ACTA ARITHMETICA
149.2 (2011)

On the depth of the relations of the maximal unramified pro-p Galois group over the cyclotomic $\mathbb{Z}_p$-extension

by

Satoshi Fujii (Yokohama)

1. Introduction. Let p be a prime number, $k/\mathbb{Q}$ a finite extension and k_∞/k the cyclotomic $\mathbb{Z}_p$-extension, where $\mathbb{Z}_p$ is the additive group of p-adic integers. Iwasawa-theoretical study of unramified pro-p extensions was developed by Ozaki [Oz2]. He proved a non-abelian Iwasawa class number formula, and therefore we are interested in the structure of the Galois group $G(k_\infty)$ of the maximal unramified pro-p extension $\mathfrak{L}(k_\infty)/k_\infty$. A basic question is: When does $G(k_\infty)$ have a simple structure? Especially, we want to study the cases where $G(k_\infty)$ is an abelian group or a non-abelian free pro-p group.

Mizusawa–Ozaki [MO] and Okano [Ok] characterized all imaginary quadratic fields k such that $G(k_\infty)$ is abelian via effective conditions. For the pth cyclotomic field $k = \mathbb{Q}(\mu_p)$, in the range of $1 < p < 1000$, Sharifi [S] also showed that $G(k_\infty)$ is abelian. Based on their results, it may be thought that the next step is to study number fields k such that $G(k_\infty)$ is a non-abelian free pro-p group. However, it seems that there is no concrete example of such a number field k yet. What is more, a number of mathematicians, including the author, suspect that $G(k_\infty)$ can never be a non-abelian free pro-p group. Recently, results which ensure the non-freeness of $G(k_\infty)$ have been obtained. Validire [V] gave a good criterion of the non-freeness of the Galois group of the maximal unramified pro-p extension of k_∞ which is completely decomposed at all primes above p by using the theory of wild étale kernels. Also in this article, for finite extensions $k/\mathbb{Q}$ such that the prime number p splits completely, we will show that Greenberg's generalized conjecture (see Conjecture 1.4 below) implies that the "derived depth" of $G(k_\infty)$ is not so large. Now we define the derived depth of pro-p groups. For a topological group G, let $G' = \overline{[G,G]}$ be the closure of the commutator group

2010 *Mathematics Subject Classification*: Primary 11R23.
Key words and phrases: unramified pro-p Galois groups, Greenberg's generalized conjecture, pseudo-null submodules.

DOI: 10.4064/aa149-2-1

of G. For a non-negative integer i, define $D_0(G) = G$, and $D_{i+1}(G) = D_i(G)'$ inductively.

Definition 1.1 (Derived depth). Let G be a pro-p group and

$$1 \to R \to F \to G \to 1$$

a minimal presentation of G by a free pro-p group F ("minimal" means that $H^1(G, \mathbb{Z}/p) \overset{\text{inf}}{\simeq} H^1(F, \mathbb{Z}/p)$). If there is a non-negative integer i such that $R \subseteq D_i(F)$ and $R \not\subseteq D_{i+1}(F)$, we say that the *derived depth* of G is i. The derived depths of the trivial group and of free pro-p groups are defined to be $-\infty$ and ∞ respectively.

For example, the derived depth of a non-trivial finitely generated free $\mathbb{Z}_p$-module M is ∞ or 1 according as $M \simeq \mathbb{Z}_p$ or not. Since a free pro-p group is a projective object in the category of pro-p groups and since $D_i(G)$ is stable under topological automorphisms for each non-negative integer i, the definition of the derived depth is independent of the choice of a minimal presentation. Note that if the derived depth of a pro-p group G is finite, then G is not a non-abelian free pro-p group. Our main result is as follows.

Main Theorem 1.2. *Let p be a prime number and $k/\mathbb{Q}$ a finite extension which is completely decomposed at p. If Greenberg's generalized conjecture holds for p and k, then the derived depth of $G(k_\infty)$ is at most* 1 *except for the case where $G(k_\infty) \simeq \mathbb{Z}_p$.*

As seen from the above results, it seems that $G(k_\infty)$ is far from being a non-abelian free pro-p group. By the way, some results concerning Greenberg's generalized conjecture have been obtained. Combining Minardi's Proposition 3.B of [M] and results of the author (Theorem 1.2 of this article and computational results in [Fu]), for the prime number 3 and imaginary quadratic fields k, we have

Corollary 1.3. *Let $p = 3$. Let $k = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field with a positive integer m such that $m \equiv 2 \bmod 3$. In the range of $1 < m < 1000$, except for four integers $m = 461, 743, 971$ and 974, the derived depth of $G(k_\infty)$ is at most* 1 *except for the case where $G(k_\infty) \simeq \mathbb{Z}_3$.*

For integers $m = 461, 743, 971$ and 974, the derived depth of $G(k_\infty)$ is only known to be greater than 0 thanks to Okano's result [Ok]. We further give examples of imaginary quadratic fields k such that the 2-rank of the ideal class group is at most 1 and the derived depth of $G(k_\infty)$ is at most 1 for the prime 2 by using a method of [Fu].

Now we set the notation of this article. For a prime number p and a number field k (not necessarily finite over $\mathbb{Q}$), we call K/k a $\mathbb{Z}_p^d$-*extension* if K/k is a Galois extension with an isomorphism $\mathrm{Gal}(K/k) \simeq \mathbb{Z}_p^d$ as topological groups. Let $X(k)$ and $G(k)$ denote the Galois groups of the maximal unramified pro-p abelian extension $L(k)/k$ and the maximal unramified pro-p extension $\mathfrak{L}(k)/k$ (not necessarily abelian), respectively. In general, there is a natural isomorphism $X(k) \simeq G(k)^{\mathrm{ab}} = G(k)/G(k)'$, where the superscript ab denotes the maximal pro-p abelian quotient. We also use the notation G^{ab} for any pro-p group G.

For a $\mathbb{Z}_p^d$-extension K/k, let

$$\Lambda(K/k) = \mathbb{Z}_p[[\mathrm{Gal}(K/k)]] = \varprojlim_{k\subseteq k'\subseteq K,\, [k':k]<\infty} \mathbb{Z}_p[\mathrm{Gal}(k'/k)]$$

denote the completed group ring of $\mathrm{Gal}(K/k)$ with coefficients in $\mathbb{Z}_p$, the projective limit is taken with respect to the natural morphisms of Galois groups. Almost all modules in this article are modules over $\Lambda(K/k)$ for a $\mathbb{Z}_p^d$-extension K/k. By Serre's isomorphism, we know that $\Lambda(K/k)$ is isomorphic to the formal power series ring $\Lambda_d = \mathbb{Z}_p[[T_1, \ldots, T_d]]$ of d-variables with coefficients in $\mathbb{Z}_p$. Hence a $\Lambda(K/k)$-module is regarded as a Λ_d-module.

A $\Lambda(K/k)$-module M is called *pseudo-null*, written $M \sim_{\Lambda(K/k)} 0$, if there are two relatively prime annihilators of M in $\Lambda(K/k)$. Equivalently, the annihilator ideal of M is not contained in any height 1 prime ideal of $\Lambda(K/k)$ (see Definition (5.1.4) of [NSW]). We write "$M \supseteq (\sim_{\Lambda(K/k)} 0) \neq 0$" to mean that M contains a non-trivial pseudo-null $\Lambda(K/k)$-submodule. Let $\widetilde{k}$ be the composite of all $\mathbb{Z}_p$-extensions of k. Then $\widetilde{k}/k$ is a $\mathbb{Z}_p^d$-extension for some positive integer d. If Leopoldt's conjecture holds for p and k then $d = r_2 + 1$, where r_2 denotes the number of complex primes of k. It is known that Leopoldt's conjecture holds for each prime number and each abelian field. Greenberg's generalized conjecture is as follows:

Conjecture 1.4 (Greenberg's generalized conjecture [G]). *For each prime number p and finite extension $k/\mathbb{Q}$, $X(\widetilde{k})$ is pseudo-null over $\Lambda(\widetilde{k}/k)$.*

2. Proof of Theorem 1.2. To prove Theorem 1.2, it suffices to show the following.

Proposition 2.1. *Let p be a prime number and k a finite extension of $\mathbb{Q}$ which is completely decomposed at p. Let*

$$1 \to R \to F \to G(k_\infty) \to 1$$

be a minimal presentation of $G(k_\infty)$ by a free pro-p group F. Suppose that there is a $\mathbb{Z}_p^d$-extension K/k such that K contains k_∞ and $X(K) \supseteq (\sim_{\Lambda(K/k)} 0) \neq 0$. Then $R \not\subseteq D_2(F)$.

We now show how to deduce Theorem 1.2 from Proposition 2.1. Observe that $\widetilde{k}/k_\infty$ is unramified. Indeed, since all primes of k lying above p split completely in $k/\mathbb{Q}$, the inertia subgroup of a prime of $\widetilde{k}$ above p

in $\mathrm{Gal}(\widetilde{k}/k)$ is isomorphic to $\mathbb{Z}_p$. Let I be the inertia subgroup of a prime of $\widetilde{k}$ lying above p in $\mathrm{Gal}(\widetilde{k}/k)$. Since all primes of k above p ramify in k_∞/k, I maps to $\mathrm{Gal}(k_\infty/k)$ injectively with finite cokernel. This shows that $I \cap \mathrm{Gal}(\widetilde{k}/k_\infty) = 1$ since $I \simeq \mathbb{Z}_p$, and hence $\widetilde{k}/k_\infty$ is unramified at all primes lying above p. It is known that $\widetilde{k}/k$ is unramified outside primes lying above p. So, we conclude that $\widetilde{k}/k_\infty$ is unramified at all primes of k_∞.

Suppose first that $X(\widetilde{k}) = 0$. From the fact that $X(\widetilde{k}) = G(\widetilde{k})^{\mathrm{ab}}$ and the pro-p version of Burnside's basis theorem, we conclude that $G(\widetilde{k}) = 1$. Hence $\mathfrak{L}(k_\infty) = \widetilde{k}$ and therefore $G(k_\infty) = \mathrm{Gal}(\widetilde{k}/k_\infty)$ is abelian since $\widetilde{k}/k_\infty$ is unramified at all primes of k_∞. Suppose next that $X(\widetilde{k}) \neq 0$. Since $\widetilde{k}$ is the composite of *all* $\mathbb{Z}_p$-extensions, it contains k_∞. From Greenberg's generalized conjecture, it follows that $X(\widetilde{k}) \sim_{\Lambda(\widetilde{k}/k)} 0$, and $X(\widetilde{k}) \neq 0$ by assumption. In particular, $X(\widetilde{k}) \supseteq (\sim_{\Lambda(\widetilde{k}/k)} 0) \neq 0$. By Proposition 2.1, we conclude that $R \not\subseteq D_2(F)$.

Now, we start to prove Proposition 2.1. Let k be a finite extension of $\mathbb{Q}$ which is completely decomposed at p. Let

$$1 \to R \to F \to G(k_\infty) \to 1$$

be a minimal presentation of $G(k_\infty)$ by a free pro-p group F. We may assume that the Iwasawa μ-invariant of k_∞/k is 0. Indeed, if the μ-invariant is greater than 0, then $X(k_\infty)$ has a subgroup of the form $\prod_{n=0}^{\infty} \mathbb{Z}/p$. Since the maximal abelian quotient F^{ab} of a free pro-p group F has no torsion element, it follows that $R \not\subseteq D_1(F)$. Note that the Iwasawa μ-invariant is 0 if and only if $X(k_\infty)$ is finitely generated over $\mathbb{Z}_p$. If $X(k_\infty)$ is finitely generated over $\mathbb{Z}_p$, by the pro-p version of Burnside's basis theorem, $G(k_\infty)$ is finitely generated as a pro-p group.

In what follows, we assume that the Iwasawa μ-invariant of the cyclotomic $\mathbb{Z}_p$-extension k_∞/k is 0. Since $G(k_\infty)$ is a finitely generated pro-p group, F is also finitely generated since $H^1(G(k_\infty), \mathbb{Z}/p) \overset{\mathrm{inf}}{\simeq} H^1(F, \mathbb{Z}/p)$. Let K/k be a $\mathbb{Z}_p^d$-extension such that $k_\infty \subseteq K$ and $X(K) \supseteq (\sim_{\Lambda(K/k)}) \neq 0$. As mentioned above, $\widetilde{k}/k_\infty$ is unramified, and hence K/k_∞ is also unramified because of $K \subseteq \widetilde{k}$.

Lemma 2.2. *There is a closed normal subgroup H of F such that H^{ab} is a finitely generated torsion-free $\Lambda(K/k_\infty)$-module and there is a surjective morphism $H^{\mathrm{ab}} \to X(K)$. In particular, $X(K)$ is finitely generated over $\Lambda(K/k_\infty)$.*

Proof. Note that K is a subfield of $\mathfrak{L}(k_\infty)$ since K/k_∞ is unramified, as mentioned above. We claim that $\mathfrak{L}(K) = \mathfrak{L}(k_\infty)$. The inclusion $\mathfrak{L}(k_\infty) \subseteq \mathfrak{L}(K)$ follows from the fact that $K\mathfrak{L}(k_\infty)/K$ is an unramified extension.

On the other hand, the maximality of $\mathfrak{L}(K)$ shows that $\mathfrak{L}(K)/k_\infty$ is a Galois extension. Since the extensions $\mathfrak{L}(K)/K$ and K/k_∞ are unramified, $\mathfrak{L}(K)/k_\infty$ is also an unramified extension. By the maximality of $\mathfrak{L}(k_\infty)$, we conclude that $\mathfrak{L}(K) \subseteq \mathfrak{L}(k_\infty)$. Therefore $\mathfrak{L}(K) = \mathfrak{L}(k_\infty)$. From this, we find that $G(K)$ is a subgroup of $G(k_\infty)$, and $G(k_\infty)/G(K) = \mathrm{Gal}(K/k_\infty)$.

Let H be the inverse image of $G(K)$ with respect to the surjective morphism $F \to G(k_\infty)$. It follows that $F/H \simeq G(k_\infty)/G(K) \simeq \mathrm{Gal}(K/k_\infty)$. Thus we obtain the following exact-commutative diagram of pro-p groups:

$$
\begin{array}{ccccccccc}
 & & & & R & & & & \\
 & & & & \downarrow & & & & \\
1 & \longrightarrow & H & \longrightarrow & F & \longrightarrow & F/H & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \text{min. pres.}} & & \downarrow{\scriptstyle \wr} & & \\
1 & \longrightarrow & G(K) & \longrightarrow & G(k_\infty) & \longrightarrow & \mathrm{Gal}(K/k_\infty) & \longrightarrow & 1
\end{array}
$$

Since the right vertical map is an isomorphism, the left vertical map is surjective with kernel R. In other words, the sequence

$$1 \to R \to H \to G(K) \to 1$$

of pro-p groups is exact. Now, we consider the abelianization of this exact sequence. Recall that $G(K)^{\mathrm{ab}} = X(K)$. Since $\mathrm{Gal}(K/k_\infty)$ acts on H^{ab} via inner automorphisms, H^{ab} can be regarded as a module over Λ_{K/k_∞}. Note that the actions of $\Lambda(K/k_\infty)$ on H^{ab} and $X(K)$ are compatible with the surjective morphism $H^{\mathrm{ab}} \to X(K)$. We thus have an exact sequence

$$R^{\mathrm{ab}}_{G(K)} \to H^{\mathrm{ab}} \to X(K) \to 0 \tag{2.1}$$

of $\Lambda(K/k_\infty)$-modules (note that $\mathrm{Gal}(K/k)$ does not act on H^{ab}). Hence it suffices to show that H^{ab} is finitely generated and torsion-free over $\Lambda(K/k_\infty)$. Then H is a desired subgroup of F. By Lyndon's resolution (see for example Proposition 1.1 of [N]), there is an exact sequence

$$0 \to H^{\mathrm{ab}} \to \Lambda(K/k_\infty)^{\oplus r} \to \Lambda(K/k_\infty) \to \mathbb{Z}_p \to 0 \tag{2.2}$$

of $\Lambda(K/k_\infty)$-modules, where r is the number of topological generators of $G(k_\infty)$. This exact sequence shows that H^{ab} is finitely generated and torsion-free over $\Lambda(K/k_\infty)$. ■

To finish the proof, we need a module-theoretic lemma.

LEMMA 2.3. *Let M be a $\Lambda(K/k)$-module which is finitely generated over $\Lambda(K/k_\infty)$. Then $M \sim_{\Lambda(K/k)} 0$ if and only if M is torsion over $\Lambda(K/k_\infty)$.*

Hachimori and Sharifi [HS] obtained the same result for p-adic Lie extensions. Their result contains Lemma 2.3. However, in our case, the proof is quite easy, so we give it here.

Proof. By Serre's isomorphism, we identify $\Lambda(K/k)$ (resp. $\Lambda(K/k_\infty)$) and Λ_d (resp. Λ_{d-1}). Hence $\Lambda_d = \Lambda_{d-1}[[T_d]]$. We regard any $\Lambda(K/k)$- (resp. $\Lambda(K/k_\infty)$-) module as a module over Λ_d (resp. Λ_{d-1}). Since M is finitely generated over Λ_{d-1}, there are generators $x_1, \ldots, x_s$ of M over Λ_{d-1}. Thus there is an $s \times s$ matrix A with entries in Λ_{d-1} such that

$$T_d \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix}.$$

Hence $\varphi(T_d) = \det(T_d - A) (\in \Lambda_{d-1}[T_d])$ is in the annihilator ideal $\mathrm{Ann}_{\Lambda_d}(M)$ of M. Put $\mathrm{Ann}_{\Lambda_d}(M) = (g_1, \ldots, g_t)$. Since $\varphi(T_d) \in \mathrm{Ann}_{\Lambda_d}(M)$, we may assume that $g_j \in \Lambda_{d-1}[T_d]$. Indeed, put $g_i = \sum_{n=0}^{\infty} a_i(n) T_d^n$ with $a_i(n) \in \Lambda_{d-1}$. Suppose that $a_i(n)$ is contained in the maximal ideal $\mathfrak{m}_{d-1}$ of Λ_{d-1} for each non-negative integer n. Then the coefficient of $g_i + \varphi(T_d)$ of degree s is $a_i(s) + 1$, which is not contained in $\mathfrak{m}_{d-1}$. Hence, if necessary, by replacing g_i with $g_i + \varphi(T_d)$, we may assume that $a_i(s) \notin \mathfrak{m}_{d-1}$. By the Weierstrass preparation theorem, there are distinguished polynomials $D_i \in \Lambda_{d-1}[T_d]$ and unit power series $U_i \in \Lambda_{d-1}[[T_d]]$ such that $g_i = D_i U_i$. Hence $(g_1, \ldots, g_t) = (D_1, \ldots, D_t)$.

If $M \sim_{\Lambda(K/k)} 0$, then $\mathrm{Ann}_{\Lambda_d}(M)$ is not contained in any height 1 prime ideal of Λ_d. Hence the polynomials $g_1, \ldots, g_t$ are relatively prime over $\Lambda_{d-1}[T_d]$. Let Ω_{d-1} be the field of fractions of Λ_{d-1}. Then there exist polynomials $h_1, \ldots, h_t \in \Omega_{d-1}[T_d]$ such that $1 = \sum_{i=1}^{t} h_i g_i$. If we choose $0 \neq h \in \Lambda_{d-1}$ so that $hh_i \in \Lambda_{d-1}[T_d]$ for each $1 \leq i \leq t$, then $h = \sum_{i=1}^{t} (hh_i) g_i \in \mathrm{Ann}_{\Lambda_d}(M)$. This shows that M is torsion over Λ_{d-1}.

Conversely, suppose that M is torsion over Λ_{d-1}. Since $\varphi(T_d)$ and elements of Λ_{d-1} are relatively prime, $\mathrm{Ann}_{\Lambda_d}(M)$ is not contained in any height 1 prime ideal of Λ_d. Therefore, $M \sim_{\Lambda(K/k)} 0$. ∎

End of proof of Proposition 2.1. Let Z be the maximal pseudo-null submodule of $X(K)$. By our assumption, Z is not trivial. By Lemma 2.3, Z is torsion over $\Lambda(K/k_\infty)$. Since H^{ab} is a torsion-free $\Lambda(K/k_\infty)$-module by the exact sequence (2.2), the surjective morphism $H^{\mathrm{ab}} \to X(K)$ is not an isomorphism. This shows that $R \not\subseteq H'$ by (2.1). Since $\mathrm{Gal}(K/k_\infty) \simeq F/H$ is abelian, we see that $F' \subseteq H$, and hence $R \not\subseteq D_2(F)$. ∎

3. Examples. In this section, we shall give examples for the prime number 2 and imaginary quadratic fields k. Let $A(k)$ be the 2-primary part of the ideal class group of k. In the following, we only deal with the case that 2 splits in an imaginary quadratic field $k = \mathbb{Q}(\sqrt{-m})$ (m is a square-free positive integer) and that $A(k)$ is cyclic. Then, by genus theory, m satisfies one of the following three conditions:

(1) $m = \ell$ is an odd prime number with $\ell \equiv 7 \bmod 8$, and so $A(k) = 0$.
(2) m is a product of two odd prime numbers ℓ_1 and ℓ_2 such that $\ell_1 \equiv 5$, $\ell_2 \equiv 3 \bmod 8$, and so $A(k)/2 \simeq \mathbb{Z}/2$.
(3) m is a product of two odd prime numbers ℓ_1 and ℓ_2 such that $\ell_1 \equiv 1$, $\ell_2 \equiv 7 \bmod 8$, and so $A(k)/2 \simeq \mathbb{Z}/2$.

The following results about $X(\widetilde{k})$ and $X(k_\infty) = G(k_\infty)^{\mathrm{ab}}$ are known.

THEOREM 3.1 (Proposition 3.A of [M]). *Let p be a prime number and k an imaginary quadratic field. If p does not divide the class number of k then $X(\widetilde{k}) \sim_{\Lambda(\widetilde{k}/k)} 0$.*

THEOREM 3.2 (Theorems 6 and 7 of [Fe], Lemma 1 of [Oz1]). *Let $p = 2$ and $k = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field with a square-free positive integer m satisfying $m \equiv 7 \bmod 8$. Let ℓ be an odd prime number and let $r(\ell)$ denote the integer m such that $\ell = \pm 1 + 2^{m+2}a$ with an odd integer a.*

(i) *Let $r(k) = \sum_{\ell|m} 2^{r(\ell)} - 1$. Then $X(k_\infty) \simeq \mathbb{Z}_2^{\oplus r(k)}$.*
(ii) *$X(k_\infty) \simeq \mathbb{Z}_2$ in exactly the following cases:*
   (a) *$m = \ell$, where ℓ is an odd prime number such that $\ell \equiv 7 \bmod 16$,*
   (b) *m is a product of two odd prime numbers ℓ_1 and ℓ_2 such that $\ell_1 \equiv 5$, $\ell_2 \equiv 3 \bmod 8$.*
(iii) *$X(\widetilde{k}) = 0$ if and only if $X(k_\infty) \simeq \mathbb{Z}_2$.*

Let $1 \to R \to F \to G(k_\infty) \to 1$ be a minimal presentation of $G(k_\infty)$ by a free pro-2 group F. If m satisfies the condition (2), or (1) and $\ell \equiv 7 \bmod 16$, then $G(k_\infty) \simeq X(k_\infty) \simeq \mathbb{Z}_2$. In these cases, we can conclude that the derived depth of $G(k_\infty)$ is ∞.

Suppose that condition (1) holds and $\ell \equiv 15 \bmod 16$. Then the Iwasawa λ-invariant of k_∞/k is greater than 1 from Theorem 3.2(i). Hence $X(\widetilde{k}) \neq 0$ by Theorem 3.2(iii). By Theorem 3.1, $X(\widetilde{k})$ is a *non-trivial* pseudo-null $\Lambda(\widetilde{k}/k)$-module. Therefore $R \not\subseteq D_2(F)$ by Proposition 2.1. For conditions (1) and (2), combining the above, we obtain

PROPOSITION 3.3.

- *If $\ell \equiv 7 \bmod 16$ and $k = \mathbb{Q}(\sqrt{-\ell})$, then $G(k_\infty) \simeq \mathbb{Z}_2$ and therefore the derived depth of $G(k_\infty)$ is ∞.*
- *If $\ell \equiv 15 \bmod 16$ and $k = \mathbb{Q}(\sqrt{-\ell})$, then the derived depth of $G(k_\infty)$ is 1.*
- *If $k = \mathbb{Q}(\sqrt{-\ell_1\ell_2})$ with prime numbers ℓ_1 and ℓ_2 satisfying $\ell_1 \equiv 5$ and $\ell_2 \equiv 3 \bmod 8$, then $G(k_\infty) \simeq \mathbb{Z}_2$ and therefore the derived depth of $G(k_\infty)$ is ∞.* ∎

Suppose that condition (3) holds. Then the Iwasawa λ-invariant of k_∞/k is greater than 1 from Theorem 3.2 and hence $X(\widetilde{k}) \neq 0$. We further divide condition (3) into two cases. First, we present a known result dealing with the case where $\left(\frac{\ell_1}{\ell_2}\right) = -1$, $\left(\frac{\cdot}{\cdot}\right)$ being the quadratic residue symbol.

THEOREM 3.4 (Proposition C of [I]; see also Theorem 2 of [IKM]). *Suppose that condition* (3) *holds and* $\left(\frac{\ell_1}{\ell_2}\right) = -1$. *Further assume that* $2^{(\ell_1-1)/4} \not\equiv (-1)^{(\ell_1-1)/8} \bmod \ell_1$. *Then* $X(\widetilde{k})$ *is a non-trivial pseudo-null* $\Lambda(\widetilde{k}/k)$*-module.*

From Theorem 3.4 and Proposition 2.1, we have

PROPOSITION 3.5. *Under the assumptions of Theorem* 3.4, *the derived depth of* $G(k_\infty)$ *is* 1.

Next, we deal with the case where $\left(\frac{\ell_1}{\ell_2}\right) = 1$.

THEOREM 3.6. *Let* $p = 2$. *Let* ℓ_1 *and* ℓ_2 *be prime numbers such that* $\ell_1 \equiv 1$, $\ell_2 \equiv 7 \bmod 8$ *and* $\left(\frac{\ell_1}{\ell_2}\right) = 1$. *Let* $k = \mathbb{Q}(\sqrt{-\ell_1\ell_2})$ *and let* $R_k(\mathfrak{m})$ *be the ray class group of* k *modulo* $\mathfrak{m}$. *Put* $2^N = \exp(A(k))$. *Suppose*

(a) *there is a positive integer* n *such that* $N + 2 < n$ *and*

$$R_k(2^n) \otimes \mathbb{Z}_2 \simeq T \oplus \mathbb{Z}/2^{a_1} \oplus \mathbb{Z}/2^{a_2}$$

with $\exp(T) < \exp(A(k))$ *and* $N < \min\{a_1, a_2\}$,

(b) *the norm of the fundamental unit of* $\mathbb{Q}(\sqrt{2\ell_1})$ *is equal to* 1.

Then $X(\widetilde{k}) \supseteq (\sim_{\Lambda(\widetilde{k}/k)} 0) \neq 0$. *In particular, the derived depth of* $G(k_\infty)$ *is* 1.

Proof. Since $k(\sqrt{\ell_1})/k$ is an unramified extension and since $A(k)/2 \simeq \mathbb{Z}/2$, $k(\sqrt{\ell_1})/k$ is a unique unramified quadratic extension. From Proposition 2 of [C] and Lemma 4.3 of [Fu], if condition (a) holds then $\widetilde{k}$ contains a non-trivial unramified extension of k, in particular $\sqrt{\ell_1} \in \widetilde{k}$. Note that the author showed in [Fu] that the group T is isomorphic to the maximal torsion subgroup of the Galois group of the maximal pro-2 abelian extension unramified at all primes lying above 2. By Kummer theory, $\#T \geq 4$. When $\left(\frac{\ell_1}{\ell_2}\right) = -1$, $\widetilde{k}$ contains no non-trivial unramified extension since $A(k)$ is always $\mathbb{Z}/2$. In fact, the condition $\exp(T) < \exp(A(k))$ does not hold. When $\left(\frac{\ell_1}{\ell_2}\right) = 1$, since $k(\sqrt{\ell_1})/k$ is unramified, $A(k) \simeq \mathbb{Z}/2^a$ with $a \geq 2$. The condition $\exp(T) < \exp(A(k))$ holds only in this case.

Since the quadratic subextension of k_∞/k is $k(\sqrt{2})$, $k(\sqrt{2\ell_1})$ is a subfield of $\widetilde{k}$, and all primes above 2 are ramified in $k(\sqrt{2\ell_1})/k$. Let K/k be a $\mathbb{Z}_2$-extension with $k(\sqrt{2\ell_1}) \subseteq K$. The author also showed in [Fu] that if $X(K)$ contains a non-trivial finite $\Lambda(K/k)$-submodule then $X(\widetilde{k}) \supseteq (\sim_{\Lambda(\widetilde{k}/k)} 0) \neq 0$.

To show the existence of a non-trivial finite submodule of $X(K)$, it suffices to prove that the lift map $i : A(k) \to A(k(\sqrt{2\ell_1}))$ is not injective. Since

$A(k)$ is a cyclic group, the injectivity of i is equivalent to the non-triviality of the restriction $i|_{A(k)[2]}$ of i to the 2-torsion subgroup $A(k)[2]$ of $A(k)$. Let $\mathfrak{l}_1$ be the prime ideal of k above ℓ_1. By genus theory, $A(k)[2]$ is generated by the class $c(\mathfrak{l}_1)$ containing $\mathfrak{l}_1$. Let $\mathfrak{L}_1$ and $\mathfrak{L}_1'$ be the primes of $k(\sqrt{2\ell_1})$ with $\mathfrak{L}_1 \neq \mathfrak{L}_1'$ lying above ℓ_1 and let $\mathfrak{l}_1^+$ be the prime of $\mathbb{Q}(\sqrt{2\ell_1})$ lying above 2. Then $\mathfrak{l}_1 = \mathfrak{L}_1\mathfrak{L}_1' = \mathfrak{l}_1^+$ in $k(\sqrt{2\ell_1})$. By genus theory, the 2-torsion subgroup of the narrow class group of $\mathbb{Q}(\sqrt{2\ell_1})$ is generated by the class containing $\mathfrak{l}_1^+$. From our assumption (b), $\mathfrak{l}_1^+$ is a principal ideal. This shows that $i|_{A(k)[2]}$ is trivial. ∎

REMARK 3.7. From Theorem 1 of [L], the lift map i is injective if and only if the norm of the fundamental unit of $\mathbb{Q}(\sqrt{2\ell_1})$ is -1.

We show examples illustrating Theorem 3.6. In the range of $1 < \ell_1, \ell_2 < 500$, for the following pairs of prime numbers (ℓ_1, ℓ_2) and the imaginary quadratic field $k = \mathbb{Q}(\sqrt{-\ell_1\ell_2})$, the derived depth of $G(k_\infty)$ is 1 by Theorem 3.6 (the computations were done by using KASH [KASH]):

$(17,47), (17,103), (17,127), (17,151), (17,191), (17,239), (17,263), (17,271), (17,383), (17,463), (73,71), (73,127), (73,223), (73,311), (73,359), (73,367), (73,439), (73,463), (73,479), (73,487), (89,167), (89,199), (89,223), (89,263), (89,271), (89,311), (89,367), (97,47), (97,79), (97,103), (97,151), (97,431), (97,487), (193,7), (193,23), (193,31), (193,191), (193,239), (193,359), (193,383), (193,479), (193,487), (233,7), (233,23), (233,271), (233,359), (241,79), (241,191), (241,223), (241,239), (241,359), (241,487), (257,23), (257,79), (257,199), (257,223), (257,479), (281,7), (281,31), (281,79), (281,191), (281,223), (281,359), (281,367), (281,439), (337,7), (337,47), (337,79), (337,103), (337,239), (337,263), (337,311), (337,431), (353,47), (353,127), (353,167), (353,311), (353,431), (401,47), (401,103), (401,223), (401,239), (401,311), (401,383), (401,487), (433,167), (433,191), (433,199), (433,223), (433,271), (433,359), (433,367), (433,383), (433,431), (433,439), (449,7), (449,167), (449,271), (449,359), (449,367), (449,431)$.

Acknowledgements. Before this work was started, Ozaki remarked that Greenberg's generalized conjecture implies that $G(k_\infty)$ cannot be a non-abelian free pro-p group for imaginary quadratic fields k. The author would like to express his thanks to Professor Manabu Ozaki for his valuable remark. The author also wishes to thank Professor Yasushi Mizusawa for the information about Lemmermeyer's result [L]. This study was done when the author was a COE researcher at Keio University.

References

[C] J. Carroll, *On determining the quadratic subfields of $\mathbb{Z}_2$-extensions of complex quadratic fields*, Compos. Math. 30 (1975), 259–271.

[KASH] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig and K. Wildanger, *KANT V4*, J. Symbolic Comput. 24 (1997), 267–283.

[Fe] B. Ferrero, *The cyclotomic $\mathbb{Z}_2$-extension of imaginary quadratic fields*, Amer. J. Math. 102 (1980), 447–459.

[Fu] S. Fujii, *Pseudo-null submodules of the unramified Iwasawa module for $\mathbb{Z}_p^2$-extensions*, Interdiscip. Inform. Sci. 16 (2010), 55–66.

[G] R. Greenberg, *Iwasawa theory—past and present*, in: Class Field Theory—Its Centenary and Prospects (Tokyo, 1998), Adv. Stud. Pure Math. 30, Math. Soc. Japan, 2001, 335–385.

[HS] Y. Hachimori and R. Sharifi, *On the failure of pseudo-nullity of Iwasawa modules*, J. Algebraic Geom. 14 (2005), 567–591.

[I] T. Itoh, *Pseudo-null Iwasawa modules for $\mathbb{Z}_2^2$-extensions*, Tokyo J. Math. 30 (2007), 199–209.

[IKM] T. Itoh, S. Kiyofuji and Y. Mizusawa, *On the Iwasawa invariants of certain non-cyclotomic $\mathbb{Z}_2$-extensions*, Manuscripta Math. 118 (2005), 227–233.

[L] F. Lemmermeyer, *Ideal class groups of cyclotomic number fields I*, Acta Arith. 72 (1995), 347–359.

[M] J. Minardi, *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, Thesis, Washington Univ., 1986.

[MO] Y. Mizusawa and M. Ozaki, *Abelian 2-class field towers over cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields*, Math. Ann. 347 (2010), 437–453.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Grundlehren Math. Wiss. 323, Springer, Berlin, 2000.

[N] T. Nguyen Quang Do, *Formations de classes et modules d'Iwasawa*, in: Number Theory (Noordwijkerhout, 1983), Lecture Notes in Math. 1068, Springer, Berlin, 1984, 167–185.

[Ok] K. Okano, *Abelian p-class field towers over the cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields*, Acta Arith. 125 (2006), 363–381.

[Oz1] M. Ozaki, *Iwasawa invariants of $\mathbb{Z}_p$-extensions over an imaginary quadratic field*, in: Class Field Theory—Its Centenary and Prospects (Tokyo, 1998), Adv. Stud. Pure Math. 30, Math. Soc. Japan, 2001, 387–399.

[Oz2] —, *Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions*, J. Reine Angew. Math. 602 (2007), 59–94.

[S] R. Sharifi, *On Galois groups of unramified pro-p extensions*, Math. Ann. 342 (2008), 297–308.

[V] R. Validire, *Sur la pro-p-extension localement cyclotomique maximale d'un corps de nombres*, http://jp.arxiv.org/pdf/0812.1687.

Satoshi Fujii
Department of Mathematical Sciences
School of Science and Engineering
Keio University
Hiyoshi, Kohoku-ku
Yokohama, Kanagawa 223-8522, Japan
E-mail: fujii@ruri.waseda.jp

Received on 9.2.2009
and in revised form on 8.10.2010 (5930)