GREENBERG'S CONJECTURE AND THE IWASAWA POLYNOMIAL

Hiroki Sumida

Introduction.

Let k be a finite extension of the field $\mathbb{Q}$ of rational numbers and p a fixed prime number. A Galois extension K of k is called a $\mathbb{Z}_p$-extension when the Galois group $\mathrm{Gal}(K/k)$ is topologically isomorphic to the additive group $\mathbb{Z}_p$ of p-adic integers. Let K be a $\mathbb{Z}_p$-extension of k, $k_n \subset K$ the unique cyclic extension over k of degree p^n and A_n the p-Sylow subgroup of the ideal class group of k_n. We denote by $\sharp A$ the number of elements of a finite set A.

Iwasawa proved the following theorem(see [I2]).

Theorem(Iwasawa). *There exist three integers $\lambda = \lambda(K/k)$, $\mu = \mu(K/k)$ and $\nu = \nu(K/k)$ such that*

$$\sharp A_n = p^{\lambda n + \mu p^n + \nu}$$

for all sufficiently large n.

Every k has at least one $\mathbb{Z}_p$-extension called the cyclotomic $\mathbb{Z}_p$-extension. We denote by k_∞ the cyclotomic $\mathbb{Z}_p$-extension of k.

Greenberg's conjecture. *If k is a totally real number field, then*

$$\lambda(k_\infty/k) = \mu(k_\infty/k) = 0 \qquad .$$

In other words the maximal unramified abelian p-extension of k_∞ is a finite extension.

By [I1], this conjecture is true for $k = \mathbb{Q}$ and p arbitrary. As experimental results, this conjecture has been verified for $p = 3$ and many real quadratic fields with small discriminants in [C], [G1], [FK], [FKW], [F], [K], [T] and [FT],

The main purpose of this paper is to give a "good" necessary and sufficient condition for Greenberg's conjecture. The condition is given in terms of some p-ramified abelian p-extensions of k_n and the Iwasawa polynomial associated to k. Here a "good" condition means that it can be checked for n as little as possible.

To check it, we need a lot of data (an "approximate" Iwasawa polynomial, basis of the ideal class group, that of the unit group and that of the semi-local unit group of k_n).

Now, to explain our condition, we present a criterion for a special case. Let k be a totally real number field and p an odd prime number. Fix a topological generator γ_0 of $\Gamma = \mathrm{Gal}(k_\infty/k)$. Let M be the maximal abelian p-extension of k_∞ unramified outside p, L the maximal unramified abelian p-extension of k_∞ and L' the maximal unramified abelian p-extension of k_∞ in which every prime divisor of k_∞ above p splits completely. Put $Y = \mathrm{Gal}(M/k_\infty)$, $I = \mathrm{Gal}(M/L)$ and $D = \mathrm{Gal}(M/L')$. As usual, we may regard these Γ-modules Y, I and D as $\Lambda = \mathbb{Z}_p[[T]]$-modules by the identification $T = \gamma_0 - 1$. Concerning the Galois group Y, the following facts are known.

Y is a finitely generated Λ-torsion Λ-module (cf. [G1,Theorem 3]).

Y has no non-trivial finite Λ-submodule(cf. [I4,Theorem 18]).

Assume that μ-invariant of Y is zero, i.e. Y is a torsion-free $\mathbb{Z}_p$-module. We denote by $\mathrm{char}(Y)$ the characteristic polynomial of the action of T on Y. Further, let M_n, L_n and L'_n be the maximal abelian extension of k_n in M, L and L' respectively. Then $\mathrm{Gal}(M_n/L'_n)$ is isomorphic to $(D + \omega_n Y)/\omega_n Y$. We can easily obtain the following more or less known criterion.

Criterion(special case). *Assume that* $\mathrm{char}(Y)$ *is irreducible in* $\mathbb{Z}_p[T]$. *Then* Y/D *is finite if only if* $(D + \omega_n Y)/\omega_n Y$ *is not trivial for some integer* $n \geq 0$, *where* $\omega_n = (1+T)^{p^n} - 1$.

This criterion is used mainly when $\mathrm{char}(Y)$ is of degree 1 by some authors(e.g. T. Fukuda, J.S. Kraft, H. Taya). Assume that Leopoldt's conjecture(see, for example, [W,Ch13]) is true for k and p, and that every prime ideal of k above p is fully ramified in k_∞. Then Y/D is finite if and only if Y/I is finite, i.e. Greenberg's conjecture is true for k and p (see Proposition 6).

In this paper, we extend this criterion to general case. As is shown above, when $\mathrm{char}(Y)$ is irreducible, we know a "good" condition. But, when $\mathrm{char}(Y)$ is reducible, the matter becomes much more complicated. In order to obtain a "good" one in general case, we need to study not only $\mathrm{Gal}(M_n/L'_n)$ but also a pair $(\mathrm{Gal}(M_n/k_\infty), \mathrm{Gal}(M_n/L'_n))$. Moreover we need to compute an "approximate" polynomial of $\mathrm{char}(Y)$ exactly. In §3, we give the general criterion(Theorem 3).

As examples, we study real quadratic fields $\mathbb{Q}(\sqrt{m})$ (m:square-free, $1 < m < 10^4$) in which $p = 3$ splits. We explain how to check our criterion for these fields. The total number of such fields is exactly 2279. T. Fukuda and H. Taya verified the conjecture for 2227 fields among these fields by using some data of the ideal class group and the p-unit group of k_1(see [FT]). Further applying our criterion to them, we verify the conjecture for at least 2236 fields. We can give some examples for which the conjecture is true but was not verified before.

An outline of this paper is as follows. In §1 we study some abelian extensions of k_n in M and the Galois groups I, D. In §2 we prepare some propositions concerning Λ and Λ-modules. In §3 we give a necessary and sufficient condition for Greenberg's conjecture in terms of Λ-module structures of certain Galois groups studied in §1. In §4 we give numerical examples. The main parts of this paper are §3 and §4.

Acknowledgements. The author wishes to express his hearty thanks to Professor Shōichi Nakajima, under whose guidance this work was done. He is also grateful to other members of the Number Theory Seminar at Komaba, Tokyo, especially to Professor Takashi Fukuda and Professor Hisao Taya for the tables of §4 and to Professor Humio Ichimura and Professor Masakazu Yamagishi for valuable comments.

§1 Some abelian extensions of k_n in M.

In this section we assume that p is an odd prime number and that every prime ideal of k above p is fully ramified in k_∞.

Let M, L, L', M_n, L_n and L'_n be the same as in Introduction. We fix a non-negative integer n. Let K_n be the maximal unramified abelian p-extension of k_n and K'_n the maximal unramified abelian p-extension of k_n in which every prime ideal of k_n above p splits completely. Further, let S_n be the set of all prime ideals of k_n above p, D_n the subgroup of A_n consisting of classes containing an ideal all of whose prime divisors are contained in S_n and $A'_n = A_n/D_n$. For a non-negative integer n and $\mathfrak{p} \in S_0$, let $\mathfrak{p}_n \in S_n$ be the unique prime ideal lying above $\mathfrak{p}$. For a prime divisor q of a field K, K_q denotes the completion of K at q and $U_q = U_{K_q}$ the principal unit group of K_q. Here we define the following groups:

$$U_n = \{(u_{\mathfrak{p}_n}) \in \prod_{\mathfrak{p}_n \in S_n} U_{\mathfrak{p}_n} \mid \prod_{\mathfrak{p}_n \in S_n} \left(\frac{u_{\mathfrak{p}_n}, k_m/k_n}{\mathfrak{p}_n} \right) = 1 \text{ for all } m \geq n\},$$

$$V_{\mathfrak{p}_n} = \bigcap_{m \geq n} N_{k_{m,\mathfrak{p}_m}/k_{n,\mathfrak{p}_n}} U_{\mathfrak{p}_m}, \quad V_n = \prod_{\mathfrak{p}_n \in S_n} V_{\mathfrak{p}_n}$$

$$W_{\mathfrak{p}_n} = \bigcap_{m \geq n} N_{k_{m,\mathfrak{p}_m}/k_{n,\mathfrak{p}_n}} k^\times_{m,\mathfrak{p}_m}, \quad W_n = \prod_{\mathfrak{p}_n \in S_n} W_{\mathfrak{p}_n}$$

where $\left(\frac{u, k'/k}{\mathfrak{p}}\right)$ is the norm residue symbol. Let u_n be the diagonal map: $k_n^\times \hookrightarrow \prod_{\mathfrak{p}_n \in S_n} k^\times_{n,\mathfrak{p}_n}$, E_n the unit group of k_n and E'_n the p-unit group of k_n. We denote by $\overline{A}$ the topological closure of A. Put

$$\overline{E_n} = \overline{U_n \cap u_n(E_n)}, \quad \overline{E'_n} = \overline{U_n \cap (u_n(E'_n) W_n)}.$$

Here note that

$$\prod_{\mathfrak{p}_n \in S_n} \left(\frac{\varepsilon', k_m/k_n}{\mathfrak{p}_n} \right) = 1$$

for any $\varepsilon' \in E'_n$ and all $m \geq n$ by the product formula.

Proposition 1. *There are isomorphisms:*

$$\begin{aligned}
&(a)\, \mathrm{Gal}(K'_n k_\infty/k_\infty) \cong \mathrm{Gal}(K'_n/k_n) \cong A'_n,\\
&(b)\, \mathrm{Gal}(L'_n/K'_n k_\infty) \cong \mathrm{Gal}(L'_n K_n/K_n k_\infty) \cong U_n/V_n\overline{E'_n},\\
&(c)\, \mathrm{Gal}(L'_n K_n/L'_n) \cong \mathrm{Gal}(K_n/K'_n) \cong D_n,\\
&(d)\, \mathrm{Gal}(L_n/L'_n K_n) \cong V_n\overline{E'_n}/V_n\overline{E_n},\\
&(e)\, \mathrm{Gal}(M_n/L_n) \cong V_n\overline{E_n}/\overline{E_n}.
\end{aligned}$$

Proof. Since we assume that every prime ideal in S_0 is fully ramified in k_∞, we have $K_n \cap k_\infty = k_n$ and $N_{k_m/k_n}\mathfrak{p}_m = \mathfrak{p}_n$ for $m \geq n$. Hence we immediately obtain (a) and (c) by class field theory. By considering k_n as a base field of the cyclotomic $\mathbb{Z}_p$-extension, we will show the other isomorphisms. For $m \geq 0$, put

$$\begin{aligned}
&k^\times_{(m)} = \{(x_\mathfrak{p}) \in (\text{the idèle group of } k) \mid \prod_{\mathfrak{p}} \left(\frac{x_\mathfrak{p}, k_m/k}{\mathfrak{p}} \right) = 1\},\\
&(k^\times_{(m)})' = \{(x_\mathfrak{p}) \in \prod_{\mathfrak{p} \in S_0} k^\times_\mathfrak{p} \mid \prod_{\mathfrak{p} \in S_0} \left(\frac{x_\mathfrak{p}, k_m/k}{\mathfrak{p}} \right) = 1\},\\
&U'_{(m)} = \{(u_\mathfrak{p}) \in \prod_{\mathfrak{p} \in S_0} U_\mathfrak{p} \mid \prod_{\mathfrak{p} \in S_0} \left(\frac{u_\mathfrak{p}, k_m/k}{\mathfrak{p}} \right) = 1\},\\
&W_{\mathfrak{p},(m)} = N_{k_{m,\mathfrak{p}_m}/k_\mathfrak{p}} k^\times_{m,\mathfrak{p}_m}, \quad V_{\mathfrak{p},(m)} = N_{k_{m,\mathfrak{p}_m}/k_\mathfrak{p}} U_{\mathfrak{p}_m}.
\end{aligned}$$

Then we have

$$\begin{aligned}
&(k^\times_{(m)})' \supset U'_{(m)} \supset \prod_{\mathfrak{p} \in S_0} V_{\mathfrak{p},(m)} \supset \prod_{\mathfrak{p} \in S_0} U^{p^m}_{\mathfrak{p}_m},\\
&(k^\times_{(m)})' \supset \prod_{\mathfrak{p} \in S_0} W_{\mathfrak{p},(m)} \supset \prod_{\mathfrak{p} \in S_0} V_{\mathfrak{p},(m)} \supset \prod_{\mathfrak{p} \in S_0} U^{p^m}_{\mathfrak{p}_m}.
\end{aligned}$$

By class field theory, the correspondences between some abelian extensions of k and subgroups of idèle group of k are as follow:

$$\begin{aligned}
&k_m \leftrightarrow k^\times k^\times_{(m)}, \quad k_m K_0 \leftrightarrow k^\times (U'_{(m)} \times \prod_{q \notin S_0} U_q),\\
&k_m K'_0 \leftrightarrow k^\times ((k^\times_{(m)})' \times \prod_{q \notin S_0} U_q).
\end{aligned}$$

Let $M_{0,m}$ be the abelian extension of k corresponding to $k^\times(\prod_{\mathfrak{p}\in S_0} U_{\mathfrak{p}}^{p^m} \times \prod_{q\notin S_0} U_q)$. It is easy to see that $M_{0,m}$ is a finite extension of k_m. Let $L_{0,m} \subseteq M_{0,m}$ the maximal unramified extension of k_m and $L'_{0,m} \subseteq M_{0,m}$ the maximal unramified extension of k_m in which every prime ideal above p splits completely. Then we have the following correspondences.

$$\begin{aligned} L_{0,m} \leftrightarrow &\langle k^\times(U_{\mathfrak{p}} \times \prod_{q\neq\mathfrak{p}} 1)k^\times(\prod_{\mathfrak{p}\in S_0} U_{\mathfrak{p}}^{p^m} \times \prod_{q\notin S_0} U_q) \cap k^\times(U'_{(m)} \times \prod_{q\notin S_0} U_q) \mid \mathfrak{p}\in S_0\rangle \\ &= k^\times(\prod_{\mathfrak{p}\in S_0} V_{\mathfrak{p},(m)} \times \prod_{q\notin S_0} U_q), \\ L'_{0,m} \leftrightarrow &\langle k^\times(k_{\mathfrak{p}}^\times \times \prod_{q\neq\mathfrak{p}} 1)k^\times(\prod_{\mathfrak{p}\in S_0} U_{\mathfrak{p}}^{p^m} \times \prod_{q\notin S_0} U_q) \cap k^\times((k_{(m)}^\times)' \times \prod_{q\notin S_0} U_q) \mid \mathfrak{p}\in S_0\rangle \\ &= k^\times(\prod_{\mathfrak{p}\in S_0} W_{\mathfrak{p},(m)} \times \prod_{q\notin S_0} U_q). \end{aligned}$$

∎

Therefore we have

$$\begin{aligned} &\mathrm{Gal}(L'_{0,m}/K'_0k_m) \cong k^\times((k_{(m)})' \times \prod_{q\notin S_0} U_q)/k^\times(\prod_{\mathfrak{p}\in S_0} W_{\mathfrak{p},(m)} \times \prod_{q\notin S_0} U_q) \\ &\cong (U'_{(m)} \times \prod_{q\notin S_0} 1)k^\times(\prod_{\mathfrak{p}\in S_0} W_{\mathfrak{p},(m)} \times \prod_{q\notin S_0} U_q)/k^\times(\prod_{\mathfrak{p}\in S_0} W_{\mathfrak{p},(m)} \times \prod_{q\notin S_0} U_q) \\ &\cong (U'_{(m)} \times \prod_{q\notin S_0} 1)/(U'_{(m)} \cap (u_0(E'_0)\prod_{\mathfrak{p}\in S_0} W_{\mathfrak{p},(m)})) \times \prod_{q\notin S_0} 1, \end{aligned}$$

$$\begin{aligned} &\mathrm{Gal}(L_{0,m}/L'_{0,m}K_0) \\ &\cong (k^\times(\prod_{\mathfrak{p}\in S_0} W_{\mathfrak{p},(m)} \times \prod_{q\notin S_0} U_q) \cap k^\times(U'_{(m)} \times \prod_{q\notin S_0} U_q))/k^\times(\prod_{\mathfrak{p}\in S_0} V_{\mathfrak{p},(m)} \times \prod_{q\notin S_0} U_q) \\ &\cong ((U'_{(m)} \cap (u_0(E'_0)\prod_{\mathfrak{p}\in S_0} W_{\mathfrak{p},(m)})) \times \prod_{q\notin S_0} 1)k^\times(\prod_{\mathfrak{p}\in S_0} V_{\mathfrak{p},(m)} \times \prod_{q\notin S_0} U_q) \\ &\qquad\qquad /k^\times(\prod_{\mathfrak{p}\in S_0} V_{\mathfrak{p},(m)} \times \prod_{q\notin S_0} U_q) \\ &\cong (U'_{(m)} \cap (u_0(E'_0)\prod_{\mathfrak{p}\in S_0} W_{\mathfrak{p},(m)})) \times \prod_{q\notin S_0} 1/(u_0(E_0)\prod_{\mathfrak{p}\in S_0} V_{\mathfrak{p},(m)}) \times \prod_{q\notin S_0} 1, \end{aligned}$$

$$\begin{aligned}
&\mathrm{Gal}(M_{0,m}/L_{0,m}) \cong k^{\times}(\prod_{\mathfrak{p}\in S_0} V_{\mathfrak{p},(m)} \times \prod_{q\notin S_0} U_q)/k^{\times}(\prod_{\mathfrak{p}\in S_0} U_{\mathfrak{p}}^{p^m} \times \prod_{q\notin S_0} U_q)\\
&\cong ((u_0(E_0)\prod_{\mathfrak{p}\in S_0} V_{\mathfrak{p},(m)}) \times \prod_{q\notin S_0} 1)k^{\times}(\prod_{\mathfrak{p}\in S_0} U_{\mathfrak{p}}^{p^m} \times \prod_{q\notin S_0} U_q)/k^{\times}(\prod_{\mathfrak{p}\in S_0} U_{\mathfrak{p}}^{p^m} \times \prod_{q\notin S_0} U_q)\\
&\cong ((u_0(E_0)\prod_{\mathfrak{p}\in S_0} V_{\mathfrak{p},(m)}) \times \prod_{q\notin S_0} 1)/((u_0(E_0)\prod_{\mathfrak{p}\in S_0} U_{\mathfrak{p}}^{p^m}) \times \prod_{q\notin S_0} 1).
\end{aligned}$$

Since

$$\begin{aligned}
&\mathrm{Gal}(L_0'/K_0'k_\infty) \cong \varprojlim \mathrm{Gal}(L_{0,m}'/K_0'k_m),\\
&\mathrm{Gal}(L_0/L_0'K_0) \cong \varprojlim \mathrm{Gal}(L_{0,m}/L_{0,m}'K_0) \text{ and}\\
&\mathrm{Gal}(M_0/L_0) \cong \varprojlim \mathrm{Gal}(M_{0,m}/L_{0,m}),
\end{aligned}$$

we obtain the isomorphisms(b)(d)(e). □

The following theorem is not needed in the following sections, but is interesting because it gives a relation between capitulation of ideals and the Galois groups I and D. See [G1] about a relation between Greenberg's conjecture and capitulation. Put $H_{n,m}' = \mathrm{Ker}(i_{n,m} : A_n' \to A_m')$ and $H_{n,m} = \mathrm{Ker}(i_{n,m} : A_n \to A_m)$ where $i_{n,m}$ is induced by the natural inclusion map $k_n \hookrightarrow k_m$.

Theorem 1. *Let k be a totally real finite extension of $\mathbb{Q}$ and n a non-negative integer. Assume that Leopoldt's conjecture is valid for $k_m (m \geq n)$ and p. Then*

$$[M_m : L_m'] \geq \sharp H_{n,m}' \cdot [M_n : L_n'] \quad \text{and} \quad [M_m : L_m] \geq \sharp H_{n,m} \cdot [M_n : L_n],$$

In particular if $H_{n,m}' \neq 0$ for some $m \geq n$, then the group $D = \mathrm{Gal}(M/L')$ is not trivial.

Proof. We have the following commutative diagram with exact rows and columns.

$$\begin{tikzcd}
 & 0 & & & \\
 & N \arrow[u] & & & \\
0 \arrow[r] & \mathrm{Gal}(M_m/K_m'k_\infty) \arrow[u] \arrow[r] & \mathrm{Gal}(M_m/k_\infty) \arrow[r] & A_m' \arrow[r] & 0 \\
0 \arrow[r] & \mathrm{Gal}(M_n/K_n'k_\infty) \arrow[u, "\times\nu_{n,m}"] \arrow[r] & \mathrm{Gal}(M_n/k_\infty) \arrow[u, "\times\nu_{n,m}"] \arrow[r] & A_n' \arrow[u, "i_{n,m}"] \arrow[r] & 0 \\
 & 0 \arrow[u] & 0 \arrow[u] & H_{n,m}' \arrow[u] &
\end{tikzcd}$$

where $\nu_{n,m} = \omega_m/\omega_n = ((1+T)^{p^m}-1)/((1+T)^{p^n}-1)$. Commutativity is nothing but [I4,Theorem 8]. The columns are exact by class field theory(cf. Proposition 1(a)). To show the rows are exact, we need the assumption. Since k_m is totally real, Leopoldt's conjecture for k_m and p implies that $[M_m : k_\infty]$ is finite(see [I4,Theorem 2]). Hence ω_m and $\mathrm{char}(\mathrm{Gal}(M/k_\infty))$ are relatively prime. On the other hand, $\mathrm{Gal}(M/k_\infty)$ has no non-trivial finite Λ-submodule (see [I4,Theorem 18]) and $\mathrm{Gal}(M_n/k_\infty) = \mathrm{Gal}(M/k_\infty)/\omega_n \mathrm{Gal}(M/k_\infty)$. Using these facts, we easily see that the rows are exact. Applying the snake lemma to the above diagram, we have an exact sequence:

$$0 \to H'_{n,m} \to N.$$

By the below lemma, we have $[L'_m : K'_m k_\infty] \le [L'_n : K'_n k_\infty]$. Therefore

$$[M_m : L'_m] = \frac{[M_m : K'_m k_\infty]}{[L'_m : K'_m k_\infty]} \ge \frac{[M_n : K'_n k_\infty] \cdot \sharp N}{[L'_n : K'_n k_\infty]} \ge [M_n : L'_n] \cdot \sharp H'_{n,m}.$$

The second inequality can be proved in a similar way. $\square$

Lemma 1. *Let the situation be the same as in Theorem 1. Then* $[L'_m : K'_m k_\infty] \le [L'_n : K'_n k_\infty]$ *and* $[L_m : K_m k_\infty] \le [L_n : K_n k_\infty]$.

Proof. Let $U_{\mathfrak{p}_n} \hookrightarrow U_{\mathfrak{p}_m}$ be the natural inclusion map. Then

$$U_{\mathfrak{p}_n} \hookrightarrow U_{\mathfrak{p}_m} \overset{\text{Norm}}{\to} U_{\mathfrak{p}_n}$$

is a multiplication by p^{m-n}. Put $k_{\infty,\mathfrak{p}_\infty} = \cup_{l\ge 0} k_{l,\mathfrak{p}_l}$ for brevity. By local class field theory, we have the following commutative diagram.

$$\begin{array}{lcc}
\mathrm{Gal}(k_{\infty,\mathfrak{p}_\infty}/k_{n,\mathfrak{p}_n}) & \cong & U_{\mathfrak{p}_n}/V_{\mathfrak{p}_n} \\
\times p^{m-n} \downarrow & & \downarrow \\
\mathrm{Gal}(k_{\infty,\mathfrak{p}_\infty}/k_{m,\mathfrak{p}_m}) & \cong & U_{\mathfrak{p}_m}/V_{\mathfrak{p}_m}.
\end{array}$$

Therefore $i'_{n,m} : U_n/V_n \to U_m/V_m$ induced by the above maps is an isomorphism. By Proposition 1(b) and $E'_n \subseteq E'_m$, we have the first inequality. The second inequality can be proved in a similar way. $\square$

§2 Some propositions concerning Λ.

Let $\mathcal{O}$ be the integer ring of a finite extension over the field $\mathbb{Q}_p$ of p-adic numbers. In this section we give some propositions concerning $\Lambda = \mathcal{O}[[T]]$ which are required in the following sections. Some of them seem to be known, but we bring them up here for convenience. Let π be a generator of the maximal ideal of $\mathcal{O}$ and $P = (\pi, T)$ the unique maximal ideal of Λ. The following proposition is known as Hensel's Lemma.

Proposition 2. *For $f(T) \in \Lambda$, assume that there exist $g_0(T)$, $h_0(T) \in \Lambda$ such that*

$$f(T) \equiv g_0(T)h_0(T) \bmod P^{e+m} \text{ and } (g_0(T), h_0(T)) \supseteq P^e$$

for $m \geq e+1 \geq 1$. Then there exist $g(T), h(T) \in \Lambda$ such that

$$f(T) = g(T)h(T),\ g(T) \equiv g_0(T) \bmod P^m \text{ and } h(T) \equiv h_0(T) \bmod P^m.$$

When we use this proposition, it is convenient to know that $(g_0(T), h_0(T)) \supseteq P^e$ if $(g_0(T), h_0(T), P^{e+1}) \supseteq P^e$. In general for a finitely generated Λ-module L and its submodule L', we have $L' \supseteq P^e L$ if $(L', P^{e+1}L) \supseteq P^e L$ by Nakayama's Lemma($(L' + P^e L)/L' = P((L' + P^e L)/L')$, see [W,Lemma 13.16]).

For $f(T) = \sum_{j=0}^{\infty} a_j T^j \in \Lambda \setminus (\pi)$, by p-adic Weierstrass preparation theorem, we can uniquely write $f(T) = P(T)U(T)$, where $P(T)$ is a distinguished, irreducible polynomial in $\mathcal{O}[T]$ and $U(T) \in \Lambda^{\times}$. Put $\lambda(f(T)) = \min\{j \mid a_j \notin (\pi)\}$, then we have $\lambda(f(T)) = \deg(P(T))$.

Proposition 3. *For $f_1(T), f_2(T) \in \Lambda \setminus (\pi)$, write $f_1(T) = P_1(T)U_1(T)$ and $f_2(T) = P_2(T)U_2(T)$, where $P_1(T)$ and $P_2(T)$ are distinguished polynomials and $U_1(T), U_2(T) \in \Lambda^{\times}$. Assume that*

$$\begin{cases} \lambda(f_1(T)) = \lambda(f_2(T)) = n \geq 1, \quad f_1(T), f_2(T) \in P^l \text{ for } l \geq 1 \\ f_1(T) \equiv f_2(T) \bmod P^{kn+1} \text{ for } k \geq 1. \end{cases}$$

Then $P_1(T) \equiv P_2(T) \bmod P^{k+l}$.

Proof. Let $f_i = \sum_{j=0}^{\infty} a_{i,j} T^j$ and put $R_i = \sum_{j=0}^{n-1} (a_{i,j}/\pi) T^j \in \mathcal{O}[T]$ and $V_i = \sum_{j=0}^{\infty} a_{i,j+n} T^j \in \Lambda^{\times}$ $(i = 1, 2)$. We define an operation $\tau = \tau_n : \Lambda \to \Lambda$ by $\tau(\sum_{j=0}^{\infty} b_j T^j) = \sum_{j=n}^{\infty} b_j T^{j-n}$. Then we have

$$U_i^{-1} = \frac{1}{V_i} \sum_{j=0}^{\infty} (-1)^j \pi^j (\tau \cdot \frac{R_i}{V_i})^j \cdot 1.$$

Here, for $h \in \Lambda$, $\tau \cdot h$ operates on $f \in \Lambda$ by $(\tau \cdot h) \cdot f = \tau(hf)$. (See [W,Proposition 7.2] and its proof. Under the notations there, we get the above formula from the last one of [W,page 114] by taking $f = f_i$ and $g = P_i$.) We have $R_1 \equiv R_2 \bmod P^{kn}$, $V_1^{-1} \equiv V_2^{-1} \bmod P^{kn+1-n}$ and $\tau(P^m) = P^{m-n}$ for $m \geq n$. Since

$$\pi^j \tau^j (P^{kn+1-n}) \subseteq P^{(n-1)(k-1-j)+k} \text{ for } 1 \leq j \leq k-1,$$

$U_1^{-1} \equiv U_2^{-1} \bmod P^k$. Therefore we have

$$P_1 - P_2 = f_1(U_1^{-1} - U_2^{-1}) + (f_1 - f_2)U_2^{-1} \equiv 0 \bmod P^{k+l}. \quad \square$$

For a finitely generated Λ-torsion Λ-module N, there is a Λ-homomorphism:

$$N \to \bigoplus_{j=1}^{r} \Lambda/(\pi^{\mu_j}) \oplus \bigoplus_{i=1}^{l} \Lambda/(f_i(T)^{n_i})$$

whose kernel and cokernel are finite, where μ_j and n_i are non-negative integers and $f_i(T)$ a distinguished, irreducible polynomial in $\mathcal{O}[T]$ (see, for example, [W,Ch13]). Put

$$\mathrm{char}(N) = \prod_{j=1}^{r} \pi^{\mu_j} \prod_{i=1}^{l} f_i(T)^{n_i}.$$

For a power series $f(T) \in \Lambda$, let $\mathcal{M}_{f(T)}$ be the set of Λ-isomorphism classes of finitely generated Λ-torsion Λ-modules N such that

$$\begin{cases} (\mathrm{char}(N)) = (f(T)) \\ N \text{ has no non-trivial finite } \Lambda\text{-submodule.} \end{cases}$$

For $f(T) \in \Lambda \setminus (0)$, we say $f(T)$ is square-free when there is no element $g(T) \in \Lambda \setminus \Lambda^\times$ such that $f(T)/g(T)^2 \in \Lambda$. Further, we say $f(T)$ is irreducible when there is no element $g(T) \in \Lambda \setminus \Lambda^\times$ such that $f(T)/g(T) \in \Lambda \setminus \Lambda^\times$.

Theorem 2. *For $f(T) \in \Lambda \setminus (\pi)$, $\mathcal{M}_{f(T)}$ is a finite set if and only if $f(T)$ is square-free.*

Proof. {Necessity} Write $f = h^2 \prod_{i=1}^{l} g_i$, where $h,\ g_i \in \Lambda \setminus \Lambda^\times$ are irreducible elements. For $k \geq 0$, let N_k be the submodule $(\pi^k, h)/(h^2)$ of $\Lambda/(h^2)$. The isomorphism class of N_k is contained in $\mathcal{M}_{h^2}$. Since $\pi^k \notin (\pi^{k+1}, h)$,

$$\begin{aligned} &[\mathrm{Ker}(\times h : N_k \to N_k) : \mathrm{Im}(\times h : N_k \to N_k)] \\ &= [\Lambda/(h) : (\pi^k, h)/(h)] = [\Lambda : (\pi^k, h)] \end{aligned}$$

is strictly monotonically increasing for k. Therefore N_k is not isomorphic to $N_{k'}$ if $k \neq k'$. Consider submodules $N_k \oplus \bigoplus_{i=1}^{l} \Lambda/(g_i)$ of $\Lambda/(h^2) \oplus \bigoplus_{i=1}^{l} \Lambda/(g_i)$. Any two of them are not isomorphic.

{Sufficiency} Step 1: We first prove that $\mathcal{M}_g$ is a finite set when g is an irreducible element of Λ. Put $n = \lambda(g)$. For every element $[N] \in \mathcal{M}_g$, fix a map:

$$\phi_N : N \hookrightarrow \Lambda/(g)$$

such that $\phi_N(N)$ is not included in $(\pi, g)/(g)$. Then $\phi_N(N)$ contains an element $\sum_{j=0}^{n-1} a_{N,j} T^j \bmod g$ where $a_{N,j} \in \mathcal{O}$ and $a_{N,n-1} \notin (\pi)$. We may write

$$g = (\sum_{j=0}^{n-1} a_{N,j} T^j) q_N + r_N$$

for $q_N, r_N \in \Lambda$ with $\lambda(q_N) = 1$ and $\lambda(r_N) \leq n-2$. Assume that for any k there exists an element $[N_k]$ in $\mathcal{M}_g$ such that π^k divides r_{N_k}. Then we have a subsequence of $\{(\sum_{j=0}^{n-1} a_{N_k,j}T^j, q_{N_k})\}$ which converges to $(Q, R) \in (\Lambda \backslash \Lambda^\times) \times (\Lambda \backslash \Lambda^\times)$. Since $r_{N_k} \to 0$ as $k \to \infty$, $g = QR$. This contradicts the above assumption. Hence there exists a non-negative integer c such that c is independent of the choice of N and that π^{c+1} does not divide r_N. Therefore $(r_N \bmod g) (\subseteq \phi_N(N))$ contains an element $\pi^c \sum_{j=0}^{n-2} b_{N,j}T^j \bmod g$ where $b_{N,j} \in \mathcal{O}$ and $b_{N,n-2} \notin (\pi)$. Next write

$$\pi^c g = \pi^c (\sum_{j=0}^{n-2} b_{N,j}T^j) q'_N + \pi^c r'_N,$$

for $q'_N, r'_N \in \Lambda$ with $\lambda(q'_N) = 2$ and $\lambda(r'_N) \leq n-3$. By the irreducibility of g we can show that $(\pi^c r'_N \bmod g)$ contains an element $\pi^{c'} \sum_{j=0}^{n-3} c_{N,j}T^j \bmod g$ where $c_{N,j} \in \mathcal{O}$, $c_{N,n-3} \notin (\pi)$ and c' is independent of the choice of N. By continuing this argument, we can show that $\phi_N(N)$ contains $\pi^{c"} \bmod g$ where $c"$ is independent of the choice of N. Therefore $\mathcal{M}_g$ is a finite set, in fact

$$\sharp \mathcal{M}_g \leq \sharp \{\Lambda\text{-submodules of a finite } \Lambda\text{-module } \Lambda/(g, \pi^{c"})\}.$$

Step 2: Let $f = \prod_{i=1}^{l} f_i$, where f_i is an irreducible element of Λ. If f is square-free, f_i and f_j are relatively prime for $i \neq j$. Let $L = \bigoplus_{i=1}^{l} \Lambda/(f_i)$ and

$$\mathrm{Pr}_i : L \to L \quad x_1 \oplus ... x_{i-1} \oplus x_i \oplus x_{i+1} ... \oplus x_l \mapsto 0 \oplus ... 0 \oplus x_i \oplus 0 ... \oplus 0.$$

For every $[N] \in \mathcal{M}_f$, fix a map

$$\phi_N : N \hookrightarrow L \quad \text{ such that } \mathrm{Pr}_i(\phi_N(N)) \not\subseteq (\pi, f_i)L \quad \text{ for all } i.$$

By step 1, $\mathrm{Pr}_i(\phi_N(N))$ includes L_i which is independent of N and is of finite index in $0 \oplus ... 0 \oplus \Lambda/(f_i) \oplus 0 ... \oplus 0$. Since $\prod_{j=1, j\neq i}^{l} f_j$ and f_i are relatively prime, $\sum_{i=1}^{l} (\prod_{j=1,j\neq i}^{l} f_j) L_i$ is of finite index in L. Here $\phi_N(N)$ includes a submodule $\sum_{i=1}^{l} (\prod_{j=1,j\neq i}^{l} f_j) L_i$ of L, which proves "if part" of this theorem. □

For $\Lambda/(\omega_n)$-modules $A \supseteq B$ and $C \supseteq D$, we say (A, B) is $\Lambda/(\omega_n)$- isomorphic to (C, D) when there exists a $\Lambda/(\omega_n)$-isomorphism from A to C which maps B onto D. We denote the $\Lambda/(\omega_n)$-isomorphism class of (A, B) by $[A, B]_n$.

Fix a power series $f(T) \in \Lambda \setminus (\pi)$. For $[N] \in \mathcal{M}_{f(T)}$, put $\mathcal{N}_N = \{N' \mid N' \subset N \text{ with } \mathrm{char}(N') \neq \mathrm{char}(N)\}$. For a non-negative integer n, define

$$\mathcal{L}_{f(T),n} = \{[N/\omega_n N, (N' + \omega_n N)/\omega_n N]_n \mid [N] \in M_{f(T)},\ N' \in \mathcal{N}_N\}.$$

In Proposition 4, we assert that $\mathcal{L}_{f^*(T),n} = \mathcal{L}_{f(T),n}$ if $f(T)$ is square-free and $f^*(T)$ is sufficiently "close" to $f(T)$. Here we define the "closeness" as follows.

If there exists $u^*(T) \in \Lambda^\times$ such that $f^*(T)u^*(T) \equiv f(T) \bmod P^m$, then we write $(f^*(T)) \equiv (f(T)) \bmod P^m$. Moreover define

$$\begin{aligned} m(f(T), n) = \min\{m \mid \mathcal{L}_{f(T),n} = \mathcal{L}_{f^*(T),n} &\text{ for all } f^*(T) \in \Lambda \\ &\text{with } (f^*(T)) \equiv (f(T)) \bmod P^m\}. \end{aligned}$$

By putting $P^\infty = 0$, we have $0 \le m(f(T), n) \le \infty$. From the definition of $m(f(T), n)$, it is easily shown that

$$m(f^*(T), n) = m(f(T), n), \text{ if } (f^*(T)) \equiv (f(T)) \bmod P^{m(f(T),n)}.$$

From now on, assume that $f(T)$ is square-free. Before giving Proposition 4, we show that a factorization of $f^*(T)$ is similar to that of $f(T)$ if $f^*(T)$ is sufficiently "close" to $f(T)$. We fix a factorization of $f(T)$ in Λ: $f(T) = \prod_{i=1}^{l} f_i(T)$ where $f_i(T) \in \Lambda \setminus \Lambda^\times$ is irreducible.

For $f(T)$ and a non-negative integer m, define

$$m_{f(T)}(m) = \min\{m' \mid m' \text{ satisfies the property(A)}\}$$

$$\text{(A)} \quad \begin{cases} \text{if } (f^*(T)) \equiv (f(T)) \bmod P^{m'}, \text{ then there exist } f_i^*(T) \in \Lambda \ (1 \le i \le l) \\ \text{satisfying } (f_i^*(T)) \equiv (f_i(T)) \bmod P^m \text{ and } f^*(T) = \prod_{i=1}^{l} f_i^*(T). \end{cases}$$

By using Proposition 2 repeatedly, we can show that there exists an integer m' satisfying the above and hence $m_{f(T)}(m) < \infty$. It is easy to see that $m_{f(T)}(m)$ is independent of the choice of the factorization.

Further we want $f_i^*(T)$ to be irreducible for all i. For an irreducible element $g(T) \in \Lambda \setminus (\pi)$, define

$$m_0(g(T)) = \min\{m' \mid m' \text{ satisfies the property(B)}\}$$

$$\text{(B)} \qquad \text{if } (g^*(T)) \equiv (g(T)) \bmod P^{m'} \text{ then } g^*(T) \text{ is irreducible.}$$

Since Λ is compact, there exists such an integer m' and $m_0(g(T)) < \infty$. We easily see that $m_0(g(T)) > \lambda(g(T))$.

Put $e_{i,j} = \min\{e" \mid (f_i(T), f_j(T)) \supseteq P^{e"}\}$, $e = \max_{i<j}\{e_{i,j}\}$ and $M = \max_{1 \le i \le l}\{m_0(f_i(T)), e+1\}$. Assume that $(f^*(T)) \equiv (f(T)) \bmod P^{m_{f(T)}(M)}$. Then there exist $f_i^*(T) \in \Lambda (1 \le i \le l)$ such that

$$\begin{cases} f_i^*(T) \text{ is irreducible in } \Lambda, \quad f^*(T) = \prod_{i=1}^{l} f_i^*(T) \\ (f_i^*(T), f_j^*(T)) \supseteq P^e \text{ for } i < j, \quad \lambda(f_i^*(T)) = \lambda(f_i(T)). \end{cases}$$

From the first three properties, $f^*(T)$ is square-free. Put

$$W = \bigoplus_{i=1}^{l} \Lambda, \quad F = (0 \oplus ...0 \oplus f_i(T) \oplus 0... \oplus 0)_{1 \leq i \leq l},$$
$$F^* = (0 \oplus ...0 \oplus f_i^*(T) \oplus 0... \oplus 0)_{1 \leq i \leq l}.$$

Let $\mathrm{Pr}'_i : W \to W$ be the map defined by

$$x_1 \oplus ...x_{i-1} \oplus x_i \oplus x_{i+1}... \oplus x_l \mapsto 0 \oplus ...0 \oplus x_i \oplus 0... \oplus 0.$$

We define a finite set of some submodules of W associated to $f(T)$. In the proof of Theorem 2(sufficiency), we show that there exists a non-negative integer c" such that $P^{c"}W \subseteq Z+F$ for all submodule Z of W with $\mathrm{Pr}'_i Z \not\subseteq (f_i(T), \pi)W$ for all i. Let $c = c(f(T))$ be the minimum integer c" satisfying the above. Define

$$\mathcal{Z} = \mathcal{Z}(f(T)) = \{Z \subseteq W \mid Z \supseteq P^c W,\ \mathrm{Pr}'_i(Z) \not\subseteq (\pi, f_i(T))W \text{ for all } i\}.$$

Proposition 4. *Let $f(T)$ be a square-free power series in $\Lambda \setminus (\pi)$.*
(a)If $(f^*(T)) \equiv (f(T)) \bmod P^{m_{f(T)}(\max\{c+1,M\})}$, then for any $[N^*] \in \mathcal{M}_{f^*(T)}$, there exists an element $Z \in \mathcal{Z}$ such that $N^* \cong (Z + F^*)/F^*$. In particular $\{\sharp\mathcal{M}_{f^*(T)} \mid (f^*(T)) \equiv (f(T)) \bmod P^{m_{f(T)}(\max\{c+1,M\})}\}$ is bounded.
(b)Assume that ω_n and $f(T)$ are relatively prime. Then there exist some integers $m_{1,n}$ and $m_{2,n}(\geq \max\{c+1, M\})$ such that

$$\omega_n Z + F^* \supseteq P^{m_{1,n}} W \ \textit{if}\ (f(T)) \equiv (f^*(T)) \bmod P^{m_{f(T)}(m_{2,n})}$$

for any $Z \in \mathcal{Z}$. Moreover the following inequality holds

$$m(f(T), n) \leq m_{f(T)}(\max\{m_{1,n}, m_{2,n}\}).$$

Proof. (a) Assume that $(f^*) \equiv (f) \bmod P^{m_f(M)}$. For each $[N^*] \in \mathcal{M}_{f^*}$, fix a map

$$\phi_{N^*} : N^* \hookrightarrow L^* = \bigoplus_{i=1}^{l} \Lambda/(f_i^*) \text{ such that } \mathrm{Pr}_i(\phi_{N^*}(N^*)) \not\subseteq (\pi, f_i^*)L^* \text{ for all } i.$$

Moreover we choose a Λ-submodule Z_{N^*} of W satisfying

$$\phi_{N^*}(N^*) = (Z_{N^*} + F^*)/F^*.$$

Since $\mathrm{Pr}'_i(Z_{N^*}) \not\subseteq (\pi, f_i^*)W = (\pi, f_i)W$ for all i, $Z_{N^*} + F \supseteq P^c W$. If $(f_i) \equiv (f_i^*) \bmod P^{c+1}$ for all i, $Z_{N^*} + F^* + P^{c+1}W \supseteq Z_{N^*} + F \supseteq P^c W$. By Nakayama's lemma, this implies $Z_{N^*} + F^* \supseteq P^c W$. Hence, for any N^*, we can choose Z_{N^*} so that $Z_{N^*} \supseteq P^c W$ and $\mathrm{Pr}'_i(Z_{N^*}) \not\subseteq (\pi, f_i)W$ for all i. Since $\mathcal{Z}$ is a finite set, (a) follows.

(b): First note that

$$\omega_n Z + F^* \supseteq \sum_{i=1}^{l} 0 \oplus ...0 \oplus (\omega_n P^c, f_i^*) \oplus 0... \oplus 0$$

and that $(\omega_n P^c, f_i^*) \supseteq P^c(\omega_n, f_i^*)$. Since f_i and ω_n are relatively prime, we can take integers $m_{1,n} = m_{1,n}(f)$ and $m_{2,n} = m_{2,n}(f)(\geq \max\{c+1, M\})$ such that

$$\omega_n Z + F^* \supseteq P^{m_{1,n}} W \text{ if } (f_i) \equiv (f_i^*) \bmod P^{m_{2,n}}$$

for any $Z \in \mathcal{Z}$. This shows the first assertion. Next, let us prove $\mathcal{L}_{f^*,n} = \mathcal{L}_{f,n}$. Put $m' = \max\{m_{1,n}, m_{2,n}\}$ and assume that $(f_i) \equiv (f_i^*) \bmod P^{m'}$ for all i. Let $[N^*]$ be any element of $\mathcal{M}_{f^*}$ and N" any element of $\mathcal{N}_{N^*}$. Then, by (a), there is an element $Z \in \mathcal{Z}$ such that $N^* \cong (Z + F^*)/F^*$. Put $N = (Z + F)/F$. Then $[N] \in \mathcal{M}_f$. We easily see that there is a submodule Z" of $Z + F^*$ such that

$$N\text{"} \cong (Z\text{"} + F^*)/F^*, \quad \mathrm{Pr}'_i(Z\text{"}) \subseteq f_i^* W \text{ for some } i.$$

Fix i such that $\mathrm{Pr}'_i(Z\text{"}) \subseteq f_i^* W$. Let ι_i be the isomorphism

$$\iota_i : (f_i^*) \to (f_i) \quad x f_i^* \mapsto x f_i.$$

Define a Λ-submodule Z' of W by

$$Z' = \{x_1 \oplus ...x_{i-1} \oplus \iota_i(x_i) \oplus x_{i+1}... \oplus x_l \mid x_1 \oplus ...x_{i-1} \oplus x_i \oplus x_{i+1}... \oplus x_l \in Z\text{"}\}.$$

Put $N' = (Z' + F)/F$. Then, as $\mathrm{Pr}'_i(Z') \subseteq f_i W$, $N' \in \mathcal{N}_N$. Now let us prove $[N^*/\omega_n N^*, N\text{"} + \omega_n N^*/\omega_n N^*]_n = [N/\omega_n N, N' + \omega_n N/\omega_n N]_n$. We have

$$\begin{aligned}(Z + F^*)/(\omega_n Z + F^*) &= (Z + F^* + P^{m_{1,n}} W)/(\omega_n Z + F^* + P^{m_{1,n}} W) \\ &= (Z + F + P^{m_{1,n}} W)/(\omega_n Z + F + P^{m_{1,n}} W) \\ &= (Z + F)/(\omega_n Z + F).\end{aligned}$$

On the other hand, we have

$$(Z\text{"} + \omega_n Z + F^*)/(\omega_n Z + F^*) = (Z' + \omega_n Z + F)/(\omega_n Z + F).$$

Therefore $\mathcal{L}_{f^*,n} \subseteq \mathcal{L}_{f,n}$. Similarly we can show that $\mathcal{L}_{f^*,n} \supseteq \mathcal{L}_{f,n}$. $\square$

Remark 1. Here we give an upper bound for $m(f(T), n)$. Put

$$e_i = \min\{e" \mid (\prod_{j=i+1}^{l} f_j(T), f_i(T)) \supseteq P^{e"}\}, \quad e' = \max\{e_i \mid 1 \leq i \leq l-1\}.$$

Then $\max\{m_{1,n}, m_{2,n}, e'+1\} + (\sum_{j=i}^{l-1} e_j) - e_i \geq e_i + 1$ for $1 \leq i \leq l-1$(if $l = 1$, put $e' = 0$). Hence we have

$$m(f(T), n) \leq m_{f(T)}(\max\{m_{1,n}, m_{2,n}\}) \leq \max\{m_{1,n}, m_{2,n}, e'+1\} + \sum_{i=1}^{l-1} e_i$$

by using Proposition 2 repeatedly.

For a power series $f(T) \in \Lambda \setminus (\pi)$ and $[N] \in \mathcal{M}_{f(T)}$, define

$$n(f(T), N) = \min\{n \mid n \text{ satisfies the property(C)}\}$$

(C) $\qquad N/\omega_n N \ncong N'/\omega_n N'$ for all $[N'] \in \mathcal{M}_{f(T)}$ with $[N'] \neq [N]$.

Put $n(f(T)) = \max\{n(f(T), N) \mid [N] \in \mathcal{M}_{f(T)}\}$ By putting $\omega_\infty = 0$, we have $0 \leq n(f(T), N) \leq n(f(T)) \leq \infty$.

Proposition 5. *Assume that $f(T) \in \Lambda \setminus (\pi)$ is square-free. Then $n(f(T))$ is finite.*

Proof. Assume that for $[N], [N'] \in \mathcal{M}_f$ and all n there exist isomorphisms $\phi_n : N/\omega_n N \xrightarrow{\sim} N'/\omega_n N'$. Let $N = (n_1, n_2, ..., n_t)$. Since N' is compact, there exist $n'_1, ..., n'_t \in N'$ which satisfy the following property: for any n there exists some integer $m \geq n-1$ such that $\phi_m(n_i) \equiv n'_i \operatorname{mod}(p, T)^n N'$. Then the map $\phi : N \to N'$ $(\phi(n_i) = n'_i)$ is a Λ-isomorphism. Therefore if $N \ncong N'$, then there exists some integer n such that $N/\omega_n N \ncong N'/\omega_n N'$. By Theorem 2 we can show that $n(f)$ is finite. □

§3 A necessary and sufficient condition.

In this section we give a necessary and sufficient condition for Greenberg's conjecture in terms of Λ-module structures of certain Galois groups. Let k be a totally real number field and p an odd prime number. We use the same notation as in the preceding sections. Put $\Lambda = \mathbb{Z}_p[[T]]$.

Proposition 6. *Assume that every prime ideal of k above p is fully ramified in k_∞ and that Leopoldt's conjecture is true for k and p. Then the following statements are equivalent.*

(1) Y/I *is finite.*

(2) $\mathrm{char}(Y) = \mathrm{char}(D)$.

This proposition is easily obtained by the following lemma.

Lemma 2. *Let the situation be the same as in Proposition 6. Then D/I is finite.*

Proof. We have $D/I \cong \lim_{\leftarrow} D_n$, where the projective limit is taken with respect to relative norms. Leopoldt's conjecture implies that the order of the maximal Γ-invariant submodule A_n^Γ of A_n is bounded as $n \to \infty$ (see [G1,Proposition 1]). Since $D_n \subseteq A_n^\Gamma$, the assertion follows. □

The following theorem and Proposition 6 give a necessary and sufficient condition for Greenberg's conjecture for k and p.

Theorem 3. *Assume that p does not divide* $\mathrm{char}(Y)$. *Then* $\mathrm{char}(D) = \mathrm{char}(Y)$ *if and only if there exist a non-negative integer n and a power series $f^*(T) \in \Lambda \setminus (\pi)$ satisfying* (1) *and* (2)*:*

(1) $(f^*(T)) \equiv (\mathrm{char}(Y)) \mod P^{m(f^*(T),n)}$

(2) *there is no pair* $(N^*, N")$ *with* $[N^*] \in \mathcal{M}_{f^*(T)}$, $N" \in \mathcal{N}_{N^*}$ *such that*
$$[Y/\omega_n Y, (D+\omega_n Y)/\omega_n Y]_n = [N^*/\omega_n N^*, (N" + \omega_n N^*)/\omega_n N^*]_n.$$

Proof. By [I4,Theorem 18], Y has no non-trivial finite Λ-submodule if $p \neq 2$. Using this fact, we can prove this theorem.

{Necessity} Assume that $\mathrm{char}(D) = \mathrm{char}(Y)$ and that $\lambda(f^*) = \lambda(\mathrm{char}(Y))$. For any $[N^*] \in \mathcal{M}_{f^*}$ and $N" \in \mathcal{N}_{N^*}$, $\mathbb{Z}_p$-rank of $N"$ is smaller than that of D. For all sufficiently large n, $\mathbb{Z}_p$-rank of $N"$(resp. D) is equal to the minimum number of generators of $\mathbb{Z}_p$-module $(N" + \omega_n N^*)/\omega_n N^*$(resp. $(D+\omega_n Y)/\omega_n Y$). Therefore the necessity follows.

{Sufficiency} Assume that $(f^*) \equiv (\mathrm{char}(Y)) \mod P^{m(f^*,n)}$. Then we have $m(f^*, n) = m(\mathrm{char}(Y), n)$. Therefore the sufficiency immediately follows from the definition of $m(\mathrm{char}(Y), n)$ □

Remark 2. As is easily seen, $Y/\omega_n Y \cong \mathrm{Gal}(M_n/k_\infty)$ and $(D+\omega_n Y)/\omega_n Y \cong \mathrm{Gal}(M_n/L_n')$. Hence, by class field theory, we can obtain knowledge on the isomorphism class $[Y/\omega_n Y, (D+\omega_n Y)/\omega_n Y]_n$ from some data of k_n(cf. Proposition 1). Next, assume k is abelian. Then we can calculate $\mathrm{char}(Y) \mod P^m$ for any

m from the Stickelberger elements by virtue of the Iwasawa main conjecture. Thus, we can obtain information on $[N^*/\omega_n N^*, (N" + \omega_n N^*)/\omega_n N^*]_n$. Further we have an upper bound for $m(\mathrm{char}(Y), n)$ when $\mathrm{char}(Y)$ is square-free(see Remark 1). For numerical calculations, see §4.

For an abelian field k, let Ψ be an irreducible character of $\Delta = \mathrm{Gal}(k/\mathbb{Q})$ over $\mathbb{Q}_p$. If p does not divide $[k : \mathbb{Q}]$ we can replace Y, D by $e_\Psi Y$, $e_\Psi D$ respectively in Theorem 3 where e_Ψ is the idempotent of Ψ, i.e. $e_\Psi = \sharp\Delta^{-1}\sum_{\sigma\in\Delta}\Psi(\sigma)\sigma^{-1}$.

We explicitly write down this condition in some cases.

Since we assume that $p \neq 2$ and that p does not divide $\mathrm{char}(Y)$, there exists an injective Λ-homomorphism with finite cokernel:

$$Y \hookrightarrow \bigoplus_{i=1}^{l} \Lambda/(f_i(T)^{n_i}),$$

where n_i is a positive integer and $f_i(T)$ a distinguished, irreducible polynomial in $\mathbb{Z}_p[T]$. Then $\mathrm{char}(Y) = \prod_{i=1}^{l} f_i(T)^{n_i}$.

{**Case 0:**Y/D **is trivial.**}

This is known as a trivial case(cf. [FK]).

Proposition 7. *Assume that* $Y/(D + \omega_0 Y) = 0$*, then* $Y = D$*. In particular* $\mathrm{char}(D) = \mathrm{char}(Y)$*.*

Proof. In this case, we have $(Y/D)/\omega_0(Y/D) = 0$. This implies that $(Y/D)/(p, T)(Y/D)$ is trivial. By Nakayama's Lemma, we have $Y/D = 0$. □

{**Case 1:**$\mathrm{char}(Y)$ **is distinguished, irreducible in** $\mathbb{Z}_p[T]$**.**}

$l = 1$ and $n_1 = 1$.

Proposition 8. *For any irreducible power series* $f(T) \in \Lambda \setminus (\pi)$*, and* $[N] \in \mathcal{M}_{f(T)}$*,* $\mathcal{N}_N = \{(0)\}$*.*

Proof. Since N has no non-trivial finite Λ-submodule, this proposition immediately follows. □

Theorem 3(case 1). *Assume that* p *dose not divide* $\mathrm{char}(Y)$*. Then* $\mathrm{char}(D) = \mathrm{char}(Y)$ *if and only if there exist a non-negative integer* n *and a power series* $f^*(T) \in \Lambda \setminus (\pi)$ *satisfying* (1) *and* (2)*:*

$$(1)\ (f^*(T)) \equiv (\mathrm{char}(Y)) \mod P^{m(f^*(T),n)}$$
$$(2)\ (D + \omega_n Y)/\omega_n Y \neq 0.$$

Proof. By Proposition 8 and Theorem 3, the assertion easily follows. □

Remark 3. In this case we need not study a pair (Y, D) to give a necessary and sufficient condition. Hence we can replace $m(f^*(T), n)$ by $m_0(f^*(T))$ i.e. all we have to know is the irreducibility of $\mathrm{char}(Y)$. In [K] and [OT], they explicitly give some procedures to check the non-triviality of $\mathrm{Gal}(M_0/L_0')$ in some case.

Let $l = 1, f_1(T) = T - a, a \in p\mathbb{Z}_p$ $(a \neq 0)$ and $n_1 = 1$. Put $\alpha = v_p(a)$, where v_p is the normalized p-adic valuation.

Proposition 9. *$\mathcal{M}_{T-a} = \{[N] \mid N = \Lambda/(T-a)\}, \mathcal{N}_N = \{(0)\}, n(T-a) = 0$ and $m(T-a, n) = \max\{\ \alpha + n, \alpha + 1\}$.*

Proof. We prove that $m(T-a, n) = \max\{\ \alpha + n, \alpha + 1\}$(the other assertions can be easily proved). If $(f^*) \equiv (T-a) \bmod P^2$ then $f^* = (T - a^*)u^*$ for some $u^* \in \Lambda^\times$ and $a^* \in p\mathbb{Z}_p$. By Proposition 3 if $(f^*) \equiv (T-a) \bmod P^{\alpha+1}$, $T - a \equiv T - a^* \bmod P^{\alpha+1}$. Note that $v_p(\omega_n(a)) = \alpha + n$, where $\omega_n(a) = (1+a)^{p^n} - 1$. Hence if $(T-a) \equiv (T-a^*) \bmod P^{\alpha+1}$, then $(T - a^*, \omega_n) \supseteq P^{\alpha+n}$. We easily see that $\max\{c+1, M\} \leq \max\{\alpha+1, 2\} = \alpha + 1$. Therefore

$$m(T-a, n) \leq \max\{m_{1,n} = \alpha + n, m_{2,n} = \alpha + 1\}$$

(see Remark 1). If $n = 0$, $\max\{\alpha + n, \alpha + 1\} = \alpha + 1$. Put $f^* = T$ and $N^* = \Lambda/(f^*)$. Then $f^* \equiv T - a \bmod P^\alpha$. We can see $N^*/\omega_0 N^* \ncong N/\omega_0 N$. If $n \geq 1$, $\max\{\alpha+n, \alpha+1\} = \alpha+n$. Put $f^* = T - (a + p^{\alpha+n-1})$ and $N^* = \Lambda/(f^*)$. Then $f^* \equiv T - a \bmod P^{\alpha+n-1}$ and $N^*/\omega_n N^*$ is a cyclic group of order $\geq p^{\alpha+n}$. Since $(T-a)(N^*/\omega_n N^*)$ is not trivial, $N^*/\omega_n N^* \ncong N/\omega_n N$. $\square$

{**Case 2:**$\mathrm{char}(Y)$ **is distinguished, square-free, reducible of degree 2.**}
$l = 2$, $f_1(T) = T - a$, $f_2(T) = T - b$, $a, b \in p\mathbb{Z}_p$ $(a \neq b,\ ab \neq 0)$ and $n_1 = n_2 = 1$. Put $\alpha = v_p(a), \beta = v_p(b)$ and $e = v_p(a-b)$. Assume that $\alpha \leq \beta$.

Proposition 10. *$\sharp\mathcal{M}_{(T-a)(T-b)} = e + 1$ and*

$$\mathcal{M}_{(T-a)(T-b)} = \{[N_k] \mid N_k = (1 \oplus 1, 0 \oplus p^k) \subseteq \Lambda/(T-a) \oplus \Lambda/(T-b)\ \ 0 \leq k \leq e\},$$

where $c \oplus d = c \bmod (T-a) \oplus d \bmod (T-b)$.

Proof. For $[N] \in \mathcal{M}_{(T-a)(T-b)}$, there exists an injective Λ-homomorphism: $\phi_N : N \to \Lambda/(T-a) \oplus \Lambda/(T-b)$. Any element in $\Lambda/(T-a) \oplus \Lambda/(T-b)$ can be expressed as $c \oplus d$, where $c, d \in \mathbb{Z}_p$. Let $m = \min\{i | p^i \oplus d \in \phi(N)\}$ and $n = \min\{i | 0 \oplus p^i \in \phi(N)\}$. Then N is isomorphic to $(p^m \oplus d, 0 \oplus p^n)$ for some $d \in \mathbb{Z}_p$. Since $(T-a)(p^m \oplus d) = 0 \oplus (b-a)d$, $N \cong (p^m \oplus 1, 0 \oplus p^k) \cong (1 \oplus 1, 0 \oplus p^k) = N_k$, where $0 \leq k \leq e$. Since

$$[\mathrm{Ker}(\times(T-b) : N_k \to N_k) : \mathrm{Im}(\times(T-a) : N_k \to N_k)] = p^{e-k},$$

$\sharp\mathcal{M}_{(T-a)(T-b)} = e + 1$. $\square$

Proposition 11. $\mathcal{N}_{N_k} = \{(p^i \oplus 0), i \geq k, (0 \oplus p^j), j \geq k, (0 \oplus 0)\}$.

Proof. If $c \not\equiv 0 \bmod (T-a)$ and $d \not\equiv 0 \bmod (T-b)$, then $(c \oplus d) \notin \mathcal{N}_{N_k}$. Since $\min\{i \mid p^i \oplus 0 \in N_k\} = k$, the assertion follows. $\square$

Proposition 12. *$n((T-a)(T-b)) = e - \alpha$.*

Proof. For $n = e - \alpha$,

$$\mathrm{Ker}(\times(T-b) : N_k/\omega_n N_k \to N_k/\omega_n N_k) = (p^k(1 \oplus 1), 0 \oplus p^k)/\omega_n N_k.$$

Since $[N_k/\omega_n N_k : \mathrm{Ker}(\times(T-b))] = p^k$, we have $n((T-a)(T-b)) \leq e - \alpha$. For $n = e - \alpha - 1 \geq 0$,

$$\phi : N_0/\omega_n N_0 \to N_1/\omega_n N_1 \quad 1 \oplus 1 \mapsto 1 \oplus 1, \;\; 0 \oplus 1 \mapsto 0 \oplus p$$

is a $\Lambda/(\omega_n)$-isomorphism. (In this case $\alpha = \beta < e$. Since $\mathrm{ord}_p(\omega_n(a) - \omega_n(b)) = e + n$, we have $\omega_n(a)(1 \oplus 1) + (\omega_n(b) - \omega_n(a))(0 \oplus p), \omega_n(b)(0 \oplus p) \in \omega_n N_1$. Hence ϕ is an isomorphism of abelian groups. Since $T(1 \oplus 1) - a(1 \oplus 1) + (a - b)(0 \oplus p), T(0 \oplus p) - b(0 \oplus p) \in \omega_n N_1$. Hence ϕ is a Λ-isomorphism.) Therefore $n((T-a)(T-b)) = e - \alpha$. $\square$

The following lemma is obtained by easy calculation.

Lemma 3. *Let $N' = (p^i \oplus 0) \in \mathcal{N}_{N_k}$. Then*

$$\begin{aligned} N_k/(N' + \omega_0 N_k) &\cong \mathbb{Z}/p^{e-k}\mathbb{Z} \oplus \mathbb{Z}/p^i\mathbb{Z} \text{ if } e - \alpha \leq k,\ k \leq i \leq k + \alpha + \beta - e \\ &\cong \mathbb{Z}/p^{e-k}\mathbb{Z} \oplus \mathbb{Z}/p^{k+\alpha+\beta-e}\mathbb{Z} \text{ if } e - \alpha \leq k,\ i \geq k + \alpha + \beta - e \\ &\cong \mathbb{Z}/p^{\alpha}\mathbb{Z} \oplus \mathbb{Z}/p^{-k-\alpha+e+i}\mathbb{Z} \text{ if } e - \alpha \geq k,\ k \leq i \leq k + \alpha + \beta - e \\ &\cong \mathbb{Z}/p^{\alpha}\mathbb{Z} \oplus \mathbb{Z}/p^{\beta}\mathbb{Z} \text{ if } e - \alpha \geq k,\ i \geq k + \alpha + \beta - e. \end{aligned}$$

Let $N' = (0 \oplus p^j) \in \mathcal{N}_{N_k}$. Then

$$\begin{aligned} N_k/(N' + \omega_0 N_k) &\cong \mathbb{Z}/p^{e-k}\mathbb{Z} \oplus \mathbb{Z}/p^{k+\alpha-e+j}\mathbb{Z} \text{ if } e - \alpha \leq k,\ k \leq j \leq \beta \\ &\cong \mathbb{Z}/p^{e-k}\mathbb{Z} \oplus \mathbb{Z}/p^{k+\alpha+\beta-e}\mathbb{Z} \text{ if } e - \alpha \leq k,\ j \geq \beta \\ &\cong \mathbb{Z}/p^{\alpha}\mathbb{Z} \oplus \mathbb{Z}/p^{j}\mathbb{Z} \text{ if } e - \alpha \geq k,\ k \leq j \leq \beta \\ &\cong \mathbb{Z}/p^{\alpha}\mathbb{Z} \oplus \mathbb{Z}/p^{\beta}\mathbb{Z} \text{ if } e - \alpha \geq k,\ j \geq \beta. \end{aligned}$$

Proposition 13. $m((T-a)(T-b),n) \leq 2e+\beta+n$.

Proof. If $(T-a) \equiv (f_1^*) \bmod P^{e+1}$ and $(T-b) \equiv (f_2^*) \bmod P^{e+1}$, then $\lambda(f_1^*) = \lambda(f_2^*) = 1$ and $(f_1^*, f_2^*) \supseteq P^e$. Put $x = \max\{e+1, \beta+1\}$. If $(T-a) \equiv (f_1^*) = (T-a^*) \bmod P^x$ and $(T-b) \equiv (f_2^*) = (T-b^*) \bmod P^x$, then $a^* \equiv a \bmod p^x$, $b^* \equiv b \bmod p^x$ and

$$(\omega_n(u_1 \oplus u_2), \omega_n(0 \oplus u_3 p^k), T-a^* \oplus 0, 0 \oplus T-b^*) \supseteq P^{e+\beta+k}(\Lambda \oplus \Lambda)$$

for any $u_1, u_2, u_3 \in \Lambda^\times$. We easily see that $\max\{c+1, M\} \leq \max\{\,e+1, e+1\} = e+1$. Since

$$\max\{m_{1,n} = e+\beta+n, m_{2,n} = x\} = e+\beta+n,$$

$m((T-a)(T-b),n) \leq e+(e+\beta+n) = 2e+\beta+n$ by Remark 1. $\square$

Theorem 3(case 2). *Assume that* p *does not divide* $\mathrm{char}(Y)$. *Then* $\mathrm{char}(D) = \mathrm{char}(Y)$ *if and only if there exist a non-negative integer* n *and* $a^*, b^* \in p\mathbb{Z}_p$ $(a^* \neq b^*,\ a^*b^* \neq 0)$ *satisfying* (1) *and* (2)*:*

(1) $((T-a^*)(T-b^*)) \equiv (\mathrm{char}(Y)) \bmod P^{m((T-a^*)(T-b^*),n)}$

(2) *there is no pair* $(N_k^*, N")$ *with* $[N_k^*] \in \mathcal{M}_{(T-a^*)(T-b^*)}$, $N" \in \mathcal{N}_{N_k^*}$ *such that*
$$[Y/\omega_n Y, (D+\omega_n Y)/\omega_n Y]_n = [N_k^*/\omega_n N_k^*, (N" + \omega_n N_k^*)/\omega_n N_k^*]_n.$$

§4 Numerical examples.

In this section we give numerical examples. We follow the notation of the preceding sections.

Let k be a real quadratic field, p an odd prime number and ψ the non-trivial primitive Dirichlet character which is associated to k. Let f_0 be the least common multiple of p and the conductor of ψ. We identify $\mathrm{Gal}(k_\infty/k)$ with $\mathrm{Gal}(k(\mu_{p^\infty})/k(\mu_p))$, where μ_{p^n} is the group of p^n-th roots of unity and $\mu_{p^\infty} = \cup_{n\geq 0}\mu_{p^n}$. We take a topological generator γ_0 of $\mathrm{Gal}(k_\infty/k)$ such that $\zeta^{\gamma_0} = \zeta^{1+f_0}$ for all $\zeta \in \mu_{p^\infty}$. Since there is no non-trivial abelian p-extension of $\mathbb{Q}_\infty$ unramified outside p, we have $Y = \mathrm{Gal}(M/k_\infty) = e_\psi Y$, where e_ψ is the idempotent of ψ. On the other hand, there exists an element $G_\psi(T) \in \Lambda = \mathbb{Z}_p[[T]]$ such that $L_p(1-s,\psi) = G_\psi((1+f_0)^s - 1)$ for all $s \in \mathbb{Z}_p$(see [I3]). By p-adic Weierstrass preparation theorem, we can uniquely express $G_\psi(T)$ in the form $p^{\mu_\psi} g_\psi(T) U_\psi(T)$, where μ_ψ is a non-negative integer, $g_\psi(T)$ a distinguished polynomial in Λ and $U_\psi(T) \in \Lambda^\times$. The Iwasawa main conjecture proved by Mazur-Wiles[MW] asserts $\mathrm{char}(e_\psi Y) = p^{\mu_\psi} g_\psi(T)$. Moreover Ferrero-Washington[FW] proved $\mu_\psi = 0$.

An "approximate" polynomial of $G_\psi(T)$ is obtained in the following way. Let ω be the Teichmüller character. $G_\psi(T)$ satisfies the following congruence:

$$G_\psi(T) \equiv -\frac{1}{2f_0p^n} \sum_{a=1,(a,f_0)=1}^{f_0p^n} a\psi\omega^{-1}(a)(1+\dot{T})^{-\gamma_n(a)} \mod((1+\dot{T})^{p^n}-1)$$

for $n \geq 0$, where $(1+\dot{T})(1+T) = 1+f_0$, $(1+f_0)^{\gamma_n(a)} \equiv za \mod p^{n+1}$ for some $(p-1)$-th root of unity $z \in \mathbb{Z}_p$ and $0 \leq \gamma_n(a) < p^n$ (see [I3,§6] and [G2]). Note that $(p,T)^{n+1} \supset ((1+\dot{T})^{p^n}-1)$. For details about computation of $G_\psi(T)$, see, for example, [EM].

Let $k = \mathbb{Q}(\sqrt{m})$ in which $p = 3$ splits, where m is a square-free integer($1 < m < 10^4$). The total number of such fields is exactly 2279.

Example 0-1. If $\deg(g_\psi(T)) = 0$, we have $M = L = k_\infty$. Hence λ and ν vanish. There are 1444 fields such that $\deg(g_\psi(T)) = 0$ among 2279 fields.

Example 0-2. If $L'_0 = k_\infty$, then we have $L' = k_\infty$ by Proposition 7. Hence $\lambda = 0$ by Proposition 6. Including those in Example 0-1, There are 1444+598 fields such that $L'_0 = k_\infty$ among the above fields. Concerning ν-invariants of those 598 fields, see [FK].

Example 1. If $g_\psi(T)$ is irreducible in $\mathbb{Z}_p[T]$ and $[M_n : L'_n] > 1$, then we have $\lambda = 0$ by Proposition 6 and Theorem 3(case 1). The index $[M_n : L'_n]$ is computed in the following way. Assume that $g_\psi(T)$ is square-free. Then there exists an injective map $Y = \mathrm{Gal}(M/k_\infty) \hookrightarrow Z = \mathbb{Z}_p[T]/(g_\psi(T))$ with finite cokernel. Hence we have $[M_n : k_\infty] = \sharp(Z/\omega_n Z)$ (see [CL,§4]). By Proposition 1(a)(b), $\sharp\,\mathrm{Gal}(L'_n/k_\infty) = \sharp A'_n \cdot \sharp(U_n/V_n\overline{E'_n})$. We have seen in the proof of Lemma 1 that $i'_{0,n} : U_0/V_0 \to U_n/V_n (\cong \mathbb{Z}_p)$ is an isomorphism. Hence we see that $U_n/V_n \to (U_0/V_0)^{p^n}$ induced by the relative norm maps is an isomorphism. Thus we have $\sharp(U_n/V_n\overline{E'_n}) = \sharp(U_0/V_0\overline{N_{k_n/k}E'_n})/p^n$. Therefore we have

$$[M_n : L'_n] = \frac{\sharp(Z/\omega_n Z)\cdot p^n}{\sharp A'_n \cdot \sharp(U_0/V_0\overline{N_{k_n/k}E'_n})}.$$

In [FT], they compute $\sharp A'_n = \sharp A_n/D_n$ and $n_0^{(n)} = v_p(p \cdot \sharp(U_0/V_0\overline{N_{k_n/k}E'_n}))$ for the above 2279 fields and $n = 0, 1$.

Let $k = \mathbb{Q}(\sqrt{727})$, $p = 3$ and σ generate $\mathrm{Gal}(k/\mathbb{Q})$. By computation, $(G_\psi(T)) \equiv (T^2+3T+18) \mod (p,T)^3$. Further we see that $T^2+3T+18$ is irreducible in $\mathbb{Z}_p[T]$ and $m_0(T^2+3T+18) = 3$. Therefore $g_\psi(T)$ is irreducible in $\mathbb{Z}_p[T]$. We get $\sharp Z/\omega_0 Z = p^2$.

On the other hand, we have

$$A_0 = 1,\ E_0 = \langle -1, \varepsilon = 728 + 27\sqrt{727}\rangle,\ E'_0 = \langle -1, \varepsilon, 3, \varepsilon' = 22 + \sqrt{727}\rangle.$$

$\mathfrak{p} = (3, \varepsilon'^{\sigma})$ is a prime ideal and $\mathfrak{p}^5 = (\varepsilon'^{\sigma})$. Here since $\sqrt{727} \equiv 22 (\operatorname{mod} \mathfrak{p}^4)$, ε is a $\mathfrak{p}$ -adic p^2-th power but not p^3-th power and ε' is a $\mathfrak{p}$-adic p-th power but not p^2-th power.

From these data on E'_0, we see that $n_0^{(0)} = 2$(see [FK] and [FT]). By these facts, we have $[M_0 : L'_0] = p$. Therefore we have $\lambda = 0$.

Here we explain how to obtain $n_0^{(0)} = 2$ from these data for convenience of readers. Since p splits in k, we have

$$\begin{aligned}
U_0 &= \{(u, u') \in (1 + p\mathbb{Z}_p)^{\oplus 2} \mid uu' = 1\} \cong 1 + p\mathbb{Z}_p, \\
V_0 &= \{1\}, \\
W_0 &= \{(\eta p^a, \eta' p^b) \mid a, b \in \mathbb{Z}, \eta^{p-1} = \eta'^{p-1} = 1\}.
\end{aligned}$$

Here we fix a topological generator x of U_0. By the above data,

$$u_0(\varepsilon) = x^{p^2 u} \text{ and } u_0(\varepsilon') = x^{pu'}(1, p^5)$$

for some $u, u' \in \mathbb{Z}_p^{\times}$. Hence $\overline{E'_0} = \overline{U_0 \cap (u_0(E'_0)W_0)} = \langle x^p \rangle$. Therefore we have $\sharp U_0/V_0\overline{E'_0} = p$ and $n_0^{(0)} = 2$.

In a similar way, we can show that the conjecture is true for $m = 2794$, 4279, 4741, 5533, 7429, 7465, 7642, 9691. For these quadratic fields, the conjecture was not verified in [FT].

Example 2. Let us deal with the case g_{ψ} is reducible. Here we give an example of case 2.

Let $k = \mathbb{Q}(\sqrt{9634})$, $p = 3$ and σ generate $\operatorname{Gal}(k/\mathbb{Q})$. By computation, $(G_{\psi}(T)) \equiv ((T-66)(T-27)) \operatorname{mod}(p, T)^5$. Hence we have $g_{\psi}(T) = (T-a)(T-b)$ $(a, b \in p\mathbb{Z}_p)$, $e = 1$, $\alpha = 1$ and $\beta = 3$ by Proposition 2 and Proposition 3. Put $f^*(T) = (T-66)(T-27)$. Moreover we have $m(f^*(T), 0) = m(g_{\psi}(T), 0) \leq 5$ by Proposition 13. This implies that $\mathcal{L}_{\mathrm{char}(Y),0} = \mathcal{L}_{f^*(T),0}$.

On the other hand, we have

$$\begin{aligned}
&A_0 = D_0 \cong \mathbb{Z}/p\mathbb{Z},\ E_0 = \langle -1, \varepsilon = 8343 + 85\sqrt{9634} \rangle \\
&E'_0 = \langle -1, \varepsilon, 3, \varepsilon' = 2252785 + 22304\sqrt{9634} \rangle.
\end{aligned}$$

$\mathfrak{p} = (3, \varepsilon'^{\sigma})$ is a prime ideal and $\mathfrak{p}^{24} = (\varepsilon'^{\sigma})$. Here since $\sqrt{9634} \equiv 20 (\operatorname{mod} \mathfrak{p}^5)$, ε is a $\mathfrak{p}$-adic p^3-th power but not p^4-th power and ε' is a $\mathfrak{p}$-adic p^2-th power but not p^3-th power.

From these data, we obtain $\overline{E_0} = \langle x^{p^3} \rangle$ and $\overline{E'_0} = \langle x^{p^2} \rangle$ in a similar way as in Example 1. First, by Proposition 1(a)(b), $\operatorname{Gal}(L'_0/k_\infty) = \operatorname{Gal}(L'_0/K'_0 k_\infty) \cong U_0/V_0\overline{E'_0} \cong \mathbb{Z}/p^2\mathbb{Z}$. Next, let us compute $\operatorname{Gal}(M_0/L'_0)$. By Proposition 1(e) and $V_0 = \{1\}$, we have $M_0 = L_0$. On the other hand, $\mathrm{Gal}(L/L')$ is a cyclic $\mathbb{Z}_p$-module, since $\mathfrak{p}_n\mathfrak{p}_n^\sigma$ is principal for all n. Thus it suffices to know $\sharp\,\mathrm{Gal}(L_0/K_0L_0')$ and $\sharp\,\mathrm{Gal}(K_0L_0'/L_0')$. As $\overline{E_0'}/\overline{E_0} \cong \mathbb{Z}/p\mathbb{Z}$, $\sharp\,\mathrm{Gal}(L_0/K_0L_0') = p$ by Proposition 1(d). By $D_0 \cong \mathbb{Z}/p\mathbb{Z}$ and Proposition 1(c), we get $\sharp\,\mathrm{Gal}(K_0L_0'/L_0') = p$. Therefore we obtain $\mathrm{Gal}(M_0/L_0') \cong \mathbb{Z}/p^2\mathbb{Z}$. As $A_0 = D_0$, we see that $L_0' \cap K_0k_\infty = k_\infty$. Hence $\mathrm{Gal}(M_0/k_\infty)$ is not a cyclic $\mathbb{Z}_p$-module. By Proposition 10($e = 1$), $\mathcal{M}_{f^*(T)}$ has two elements $[N_0^*]$ and $[N_1^*]$. Now we prove $\mathrm{char}(D) = \mathrm{char}(Y)$. By Theorem 3(case 2), all we have to do is to show that there is no element $N" \in \mathcal{N}_{N_k^*}$ such that $[Y/\omega_0Y, (D+\omega_0Y)/\omega_0Y]_0 = [N_k^*/\omega_0N_k^*, (N" + \omega_0N_k^*)/\omega_0N_k^*]_0$ for $k = 0, 1$. Proposition 11 gives us all elements of $\mathcal{N}_{N_k^*}$. Then, using Lemma 3, we have no element $N" \in \mathcal{N}_{N_0^*}$ such that $(N" + \omega_0N_0^*)/\omega_0N_0^* \cong \mathrm{Gal}(M_0/L_0') \cong \mathbb{Z}/p^2\mathbb{Z}$ and that $N_0^*/(N" + \omega_0N_0^*) \cong \mathrm{Gal}(L_0'/k_\infty) \cong \mathbb{Z}/p^2\mathbb{Z}$. On the other hand, $N_1^*/\omega_0N_1^*$ is a cyclic $\mathbb{Z}_p$-module, but $Y/\omega_0Y = \mathrm{Gal}(M_0/k_\infty)$ is not cyclic. Therefore the above assertion follows.

Of course, we can show $\mathrm{char}(D) = \mathrm{char}(Y)$ by directly studying $[Y/\omega_0Y, (D+\omega_0Y)/\omega_0Y]_0$. In the above case, we have the following isomorphisms by class field theory(cf. Proposition 1).

$$\begin{array}{ccc} Y/\omega_0Y & \cong & \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^3\mathbb{Z} \\ \bigcup\!\mid & & \bigcup\!\mid \\ (D+\omega_0Y)/\omega_0Y & \cong & (1 \oplus p). \end{array}$$

Using this fact, we can show that $D \notin \mathcal{N}_Y$ by Theorem 3(case 2) and Proposition 11.

In the following tables, we write the number of quadratic fields satisfying conditions concerning (1) $\deg(g_\psi(T))$, (2)reducibility of $g_\psi(T)$, (3) M_0 and L_0', (4) L_0' and k_∞ among 2279 fields. For example, 430(393) in Table 1 means that there are 430 fields which satisfy the following conditions (1)(2)(3) and that 393 fields satisfy (4) further. (1)$\deg(g_\psi(T)) = 1$. (2)$g_\psi(T)$ is irreducible in $\mathbb{Z}_p[T]$. (3)$M_0 \supsetneq L_0'$. (4)$L_0' = k_\infty$.

Table 1: The number of quadratic fields ($n = 0$)

	Irred.	polyn.	Red.	polyn.
$\deg(g_\psi(T))$	$M_0 \supsetneq L_0'(= k_\infty)$	$M_0 = L_0'$	$M_0 \supsetneq L_0'$	$M_0 = L_0'$
1	430(393)	119	0	0
2	146(130)	41	17(14)	0
3	29(28)	9	15(11)	2
4	12(12)	3	5(3)	0
≥ 5	5(5)	0	2(2)	0

Table 2: The number of quadratic fields ($n = 1$)

	Irred.	polyn.	Red.	polyn.
$\deg(g_\psi(T))$	$M_1 \supsetneq L_1'$	$M_1 = L_1'$	$M_1 \supsetneq L_1'$	$M_1 = L_1'$
1	517	32	0	0
2	185	2	17	0
3	37	1	17	0
4	15	0	5	0
≥ 5	5	0	2	0

By Table 1, Example 0 and Example 2 Greenberg's conjecture is true for at least $2097 = 1444 + 430 + 146 + 29 + 12 + 5 + 14 + 11 + 3 + 2 + 1$ fields among 2279 fields. Moreover, by Table 2, the conjecture is true for at least $2234 = 1444 + 517 + 185 + 37 + 15 + 5 + 14 + 11 + 3 + 2 + 1$ fields. Further in [FT] the conjecture is verified for $\mathbb{Q}(\sqrt{2659})$ and $\mathbb{Q}(\sqrt{8374})$ which are not contained in 2234 fields above.

References

[C] A. Candiotti, *Computation of Iwasawa invariants and K_2*, Compositio Math. **29** (1974), 89–111.

[CL] J[redacted] Coates and S. Lichtenbaum, *On l-adic zeta functions*, Ann. of Math.(2) **98** (1973), 498–550.

[EM] R.[redacted] Ernvall and T. Metsänkylä, *Computation of the zeros of p-adic L-functions*, Math. Comp. **58** (1992), 815–830.

[FK] T[redacted] Fukuda and K. Komatsu, *On $\mathbb{Z}_p$-extensions of real quadratic fields*, J. Math.Soc.Japan **38** (1986), 95–102.

[FKW] T. F[redacted]kuda, K. Komatsu and H. Wada, *A remark on the λ-invariant of real quadratic fields*, Proc. Japan Acad. Ser. A **62** (1986), 318–319.

[F] T. Fukuda, *Iwasawa's λ-invariants of certain real quadratic fields*, Proc. Japan Acad. Ser. A **65** (1989), 260–262.

[FT] T[redacted] Fukuda and H. Taya, *The Iwasawa λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields*, Acta Arith. **69** (1995), 277–292.

[FW] B.[redacted] Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.

[G1] R[redacted] Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.

[G2] R[redacted] Greenberg, *On p-adic L-functions and cyclotomic fields II*, Nagoya Math. J. **67** (1977), 139–158.

[I1] [redacted]. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.

[I2] [redacted]. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226.

[I3] [redacted]. Iwasawa, *Lectures on p-adic L-functions*, Ann. of Math. Stud. no. 74, Princeton Univ. Press: Princeton, N.J. (1972).

[I4] [redacted]. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[K] [redacted]S. Kraft, *Iwasawa invariants of CM fields*, J. Number Theory **32** (1989), 65–77.

[OT] M[redacted] Ozaki and H. Taya, *A note on Greenberg's conjecture of real abelian number fields*, submitted for publication (1995).

[MW] B. [redacted]azur and A. Wiles, *Class fields of abelian extensions of $\mathbb{Q}$*, Invent. Math. **76** (1984), 179–330.

[T] H. Taya, *On the Iwasawa λ-invariants of real quadratic fields*, Tokyo J. Math. **16** (1993), 121–130.

[W] L[redacted] Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. no. 83, Springer: New York (1982).

Hiroki Sumida
Department of Mathematical Sciences
University of Tokyo
3-8-1 Komaba, Meguro-ku,Tokyo, 153
Japan