Annales Academiæ Scientiarum Fennicæ
Series A. I. Mathematica
Volumen 1, 1975, 343 – 353

ON THE IWASAWA INVARIANTS OF IMAGINARY ABELIAN FIELDS

TAUNO METSÄNKYLÄ

1. Introduction

Let E be an absolutely abelian number field and let p be a prime. A Galois extension of E is called a $\boldsymbol{Z}_p$-extension if its Galois group is isomorphic to the additive group of $\boldsymbol{Z}_p$, the ring of p-adic integers.

Fix a natural number m not divisible by p. For $n \geqq 0$, denote by F_n the cyclotomic field of $m\,q\,p^n$th roots of unity, where $q = p$ if $p > 2$ and $q = 4$ if $p = 2$. If $E = F_0$, then the union F_∞ of all the fields F_n is a $\boldsymbol{Z}_p$-extension of E. More generally, if E is a subfield of F_0 with conductor m or mq, then there exists a unique $\boldsymbol{Z}_p$-extension E_∞ of E, called the basic $\boldsymbol{Z}_p$-extension, which is contained in F_∞.

Denote by $\lambda = \lambda(E)$ and $\mu = \mu(E)$ the Iwasawa invariants of E, i.e. the Iwasawa invariants of the basic $\boldsymbol{Z}_p$-extension E_∞/E. It is well known that λ and μ are non-negative integers having the following connection with the class numbers h_n of the intermediate fields E_n of E and E_∞: if $[E_n : E] = p^n$ and if the highest power of p dividing h_n is $p^{e(n)}$, then, for all sufficiently large n, $e(n)$ is of the form $\lambda\, n + \mu\, p^n + \nu$, where ν is also an integer independent of n. Iwasawa [9] has conjectured that $\mu = 0$ for every E and p; the conjecture has been proved by B. Ferrero in the cases $p = 2$ and $p = 3$ (as yet unpublished).

In what follows we shall assume that E is imaginary, and put $\lambda = \lambda^+ + \lambda^-$, $\mu = \mu^+ + \mu^-$, where λ^+ and μ^+ are the Iwasawa invariants of the maximal real subfield of E. Thus, if $p^{a(n)}$ denotes the highest power of p dividing the first factor of the class number of E_n, we have $a(n) = \lambda^- n + \mu^- p^n + \nu^-$ (ν^- an integer) for all large n. While the normal approach to λ and μ is via the general theory of $\boldsymbol{Z}_p$-extensions (see [6], [10]), there is also another way of introducing λ^- and μ^-, namely the use of Iwasawa's theory of p-adic L-functions (see [7]). This method has been applied by Iwasawa [8] in case $E = F_0$. In the

doi:10.5186/aasfm.1975.0111

present note we shall first apply the same method to the case of a general E and an arbitrary odd prime p, and show the existence of the invariants λ^- and μ^- as sums of certain components which arise naturally from considering the characters of E. Furthermore, using results from [11] we shall obtain immediately a criterion for the vanishing of μ^-. This criterion, together with some facts proved essentially in [11], will then be applied to give a relationship between the invariants λ^- and μ^- of two abelian fields of a certain type.

2. Characters and p-adic L-functions

Throughout the following, let p be a fixed odd prime. As usual, let $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{Z}_p$, and $\boldsymbol{Q}_p$ stand for the ring of rational integers, the field of rational numbers, the ring of p-adic integers, and the field of p-adic numbers, respectively. Denote by $|\,.\,|$ the p-adic valuation on a fixed algebraic closure Ω_p of $\boldsymbol{Q}_p$.

Let χ be a Dirichlet character. We shall always assume that χ is primitive, and denote its conductor by f_χ. Let $U(f)$ denote the group of all characters χ with $f_\chi \mid f$.

Suppose that m is a natural number prime to p. For each $n \geqq 0$, denote by G_n the multiplicative residue class group $\bmod\, m\,p^{n+1}$, consisting of all elements $\sigma_n(a) = a + m\,p^{n+1}\boldsymbol{Z}$, where $(a\,,m\,p) = 1$. It is known that $G_n = \Delta_n \times \Gamma_n$ (direct product), where

$$\Delta_n = \{\,\sigma_n(a) \mid a^{p-1} \equiv 1 \pmod{p^{n+1}}\,\}\,,$$

$$\Gamma_n = \{\,\sigma_n(a) \mid a \equiv 1 \pmod{m\,p}\,\}$$

(see e.g. [5], pp. 78–81, [8], p. 67). From this it follows that

$$U(m\,p^{n+1}) = U(m\,p) \times T_n\,,$$

where T_n is the group of all characters π satisfying the conditions $f_\pi \mid p^{n+1}$ and $\pi(a) = 1$ whenever $\sigma_n(a) \in \Delta_n$. Usually the elements of $U(m\,p)$ and T_n are called characters of first and second kind, respectively. Note that T_n is a cyclic group of order p^n.

The unit group of $\boldsymbol{Z}_p$ can be written in the form $\boldsymbol{V} \times \boldsymbol{D}$, where $\boldsymbol{V}$ is the group of all $(p-1)$st roots of unity and $\boldsymbol{D}$ the group of principal units. For any p-adic unit a, let $\omega(a)$ denote the projection of a on $\boldsymbol{V}$ under this decomposition. Then ω can be regarded, in an obvious manner, as a character with order $p-1$ and conductor p. In particular, $\omega \in U(m\,p)$.

Now let $L_p(s\,;\chi)$ be the p-adic L-function for an even character

$\chi \in U(m\,p^{n+1})$. For our purposes it suffices to consider the value of $L_p(s\,;\,\chi)$ at $s = 0$; a well-known formula ([8], p. 30) asserts that

$$(1) \qquad L_p(0\,;\,\chi) = -(1 - (\chi\,\omega^{-1})(p))\,B_1(\chi\,\omega^{-1})\,,$$

where $B_1(\chi)$ denotes the first generalized Bernoulli number belonging to the character χ . Put $\chi = \theta\,\pi$ with $\theta \in U(m\,p)$ and $\pi \in T_n$; then $f_\theta = m_0$ or $m_0\,p$ with $m_0 \mid m$. Let K be a finite extension of Q_p in Ω_p , containing the numbers $\theta(a)$ for all $a \in Z$, and let $\mathfrak{o}$ be the ring of local integers in K . It follows from Iwasawa's theory of p-adic L-functions that

$$(2) \qquad L_p(0\,;\,\chi) = 2f(\pi\,(1 + m_0\,p)^{-1} - 1\,;\,\theta)$$

([8], p. 87), where $f(x\,;\,\theta)$ is a certain power series with coefficients in $\mathfrak{o}$, if $\theta \neq \chi_0$ (i.e., θ is non-principal), and $f(x\,;\,\chi_0)$ is a quotient of two such power series.

3. The invariants λ^- and μ^- of imaginary abelian fields

Let $E\,/\,Q$ be a finite imaginary abelian extension. When investigating the invariants λ^- and μ^- of the basic Z_p-extension $E_\infty\,/\,E$ we may assume without loss of generality that the conductor of E is of the form m or $m\,p$.

Let F_0 , F_1 ,... denote the cyclotomic fields defined in the introduction. We shall identify Gal $(F_n/\,Q)$, the Galois group of $F_n/\,Q$, with the group G_n in the usual manner. Then

$$\mathrm{Gal}\,(F_n\,/\,F_0) = \Gamma_n\,, \qquad \mathrm{Gal}\,(F_0\,/\,Q) = G_0 = \Delta_0\,.$$

Moreover, the character group Ch (F_n) belonging to the extension $F_n\,/\,Q$ is $U(m\,p^{n+1})$.

Put $Y = \mathrm{Ch}\,(E)$ and note that Y is a subgroup of $U(m\,p)$. Let

$$E = E_0 \subset E_1 \subset \ldots \subset E_n \subset \ldots$$

be the infinite tower of fields determining the Z_p-extension $E_\infty\,/\,E$. Then we have Gal $(E_n\,/\,E) \simeq \Gamma_n$ and

$$F_n = F_0\,E_n\,, \qquad E = F_0 \cap E_n$$

for every $n \geqq 0$. Hence Gal $(F_n/\,E_n)$ is a subgroup of Δ_n and it follows easily that

$$\mathrm{Ch}\,(E_n) = Y \times T_n\,.$$

Now let

$$X = X(E) = \{\,\theta\,\omega \mid \theta \in Y^-\,,\ \theta \neq \omega^{-1}\,\}\,,$$

where by Y^- is meant the subset of Y consisting of all odd characters. Note that the set X is empty if and only if E is the cyclotomic field of 3rd roots of unity. Let h_n and h_n^+ denote the class numbers of E_n and its maximal real subfield, respectively. We shall prove the following lemma on $h_n^- = h_n / h_n^+$.

Lemma 1. *Put*

$$A(x) = \prod_{\theta \in X} f(x\,;\,\theta)\,;$$

then

$$|h_n^- / h_0^-| = |\prod_{\zeta \in W_n} A(\zeta - 1)| \qquad (n \geqq 1)\,,$$

where W_n *denotes the set of all* p^n*th roots of unity except* 1.

Proof. We start from the formula ([4], p. 12)

$$h_n^- = Q_n\, w_n \prod_{\chi} \Big(- \frac{1}{2 f_\chi} \sum_{a=1}^{f_\chi} a\, \chi(a) \Big) \qquad (n \geqq 0)\,,$$

where $Q_n = 1$ or 2, w_n is the number of roots of unity in E_n, and the product is extended over all odd characters χ in $Y \times T_n$. Let us fix a generator π_n of T_n. Noting that

$$f_\chi^{-1} \sum_{a=1}^{f_\chi} a\, \chi(a) = B_1(\chi)$$

(see e.g. [8], p. 14) we then obtain

$$\text{(3)} \qquad | h_n^- / h_0^- | = | (w_n / w_0) \prod_{\theta \in Y^-} \prod_{k=1}^{p^n - 1} (- \tfrac{1}{2} B_1(\theta\, \pi_n^k)) | \qquad (n \geqq 1)\,.$$

Consider a character $\chi = \theta\, \omega\, \pi_n^k$ with $\theta \in Y^-$, $1 \leqq k \leqq p^n - 1$. We have $\chi(-1) = 1$, $(\chi\, \omega^{-1})(p) = 0$ and $f_{\theta\omega} = m_0$ or $m_0\, p$, where $m_0 | m$. Hence, by combining (1) and (2) we find that

$$- B_1(\theta\, \pi_n^k) = 2 f(\zeta_\chi - 1\,;\, \theta\, \omega) \qquad (\zeta_\chi = \pi_n\, (1 + m_0\, p)^{-k})\,.$$

It is easy to see that ζ_χ ranges over W_n as k runs through $1, \ldots, p^n - 1$. Thus (3) becomes

$$\text{(4)} \qquad |h_n^- / h_0^-| = | (w_n / w_0) \prod_{\theta \in Y^-} \prod_{\zeta \in W_n} f(\zeta - 1\,;\, \theta\, \omega) | \qquad (n \geqq 1)\,.$$

Now we have to distinguish between two cases, according to whether E contains the pth roots of unity or not.

Assume first that $W_1 \subset E$. Then $\omega \in Y^-$ and the right hand side of (4) contains the factor

$$| \prod_{\zeta \in W_n} f(\zeta - 1\,;\, \chi_0)| = |p^n|^{-1}$$

([8], p. 92). On the other hand, $w_n = w_0 p^n$, so that the assertion of the lemma follows.

If W_1 is not contained in E, we have $\omega \notin Y^-$ and $w_n = w_0$. Thus our assertion is immediate from (4).

Remark 1. If $|A(\zeta-1)| < 1$ for some $\zeta \in W_n$, then $|A(0)| < 1$ and so $|A(\zeta-1)| < 1$ for every $\zeta \in W_n$. Consequently, it follows from Lemma 1 that

(i) p divides h_n^-/h_0^- $(n \geqq 1)$ if and only if p divides h_1^-/h_0^-;

(ii) if p divides h_n^-/h_0^- $(n \geqq 1)$, then p^n divides h_n^-/h_0^-.

In particular, if $m = 1$ (i.e., E is a subfield of the cyclotomic field of pth roots of unity), then an obvious modification of the proof of Lemma 1 leads to the formula

$$|h_n^-| = \Big|\prod_{\zeta \in W_n \cup \{1\}} A(\zeta-1)\Big| \qquad (n \geqq 0),$$

so that we obtain the following simpler results:

(i′) $p \mid h_n^-$ if and only if $p \mid h_0^-$;

(ii′) if $p \mid h_n^-$, then $p^{n+1} \mid h_n^-$.

Another proof for (i′) and (ii′) has been given by Adachi [1].

Now suppose that the field K associated with the power series $f(x;\theta)$ is the extension of $\boldsymbol{Q}_p$ generated by all numbers $\theta(a)$, where $\theta \in X(E)$ and $a \in \boldsymbol{Z}$. Let e denote the ramification index of $K/\boldsymbol{Q}_p$, let π be a fixed prime element of the ring $\mathfrak{o}$, and let $\mathfrak{p} = \pi\mathfrak{o}$.

Lemma 2. *For $\theta \in X(E)$, define non-negative integers $\lambda_\theta = \lambda_\theta(E)$ and $\mu_\theta = \mu_\theta(E)$ by*

$$f(x;\theta) = \pi^{\mu_\theta} \sum_{k=0}^{\infty} \alpha_k x^k \qquad (\alpha_k \in \mathfrak{o}),$$

$$\alpha_k \equiv 0 \pmod{\mathfrak{p}} \ \textit{for}\ 0 \leqq k < \lambda_\theta,$$

$$\alpha_k \not\equiv 0 \pmod{\mathfrak{p}} \ \textit{for}\ k = \lambda_\theta.$$

Then the numbers

$$\lambda^- = \sum_{\theta \in X} \lambda_\theta, \qquad \mu^- = e^{-1} \sum_{\theta \in X} \mu_\theta$$

are the invariants $\lambda^-(E)$, $\mu^-(E)$ of the extension E_∞/E.

Proof. We have

$$A(x) = \prod_{\theta \in X} f(x;\theta) = \pi^{e\mu^-} B(x),$$

where

$$B(x) = \sum_{k=0}^{\infty} \beta_k x^k \qquad (\beta_k \in \mathfrak{o})$$

with $\beta_k \equiv 0 \pmod{\mathfrak{p}}$ for $0 \leqq k < \lambda^-$ and $\beta_k \not\equiv 0 \pmod{\mathfrak{p}}$ for $k = \lambda^-$. Let t be the least non-negative integer such that $e\,\lambda^- < (p-1)\,p^t$. Assuming that $n > t$ and $\zeta \in W_n - W_{n-1}$ we then find that $|\pi| < |\zeta - 1|^{\lambda^-}$ and so, furthermore,

$$|A(\zeta-1)| = |\pi^{e\mu^-} B(\zeta-1)| = |p^{\mu^-}|\,|\zeta-1|^{\lambda^-} .$$

This together with Lemma 1 yields

$$|h_n^-| = |p^{a(n)}| , \qquad a(n) = \lambda^- n + \mu^- p^n + \nu^- \qquad (n > t) ,$$

where ν^- is an integer independent of n.

Remark 2. Suppose that $E \subset E'$, where E' is abelian with conductor m' or $m'\,p$, m' being prime to p. Then $X(E) \subset X(E')$. Therefore, if $\theta \in X(E)$ then $\lambda_\theta(E) = \lambda_\theta(E')$ and $e'\,\mu_\theta(E) = e\,\mu_\theta(E')$, where e' is the ramification index of the extension $K' / \boldsymbol{Q}_p$ determined by $X(E')$.

It should be noted that the numbers $\lambda_\theta(F_0)$, $\mu_\theta(F_0)$ have been introduced and investigated by the author in [11]. (Cf. [11], Remark (ii) of Section 4.)

4. On the vanishing of λ^- and μ^-

As an immediate consequence of Remark 1 we may state that the condition

$$\lambda^- = \mu^- = 0 \tag{5}$$

is equivalent to $(p\,, h_1^- / h_0^-) = 1$, and if $m = 1$, (5) is equivalent to $(p\,, h_0^-) = 1$. The latter statement is also implied by the following stronger result, proved essentially in [11] (Lemma 2): for $\theta = \omega^u \in X(E)$, $\lambda_\theta(E) = \mu_\theta(E) = 0$ if and only if the uth Bernoulli number B_u is prime to p. Indeed, if $m = 1$ then $(p\,, h_0^-) = 1$ is equivalent to the fact that the numbers B_u are prime to p whenever $\omega^u \in X(E)$ (see [2], [1]).

We shall now give a general criterion for the vanishing of $\mu_\theta(E)$. For $n \geqq 0$, let $\gamma_n(a)$ be the projection of $\sigma_n(a)$ on Γ_n under the direct decomposition $G_n = \Delta_n \times \Gamma_n$, so that $\gamma_n(a)$ runs through the elements of Γ_n, say g_{nk} $(k = 0, \ldots, p^n - 1)$, as $\sigma_n(a)$ runs through G_n. For $\theta \in X(E)$, put

$$\xi_n = -\,(2\,m\,p^{n+1})^{-1} \sum_{\substack{a=1 \\ (a,mp)=1}}^{mp^{n+1}} a\,\theta(a)\,\omega^{-1}(a)\,\gamma_n(a)^{-1} = \sum_{k=0}^{p^n-1} S_{nk}\,g_{nk} .$$

We know that ξ_n belongs to the group algebra $\mathfrak{o}[\Gamma_n]$, i.e. the numbers $S_{nk} = S_{nk}(\theta\,; E)$ belong to $\mathfrak{o}$, and that $\xi_{n+1} \mapsto \xi_n$ under the morphism $\mathfrak{o}[\Gamma_{n+1}] \to \mathfrak{o}[\Gamma_n]$, induced by $\sigma_{n+1}(a) \mapsto \sigma_n(a)$ ([8], pp. 72–76). Let R

denote the inverse limit of the $\mathfrak{o}[\Gamma_n]$ with respect to these morphisms. Then $\xi = \lim \xi_n$ is a well-defined element of R and closely connected with the power series $f(x\,;\theta) \in \mathfrak{o}[[x]]$. Indeed, ξ is the image of $f(x\,;\theta)$ under the unique isomorphism $\tau : \mathfrak{o}[[x]] \to R$, determined by the condition $\tau(1+x) = \lim \gamma_n(1+m\,p)$. This enables us to formulate the following lemma (see [11], Lemma 5).

Lemma 3. *A necessary and sufficient condition for* $\mu_\theta(E) > 0$ *is that*

$$S_{nk}(\theta\,;E) \equiv 0 \pmod{\mathfrak{p}} \tag{6}$$

for all $n \geqq 0$ *and all* $k \in I_n = \{0, \dots, p^n - 1\}$.

From this it is seen that $\mu^-(E) > 0$ if and only if there is at least one $\theta \in X(E)$ such that the infinite system of congruences (6) is satisfied.

Remark 3. If $\theta \in X(E)$, then $\lambda_\theta(E) = \mu_\theta(E) = 0$ is equivalent to the condition $S_{00}(\theta\,;E) \not\equiv 0 \pmod{\mathfrak{p}}$. This is proved in [11] under the assumption that the conductors of θ and $\theta\,\omega^{-1}$ are equal to $m\,p$. However, this restriction is unnecessary, since an inspection of the above isomorphism τ shows that, in any case,

$$f(0\,;\theta) = S_{00}(\theta\,;E)\,.$$

Remark 4. A sufficient condition for $\mu_\theta(E) > 0$ is that

$$S_{nk}(\theta\,;E) \equiv S_{n0}(\theta\,;E) \pmod{\mathfrak{p}}$$

for all $n \geqq 1$ and all $k \in I_n$, as can be verified in the following way. By considering the morphism $\mathfrak{o}[\Gamma_{n+1}] \to \mathfrak{o}[\Gamma_n]$ mentioned above one finds that

$$S_{nk} = \sum_h S_{n+1,\,h}\,,$$

the sum being extended over those $h \in I_{n+1}$ for which $g_{n+1,\,h} \mapsto g_{nk}$. Obviously, the number of such h is p, so that

$$S_{nk} \equiv \sum_h S_{n+1,\,0} \equiv p\,S_{n+1,\,0} \equiv 0 \pmod{\mathfrak{p}} \qquad (n \geqq 0\,,\ k \in I_n)\,.$$

For the rest of this section we assume that $m = 1$ and $p > 3$. Denote by P the cyclotomic field of pth roots of unity; then

$$X(P) = \{\,\omega^u \mid u = 2, 4, \dots, p-3\,\}$$

and E is a subfield of P.

We shall introduce some further notation. Let $s = (p-1)/2$, let r be a primitive root $\bmod\, p^{n+1}$ for all $n \geqq 0$, and let $r_n(i)$ be the least positive residue of $r^i \pmod{p^{n+1}}$. Denote by α the primitive $(p-1)$st root of unity satisfying

$$\omega(a) = \alpha^i \qquad \text{for } a \equiv r^i \pmod{p}\,.$$

For rational integers h and u, put

$$R_n(h\,,u) \;=\; \sum_{i=0}^{p-2} r_n(i\,p^n + h)\,\alpha^{i(u-1)} \qquad (n \geqq 0)\,.$$

Then we have the following supplement to Lemma 3.

Lemma 4. *If* $E \subset P$ *and* $\omega^u \in X(E)$, *then*

$$-\,2\,p^{n+1}\,S_{nk}(\omega^u\,;E) \;=\; R_n(k\,,u)\,\alpha^{k(u-1)} \qquad (n \geqq 0\,,\; k \in I_n)\,,$$

provided the elements g_{nk} *of* Γ_n *are suitably ordered.*

For the proof, see [11], proof of Lemma 8.

It will be useful to notice that $R_n(h\,,u)$ satisfies the conditions

$$\text{(7)}\qquad R_n(h\,,u) \;=\; 2\sum_{i=0}^{s-1} r_n(i\,p^n + h)\,\alpha^{i(u-1)} \;-\; 2\,p^{n+1}\,(1-\alpha^{u-1})^{-1}\,,$$

$$\text{(8)}\quad R_n(h\,,u)\,\alpha^{j(u-1)} \;=\; R_n(g\,,u) \qquad \text{for } h \equiv j\,p^n + g \pmod{(p-1)\,p^n}\,.$$

5. An example: the invariants of a quadratic field

Let $E = \boldsymbol{Q}((-3)^{1/2})$ and $p > 3$. Then $X(E)$ contains only one element, namely $\theta\,\omega$, where $\theta(a) = (a/3)$ (the Legendre symbol). Hence, in this case $\mathfrak{o} = \boldsymbol{Z}_p$. Moreover,

$$\lambda^+(E) \;=\; \lambda(\boldsymbol{Q}) \;=\; 0\,, \qquad \mu^+(\mathrm{E}) \;=\; \mu(\boldsymbol{Q}) \;=\; 0$$

([6], p. 225) and so $\lambda(E) = \lambda^-(E) = \lambda_{\theta\omega}(E)$, $\mu(E) = \mu^-(E) = \mu_{\theta\omega}(E)$. We shall first employ Lemma 3 to prove that $\mu(E) = 0$.

Now

$$S_{nk} \;=\; -\,(6\,p^{n+1})^{-1}\sum_a a\,(a/3)\,,$$

where the summation is extended over the values of a satisfying the conditions $1 \leqq a < 3\,p^{n+1}$, $(a\,,3\,p) = 1$, $\gamma_n(a)^{-1} = g_{nk}$. Let $c_{n1}(i)$ and $c_{n2}(i)$ be positive integers less than $3\,p^{n+1}$ such that

$$c_{n1}(i) \;\equiv\; c_{n2}(i) \;\equiv\; r^i \pmod{p^{n+1}}\,,$$

$$c_{n1}(i) \;\equiv\; 1,\; c_{n2}(i) \;\equiv\; -1 \pmod{3}\,.$$

Then Δ_n can be written in the form

$$\Delta_n \;=\; \{\,\sigma_n(a)\mid a = c_{n1}(ip^n) \text{ or } a = c_{n2}(ip^n)\,,\; i \;=\; 0, \ldots, p-2\,\}\,.$$

After a suitable rearrangement of the elements g_{nk} of Γ_n we therefore get

$$S_{nk} \;=\; -\,(6\,p^{n+1})^{-1}\sum_{i=0}^{p-2}\,[c_{n1}(i\,p^n + k) - c_{n2}(i\,p^n + k)]\,.$$

Furthermore, $c_{n1}(i\,p^n + k) - c_{n2}(i\,p^n + k) = \pm b_i\,p^{n+1}$, where each b_i is equal to 1 or 2 and, as is easy to see, $b_i = b_{i+s}$. Hence

$$S_{nk} = -\tfrac{1}{3}\sum_{i=0}^{s-1}(\pm b_i)\,, \qquad \left|\sum_{i=0}^{s-1}(\pm b_i)\right| < p\,.$$

Now, if $\mu > 0$ then Lemma 3 shows that all the numbers S_{nk} vanish. But this would imply that $f(x\,;\theta\,\omega) = 0$, which is impossible by Lemma 1. Consequently, $\mu = 0$.

We are also able to determine those primes p for which $\lambda = 0$. In fact, using (2) and (1) we may calculate $f(0\,;\theta\,\omega)$ as follows:

$$f(0\,;\theta\,\omega) = \tfrac{1}{2}L_p(0\,;\theta\,\omega) = -\tfrac{1}{2}(1-(p/3))\,B_1(\theta) = (1-(p/3))/6\,.$$

From this we infer that $\lambda = 0$ if and only if $p \equiv 2 \pmod 3$.

We note that the Iwasawa invariants of imaginary quadratic fields have been examined by Gold in several papers (e.g. [3]).

6. A relationship between the invariants of certain fields

Let $p > 3$ and let l be a prime, $l \equiv 1 \pmod p$. From now on, we shall assume that E is the abelian field with conductor $l\,p$, which is of degree p over P.

Put $t = (l-1)/p$ and denote by ψ a generating character mod l. Then

$$\mathrm{Ch}\,(E) = \{\,\psi^{tv}\,\omega^u \mid 0 \leqq v \leqq p-1\,,\ 0 \leqq u \leqq p-2\,\}$$

and so

$$X(E) = \{\,\psi^{tv}\,\omega^u \mid 0 \leqq v \leqq p-1\,,\ 2 \leqq u \leqq p-3\,,\ 2 \mid u\,\}\,.$$

It follows from [11] (Lemma 10) that if $\chi = \psi^{tv}\,\omega^u \in X(E) - X(P)$, then

$$S_{nk}(\chi\,;E) \equiv$$
$$-\,p^{-n-1}\sum_{i=0}^{s-1}[r_n(i\,p^n+k) - r_n(i\,p^n+k-d_n)]\,\alpha^{(i+k)(u-1)} \pmod{\mathfrak{p}} \tag{9}$$

$(n \geqq 0\,,\ k \in I_n)$, where d_n is defined by $l \equiv r_n(d_n) \pmod{p^{n+1}}$. This result expresses a certain connection between the μ^--invariants of E and P. In fact, we may formulate the following theorem, the first part of which is essentially proved in [11].

Theorem. (i) *If* $\mu_\theta(P) > 0$ *for some* $\theta = \omega^u \in X(P)$, *then* $\mu_\chi(E) > 0$ *for all* $\chi = \psi^{tv}\,\omega^u \in X(E)$.

(ii) *Suppose that* $l \not\equiv 1 \pmod{p^2}$. *If* $\mu_\chi(E) > 0$ *for some* $\chi = \psi^{tv}\,\omega^u \in X(E) - X(P)$, *then* $\mu_\theta(P) > 0$ *for* $\theta = \omega^u$.

Proof. For the proof of (i), see [11], proof of Theorem 3. We shall now prove (ii). Using Lemma 3 we get that

$$S_{nk}(\psi^{tv}\,\omega^u\,;E) \equiv 0 \pmod{\mathfrak{p}}$$

whenever $n \geqq 0$ and $k \in I_n$. This implies, by (9), that

$$\sum_{i=0}^{s-1} r_n(i\,p^n + k)\,\alpha^{i(u-1)} \equiv \sum_{i=0}^{s-1} r_n(i\,p^n + k - d_n)\,\alpha^{i(u-1)} \pmod{p^{n+2}}$$

for all these n and k. In view of (7) and (8) it then follows that

$$R_n(h\,,u) \equiv R_n(h-d_n\,,u) \pmod{p^{n+2}} \tag{10}$$

for all $n \geqq 0$ and all $h \in \mathbf{Z}$.

Since $l \equiv 1 \pmod{p}$, we have $r_n(d_n) \equiv 1 \pmod{p}$ and so d_n is divisible by $p-1$ $(n \geqq 0)$. On the other hand, $l \not\equiv 1 \pmod{p^2}$ so that d_n is not divisible by p for $n \geqq 1$. Let us fix some $n \geqq 1$ and some $k \in I_n$. Let z satisfy the congruence $d_n z \equiv k \pmod{p^n}$. Then

$$k \equiv k\,p^n + d_n z \pmod{(p-1)\,p^n}$$

and therefore, by (8),

$$R_n(k\,,u)\,\alpha^{k(u-1)} = R_n(d_n z\,,u)\,.$$

Combined with (10) this yields

$$R_n(k\,,u)\alpha^{k(u-1)} \equiv R_n(0\,,u) \pmod{p^{n+2}}\,.$$

We now apply Lemma 4 to rewrite the last congruence as

$$S_{nk}(\omega^u\,;P) \equiv S_{n0}(\omega^u\,;P) \pmod{p}\,.$$

Because this holds for all $n \geqq 1$ and $k \in I_n$, our assertion follows from the result stated in Remark 4.

Corollary. (i) *If* $\mu^-(P) > 0$, *then* $\mu^-(E) > 1$.

(ii) *Provided that* $l \not\equiv 1 \pmod{p^2}$, *if* $\mu^-(P) = 0$ *then* $\mu^-(E) = 0$ *and* $\lambda^-(E) \geqq (p-1)(p-3)/2$.

Proof. For (i), it is enough to apply part (i) of the theorem to

$$\mu^-(E) = \mu^-(P) + e^{-1} \sum_{\chi \in X(E)-X(P)} \mu_\chi(E)\,.$$

To establish (ii), let $\mu^-(P) = 0$. Then the result $\mu^-(E) = 0$ is immediate from part (ii) of the theorem. Moreover, since $d_0 \equiv 0 \pmod{p-1}$ it follows from (9) that $S_{00}(\chi\,;E) \equiv 0 \pmod{\mathfrak{p}}$ for every $\chi \in X(E) - X(P)$. But $\mu_\chi(E) = 0$ and so the result of Remark 3 tells us that $\lambda_\chi(E) > 0$. Accordingly, $\lambda^-(E)$ is greater than or equal to the number of elements of $X(E) - X(P)$, as was to be proved.

The above result that $\mu^{-}(P) = 0$ implies $\mu^{-}(E) = 0$ follows also from a more general result proved by Iwasawa ([9], p. 10) by another method.

As pointed out in [11], it follows from part (i) of the theorem that $\mu^{-}(P) > 0$ implies the existence of Z_p-extensions F_∞/F_0 with arbitrarily large μ^{-}. Similarly, if $\mu^{-}(P) = 0$, part (ii) gives us Z_p-extensions F_∞/F_0 with arbitrarily large λ^{-}. It also gives, for every regular prime p, infinitively many basic Z_p-extensions E_∞/E with $\mu^{-} = 0$, $\lambda^{-} > 0$.

References

[1] Adachi, N.: Generalization of Kummer's criterion for divisibility of class numbers. - J. Number Theory 5, 1973, 253—265.

[2] Carlitz, L.: The first factor of the class number of a cyclic field. - Canad. J. Math. 6, 1954, 23—26.

[3] Gold, R.: The nontriviality of certain $\mathbf{Z}_l$-extensions. - J. Number Theory 6, 1974, 369—373.

[4] Hasse, H.: Über die Klassenzahl abelscher Zahlkörper. - Akademie-Verlag, Berlin, 1952.

[5] —»— Vorlesungen über Zahlentheorie. 2. Aufl. - Springer-Verlag, Berlin—Göttingen—Heidelberg—New York, 1964.

[6] Iwasawa, K.: On Γ-extensions of algebraic number fields. - Bull. Amer. Math. Soc. 65, 1959, 183—226.

[7] —»— On p-adic L-functions. - Ann. of Math. 89, 1969, 198—205.

[8] —»— Lectures on p-adic L-functions. - Princeton University Press, Princeton, 1972.

[9] —»— On the μ-invariants of $\mathbf{Z}_l$-extensions. - Number theory, algebraic geometry and commutative algebra, in honor of Y. Akizuki, Kinokuniya, Tokyo, 1973, 1—11.

[10] —»— On $\mathbf{Z}_l$-extensions of algebraic number fields. - Ann. of Math. 98, 1973, 246—326.

[11] Metsänkylä, T.: On the cyclotomic invariants of Iwasawa. - Math. Scand. 37, 1975, 61—75.

University of Turku
Department of Mathematics
SF-20500 Turku 50
Finland

Received 10 June 1975