ACTA ARITHMETICA
LXXIV.2 (1996)

On cyclotomic $\mathbb{Z}_p$-extensions of real quadratic fields

by

Hisao Taya (Tokyo)

Dedicated to my father Kyuji Taya
on his sixtieth birthday

1. Introduction. Let p be a fixed odd prime number and $\mathbb{Z}_p$ the ring of p-adic integers. Let k be a real quadratic field in which p splits, say $(p) = \mathfrak{p}\mathfrak{p}'$ in k, where $\mathfrak{p} \neq \mathfrak{p}'$. In the previous paper [6] we studied Greenberg's conjecture for k and p: the conjecture asserts that both $\lambda_l(K)$ and $\mu_l(K)$ always vanish for any totally real number field K and any prime number l (cf. [8]). Here, and in what follows, for an algebraic number field K and a prime number l, $\lambda_l(K)$ and $\mu_l(K)$ denote the Iwasawa λ- and μ-invariants, respectively, of the cyclotomic $\mathbb{Z}_l$-extension of K (cf. [9]). In our situation that k is a real quadratic field, it is known that $\mu_p(k)$ always vanishes by the Ferrero–Washington theorem (cf. [3]), but it is not known whether $\lambda_p(k)$ also vanishes.

To study Greenberg's conjecture for real quadratic fields in which p splits, we defined in [12] two invariants $n_0^{(r)}$ and $n_2^{(r)}$ for any integer $r \geq 0$, as follows: For the cyclotomic $\mathbb{Z}_p$-extension

$$k = k_0 \subset k_1 \subset \ldots \subset k_n \subset \ldots \subset k_\infty$$

with Galois group $\Gamma = \mathrm{Gal}(k_\infty/k)$, let E_n be the group of units in k_n, $\mathfrak{p}_n$ (resp. $\mathfrak{p}'_n$) the unique prime ideal of k_n lying over $\mathfrak{p}$ (resp. $\mathfrak{p}'$) and d_n the order of the ideal class $Cl(\mathfrak{p}'_n)$ represented by $\mathfrak{p}'_n$ in the ideal class group of k_n (this equals the order of $Cl(\mathfrak{p}_n)$). For each $m \geq n \geq 0$, we denote by $N_{m,n}$ the norm map from k_m to k_n. Then, for any integer $r \geq 0$, we can choose $\alpha_r \in k_r$ such that ${\mathfrak{p}'_r}^{d_r} = (\alpha_r)$. Let ε be the fundamental unit of k. Now two

1991 *Mathematics Subject Classification*: Primary 11R23, 11R11, 11R27, 11R29.
Key words and phrases: Iwasawa invariants, real quadratic fields, unit groups, ambiguous ideal class groups.
Research supported in part by Waseda University Grant for Special Research Projects 94A-129.

positive integers $n_0^{(r)}$ and $n_2^{(r)}$, which are invariants of k, are defined by

$$\mathfrak{p}^{n_0^{(r)}} \parallel (N_{r,0}(\alpha_r)^{p-1} - 1) \text{ in } k \quad \text{and} \quad p^{n_2^{(r)}} = p^{n_2}(E_0 : N_{r,0}(E_r)),$$

where n_2 denotes the positive integer such that $\mathfrak{p}^{n_2} \parallel (\varepsilon^{p-1} - 1)$ in k (see also [5] and [6]). Though α_r is not unique, $n_0^{(r)}$ is uniquely determined under the condition $n_0^{(r)} \le n_2^{(r)}$. We put $n_0 = n_0^{(0)}$, noting that $n_2 = n_2^{(0)}$.

In the present paper, we shall study the properties of the invariants $n_0^{(r)}$ and $n_2^{(r)}$, and give a certain criterion for the vanishing of $\lambda_p(k)$ in terms of $n_0^{(r)}$. To be more precise, we first show in Section 2 an alternative definition of $n_0^{(r)}$ and $n_2^{(r)}$, which seems more natural than the former one (cf. Lemma 2 and Remark 1). Secondly, by determining the structure of certain quotient groups of the p-unit group (resp. the unit group) of k_r (cf. Lemmas 5 and 7), we give in Section 3 the ambiguous p-class number formula (resp. the ambiguous class number formula) of intermediate fields of k_∞/k_r in terms of $n_0^{(r)}$ (resp. $n_2^{(r)}$) (cf. Theorems 1 and 2). In Section 3 we also mention the p-adic L-function and the order of certain Galois groups (cf. Proposition 1). Thirdly, we give in Section 4 the following criterion which is the main theorem of this paper:

Theorem (cf. Theorem 4). *Let p and k be as above. Let A_0 be the p-Sylow subgroup of the ideal class group of k. Then $\lambda_p(k)$ vanishes if and only if the following two conditions are satisfied*:

(1) *Every ideal class of A_0 becomes principal in k_n for some integer $n \ge 0$.*

(2) $n_0^{(r)} = r + 1$ *for some integer $r \ge 0$.*

In the previous paper [6], we gave a certain necessary and sufficient condition for the vanishing of $\lambda_p(k)$ under an assumption under which it is easily seen that condition (1) holds (see Theorem 2 of [6] or Corollary 4). The criterion stated in our main theorem is a generalization of Theorem 2 of [6] (and hence of Theorem of [4] and Theorem 1 of [5]). Making a comparison with the case where p does not split in k, the criterion shows the difference of situations between the splitting case and the non-splitting case (cf. Remark 2). Finally, in the last section, we make an additional remark about the verification of the vanishing of $\lambda_p(k)$ based on our main theorem.

The notation introduced above will be used in the same meaning throughout this paper. Moreover, we denote by $\alpha_r \in k_r$ a generator of $\mathfrak{p}_r'^{d_r}$ satisfying

$$\mathfrak{p}^{n_0^{(r)}} \parallel (N_{r,0}(\alpha_r)^{p-1} - 1) \quad \text{and} \quad n_0^{(r)} \le n_2^{(r)},$$

that is to say, $\alpha_r \in k_r$ is a generator of $\mathfrak{p}_r'^{d_r}$ which determines $n_0^{(r)}$.

2. Some lemmas. In this section, we shall describe some properties of $n_0^{(r)}$ and $n_2^{(r)}$. The following lemma, which is a basic fact, is an immediate consequence of the definitions of $n_0^{(r)}$ and $n_2^{(r)}$.

LEMMA 1. *For each integer $r \geq 0$,*

(1) $r+1 \leq n_0^{(r)} \leq n_2^{(r)}$,
(2) $n_0^{(r)} \leq n_0^{(r+1)} \leq n_0^{(r)}+1$,
(3) $n_2^{(r)} \leq n_2^{(r+1)} \leq n_2^{(r)}+1$.

In particular, if $n_0^{(r)} = r+1$ (resp. $n_2^{(r)} = r+1$) for some integer $r \geq 0$, then $n_0^{(s)} = s+1$ (resp. $n_2^{(s)} = s+1$) for all integers $s \geq r$.

Let $k_{\mathfrak{p}}$ be the completion of a real quadratic field k at $\mathfrak{p}$ and fix a prime element of $k_{\mathfrak{p}}$ throughout this section. Let $\Omega_{\mathfrak{p}}$ denote the completion of the algebraic closure of $k_{\mathfrak{p}}$ and $\widetilde{D}$ the subgroup of the multiplicative group $\Omega_{\mathfrak{p}}^{\times}$ consisting of elements $u \in \Omega_{\mathfrak{p}}$ such that $v_{\mathfrak{p}}(u-1) > 0$, $v_{\mathfrak{p}}$ being the $\mathfrak{p}$-adic normalized valuation on $\Omega_{\mathfrak{p}}$. Moreover, we denote by $\log_{\mathfrak{p}}$ the $\mathfrak{p}$-adic logarithm extended to $\Omega_{\mathfrak{p}}$ so that $\log_{\mathfrak{p}}(v) = 0$ for all $v \in \Omega_{\mathfrak{p}} \setminus \widetilde{D}$ and that $\log_{\mathfrak{p}}(uv) = \log_{\mathfrak{p}}(u) + \log_{\mathfrak{p}}(v)$ for all $u, v \in \Omega_{\mathfrak{p}}$ (cf. [10] or [13]). Since p splits in k, $k_{\mathfrak{p}}$ is isomorphic to the field $\mathbb{Q}_p$ of p-adic numbers. Therefore, $v_{\mathfrak{p}}$ and $\log_{\mathfrak{p}}$ can be essentially identified with the p-adic valuation v_p and the p-adic logarithm $\log_p$, respectively. However, we will use the former notation to specify the fixed prime.

Let E_n^* be the group of $\mathfrak{p}$-units in k_n, i.e., the group of elements ε_n of k_n with $v_{\mathfrak{l}}(\varepsilon_n) = 0$ for all prime ideals $\mathfrak{l}$ of k_n outside $\mathfrak{p}$. The following lemma is now obvious, but its proof will be given for the sake of completeness.

LEMMA 2. *For each integer $r \geq 0$,*

(1) $n_0^{(r)} = \min\{v_{\mathfrak{p}}(\log_{\mathfrak{p}}(N_{r,0}(\varepsilon_r^*))) \mid \varepsilon_r^* \in E_r^*\}$,
(2) $n_2^{(r)} = \min\{v_{\mathfrak{p}}(\log_{\mathfrak{p}}(N_{r,0}(\varepsilon_r))) \mid \varepsilon_r \in E_r\}$.

Proof. We first prove (2). Let $\varepsilon_r \in E_r$. Then $N_{r,0}(\varepsilon_r) = \pm\varepsilon^{a(E_0:N_{r,0}(E_r))}$, where ε denotes the fundamental unit of k and $a \in \mathbb{Z}$. If $a = 0$, then $v_{\mathfrak{p}}(\log_{\mathfrak{p}}(N_{r,0}(\varepsilon_r))) = \infty$. Thus we may assume that $a \neq 0$. From the definition of n_2 and Lemma 5.5 of [13], it follows that $v_{\mathfrak{p}}(\log_{\mathfrak{p}}(\varepsilon)) = n_2$, which implies that

$$\begin{aligned} v_{\mathfrak{p}}(\log_{\mathfrak{p}}(N_{r,0}(\varepsilon_r))) &= v_{\mathfrak{p}}(a(E_0 : N_{r,0}(E_r))\log_{\mathfrak{p}}(\varepsilon)) \\ &= v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}((E_0 : N_{r,0}(E_r))) + n_2 \\ &= v_{\mathfrak{p}}(a) + n_2^{(r)} \geq n_2^{(r)}. \end{aligned}$$

On the other hand, there exists an element ε_r of E_r such that $N_{r,0}(\varepsilon_r) = \pm\varepsilon^{(E_0:N_{r,0}(E_r))}$, so that $a = 1$. Hence the assertion holds.

Next we prove (1). Let $\varepsilon_r^* \in E_r^*$. Then we can write $\varepsilon_r^* = \varepsilon_r \alpha_r^b$ with $\varepsilon_r \in E_r$ and $b \in \mathbb{Z}$. Here α_r denotes a generator of ${\mathfrak{p}'_r}^{d_r}$ which determines $n_0^{(r)}$ as in the introduction. Similarly, it follows that $v_{\mathfrak{p}}(\log_{\mathfrak{p}}(N_{r,0}(\alpha_r))) = n_0^{(r)}$. Further, we have

$$\begin{aligned} v_{\mathfrak{p}}(\log_{\mathfrak{p}}(N_{r,0}(\varepsilon_r^*))) &= v_{\mathfrak{p}}(\log_{\mathfrak{p}}(N_{r,0}(\varepsilon_r)) + b\log_{\mathfrak{p}}(N_{r,0}(\alpha_r))) \\ &\geq \min\{v_{\mathfrak{p}}(\log_{\mathfrak{p}}(N_{r,0}(\varepsilon_r))), v_{\mathfrak{p}}(b\log_{\mathfrak{p}}(N_{r,0}(\alpha_r)))\} \\ &\geq \min\{n_2^{(r)}, n_0^{(r)}\} \geq n_0^{(r)}. \end{aligned}$$

Therefore we obtain the desired result. ∎

Remark 1. We may define the invariants $n_0^{(r)}$ and $n_2^{(r)}$ by (1) and (2), respectively, in Lemma 2.

3. The ambiguous class number formulae. In [4], Fukuda and Komatsu explicitly gave the genus formula for the p-part of ambiguous class groups of intermediate fields of k_∞/k in terms of n_2 (cf. Proposition 1 of [4] or Corollary 2). In this section, for any integer $r \geq 0$, we generalize this formula in terms of $n_2^{(r)}$ and also give an analogous formula in terms of $n_0^{(r)}$.

For the cyclotomic $\mathbb{Z}_p$-extension k_∞ of a real quadratic field k, let k_n be the unique intermediate field of k_∞/k of degree p^n, $k_{\mathfrak{p}_n}$ the completion of k_n at $\mathfrak{p}_n$ and $E_{\mathfrak{p}_n}$ the group of units in $k_{\mathfrak{p}_n}$. Since p splits in k, we may identify $k_{\mathfrak{p}}$ with $\mathbb{Q}_p$ in what follows. Thus, by embedding k in $\mathbb{Q}_p$, we may write $N_{r,0}(\alpha_r)^{p-1} \in k$ in the form of a p-adic integer as follows:

$$N_{r,0}(\alpha_r)^{p-1} = 1 + p^{n_0^{(r)}} x_r, \qquad x_r \in \mathbb{Z}_p^\times.$$

Here $\alpha_r \in k_r$ is the same as in the last part of the introduction. Now we put

$$U_n = \{u \in E_{\mathfrak{p}_n} \mid u \equiv 1 \pmod{\mathfrak{p}_n}\}$$

and

$$U_n^{(r)} = \{u \in U_n \mid N_{n,0}(u) \equiv 1 \pmod{p^{n+r+1}}\}$$

for any integer $n, r \geq 0$. Then we easily see that

$$U_n \supset U_n^{(0)} \supset U_n^{(1)} \supset \ldots \supset U_n^{(r)} \supset \ldots$$

Applying local class field theory, we can prove the following (see, e.g., [11] in which we assumed that $r \geq s$, but, in fact, its proof works without such an assumption).

Lemma 3. *Let r be a non-negative integer. Then $N_{r+s,r}(U_{r+s}) = U_r^{(s)}$ for all integers $s \geq 0$.*

First, we shall give the genus formula for the p-part of ambiguous p-class groups of intermediate fields of k_∞/k_r in terms of $n_0^{(r)}$, which is analogous to a generalization of Proposition 1 of [4]. Let Γ_r be the Galois group

$\mathrm{Gal}(k_\infty/k_r)$ of k_∞ over k_r (so $\Gamma = \Gamma_0$), A'_n the p-Sylow subgroup of the p-ideal class group of k_n and $A'^{\Gamma_r}_n$ the subgroup of A'_n consisting of p-ideal classes which are invariant under the action of Γ_r, namely, the p-part of the ambiguous p-class group of k_n over k_r. Here, by the p-ideal class group of k_n, we mean the ideal class group of the ring of p-integers in k_n; a p-integer in k_n means an element α of k_n with $v_{\mathfrak{l}}(\alpha) \ge 0$ for all prime ideals $\mathfrak{l}$ of k_n outside p, namely, outside $\mathfrak{p}_n$ and $\mathfrak{p}'_n$. Note that if A_n denotes the p-Sylow subgroup of the ideal class group of k_n and D_n the subgroup of A_n consisting of ideal classes represented by products of prime ideals of k_n lying over p, then $A'_n \simeq A_n/D_n$.

Moreover, let E'_n be the group of p-units in k_n, i.e., the group of elements ε_n of k_n with $v_{\mathfrak{l}}(\varepsilon_n) = 0$ for all prime ideals $\mathfrak{l}$ of k_n outside p, namely, outside $\mathfrak{p}_n$ and $\mathfrak{p}'_n$. Using the above lemma, we show two lemmas.

LEMMA 4. *Let r be a non-negative integer. Then $E'_r = E'_r \cap N_{n,r}(k_n^\times)$ for all integers n with $r \le n \le n_0^{(r)} - 1$.*

P r o o f. First we prove the case where $n = n_0^{(r)} - 1$. Let $\mathbb{Q}_r$ be the unique intermediate field of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ with degree p^r and π_r the image of $1 - \zeta_{p^{r+1}}$ under the norm map from $\mathbb{Q}(\zeta_{p^{r+1}})$ to $\mathbb{Q}_r$, where $\zeta_{p^{r+1}}$ denotes a primitive p^{r+1}th root of unity. Then we see that E'_r is generated by E_r, α_r and π_r. Since π_r is a global norm from k_n, it suffices to prove that any element of the $\mathfrak{p}$-unit group E^*_r is a global norm from k_n.

Let $\varepsilon^*_r \in E^*_r$. Then Lemma 2 shows that $N_{r,0}(\varepsilon^*_r)^{p-1} = 1 + p^{n_0^{(r)}} y_r$ with $y_r \in \mathbb{Z}_p$, so that

$$N_{r,0}(\varepsilon^{*p-1}_r) \equiv 1 \pmod{p^{r+(n_0^{(r)}-r-1)+1}}.$$

Thus $\varepsilon^{*p-1}_r \in U_r^{(n_0^{(r)}-r-1)}$. By Lemma 3, $\varepsilon^{*p-1}_r \in N_{n_0^{(r)}-1,r}(U_{n_0^{(r)}-1})$. Since any prime ideal which does not lie over p is unramified in k_∞/k, the product formula for the norm residue symbol and Hasse's norm theorem imply that ε^{*p-1}_r is a global norm from $k_{n_0^{(r)}-1}$, and so is ε^*_r. Therefore $E^*_r \subset N_{n_0^{(r)}-1,r}(k^\times_{n_0^{(r)}-1})$, and hence $E'_r \subset N_{n_0^{(r)}-1,r}(k^\times_{n_0^{(r)}-1})$. Thus the assertion follows.

Now assume that n is an integer with $r \le n < n_0^{(r)} - 1$. Since

$$N_{n_0^{(r)}-1,r}(k^\times_{n_0^{(r)}-1}) \subset N_{n,r}(k_n^\times),$$

it follows that $E'_r \subset N_{n,r}(k_n^\times)$. This completes the proof. ∎

It is well known that E'_r is a finitely generated abelian group of $\mathbb{Z}$-rank $2p^r + 1$. However, the following lemma holds.

Lemma 5. *Let r be a non-negative integer. Then*

$$E'_r/(E'_r \cap N_{n,r}(k_n^\times)) \simeq \mathbb{Z}/p^{n-n_0^{(r)}+1}\mathbb{Z}$$

for all integers $n \ge n_0^{(r)}$.

Proof. For an element α_r of E'_r which is used to determine $n_0^{(r)}$, we see that

$$N_{r,0}(\alpha_r)^{(p-1)p^{n-n_0^{(r)}}} = 1 + p^n x_r, \quad x_r \in \mathbb{Z}_p^\times.$$

Now assume that $\alpha_r^{(p-1)p^{n-n_0^{(r)}}} \in N_{n,r}(k_n^\times)$ for some $n \ge n_0^{(r)}$. Then, since $\alpha_r^{(p-1)p^{n-n_0^{(r)}}} = N_{n,r}(\beta_n)$ for some $\beta_n \in k_n$, we have

$$N_{r,0}(\alpha_r^{p^{n-n_0^{(r)}}})^{p-1} = N_{n,0}(\beta_n)^{p-1} = 1 + p^{n+1} y_r, \quad y_r \in \mathbb{Z}_p,$$

which contradicts the above equality. Hence $\alpha_r^{(p-1)p^{n-n_0^{(r)}}}$ is not a global norm from k_n, and neither is $\alpha_r^{p^{n-n_0^{(r)}}}$. However, since

$$N_{r,0}(\alpha_r)^{(p-1)p^{n-n_0^{(r)}+1}} = 1 + p^{n+1} x_r, \quad x_r \in \mathbb{Z}_p^\times,$$

for all $n \ge n_0^{(r)}$, we have

$$N_{r,0}(\alpha_r^{(p-1)p^{n-n_0^{(r)}+1}}) \equiv 1 \pmod{p^{r+(n-r)+1}}.$$

It follows from Lemma 3 that $\alpha_r^{p^{n-n_0^{(r)}+1}}$ is a local norm from $k_{\mathfrak{p}_n}$. Thus the product formula for the norm residue symbol and Hasse's norm theorem imply that $\alpha_r^{p^{n-n_0^{(r)}+1}}$ is a global norm from k_n. Therefore we find that $E'_r/(E'_r \cap N_{n,r}(k_n^\times))$ has an element of order $p^{n-n_0^{(r)}+1}$.

On the other hand, since the relative degrees of $\mathfrak{p}_n$ and $\mathfrak{p}'_n$ over k_r are 1, it follows from the genus formula for ambiguous p-class groups (cf. Appendix in [2]) that

$$|A_n'^{\Gamma_r}| = |A'_r| \frac{p^{n-r}}{(E'_r : E'_r \cap N_{n,r}(k_n^\times))}.$$

Hence, by Lemma 4,

$$\begin{aligned} |A_n'^{\Gamma_r}| &= |A'_r| p^{n_0^{(r)}-1-r} \frac{p^{n-n_0^{(r)}+1}}{(E'_r : E'_r \cap N_{n,r}(k_n^\times))} \\ &= |A'^{\Gamma_r}_{n_0^{(r)}-1}| \frac{p^{n-n_0^{(r)}+1}}{(E'_r : E'_r \cap N_{n,r}(k_n^\times))}. \end{aligned}$$

Since k_∞/k is totally ramified at p, we see by class field theory that $|A_n'^{\Gamma_r}| \ge |A'^{\Gamma_r}_{n_0^{(r)}-1}|$, which implies that $(E'_r : E'_r \cap N_{n,r}(k_n^\times)) \le p^{n-n_0^{(r)}+1}$. Therefore our lemma follows. ∎

By combining Lemmas 4 and 5, the next theorem is concluded from the genus formula for ambiguous p-class groups (cf. Appendix in [2]).

THEOREM 1. *Let p be an odd prime number and k a real quadratic field in which p splits. Further, let r be a non-negative integer. Then*

$$|A_n'^{\Gamma_r}| = \begin{cases} |A_r'|p^{n-r} & \text{if } r \le n < n_0^{(r)} - 1, \\ |A_r'|p^{n_0^{(r)}-r-1} & \text{if } n \ge n_0^{(r)} - 1. \end{cases}$$

In particular, $|A_n'^{\Gamma_r}|$ remains bounded as $n \to \infty$.

Putting $r = 0$ in Theorem 1, we obtain the following:

COROLLARY 1. *Let k and p be as in Theorem 1. Then*

$$|A_n'^{\Gamma}| = \begin{cases} |A_0'|p^{n} & \text{if } n < n_0 - 1, \\ |A_0'|p^{n_0-1} & \text{if } n \ge n_0 - 1. \end{cases}$$

Next, we shall give the genus formula for the p-part of ambiguous class groups of intermediate fields of k_∞/k_r in terms of $n_2^{(r)}$, which is a generalization of Proposition 1 in [4]. Let A_n be the p-Sylow subgroup of the ideal class group of k_n and $A_n^{\Gamma_r}$ the subgroup of A_n consisting of ideal classes which are invariant under the action of $\Gamma_r = \mathrm{Gal}(k_\infty/k_r)$, namely, the p-part of ambiguous class group of k_n over k_r. Then, by replacing E_r' by E_r, A_r' by A_r, $A_n'^{\Gamma_r}$ by $A_n^{\Gamma_r}$ and $n_0^{(r)}$ by $n_2^{(r)}$, respectively, the above argument leads to the following two lemmas.

LEMMA 6. *Let r be a non-negative integer. Then $E_r = E_r \cap N_{n,r}(k_n^\times)$ for all integers n with $r \le n \le n_2^{(r)} - 1$.*

LEMMA 7. *Let r be a non-negative integer. Then*

$$E_r/(E_r \cap N_{n,r}(k_n^\times)) \simeq \mathbb{Z}/p^{n-n_2^{(r)}+1}\mathbb{Z}$$

for all integers $n \ge n_2^{(r)}$.

The unit group E_r is a finitely generated abelian group of $\mathbb{Z}$-rank $2p^r - 1$. However, we should note that $E_r/(E_r \cap N_{n,r}(k_n^\times))$ is cyclic. By combining Lemmas 6 and 7, we obtain the following:

THEOREM 2. *Let p be an odd prime number and k a real quadratic field in which p splits. Further, let r be a non-negative integer. Then*

$$|A_n^{\Gamma_r}| = \begin{cases} |A_r|p^{n-r} & \text{if } r \le n < n_2^{(r)} - 1, \\ |A_r|p^{n_2^{(r)}-r-1} & \text{if } n \ge n_2^{(r)} - 1. \end{cases}$$

In particular, $|A_n^{\Gamma_r}|$ remains bounded as $n \to \infty$.

Also, putting $r = 0$ in Theorem 2, we obtain the following:

Corollary 2 (cf. Proposition 1 of [4] or of [5]). *Let k and p be as in Theorem 2. Then*

$$|A_n^{\Gamma}| = \begin{cases} |A_0|p^n & \text{if } n < n_2 - 1, \\ |A_0|p^{n_2-1} & \text{if } n \geq n_2 - 1. \end{cases}$$

Finally, we give the following:

Proposition 1. *Let k and p be as in Theorem 2, and let χ denote the non-trivial p-adic Dirichlet character associated with k, $L_p(s,\chi)$ the p-adic L-function associated with χ and M the maximal abelian p-extension of k which is unramified outside the prime ideals over p. Then*

(1) $|A_n^{\Gamma}| = p^{v_p(L_p(1,\chi))}$ *for all integers* $n \geq n_2 - 1$,
(2) $|\mathrm{Gal}(M/k_\infty)| = p^{v_p(L_p(1,\chi))}$.

In particular, if L denotes the maximal abelian unramified p-extension (i.e., the Hilbert p-class field) of k, then $|\mathrm{Gal}(M/k_\infty L)| = p^{n_2-1}$. Here v_p denotes the p-adic valuation normalized by $v_p(p) = 1$.

Proof. First we prove (1). Let R_p be the p-adic regulator of k and $\log_p$ the p-adic logarithm. Since $R_p = \log_p(\varepsilon)$, we easily see that $v_p(R_p) = n_2$ (cf. Lemma 5.5 of [3]). Let Δ be the discriminant of k and h the class number of k. Then the p-adic class number formula (cf. [13]) implies that

$$L_p(1,\chi) = \frac{2hR_p}{\sqrt{\Delta}}\left(1 - \frac{\chi(p)}{p}\right).$$

Hence $v_p(L_p(1,\chi)) = v_p(h) + n_2 - 1$. Therefore (1) follows from Corollary 2.

We next prove (2). Let N denote the norm map from k to $\mathbb{Q}$ and w the number of the roots of unity contained in $k(\zeta_p)$, where ζ_p is a primitive pth root of unity. Then it follows from the result of Coates (cf. Lemma 8 in Appendix of [1]) that

$$\begin{aligned} v_p(|\mathrm{Gal}(M/k_\infty)|) &= v_p\left(\frac{whR_p}{\sqrt{\Delta}}(1 - N(\mathfrak{p})^{-1})(1 - N(\mathfrak{p}')^{-1})\right) \\ &= v_p(h) + n_2 - 1. \end{aligned}$$

This proves (2).

Since k_∞/k is totally ramified at p, we have $|\mathrm{Gal}(k_\infty L/k_\infty)| = |\mathrm{Gal}(L/k)|$. Hence the last assertion immediately follows from (1), (2) and Corollary 2. ∎

4. A criterion for the vanishing of $\lambda_p(k)$. We shall next give a necessary and sufficient condition for $\lambda_p(k)$ to vanish in terms of $n_0^{(r)}$. As in the preceding section, for the cyclotomic $\mathbb{Z}_p$-extension k_∞ of a real quadratic field k, let A_n be the p-Sylow subgroup of the ideal class group of k_n, A_n^{Γ} the subgroup of A_n consisting of ideal classes which are invariant under the action of $\Gamma = \mathrm{Gal}(k_\infty/k)$ and D_n the subgroup of A_n consisting of ideal classes represented by products of prime ideals of k_n lying over p. We first refer to the following theorem of Greenberg.

THEOREM 3 (cf. Theorems 1 and 2 of [8]). *Let K be a totally real number field and l a fixed prime number. Let K_∞ denote the cyclotomic $\mathbb{Z}_l$-extension of K and K_n the unique intermediate field of K_∞/K of degree l^n.*

(1) *Assume that l splits completely in K and also that Leopoldt's conjecture is valid for K and l. Then $\lambda_l(K) = \mu_l(K) = 0$ if and only if $A_n^\Gamma(K) = D_n(K)$ for all sufficiently large integers n.*

(2) *Assume that only one prime ideal of K lies over l and also that this prime is totally ramified in K_∞/K. Then $\lambda_l(K) = \mu_l(K) = 0$ if and only if every ideal class of A_0 becomes principal in K_n for some integer $n \geq 0$.*

Here, $A_n^\Gamma(K)$ and $D_n(K)$ denote the corresponding objects of K to A_n^Γ and D_n respectively.

In our situation, Corollary 2 gives the explicit description of the order $|A_n^\Gamma|$. Hence, by this theorem, we see that it is important to study $|D_n|$. The following lemma, which was proved in [6] as a key lemma, partially gives the behavior of $|D_n|$.

LEMMA 8 (cf. Lemma 7 of [6]). *Let r be a non-negative integer, and let s be a non-negative integer and t the integer such that $|D_{r+s}| = p^t|D_r|$. Then*

$$n_0^{(r)} + t \geq \min\{n_0^{(r+s)}, n_2^{(r)}\}.$$

For a fixed integer $r \geq 0$, we choose $n \geq n_2^{(r)} - 1$ and write $n = r + s$ with a non-negative integer s. Then it follows from Lemma 1 that $n_0^{(r+s)} \geq r + s + 1 \geq n_2^{(r)}$. Hence Lemma 8 shows that $t \geq n_2^{(r)} - n_0^{(r)}$, where t denotes the same as in Lemma 8. Further, noting that $|D_n|$ remains bounded as $n \to \infty$, we obtain the following as a corollary to Lemma 8.

COROLLARY 3. *Let r be a non-negative integer. Then $|D_n| \geq |D_r|p^{n_2^{(r)} - n_0^{(r)}}$ for all integers $n \geq n_2^{(r)} - 1$. In particular, we have $n_0^{(s)} = n_2^{(s)}$ for all sufficiently large integers s.*

Let $\overline{A}_n^\Gamma$ be the subgroup of A_n consisting of ideal classes each of which contains an ideal invariant under the action of $\Gamma = \mathrm{Gal}(k_\infty/k)$, namely, the p-part of the ambiguous class group of k_n over k containing an ambiguous ideal. Then the following lemma is an immediate consequence of the genus formula and the definition of $n_2^{(r)}$.

LEMMA 9. *For each integer $r \geq 0$, we have $|\overline{A}_r^\Gamma| = |A_0|p^{r+n_2-n_2^{(r)}}$.*

Note that $D_n \subset \overline{A}_n^{\Gamma} \subset A_n^{\Gamma}$. We first give the following lemma concerning the relation between $\overline{A}_n^{\Gamma}$ and A_n^{Γ}.

LEMMA 10. *The following two statements are equivalent*:

(1) $A_r^{\Gamma} = \overline{A}_r^{\Gamma}$ *for all sufficiently large integers* r.

(2) $n_0^{(r)} = r + 1$ *for some integer* $r \geq 0$.

Proof. Assume that statement (1) is true. Then it follows from Corollary 2 and Lemma 9 that $n_2^{(r)} = r + 1$ for all sufficiently large r. Hence, by Corollary 3, we have $n_0^{(r)} = r + 1$ for all sufficiently large r. Therefore (1) implies (2).

Assume next that statement (2) is true. Then Lemma 1 implies that $n_0^{(s)} = s + 1$ for all $s \geq r$. By Corollary 3, we also have $n_2^{(s)} = s + 1$ for all sufficiently large s. It follows from Lemma 9 that $|\overline{A}_s^{\Gamma}| = |A_0|p^{n_2 - 1}$. Thus by Corollary 2, $\overline{A}_s^{\Gamma} = A_s^{\Gamma}$ for all sufficiently large s. This completes the proof of our lemma. ∎

Next we give the following lemma concerning the relation between D_n and $\overline{A}_n^{\Gamma}$.

LEMMA 11. *The following two statements are equivalent*:

(1) $\overline{A}_r^{\Gamma} = D_r$ *for all sufficiently large integers* r.

(2) *Every ideal class of* A_0 *becomes principal in* k_n *for some integer* $n \geq 0$.

Proof. Let $i_{0,n}$ denote the natural map from the ideal group of k to that of k_n. First, we note that $\overline{A}_n^{\Gamma} = i_{0,n}(A_0)D_n$. This implies that statement (1) is equivalent to the assertion that $i_{0,r}(A_0) \subset D_r$ for all sufficiently large r. Since every ideal class of D_r becomes principal in k_n for all n sufficiently larger than r, this assertion is equivalent to statement (2). We have thus proved the lemma. ∎

Recall that $\mu_p(k)$ always vanishes in our situation. Combining Lemmas 10 and 11, we immediately conclude the following criterion for the vanishing of $\lambda_p(k)$.

THEOREM 4. *Let* p *be an odd prime number and* k *a real quadratic field in which* p *splits. Then* $\lambda_p(k)$ *vanishes if and only if the following two conditions are satisfied*:

(1) *Every ideal class of* A_0 *becomes principal in* k_n *for some integer* $n \geq 0$.

(2) $n_0^{(r)} = r + 1$ *for some integer* $r \geq 0$.

Remark 2. If p remains prime in k or if it is ramified in k, then the unique prime ideal of k lying over p is totally ramified in k_∞/k. Hence, in both cases, Greenberg's theorem (Theorem 3) asserts that $\lambda_p(k)$ vanishes if and only if every ideal class of A_0 becomes principal in k_n for some integer $n \geq 0$. Thus, Theorem 4 seems to be interesting when compared with the case where p does not split in k.

Since every ideal class of D_0 becomes principal in k_n for some sufficiently large n, we obtain the following corollary to Theorem 4. This, which is one of the main results in the previous paper [6], often enables us to obtain numerical examples of k's with $\lambda_p(k) = 0$.

COROLLARY 4 (cf. Theorem 2 of [6]). *Let k and p be as in Theorem 4. Assume that $A_0 = D_0$. Then $\lambda_p(k) = 0$ if and only if $n_0^{(r)} = r + 1$ for some integer $r \geq 0$.*

5. An additional remark. We now make a simple remark on verification of the vanishing of $\lambda_p(k)$ based on Theorem 4. Let k and p be as in the preceding section. In [7] we introduced the following fact which is an immediate consequence of Theorem 3, Corollaries 2 and 3.

LEMMA 12 (cf. Proposition 2 of [7]). *The following two conditions are equivalent*:

(1) $\lambda_p(k) = 0$.
(2) $|D_r| = |A_0| p^{n_2 - 1 - n_2^{(r)} + n_0^{(r)}}$ *for some integer $r \geq 0$.*

Let $i_{0,n}$ denote the natural map from the ideal group of k to that of the intermediate field k_n of the cyclotomic $\mathbb{Z}_p$-extension k_∞/k. Then the following holds:

PROPOSITION 2. *Let k and p be as in Theorem 4. Let r be a non-negative integer. Then $|D_r| = |A_0| p^{n_2 - 1 - n_2^{(r)} + n_0^{(r)}}$ if and only if the following two conditions are satisfied*:

(1) $i_{0,r}(A_0) \subset D_r$.
(2) $n_0^{(r)} = r + 1$.

In particular, *if both of the conditions hold*, *then $\lambda_p(k) = 0$.*

Proof. Assume that $|D_r| = |A_0| p^{n_2 - 1 - n_2^{(r)} + n_0^{(r)}}$. Put $n_0^{(r)} = r + s$ with an integer $s \geq 1$. Then Lemma 9 says that

$$\frac{|\overline{A}_r^{\Gamma}|}{|D_r|} = \frac{|A_0| p^{r + n_2 - n_2^{(r)}}}{|A_0| p^{n_2 - 1 - n_2^{(r)} + n_0^{(r)}}} = p^{r + 1 - n_0^{(r)}}.$$

Hence $|\overline{A}_r^{\Gamma}| = |D_r| p^{1-s}$. On the other hand, since $D_n \subset \overline{A}_n^{\Gamma}$, we see that $1 - s \geq 0$, so $s = 1$, which means that condition (2) holds. Moreover, this implies that $\overline{A}_r^{\Gamma} = D_r$, which is equivalent to condition (1) as mentioned in the proof of Lemma 11.

Next assume that both (1) and (2) are satisfied. We have $|D_r| = |A_0|p^{r+n_2-n_2^{(r)}}$ by Lemma 9, because condition (1) holds if and only if $\overline{A}_r^{\Gamma} = D_r$. It then follows from (2) that $|D_r| = |A_0|p^{n_2-1-n_2^{(r)}+n_0^{(r)}}$. Thus the proof is completed. ∎

Let us put $p = 3$ and $k = \mathbb{Q}(\sqrt{m})$, where m denotes a positive square-free integer less than 100000 satisfying $m \equiv 1 \pmod 3$. In our previous papers [6] ($1 \le m \le 10000$) and [7] ($10000 \le m \le 100000$), we gave the data of $|A_r|$, $|D_r|$, $n_0^{(r)}$ and $n_2^{(r)}$ of $k = \mathbb{Q}(\sqrt{m})$ with $r \le 1$ and $p = 3$, and found that $\lambda_3(k)$ vanishes for most of these k's. Although the criterion given in Theorem 4 could be used to yield many numerical examples of k's with $\lambda_p(k) = 0$, no new examples with $\lambda_3(k) = 0$ among these k's can emerge on the ground of those data for $r \le 1$ alone and it is not efficient in yielding numerical examples given in [6] and [7] more easily (other results are sometimes more efficient as mentioned in [6]). Here is the reason. In our previous verification, we used Lemma 12 as a sufficient condition for the vanishing of $\lambda_3(k)$. Hence, Proposition 2 tells us that if we make use of (1) of Proposition 2 as a sufficient condition for (1) of Theorem 4 to hold, then no new examples with $\lambda_3(k) = 0$ can emerge from those data for $r \le 1$ alone. Therefore, to get new numerical examples of k's with $\lambda_3(k) = 0$ based on Theorem 4, we have to have the data for $r \ge 2$, or we have to find a sharper sufficient condition to assure that every ideal class of A_0 becomes principal in k_∞. But a capitulation problem seems to be difficult in general.

We finally mention that in the case $p = 3$, Takashi Fukuda is computing the invariants $n_0^{(r)}$ and $n_2^{(r)}$ with $r \ge 2$ to verify whether $\lambda_3(k)$ vanishes for the remaining k's in the above range. For further details, see his forthcoming paper.

References

[1] J. Coates, *p-adic L-functions and Iwasawa's theory*, in: Algebraic Number Fields, Durham Symposium, 1975, A. Fröhlich (ed.), Academic Press, 1977, 269–353.

[2] L. Federer, *P-adic L-functions, regulators, and Iwasawa modules*, Ph.D. Thesis, Princeton University, 1982.

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

[4] T. Fukuda and K. Komatsu, *On the λ invariants of $\mathbb{Z}_p$-extensions of real quadratic fields*, J. Number Theory 23 (1986), 238–242.

[5] —, —, *On $\mathbb{Z}_p$-extensions of real quadratic fields*, J. Math. Soc. Japan 38 (1986), 95–102.

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

[7] T. Fukuda and H. Taya, *Computational research on Greenberg's conjecture for real quadratic fields*, Mem. School Sci. Engrg. Waseda Univ. Tokyo 58 (1994), 175–203.
[8] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. 98 (1976), 263–284.
[9] K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. 65 (1959), 183–226.
[10] —, *Lectures on p-Adic L-Functions*, Ann. of Math. Stud. 74, Princeton Univ. Press, Princeton, N.J., 1972.
[11] H. Taya, *On the Iwasawa λ-invariants of real quadratic fields*, Tokyo J. Math. 16 (1993), 121–130.
[12] —, *Computation of $\mathbb{Z}_3$-invariants of real quadratic fields*, Math. Comp., to appear.
[13] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer, New York, 1982.

DEPARTMENT OF MATHEMATICS
SCHOOL OF SCIENCE AND ENGINEERING
WASEDA UNIVERSITY
3-4-1, OKUBO SHINJUKU-KU
TOKYO, 169 JAPAN
E-mail: TAYA@CFI.WASEDA.AC.JP

Received on 8.12.1994
and in revised form on 11.7.1995 (2710)