${}^+P_n/N_{n,m}({}^+P_m)={}^+P_nS_m/S_m$ and $[{}^+P_n:N_{n,m}({}^+P_m)]\leqq[{}^+P_m:S_m]=[D:0]$. Since $N_{n,m}({}^+P_m)$ decreases as m increases, it follows that

$${}^+P'_n=N_{n,m}({}^+P_m)=N_{n,m}(S_m)\,,$$

whenever m is sufficiently large. We fix such an m and put

$$P''_n=N_{n,m}(S'_m)\,.$$

It then follows from $S'_n\cong\boldsymbol{Z}[{}^+G_m]$ that $P''_n\cong\boldsymbol{Z}[{}^+G_n]$ as G-groups. Since $[S_m:S'_m]$ is finite and prime to p, so is $[N_{n,m}(S_m):N_{n,m}(S'_m)]=[{}^+P'_n:P''_n]$.

COROLLARY.

i) *For any n and $s\geqq0$, there exists a $\boldsymbol{Z}_p[G]$-isomorphism*

$${}^+P'_n/({}^+P'_n)^{p^s}\cong(\boldsymbol{Z}/p^s\boldsymbol{Z})[{}^+G_n]\,.$$

ii) *For any k and $m\geqq n\geqq0$,*

$$H^k(\Gamma_n/\Gamma_m,{}^+P'_m)=0\,.$$

iii) *For $m\geqq n\geqq0$,*

13) The definition of κ-isomorphisms and κ-homomorphisms given here, as well as that of u^σ and χ^σ in the above, differs slightly from those given in [8], [9]. We feel that the present definitions are more adequate.

$$ {}^+P'_n = N_{n,m}({}^+P'_m) = {}^+P_n \cap {}^+P'_m = F_n \cap {}^+P'_m , $$

so that the natural homomorphism ${}^+P_n/{}^+P'_n \to {}^+P_m/{}^+P'_m$ *is injective. If* m *is sufficiently larger than* n, *then*

$$ {}^+P'_n = N_{n,m}({}^+P_m) . $$

iv) *If* n *is sufficiently large,* $n \geqq n_0$, *then*

$$ {}^+P_m = {}^+P_n {}^+P'_m , \qquad m \geqq n , $$

so that ${}^+P_n/{}^+P'_n \to {}^+P_m/{}^+P'_m$ *is also surjective, and*

$$ {}^+P_n/{}^+P'_n \cong {}^+P_m/{}^+P'_m , \qquad m \geqq n \geqq n_0 . $$

The groups ${}^+P_n/{}^+P'_n, n \geqq n_0$, *are* κ*-isomorphic to the finite* p*-primary* $\boldsymbol{Z}_p[G]$*-module* D *defined in the above.*

PROOF. i) Since $[{}^+P'_n : {}^+P''_n]$ is prime to p, we have

$$ {}^+P'_n/({}^+P'_n)^{p^s} \cong {}^+P''_n/({}^+P''_n)^{p^s} \cong (\boldsymbol{Z}/p^s\boldsymbol{Z})[{}^+G_n] . $$

ii) This follows immediately from $H^k(\Gamma_n/\Gamma_m, {}^+P'_m/{}^+P''_m) = H^k(\Gamma_n/\Gamma_m, {}^+P''_m) = 0$.

iii) It has already been proved in the above that ${}^+P'_n = N_{n,m}({}^+P_m)$ for $m \gg n$. Given any $m \geqq n$, choose a large $l \geqq m$ so that ${}^+P'_m = N_{m,l}({}^+P_l)$ and ${}^+P'_n = N_{n,l}({}^+P_l)$. Since $N_{n,l} = N_{n,m} \circ N_{m,l}$, we obtain ${}^+P'_n = N_{n,m}({}^+P'_m)$. It then follows from $H^0(\Gamma_n/\Gamma_m, {}^+P'_m) = 0$ that ${}^+P'_n = N_{n,m}({}^+P'_m) = F_n \cap {}^+P'_m = {}^+P_n \cap {}^+P'_m$.

iv) Since D is a finite p-primary $\boldsymbol{Z}_p[G]$-module, there exists an integer $n_0 \geqq 0$ such that Γ_{n_0} acts trivially on D. We may assume that $p^{n_0}D = 0$. Let $n \geqq n_0$ and let m be sufficiently larger than n so that ${}^+P'_n = N_{n,m}({}^+P_m)$. Since ${}^+P_m/S_m$ is κ-isomorphic to D, Γ_n acts trivially on ${}^+P_m/S_m$. Hence $({}^+P_m)^{\omega_n}$ is a submodule of S_m, and $H^1(\Gamma_n/\Gamma_m, S_m) = 0$ implies $({}^+P_m)^{\omega_n} = S_m^{\omega_n}$. It follows that ${}^+P_m = ({}^+P_m \cap F_n)S_m = {}^+P_n S_m$ and ${}^+P_m/S_m = {}^+P_n S_m/S_m = {}^+P_n/N_{n,m}(P_m^+) = {}^+P_n/{}^+P'_n$. Therefore ${}^+P_n/{}^+P'_n, n \geqq n_0$, is κ-isomorphic to D. For any $m \geqq n \geqq n_0$, we then see that ${}^+P_n/{}^+P'_n \to {}^+P_m/{}^+P'_m$ is surjective and ${}^+P_m = {}^+P_n {}^+P'_m$.

From the above, we can obtain similar results for P'_n, E'_n, and ${}^+E'_n$. For example:

$$ N_{n,m}({}^+E'_m) = {}^+E'_n , \qquad m \geqq n \geqq 0 . $$

Some of these results were already obtained in [9].

2.2. Let Φ_n^* be as before the multiplicative group of the local field Φ_n. For any $m \geqq n$, $N_{n,m}(\Phi_m^*)$ is a subgroup of Φ_n^*. Let

$$ \Phi'_n = \bigcap_{m \geqq n} N_{n,m}(\Phi_n^*) , $$

and let

$$ U'_n = U_n \cap \Phi'_n , \qquad U'_{n,0} = U_{n,0} \cap \Phi'_n . $$

Clearly Φ'_n, U'_n, and $U'_{n,0}$ are subgroups of Φ_n^*. Since $N_{n,m}(\pi_m) = \pi_n$ and

$N_{n,m}(v)=v$ for any v in $\boldsymbol{V}$, $m\geqq n$, we see immediately that

$$\Phi'_n=\Pi_n\times U'_n,\qquad U'_n=U'_{n,0}\times\boldsymbol{V}.$$

PROPOSITION 9.

i) *Φ'_n is a closed subgroup of Φ^*_n, consisting of all α in Φ_n such that $N_n(\alpha)$ is a power of p, and U'_n is a compact subgroup of U_n, consisting of all β in U_n such that $N_n(\beta)=1$,*

ii) $\Phi^*_n=\Phi'_n\times\boldsymbol{U}_0$, $U_n=U'_n\times\boldsymbol{U}_0=U'_{n,0}\times\boldsymbol{U}$.

iii) $N_{n,m}(\Phi'_m)=\Phi'_n$, $N_{n,m}(U'_m)=U'_n$, $N_{n,m}(U'_{m,0})=U'_{n,0}$, $\quad m\geqq n$.

PROOF. i) By local class field theory[14], $\boldsymbol{Q}^*_p/N_m(\Phi^*_m)$ is a cyclic group of order $(p-1)p^m$. Since $p=N_m(\pi_m)$ is contained in $N_m(\Phi^*_m)$, we see from $\boldsymbol{Q}^*_p=\{p\}\times\boldsymbol{V}\times\boldsymbol{U}_0$ that $N_m(\Phi^*_m)=\{p\}\times\boldsymbol{U}_0^{p^m}$; here we denote by $\{p\}$ the multiplicative group generated by p. Again by local class field theory, an element α in Φ_n is contained in $N_{n,m}(\Phi^*_m)$, $m\geqq n$, if and only if $N_n(\alpha)$ is contained in $N_m(\Phi^*_m)$. Hence α is in Φ'_n if and only if $N_n(\alpha)$ is contained in the intersection of $N_m(\Phi^*_m)=\{p\}\times\boldsymbol{U}_0^{p^m}$ for all $m\geqq n$, namely, in $\{p\}$. It then follows immediately that U'_n consists of all β in U_n such that $N_n(\beta)=1$. It also follows that Φ'_n is a closed subgroup of Φ^*_n, and that U'_n is a compact subgroup of U_n.

ii) Let α be any element of Φ^*_n, and let $N_n(\alpha)=p^ta$ with a in $\boldsymbol{U}_0^{p^n}=\boldsymbol{U}_0^{(p-1)p^n}$. Then $a=b^{(p-1)p^n}=N_n(b)$ for some b in $\boldsymbol{U}_0$, and $N_n(\alpha b^{-1})=p^t$ so that αb^{-1} is contained in Φ'_n. Hence $\Phi^*_n=\Phi'_n\boldsymbol{U}_0$. Since $N_n(b)=b^{(p-1)p^n}\neq1$ for any $b\neq1$ in $\boldsymbol{U}_0$, we have $\Phi'_n\cap\boldsymbol{U}_0=1$. Therefore $\Phi^*_n=\Phi'_n\times\boldsymbol{U}_0$. It then follows immediately that $U_n=U'_n\times\boldsymbol{U}_0=U'_{n,0}\times\boldsymbol{U}$.

iii) It is obvious that $N_{n,m}(\Phi'_m)$ is contained in Φ'_n, $m\geqq n$. Let α be any element of Φ'_n. Then $\alpha=N_{n,m}(\alpha')$ with α' in Φ^*_m. By ii), $N_n(\alpha)=N_m(\alpha')$ is a power of p. Hence α' is in Φ'_m, again by ii). Therefore α is contained in $N_{n,m}(\Phi'_m)$. Thus $\Phi'_n=N_{n,m}(\Phi'_m)$. It is then clear that $U'_n=N_{n,m}(U'_m)$, $U'_{n,0}=N_{n,m}(U'_{m,0})$.

Now, let X_n denote the inverse limit of the sequence of finite groups $\Phi'_n/\Phi'^{p^s}_n$, $s\geqq0$, relative to the natural homomorphisms $\Phi'_n/\Phi'^{p^t}_n\to\Phi'_n/\Phi'^{p^s}_n$, $t\geqq s$:

$$X_n=\varprojlim\Phi'_n/\Phi'^{p^s}_n.$$

X_n is a p-primary compact abelian group, and for any a in $\boldsymbol{Z}_p$ and x in X_n, x^a is defined as usual. Since $\boldsymbol{V}$ is the intersection of all $\Phi'^{p^s}_n$, $s\geqq0$, the natural map $\Phi'_n\to X_n$ imbeds $\Phi'_n/\boldsymbol{V}=\Pi_n\times U'_{n,0}$ in X_n as a dense subgroup of X_n, and we see that

$$X_n=\overline{\Pi}_n\times U'_{n,0},$$

where $\overline{\Pi}_n$ denotes the closure of Π_n in X_n, consisting of all elements of the form π_n^a with a in $\boldsymbol{Z}_p$.

14) For local and global class field theory used here and in the following, see [1], [3], and [4].

Clearly the surjective homomorphism $N_{n,m}: \Phi'_m \to \Phi'_n$ induces a continuous surjective homomorphism $N_{n,m}: X_m \to X_n$, $m \geqq n$. Let X be the inverse limit of X_n, $n \geqq 0$, relative to such homomorphisms:

$$X = \lim X_n .$$

Then X is again a p-primary compact abelian group, and x^a is defined for any a in $\boldsymbol{Z}_p$ and x in X. Furthermore, since Φ'_n is invariant under the action of the Galois group G, we may extend the action of G on X_n, $n \geqq 0$, and on X in the natural way. Thus X_n, $n \geqq 0$, and X are compact $\boldsymbol{Z}_p[G]$-groups.

Let Ψ_n be the maximal p-primary abelian extension of Φ_n in Ω. Clearly Φ is contained in Ψ_n, and these Ψ_n, $n \geqq 0$, form an increasing sequence of subfields of Ω. Let Ψ be the union of all Ψ_n, $n \geqq 0$; Ψ is the maximal p-primary abelian extension of Φ contained in Ω. Since $\Psi/\boldsymbol{Q}_p$ is a Galois extension, $G = G(\Phi/\boldsymbol{Q}_p)$ acts on the abelian normal subgroup $G(\Psi/\Phi)$ of $G(\Psi/\boldsymbol{Q}_p)$ in the obvious manner.

PROPOSITION 10. *There exists a canonical G-isomorphism*

$$X \to G(\Psi/\Phi)$$

which induces isomorphisms

$$X^{(n)} \cong X_n \cong G(\Psi_n/\Phi), \qquad n \geqq 0 .$$

PROOF. Let $G(\Psi_m/\Phi) \to G(\Psi_n/\Phi)$, $m \geqq n$, be the natural homomorphism of Galois groups. Then by local class field theory, there exists a canonical isomorphism $X_n \to G(\Psi_n/\Phi)$ for each $n \geqq 0$ such that the following diagram is commutative:

$$\begin{array}{ccc} X_m & \longrightarrow & G(\Psi_m/\Phi) \\ \downarrow & & \downarrow \\ X_n & \longrightarrow & G(\Psi_n/\Phi), \end{array} \qquad m \geqq n .$$

Hence we have a G-isomorphism of X onto $G(\Psi/\Phi)$ such that

$$\begin{array}{ccc} X & \longrightarrow & G(\Psi/\Phi) \\ \downarrow & & \downarrow \\ X_n & \longrightarrow & G(\Psi_n/\Phi) \end{array}$$

is commutative. Since $\sigma(1+p)^{p^n}$ generates $\Gamma_n = G(\Phi/\Phi_n)$ topologically, and since Ψ_n is the maximal abelian extension of Φ_n contained in Ψ, we see that $G(\Psi/\Psi_n) = G(\Psi/\Phi)^{\omega_n}$. However, $G(\Psi/\Psi_n)$ is the kernel of the surjective homomorphism $G(\Psi/\Phi) \to G(\Psi_n/\Phi)$. Hence it follows from the above diagram that $X \to X_n$ is also surjective, and its kernel is X^{ω_n}, thus proving $X^{(n)} = X/X^{\omega_n} \cong X_n$.

2.3. Let A be any subgroup of Φ'_n. Then the closure of the image of A under $\Phi'_n \to X_n$ defines a closed subgroup of X_n. Since the norm, from F_n

to $\boldsymbol{Q}$, of any element in P_n is a power of p, it follows from Proposition 9 that P_n is contained in Φ'_n. Let Y_n be the closed subgroup of X_n determined by P_n as stated in the above, and let Y'_n and Z_n denote the closed subgroups of X_n defined similarly by P'_n and Q_n, respectively.

Let

$$E_{n,0}=E_n\cap U_{n,0}\,,\qquad E'_{n,0}=E'_n\cap U_{n,0}\,,\qquad C_{n,0}=C_n\cap U_{n,0}\,,$$

and let $\bar{E}_n, \bar{E}_{n,0}$, etc. denote the closures of the respective groups in U_n in the $\mathfrak{p}_n$-adic topology of Φ_n. Since

$$\pi_n^{\sigma-1}\equiv\kappa(\sigma)\mod\mathfrak{p}_n\,,$$

we see that

$$\bar{E}_n=\bar{E}_{n,0}\times\boldsymbol{V}\,,\qquad \bar{E}'_n=\bar{E}'_{n,0}\times\boldsymbol{V}\,,\qquad \bar{C}_n=\bar{C}_{n,0}\times\boldsymbol{V}\,.$$

Since $[P_n:\Pi_n\times E_{n,0}]=[E_n:E_{n,0}]$ is prime to p, we also have

$$Y_n=\overline{\Pi}_n\times\bar{E}_{n,0}$$

in $X_n=\overline{\Pi}_n\times U'_{n,0}$. Similarly

$$Y'_n=\overline{\Pi}_n\times\bar{E}'_{n,0}\,,\qquad Z_n=\overline{\Pi}_n\times\bar{C}_{n,0}\,.$$

Hence it follows that

$$\begin{aligned}
&X_n/Y_n=U'_{n,0}/\bar{E}_{n,0}=U'_n/\bar{E}_n\,,\\
&X_n/Y'_n=U'_{n,0}/\bar{E}'_{n,0}=U'_n/\bar{E}'_n\,,\\
&X_n/Z_n=U'_{n,0}/\bar{C}_{n,0}=U'_n/\bar{C}_n\,,\\
&Y'_n/Z_n=\bar{E}'_{n,0}/\bar{C}_{n,0}=\bar{E}'_n/\bar{C}_n\,,\qquad n\geqq 0\,.
\end{aligned}$$

It is clear that for any $m\geqq n$, $N_{n,m}: X_m\to X_n$ maps Y_m, Y'_m, and Z_m into Y_n, Y'_n and Z_n respectively. Hence we may define the inverse limits:

$$Y=\varprojlim Y_n\,,\qquad Y'=\varprojlim Y'_n\,,\qquad Z=\varprojlim Z_n\,,$$

relative to the homomorphisms $N_{n,m}$, $m\geqq n$, and we may consider Y, Y' and Z as closed $\boldsymbol{Z}_p[G]$-subgroups of X. However, by Proposition 8, $N_{n,m}(P_m)=P'_n$ whenever m is sufficiently larger than n. Hence also $N_{n,m}(Y_m)=Y'_n$ for $m\gg n$, and we see that

$$Y=Y'\,.$$

PROPOSITION 11. *X/Y is the inverse limit of $U'_n/\bar{E}'_n$, $n\geqq 0$, and the natural homomorphism $X/Y\to U'_n/\bar{E}'_n$ induces an isomorphism $(X/Y)^{(n)}\to U'_n/\bar{E}'_n$:*

$$X/Y=\varprojlim U'_n/\bar{E}'_n\,,\qquad (X/Y)^{(n)}=U'_n/\bar{E}'_n\,.$$

Similarly,

$$X/Z=\varprojlim U'_n/\bar{C}_n\,,\qquad (X/Z)^{(n)}=U'_n/\bar{C}_n\,.$$

PROOF. Since $N_{n,m}(P'_m)=P'_n$, $m\geqq n$, we have $N_{n,m}(Y'_m)=Y'_n$, $m\geqq n$.

Hence the natural homomorphism $X \to X_n$ maps Y' onto Y'_n. Since $Y = Y'$, $X/Y = \lim X_n/Y'_n = \lim U'_n/\bar{E}'_n$. By Proposition 10, the kernel of $X \to X_n$ is X^{ω_n}. Hence the kernel of $X \to X_n/Y'_n$ is $Y'X^{\omega_n}$. Since $X \to X_n/Y'_n$ is surjective, we have $X_n/Y'_n \cong X/Y'X^{\omega_n} = (X/Y')^{\sigma_n}$. The proof is similar for X/Z.

For each $n \geqq 0$, let L'_n denote the maximal unramified p-primary abelian extension of F_n contained in Ω, and let $L_n = FL'_n$. Then the union of the increasing sequence of subfields L_n, $n \geqq 0$, in Ω defines the maximal unramified p-primary abelian extension L over F in Ω. Let K_n be the maximal p-primary abelian extension of F_n, in Ω, such that no prime ideal of F_n different from (π_n) is ramified in that extension. The union of the increasing sequence of subfields K_n, $n \geqq 0$, in Ω again defines a p-primary abelian extension K of F, containing the above L. Since K is obviously a Galois extension of $\boldsymbol{Q}$, the Galois group G of $F/\boldsymbol{Q}$ acts on the abelian normal subgroup $G(K/F)$ of $G(K/\boldsymbol{Q})$. Similarly G also acts on $G(L/F)$ and $G(K/L)$[15].

PROPOSITION 12. *There exists a G-isomorphism:*

$$G(K/L) \to X/Y .$$

PROOF. We know that

$$X/Y = \lim X_n/Y_n = \lim U'_n/\bar{E}_n .$$

By class field theory, there exists a canonical G-isomorphism $G(K_n/L'_n) \to U_n/\bar{E}_n$, inducing a G-isomorphism $G(K_n/L_n) \to U'_n/\bar{E}_n$[16]. Let $G(K_m/L_m) \to G(K_n/L_n)$ be the homomorphism obtained by restricting the action of $G(K_m/L_m)$ on K_n. Then the following diagram is commutative:

$$\begin{array}{ccc} G(K_m/L_m) & \longrightarrow & U'_m/\bar{E}_m \\ \downarrow & & \downarrow \\ G(K_n/L_n) & \longrightarrow & U'_n/\bar{E}_n , \end{array} \qquad m \geqq n .$$

Since $G(K/L)$ is the inverse limit of $G(K_n/L_n)$, $n \geqq 0$, relative to $G(K_m/L_m) \to G(K_n/L_n)$, $m \geqq n$, we obtain from the above a G-isomorphism $G(K/L) \to X/Y$.

2.4. As in the proof of Proposition 11, we see that

$$Y/Z = Y'/Z = \lim Y'_n/Z_n = \lim \bar{E}'_n/\bar{C}_n .$$

Let ${}^+\Phi_n$ be the closure of ${}^+F_n$ in Φ_n, and let

$${}^+\bar{E}'_n = {}^+\Phi_n \cap \bar{E}'_n , \qquad {}^+\bar{C}_n = {}^+\Phi_n \cap \bar{C}_n , \qquad n \geqq 0 .$$

15) For the extensions L/F and K/F, see [9], § 5, § 6.

16) See [9], § 6.

Then ${}^+\bar{E}'_n$ and ${}^+\bar{C}_n$ are also closures of ${}^+E'_n$ and ${}^+C_n$ in U_n, and $\bar{E}'_n = {}^+\bar{E}'_n \times W_n$, $\bar{C}_n = {}^+\bar{C}_n \times W_n$ so that

$$\bar{E}'_n/\bar{C}_n = {}^+\bar{E}'_n/{}^+\bar{C}_n = {}^+(\bar{E}'_n/\bar{C}_n).$$

Hence

$$Y/Z = {}^+(Y/Z).$$

In general, for any finite abelian group $\mathfrak{G}$, let $(\mathfrak{G})_p$ denote the Sylow p-subgroup of $\mathfrak{G}$. Since ${}^+E_n/{}^+C_n$ is a finite group, so is ${}^+E'_n/{}^+C_n$. Let A denote the inverse limit of the p-groups $({}^+E'_n/{}^+C_n)_p$, $n \geqq 0$, relative to the homomorphisms $N_{n,m}: ({}^+E'_m/{}^+C_m)_p \to ({}^+E'_n/{}^+C_n)_p$, $m \geqq n$. Clearly A is a compact p-primary $\boldsymbol{Z}_p[G]$-group. Since $N_{n,m}({}^+E'_m) = {}^+E'_n$, $m \geqq n$, $N_{n,m}: ({}^+E'_m/{}^+C_m)_p \to ({}^+E'_n/{}^+C_n)_p$ is surjective. Hence $A \to ({}^+E'_n/{}^+C_n)_p$ is also surjective for every $n \geqq 0$. On the other hand, as $H^k(\Gamma_n/\Gamma_m, {}^+P'_m) = H^k(\Gamma_n/\Gamma_m, {}^+Q_m) = 0$ for any k and $m \geqq n \geqq 0$, we see that the kernel of $N_{n,m}: {}^+E'_m/{}^+C_m = {}^+P'_m/{}^+Q_m \to {}^+E'_n/{}^+C_n = {}^+P'_n/{}^+Q_n$ is $({}^+E'_m/{}^+C_m)^{\omega_n}$. Therefore, the kernel of $N_{n,m}: ({}^+E'_m/{}^+C_m)_p \to ({}^+E'_n/{}^+C_n)_p$ is $({}^+E'_m/{}^+C_m)_p^{\omega_n}$, and hence the kernel of $A \to ({}^+E'_n/{}^+C_n)_p$ is A^{ω_n}. Thus we obtain a $\boldsymbol{Z}_p[G]$-isomorphism

$$A^{(n)} = A/A^{\omega_n} \to ({}^+E'_n/{}^+C_n)_p, \qquad n \geqq 0.$$

Since ${}^+E'_n/{}^+C_n$ is finite, ${}^+E'_n{}^+\bar{C}_n/{}^+\bar{C}_n$ is also finite. Hence ${}^+E'_n{}^+\bar{C}_n$ is closed in U_n, and we see that ${}^+\bar{E}'_n = {}^+E'_n{}^+\bar{C}_n$. Therefore, the injection ${}^+E'_n \to {}^+\bar{E}'_n$ induces a surjective homomorphism ${}^+E'_n/{}^+C_n \to {}^+\bar{E}'_n/{}^+\bar{C}_n$. As ${}^+\bar{E}'_n/{}^+\bar{C}_n = Y'_n/Z_n$ is a finite p-group, $({}^+E'_n/{}^+C_n)_p \to {}^+\bar{E}'_n/{}^+\bar{C}_n = \bar{E}'_n/\bar{C}_n$ is also surjective. Hence we obtain a surjective $\boldsymbol{Z}_p[G]$-homomorphism

$$A \to Y/Z.$$

We shall next show that it is injective.

Suppose that there exists an element $a \neq 1$ in the kernel of $A \to Y/Z$. Since A is a p-primary compact group, there is an integer $d \geqq 1$ such that a is not contained in A^{p^d}. For each $n \geqq 0$, let a_n denote the image of a under $A \to ({}^+E'_n/{}^+C_n)_p$, and let α_n be an element of ${}^+E'_n$ representing a_n mod ${}^+C_n$. Since a is in the kernel of $A \to Y/Z$, a_n is mapped to the identity under $({}^+E'_n/{}^+C_n)_p \to {}^+\bar{E}'_n/{}^+\bar{C}_n$. Hence α_n is contained in ${}^+\bar{C}_n$, and there exist an element β_n in ${}^+E'_n \cap U_n^{q_n}$ and an element γ_n in ${}^+C_n$ such that $\alpha_n = \beta_n\gamma_n$. As $N_{n,m}(a_m) = a_n$, $m \geqq n$, we have $\alpha_n{}^+C_n = N_{n,m}(\alpha_m){}^+C_n = N_{n,m}(\beta_m){}^+C_n$. Since a is not contained in A^{p^d}, α_n does not belong to $({}^+E'_n)^{p^d}{}^+C_n$ whenever n is sufficiently large. Hence $N_{n,m}(\beta_m)$, $m \geqq n$, is not contained in $({}^+E'_n)^{p^d}$, if n is large. On the other hand, it follows from Corollary iii), iv) of Proposition 8 that there exists an integer $e \geqq 0$ such that $({}^+P_n/{}^+P'_n)^{p^e} = 1$ for every $n \geqq 0$. In the following, we shall fix an n such that $n \geqq d+e$ and that $N_{n,m}(\beta_m)$ is not contained in $({}^+E'_n)^{p^d}$ for any $m \geqq n$.

For each $m \geqq n$, let B_m denote the multiplicative group generated by

β_m^σ, $\sigma \in G$. Then B_m is a G-subgroup of ${}^+E'_m \cap U_m^{q_m}$, and $N_{n,m}(B_m)$ is not contained in $({}^+E'_n)^{p^d}$. Let D_m, D'_m, and D''_m denote the images of B_m under the natural homomorphisms ${}^+P'_m \to {}^+P'_m/({}^+P'_m)^{p^d}$, ${}^+P'_m \to {}^+P'_m/({}^+P'_m)^{q_m}$, and ${}^+P_m \to {}^+P_m/({}^+P_m)^{q_m}$ respectively. Let r_m be the rank of D_m. As an abelian group, ${}^+P'_m/\{\pm 1\}$ is isomorphic to $\boldsymbol{Z}^s$, where $s = \frac{1}{2}(p-1)p^m$. Hence ${}^+P'_m/({}^+P'_m)^{q_m} \cong (\boldsymbol{Z}/q_m\boldsymbol{Z})^s$ and $({}^+P'_m)^{p^d}/({}^+P'_m)^{q_m} \cong (\boldsymbol{Z}/q_{m-d}\boldsymbol{Z})^s$. We then see easily that D'_m contains a subgroup isomorphic to $(\boldsymbol{Z}/q_{m-d}\boldsymbol{Z})^{r_m}$. Now the kernel of the natural homomorphism ${}^+P'_m/({}^+P'_m)^{q_m} \to {}^+P_m/({}^+P_m)^{q_m}$ is a subgroup of $({}^+P_m)^{q_m}/({}^+P'_m)^{q_m} \cong {}^+P_m/{}^+P'_m$, and D'_m is mapped onto D''_m under that homomorphism. Since $({}^+P_m/{}^+P'_m)^{p^e} = 1$, it follows from the above that D''_m contains a subgroup isomorphic to $(\boldsymbol{Z}/q_{m-d-e}\boldsymbol{Z})^{r_m}$.

Let L''_m denote the abelian extension of F_m generated by the q_m-th roots of elements in B_m. Since ${}^+P_m \cap (F_m^*)^{q_m} = {}^+P_m^{q_m}$, the Galois group $G(L''_m/F_m)$ is isomorphic to $D''_m = B_m({}^+P_m)^{q_m}/({}^+P_m)^{q_m}$ as abelian groups. On the other hand, since B_m is contained in ${}^+E'_m \cap U_m^{q_m}$, L''_m/F_m is unramified. Hence L''_m is contained in the maximal unramified abelian p-extension L'_m over F_m. It then follows from the above that the Galois group $G(L'_m/F_m)$ contains a subgroup isomorphic to $(\boldsymbol{Z}/q_{m-d-e}\boldsymbol{Z})^{r_m}$. However, since $G(L/F)$ is a strictly Γ-finite Γ-group, there exists an integer $f \geqq 0$ such that the rank of $G(L'_m/F_m)^{p^f}$ does not exceed a fixed integer $r \geqq 0$ for every $m \geqq 0$[17]. Hence we see that $r_m \leqq r$ whenever $m \geqq d+e+f$.

Now, since D_m is a subgroup of ${}^+P'_m/({}^+P'_m)^{p^d}$ with rank r_m, it follows from the above that the order of D_m does not exceed p^{dr} for any $m \geqq n, d+e+f$. Hence we can find a large m such that $N_{n,m}(D_m) = 1$. As $D_m = B_m({}^+P'_m)/({}^+P'_m)^{p^d}$, $N_{n,m}(B_m)$ is then contained in $({}^+P'_m)^{p^d}$. On the other hand, Corollary iii) of Proposition 8 implies that $({}^+P'_m)^{p^d} \cap F_n = ({}^+P'_m \cap F_n)^{p^d} = ({}^+P'_n)^{p^d}$. It also follows from ${}^+P'_n = {}^+\Pi_m \times {}^+E'_n$ that $({}^+P'_n)^{p^d} \cap E_n = ({}^+E'_n)^{p^d}$. Hence the group $N_{n,m}(B_m)$, which is obviously a subgroup of E_n, must be contained in $({}^+E'_n)^{p^d}$. However we have chosen n so that $N_{n,m}(B_m)$ is not contained in $({}^+E'_n)^{p^d}$ for any $m \geqq n$. Hence we have a contradiction, and we see that there exists no $a \neq 1$ in the kernel of $A \to Y/Z$. Thus the homomorphism $A \to Y/Z$ is injective, and the following proposition is proved:

PROPOSITION 13. *Y/Z is the inverse limit of $({}^+E'_n/{}^+C_n)_p$, $n \geqq 0$ relative to $N_{n,m}: ({}^+E'_m/{}^+C_m)_p \to ({}^+E'_n/{}^+C_n)_p$, $m \geqq n$, and the natural homomorphism $Y/Z \to ({}^+E'_n/{}^+C_n)_p$ induces an isomorphism $(Y/Z)^{(n)} \to ({}^+E'_n/{}^+C_n)_p$:*

$$Y/Z = \lim ({}^+E'_n/{}^+C_n)_p\,, \qquad (Y/Z)^{(n)} = ({}^+E'_n/{}^+C_n)_p\,. \qquad n \geqq 0\,.$$

17) See [9], §5 and [8], 1.4.

§ 3

3.1. For any α, β in Φ_n^*, let

$$(\alpha, \beta)_n$$

denote Hilbert's norm residue symbol for the power q_n in the local field Φ_n. The symbol $(\alpha, \beta)_n$ defines a pairing

$$\Phi_n^* \times \Phi_n^* \to W_n$$

with the following properties[18]:

i) $(\alpha, \beta)_n = (\beta, \alpha)_n^{-1}$, $(\alpha^\sigma, \beta^\sigma)_n = (\alpha, \beta)_n^{\kappa(\sigma)}$, $\sigma \in G$,

ii) $(\alpha, \beta)_m^{p^{m-n}} = (N_{n,m}(\alpha), \beta)_n$, $\alpha \in \Phi_m^*$, $\beta \in \Phi_n^*$, $m \geqq n$,

iii) $(\alpha, \beta)_n = 1$ if and only if α is the norm of an element in $\Phi_n(\beta^{q_n^{-1}})$,

iv) $(\alpha, \Phi_n^*) = 1$ (or $(\Phi_n^*, \alpha) = 1$) if and only if α belongs to $(\Phi_n^*)^{q_n}$; hence $(\alpha, \beta)_n$ induces a non-degenerate pairing

$$(\Phi_n^*/(\Phi_n^*)^{q_n}) \times (\Phi_n^*/(\Phi_n^*)^{q_n}) \to W_n .$$

v) (Artin-Hasse's explicit formula) For any β in $U_{n,0}$, both $q_n^{-1}T_n(\log \beta)$ and $q_n^{-1}T_n(\zeta_n \pi_n^{-1} \log \beta)$ are contained in $\boldsymbol{Z}_p$, and

$$(\zeta_n, \beta)_n = \zeta_n^{q_n^{-1}T_n(\log \beta)},$$

$$(\pi_n, \beta)_n = \zeta_n^{q_n^{-1}T_n(\zeta_n \pi_n^{-1} \log \beta)}.$$

Let β be an element of $U_{n,0}$; and ξ, an element of $\mathfrak{X}_n$. Since $T_n(q_n \mathfrak{X}_n \log \beta) \equiv 0 \bmod q_n \boldsymbol{Z}_p$, $\zeta_n^{T_n(\xi \log \beta)}$ depends only upon the coset ξ' of $\xi \bmod q_n \mathfrak{X}_n$. Hence we may write $\zeta_n^{T_n(\xi' \log \beta)}$ for $\zeta_n^{T_n(\xi \log \beta)}$.

PROPOSITION 14. *There exists a unique map*

$$\psi_n : \Phi_n' \to \mathfrak{X}_n/q_n\mathfrak{X}_n$$

such that

$$(\alpha, \beta)_n = \zeta_n^{T_n(\psi_n(\alpha) \log \beta)}, \qquad \alpha \in \Phi_n', \beta \in U_{n,0}.$$

ψ_n is a surjective κ-homomorphism:

$$\psi_n(\alpha^\sigma) = \kappa(\sigma)\psi_n(\alpha)^\sigma, \qquad \alpha \in \Phi_n', \sigma \in G.$$

PROOF. Let α be fixed in Φ_n'. Since $N_{n,2n+1}(W_{2n+1}) = W_n$, $(\alpha, W_n)_n = 1$ by i) and iii). As W_n is the kernel of the log map: $U_{n,0} \to \mathfrak{L}_n$, $(\alpha, \beta)_n$ depends only upon $\log \beta$ for any β in $U_{n,0}$. Hence $\log \beta \to \iota((\alpha, \beta)_n)$ defines a homomorphism $\mathfrak{L}_n \to \boldsymbol{Q}_n/\boldsymbol{Z}_p$, $\iota : W \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ being the homomorphism fixed in 1.5. Since $\Phi_n/\mathfrak{X}_n$ is dual to $\mathfrak{L}_n$, there exists an element α'' in Φ_n such that $\iota((\alpha, \beta)_n) = \langle \alpha'', \log \beta \rangle_n$ for any β in $U_{n,0}$. We then have

$$(\alpha, \beta)_n = \zeta_n^{T_n(\alpha' \log \beta)},$$

18) See [4], II, § 11, § 19 and [2].

with $\alpha' = q_n\alpha''$. Since $T_n(\alpha' \log \beta)$ is in $\boldsymbol{Z}_p$ for any β in $U_{n,0}$, α' is contained in $\mathfrak{X}_n$. Let $\psi_n(\alpha)$ denote the coset of α' mod $q_n\mathfrak{X}_n$. Then we have

$$(\alpha, \beta)_n = \zeta_n^{T_n(\psi_n(\alpha) \log \beta)}, \qquad \beta \in U_{n,0}.$$

It is clear from the definition of $\mathfrak{X}_n$ that $\psi_n(\alpha)$ is uniquely determined for α by the above equality. Since $(\alpha, \beta)_n$ is multiplicative in α, it follows in particular that $\psi_n : \Phi_n' \to \mathfrak{X}_n/q_n\mathfrak{X}_n$ is a homomorphism. It also follows from i) that

$$\begin{aligned}(\alpha^\sigma, \beta^\sigma)_n &= (\alpha, \beta)_n^{\kappa(\sigma)} = \zeta_n^{\kappa(\sigma) T_n(\psi_n(\alpha) \log \beta)} \\ &= \zeta_n^{T_n(\kappa(\sigma)\psi_n(\alpha)^\sigma \log \beta^\sigma)}, \qquad \sigma \in G, \beta^\sigma \in U_{n,0}.\end{aligned}$$

Hence by the uniqueness mentioned above, we have

$$\psi_n(\alpha^\sigma) = \kappa(\sigma)\psi_n(\alpha)^\sigma, \qquad \sigma \in G, \alpha \in \Phi_n'.$$

To show that ψ_n is surjective, let α' be any element of $\mathfrak{X}_n$. Let $\psi : \Phi_n^* \to W_n$ be an extension of the homomorphism $U_{n,0} \to W_n$ defined by $\beta \to \zeta_n^{T_n(\alpha' \log \beta)}$; such an extension exists because $\Phi_n^* = \Pi_n \times U_{n,0} \times \boldsymbol{V}$. Since $W_n^{q_n} = 1$, ψ is trivial on $(\Phi_n^*)^{q_n}$. Hence it follows from iv) that there exists an α in Φ_n^* such that

$$(\alpha, \beta)_n = \zeta_n^{T_n(\alpha' \log \beta)}, \qquad \beta \in U_{n,0}.$$

Since $(\alpha, \zeta_n)_n = \zeta_n^{T_n(\alpha' \log \zeta_n)} = 1$, α is contained in $N_{n,2n+1}(\Phi_{2n+1}^*) = N_{n,2n+1}(\Phi_{2n+1}' \times \boldsymbol{U}_0^{q_n}) = \Phi_n' \times \boldsymbol{U}_0^{q_n}$. As $(\alpha, \beta)_n$ is unchanged when α is replaced by any element of $\alpha \boldsymbol{U}_0^{q_n}$, we may assume that α is contained in Φ_n'. Then we have $\alpha' = \psi_n(\alpha)$ and we see that ψ_n is surjective.

Let $f : X \to \mathfrak{X}$ be any κ-homomorphism. Then

$$f(x^{\omega_n}) \equiv \omega_n f(x) \mod q_n\mathfrak{X}, \qquad x \in X.$$

Hence f maps X^{ω_n} into $\omega_n\mathfrak{X} + q_n\mathfrak{X}$. Since $X_n = X^{(n)} = X/X^{\omega_n}$ by Proposition 10 and since $\omega_n\mathfrak{X} + q_n\mathfrak{X}$ is contained in the kernel of $\mathfrak{X} \to \mathfrak{X}_n/q_n\mathfrak{X}_n$, we see that f induces a homomorphism $X_n \to \mathfrak{X}_n/q_n\mathfrak{X}_n$, and hence also a homomorphism $\Phi_n' \to \mathfrak{X}_n/q_n\mathfrak{X}_n$.

THEOREM 4. *There exists a unique κ-isomorphism*

$$f : X \to \mathfrak{X}$$

which induces $\psi_n : \Phi_n' \to \mathfrak{X}_n/q_n\mathfrak{X}_n$ for every $n \geqq 0$.

PROOF. Let $m \geqq n$. For any α in Φ_m' and β in $U_{n,0}$, we have

$$\begin{aligned}(N_{n,m}(\alpha), \beta)_n &= (\alpha, \beta)_m^{p^{m-n}} = \zeta_n^{T_m(\psi_m(\alpha) \log \beta)} \\ &= \zeta_n^{T_n(T_{n,m}(\psi_m(\alpha)) \log \beta)}.\end{aligned}$$

This shows that

$$\psi_n(N_{n,m}(\alpha)) = T_{n,m}(\psi_m(\alpha)), \qquad \alpha \in \Phi_m',$$

namely that the following diagram is commutative:

$$\begin{array}{ccc} \Phi'_m & \longrightarrow & \mathfrak{X}_m/q_m\mathfrak{X}_m \\ \downarrow N_{n,m} & & \downarrow T_{n,m} \\ \Phi'_n & \longrightarrow & \mathfrak{X}_n/q_n\mathfrak{X}_n \end{array} \qquad m \geqq n .$$

Since $(\Phi'_n)^{q_n}$ is contained in the kernel of ψ_n, ψ_n induces a homomorphism $f_n : X_n \to \mathfrak{X}_n/q_n\mathfrak{X}_n$. For these f_n, $n \geqq 0$, we then have commutative diagrams similar to the one in the above. Since $\mathfrak{X}$ is also the inverse limit of $\mathfrak{X}_n/q_n\mathfrak{X}_n$, $n \geqq 0$, we obtain a continuous homomorphism $f : X \to \mathfrak{X}$ which induces f_n and ψ_n for every $n \geqq 0$. By Proposition 14, ψ_n is a surjective κ-homomorphism. Hence f_n and f are also surjective κ-homomorphisms.

Suppose that $f(x) = 0$ for an element x in X. Let x_n be the image of x under $X \to X_n$, and let α_n be an element of Φ'_n representing $x_n \bmod (\Phi'_n)^{q_n}$. Then $f(x) = 0$ implies $f_n(x_n) = 0$ and $\psi_n(\alpha_n) = 0$. It follows that $(\alpha_n, \beta)_n = 1$ for every β in $U_{n,0}$, and hence also for every β in $U_n = U_{n,0} \times \boldsymbol{V}$, $n \geqq 0$. Since $x_n = N_{n,2n+1}(x_{2n+1})$, we have $\alpha_n \equiv N_{n,2n+1}(\alpha_{2n+1}) \bmod (\Phi'_n)^{q_n}$. As $\pi_n = \pi_{2n+1}^{q_n}\beta$ with β in U_{2n+1}, we see that

$$\begin{aligned} (\alpha_n, \pi_n)_n &= (N_{n,2n+1}(\alpha_{2n+1}), \pi_n)_n = (\alpha_{2n+1}, \pi_n)_{2n+1}^{q_n} \\ &= (\alpha_{2n+1}, \pi_{2n+1})_{2n+1}^{q_{2n+1}}(\alpha_{2n+1}, \beta)_{2n+1} \\ &= 1 . \end{aligned}$$

It then follows from $\Phi_n^* = \Pi_n \times U_n$ that $(\alpha_n, \Phi_n^*)_n = 1$. Therefore, by iv), α_n is contained in $(\Phi_n^*)^{q_n}$, and x_n belongs to $X_n^{q_n}$ for every $n \geqq 0$. Hence $x = 1$, and f is injective. As X is compact, f is then a topological isomorphism. The uniqueness is obvious.

The definition of ψ_n, and hence also the definition of f depend upon the choice of the sequence of roots of unity ζ_n, $n \geqq 0$, namely, the choice of the isomorphism $\iota : W \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$. Nevertheless, f is essentially unique in the following sense; let $\iota' : W \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ be any other isomorphism and let $f' : X \to \mathfrak{X}$ be the κ-isomorphism defined by ι'. Then there exists a p-adic unit u such that $\iota(\zeta) = u\iota'(\zeta)$ for every ζ in W, and such that

$$f'(x) = uf(x) , \qquad x \in X .$$

Let $\mathfrak{Z}$ be the submodule of $\mathfrak{X}$ defined in 1.6, and let Z be the subgroup of X defined in 2.3. Then:

PROPOSITION 15.

$$f(Z) = \mathfrak{Z} .$$

PROOF. Let $f(Z) = \mathfrak{Z}'$, and let $\mathfrak{Z}'_n$ be the image of $\mathfrak{Z}'$ under $\mathfrak{X} \to \mathfrak{X}_n$. It follows from Artin-Hasse's explicit formula that

$$\psi_n(\pi_n) = \mu_n + q_n\mathfrak{X}_n .$$

Hence

$$\psi_n(\pi_n^\sigma)=\kappa(\sigma)\mu_n^\sigma+q_n\mathfrak{X}_n \qquad \sigma\in G,$$

by Proposition 14. Therefore $\psi_n(Q_n)=(\mathfrak{Z}_n+q_n\mathfrak{X}_n)/q_n\mathfrak{X}_n$, and consequently $f_n(Z_n)=(\mathfrak{Z}_n+q_n\mathfrak{X}_n)/q_n\mathfrak{X}_n$. However, since

$$\begin{array}{ccc} X & \xrightarrow{f} & \mathfrak{X} \\ \downarrow & & \downarrow \\ X_n & \xrightarrow{f_n} & \mathfrak{X}_n/q_n\mathfrak{X}_n \end{array}$$

is commutative, we see that $f_n(Z_n)=(\mathfrak{Z}'_n+q_n\mathfrak{X}_n)/q_n\mathfrak{X}_n$. Hence $\mathfrak{Z}_n+q_n\mathfrak{X}_n=\mathfrak{Z}'_n+q_n\mathfrak{X}_n$. We then obtain $\mathfrak{Z}=\mathfrak{Z}'$, q. e. d.

3.2. Let

$$\mathfrak{Y}=f(Y),$$

and let $\mathfrak{Y}_n$ be the image of $\mathfrak{Y}$ under $\mathfrak{X}\to\mathfrak{X}_n$ $(n\geqq 0)$. $\mathfrak{Y}$ is a closed $\boldsymbol{Z}_p[G]$-submodule of $\mathfrak{X}$ containing $\mathfrak{Z}$, and

$$\mathfrak{X}/\mathfrak{Y}=\lim \mathfrak{X}_n/\mathfrak{Y}_n,$$

$$\mathfrak{Y}/\mathfrak{Z}=\lim \mathfrak{Y}_n/\mathfrak{Z}_n,$$

in the obvious manner. Similarly for ${}^{\pm}(\mathfrak{X}/\mathfrak{Y})$, etc.

It follows from Corollary i) of Proposition 8 that for each $n\geqq 0$, there exists an element α_n in ${}^+P'_n$ such that ${}^+P'_n/({}^+P'_n)^p$ is generated by the cosets of α_n^ρ, $\rho\in{}^+G_n$. Using the same corollary, we also see readily that we may choose α_n so that $N_{n,n+1}(\alpha_{n+1})=\alpha_n$, $n\geqq 0$. Let y_n denote the image of α_n under ${}^+P'_n\to{}^+Y'_n=(Y'_n)^{+^\varepsilon}$. Then ${}^+Y'_n$ is generated by y_n over $\boldsymbol{Z}_p[G]$, and $N_{n,m}(y_m)=y_n$ for any $m\geqq n\geqq 0$. Let y be the element of ${}^+Y$ determined by these y_n, $n\geqq 0$. It follows from the above that the elements y^σ, $\sigma\in G$, generate a dense subgroup of ${}^+Y$. Hence $f(y)^\sigma$, $\sigma\in G$, also generate a dense subgroup of ${}^-\mathfrak{Y}=f({}^+Y)$.

Let i be odd and $i\neq p-2$. By Theorem 2 and Proposition 1, we have $\boldsymbol{Z}_p[G]$-isomorphisms ${}^i\mathfrak{X}\to{}^i\mathfrak{R}\to\Lambda=\boldsymbol{Z}_p[[T]]$. Let ${}^ih$ be the element of Λ corresponding to ${}^i\varepsilon(f(y))$ in ${}^i\mathfrak{X}$. Then we have isomorphisms of compact Γ-modules

$${}^i\mathfrak{Y}\to({}^ih)=\Lambda{}^ih, \qquad {}^i\mathfrak{X}/{}^i\mathfrak{Y}\to\Lambda/({}^ih).$$

Since ${}^i\mathfrak{Z}\to({}^ig)$ under the same map ${}^i\mathfrak{X}\to\Lambda$, we see that the ideal $({}^ig)$ is contained in $({}^ih)$, namely, that

$${}^ig={}^ih{}^ik,$$

for some ${}^ik$ in Λ. It follows that

$${}^i(\mathfrak{Y}/\mathfrak{Z})={}^i\mathfrak{Y}/{}^i\mathfrak{Z}\cong\Lambda/({}^ik).$$

Since ${}^{p-2}(\mathfrak{X}/\mathfrak{Z})\cong{}^{p-2}(\mathfrak{A}/\mathfrak{B})=0$, we have

$${}^{p-2}(\mathfrak{X}/\mathfrak{Y})={}^{p-2}(\mathfrak{Y}/\mathfrak{Z})=0.$$

Hence the above result also holds for $i=p-2$, if we put simply ${}^{p-2}g={}^{p-2}h={}^{p-2}k=1$.

PROPOSITION 16. *Both* $^-(\mathfrak{X}/\mathfrak{Y})$ *and* $^-(\mathfrak{Y}/\mathfrak{Z})=\mathfrak{Y}/\mathfrak{Z}$ *are regular strictly* Γ*-finite* Γ*-modules, and*

$$^-(\mathfrak{X}/\mathfrak{Y})^{(n)}={}^-\mathfrak{X}_n/{}^-\mathfrak{Y}_n\,,$$

$$^-(\mathfrak{Y}/\mathfrak{Z})^{(n)}={}^-\mathfrak{Y}_n/{}^-\mathfrak{Z}_n\,, \qquad n\geqq 0\,.$$

PROOF. We first notice that since $^+(Y/Z)=Y/Z$ and Y/Z is κ-isomorphic to $\mathfrak{Y}/\mathfrak{Z}$, we have $^-(\mathfrak{Y}/\mathfrak{Z})=\mathfrak{Y}/\mathfrak{Z}$. We also know by Theorem 2 that $^-(\mathfrak{X}/\mathfrak{Z})$ is strictly Γ-finite. Hence both $^-(\mathfrak{X}/\mathfrak{Y})$ and $^-(\mathfrak{Y}/\mathfrak{Z})$ are strictly Γ-finite. Let i be any odd index. Then $^i(\mathfrak{X}/\mathfrak{Y})$ is strictly Γ-finite, and $^i(\mathfrak{X}/\mathfrak{Y})\cong A/(^ih)$. As we have noticed in 1.4, a strictly Γ-finite Γ-module of the type $A/(g)$ is always regular. Hence $^i(\mathfrak{X}/\mathfrak{Y})$ is regular. Therefore $^-(\mathfrak{X}/\mathfrak{Y})$, the direct sum of such $^i(\mathfrak{X}/\mathfrak{Y})$, is also regular. Similarly $^-(\mathfrak{Y}/\mathfrak{Z})$ is regular.

Since $^-(\mathfrak{X}/\mathfrak{Z})^{(n)}={}^-\mathfrak{X}_n/{}^-\mathfrak{Z}_n$ by Theorem 2, we see immediately that $^-(\mathfrak{X}/\mathfrak{Y})^{(n)}={}^-\mathfrak{X}_n/{}^-\mathfrak{Y}_n$, $n\geqq 0$. On the other hand, as $^-(\mathfrak{X}/\mathfrak{Y})$ is regular, we have $^-(\mathfrak{X}/\mathfrak{Y})^{(n)}={}^-(\mathfrak{X}/\mathfrak{Z})^{(n)}/{}^-(\mathfrak{Y}/\mathfrak{Z})^{(n)}$. Hence $^-(\mathfrak{Y}/\mathfrak{Z})^{(n)}$ and ${}^-\mathfrak{Y}_n/{}^-\mathfrak{Z}_n$ have the same finite order. However, it is clear that $\omega_n(^-(\mathfrak{Y}/\mathfrak{Z}))$ is contained in the kernel of the natural homomorphism $^-(\mathfrak{Y}/\mathfrak{Z})\to{}^-\mathfrak{Y}_n/{}^-\mathfrak{Z}_n$. Hence we see from the above that $^-(\mathfrak{Y}/\mathfrak{Z})^{(n)}={}^-(\mathfrak{Y}/\mathfrak{Z})/\omega_n(^-(\mathfrak{Y}/\mathfrak{Z}))\to{}^-\mathfrak{Y}_n/{}^-\mathfrak{Z}_n$ is an isomorphism.

Now, the map $f: X\to\mathfrak{X}$ induces κ-isomorphisms

$$X/Y\to\mathfrak{X}/\mathfrak{Y}\,,$$

$$Y/Z\to\mathfrak{Y}/\mathfrak{Z}\,,$$

$$X/Z\to\mathfrak{X}/\mathfrak{Z}\,.$$

Of these six $\boldsymbol{Z}_p[G]$-groups, the arithmetic properties of X/Y and Y/Z are given by Proposition 12 and Proposition 13 respectively, and the algebraic structure of $\mathfrak{X}/\mathfrak{Z}$ is described in Theorem 2. Using these facts, we shall next study some arithmetic consequences of the above κ-isomorphisms.

3.3. Let S_n denote the Sylow p-subgroup of the ideal class group of F_n, $n\geqq 0$. The injection of the ideal group of F_n into the ideal group of F_m, $m\geqq n$, induces a homomorphism $S_n\to S_m$. Let S denote the direct limit of S_n, $n\geqq 0$, relative to these maps $S_n\to S_m$, $m\geqq n$. Clearly S_n, $n\geqq 0$, and S are $\boldsymbol{Z}_p[G]$-groups in the natural manner so that ${}^\pm S_n$, ${}^\pm S$, etc. are defined. It is known that ${}^-S_n\to{}^-S_m$ is injective for any $m\geqq n$[19]. Hence we may consider ^-S simply as the union of all ${}^-S_n$, $n\geqq 0$.

Let L/F and K/F be the abelian extensions defined in 2.3. Let c be an ideal class in ^-S and let $\mathfrak{a}$ be an ideal of an F_n representing the class c.

19) See [9], § 10, Theorem 15.

Then $\mathfrak{a}^{p^m}=(a)$ for some integer $m\geqq 0$ and for some a in F_n^*. Let α be a p^m-th root of a in Ω. It follows from the definition of K that α is contained in K. For any g in ${}^+G(K/F)$, we put

$$(g, c)=\iota(\alpha^{g-1});$$

since α^{g-1} is a p^m-th root of unity in W, the right-hand side is an element of $\boldsymbol{Q}_p/\boldsymbol{Z}_p$. We can then show that (g, c) depends only upon g and c, and defines a dual pairing of the compact abelian group ${}^+G(K/F)$ and the discrete abelian group ${}^-S$ into $\boldsymbol{Q}_p/\boldsymbol{Z}_p$:

$${}^+G(K/F)\times {}^-S\to \boldsymbol{Q}_p/\boldsymbol{Z}_p,$$

such that

$$(g^\sigma, c^\sigma)=\kappa(\sigma)(g, c), \qquad \sigma\in G^{20)}.$$

Let L'/F denote the maximal sub-extension of L/F such that the Galois group $G(L'/F)$ is a regular Γ-group. It is known that L/L' is a finite extension and ${}^-G(L/F)={}^-G(L'/F)^{21)}$. Let ${}^-S'$ and ${}^-S''$ denote the annihilators of ${}^+G(K/L')$ and ${}^+G(K/L)$ in ${}^-S$ respectively, with respect to the above pairing. Then we have similar pairings

$${}^+G(K/L')\times({}^-S/{}^-S')\to \boldsymbol{Q}_p/\boldsymbol{Z}_p,$$
$${}^+G(K/L)\times({}^-S/{}^-S'')\to \boldsymbol{Q}_p/\boldsymbol{Z}_p,$$
$${}^+G(L'/F)\times {}^-S'\to \boldsymbol{Q}_p/\boldsymbol{Z}_p,$$
$${}^+G(L/F)\times {}^-S''\to \boldsymbol{Q}_p/\boldsymbol{Z}_p.$$

Clearly ${}^-S'$ is contained in ${}^-S''$, and ${}^-S''/{}^-S'$ is dual to the finite group ${}^+G(L/L')$. Since ${}^+G(L'/F)$ is a regular Γ-group, ${}^-S'$ is also regular. It follows that ${}^-S'$ is the maximal regular subgroup of the discrete Γ-finite Γ-group ${}^-S''$.

PROPOSITION 17. *Let c be an element of order p^m, $m\geqq 0$, in ${}^-S_n$. Then the following properties for c are equivalent:*

i) *c is contained in ${}^-S_n''={}^-S''\cap {}^-S_n$,*

ii) *There exist an integer $s\geqq m$ and an ideal $\mathfrak{a}$ in the class c such that $\mathfrak{a}^{p^s}=(a)$ with an element a in $F_n^*\cap \Phi_n^{p^s}$,*

iii) *For any integer $s\geqq m$ and for any ideal $\mathfrak{a}$ in the class c, there exists an element a in $F_n^*\cap \Phi_n^{p^s}$ such that $\mathfrak{a}^{p^s}=(a)$.*

PROOF. Clearly iii) implies ii). Let s, $\mathfrak{a}$, and a be as stated in ii). Let $l\geqq n$, s, and let α be a p^s-th root of a in Ω. By the assumption on a, $F_l(\alpha)/F_l$ is an unramified abelian p-extension so that α is contained in L_l', and hence in L. Consequently $\alpha^{g-1}=1$ for every g in $G(K/L)$, and $({}^+G(K/L), c)=0$. Therefore, c is contained in ${}^-S''$, and we see that ii) implies i).

20) See [9], § 8.

21) See [9], § 10, Theorem 16.

Suppose next that c belongs to ${}^{-}S''$. Let s and $\mathfrak{a}$ be as stated in iii). Since c is an element of ${}^{-}S_n$, we have $c^{1+\delta}=1$ for $\delta=\sigma(-1)$. Let $c_1=c^{1/2}$. Then $c=c_1^{1-\delta}$. Let $\mathfrak{a}_1$ be an ideal of c_1, prime to (π_n). Since $c_1^{p^m}=1$, we have $\mathfrak{a}_1^{p^s}=(a_1)$ with some a_1 in $F_n^* \cap U_n$. Let $\mathfrak{a}_2=\mathfrak{a}_1^{1-\delta}$, $a_2=a_1^{1-\delta}$ so that $\mathfrak{a}_2$ is an ideal of the class c satisfying $\mathfrak{a}_2^{p^s}=(a_2)$, $a_2^{1+\delta}=1$. Let α be a p^s-th root of a_2 in K. Since $({}^{+}G(K/L), c)=1$, it follows from the definition of the pairing that $\alpha^{g-1}=1$ for every g in ${}^{+}G(K/L)$. On the other hand, we see from $a_2^{1+\delta}=1$ that $\alpha^{g-1}=1$ for every g in ${}^{-}G(K/L)$. Hence $\alpha^{g-1}=1$ for any g in $G(K/L)$, and α must be an element of L. Let $l \geqq n, s$. Then $F_l(\alpha)/F_l$ is an unramified cyclic extension, and the principal prime ideal (π_l) is completely decomposed in $F_l(\alpha)$. Hence a_2 is contained in $\Phi_l^{p^s}$, and consequently in ${}^{-}U_l^{p^s}$. However ${}^{-}U_l$ is the direct product of W_l and a subgroup which is G-isomorphic to ${}^{-}(\boldsymbol{Z}_p[G_l])$[22]. It follows that $a_2=\zeta_n^i a_2'$ where i is a suitable integer and a_2' is an element of ${}^{-}U_n^{p^s}$. Thus $\mathfrak{a}_2^{p^s}=(a_2')$ with a_2' in $F_n^* \cap \Phi_n^{p^s}$. Since $\mathfrak{a}$ and $\mathfrak{a}_2$ belong to the same class c, there exists an element b in F_n^* such that $\mathfrak{a}=b\mathfrak{a}_2$. Then $\mathfrak{a}^{p^s}=(a)$ with $a=b^{p^s}a_2'$ in $F_n^* \cap \Phi_n^{p^s}$. Hence i) implies iii).

THEOREM 5. *There exists a dual pairing of the compact abelian group* ${}^{-}(\mathfrak{X}/\mathfrak{Y})$ *and the discrete abelian group* ${}^{-}S/{}^{-}S''$ *into* $\boldsymbol{Q}_p/\boldsymbol{Z}_p$:

$$ {}^{-}(\mathfrak{X}/\mathfrak{Y}) \times ({}^{-}S/{}^{-}S'') \to \boldsymbol{Q}_p/\boldsymbol{Z}_p , $$

such that

$$ (\tilde{x}^\sigma, \tilde{c}^\sigma)=(\tilde{x}, \tilde{c}), \qquad \sigma \in G , $$

for any $\tilde{x}$ *in* ${}^{-}(\mathfrak{X}/\mathfrak{Y})$ *and* $\tilde{c}$ *in* ${}^{-}S/{}^{-}S''$.

PROOF. By Proposition 12, ${}^{+}G(K/L)={}^{+}(X/Y)$. Hence the map: $X/Y \to \mathfrak{X}/\mathfrak{Y}$ induces a κ-isomorphism ${}^{+}G(K/L) \to {}^{-}(\mathfrak{X}/\mathfrak{Y})$. Combining this with the pairing ${}^{+}G(K/L) \times ({}^{-}S/{}^{-}S'') \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$, we obtain a pairing ${}^{-}(\mathfrak{X}/\mathfrak{Y}) \times ({}^{-}S/{}^{-}S'') \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ as stated in the theorem.

Suppose that $\iota: W \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ is replaced by $\iota': W \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$. Then $\iota=u\iota'$ with u in $\boldsymbol{U}$, and f is replaced by $f'=uf$. Hence $(\tilde{x}, \tilde{c})$ is unchanged, and we see that the pairing is canonically defined. More precisely, the value of $(\tilde{x}, \tilde{c})$ can be computed explicitly as follows: Let c be an element of ${}^{-}S_n$ $(n \geqq 0)$ representing $\tilde{c}$, and let $\mathfrak{a}$ be any ideal of the class c, prime to (π_n). Let $\mathfrak{a}^{p^m}=(a)$, $m \geqq 0$, with an element a in F_n^*. We may assume that $a \equiv 1 \bmod \pi_n$, because every non-zero residue class mod π_n contains a unit of F_n. Let x be an element of ${}^{-}\mathfrak{X}$ representing $\tilde{x}$, and let x_n be the image of x under ${}^{-}\mathfrak{X} \to {}^{-}\mathfrak{X}_n$. Then:

PROPOSITION 18.

$$ (\tilde{x}, \tilde{c})=\mathrm{Res}\,(p^{-m}T_n(x_n \log a)) . $$

PROOF. We fix an $s \geqq m, n$. Let α be a p^m-th root of a in K. Let g be

22) See [9], § 11, Theorem 19.

the element of ${}^{+}G(K/L)$ corresponding to $\tilde{x}$ in ${}^{-}(\mathfrak{X}/\mathfrak{Y})$, and let g' be the restriction of g on K_s. We choose an element b in U_s' such that g' is mapped to b mod $\bar{E}_s$ under the isomorphism $G(K_s/L_s)\to U_s'/\bar{E}_s = X_s/Y_s$. Then $\psi_s(b)=f_s(b)=x_s$ mod $q_s\mathfrak{X}_s$, where x_s denotes the image of x under ${}^{-}\mathfrak{X}\to{}^{-}\mathfrak{X}_s$, and ψ_s and f_s are the maps defined in 3.1. Hence it follows from the definition of $(\tilde{x},\tilde{c})$ and $(\ ,\ )_s$ that

$$\begin{aligned}(\tilde{x},\tilde{c}) &= (g,c) = \iota(\alpha^{g-1}) = \iota(\alpha^{g'-1})\\ &= \iota((b, a^{p^{s+1-m}})_s) = p^{s+1-m}\iota((b,a)_s)\\ &= p^{s+1-m}\iota(\zeta_s^{T_s(x_s\log a)})\\ &= p^{s+1-m}\operatorname{Res}(q_s^{-1}T_s(x_s\log a))\\ &= \operatorname{Res}(p^{-m}T_n(T_{n,s}(x_s)\log a))\\ &= \operatorname{Res}(p^{-m}T_n(x_n\log a)),\end{aligned}$$

q. e. d.

The formula indicates clearly that the pairing is independent of the choice of $\iota: W\to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ and that $(\tilde{x}^\sigma,\tilde{c}^\sigma)=(\tilde{x},\tilde{c})$ for any σ in G. It is to be noted that we can also define $(\tilde{x},\tilde{c})$ by the above formula and then prove directly that it gives a dual pairing of ${}^{-}(\mathfrak{X}/\mathfrak{Y})$ and ${}^{-}S/{}^{-}S''$ into $\boldsymbol{Q}_p/\boldsymbol{Z}_p$.

3.4. It is known that the discrete Γ-group ${}^{-}S$ is regular and that ${}^{-}S_n$ consists of all those elements in ${}^{-}S$ which are invariant under the automorphisms of $\Gamma_n = G(F/F_n)$[23]. Hence $N_{n,m}: {}^{-}S_m\to{}^{-}S_n$ induces an isomorphism ${}^{-}S_m^{(n)} = {}^{-}S_m/{}^{-}S_m^{\omega_n}\to{}^{-}S_n$, $m\geqq n\geqq 0$.

Let c_0 be any element of ${}^{-}S_0$. Since $N_{n,m}: {}^{-}S_m\to{}^{-}S_n$, $m\geqq n\geqq 0$, is surjective, we can find c_n, $n\geqq 1$, so that $N_{n,m}(c_m)=c_n$ for any $m\geqq n\geqq 0$. For each $n\geqq 0$, we then define a $\boldsymbol{Z}_p[G]$-homomorphism

$$\rho_n: \mathfrak{R}_n\to{}^{-}S_n,$$

by

$$\rho_n(\alpha)=c_n^\alpha, \qquad \alpha\in\mathfrak{R}_n.$$

Since $c_n^{-\varepsilon}=c_n$, we have $\rho_n(\mathfrak{R}_n)=\rho_n({}^{-}\mathfrak{R}_n)$. We also know by a classical result on cyclotomic fields[24] that $\rho_n(\alpha)=c_n^\alpha=1$ for any α in $\mathfrak{R}_n\cap\mathfrak{R}_n\xi_n^*$. Let $\mathfrak{A}_n^*$ and $\mathfrak{B}_n^*$ be the $\boldsymbol{Z}_p[G]$-modules defined in 1.4. Then ${}^{-}\mathfrak{A}_n^*={}^{-}\mathfrak{B}_n^*+{}^{-}\mathfrak{R}_n$ and ${}^{-}\mathfrak{B}_n^*=\mathfrak{R}_n{}^{-}\xi_n^*$ so that

$${}^{-}\mathfrak{A}_n^*/{}^{-}\mathfrak{B}_n^* = {}^{-}\mathfrak{R}_n/({}^{-}\mathfrak{R}_n\cap\mathfrak{R}_n{}^{-}\xi_n^*) = {}^{-}\mathfrak{R}_n/({}^{-}\mathfrak{R}_n\cap\mathfrak{R}_n\xi_n^*).$$

Hence it follows from the above that ρ_n induces a $\boldsymbol{Z}_p[G]$-homomorphism

$$\rho_n': {}^{-}\mathfrak{A}_n^*/{}^{-}\mathfrak{B}_n^*\to{}^{-}S_n.$$

Since $N_{n,m}(c_m)=c_n$, $m\geqq n\geqq 0$, we have

23) See [**9**], § 10.

24) See [**10**], § 3.

$$\rho'_n = \rho'_m \circ t'_{m,n}\,, \qquad m \geqq n \geqq 0\,,$$

for the homomorphism $t'_{m,n} : {}^-\mathfrak{A}_n^* / {}^-\mathfrak{B}_n^* \to {}^-\mathfrak{A}_m^* / {}^-\mathfrak{B}_m^*$ defined in 1.2. It then follows that

$$\rho'_n \circ t_{n,m} = \rho'_m \circ \nu_{n,m} = N_{n,m} \circ \rho'_m\,, \qquad m \geqq n \geqq 0\,.$$

Hence the maps $\rho'_n, n \geqq 0$, define a homomorphism from the inverse limit ${}^-(\mathfrak{A}^*/\mathfrak{B}^*)$ of ${}^-\mathfrak{A}_n^* / {}^-\mathfrak{B}_n^*, n \geqq 0$, into the inverse limit of ${}^-S_n, n \geqq 0$, relative to the homomorphisms $N_{n,m} : {}^-S_m \to {}^-S_n$. However, we can see by class field theory that the inverse limit of ${}^-S_n, n \geqq 0$, is canonically isomorphic to the inverse limit of ${}^-G(L'_n/F_n), n \geqq 0$, relative to the natural maps ${}^-G(L'_m/F_m) \to {}^-G(L'_n/F_n)$, $m \geqq n \geqq 0$, namely, to the Galois group ${}^-G(L/F)$. Thus we obtain a $\boldsymbol{Z}_p[G]$-homomorphism

$$\rho : {}^-(\mathfrak{A}^*/\mathfrak{B}^*) \to {}^-G(L/F)\,,$$

depending upon the sequence of elements $c_n, n \geqq 0$.

Suppose that $c_0^{(1)}, \cdots, c_0^{(r)}$ generate ${}^-S_0$ over $\boldsymbol{Z}_p[G]$. Let $\rho^{(j)} : {}^-(\mathfrak{A}^*/\mathfrak{B}^*) \to {}^-G(L/F)$ be the homomorphism defined by a sequence of elements $c_n^{(j)}, n \geqq 0$, starting with $c_0^{(j)}$ $(1 \leqq j \leqq r)$. We then see easily that the homomorphism $\rho : {}^-(\mathfrak{A}^*/\mathfrak{B}^*)^r \to {}^-G(L/F)$ defined by these $\rho^{(1)}, \cdots, \rho^{(r)}$ is surjective. Hence ${}^-G(L/F)$ is always a homomorphic image of the $\boldsymbol{Z}_p[G]$-module ${}^-(\mathfrak{A}^*/\mathfrak{B}^*)^r$ for some integer $r \geqq 1$. We shall next consider the case $r = 1$.

In general, let A be a p-primary compact G-module on which G of course acts continuously. For simplicity, we call A G-cyclic when A contains an element a such that the elements $\sigma a, \sigma \in G$, generate a dense subgroup of A. For example, both ${}^-\mathfrak{Y}$ and ${}^-\mathfrak{Z}$ are G-cyclic modules.

Let $A = {}^+A \oplus {}^-A = {}^0A \oplus \cdots \oplus {}^{p-2}A$ be the decompositions of A defined as usual. Then we see easily that each of the following conditions is necessary and sufficient for A to be G-cyclic:

1) $A^{(0)} = A/A^{\omega_0}$ is G-cyclic,

2) Both ${}^+A$ and ${}^-A$ are G-cyclic,

3) Every ${}^iA, 0 \leqq i \leqq p-2$, is a Γ-module of the type $\Lambda/(g), g \in \Lambda$,

4) Every ${}^iA^{(0)} = {}^iA/{}^iA^{\omega_0}, 0 \leqq i \leqq p-2$, is cyclic over $\boldsymbol{Z}_p$, namely, every ${}^iA^{(0)}$ is either isomorphic to $\boldsymbol{Z}_p$ or to a finite cyclic group with order a power of p.

For the Galois group $G(L/F)$, we have natural isomorphisms $G(L/F)^{(0)} \to G(L'_0/F_0) \to S_0$. Hence $G(L/F)$ is G-cyclic if and only if the finite group S_0 is G-cyclic.

PROPOSITION 19. *The following properties for S_0 are equivalent:*

i) *S_0 is G-cyclic,*

ii) *${}^-S_0$ is G-cyclic,*

iii) *${}^iS_0$ is cyclic for every index i,*

iv) *${}^iS_0$ is cyclic for every odd i.*

PROOF. It is sufficient to show that iv) implies iii). Let ${}^-S_0^{(p)}$ denote the subgroup of all c in ${}^-S_0$ such that $c^p=1$. Then the pairing ${}^+G(K/F)\times{}^-S\to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ in 3.3 induces a non-degenerate pairing

$$({}^+G(K_0/F_0)/{}^+G(K_0/F_0)^p)\times {}^-S_0^{(p)}\to \boldsymbol{Q}_p/\boldsymbol{Z}_p\,,$$

such that

$$(g^\sigma, c^\sigma)=\kappa(\sigma)(g,c) \qquad\qquad \sigma\in\Delta\,.$$

Hence we see that

$$\operatorname{rank} {}^iG(K_0/F_0)=\operatorname{rank} {}^jS_0\,,$$

for any even i and odd j such that $i+j\equiv 1 \bmod p-1$. On the other hand, since ${}^iG(K_0/L_0)\cong {}^iU_0'/{}^i\bar{E}_0={}^iU_{0,0}'/{}^i\bar{E}_{0,0}$ as stated in the proof of Proposition 12, and since $\operatorname{rank} {}^iU_{0,0}'=0$ or 1 according as $i=0$ or $i\neq 0$, we know that $\operatorname{rank} {}^iG(K_0/L_0)\leqq 1$ for any even index i. Hence $\operatorname{rank} {}^iG(K_0/F_0)$ is either equal to $\operatorname{rank} {}^iG(L_0/F_0)$ or equal to $1+\operatorname{rank} {}^iG(L_0/F_0)$. However, by class field theory, ${}^iG(L_0/F_0)$ is isomorphic to ${}^iS_0$. Therefore, it follows from the above that

$$\operatorname{rank} {}^iS_0\leqq \operatorname{rank} {}^jS_0\leqq 1+\operatorname{rank} {}^iS_0\,, \tag{6}$$

for even i and odd j satisfying $i+j\equiv 1 \bmod p-1$. Hence if ${}^jS_0$ is cyclic, so is ${}^iS_0$, and we see that iii) follows from iv).

PROPOSITION 20. *Suppose that S_0 is G-cyclic. Then there exist $\boldsymbol{Z}_p[G]$-isomorphisms*

$${}^+G(L'/F)\to {}^+(Y/Z)=Y/Z\,,$$

$${}^-G(L'/F)={}^-G(L/F)\to {}^-(\mathfrak{A}^*/\mathfrak{B}^*)\,.$$

There also exist dual pairings

$${}^-(\mathfrak{X}/\mathfrak{Y})\times({}^-S/{}^-S')\to \boldsymbol{Q}_p/\boldsymbol{Z}_p\,,$$

$${}^-(\mathfrak{Y}/\mathfrak{Z})\times {}^-S'\to \boldsymbol{Q}_p/\boldsymbol{Z}_p\,,$$

$${}^-(\mathfrak{X}/\mathfrak{Z})\times {}^-S\to \boldsymbol{Q}_p/\boldsymbol{Z}_p\,,$$

such that

$$[x^\sigma, c^\sigma]=[x,c]\,, \qquad\qquad \sigma\in G\,.$$

PROOF. Since S_0 is G-cyclic, so is ${}^-S_0$ by Proposition 19. Hence ${}^-S_0$ has an element c_0 whose conjugates c_0^σ, $\sigma\in G$, generate ${}^-S_0$. Let c_n, $n\geqq 1$, be chosen from ${}^-S_n$ as stated in the above. Since $N_{0,n}(c_n)=c_0$ and since $N_{0,n}:{}^-S_n\to {}^-S_0$ induces an isomorphism of ${}^-S_n/{}^-S_n^{\omega_0}$ onto ${}^-S_0$, ${}^-S_n/{}^-S_n^{\omega_0}$ is generated by the cosets of c_n^σ, $\sigma\in G$. We then see that ${}^-S_n$ itself is generated by c_n^σ, $\sigma\in G$, and the map $\rho_n:\mathfrak{R}_n\to {}^-S_n$ is surjective. Since $\rho_n({}^-\mathfrak{R}_n)=\rho_n(\mathfrak{R}_n)$, $\rho_n':{}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*={}^-\mathfrak{R}_n/({}^-\mathfrak{R}_n\cap \mathfrak{R}_n\xi_n^*)\to {}^-S_n$ is also surjective. However, ${}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*$ is isomorphic to ${}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n$ as abelian groups so that the order of ${}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*$ is equal to the exact power of p dividing the first factor ${}^-h_n$ of the class number of F_n, namely, to the order of ${}^-S_n$. Hence ρ_n' must be an isomorphism. Therefore

$\rho : {}^-(\mathfrak{A}^*/\mathfrak{B}^*) \to {}^-G(L/F)$ is also an isomorphism.

By Proposition 5, we have a non-degenerate pairing $({}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n) \times ({}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*) \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ for each $n \geqq 0$. Using the isomorphisms $\varphi_n : {}^-(\mathfrak{X}/\mathfrak{Z})^{(n)} = {}^-\mathfrak{X}_n/{}^-\mathfrak{Z}_n \to {}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n$ and $\rho_n' : {}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^* \to {}^-S_n$, we obtain a non-degenerate pairing $[x, c]_n : {}^-(\mathfrak{X}/\mathfrak{Z})^{(n)} \times {}^-S_n \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ such that

$$[x^\sigma, c^\sigma]_n = [x, c]_n , \qquad \sigma \in G ,$$

$$[N_{n,m}(x), c]_n = [x, c]_m , \qquad m \geqq n \geqq 0 ,$$

where the element x in the second equality stands for an arbitrary element in ${}^-(\mathfrak{X}/\mathfrak{Z})^{(m)}$. Since ${}^-(\mathfrak{X}/\mathfrak{Z})$ is the inverse limit of ${}^-(\mathfrak{X}/\mathfrak{Z})^{(n)}$, $n \geqq 0$, and ${}^-S$ is the direct limit of ${}^-S_n$, $n \geqq 0$, it is clear that the above pairings $[x, c]_n$, $n \geqq 0$, define a dual pairing

$${}^-(\mathfrak{X}/\mathfrak{Z}) \times {}^-S \to \boldsymbol{Q}_p/\boldsymbol{Z}_p ,$$

such that $[x^\sigma, c^\sigma] = [x, c]$ for any σ in G.

Now, let A and B denote the annihilators of ${}^-S'$ and ${}^-S''$ in ${}^-(\mathfrak{X}/\mathfrak{Z})$ respectively, with regard to the above pairing of ${}^-(\mathfrak{X}/\mathfrak{Z})$ and ${}^-S$. Then we have similar pairings

$$({}^-(\mathfrak{X}/\mathfrak{Z})/A) \times {}^-S' \to \boldsymbol{Q}_p/\boldsymbol{Z}_p ,$$

$$B \times ({}^-S/{}^-S'') \to \boldsymbol{Q}_p/\boldsymbol{Z}_p .$$

Hence it follows from Theorem 5 that B is $\boldsymbol{Z}_p[G]$-isomorphic to ${}^-(\mathfrak{X}/\mathfrak{Y})$ and consequently that ${}^iB \cong {}^i(\mathfrak{X}/\mathfrak{Y}) \cong \Lambda/({}^ih)$ for every odd i; here $\Lambda = \boldsymbol{Z}_p[[T]]$, and ${}^ih$ is an element of Λ as defined in 3.2. On the other hand, we know that there exists a $\boldsymbol{Z}_p[G]$-isomorphism ${}^i\lambda : {}^i(\mathfrak{X}/\mathfrak{Z}) \to \Lambda/({}^ig)$ for each odd i. Let ${}^ib$ be the image of $1 \bmod ({}^ih)$ under an isomorphism $\Lambda/({}^ih) \to {}^iB$, and let ${}^if$ be an element of Λ such that ${}^i\lambda({}^ib) = {}^if \bmod ({}^ig)$. Then ${}^i\lambda({}^iB) = ({}^if, {}^ig)/({}^ig)$, and we see from the isomorphisms $\Lambda/({}^ih) \to {}^iB \to {}^i\lambda({}^iB)$ that an element u of Λ belongs to $({}^ih)$ if and only if $u{}^if$ is contained in $({}^ig)$. Since ${}^ig = {}^ih{}^ik$, it follows that ${}^if$ is divisible by ${}^ik$ in Λ: ${}^if = {}^ik'{}^ik$, and that ${}^ik'$ is not a zero-divisor $\bmod ({}^ih)$. As ${}^ih \neq 0$, we then see that $({}^ik', {}^ih)$ is a primary ideal of Λ, belonging to the maximal ideal of the 2-dimensional local ring Λ. Hence $\Lambda/({}^ik', {}^ih)$ is a finite module. Let ${}^iA'$ be the inverse image of $({}^ik)/({}^ig)$ under ${}^i\lambda : {}^i(\mathfrak{X}/\mathfrak{Z}) \to \Lambda/({}^ig)$. Since $({}^if, {}^ig) = ({}^ik', {}^ih)({}^ik)$, we have ${}^iA'/{}^iB \cong ({}^ik)/({}^if, {}^ig) = \Lambda/({}^ik', {}^ih)$ and ${}^i(\mathfrak{X}/\mathfrak{Z})/{}^iA' \cong \Lambda/({}^ik) \cong {}^i(\mathfrak{Y}/\mathfrak{Z})$. Hence ${}^iA'/{}^iB$ is finite and ${}^i(\mathfrak{X}/\mathfrak{Z})/{}^iA'$ is a regular Γ-module. On the other hand, as A/B is dual to ${}^-S''/{}^-S'$, A/B is finite, and so is ${}^iA/{}^iB$. Since ${}^i(\mathfrak{X}/\mathfrak{Z})/{}^iA$ is dual to the regular Γ-module ${}^{-i}S'$, ${}^i(\mathfrak{X}/\mathfrak{Z})/{}^iA$ is also regular. Therefore both ${}^iA'/{}^iB$ and ${}^iA/{}^iB$ are finite submodules of the Γ-module ${}^i(\mathfrak{X}/\mathfrak{Z})/{}^iB$ with regular factor modules, and we see that ${}^iA' = {}^iA$[25]. It follows

25) A discrete Γ-finite module has a unique maximal regular submodule. See [8], 1.4.

that ${}^{i}(\mathfrak{X}/\mathfrak{Z})/{}^{i}A \cong {}^{i}(\mathfrak{Y}/\mathfrak{Z})$ for every odd i, and we have a $\boldsymbol{Z}_p[G]$-isomorphism

$$ {}^{-}(\mathfrak{X}/\mathfrak{Z})/A \to {}^{-}(\mathfrak{Y}/\mathfrak{Z}) . $$

Combining it with $({}^{-}(\mathfrak{X}/\mathfrak{Z})/A) \times {}^{-}S' \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$, we obtain a dual pairing ${}^{-}(\mathfrak{Y}/\mathfrak{Z}) \times {}^{-}S' \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$.

The pairing ${}^{-}(\mathfrak{X}/\mathfrak{Z}) \times {}^{-}S \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ also induces a similar pairing $A \times ({}^{-}S/{}^{-}S') \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$. However, it has been proved in the above that ${}^{i}A \cong ({}^{i}k)/({}^{i}g) = A/({}^{i}h) \cong {}^{i}(\mathfrak{X}/\mathfrak{Y})$. Hence $A \cong {}^{-}(\mathfrak{X}/\mathfrak{Y})$, and we have a pairing ${}^{-}(\mathfrak{X}/\mathfrak{Y}) \times ({}^{-}S/{}^{-}S') \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$.

Finally, combining the pairing ${}^{-}(\mathfrak{Y}/\mathfrak{Z}) \times {}^{-}S' \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ with the κ-isomorphism ${}^{+}(Y/Z) \to {}^{-}(\mathfrak{Y}/\mathfrak{Z})$, we obtain a dual pairing ${}^{+}(Y/Z) \times {}^{-}S' \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ such that $[y^{\sigma}, c^{\sigma}] = \kappa(\sigma)[y, c]$ for any σ in G. As stated in 3.3, there also exists a dual pairing ${}^{+}G(L'/F) \times {}^{-}S' \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ such that $(g^{\sigma}, c^{\sigma}) = \kappa(\sigma)(g, c)$ for any σ in G. It follows that ${}^{+}(Y/Z) = Y/Z$ is $\boldsymbol{Z}_p[G]$-isomorphic to ${}^{+}G(L'/F)$.

Since ${}^{-}G(L/F)^{(n)} = {}^{-}G(L_n'/F_n) \cong {}^{-}S_n$, $n \geqq 0$, the isomorphism ${}^{-}G(L/F) \cong {}^{-}(\mathfrak{A}^*/\mathfrak{B}^*)$ implies

$$ {}^{-}S_n \cong {}^{-}\mathfrak{A}_n^*/{}^{-}\mathfrak{B}_n^* , \qquad n \geqq 0 . $$

As stated in [**10**], this gives us a group-theoretical interpretation of the p-part of the classical class number formula (I) for the first factor ${}^{-}h_n$ of the class number of F_n. We also notice that the existence of a $\boldsymbol{Z}_p[G]$-isomorphism ${}^{-}G(L/F) \to {}^{-}(\mathfrak{A}^*/\mathfrak{B}^*)$ implies conversely that S_0 is G-cyclic, because ${}^{-}S_0 \cong {}^{-}\mathfrak{A}_0^*/{}^{-}\mathfrak{B}_0^* = {}^{-}\mathfrak{R}_0/({}^{-}\mathfrak{R}_0 \cap \mathfrak{R}_0\xi_0^*)$ and ${}^{-}\mathfrak{R}_0$ is G-cyclic.

To obtain a similar result from ${}^{+}G(L'/F) \cong Y/Z$, we assume that $G(L/F)$ is a regular Γ-groups. Then $L' = L$, and ${}^{+}G(L'/F)^{(n)} = {}^{+}G(L/F)^{(n)} \cong {}^{+}S_n$, $n \geqq 0$. On the other hand, the regularity of $G(L/F)$ also implies $E_n' = E_n$, $n \geqq 0$[26] so that $(Y/Z)^{(n)} = ({}^{+}E_n/{}^{+}C_n)_p$ by Proposition 13. Hence we see from ${}^{+}G(L'/F) \cong Y/Z$ that

$$ {}^{+}S_n \cong ({}^{+}E_n/{}^{+}C_n)_p , \qquad n \geqq 0 , $$

as $\boldsymbol{Z}_p[G]$-groups. This may be considered as a group-theoretical interpretation of the p-part of the classical class number formula (II) for the second factor ${}^{+}h_n$ of the class number of F_n, because the p-part of (II) simply states that the order of ${}^{+}S_n$ is equal to the order of $({}^{+}E_n/{}^{+}C_n)_p$. Without assuming that $G(L/F)$ is regular, we can still obtain a certain group-theoretical relation between ${}^{+}S_n$ and $({}^{+}E_n/{}^{+}C_n)_p$ by using Corollary iv) of Proposition 8. But we omit the detail here.

Finally, we notice that unlike the pairing given in Theorem 5, the isomorphisms and the pairings in the preceding proposition are not canonical. We feel that some essential link is still missing in the relation between ${}^{-}(\mathfrak{X}/\mathfrak{Z})$ and ${}^{-}S$.

---

26) See [**9**], § 9, Theorem 14.

3.5. Suppose now that the prime number p is properly irregular; namely, that the second factor ${}^+h_0$ of the class number of F_0 is prime to p. Then ${}^+S_0=1$, and it follows from (6) that ${}^jS_0$ is cyclic for every odd j. Hence S_0 is G-cyclic by Proposition 19, and we see from Proposition 20 that ${}^-S_n \cong {}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*$, $n \geqq 0$. However, in this case, we can also proceed as follows, without referring to the result of 3.4.

It is known that the assumption on ${}^+h_0$ implies that ${}^+h_n$ is not divisible by p for any $n \geqq 0$[27] Hence the class number formula (II) shows that $({}^+E_n/{}^+C_n)_p=1$. It then follows from Proposition 13 that $Y/Z=1$. Therefore ${}^-(\mathfrak{Y}/\mathfrak{Z})=\mathfrak{Y}/\mathfrak{Z}=0$, and ${}^-(\mathfrak{X}/\mathfrak{Y})={}^-(\mathfrak{X}/\mathfrak{Z})$. On the other hand, the fact that ${}^+h_n$ is prime to p also implies that ${}^+S_n=1$ and ${}^+G(L_n'/F_n)=1$, $n \geqq 0$. Hence ${}^+S=1$, ${}^-S=S$, ${}^+G(L/F)=1$, and consequently ${}^-S''=1$, because ${}^-S''$ is dual to ${}^+G(L/F)$ as explained in 3.3. We then see from Theorem 5 that there exists a canonical dual pairing

$$ {}^-(\mathfrak{X}/\mathfrak{Z}) \times S \to \boldsymbol{Q}_p/\boldsymbol{Z}_p $$

such that $[x^\sigma, c^\sigma]=[x, c]$ for any σ in G. Hence we also have, for each $n \geqq 0$, a similar non-degenerate pairing

$$ {}^-\mathfrak{X}_n/{}^-\mathfrak{Z}_n \times S_n \to \boldsymbol{Q}_p/\boldsymbol{Z}_p . $$

It follows in particular that ${}^-\mathfrak{X}_n/{}^-\mathfrak{Z}_n$ is finite. Hence ${}^-\mathfrak{A}_n/{}^-\mathfrak{B}_n$ is also finite by Theorem 2. The proof of Proposition 4 then shows that ${}^iD_n \neq 0$ for every odd i and that the order of S_n, which equals the order of ${}^-\mathfrak{X}_n/{}^-\mathfrak{Z}_n$, is equal to the exact power of p dividing $2q_n \prod \left(-\frac{1}{2}{}^iD_n\right)$. Since $S_n={}^-S_n$, this is nothing but the p-part of the class number formula (I). We also see from Proposition 5 that S_n is $\boldsymbol{Z}_p[G]$-isomorphic to ${}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*$.

There exists an essential difference between the above proof and the one which uses Proposition 20. Whereas the isomorphism $S_n={}^-S_n \cong {}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*$ obtained from Proposition 20 is not canonical, the pairing ${}^-\mathfrak{X}_n/{}^-\mathfrak{Z}_n \times S_n \to \boldsymbol{Q}_p/\boldsymbol{Z}_p$ in the above is canonical and is explicitly given by Proposition 18. Furthermore, in the proof of Proposition 20, we had to use the class number formula (I) in the form that ${}^-S_n$ and ${}^-\mathfrak{A}_n^*/{}^-\mathfrak{B}_n^*$ have the same order. However, in the above proof, in addition to the assumption that ${}^+h_0$ is not divisible by p, we have used only the class number formula (II) to the effect that $[{}^+E_n : {}^+C_n]$ is finite and prime to p, and have proved the p-part of the class number formula (I) by purely algebraic deduction.

Massachusetts Institute of Technology

27) See [6].

Bibliography

[1] E. Artin, Algebraic numbers and algebraic functions, Lecture notes at Princeton Univ., 1950–1951.

[2] E. Artin und H. Hasse, Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln, Abh. Math. Sem. Univ. Hamburg, 6 (1928), 146–162.

[3] E. Artin and J. Tate, Class field theory, Lecture notes at Princeton Univ., 1951–1952.

[4] H. Hasse, Bericht über die neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, I, Ia, II, Leipzig und Berlin, 1930.

[5] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Berlin, 1952.

[6] K. Iwasawa, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg, 20 (1956), 257–258.

[7] K. Iwasawa, On some invariants of cyclotomic fields, Amer. J. Math., 80 (1958), 773–783.

[8] K. Iwasawa, On some properties of Γ-finite modules, Ann. of Math., 70 (1959), 291–312.

[9] K. Iwasawa, On the theory of cyclotomic fields. Ann. of Math., 70 (1959), 530–561.

[10] K. Iwasawa, A class number formula for cyclotomic fields, Ann. of Math., 76 (1962), 171–179.

[11] J.-P. Serre, Classes des corps cyclotomiques, Seminaire Bourbaki, Exposé 174 (1958/1959).