COMPOSITIO MATHEMATICA

KUNIAKI HORIE

CM-fields with all roots of unity

Compositio Mathematica, tome 74, nº 1 (1990), p. 1-14
<http://www.numdam.org/item?id=CM_1990__74_1_1_0>

Compositio Mathematica **74**: 1–14, 1990.

CM-fields with all roots of unity

KUNIAKI HORIE
Department of Mathematics (Kyoyobu), Yamaguchi University, Yoshida, Yamaguchi 753, Japan

Received 22 May 1989; accepted 23 August 1989

Let $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$, and $\mathbb{P}$ be the rational number field, the rational integer ring, the set of positive integers, and that of prime numbers, respectively. For each $p \in \mathbb{P}$, let $\mathbb{Q}_p$ denote the p-adic number field and $\mathbb{Z}_p$ the p-adic integer ring. We denote by $\hat{\mathbb{Z}}$ the direct product of all $\mathbb{Z}_p$, $p \in \mathbb{P}$:

$$\hat{\mathbb{Z}} = \prod_{p \in \mathbb{P}} \mathbb{Z}_p.$$

Let $\mathbb{N}'$ denote the set of at most countable cardinal numbers. Writing ∞ for the countable cardinal number, we then understand that $\mathbb{N}' = \mathbb{N} \cup \{0, \infty\}$. The additive group of each topological ring R will be denoted by the same letter R; for any $v \in \mathbb{N}'$, we let $\Pi^v R$ and $\oplus^v R$ denote respectively the direct product and the direct sum of v copies of R. Now, let $\mathbb{C}$ be the complex number field, j the complex conjugation of $\mathbb{C}$, and J the Galois group of $\mathbb{C}$ over the real number field; $J = \{1, j\}$. For any (multiplicative) abelian group $\mathfrak{M}$ acted on by J, we put

$$\mathfrak{M}^- = \{\tau \in \mathfrak{M} \mid \tau^j = \tau^{-1}\}.$$

Then, viewing $\mathfrak{M}$ as a module over the group ring $\mathbb{Z}[J]$, we have $(\mathfrak{M}^-)^2 \subseteq \mathfrak{M}^{1-j} \subseteq \mathfrak{M}^-$. We shall suppose, throughout the following, all algebraic number fields to be contained in $\mathbb{C}$. For each algebraic number field F, let C_F denote the ideal class group of F, $\tilde{F}$ the maximal unramified abelian extension over F, and F^+ the maximal real subfield of F. In general, C_F is isomorphic to a subgroup of $\oplus^\infty(\mathbb{Q}/\mathbb{Z})$ while the Galois group $G(\tilde{F}/F)$ of $\tilde{F}/F$ is isomorphic to a topological quotient group of (the additive group of) $\Pi^\infty \hat{\mathbb{Z}}$; hereafter $G(\ )$ will denote the Galois group of the Galois extension in the parenthesis. When F is a CM-field, J acts on C_F and on $G(\tilde{F}/F)$ in the usual manner. We denote by $\mathbb{K}$ the maximal CM-field, so that $\mathbb{K}^+$ is nothing but the maximal totally real algebraic number field. We put

$$\zeta_n = e^{2\pi i/n} \quad \text{for each } n \in \mathbb{N}.$$

As is well known, the maximal abelian extension over $\mathbb{Q}$, which we denote by $\mathbb{Q}_{ab}$, is generated by all ζ_n, $n \in \mathbb{N}$, over $\mathbb{Q}$:

$$\mathbb{Q}_{ab} = \mathbb{Q}(\zeta_n \mid n \in \mathbb{N}).$$

In this paper, introducing first the notion of "wild extension", we shall generalize some results of Uchida [9] on unramified solvable extensions of algebraic number fields. We shall next show that for any CM-field K containing $\mathbb{Q}_{ab}$,

$$G(\tilde{K}/K) \cong \prod^{\infty} \hat{\mathbb{Z}} = \prod_{p \in \mathbb{P}} \left(\prod^{\infty} \mathbb{Z}_p \right) \quad \text{and} \quad G(\tilde{K}/K)^- \cong \prod^{\infty} \hat{\mathbb{Z}}.$$

On the other hand, we shall deduce from the above generalization that, given any map $f: \mathbb{P} \to \mathbb{N}'$, there exist infinitely many CM-fields $K \supseteq \mathbb{Q}_{ab}$ such that

$$C_K = C_K^- \cong \bigoplus_{p \in \mathbb{P}} \left(\bigoplus^{f(p)} (\mathbb{Q}_p/\mathbb{Z}_p) \right).$$

Moreover some related results, such as the following, will be added: $C_{\mathbb{K}} = C_{\mathbb{K}}^- = \{1\}$ (cf. [6]) while

$$C_K \cong \bigoplus^{\infty} (\mathbb{Q}/\mathbb{Z}), \quad (C_K^-)^2 = C_K^{1-j} \cong \bigoplus^{\infty} (\mathbb{Q}/\mathbb{Z})$$

for every CM-field $K \supseteq \mathbb{Q}_{ab}$ which is contained in a nilpotent extension over some finite algebraic number field in K^+ (cf. [1]). In the last part of the paper, we shall unite our results on wild extensions with classical results of Iwasawa [3] on solvable extensions.

We conclude this introduction by giving additional notations and remarks. Let F be any algebraic number field and let I_F denote the ideal group of F. An ideal of F, i.e., an element of I_F is considered to be an ideal of any algebraic number field F' containing F via the natural imbedding of I_F into the ideal group of F'. For each algebraic number $\alpha \neq 0$ (in $\mathbb{C}$), the principal ideal of $\mathbb{Q}(\alpha)$ generated by α is a principal ideal of any algebraic number field containing α, in the above sense, and will be denoted by (α). We shall write $F^\times$ for the multiplicative group of F. Throughout the paper, we shall often use basic facts in [8] on Galois cohomology, without mentioning this bibliography.

Acknowledgement

The author would like to express his sincere gratitude to Professor Yuji Kida for helpful conversations and for kindly teaching the author his unpublished results.

1. Let k be any algebraic number field. An algebraic extension K over k is called wild when K/k is a Galois extension, every infinite prime of k is unramified in K, and for each finite prime $\mathfrak{P}$ of K, the inertia group of $\mathfrak{P}$ for K/k coincides with the ramification group of $\mathfrak{P}$ for K/k. As easily seen from this definition, the following lemma holds.

LEMMA 1. *With k as above, let $\mathfrak{s}$ be a set of finite primes of k and $\mathscr{F}$ a family of algebraic extensions over k. If all fields in $\mathscr{F}$ are wild extensions over k unramified outside $\mathfrak{s}$, then the composite of fields in $\mathscr{F}$ is also a wild extension over k unramified outside $\mathfrak{s}$.*

Thus, given a set $\mathfrak{s}$ of finite primes of an algebraic number field k, there exists the maximal wild extension over k unramified outside $\mathfrak{s}$. We then denote by $k^{\mathfrak{s}}_{\mathrm{ws}}$ the intersection of this field and the maximal solvable extension over k: $k^{\mathfrak{s}}_{\mathrm{ws}}$ is nothing but the maximal wild solvable extension over k unramified outside $\mathfrak{s}$.

Next, for any positive integer m, we take the abelian extension

$$\mathfrak{C} = \mathbb{Q}(\zeta_q \mid q \in \mathbb{P}, \equiv 1 \ (\mathrm{mod}\, m))$$

over $\mathbb{Q}$, and denote by $\mathbb{Q}^{(m)}$ the minimal intermediate field of $\mathfrak{G}/\mathbb{Q}$ such that $G(\mathfrak{G}/\mathbb{Q}^{(m)})^m = \{1\}$:

$$\mathbb{Q}^{(m)} = \{\alpha \in \mathfrak{G} \mid \alpha^\sigma = \alpha \text{ for all } \sigma \in G(\mathfrak{G}/\mathbb{Q}) \text{ with } \sigma^m = 1\}.$$

Let us now prove

THEOREM 1. *Let F be an algebraic number field containing $\mathbb{Q}^{(m)}$ for some $m \in \mathbb{N}$ and let $\mathfrak{S}$ be a set of finite primes of F. Then the cohomological dimension of the Galois group of $F^{\mathfrak{S}}_{\mathrm{ws}}$ over F is at most equal to* 1:

$$\mathrm{cd}\, G(F^{\mathfrak{S}}_{\mathrm{ws}}/F) \leqslant 1.$$

Proof. Let p be any prime number, S the set of prime numbers obtained by restricting the primes in $\mathfrak{S}$ on $\mathbb{Q}$, and K an intermediate field of $F^{\mathfrak{S}}_{\mathrm{ws}}/F$ such that $G(F^{\mathfrak{S}}_{\mathrm{ws}}/K)$ is a Sylow p-subgroup of $G(F^{\mathfrak{S}}_{\mathrm{ws}}/F)$. It suffices to show that

$$\mathrm{cd}\, G(F^{\mathfrak{S}}_{\mathrm{ws}}/K) \leqslant 1. \tag{1}$$

However, in the case $p \notin S$, this follows immediately from Theorem 1 of [9].

Indeed $F_{ws}^{\mathfrak{S}}$ is then the maximal unramified p-extension over K and K contains $\mathbb{Q}^{(m)}$ by the assumption.

Assume now that $p \in S$. In this case, we can prove (1) by modifying the proof of Theorem 1 of [9], as follows. Let L be any finite Galois extension over K in $F_{ws}^{\mathfrak{S}}$. For simplicity, we put

$$\mathfrak{G} = G(L/K).$$

Let W_p denote the group of pth roots of unity in $\mathbb{C}$: $W_p = \langle \zeta_p \rangle \cong \mathbb{Z}/p\mathbb{Z}$. Let us identify $G(L(\zeta_p)/K(\zeta_p))$ with $\mathfrak{G}$ so that $\mathfrak{G}$ acts on $L(\zeta_p)^\times$ and, trivially, on W_p. Assuming that

$$H^2(\mathfrak{G}, W_p) \neq \{1\}, \quad \text{i.e.,} \quad \mathfrak{G} \neq \{1\},$$

we take any 2-cocycle $\delta: \mathfrak{G} \times \mathfrak{G} \to W_p$ whose cohomology class in $H^2(\mathfrak{G}, W_p)$ is not trivial. Let

$$\{1\} \to W_p \to \mathfrak{F} \xrightarrow{\psi} \mathfrak{G} \to \{1\}$$

be the group extension of $\mathfrak{G}$ by W_p corresponding to δ, with the natural projection $\psi: \mathfrak{F} \to \mathfrak{G}$. For the proof of (1), it is now sufficient to find a Galois extension L' over K containing L such that there exists a $\mathfrak{G}$-isomorphism $\iota: G(L'/K) \xrightarrow{\sim} \mathfrak{F}$ for which $\iota(G(L'/L)) = W_p$ and the composite $\psi \circ \iota$ coincides with the restriction map $G(L'/K) \to \mathfrak{G}$.

Since $K(\zeta_p) \supseteq F \supseteq \mathbb{Q}^{(m)}$, Lemma 1 of [9] implies that the local degree of $K(\zeta_p)/\mathbb{Q}$ at each finite prime of $K(\zeta_p)$ is divisible by p^∞. Furthermore all infinite primes of $K(\zeta_p)$ are unramified in $L(\zeta_p)$. Hence, as in the proof of Lemma 5 of [11], we obtain

$$H^2(\mathfrak{G}, L(\zeta_p)^\times) = \{1\}.$$

In particular, δ is considered to be a 2-coboundary $\mathfrak{G} \times \mathfrak{G} \to L(\zeta_p)^\times$, namely, there exists a homomorphism $\beta: \mathfrak{G} \to L(\zeta_p)^\times$ such that

$$\delta(\sigma, \tau) = \beta(\tau)^\sigma \beta(\sigma\tau)^{-1} \beta(\sigma), \quad \sigma, \tau \in \mathfrak{G}.$$

Here, since each $\delta(\sigma, \tau)$ is in W_p and, as is well known, $H^1(\mathfrak{G}, L(\zeta_p)^\times) = \{1\}$, there also exists an element η of $L(\zeta_p)^\times$ such that

$$\beta(\sigma)^p = \eta^{\sigma - 1} \quad \text{for all } \sigma \in \mathfrak{G}.$$

Let $n = [L(\zeta_p):L]$, let ρ be a generator of the cyclic group $G(L(\zeta_p)/L)$, and choose an integer r satisfying

$$\zeta_p^\rho = \zeta_p^r, \quad r^n \equiv 1 \pmod p, \quad r^n \not\equiv 1 \pmod p.$$

The group ring $\mathbb{Z}[G(L(\zeta_p)/L)]$ acts on $L(\zeta_p)^\times$ in the obvious manner. By Lemma 2 of [9], we may assume that

$$\eta = \omega^\theta \xi^p \quad \text{for suitable } \omega, \xi \in L(\zeta_p)^\times,$$

where θ is the element of $\mathbb{Z}[G(L(\zeta_p)/L)]$ defined by

$$\theta = \sum_{\nu=0}^{n-1} r^{n-\nu} \rho^\nu.$$

Let m_0 denote the product of distinct prime divisors of m different from p. As K contains $\mathbb{Q}^{(m)}$, there exists a Galois extension L_0/K_0 of finite algebraic number fields with the following properties:

(i) $L_0 \cap K = K_0, \quad L_0 K = L, \quad [L_0(\zeta_p):L_0] = n,$

(ii) L_0 is unramified over K_0 outside p; further, all prime ideals of K_0 dividing m_0 are completely decomposed in L_0,

(iii) η, ω, ξ, and all $\beta(\sigma)$, $\sigma \in \mathfrak{G}$, lie in $L_0(\zeta_p)$.

By (ii) above, the approximation theorem guarantees the existence of an element a of $K_0(\zeta_p)^\times$ such that, for each prime ideal $\mathfrak{v}$ of $K_0(\zeta_p)$ dividing m_0, ω/a is a pth power in the $\mathfrak{v}$-adic completion of $K_0(\xi_p)$ and $\mathfrak{w}(\omega/a) > 0$ for every real archimedian valuation $\mathfrak{w}$ of $L_0(\zeta_p)$. Then the same discussion as in page 314 of [9] shows that the principal ideal $(\eta a^{-\theta})$ is expressed in the form

$$(\eta a^{-\theta}) = \mathfrak{n}^\theta \mathfrak{a}^p \mathfrak{b}.$$

Here $\mathfrak{n}$ is an ideal of $K_0(\zeta_p)$ prime to mp, $\mathfrak{a}$ an ideal of $L_0(\zeta_p)$ prime to p, and $\mathfrak{b}$ that of $L_0(\zeta_p)$ whose numerator and denominator are products of prime ideals of $L_0(\zeta_p)$ dividing p. With t the order of the Frobenius automorphism

$$\left(\frac{K_0(\zeta_{mp})/K_0(\zeta_p)}{\mathfrak{n}}\right),$$

let K_1 be an extension of degree t over K_0 contained in K. By the Tschebotareff density theorem, there exists a prime ideal $\mathfrak{q}$ of $K_1(\zeta_p)$ unramified for $K_1(\zeta_p)/\mathbb{Q}$, of degree 1 over $\mathbb{Q}$, and belonging to the class of $\mathfrak{n}$ in the ray class group of $K_1(\zeta_p)$ modulo $(mp)\mathfrak{r}_\infty$ where $\mathfrak{r}_\infty$ is the product of all real infinite primes of $K_1(\zeta_p)$. It follows that $\mathfrak{q}\mathfrak{n}^{-1} = (b)$ for some $b \in K_1(\zeta_p)$ with $b \equiv 1 \pmod{(mp)\mathfrak{r}_\infty}$. The field $L(\zeta_p, \sqrt[p]{\eta a^{-\theta} b^{\theta}}) = L(\zeta_p, \sqrt[p]{(\omega a^{-1} b)^{\theta}})$ is then an abelian extension of degree np over L. Furthermore the cyclic extension of degree p over L in that field becoms a Galois extension over K, which can be taken as the before-mentioned field L'. To prove this final assertion, one may only check the last part of the proof of Theorem 1 in [9]; so we omit the detail.

For any algebraic number field k, let k_{nil} denote the maximal nilpotent extension over k. The proof of Theorem 2 in [9], together with the above theorem, yields the following result.

THEOREM 2. *Let F be an algebraic number field such that*

$$\mathbb{Q}^{(m)} \subseteq F \subseteq k_{\mathrm{nil}}$$

for some positive integer m and some finite algebraic number field k in F. Let $\mathfrak{S}$ be a set of finite primes of F. Then $G(F^{\mathfrak{S}}_{\mathrm{ws}}/F)$ is isomorphic to the solvable completion of a free group with countable free generators.

Finally we add a result which follows immediately from the definition of a wild extension.

LEMMA 2. *Let k be an algebraic number field and $\mathfrak{s}$ a set of finite primes of k. Then:*
(i) *for any intermediate field F of $k^{\mathfrak{s}}_{\mathrm{ws}}/k$,*

$$F^{\mathfrak{S}}_{\mathrm{ws}} = k^{\mathfrak{s}}_{\mathrm{ws}}$$

where $\mathfrak{S}$ is the set of all primes of F lying above primes in $\mathfrak{s}$,
(ii) *if k is totally real, then so is $k^{\mathfrak{s}}_{\mathrm{ws}}$.*

2. For any multiplicative abelian group M on which J acts, we let

$$\mathfrak{M}^{+} = \{\tau \in \mathfrak{M} \mid \tau^{j} = \tau\},$$

so that $(\mathfrak{M}^{+})^2 \subseteq \mathfrak{M}^{1+j} \subseteq \mathfrak{M}^{+}$, $\mathfrak{M}^{1+j} \cong \mathfrak{M}/\mathfrak{M}^{-}$ and $\mathfrak{M}^{1-j} \cong \mathfrak{M}/\mathfrak{M}^{+}$. The purpose of this section is to prove the following.

THEOREM 3. *Let K be any CM-field containing $\mathbb{Q}_{\mathrm{ab}}$. Then, as profinite groups,*

$$G(\tilde{K}/K)^{-} \cong \prod^{\infty} \hat{\mathbb{Z}}, \quad G(\tilde{K}/K) \cong \prod^{\infty} \hat{\mathbb{Z}}.$$

Furthermore

$$G(\tilde{K}/K)^{+} \cong \prod^{\infty} \hat{\mathbb{Z}}$$

if K is contained in k_{nil} for some finite algebraic number field k in K^+.

For the proof of the above, we need

LEMMA 3. *Let L be a* CM-*field. Then*
(i) $G(\tilde{L}/L)^- \supseteq G(\tilde{L}/\tilde{L}\cap\mathbb{K}) \supseteq G(\tilde{L}/L)^{1-j}$,
(ii) *for any* CM-*field $L' \supseteq L$, $G(\tilde{L}/L)^{1-j}$ is contained in the image of $G(\widetilde{L'}/L')^-$ under the restriction map $G(\widetilde{L'}/L') \to G(\tilde{L}/L)$.*

Proof. Let F be any CM-field in L of finite degree. Since C_F^- contains the kernel of the norm map $C_F \to C_{F^+}$, it follows from class field theory that $G(\tilde{F}/F)^-$ contains $G(\tilde{F}/F\widetilde{F^+})$, the kernel of the restriction map $G(\tilde{F}/F) \to G(\widetilde{F^+}/F^+)$. Thus we have $G(\tilde{L}/L)^- \supseteq G(\tilde{L}/L\widetilde{L^+})$, which implies $G(\tilde{L}/L)^- \supseteq G(\tilde{L}/\tilde{L}\cap\mathbb{K})$ by $L\widetilde{L^+} \subseteq \tilde{L}\cap\mathbb{K}$. Furthermore, since $\tilde{L}\cap\mathbb{K}$ is a CM-field and an abelian extension over L, it is also an abelian extension over L^+ so that $G(\tilde{L}/\tilde{L}\cap\mathbb{K}) \supseteq G(\tilde{L}/L)^{1-j}$. This completes the proof of (i). We obtain (ii) from (i), noting that the restriction max in (ii) induces a surjective homomorphism $G(\widetilde{L'}/\widetilde{L'}\cap\mathbb{K}) \to G(\tilde{L}/\tilde{L}\cap\mathbb{K})$.

Proof of Theorem 3. Let A be any non-trivial finite abelian group. We can then take a cyclotomic field F such that $G(\tilde{F}/F)^{1-j}$ has a subgroup isomorphic to A (see, e.g., [2]). Hence it follows from Lemma 3 that there exists a group homomorphism of $G(\tilde{K}/K)^-$ onto A. On the other hand, $G(\tilde{K}/K)^-$ is torsion-free since so is $G(\tilde{K}/K)$ by Theorem 1 of [9]. Consequently

$$G(\tilde{K}/K)^- \cong \prod^{\infty} \hat{\mathbb{Z}}, \quad G(\tilde{K}/K) \cong \prod^{\infty} \hat{\mathbb{Z}}.$$

As K^+ includes $\mathbb{Q}^{(2)}$ and $G(\widetilde{K^+}/K^+)^2$ is the image of $G(\tilde{K}/K)^{1+j}$ under the restriction map $G(\tilde{K}/K) \to G(\widetilde{K^+}/K^+)$, the last assertion of Theorem 3 is now an immediate consequence of Theorem 2 in [9].

3. The main result of the present section is as follows.

THEOREM 4. *For any given map $f\colon \mathbb{P} \to \mathbb{N}'$, there exist infinitely many* CM-*fields K containing $\mathbb{Q}_{\mathrm{ab}}$ such that*

$$C_K = C_K^- \cong \bigoplus_{p\in\mathbb{P}} \left(\bigoplus^{f(p)} (\mathbb{Q}_p/\mathbb{Z}_p) \right).$$

To prove this, we prepare some notations and show two lemmas.

Let F be any algebraic number field. We then denote by F_{ws} the maximal wild solvable extension over F, namely, put

$$F_{\mathrm{ws}} = F_{\mathrm{ws}}^{\mathfrak{U}}$$

where $\mathfrak{U}$ is the set of all finite primes of F. We denote by M_F the maximal abelian extension over F in F_{ws}. For each $p \in \mathbb{P}$, let $C_F(p)$ and $M_{F,p}$ denote respectively the p-primary component of C_F and the maximal p-extension over F in M_F, i.e., the maximal abelian p-extension over F unramified outside p; so that if F is a CM-field, $C_F(p)$ and $G(M_{F,p}/F)$, as well as $G(M_F/F)$, naturally become J-modules. Here, by a J-module, we mean of course an abelian group on which J acts. For any profinite group H, we let H^{ab} denote the maximal abelian quotient of H, i.e., the quotient group of H modulo the topological commutator subgroup of H. When H itself is a profinite abelian group, we let H^* denote the Pontryagin dual of H.

LEMMA 4. *Let p be any prime number. Let K be a* CM*-field containing* $\mathbb{Q}^{(m)}$ *for* some $m \in \mathbb{N}$ *and* $\mathbb{Q}(\zeta_{p^n})$ *for all* $n \in \mathbb{N}$. *Then* $C_K(p)$ *is a divisible group and, as discrete groups,*

$$(C_K(p)^-)^2 = C_K(p)^{1-j} \cong G(M_{K^+,p}/K^+)^*.$$

Proof. It is obvious that $G(M_{K,p}/K)$ is isomorphic to the Sylow p-subgroup of $G(K_{ws}/K)^{\mathrm{ab}}$. However, since $K \supseteq \mathbb{Q}^{(m)}$ with $m \in \mathbb{N}$, Theorem 1 implies that $\mathrm{cd}\, G(K_{ws}/K) \leqslant 1$. Therefore $G(M_{K,p}/K)$ becomes a torsion-free $\mathbb{Z}_p$-module. Similarly, noticing $K^+ \supseteq \mathbb{Q}^{(2m)}$, we can see again from Theorem 1 that $G(M_{K^+,p}/K^+)$ is a torsion-free $\mathbb{Z}_p$-module.

The rest of the proof is devoted to essentially known discussions on the Kummer extension $M_{K,p}$ over K (cf. [5]). We let $\mathfrak{R}$ denote the quotient of the subgroup

$$\{\alpha \in M_{K,p} \mid \alpha^{p^n} \in K^\times \text{ for some integer } n \geqslant 0\}$$

of $M_{K,p}^\times$ modulo $K^\times$, which becomes a J-module in the obvious manner. Let L be the maximal abelian extension over K^+ in $M_{K,p}$, namely, the intermediate field of $M_{K,p}/K$ such that $G(M_{K,p}/L) = G(M_{K,p}/K)^{1-j}$. Then the natural isomorphism $\mathfrak{R} \xrightarrow{\sim} G(M_{K,p}/K)^*$ in Kummer theory induces

$$\mathfrak{R}^- \cong (G(M_{K,p}/K)/G(M_{K,p}/K)^{1-j})^* \cong G(L^+/K^+)^*.$$

Here $\mathfrak{R}$ is a divisible group; indeed we have shown that $G(M_{K,p}/K)$ is a torsion-free $\mathbb{Z}_p$-module. Hence

$$\mathfrak{R}^{1-i} = (\mathfrak{R}^-)^2 \cong (G(L^+/K^+)^*)^2. \tag{2}$$

Now let z be any class in $\mathfrak{R}$. We take an element α of z, so that $\alpha^{p^r} \in K^\times$ for some integer $r \geqslant 0$. Since all $\mathbb{Q}(\alpha^{p^r}, \zeta_{p^n})$, $n \in \mathbb{N}$, are subfields of K, there exists an intermediate field k of $K/\mathbb{Q}(\alpha^{p^r}, \zeta_{p^r})$ with finite degree such that $k(\alpha)$ is unramified over k outside p and that each prime ideal of $\mathbb{Q}(\alpha^{p^r})$ dividing p is a p^rth power in the ideal group I_k of k. Therefore

$$(\alpha^{p^r}) = \mathfrak{a}^{p^r} \quad \text{for some } \mathfrak{a} \in I_K.$$

We then denote by c_z the ideal class in $C_K(p)$ containing $\mathfrak{a}$, which actually does not depend on the choice of α, $\mathfrak{a}$.

Thus, letting each class z' in $\mathfrak{K}$ correspond to $c_{z'}$, we obtain a J-module homomorphism $\mathfrak{K} \to C_K(p)$. Let E denote the unit group of K and define a J-module $\mathfrak{E}$ by

$$\mathfrak{E} = \{\alpha \in M_{K,p} \mid \alpha^{p^n} \in E \text{ for some } n \in \mathbb{Z}, \geqslant 0\}/E.$$

As easily seen, the above homomorphism induces the following exact sequence of J-modules:

$$\{1\} \to \mathfrak{E} \to \mathfrak{K} \to C_K(p) \to \{1\}. \tag{3}$$

In particular, it follows that $C_K(p)$ is a divisible group, whence

$$(C_K(p)^-)^2 = C_K(p)^{1-j}. \tag{4}$$

We also have

$$(\mathfrak{E}^-)^2 = \mathfrak{E}^{1-j} = \{1\}, \tag{5}$$

because the group of roots of unity in K is p-divisible. Therefore, in the case $p > 2$, the last assertion $C_K(p)^{1-j} \cong G(M_{K^+,p}/K^+)^*$ follows from (2), (3), (5), and the fact $L^+ = M_{K^+,p}$.

In the case $p = 2$, L is the maximal abelian 2-extension over K^+ unramified outside the primes of K^+ which are infinite or lie above 2. Hence L^+ is an abelian extension over $M_{K^+,2}$ such that $G(L^+/M_{K^+,2})^2 = \{1\}$. We can therefore view $G(M_{K^+,2}/K^+)^*$ as a subgroup of $G(L^+/K^+)^*$ containing $(G(L^+/K^+)^*)^2$. However $G(M_{K^+,2}/K^+)^*$ is a divisible group and, by (2), so is $(G(L^+/K^+)^*)^2$. Consequently we have $G(M_{K^+,2}/K^+)^* = (G(L^+/K^+)^*)^2$. This together with (2), (3), (4), and (5) completes the proof of Lemma 4 for the case $p = 2$.

The following lemma is an immediate consequence of Lemma 4.

LEMMA 5. *For any* CM-*field* $K \supseteq \mathbb{Q}_{\mathrm{ab}}$, C_K *is divisible and*

$$(C_K^-)^2 = C_K^{1-j} \cong G(M_{K^+}/K^+)^*.$$

Proof of Theorem 4. Let F be any totally real finite Galois extension over $(\mathbb{Q}_{ab})^+$ such that $G(F/(\mathbb{Q}_{ab})^+)$ is isomorphic to a non-abelian simple group; for example, we may take as F a composite field of $(\mathbb{Q}_{ab})^+$ and a finite real Galois extension over $\mathbb{Q}$ with Galois group a symmetric group of degree $\geqslant 5$. Since $\mathbb{Q}^{(2)} \subseteq F \subseteq \mathbb{Q}(\alpha)_{nil}$ for any primitive element α of $F/(\mathbb{Q}_{ab})^+$, Theorem 2 implies that $G(F_{ws}/F)$ is isomorphic to a free pro-solvable group with countable free generators.

Next, let p be any prime number and T an inertia group for F_{ws}/F of a prime of F_{ws} lying above p. As every Sylow p-subgroup of $G(F_{ws}/F)$ is free, T is a free pro-p-group. With n being any positive integer, let q be a prime number $\equiv 1$ (mod p^n) such that p is not a pth power (mod q); the existence of q is guaranteed by Tschebotareff's density theorem. Let N be the cyclic extension of degree p over $\mathbb{Q}$ with conductor q. We note that p remains prime in N. Let N_∞ denote the basic $\mathbb{Z}_p$-extension over N. It then follows from [4] that the unique prime of N_∞ above p is fully ramified in $M_{N_\infty,p}$. Furthermore, by [10], $G(M_{N_\infty,p}/N)$ is isomorphic to $\Pi^r\, \mathbb{Z}_p$ where

$$r = (p-1)\left(\mathrm{ord}_p \frac{q^{2(p-1)}-1}{4} - 2\right) \geqslant (p-1)(n-3),$$

ord_p denoting the p-adic exponential valuation. Hence T has at least r free generators, while n is an arbitrary positive integer. Thus T must be a free pro-p-group with countable free generators.

Now, let f be any map $\mathbb{P} \to \mathbb{N}'$. By the above discussion, we can take for each $p \in \mathbb{P}$, an intermediate field F_p of F_{ws}/F such that $G(F_{ws}/F_p)$ is contained in an inertia group, for F_{ws}/F, of a prime of F_{ws} above p and has exactly $f(p)$ free generators as a free pro-p-group. Let K be the composite of $\mathbb{Q}_{ab}$ and the intersection of all F_p, $p \in \mathbb{P}$. It is clear that

$$K \subseteq \mathbb{K}, \quad K^+ = \bigcap_{p \in \mathbb{P}} F_p.$$

However, as $\widetilde{K^+} \subseteq F_p$ for all $p \in \mathbb{P}$, we have $\widetilde{K^+} = K^+$. Therefore we see easily from the principal ideal theorem that

$$C_{K^+} = \{1\} \quad \text{whence} \quad C_K = C_K^-. \tag{6}$$

On the other hand, it follows from the choices of F_p, $p \in \mathbb{P}$, that

$$G(F_{ws}/K^+)^{ab} \cong \prod_{p \in \mathbb{P}} \left(\prod^{f(p)} \mathbb{Z}_p \right).$$

Since $(K^+)_{ws} = F_{ws}$ by Lemma 2, we also have $G(M_{K^+}/K^+) \cong G(F_{ws}/K^+)^{ab}$. Hence, by Lemma 5 and (6),

$$C_K = (C_K^-)^2 \cong (G(F_{ws}/K^+)^{ab})^* \cong \bigoplus_{p \in \mathbb{P}} \left(\bigoplus^{f(p)} (\mathbb{Q}_p/\mathbb{Z}_p) \right).$$

Furthermore, for any finite Galois extension F' over $(\mathbb{Q}_{ab})^+$ in $\mathbb{K}^+$ with $G(F'/(\mathbb{Q}_{ab})^+)$ a non-abelian simple group, the composite $F'_{ws}\mathbb{Q}_{ab}$ contains K if and only if $F' = F$. Theorem 4 is therefore proved.

Of course, for CM-fields containing $\mathbb{Q}_{ab}$ but not "so large", we can get a result analogous to that of Brumer [1].

PROPOSITION 1. *Let K be a CM-field containing $\mathbb{Q}_{ab}$ such that $K \subseteq k_{nil}$ for some finite algebraic number field k in K^+. Then $(C_K^-)^2 = C_K^{1-j}$ is isomorphic to the direct sum of countably infinite copies of $\mathbb{Q}/\mathbb{Z}$.*

Proof. This follows immediately from Theorem 2 and Lemma 5.

REMARK. Under the hypothesis of Proposition 1, we also have

$$C_K \cong \bigoplus^{\infty} (\mathbb{Q}/\mathbb{Z}).$$

Moreover it might be remarkable that $C_F^+ = C_{F^+} = \{1\}$ holds for every CM-field $F \supseteq \mathbb{Q}_{ab}$ if the so-called Greenberg conjecture in Iwasawa theory is generally true.

We next consider when the ideal class group of a CM-field $\supseteq \mathbb{Q}_{ab}$ vanishes.

LEMMA 6. *Let p and K be the same as in Lemma 4. Then the three conditions $C_K(p) = \{1\}$, $C_K(p)^- = \{1\}$, and $M_{K^+,p} = K^+$ are equivalent.*

Proof. By Lemma 4, the condition $M_{K^+,p} = K^+$ is a necessary one for $C_K(p)^- = \{1\}$. So it suffices to prove that $M_{K^+,p} = K^+$ implies $C_K(p) = \{1\}$. The principal ideal theorem shows, however, that $C_{K^+}(p) = \{1\}$ holds if K^+ coincides with the maximal unramified abelian p-extention over K^+. Hence, in the case $M_{K^+,p} = K^+$, we certainly have $C_{K^+}(p) = \{1\}$ so that $C_K(p) = C_K(p)^-$. We have further, by Lemma 4, $C_K(p)^2 = C_K(p)$ and $(C_K(p)^-)^2 = \{1\}$. Then $C_K(p)$ vanishes as desired.

We thus obtain

PROPOSITION 2. *For any CM-field $K \supseteq \mathbb{Q}_{ab}$, the following conditions are equivalent.*

(i) $C_K = \{1\}$,

(ii) $C_K^- = \{1\}$,

(iii) $M_{K^+} = K^+$,

(iv) $(K^+)_{ws} = K^+$,

(v) $K^+ = k_{ws}$ for some subfield k of $\mathbb{K}^+$.

In particular, $C_{\mathbb{K}} = \{1\}$ (cf. [6]).

4. In this final section, we generalize some results of the preceding sections.

Let F be any algebraic number field, $\mathfrak{T}$ a set of finite primes of F, and $\mathfrak{S}$ a subset of $\mathfrak{T}$. We take the family $\mathscr{G}$ of all Galois extensions F' over F unramified outside $\mathfrak{T}$ such that for each prime $\mathfrak{B}$ of F' whose restriction on F lies in $\mathfrak{S}$, the first ramification field of $\mathfrak{B}$ for F'/F coincides with the inertia field of $\mathfrak{B}$ for F'/F. Let $\Omega_F^{\mathfrak{S},\mathfrak{T}}$ denote the composite of all fields in $\mathscr{G}$. Then, as easily seen, $\Omega_F^{\mathfrak{S},\mathfrak{T}}$ also belongs to $\mathscr{G}$, i.e., $\Omega_F^{\mathfrak{S},\mathfrak{T}}$ is the maximal field in $\mathscr{G}$. We denote by $F_{\mathrm{sol}}^{\mathfrak{S},\mathfrak{T}}$ the intersection of $\Omega_F^{\mathfrak{S},\mathfrak{T}}$ and the maximal solvable extension over F. Note that $F_{\mathrm{sol}}^{\mathfrak{S},\mathfrak{S}} = F_{\mathrm{ws}}^{\mathfrak{S}}$. The discussions of [9] and section 1 now lead us to the following result, which implies Theorems 6, 7 of [3] as well as our Theorems 1, 2.

THEOREM 5. *If* $F \supseteq \mathbb{Q}^{(m)}$ *for some* $m \in \mathbb{N}$, *then*

$$\operatorname{cd} G(\Omega_F^{\mathfrak{S},\mathfrak{T}}/F) \leqslant 1, \quad \operatorname{cd} G(F_{\mathrm{sol}}^{\mathfrak{S},\mathfrak{T}}/F) \leqslant 1.$$

If, furthermore, $F \subseteq k_{\mathrm{nil}}$ *for some finite algebraic number field* k in F, then $G(F_{\mathrm{sol}}^{\mathfrak{S},\mathfrak{T}}/F)$ *is isomorphic to a free pro-solvable group with countable free generators.*

To weaken lastly the hypothesis of Proposition 1, we start with proving

PROPOSITION 3. *Let* F *be an algebraic number field containing* $\mathbb{Q}^{(m)}$ *for some* $m \in \mathbb{N}$. *Then* C_F *is a divisible group.*

Proof (cf. [1]). Let n be any positive integer and c any ideal class in C_F. It suffices to show that

$$x^n = c \quad \text{for some} \quad x \in C_F. \tag{7}$$

We write u for the order of c. Now there exists an element α of $\mathbb{Q}(\zeta_{mn})$ satisfying $F(\alpha) = F(\zeta_{mn}) \cap \tilde{F}$. There also exists an intermediate field k of $F/F \cap \mathbb{Q}(\zeta_{mn})$ with finite degree such that c contains an ideal $\mathfrak{a}$ of k whose uth power is principal in k and that α lies in $\tilde{k}$ whence $k(\alpha) = \tilde{k} \cap k(\zeta_{mn})$. Let q be a prime number $\equiv 1 \pmod{mu}$ not dividing the discriminant of k. Let k' be the composite of k and the cyclic extension of degree u over $\mathbb{Q}$ with conductor q. Note that F contains k'. Obviously the norm of $\mathfrak{a}$ for k'/k is $\mathfrak{a}^u$, a principal ideal of k. Hence, by class field theory, we have

$$\left(\frac{\tilde{k}'/k'}{\mathfrak{a}}\right) \in G(\tilde{k}'/k'\tilde{k}).$$

Since $\tilde{k}' \cap k'(\zeta_{mn}) = k'(\alpha) = k'(\tilde{k} \cap k(\zeta_{mn})) \subseteq k'\tilde{k}$, Tschebotareff's density theorem shows that there exists a prime ideal $\mathfrak{J}$ of k' unramified for $k'/\mathbb{Q}$, of degree 1 over $\mathbb{Q}$, belonging to the ideal class of $\mathfrak{a}$ in $C_{k'}$, and completely decomposed in $k'(\zeta_{mn})$. Let l be the prime number divisible by $\mathfrak{J}$, so that $l \equiv 1 \pmod{mn}$. Let k'' be the composite of k' and the cyclic extension of degree n over $\mathbb{Q}$ with conductor l. As k'' is an intermediate field of F/k' of degree n over k' in which $\mathfrak{J}$ is fully ramified, we can then take, as x of (7), the ideal class in C_F that contains the prime ideal of k'' dividing $\mathfrak{J}$.

THEOREM 6. *Let K be a* CM-*field such that*

$$\mathbb{Q}(\zeta_{2p} \mid p \in \mathbb{P}) \subseteq K \subseteq k_{\text{nil}}$$

with a subfield k of K^+ of finite degree. Then

$$(C_K^-)^2 = C_K^{1-j} \cong \bigoplus^{\infty} (\mathbb{Q}/\mathbb{Z}), \quad C_K \cong \bigoplus^{\infty} (\mathbb{Q}/\mathbb{Z}).$$

Proof. Let L be the composite of the maximal unramified Kummer extensions of exponents $2p$ over K for all $p \in \mathbb{P}$. Let E denote the unit group of K and E' the subgroup of $L^\times$ generated by the $2p$th roots in $L^\times$ of elements of E for all $p \in \mathbb{P}$. As J acts on $G(L/K)$ and on the quotient group E'/E in the obvious manner, we obtain from Kummer theory the following exact sequence of J-modules:

$$\{1\} \to E'/E \to G(L/K)^* \to C_K$$

(see the proof of Lemma 3 in [1] or of Lemma 4). This induces an exact sequence

$$\{1\} \to (E'/E)^- \to G(L_0/K^+)^* \to C_K^-,$$

where L_0 denotes the maximal abelian extension over K^+ in L^+. However, $((E'/E)^-)^2 \subseteq (E'/E)^{1-j} \subseteq WE/E$ with W the group of roots of unity in L while L_0 contains all unramified abelian extensions of degrees $2p$, $p \in \mathbb{P}$, over the intermediate field K^+ of $k_{\text{nil}}/\mathbb{Q}^{(2)}$. Hence, by Theorem 2 of [9], C_K^- has a subgroup isomorphic to

$$\bigoplus_{p \in \mathbb{P}} \left(\bigoplus^{\infty} (\mathbb{Z}_p/2p\mathbb{Z}_p) \right).$$

Thus Proposition 3 completes the proof of Theorem 6.

References

[1] A. Brumer, The class group of all cyclotomic integers. *J. Pure Appl. Algebra* 20 (1981) 107–111.
[2] K. Horie, On Iwasawa λ^--invariants of imaginary abelian fields. *J. Number Theory* 27 (1987) 238–252.
[3] K. Iwasawa, On solvable extensions of algebraic number fields. *Ann. Math.* 58 (1953) 548–572.
[4] K. Iwasawa, A note on class numbers of algebraic number fields. *Abh. Math. Sem. Univ. Hamburg* 20 (1956) 257–258.
[5] K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields. *Ann. Math.* 98 (1973) 246–326.
[6] K. Iwasawa, Some remarks on Hecke characters. In: *Algebraic Number Theory* (Kyoto Int. Sympos., 1976), Tokyo, *Japanese Soc. Promotion Sci.*, 1977, pp. 99–108.
[7] K. Iwasawa, Riemann-Hurwitz formula and p-adic Galois representations for number fields. *Tôhoku Math. J.* 33 (1981) 263–288.
[8] J.-P. Serre, *Cohomologie galoisienne* (*Lect. Notes Math.*, vol. 5). Berlin, Springer, 1964.
[9] K. Uchida, Galois groups of unramified solvable extensions. *Tôhoku Math. J.* 34 (1982) 311–317.
[10] K. Wingberg, Duality theorems for Γ-extensions of algebraic number fields. *Comp. Math.* 55 (1985) 338–381.