RIMS Kôkyûroku Bessatsu
B25 (2011), 95–101

Greenberg's generalized conjecture and unramified Galois groups over the cyclotomic $\mathbb{Z}_p$-extensions

By

Satoshi Fujii*

Abstract

Let p be a fixed prime number and k a number field. Recently, the studies of the Galois group $G(k_\infty)$ of the maximal unramified pro-p extension $\mathcal{L}(k_\infty)/k_\infty$ over the cyclotomic $\mathbb{Z}_p$-extension k_∞ of k are being developed. In this subject, to find number fields k such that $G(k_\infty)$ is a non-abelian free pro-p group is a very important problem. However, it seems that there is no concrete such example of a number field k. In this article, we show roughly if Greenberg's generalized conjecture holds for p and k then $G(k_\infty)$ can not be a non-abelian free pro-p group. We also show some examples of imaginary abelian fields k.

§ 1. Introduction

This article is written as a report of the talk of the author at "Algebraic Number Theory and Related Topics". Around the subjects of this article are already submitted ([1] and [2]) and published as a report ([3], not refereed), so we will give a survey of the topics about the talk specifically.

Let p be a fixed prime number, $\mathbb{Z}_p$ the ring of all p-adic integers and $k/\mathbb{Q}$ a finite extension. We call K/k a $\mathbb{Z}_p$-extension if K/k is a Galois extension such that its Galois group $\mathrm{Gal}(K/k)$ is isomorphic to the additive group of $\mathbb{Z}_p$ as topological groups. From the theory of cyclotomic fields, there is a unique $\mathbb{Z}_p$-extension k_∞ contained in the field $k(\mu_{p^\infty})$ obtained by adjoining all p-power-th roots of unity μ_{p^∞}. We call k_∞ the cyclotomic $\mathbb{Z}_p$-extension of a number field k. Let $\mathcal{L}(k_\infty)/k_\infty$ be the maximal unramified pro-p extension and $G(k_\infty) = \mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty)$ its Galois group. For the topics of $G(k_\infty)$, there is an excellent report by Mizusawa [9], so we concentrate to discuss on the relationship between the freeness of $G(k_\infty)$ and Greenberg's generalized conjecture.

Received March 31, 2010. Revised August 06, 2010.
2000 Mathematics Subject Classification(s): 11R23
*Keio University, Yokohama, Japan. e-mail: moph@a2.keio.jp

The problem considered in this article is as follows:

Problem. Is there a number field k such that $G(k_\infty)$ is a non-abelian free pro-p group?

If such k exists, then we can find interesting examples of p-class field towers ([4]). However, it seems that there is no concrete affirmative example of an answer to the above problem yet. Further, it is considered that $G(k_\infty)$ never be a non-abelian free pro-p group. When the prime number p splits completely in $k/\mathbb{Q}$, as we will see later, Greenberg's generalized conjecture (see the following sections) ensures this.

Theorem 1.1. *If the prime number p splits completely in a finite extension $k/\mathbb{Q}$ and if Greenberg's generalized conjecture holds for p and k, then $G(k_\infty)$ is not a non-abelian free pro-p group.*

Here we give some remarks.
• The author must mention here that Ozaki [10] remarked that Greenberg's generalized conjecture for p and an imaginary quadratic field k which is decomposed at p implies that $G(k_\infty)$ is not a non-abelian free pro-p group. Now, we obtain the same conclusion for each number field k in which given prime number p splits completely.
• Under the assumption of Theorem 1.1, more strictly, the maximal metabelian quotient of $G(k_\infty)$ can not be a non-abelian, free-metabelian pro-p group.
• The author do not know a relationship between the structure of $G(k_\infty)$ as a pro-p group and Greenberg's generalized conjecture when the prime number p does not split completely in $k/\mathbb{Q}$. To find a connection between the structure of $G(k_\infty)$ and Greenberg's generalized conjecture for general number fields seems an interesting and important problem.

§ 2. $\mathbb{Z}_p^d$-extensions, Greenberg's generalized conjecture and $G(k_\infty)$

§ 2.1. $\mathbb{Z}_p^d$-extensions

At first, we give a summary of the theory of $\mathbb{Z}_p^d$-extensions and Greenberg's generalized conjecture. We call $k^{(d)}/k$ a $\mathbb{Z}_p^d$-extension if $k^{(d)}/k$ is a Galois extension such that its Galois group $\mathrm{Gal}(k^{(d)}/k)$ is isomorphic to the d-copies $\mathbb{Z}_p^d$ of the additive group of $\mathbb{Z}_p$ as topological groups. Let $k^{(d)}/k$ be a $\mathbb{Z}_p^d$-extension and let $X(k^{(d)}) = \mathrm{Gal}(L(k^{(d)})/k^{(d)})$ be the Galois group of the maximal unramified abelian pro-p extension $L(k^{(d)})/k^{(d)}$. The maximality of $L(k^{(d)})$ shows that $L(k^{(d)})/k$ is a Galois extension, hence $\mathrm{Gal}(k^{(d)}/k)$ acts on $X(k^{(d)})$ via the inner automorphism. By extending this action linearly and

continuously, the completed group ring

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

acts also on $X(k^{(d)})$, the projective limit is taken with respect to the natural restriction maps of Galois groups. Note that $\mathbb{Z}_p[[\mathrm{Gal}(k^{(d)}/k)]]$ is isomorphic to the formal power series ring $\Lambda_d = \mathbb{Z}_p[[T_1, \ldots, T_d]]$ of d-variables with coefficients in $\mathbb{Z}_p$ non-canonically. Hence $X(k^{(d)})$ can be seen as a Λ_d-module. Then it is known that $X(k^{(d)})$ is a finitely generated torsion Λ_d-module.

§ 2.2. Greenberg's generalized conjecture

In what follows, for simplicity, we assume that Leopoldt's conjecture holds for p and k. It is well known that Leopoldt's conjecture holds for each abelian field. Let $\tilde{k}$ be the composite of all $\mathbb{Z}_p$-extensions of k. Then $\tilde{k}/k$ is a $\mathbb{Z}_p^{r_2+1}$-extension (under the assumption that Leopoldt's conjecture holds), where r_2 is the number of complex primes of k (see for example [12]). We show some examples:

- If $k = \mathbb{Q}$, then $\tilde{k} = \mathbb{Q}_\infty$, the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. In general $\tilde{k} = k_\infty$ for totally real fields k.
- If k is a totally imaginary field, then $\mathrm{Gal}(\tilde{k}/k) \simeq \mathbb{Z}_p^{\frac{[k:\mathbb{Q}]}{2}+1}$. In particular, if k is an imaginary quadratic field then $\tilde{k}/k$ is a $\mathbb{Z}_p^2$-extension.

Greenberg's Generalized conjecture states that $X(\tilde{k})$ is not so big.

Conjecture. *(Greenberg's generalized Conjecture [6])* $X(\tilde{k})$ is a pseudo-null Λ_{r_2+1}-module.

A Λ_d-module M is called pseudo-null if there are two relatively prime annihilators in Λ_d of M. Original Greenberg's conjecture [5] asserts that $X(k_\infty)$ is finite for all totally real fields k. It is known that a Λ_1-module is finite if and only if is pseudo-null. Since $\tilde{k} = k_\infty$ for totally real fields k (under the assumption that Leopoldt's conjecture holds), Greenberg's generalized conjecture is regarded as a generalization of original Greenberg's conjecture for all number fields. Here we show results concerning Greenberg's generalized conjecture for imaginary abelian fields. For a number field k and a prime number p, let $A(k)$ be the p-part of the ideal class group of k and $D(k)$ the subgroup of $A(k)$ which consists of all ideal classes in $A(k)$ containing a power of primes of k lying above p.

Theorem 2.1. *(Minardi [8]) Let k be an imaginary quadratic field and p a prime number. If $A(k) = D(k)$ then $X(\tilde{k})$ is pseudo-null.*

Theorem 2.2. *(Itoh [7]) Let k be an imaginary abelian quartic field and p an odd prime number which splits completely in $k/\mathbb{Q}$. Let k^+ be the maximal totally real subfield of k. Suppose that $A(k) = 0$ and $X(k_\infty^+) = 0$. Then $X(\tilde{k})$ is pseudo-null.*

Theorem 2.3. *(Sharifi [11]) Let p be an odd prime number less than* 1000 *and $k = \mathbb{Q}(\mu_p)$ the p-th cyclotomic field. Then $X(\tilde{k})$ is pseudo-null.*

In the module theoretic view point, the method of deducing the pseudo-nullity of $X(\tilde{k})$ of the above results is finding a "good" sub-$\mathbb{Z}_p^d$-extension $k^{(d)}$ of $\tilde{k}/k$. In Minardi's and Itoh's results, they found a $\mathbb{Z}_p$- or $\mathbb{Z}_p^2$-extension $k^{(d)}$ ($d = 1$ or 2) such that the $\mathrm{Gal}(\tilde{k}/k^{(d)})$-coinvariant $X(\tilde{k})_{\mathrm{Gal}(\tilde{k}/k^{(d)})}$ of $X(\tilde{k})$, the maximal quotient module on which $\mathrm{Gal}(\tilde{k}/k^{(d)})$ acts trivially, is pseudo-null over Λ_d. This shows the pseudo-nullity of $X(\tilde{k})$ over Λ_{r_2+1}. In Sharifi's result, he found a $\mathbb{Z}_p^2$-extension $k^{(2)}$ such that $X(k^{(2)})$ is a finitely generated $\mathbb{Z}_p$-module. This also shows the pseudo-nullity of $X(\tilde{k})$. Of course, showing the pseudo-nullity of $X(k^{(d)})_{\mathrm{Gal}(\tilde{k}/k^{(d)})}$ or the finitely generation of $X(k^{(2)})$ is the most important part in their proofs.

On the other hand, the author found a new method showing the pseudo-nullity of $X(k^{(2)})$ for certain $\mathbb{Z}_p^2$-extensions $k^{(2)}/k$.

Theorem 2.4. *(F [1]) Let p be an odd prime number and k an imaginary quadratic field. Let s be the number of primes of k lying above p. Let k_1 be an intermediate field of $\tilde{k}/k$ such that k_1/k is ramified at all primes of k lying above p and that $[k_1 : k] = p$. If $\dim_{\mathbb{F}_p} D(k_1)/p = s$ then $X(\tilde{k})$ has a non-trivial pseudo-null submodule. Furthermore, if the non-trivial part of the Iwasawa polynomial related to the Kubota-Leopoldt's p-adic L-function of k is irreducible then $X(\tilde{k})$ is itself pseudo-null.*

Points of this result are looking up the existence of non-trivial pseudo-null submodules of $X(\tilde{k})$, and using two independent $\mathbb{Z}_p$-extensions, one of which is the cyclotomic $\mathbb{Z}_p$-extension k_∞. We show keys of the proof.

- Since p is an odd prime number and since k is an imaginary quadratic field, it is well known that $X(k_\infty)$ has no non-trivial finite submodules. From this fact, we can prove that if $X(\tilde{k})$ has no non-trivial pseudo-null submodules, then the length of a minimal free resolution of $X(\tilde{k})$ as a Λ_2-module is equal to or less than 1.

- Let $k^{(1)}$ be a $\mathbb{Z}_p$-extension of k containing k_1. Then, from our assumption that $\dim_{\mathbb{F}_p} D(k_1)/p = s$, we can prove that $X(\tilde{k})_{\mathrm{Gal}(\tilde{k}/k^{(1)})}$ has a non-trivial finite submodule. This shows that the length of a minimal free resolution of $X(\tilde{k})$ is greater than 1. Therefore, from the above fact and our assumption, we can conclude that $X(\tilde{k})$ has a non-trivial pseudo-null submodule.

- From a property of Fitting ideals and the irreducibility of the polynomial related to the p-adic L-function of k, we can prove that the Fitting ideal of $X(\tilde{k})$ as a module over Λ_2 contains a prime element. Therefore, by using another property of Fitting ideals, if $X(\tilde{k})$ has a non-trivial pseudo-null submodule then $X(\tilde{k})$ is itself pseudo-null.

Here we give examples of number fields for which Greenberg's generalized conjecture holds.

- By Minardi's result, for 9 imaginary quadratic fields with class number 1 and each prime number p, Greenberg's generalized conjecture holds.

- Combining the results of Minardi and the author, and computational results, in the range of $1 < m < 1000$, for the prime number 3 and imaginary quadratic fields $k = \mathbb{Q}(\sqrt{-m})$ with square-free integers m such that $m \equiv 2 \bmod 3$, we see that $X(\tilde{k})$ is pseudo-null except for four integers $m = 461, 743, 971$ and 974. The author do not know even that $X(\tilde{k})$ has a non-trivial pseudo-null submodule or not for these four integers.

§ 2.3. Greenberg's generalized conjecture and $G(k_\infty)$ – A sketch of the proof of Theorem 1.1

Let p be a prime number and $k/\mathbb{Q}$ a finite extension such that the prime number p splits completely. For simplicity, we assume that k is abelian here. Then,
• $G(k_\infty)$ is a finitely generated pro-p group by Ferrero–Washington's theorem and pro-p version of Burnside's theorem,
• Leopoldt's conjecture holds for p and k.
Suppose that Greenberg's generalized conjecture holds for p and k, that is, $X(\tilde{k})$ is a pseudo-null Λ_{r_2+1}-module. We also assume here that $X(\tilde{k}) \neq 0$. Let $\varphi : F \to G(k_\infty)$ be a minimal presentation of $G(k_\infty)$ by a free pro-p group F. We must show that φ is not isomorphic. The story of the proof is as follows:

- Since the prime number p splits completely, the $\mathbb{Z}_p^{r_2}$-extension $\tilde{k}/k_\infty$ is unramified at each prime of k_∞. When $r_2 = 0$, we shall let $\mathbb{Z}_p^0$ be the trivial group, hence $\tilde{k} = k_\infty$. From the maximality of $\mathcal{L}(k_\infty)$, $L(\tilde{k})$ is a subfield of $\mathcal{L}(k_\infty)$, and hence $G(\tilde{k}) = \mathrm{Gal}(\mathcal{L}(k_\infty)/\tilde{k})$ is a subgroup of $G(k_\infty)$. Note that the abelianization $G(\tilde{k})^{\mathrm{ab}} = G(\tilde{k})/[G(\tilde{k}), G(\tilde{k})]$ of $G(\tilde{k})$ is $X(\tilde{k})$.

- By an identification $\mathbb{Z}_p[[\mathrm{Gal}(\tilde{k}/k_\infty)]] \simeq \Lambda_{r_2}$, we consider the Λ_{r_2}-module structure of $X(\tilde{k})$. When $r_2 = 0$, we let $\Lambda_0 = \mathbb{Z}_p$. It is known that if $X(\tilde{k})$ is pseudo-null over Λ_{r_2+1} then $X(\tilde{k})$ is torsion over Λ_{r_2}.

- Put $H = \varphi^{-1}(G(\tilde{k}))$. Then, the abelianization $H^{\mathrm{ab}} = H/\overline{[H,H]}$ of H is a Λ_{r_2}-module of finitely generated and Λ_{r_2}-torsion free. Note that the minimal presentation φ induces a surjective morphism $\varphi|_H^{\mathrm{ab}} : H^{\mathrm{ab}} \to X(\tilde{k})$ of Λ_{r_2}-modules. If φ is an isomorphism then $\varphi|_H^{\mathrm{ab}}$ is also an isomorphism.

Combining the above, we give the conclusion.

$$\begin{aligned} X(\tilde{k}) \text{ is pseudo-null over } \Lambda_{r_2+1} &\implies X(\tilde{k}) \text{ is torsion over } \Lambda_{r_2} \\ &\implies \varphi|_H^{\mathrm{ab}} : H^{\mathrm{ab}} \to X(\tilde{k}) \text{ is not an isomorphism} \\ &\implies \varphi : F \to G(k_\infty) \text{ is not an isomorphism.} \end{aligned}$$

This completes the proof of Theorem 1.1. □

For an imaginary abelian quartic field k in which a given prime number p splits completely, the $\mathbb{Z}_p$-rank of $X(k_\infty)$ is greater than 1. Hence $G(k_\infty)$ is not isomorphic to 1 or $\mathbb{Z}_p$. Therefore, if $A(k) = 0$ and $X(k_\infty^+) = 0$ then $G(k_\infty)$ is not a non-abelian free pro-p group by Itoh's result.

Let $k = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field with a positive square-free integer m such that $m \equiv 2 \bmod 3$, then the prime 3 splits in k. As a consequence of Theorem 1.1, 2.4, 2.1 and the computational result (see the previous subsection), for $p = 3$ and $1 < m < 1000$ except for four integers $m = 461, 743, 971$ and 974, $G(k_\infty)$ is not a non-abelian free pro-3 group. For exceptional these integers m, we only know that $G(k_\infty)$ is non-abelian.

§ 3. Problems

Against the expectation of the problem in section 1, we shall raise a problem.

Problem 1. For every prime number p and finite extension $k/\mathbb{Q}$, is not $G(k_\infty)$ a non-abelian free pro-p group?

When the prime number p splits completely in $k/\mathbb{Q}$, Greenberg's generalized conjecture ensures this problem. (However, it seems that there is no theory which ensures Greenberg's generalized conjecture...) As mentioned in section 1, at least, the author does not know a relationship between $G(k_\infty)$ and Greenberg's generalized conjecture when the prime number p does not split completely. So, we shall raise again the following problem, which weakened problem 1 from the view point of Greenberg's generalized conjecture.

Problem 2. Find a connection between the structure of $G(k_\infty)$ and Greenberg's

generalized conjecture for general finite extensions $k/\mathbb{Q}$.

As discussed in [4] (see also the Remark in [4]), it seems that there is a connection between $G(k_\infty)$ and Greenberg's generalized conjecture when k is an imaginary quadratic field in which p does not necessary split. However, the author could not formulate explicitly such connections.

References

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

[2] Fujii, S., On the depth of the relations of the maximal unramified pro-p Galois group over the cyclotomic $\mathbb{Z}_p$-extensions, submitted.

[3] Fujii, S., Non-abelian Iwasawa theory of cyclotomic $\mathbb{Z}_p$-extensions, The COE Seminar on Mathematical Sciences 2007, 85–97, Sem. Math. Sci., **37**, Keio Univ., Yokohama, 2008.

[4] Fujii, S. and Okano, K., Some problems on p-class field towers, Tokyo J. Math., **30** (2007), 211–222.

[5] Greenberg, R., On the Iwasawa invariants of totally real number fields, Amer. J. Math., **98** (1976), 263–284.

[6] Greenberg, R., Iwasawa theory-past and present, Advanced Studies in Pure Math., **30** (2001), 335–385.

[7] Itoh, T., On multiple $\mathbb{Z}_p$-extensions of imaginary abelian quartic fields, preprint.

[8] Minardi, J., Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields, Thesis (1986), Washington University.

[9] Mizusawa, Y., On unramified pro-p Galois groups over cyclotomic $\mathbb{Z}_p$-extensions – A survey, RIMS Kôkyûroku Bessatsu, **4** (2007), 223–233.

[10] Ozaki, M., Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions, (Japanese) Young philosophers in number theory (Kyoto, 2001), RIMS Kôkyûroku, **1256** (2002), 25–37.

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

[12] Washington, L., Introduction to cyclotomic fields, second edition, GTM **83**, Springer, 1997.