On the Vanishing of Iwasawa Invariants of Certain Cyclic Extensions of $\boldsymbol{Q}$ with Prime Degree

By Takashi FUKUDA

Department of Mathematics, College of Industrial Technology, Nihon University

(Communicated by Shokichi IYANAGA, M. J. A., June 12, 1997)

Abstract: Let ℓ be an odd prime. In [2], Yamamoto gave a condition for (ℓ, ℓ)-extensions K of $\boldsymbol{Q}$, under which the Iwasawa invariants $\lambda_\ell(K)$ and $\mu_\ell(K)$ vanish. In this note, we shall give a condition for (ℓ, ℓ)-extensions K of $\boldsymbol{Q}$, which is weaker than the condition given in [2], under which we have $\lambda_\ell(k) = \mu_\ell(k) = 0$ for any subfields k of K with $[k:\boldsymbol{Q}] = \ell$. Our proof is based on Greenberg's original idea (cf. [1]), which is more elementary than that in [2], using the capitulation of the ℓ-part of the ideal class group of k in the initial layer of the cyclotomic $\boldsymbol{Z}_\ell$-extension of k to assure $\lambda_\ell(k) = \mu_\ell(k) = 0$.

Key words: Capitulation; Iwasawa invariants.

1. Introduction. Throughout the paper, we fix an odd prime number ℓ. For a cyclic extension k of $\boldsymbol{Q}$ of degree ℓ, we denote by $A(k)$ the ℓ-primary part of the ideal class proup of k and $B(k)$ the subgroup of $A(k)$ consisting of elements which are invariant under the action of the Galois group $G(k/\boldsymbol{Q})$. Let $p_1, p_2, \cdots, p_s$ be the prime numbers which are ramified in $k/\boldsymbol{Q}$ and let $\mathfrak{p}_i$ be the prime ideal of k lying over p_i. Then it is easy to see from the genus theory that $B(k)$ is an ℓ-elementary abelian group of rank $s-1$ generated by $\mathrm{cl}(\mathfrak{p}_1), \mathrm{cl}(\mathfrak{p}_2), \cdots, \mathrm{cl}(\mathfrak{p}_s)$. Let $\bar{k}$ (resp. $\tilde{k}$) be the ℓ-part of the Hilbert class field (resp. genus field) of k. Then we have the isomorphism $A(k) \xrightarrow{\sim} G(\bar{k}/k)$ and hence the surjective homomorphism

$$\varphi : A(k) \ni \mathrm{cl}(\mathfrak{a}) \mapsto \left(\frac{\tilde{k}/k}{\mathfrak{a}}\right) \in G(\tilde{k}/k)$$

through the Artin map.

The next lemma and corollary permit us to handle the capitulation problem in k by computation in the Galois group $G(\tilde{k}/k)$.

Lemma 1.1. *We have $A(k) = B(k)$ if and only if the restriction map $\varphi \mid B(k) : B(k) \to G(\tilde{k}/k)$ is surjective.*

Proof. Let $\bar{G} = G(\bar{k}/\boldsymbol{Q})$, $X = G(\bar{k}/k)$ and $G = G(k/\boldsymbol{Q}) = \langle\sigma\rangle$. Then G acts on X by an inner automorphism. Since at least one prime ideal is totally ramified in $k/\boldsymbol{Q}$, the group extension $1 \to X \to \bar{G} \to G \to 1$ splits. Hence we see that $[\bar{G}, \bar{G}] = X^{\sigma-1}$ and so $A(k)/A(k)^{\sigma-1} \simeq X/X^{\sigma-1} \simeq G(\tilde{k}/k)$ as G-module. Assume that $\varphi \mid B(k)$ is surjective. Then $A(k) = B(k)A(k)^{\sigma-1}$. Since the order of σ is ℓ and the order of $A(k)$ is a power of ℓ, this implies $A(k) = B(k)$. The converse is trivial.

Corollary 1.2. *Assume that $\varphi \mid B(k)$ is surjective. Then an ideal $\mathfrak{a}$ of k whose class belongs to $A(k)$ is principal if and only if* $\left(\frac{\tilde{k}/k}{\mathfrak{a}}\right) = 1$.

Proof. We have $\bar{k} = \tilde{k}$ because $A(k) = B(k)$.

2. Results. For a prime number p congruent to one modulo ℓ, we denote by k_p the unique subfield of $\boldsymbol{Q}(\zeta_p)$ of degree ℓ, where ζ_p is a primitive p-th root of unity. Let q be another prime number congruent to one modulo ℓ. Then $k_p k_q$ is an (ℓ, ℓ)-extension of $\boldsymbol{Q}$ and has $\ell - 1$ subfields which are cyclic extensions of $\boldsymbol{Q}$ of degree ℓ, in which both p and q are ramified. Let k be one of such subfields and $\mathfrak{p}_p$ (resp. $\mathfrak{p}_q$) the prime ideal of k lying over p (resp. q). Then $B(k) = \langle \mathrm{cl}(\mathfrak{p}_p), \mathrm{cl}(\mathfrak{p}_q)\rangle$ and $|B(k)| = \ell$. Note that $k_p k_q$ is the ℓ-part of the genus field of $k/\boldsymbol{Q}$. Since $\mathfrak{p}_p$ is ramified in $k/\boldsymbol{Q}$, $\left(\frac{k_p k_q/k}{\mathfrak{p}_p}\right)$ is trivial if and only if $\left(\frac{k_q/\boldsymbol{Q}}{p}\right)$ is trivial. Let $\left(\frac{p}{q}\right)_\ell$ denote the ℓ-th power residue symbol. Then the following lemma is an immediate consequence of Lemma 1.1.

Lemma 2.1. *We have $|A(k)| = \ell$ if and*

1991 Mathematics Subject Classification, Primary 11R23.

only if $\left(\frac{p}{q}\right)_\ell \neq 1$ *or* $\left(\frac{q}{p}\right)_\ell \neq 1$.

Now let $\boldsymbol{Q}_1$ be the initial layer of the cyclotomic $\boldsymbol{Z}_\ell$-extension of $\boldsymbol{Q}$, namely the unique subfield of $\boldsymbol{Q}(\zeta_{\ell^2})$ of degree ℓ. Then $k\boldsymbol{Q}_1$ is the initial layer of the cyclotomic $\boldsymbol{Z}_\ell$-extension of k. The following Theorem 2.2 is our main theorem which gives a sufficient condition to the fact that the natural map $A(k) \to A(k\boldsymbol{Q}_1)$ induced from the inclusion map $k \to k\boldsymbol{Q}_1$ is zero map, leading to the vanishing of the Iwasawa invariants $\lambda_\ell(k)$ and $\mu_\ell(k)$, as proved in the next paragraph.

Theorem 2.2. *Let p and q be distinct prime numbers congruent to one modulo ℓ satisfying* $\left(\frac{\ell}{p}\right)_\ell \neq 1$, $\left(\frac{p}{q}\right)_\ell \neq 1$, $q \not\equiv 1 \pmod{\ell^2}$. *Let x, y, $z \in \boldsymbol{F}_\ell$ such that* $\left(\frac{q\ell^x}{p}\right)_\ell = 1$, $\left(\frac{\ell p^y}{q}\right)_\ell = 1$ *and* $pq^z \equiv 1 \pmod{\ell^2}$. *If $xyz \neq -1$, then for any subfield k of k_pk_q of degree ℓ which is different from k_p and k_q, the order of $A(k)$ is ℓ and the map $A(k) \to A(k\boldsymbol{Q}_1)$ is trivial.*

Corollary 2.3. *Let p, q, x, y and z be as in Theorem 2.2. If $xyz \neq -1$, then for any subfield k of k_pk_q of degree ℓ, the Iwasawa invariants $\lambda_\ell(k)$ and $\mu_\ell(k)$ are both zero.*

Remark. The condition of Theorem 1 in [2] means $xyz = 0$ which is a special case of $xyz \neq -1$.

3. *Proof.* Let p, q, x, y, z be as in Theorem 2.2 and put

$$\sigma = \left(\frac{k_p/\boldsymbol{Q}}{\ell}\right),\ \tau = \left(\frac{k_q/\boldsymbol{Q}}{p}\right),\ \eta = \left(\frac{\boldsymbol{Q}_1/\boldsymbol{Q}}{q}\right).$$

The condition in Theorem 2.2 means that $G(k_p/\boldsymbol{Q}) = \langle\sigma\rangle$, $G(k_q/\boldsymbol{Q}) = \langle\tau\rangle$, $G(\boldsymbol{Q}_1/\boldsymbol{Q}) = \langle\eta\rangle$ and

$$\left(\frac{k_p/\boldsymbol{Q}}{q}\right) = \sigma^{-x},\ \left(\frac{k_q/\boldsymbol{Q}}{\ell}\right) = \tau^{-y},\ \left(\frac{\boldsymbol{Q}_1/\boldsymbol{Q}}{p}\right) = \eta^{-z}.$$

We identify $G(k_p/\boldsymbol{Q})$ with $G(k_pk_q/k_q)$ and $G(k_q/\boldsymbol{Q})$ with $G(k_pk_q/k_p)$. We consider σ and τ as elements of $G(k_pk_q/\boldsymbol{Q})$. Let k be a subfield of k_pk_q of degree ℓ which is different from k_p and k_q. Then $G(k_pk_q/k) = \langle\sigma\tau^i\rangle$ for some $i \in \boldsymbol{F}_\ell^\times$. We have $|A(k)| = \ell$ from Lemma 2.1. Since $B(k) = \langle \mathrm{cl}(\mathfrak{p}_p), \mathrm{cl}(\mathfrak{p}_q)\rangle$ and $|B(k)| = \ell$, there exists a non-trivial relation between $\mathrm{cl}(\mathfrak{p}_p)$ and $\mathrm{cl}(\mathfrak{p}_q)$. We can find this relation using Corollary 1.2. Namely, since

$$\left(\frac{k_pk_q/k}{\mathfrak{p}_p}\right)\Big|_{k_q} = \left(\frac{k_q/\boldsymbol{Q}}{p}\right) = \tau,$$

$$\left(\frac{k_pk_q/k}{\mathfrak{p}_q}\right)\Big|_{k_p} = \left(\frac{k_p/\boldsymbol{Q}}{q}\right) = \sigma^{-x},$$

we have

$$\left(\frac{k_pk_q/k}{\mathfrak{p}_p}\right) = \sigma^{i^{-1}}\tau,\quad \left(\frac{k_pk_q/k}{\mathfrak{p}_q}\right) = \sigma^{-x}\tau^{-xi}$$

and hence we can conclude that $\mathfrak{p}_p^{xi}\mathfrak{p}_q$ is principal in k.

Our goal is to show that both $\mathfrak{p}_p$ and $\mathfrak{p}_q$ become principal in $k\boldsymbol{Q}_1$. For that purpose, we look for another relations between $\mathrm{cl}(\mathfrak{p}_p)$ and $\mathrm{cl}(\mathfrak{p}_q)$ in $k\boldsymbol{Q}_1$ using subfields of $K = k_pk_q\boldsymbol{Q}_1$. In this case, we identify $G(k_p/\boldsymbol{Q})$ with $G(K/k_q\boldsymbol{Q}_1)$, $G(k_q/\boldsymbol{Q})$ with $G(K/k_p\boldsymbol{Q}_1)$ and $G(\boldsymbol{Q}_1/\boldsymbol{Q})$ with $G(K/k_pk_q)$ canonically. We consider σ, τ and η as elements of $G(K/\boldsymbol{Q})$ and identify $G(K/\boldsymbol{Q})$ with $\boldsymbol{F}_\ell^3$ by the correspondence

$$\sigma \leftrightarrow \begin{pmatrix}1\\0\\0\end{pmatrix},\ \tau \leftrightarrow \begin{pmatrix}0\\1\\0\end{pmatrix},\ \eta \leftrightarrow \begin{pmatrix}0\\0\\1\end{pmatrix}.$$

In this situation, the above k corresponds to $\langle\sigma\tau^i, \eta\rangle$. Let F be a subfield of $k\boldsymbol{Q}_1$ of degree ℓ in which three primes p, q and ℓ are ramified. Such F corresponds to $\langle\sigma\tau^i, \sigma\eta^t\rangle$ for some $t \in \boldsymbol{F}_\ell^\times$. Let $\mathfrak{P}_p$, $\mathfrak{P}_q$ and $\mathfrak{P}_\ell$ be the prime ideals of F lying over p, q and ℓ respectively. Since $\mathfrak{P}_p = \mathfrak{p}_p$ and $\mathfrak{P}_q = \mathfrak{p}_q$ in $k\boldsymbol{Q}_1$, a relation between $\mathfrak{P}_p$, $\mathfrak{P}_q$ and $\mathfrak{P}_\ell$ in F shifts to the same relation between $\mathfrak{p}_p$, $\mathfrak{p}_q$ and $\mathfrak{P}_\ell$ in $k\boldsymbol{Q}_1$. Note that K is the genus field of $F/\boldsymbol{Q}$ because K/F is an unramified (ℓ, ℓ)-extension and $|B(F)| = \ell^2$. We start from the matrix with entries in $\boldsymbol{F}_\ell$

$$M = \begin{pmatrix} * & -x & 1\\ 1 & * & -y\\ -z & 1 & * \end{pmatrix}$$

and put

$$M(i, t) = \begin{pmatrix} i^{-1} - zt^{-1} & -x & 1\\ 1 & -(x + t^{-1})i & -y\\ -z & 1 & (1 + yi^{-1})t \end{pmatrix}.$$

Columns of $M(i, t)$ correspond to $\left(\frac{K/F}{\mathfrak{P}_p}\right)$, $\left(\frac{K/F}{\mathfrak{P}_q}\right)$ and $\left(\frac{K/F}{\mathfrak{P}_\ell}\right)$. To describe relations between $\mathfrak{P}_p$, $\mathfrak{P}_q$ and $\mathfrak{P}_\ell$, we construct matrices $N(i)$, $\tilde{N}(i)$ below using Lemma 1.1 and Corollary 1.2. Namely, we choose a non-zero column vector $\boldsymbol{a}_t \in \boldsymbol{F}_\ell^3$ such that $M(i, t)\boldsymbol{a}_t = 0$ if $\mathrm{rank}\, M(i, t) = 2$ and put $\boldsymbol{a}_t = 0$ if $\mathrm{rank}\, M(i, t) \neq 2$ and put

$$N(i) = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \cdots\ \boldsymbol{a}_{\ell-1}).$$

This matrix describes relations between $\mathfrak{P}_p$, $\mathfrak{P}_q$

and $\mathfrak{P}_\ell$ in $k\boldsymbol{Q}_1$ because $\varphi \mid B(F)$ is surjective if and only if rank $M(i, t) = 2$. There are, moreover, two more relations between $\mathfrak{P}_p$, $\mathfrak{P}_q$ and $\mathfrak{P}_\ell$ because $\mathfrak{p}_p^{xi}\mathfrak{p}_q$ is principal in k and $\mathfrak{P}_\ell$ becomes principal in $k\boldsymbol{Q}_1$ as the class number of $\boldsymbol{Q}_1$ is prime to ℓ. Adding to $N(i)$ the matrix with two columns as N' describing these relations, we obtain

$$\tilde{N}(i) = (N' \ N(i)), \text{ where } N' = \begin{pmatrix} xi & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then we have

Lemma 3.1. *If* rank $\tilde{N}(i) = 3$, *then* $A(k)$ *capitulates in* $k\boldsymbol{Q}_1$.

Proof of Theorem 2.2. Fix $i \in \boldsymbol{F}_\ell^\times$. First assume that $z = 0$. Then we let $t = i$ and obtain from $M(i, i)$ by fundamental row operations

$$\begin{pmatrix} 1 & 0 & i + xyi + xi^2 \\ 0 & 1 & y + i \\ 0 & 0 & 0 \end{pmatrix}.$$

Hence the rank of $M(i, i)$ is 2 and we get the following submatrix N_1 of $\tilde{N}(i)$:

$$N_1 = \begin{pmatrix} xi & 0 & i + xyi + xi^2 \\ 1 & 0 & y + i \\ 0 & 1 & -1 \end{pmatrix}.$$

Since $\det N_1 = i \neq 0$, we see that $A(k)$ capitulates in $k\boldsymbol{Q}_1$ from Lemma 3.1. Next assume that $z \neq 0$ and let $t = zi$. Then we obtain from $M(i, zi)$ by fundamental row operations

$$\begin{pmatrix} 1 & -xi - xy - z^{-1} & 0 \\ 0 & -x & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Hence we get again, similarly as above, a submatrix N_2 of $\tilde{N}(i)$:

$$N_2 = \begin{pmatrix} xi & 0 & xi + xy + z^{-1} \\ 1 & 0 & 1 \\ 0 & 1 & x \end{pmatrix}.$$

Since $\det N_2 = z^{-1}(xyz + 1) \neq 0$, we see that $A(k)$ capitulates in $k\boldsymbol{Q}_1$. □

To prove Corollary 2.3, we first note that $|A(k_p)| = |A(k_q)| = 1$. Hence, for any subfield k of k_pk_q of degree ℓ, we see that $A(k)$ capitulates in $k\boldsymbol{Q}_1$. If ℓ remains prime in k, then Theorem 1 in [1] immediately yields $\lambda_\ell(k) = \mu_\ell(k) = 0$. So we restrict our attention to the case which ℓ splits in k. In this case, the following lemma, which was given as a remark in [1], is useful.

Lemma 3.2. *Assume that ℓ splits completely in k and there exists a unit $\varepsilon \in k$ such that $\varepsilon^{\ell-1} \not\equiv 1 \pmod{\ell^2}$. Then the capitulation of $A(k)$ in an intermediate field of the cyclotomic $\boldsymbol{Z}_\ell$-extension of k implies the vanishing of $\lambda_\ell(k)$ and $\mu_\ell(k)$.*

Proof of Corollary 2.3. It is enough to show that there exists a unit $\varepsilon \in k$ such that $\varepsilon^{\ell-1} \not\equiv 1 \pmod{\ell^2}$ for k in which ℓ splits. The decomposition group of ℓ for $k_pk_q/\boldsymbol{Q}$ is generated by the Frobenius automorphism $\left(\frac{k_pk_q/\boldsymbol{Q}}{\ell}\right)$ because $k_pk_q \subset \boldsymbol{Q}(\zeta_{pq})$ and its order is ℓ because $\left(\frac{\ell}{p}\right)_\ell \neq 1$. So there exists just one subfield k of k_pk_q of degree ℓ in which ℓ splits completely. Considering the canonical isomorphism

$$(\boldsymbol{Z}/pq\boldsymbol{Z})^\times \ni x \bmod pq \mapsto (x \bmod p,\ x \bmod q) \in (\boldsymbol{Z}/p\boldsymbol{Z})^\times \times (\boldsymbol{Z}/q\boldsymbol{Z})^\times,$$

we see that

$$\left(\frac{k_pk_q/\boldsymbol{Q}}{\ell}\right) = \sigma\tau^{-y}.$$

Hence $G(k_pk_q/k) = \langle \sigma\tau^{-y} \rangle$. First assume that $y \neq 0$. Then, by letting $i = -y$, we see that $\mathfrak{p}_p^{-xy}\mathfrak{p}_q = (\alpha)$ for some $\alpha \in k$ and so $p^{-xy}q = \alpha^\ell\varepsilon$ for some unit ε of k. Since $p^{-xy}q \equiv q^{xyz+1} \pmod{\ell^2}$ and $xyz \neq -1$, we see that ε has desired property. Next assume that $y = 0$. Then $k = k_q$. We can find a unit ε in a similar manner. □

References

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

[2] G. Yamamoto: On the vanishing of Iwasawa invariants of certain (p, p)-extensions of $\boldsymbol{Q}$. Proc. Japan Acad., **73A**, 45–47 (1997).