61. Remarks on Z_p-extensions of Number Fields

By Takashi FUKUDA

Department of Mathematics, College of Industrial Technology, Nihon University

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1994)

Let p be any prime number and k any finite extension of the rational number field $\boldsymbol{Q}$. Let K be a $\boldsymbol{Z}_p$-extension of k, namely, a Galois extension whose Galois group is topologically isomorphic to the p-adic integer ring $\boldsymbol{Z}_p$. For an integer $n \geqq 0$, we denote by k_n the intermediate field of K/k with degree p^n over k and by A_n the p-Sylow subgroup of the ideal class group of k_n. Let L (resp. L_n) be the p-Hilbert class field of K (resp. k_n). Then $X = G(L/K)$ becomes a module over the formal power series ring $\Lambda = \boldsymbol{Z}_p[[T]]$ if we define the action of $1 + T$ by an inner automorphism induced from a fixed topological generator of $G(K/k)$. It is known that X is finitely generated over Λ. For $m \geqq n \geqq 0$, let $\omega_n = (1+T)^{p^n} - 1 \in \Lambda$ and $\nu_{n,m} = \omega_m/\omega_n \in \Lambda$. We fix an integer $n_0 \geqq 0$ such that any prime of K which is ramified in K/k is totally ramified in K/k_{n_0}. Let $\mu_p(K/k)$ and $\lambda_p(K/k)$ denote the Iwasawa invariants of K/k. For a $\boldsymbol{Z}_p$-module M, $|M|$ denotes the cardinal number of M and $\mathrm{rank}(M)$ denotes the dimension of M/pM over $\boldsymbol{F}_p$. First we mention a general property of a $\boldsymbol{Z}_p$-extension.

Theorem 1. *Let K/k be any $\boldsymbol{Z}_p$-extension.*
(1) *If there exists an integer $n \geqq n_0$ such that $|A_{n+1}| = |A_n|$, then $|A_m| = |A_n|$ for all $m \geqq n$. In particular, we see that $\mu_p(K/k) = \lambda_p(K/k) = 0$.*
(2) *If there exists an integer $n \geqq n_0$ such that $\mathrm{rank}(A_{n+1}) = \mathrm{rank}(A_n)$, then $\mathrm{rank}(A_m) = \mathrm{rank}(A_n)$ for all $m \geqq n$. In particular, we see that $\mu_p(K/k) = 0$.*

Proof. Note that $\mu_p(K/k_{n_0}) = p^{n_0}\mu_p(K/k)$ and $\lambda_p(K/k_{n_0}) = \lambda_p(K/k)$. Hence we may assume that $n_0 = 0$. Let $Y = G(L/KL_0)$. Then, for any $n \geqq 0$, we have the following commutative diagram, where $A_n \to A_0$ is induced from the norm map $k_n \to k_0$ and $X/\nu_{0,n}Y \to X/Y$ is the restriction map (cf. [2]).

$$\begin{array}{ccc} A_n & \simeq & X/\nu_{0,n}Y \\ \downarrow & & \downarrow \\ A_0 & \simeq & X/Y \end{array}$$

(1) Assume that $|A_1| = |A_0|$. Then $A_1 \to A_0$ is an isomorphism and $X/\nu_{0,1}Y \to X/Y$ is also. Therefore, $\nu_{0,1}Y = Y$. Now $\nu_{0,1}$ is contained in the unique maximal ideal $\langle p, T\rangle$ of Λ and Y is also finitely generated over Λ. Hence $Y = 0$ from Nakayama's lemma and $A_n \simeq X$ for all $n \geqq 0$. (2) Assume that $\mathrm{rank}(A_1) = \mathrm{rank}(A_0)$. Then $A_1/pA_1 \simeq A_0/pA_0$. Therefore we see that $X/(\nu_{0,1}Y + pX) \simeq X/(Y + pX)$ and $\nu_{0,1}Y + pX = Y + pX$. Let $Z = (Y + pX)/pX$. Then $\nu_{0,1}Z = (\nu_{0,1}Y + pX)/pX = (Y + pX)/pX = Z$. Hence $Z = 0$ again from Nakayama's lemma and $Y \subset pX$. Then, $\mathrm{rank}(A_n) = \mathrm{rank}(X/\nu_{0,n}Y) = \mathrm{rank}(X/(\nu_{0,n}Y + pX)) = \mathrm{rank}(X/pX) = \mathrm{rank}(X)$ for all $n \geqq 0$.

Next, we consider a capitulation problem in a $\boldsymbol{Z}_p$-extension. For $m \geqq n \geqq 0$, let $H_{n,m}$ be the kernel of the map $A_n \to A_m$ induced from the natural inclusion $k_n \to k_m$. In [1], Greenberg related the behavior of $|A_n|$ to $H_{n,m}$. In particular he obtained the following result for certain type of $\boldsymbol{Z}_p$-extensions.

Theorem (Greenberg). *Let K/k be a $\boldsymbol{Z}_p$-extension of a totally real number field k. Assume that only one prime of k lies over p and that this prime is totally ramified in K/k. Then $H_{0,n} = A_0$ for some $n \geqq 0$ if and only if $|A_n|$ is bounded as $n \to \infty$.*

We shall give an explicit form and a simple proof of this theorem.

Theorem 2. *Let K/k be a $\boldsymbol{Z}_p$-extension of any number field k. Assume that only one prime of k lies over p and that this prime is totally ramified in K/k.*
(1) *If $H_{0,n} = A_0$ for some $n \geqq 1$, then $|A_m| = |A_n|$ for all $m \geqq n$.*
(2) *If $|A_{n+1}| = |A_n|$ for some $n \geqq 0$ and the exponent of A_n is p^r, then $H_{n,n+r} = A_n$. In particular, $H_{0,n+r} = A_0$.*

We prepare the following easy lemma.

Lemma. $\nu_{n,m} \equiv p^{m-n} \pmod{\omega_n}$ *for all $m \geqq n \geqq 0$.*

Proof. Note that $\nu_{n,n+1} = ((\omega_n + 1)^p - 1)/\omega_n \equiv p \pmod{\omega_n}$. Then $\nu_{n,m} = \nu_{n,n+1} \cdot \nu_{n+1,n+2} \cdot \cdots \cdot \nu_{m-1,m} = p^{m-n} \pmod{\omega_n}$.

Proof of Theorem 2. From the assumption, we get the following two commutative diagrams for all $m \geqq n \geqq 0$, where $X/\omega_n X \to X/\omega_m X$ is defined by $x \bmod \omega_n X \mapsto \nu_{n,m} x \bmod \omega_m X$ and $X/\omega_m X \to X/\omega_n X$ is the restriction map (cf. [2]).

$$\begin{array}{ccc} A_m & \simeq & X/\omega_m X \\ \uparrow & & \uparrow \\ A_n & \simeq & X/\omega_n X \end{array} \qquad \begin{array}{ccc} A_m & \simeq & X/\omega_m X \\ \downarrow & & \downarrow \\ A_n & \simeq & X/\omega_n X \end{array}$$

(1) If $H_{0,n} = A_0$, then $\nu_{0,n} X = \omega_n X = \omega_0(\nu_{0,n} X)$. Since $\omega_0 \in \langle p, T \rangle$ and X is a finitely generated Λ-module, we have $\nu_{0,n} X = 0$. Hence, $\omega_n X = 0$ and $A_m \simeq X$ for all $m \geqq n$. (2) It follows from $|A_{n+1}| = |A_n|$ that $X/\omega_{n+1} X \simeq X/\omega_n X$ and hence $\omega_n X = \omega_{n+1} X = \nu_{n,n+1}(\omega_n X)$. Since $\nu_{n,n+1} \in \langle p, T \rangle$, we have $\omega_n X = 0$. Note that $H_{n,n+r} = A_n$ is equivalent to $\nu_{n,n+r} X = \omega_{n+r} X = \omega_n(\nu_{n,n+r} X)$, therefore to $\nu_{n,n+r} X = 0$ because $\omega_n \in \langle p, T \rangle$. Now from the lemma and the assumption $p^r A_n = 0$, we see that $\nu_{n,n+r} X \subset p^r X + \omega_n X \subset \omega_n X = 0$. Hence, $H_{n,n+r} = A_n$.

In the situation of Theorem 2, $|A_n|$ is not bounded if $H_{0,n} \neq A_0$ for all $n \geqq 1$. In this case, we can give an explicit lower bound of $|A_n|$.

Proposition. *Let K/k be as in Theorem 2. Assume that $A_0 \neq 0$ and $H_{0,n} = 0$ for some $n \geqq 0$, then $|A_n| \geqq |A_0| p^n$.*

Proof. We use the left one of the preceding diagrams. First we note that $|A_i| < |A_{i+1}|$ is equivalent to $\omega_i X \neq 0$. Assume that $\omega_{n-1} X = 0$. Then, $A_{n-1} \simeq X/\omega_{n-1} X \simeq X$ and X is finite. If x is any element of X such that $\nu_{0,n} x = 0$, then $x \in \omega_0 X$ because $X/\omega_0 X \to X/\omega_n X$ is injective and hence $\nu_{0,n-1} x = 0$. Next we conclude that $\nu_{0,n-1} X = 0$. In fact, if we assume that $\nu_{0,n-1} X \neq 0$, there exists $x \in X$ such that $\nu_{0,n-1} x \neq 0$. Then we see that $p\nu_{0,n-1} x = \nu_{n-1,n} \nu_{0,n-1} x = \nu_{0,n} x \neq 0$ from the lemma and the above observation. Iterating this operation by replacing x with px, we see that $p^r \nu_{0,n-1} x \neq 0$

for all $r \geqq 0$. This is a contradiction because X is finite. Hence $\nu_{0,n-1}X = 0$. Then, $A_0 \to A_{n-1}$ is a zero map and $A_0 \to A_n$ is also. But this contradicts the assumption $A_0 \neq 0$. Hence $\omega_{n-1}X \neq 0$. Then, for $0 \leqq i \leqq n-1$, we have $\omega_i X \neq 0$ and hence $|A_i| < |A_{i+1}|$. From this inequality, the claim follows.

Example. Finally we apply Theorem 1 to the cyclotomic $\boldsymbol{Z}_3$-extension K of a real quadratic field k. Let $k = \boldsymbol{Q}(\sqrt{m})$, where $m = 3137, 3719, 4409, 6809, 7226$ or 9998. Then (3) is the unique prime ideal of k lying over 3 and it is totally ramified K/k. Furthermore we see that $|A_0| = |A_1| = 9$ by the method of [3]. Hence $|A_n| = 9$ for all $n \geqq 0$. Namely, Greenberg's conjecture is valid for these k's and $p = 3$.

References

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

[2] K. Iwasawa: On $\boldsymbol{Z}_l$-extensions of algebraic number fields. Ann. of Math., **98**, 246–326 (1973).

[3] S. Māki: The determination of units in real cyclic sextic fields. Lect, Notes in Math., vol. 797, Springer-Verlag, Berlin, Heidelberg, New York (1980).