Takashi Agoh

Stickelberger subideals related to Kummer type congruences

Mathematica Slovaca, Vol. 48 (1998), No. 4, 347--364

Persistent URL: http://dml.cz/dmlcz/129907

Math. Slovaca, **48** (1998), No. 4, 347–364

Mathematica Slovaca
©1998
Mathematical Institute
Slovak Academy of Sciences

Dedicated to Paulo Ribenboim

STICKELBERGER SUBIDEALS RELATED TO KUMMER TYPE CONGRUENCES

Takashi Agoh

(*Communicated by Stanislav Jakubec*)

ABSTRACT. A new type of the Kummer system of congruences is considered and some equivalent systems are discussed by using a polynomial identity. Further we define a special Stickelberger subideal in a certain group ring and transfer the Fueter type system into the group ring. Afterwards, by evaluating the determinant of a special matrix we deduce the index formula between the group ring and the Stickelberger subideal in terms of the relative class number of the lth cyclotomic field (where $l \geq 5$ is an odd prime).

1. Introduction

Let $l \geq 5$ be an odd prime, $\mathbb{Z}$ the ring of integers, $\mathbb{Q}$ the rational number field and $\mathbb{Q}(\zeta)$ the cyclotomic field over $\mathbb{Q}$ defined by a primitive lth root of unity $\zeta = e^{2\pi i/l}$. Further let $\Gamma = \{N_1, N_2, \dots, N_n\}$ be the set of positive integers $N_1, N_2, \dots, N_n$ $(1 \leq n \leq l-2)$ such that $2 \leq N_i \leq l-1$ $(i = 1, 2, \dots, n)$ and $N_i \neq N_j$ if $i \neq j$, B_m the mth Bernoulli number defined by

$$\frac{x}{e^x - 1} = \sum_{m=0}^{\infty} \frac{B_m}{m!} x^m$$

and $\varphi_k(x)$ the Mirimanoff polynomial, i.e.,

$$\varphi_k(x) = \sum_{v=1}^{l-1} v^{k-1} x^v \qquad (k \in \mathbb{Z}).$$

AMS Subject Classification (1991): Primary 11D41, 11R54, 11B68.
Key words: Stickelberger ideal, Kummer system of congruences, class number formula, cyclotomic field, Bernoulli number, Mirimanoff polynomial.

The following system of congruences (in equivalent form) was first introduced by Kummer [K] in connection with the first case of Fermat's last theorem:

$$\begin{aligned} &\varphi_{l-1}(t) \equiv 0 \pmod{l}, \\ &B_{2m}\varphi_{l-2m}(t) \equiv 0 \pmod{l} \qquad (1 \le m \le (l-3)/2). \end{aligned} \tag{K}$$

This system has many interesting variations and consequences (see, e.g., [A_1], [A_2], [G], [R]). In Skula's papers [S_1], [S_2] this system was investigated from the viewpoint of the Stickelberger ideal in a certain group ring.

We now consider the following new system of congruences:

$$\begin{aligned} &\varphi_{l-1}(t) \equiv 0 \pmod{l}, \\ &B_{2m}^{(\Gamma)}\varphi_{l-2m}(t) \equiv 0 \pmod{l} \qquad (1 \le m \le (l-3)/2), \end{aligned} \tag{K(Γ)}$$

where

$$B_k^{(\Gamma)} = \prod_{N\in\Gamma}(N^k - 1)\cdot\frac{B_k}{k} \qquad (k \ge 1).$$

The system (K(Γ)) was first observed by Benneton [B] in the case $\Gamma = \{2\}$ (for another approach, see [S_3]), and it was recently investigated for the cases $\#\Gamma = 1$ and 2 in [AS] and [AM], respectively, by means of the Stickelberger subideals.

It is easily seen that if Γ' ($\neq \emptyset$) is any subset of Γ, then the solution τ of (K) or (K(Γ')) is also a solution of (K(Γ)). Further we may state that if all the elements of Γ are primitive roots mod l, then the systems (K), (K(Γ')) and (K(Γ)) are mutually equivalent, in other words, these systems have the solutions in common. In addition, we note that if $i_\Gamma(l) = \#\{m \mid B_{2m}^{(\Gamma)} \equiv 0 \pmod{l},\ 1 \le m \le (l-3)/2\}$, then the number of non-trivial congruences in (K(Γ)) is at most $(l-1)/2 - i_\Gamma(l)$.

The main purpose of this paper is to investigate a Stickelberger subideal relating to the Kummer type system of congruences and deduce the index formula of this subideal in the group ring $\mathbb{Z}[G]$, where G is a cyclic group of order $l-1$.

Section 2 is devoted to deducing various systems of congruences equivalent to (K(Γ)) by using a certain polynomial identity including all the terms in (K(Γ)). In Section 3, a special Stickelberger subideal $\mathcal{B}_\Gamma$ in $\mathbb{Z}[G]$ is introduced and one of systems (the Fueter type system) equivalent to (K(Γ)) is observed by means of this subideal. In Section 4, we define a matrix $\mathbf{K}_\Gamma$ with the entries concerned in the Fueter type system and evaluate its determinant in terms of the relative class number h^- of $\mathbb{Q}(\zeta)$. Using these results, we finally deduce the index formula of the Stickelberger subideal $\mathcal{B}_\Gamma$ in $\mathbb{Z}[G]$. In addition, using the Iwasawa class number formula we calculate some indices between the Stickelberger subideals.

2. Some systems equivalent to $(\mathrm{K}(\Gamma))$

In this section we will exploit various systems of congruences equivalent to $(\mathrm{K}(\Gamma))$ using a certain polynomial identity which includes all the terms in $(\mathrm{K}(\Gamma))$.

For a fixed non-empty set Γ as stated in the Introduction, let $\mathcal{P} = \mathcal{P}(\Gamma)$ be the power set of Γ and put for an element $P \in \mathcal{P}$

$$\mu(P) = \begin{cases} 1 & \text{if } P = \emptyset, \\ \prod_{N \in P} N & \text{otherwise.} \end{cases}$$

Also we define

$$S_m(n; \Gamma) = \sum_{P \in \mathcal{P}} (-1)^{\# \tilde{P}} \mu(P)^{m+1} S_m(n\mu(\tilde{P})) \qquad (m \geq 0, \ n \geq 1),$$

where $\tilde{P} = \Gamma \setminus P$ for each $P \in \mathcal{P}$ and $S_m(k) = 1^m + 2^m + \cdots + k^m$.

We first deduce the following polynomial identity, in which all the terms of the system $(\mathrm{K}(\Gamma))$ are included:

PROPOSITION 2.1. *Let $1 \leq k \leq l-1$ and $m \leq l-3$. Then*

$$\begin{aligned} &\frac{1}{2} \prod_{N \in \Gamma} (N-1) \cdot \big(k\mu(\Gamma)\big)^{l-2-m} \varphi_{l-1}(t) \\ &+ \sum_{j=2}^{l-2-m} \binom{l-2-m}{j-1} \big(k\mu(\Gamma)\big)^{l-1-m-j} \left\{B_j^{(\Gamma)} \varphi_{l-j}(t)\right\} \\ &= \sum_{v=1}^{l-1} S_{l-2-m}(vk\,;\Gamma) v^m t^v . \end{aligned}$$

P r o o f. We set

$$\begin{aligned} B(x) &= \frac{x}{\mathrm{e}^x - 1} \qquad \text{(the generating function of Bernoulli numbers),} \\ W_\Gamma(x) &= \frac{1}{x} \sum_{P \in \mathcal{P}} (-1)^{\# \tilde{P}} B\big(\mu(P)x\big), \\ A_{k,m}(t,x) &= \{B(x)\,\mathrm{e}^x\} \varphi_{m+1}(t\,\mathrm{e}^{kx}) - \varphi_{m+1}(t) B(x). \end{aligned}$$

Here we have the identity

$$A_{k,m}(t,x) = x \sum_{v=1}^{l-1} \left(\sum_{j=0}^{vk} \mathrm{e}^{jx} \right) v^m t^v \qquad (\text{cf., } [\mathrm{A}_1;\ 3.3]).$$

Since $B(x)\,\mathrm{e}^x = x + B(x)$, it follows that

$$\begin{aligned}
&\sum_{P\in\mathcal{P}} (-1)^{\#\tilde{P}} A_{k\mu(\tilde{P}),m}\big(t, \mu(P)x\big) \\
&= \Bigg(\sum_{P\in\mathcal{P}} (-1)^{\#\tilde{P}} B\big(\mu(P)x\big)\,\mathrm{e}^{\mu(P)x}\Bigg)\varphi_{m+1}\big(t\,\mathrm{e}^{k\mu(\Gamma)x}\big) \\
&\qquad\qquad\qquad - \varphi_{m+1}(t) \sum_{P\in\mathcal{P}} (-1)^{\#\tilde{P}} B\big(\mu(P)x\big) \\
&= \Bigg(\sum_{P\in\mathcal{P}} (-1)^{\#\tilde{P}} \big\{\mu(P)x + B\big(\mu(P)x\big)\big\}\Bigg)\varphi_{m+1}\big(t\,\mathrm{e}^{k\mu(\Gamma)x}\big) \\
&\qquad\qquad\qquad - \varphi_{m+1}(t) \sum_{P\in\mathcal{P}} (-1)^{\#\tilde{P}} B\big(\mu(P)x\big) \\
&= x\Bigg(\prod_{N\in\Gamma}(N-1) + W_\Gamma(x)\Bigg)\varphi_{m+1}\big(t\,\mathrm{e}^{k\mu(\Gamma)x}\big) - xW_\Gamma(x)\varphi_{m+1}(t)\,,
\end{aligned}$$

which gives

$$\begin{aligned}
&\Bigg(\prod_{N\in\Gamma}(N-1) + W_\Gamma(x)\Bigg)\varphi_{m+1}\big(t\,\mathrm{e}^{k\mu(\Gamma)x}\big) - W_\Gamma(x)\varphi_{m+1}(t) \\
&= \sum_{P\in\mathcal{P}} (-1)^{\#\tilde{P}} \mu(P) \sum_{v=1}^{l-1} \Bigg(\sum_{j=0}^{vk\mu(\tilde{P})} \mathrm{e}^{j\mu(P)x}\Bigg) v^m t^v\,.
\end{aligned}$$

Since for $n \geq 0$

$$\begin{aligned}
\left[\frac{\mathrm{d}^n}{\mathrm{d}x^n} W_\Gamma(x)\right]_{x=0} &= \frac{1}{n+1}\Bigg(\sum_{P\in\mathcal{P}} (-1)^{\#\tilde{P}} \mu(P)^{n+1}\cdot B_{n+1}\Bigg) = B_{n+1}^{(\Gamma)}\,, \\
\left[\frac{\mathrm{d}^n}{\mathrm{d}x^n}\varphi_{m+1}\big(t\,\mathrm{e}^{k\mu(\Gamma)x}\big)\right]_{x=0} &= \big(k\mu(\Gamma)\big)^n \varphi_{m+n+1}(t)\,,
\end{aligned}$$

we get by making use of Leibniz's theorem for the above functional equality

$$\prod_{N\in\Gamma}(N-1)\cdot(k\mu(\Gamma))^{l-2-m}\varphi_{l-1}(t)$$
$$+\sum_{i=0}^{l-2-m}\binom{l-2-m}{i}(k\mu(\Gamma))^{l-2-m-i}\left\{B_{i+1}^{(\Gamma)}\varphi_{l-1-i}(t)\right\}-B_{l-m-1}^{(\Gamma)}\varphi_{m+1}(t)$$
$$=\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}}\mu(P)\sum_{v=1}^{l-1}\left(\sum_{j=1}^{k\mu(\tilde{P})v}(j\mu(P))^{l-2-m}\right)v^m t^v$$
$$=\sum_{v=1}^{l-1}S_{l-2-m}(vk;\Gamma)v^m t^v\,.$$

Noting that $B_1^{(\Gamma)}=(-1/2)\prod_{N\in\Gamma}(N-1)$, this leads to the indicated relation. □

We shall derive some systems equivalent to (K(Γ)) using Proposition 2.1, which have similar forms to those of the systems in [A_2; Theorem 1] and [AS; Theorem 3.3] presented for the systems (K) and (K(Γ)) with $\Gamma=\{N\}$, respectively.

THEOREM 2.2. *The system* (K(Γ)) *is equivalent to any one of the following systems of congruences:*

$$\sum_{v=1}^{l-1}S_{l-3}(vk;\Gamma)vt^v\equiv 0\pmod{l}\qquad(1\le k\le l-1),\tag{I}$$

$$\sum_{v=1}^{l-1}S_{l-2}(vk;\Gamma)\,t^v\equiv 0\pmod{l}\qquad(1\le k\le l-1),\tag{II}$$

$$\begin{gathered}\varphi_{l-1}(t)\equiv 0\pmod{l},\\ \sum_{v=1}^{l-1}S_{l-2-m}(vk;\Gamma)v^m t^v\equiv 0\pmod{l}\\ (2\le m\le l-3;\ \ k\ \textit{is any fixed integer with}\ 1\le k\le l-1).\end{gathered}\tag{III$_k$}$$

P r o o f . Suppose that τ is a solution of (K(Γ)). Then we see from Proposition 2.1 that τ is a solution of

$$\sum_{v=1}^{l-1}S_{l-2-m}(vk;\Gamma)v^m t^v\equiv 0\pmod{l}\qquad(1\le k\le l-1;\ \ 0\le m\le l-3).$$

This shows that the solution τ of (K(Γ)) satisfies the systems (I), (II) and (III_k). Conversely, if τ is a solution of the above congruence for certain k and

m $(1 \le k \le l-1,\ 0 \le m \le l-3)$, then we know from Proposition 2.1 that τ is a solution of the congruence

$$\frac{1}{2}\prod_{N\in\Gamma}(N-1)\cdot\big(k\mu(\Gamma)\big)^{l-2-m}\varphi_{l-1}(t)$$
$$+\sum_{j=2}^{l-2-m}\binom{l-2-m}{j-1}\big(k\mu(\Gamma)\big)^{l-1-m-j}\left\{B_j^{(\Gamma)}\varphi_{l-j}(t)\right\}\equiv 0 \pmod{l}.$$

For a fixed integer m with $0 \le m \le l-3$, let $\mathbf{D} = [a_{ij}]_{1\le i,\,j\le l-2-m}$ be a square matrix of order $l-2-m$ with the entries $a_{ij} = i^j$. Since $\det \mathbf{D}$ is a determinant of the Vandermonde type, it is easily seen that $\det \mathbf{D} \not\equiv 0 \pmod{l}$. Therefore, we see that if τ is a solution of (I) or (II), then τ is also a solution of $(\mathrm{K}(\Gamma))$. On the other hand, for a fixed integer k with $1 \le k \le l-1$, by taking successively $m = l-3, l-5, \ldots, 2$ in the latter congruence one knows that τ is a solution of $(\mathrm{K}(\Gamma))$. This completes the proof of the theorem. □

Next, we shall discuss the Fueter type system of congruences.

PROPOSITION 2.3. *Suppose that $\tau \equiv 1 \pmod{l}$ is not a solution of $(\mathrm{K}(\Gamma))$ only for the case $\#\Gamma = 1$. Then τ is a solution of the system $(\mathrm{K}(\Gamma))$ if and only if τ is a solution of the system of congruences*

$$\sum_{v=1}^{l-1}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{k\mu(\tilde{P})v}{l}\right]\right)\frac{1}{v}t^v \equiv 0 \pmod{l} \qquad (\mathrm{F}(\Gamma))$$
$$(1 \le k \le l-1),$$

where $[x]$ is the greatest integer $\le x$ for a real number x.

Proof. The case $\#\Gamma = 1$ was treated in [AS; Proposition 3.5]. So assume that $\#\Gamma \ge 2$. Take $m = -1$ in the polynomial identity of Proposition 2.1:

$$\frac{1}{2}\prod_{N\in\Gamma}(N-1)\cdot\big(k\mu(\Gamma)\big)^{l-1}\varphi_{l-1}(t)+\sum_{j=2}^{l-1}\binom{l-1}{j-1}\big(k\mu(\Gamma)\big)^{l-j}\left\{B_j^{(\Gamma)}\varphi_{l-j}(t)\right\}$$
$$=\sum_{v=1}^{l-1}S_{l-1}(vk\,;\Gamma)\frac{1}{v}t^v.$$

Here, by the von Staudt-Clausen theorem $B_{l-1}^{(\Gamma)} \equiv (1/l) \prod_{N\in\Gamma} (N^{l-1}-1) \equiv 0 \pmod{l}$ if $\#\Gamma \geq 2$. On the other hand, by Fermat's theorem we have

$$\begin{aligned} S_{l-1}(vk;\Gamma) &= \sum_{P\in\mathcal{P}} (-1)^{\#\tilde{P}} \mu(P)^l S_{l-1}(k\mu(\tilde{P})v) \\ &\equiv \sum_{P\in\mathcal{P}} (-1)^{\#\tilde{P}} \mu(P) \left(k\mu(\tilde{P})v - \left[\frac{k\mu(\tilde{P})v}{l}\right]\right) \\ &\equiv \sum_{P\in\mathcal{P}} (-1)^{\#\tilde{P}-1} \mu(P) \left[\frac{k\mu(\tilde{P})v}{l}\right] \pmod{l}, \end{aligned}$$

which implies the result by the same argument as in the proof of Theorem 2.2. □

We note that the following original form of the system $(\mathrm{F}(\Gamma))$ was first considered by Fueter [F] in 1922:

$$\sum_{v=1}^{l-1} \left[\frac{kv}{l}\right] \frac{1}{v} t^v \equiv 0 \pmod{l} \qquad (1 \leq k \leq l-1). \tag{F}$$

We can say that the solution τ of the Kummer system (K) is also a solution of (F), hence of $(\mathrm{F}(\Gamma))$. In [S_2] the equivalent system to (F) was investigated by means of the Stickelberger ideal. Similarly, we shall discuss the generalized system $(\mathrm{F}(\Gamma))$ for $\#\Gamma \geq 1$ from the viewpoint of the Stickelberger subideal in the next section.

3. A special ideal $\mathcal{B}_\Gamma$ and the system $(\mathrm{F}(\Gamma))$

In this section we shall define a special element β_Γ depending on Γ and study some basic properties of β_Γ. Further, using this element β_Γ we define an ideal $\mathcal{B}_\Gamma$ of the group ring $R = \mathbb{Z}[G]$, which is involved in the Stickelberger ideal $\mathcal{I}$ for the lth cyclotomic field $\mathbb{Q}(\zeta_l)$. Subsequently, we shall observe the equivalent system to $(\mathrm{F}(\Gamma))$ in Proposition 2.3 by means of the Stickelberger subideal $\mathcal{B}_\Gamma$ of $\mathcal{I}$.

Let r be a primitive root mod l, r_i the least positive residue of r^i modulo l, $G = \{1, s, s^2, \ldots, s^{l-2}\}$ a multiplicative cyclic group of order $l-1$ generated by s and $R = \mathbb{Z}[G] = \left\{\alpha = \sum_{i=0}^{l-2} a_i s^i \mid a_i \in \mathbb{Z}\right\}$ the group ring of G over $\mathbb{Z}$.

We now offer the following special elements of R, which are concerned in a basis of the Stickelberger ideal $\mathcal{I}$ defined below:

$$\gamma = \sum_{i=0}^{l-2} r_{-i} s^i, \qquad \gamma_k = \sum_{i=0}^{l-2} \left[\frac{r_k r_{-i}}{l}\right] s^i \quad (k \in \mathbb{Z}), \qquad \delta = \sum_{i=0}^{l-2} s^i.$$

Let $R' = \{\alpha \in R \mid (1+s^{(l-1)/2})\alpha \in \delta\mathbb{Z}\}$ be a subring of R. For an element $\alpha = \sum_{i=0}^{l-2} a_i s^i$ of R', the equality $a_j + a_{j+(l-1)/2} = a_k + a_{k+(l-1)/2}$ $(0 \le j, k \le (l-3)/2)$ always holds. Here we may state that one of bases of R' regarded as a $\mathbb{Z}$-module is given by

$$S' = \{\varepsilon_j \mid 0 \le j \le (l-3)/2\} \cup \{\varepsilon\} \qquad \text{(cf., [S}_2\text{])},$$

where

$$\varepsilon_j = s^j(1 - s^{(l-1)/2}) \quad (j \in \mathbb{Z}) \qquad \text{and} \qquad \varepsilon = \sum_{i=0}^{(l-3)/2} s^i .$$

The Stickelberger ideal $\mathcal{I}$ of R is defined by $\mathcal{I} = R \cap (\gamma/l)R$ with the Stickelberger element γ/l in the group ring $\mathbb{Q}[G]$ over $\mathbb{Q}$ (see [W; §6.2]). Therefore, for an element $\alpha \in \mathcal{I}$ there exists $\nu \in R$ satisfying $l\alpha = \nu\gamma$. It is easily seen that $\mathcal{I} \subseteq R'$ and the above elements γ, γ_k, δ belong to the ideal $\mathcal{I}$. Further we may assert that these elements satisfy the relation

$$\gamma_k + \gamma_{k+(l-1)/2} = \gamma - \delta \qquad (k \in \mathbb{Z}).$$

Noticing that $\gamma = \gamma_{(l-1)/2} + \delta$, we present a basis of $\mathcal{I}$ given by Skula [S_2; Theorem 2.7].

THEOREM 3.1. *The system $\{\gamma_k \mid 1 \le k \le (l-1)/2\} \cup \{\delta\}$ forms a basis of the Stickelberger ideal $\mathcal{I}$ considered as a $\mathbb{Z}$-module.*

Referring to the form of the system $(\mathrm{F}(\Gamma))$ we define the following special element β_Γ of R depending on a non-empty set Γ:

$$\beta_\Gamma = \sum_{i=0}^{l-2} \left(\sum_{P \in \mathcal{P}} (-1)^{\#\tilde{P}-1} \mu(P) \left[\frac{\mu(\tilde{P}) r_{-i}}{l} \right] \right) s^i .$$

We will show that the element β_Γ belongs to $\mathcal{I}$. Without loss of generality, assume that $\tilde{P} = \{N_1, N_2, \dots, N_k\}$ $(\neq \emptyset)$ and $N_j = r_{m_j}$ $(j = 1, 2, \dots, k)$ for a given primitive root r mod l. Then, letting $m = m(\tilde{P}) = m_1 + m_2 + \dots + m_k$ we have

$$\mu(\tilde{P}) r_{-i} = \left[\frac{\mu(\tilde{P}) r_{-i}}{l} \right] l + r_{m-i}, \qquad r_m r_{-i} = \left[\frac{r_m r_{-i}}{l} \right] l + r_{m-i} .$$

Noting that $\mu(\tilde{P}) \equiv r_m \pmod{l}$ and $1 \le r_m \le l-1$, these relations offer

$$\begin{aligned} \left[\frac{\mu(\tilde{P}) r_{-i}}{l} \right] &= \frac{(\mu(\tilde{P}) - r_m) r_{-i}}{l} + \left[\frac{r_m r_{-i}}{l} \right] \\ &= \left[\frac{\mu(\tilde{P})}{l} \right] r_{-i} + \left[\frac{r_m r_{-i}}{l} \right] \qquad (0 \le i \le l-2), \end{aligned}$$

which is also valid for the case $\tilde{P}=\emptyset$ (i.e., $\mu(\tilde{P})=1$). Therefore, it follows that

$$\begin{aligned}\beta_\Gamma &= \sum_{i=0}^{l-2}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left(\left[\frac{\mu(\tilde{P})}{l}\right]r_{-i}+\left[\frac{r_m r_{-i}}{l}\right]\right)\right)s^i\\ &= \left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})}{l}\right]\right)\gamma+\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\gamma_m\,.\end{aligned}$$

If m' is the non-negative least residue of m modulo $(l-1)/2$, then $\gamma_m = \gamma_{(l-1)/2}-\gamma_{m'}$, hence taking consideration of Theorem 3.1 we see $\beta_\Gamma\in\mathcal{I}$.

For the element $\beta_\Gamma\in\mathcal{I}$ we obtain:

PROPOSITION 3.2. *Let j be an integer. Then*

$$s^j\beta_\Gamma=\sum_{i=0}^{l-2}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})r_{-i+j}}{l}\right]\right)s^i$$

and

$$s^j\beta_\Gamma+s^{j+(l-1)/2}\beta_\Gamma=\prod_{N\in\Gamma}(N-1)\cdot\delta\,.$$

Proof. The expression of $s^j\beta$ can be easily deduced. Since for a positive integer a prime to l

$$\left[\frac{ar_{-i+j+(l-1)/2}}{l}\right]=\left[\frac{a(l-r_{-i+j})}{l}\right]=a-1-\left[\frac{ar_{-i+j}}{l}\right],$$

we deduce

$$\begin{aligned}&s^{j+(l-1)/2}\beta_\Gamma\\ &=\sum_{i=0}^{l-2}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})r_{-i+j+(l-1)/2}}{l}\right]\right)s^i\\ &=-\sum_{i=0}^{l-2}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)+\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})r_{-i+j}}{l}\right]\right)s^i\\ &=\prod_{N\in\Gamma}(N-1)\cdot\delta-s^j\beta_\Gamma\,,\end{aligned}$$

which proves the result. □

DEFINITION 3.3. We denote by $\mathcal{B}_\Gamma$ the ideal of R generated by the elements β_Γ and δ, thus

$$\mathcal{B}_\Gamma=\{\eta\beta_\Gamma+a\,\delta \mid \eta\in R,\ a\in\mathbb{Z}\}\subseteq\mathcal{I}.$$

By Theorem 3.1 we know that the elements of $\{s^j\beta_\Gamma \mid 0 \le j \le (l-3)/2\} \cup \{\delta\}$ are generators of the $\mathbb{Z}$-module $\mathcal{B}_\Gamma$.

Here we shall derive a certain system equivalent to (F(Γ)) in Proposition 2.3 by means of the elements $\alpha \in \mathcal{B}_\Gamma$. For this purpose we define the following polynomial $f_\alpha(t)$ $(\alpha \in R)$ introduced by Skula [S$_1$; 1.3]:

DEFINITION 3.4. For an element $\alpha = \sum_{i=0}^{l-2} a_i s^i$ of R, define the polynomial $f_\alpha(t)$ as follows:

$$f_\alpha(t) = \sum_{v=1}^{l-1} a_{-\operatorname{ind} v} \frac{1}{v} t^v ,$$

where $\operatorname{ind} v$ means the index of $v \in \mathbb{Z}$, $l \nmid v$, relating to the primitive root $r \bmod l$ and a_k $(k \in \mathbb{Z})$ may be replaced by a_i $(0 \le i \le l-2)$ whenever $k \equiv i \pmod{l-1}$.

Using the above polynomial we can state:

THEOREM 3.5. *The system* (F(Γ)) *of* Proposition 2.3 *is equivalent to the system*

$$f_\alpha(t) \equiv 0 \pmod{l} \qquad (\alpha \in \mathcal{B}_\Gamma).$$

Proof. Let k and u be integers satisfying $r_u = k$ $(1 \le k \le l-1,$ $0 \le u \le l-2)$. Based on Proposition 3.2 we let

$$\alpha = s^u \beta_\Gamma = \sum_{i=0}^{l-2} \left(\sum_{P \in \mathcal{P}} (-1)^{\#\tilde{P}-1} \mu(P) \left[\frac{\mu(\tilde{P}) r_{-i+u}}{l} \right] \right) s^i \in \mathcal{B}_\Gamma .$$

Then it follows that

$$\begin{aligned} f_\alpha(t) &= \sum_{v=1}^{l-1} \left(\sum_{P \in \mathcal{P}} (-1)^{\#\tilde{P}-1} \mu(P) \left[\frac{\mu(\tilde{P}) r_{\operatorname{ind} v + u}}{l} \right] \right) \frac{1}{v} t^v \\ &= \sum_{v=1}^{l-1} \left(\sum_{P \in \mathcal{P}} (-1)^{\#\tilde{P}-1} \mu(P) \left[\frac{\mu(\tilde{P}) \overline{vk}}{l} \right] \right) \frac{1}{v} t^v \\ &= \sum_{v=1}^{l-1} \left(\sum_{P \in \mathcal{P}} (-1)^{\#\tilde{P}-1} \mu(P) \left(\left[\frac{\mu(\tilde{P}) vk}{l} \right] - \mu(\tilde{P}) \left[\frac{vk}{l} \right] \right) \right) \frac{1}{v} t^v \\ &= \sum_{v=1}^{l-1} \left(\sum_{P \in \mathcal{P}} (-1)^{\#\tilde{P}-1} \mu(P) \left[\frac{k \mu(\tilde{P}) v}{l} \right] \right) \frac{1}{v} t^v , \end{aligned}$$

where $\overline{n}$ means the least non-negative residue of $n \ge 1$ modulo l. On the other hand, since $[a(l-1)/l] = a - 1 - [a/l]$ for a positive integer a prime to l, one can state

$$\begin{aligned}
&\sum_{v=1}^{l-1}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})v}{l}\right]\right)\frac{1}{v}t^{v}\\
&\qquad+\sum_{v=1}^{l-1}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})(l-1)v}{l}\right]\right)\frac{1}{v}t^{v}\\
&=\sum_{v=1}^{l-1}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}(\mu(\Gamma)v-\mu(P))\right)\frac{1}{v}t^{v}\\
&\equiv\prod_{N\in\Gamma}(N-1)\cdot f_{\delta}(t)\pmod{l},
\end{aligned}$$

where $\prod_{N\in\Gamma}(N-1)\not\equiv 0 \pmod{l}$. So the theorem follows. □

4. The index of the Stickelberger subideal $\mathcal{B}_\Gamma$

In this section we define a special matrix $\mathbf{K}_\Gamma$ and evaluate its determinant in terms of the relative class number h^- of $\mathbb{Q}(\zeta_l)$. Subsequently, using this evaluation we derive the index formula of the Stickelberger subideal $\mathcal{B}_\Gamma$ of $\mathcal{I}$ in the group ring R'.

For an element $\xi=\sum_{i=0}^{l-2}c_i s^i$ of the group ring $\mathbb{Q}[G]$ of G over $\mathbb{Q}$, there exist uniquely rational numbers c_{hk} $(0\le h,k\le (l-3)/2)$ such that

$$\varepsilon_h\xi=\sum_{k=0}^{(l-3)/2}c_{hk}\varepsilon_k \qquad (h=0,1,\ldots,(l-3)/2).$$

Now, consider the following square matrix $\mathbf{C}(\xi)$ of order $(l-1)/2$:

$$\mathbf{C}(\xi)=[c_{hk}]_{0\le h,\,k\le (l-3)/2}.$$

Sinnott's Lemma stated in [S; Lemma 1.2(b)] can be formulated as follows:

Lemma 4.1. *Let X^- be the set of all odd characters of G. For an element $\xi=\sum_{i=0}^{l-2}c_i s^i\in\mathbb{Q}[G]$ $(c_i\in\mathbb{Q})$*

$$\det\mathbf{C}(\xi)=\prod_{\chi\in X^-}\sum_{i=0}^{l-2}c_i\chi(s)^i.$$

Denoting by f the order of $N \mod l$ we put

$$\omega(N) = \begin{cases} (N^{f/2}+1)^{(l-1)/f} & \text{if } f \text{ is even,} \\ (N^f-1)^{(l-1)/(2f)} & \text{if } f \text{ is odd.} \end{cases}$$

Using this notation we further define $\Omega(\Gamma)$ by

$$\Omega(\Gamma) = \prod_{N\in\Gamma} \omega(N).$$

By making use of Lemma 4.1 we shall calculate $\det \mathbf{C}(\xi)$ for $\xi = \beta_\Gamma$ and prove:

PROPOSITION 4.2. *Let h^- be the relative class number of $\mathbb{Q}(\zeta_l)$. Then*

$$\det \mathbf{C}(\beta_\Gamma) = (-1)^{(l-1)/2} 2^{(l-3)/2} \frac{\Omega(\Gamma)}{l} h^-.$$

Proof. We shall essentially follow the same proof as in [AS; Proposition 5.5] given for the case $\#\Gamma = 1$. It is well-known that h^- can be expressed as

$$h^- = 2l \prod_{\chi\in X^-} \left(-\tfrac{1}{2}B_{1,\chi}\right) \qquad \text{(see, e.g., [W])},$$

where $B_{1,\chi}$ is the generalized first Bernoulli number for an odd character χ of G, i.e., $B_{1,\chi} = (1/l)\sum_{a=1}^{l-1}\chi(a)a$. Also, we easily see that for each $N \in \Gamma$

$$\sum_{a=1}^{l-1}\left\langle\frac{Na}{l}\right\rangle\overline{\chi}(a) = \frac{\chi(N)}{l}\sum_{a=1}^{l-1} a\overline{\chi}(a), \qquad \prod_{\chi\in X^-}(N-\chi(N)) = \omega(N),$$

where $\overline{\chi}$ is the conjugate character of χ and $\langle\theta\rangle$ is the fractional part of θ for a real number θ, so $\langle\theta\rangle = \theta - [\theta]$. Using these relations we obtain from Lemma 4.1

$$\begin{aligned}
\det \mathbf{C}(\beta_\Gamma) &= \prod_{\chi\in X^-}\sum_{i=0}^{l-2}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})r_{-i}}{l}\right]\right)\chi(s)^i \\
&= \prod_{\chi\in X^-}\sum_{a=1}^{l-1}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})a}{l}\right]\right)\overline{\chi}(a) \\
&= \prod_{\chi\in X^-}\sum_{a=1}^{l-1}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left(\frac{\mu(\tilde{P})a}{l} - \left\langle\frac{\mu(\tilde{P})a}{l}\right\rangle\right)\right)\overline{\chi}(a) \\
&= \prod_{\chi\in X^-}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\big(\mu(\tilde{P}) - \chi(\mu(\tilde{P}))\big)\cdot\frac{1}{l}\sum_{a=1}^{l-1}a\overline{\chi}(a)\right)
\end{aligned}$$

$$= \prod_{\chi \in X^-} \left(\sum_{P \in \mathcal{P}} (-1)^{\#\tilde{P}} \mu(P) \chi(\mu(\tilde{P})) \cdot \frac{1}{l} \sum_{a=1}^{l-1} a\overline{\chi}(a) \right)$$
$$= \prod_{\chi \in X^-} \prod_{N \in \Gamma} (N - \chi(N)) \cdot \prod_{\chi \in X^-} \left(\frac{1}{l} \sum_{a=1}^{l-1} a\chi(a) \right)$$
$$= (-2)^{(l-1)/2} \Omega(\Gamma) \cdot \prod_{\chi \in X^-} \left(-\frac{1}{2} B_{1,\chi} \right)$$
$$= (-1)^{(l-1)/2} 2^{(l-3)/2} \frac{\Omega(\Gamma)}{l} h^- ,$$

as indicated. This completes the proof. □

We consider the square matrix $\mathbf{K}_\Gamma$ of order $(l-1)/2$ as follows:

Definition 4.3. For a non-empty set Γ, define the square matrix of order $(l-1)/2$ as follows:

$$\mathbf{K}_\Gamma = [k_{ij}]_{1 \le i,\, j \le (l-1)/2} ,$$

where

$$k_{ij} = \sum_{P \in \mathcal{P}} (-1)^{\#\tilde{P}-1} \mu(P) \left[\frac{\overline{ij}\mu(\tilde{P})}{l} \right] - \frac{1}{2} \prod_{N \in \Gamma} (N - 1) .$$

The matrix $\mathbf{K}_\Gamma$ for the case $\#\Gamma = 1$ was considered in [AS] and its determinant was calculated in terms of the relative class number h^- of $\mathbb{Q}(\zeta_l)$. We would like to extend this result to more general situation for the case $\#\Gamma \ge 1$.

To decide the sign of $\det \mathbf{K}_\Gamma$ we need the following proposition [AS; Proposition 4.5]:

Proposition 4.4. *Let a_{uv} be complex numbers satisfying $a_{u+(l-1)/2,v} = a_{u,v+(l-1)/2} = -a_{uv}$ for all integers u, v. If $\mathbf{A}$ and $\mathbf{K}$ are the matrices defined by $\mathbf{A} = [a_{uv}]_{0 \le u,\, v \le (l-3)/2}$ and $\mathbf{K} = [k_{ij}]_{1 \le i,\, j \le (l-1)/2}$ with $k_{ij} = a_{\operatorname{ind} i, -\operatorname{ind} j}$, then*

$$\det \mathbf{K} = (-1)^{(l-1)(l-3)/8} \det \mathbf{A} .$$

Note that the above proposition is also applicable to the transposed matrices $\mathbf{A}^{\mathrm{T}}$ and $\mathbf{K}^{\mathrm{T}}$.

Now we can evaluate $\det \mathbf{K}_\Gamma$ and give the following formula:

Theorem 4.5.

$$\det \mathbf{K}_\Gamma = (-1)^{(l^2-1)/8} \frac{\Omega(\Gamma)}{2l} h^- .$$

Proof. For integers u, v put

$$a_{uv} = \sum_{P \in \mathcal{P}} (-1)^{\#\tilde{P}-1} \mu(P) \left[\frac{\mu(\tilde{P}) r_{-u+v}}{l} \right] - \frac{1}{2} \prod_{N \in \Gamma} (N - 1)$$

and consider the square matrix of order $(l-1)/2$:

$$\mathbf{A}_\Gamma = [a_{uv}]_{0\le u,\, v\le (l-3)/2}\,.$$

We first want to show that a_{uv} satisfies the condition of Proposition 4.4, that is, $a_{u+(l-1)/2,v} = a_{u,v+(l-1)/2} = -a_{uv}$. For brevity set $\Pi_\Gamma = \prod_{N\in\Gamma}(N-1)$. By direct calculation one has

$$\begin{aligned}
a_{u+(l-1)/2,v} &= a_{u,v+(l-1)/2}\\
&= \sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})r_{-u+v+(l-1)/2}}{l}\right] - \frac{1}{2}\Pi_\Gamma\\
&= \sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})(l-r_{-u+v})}{l}\right] - \frac{1}{2}\Pi_\Gamma\\
&= \sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left(\mu(\tilde{P})-1-\left[\frac{\mu(\tilde{P})r_{-u+v}}{l}\right]\right) - \frac{1}{2}\Pi_\Gamma\\
&= \Pi_\Gamma - \sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})r_{-u+v}}{l}\right] - \frac{1}{2}\Pi_\Gamma\\
&= -a_{uv}\,,
\end{aligned}$$

as desired. Noting that $r_{-k-(l-1)/2+h} = l - r_{-k+h}$ $(0\le k,h\le (l-3)/2)$, we can deduce from Proposition 3.2

$$\begin{aligned}
\varepsilon_h\beta_\Gamma &= \left(s^h - s^{h+(l-1)/2}\right)\beta_\Gamma = 2s^h\beta_\Gamma - \Pi_\Gamma\delta\\
&= 2\sum_{k=0}^{(l-3)/2}\left\{\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left(\left[\frac{\mu(\tilde{P})r_{-k+h}}{l}\right]s^k\right.\right.\\
&\qquad\left.\left. + \left[\frac{\mu(\tilde{P})r_{-k-(l-1)/2+h}}{l}\right]s^{k+(l-1)/2}\right)\right\} - \Pi_\Gamma\delta\\
&= 2\sum_{k=0}^{(l-3)/2}\left\{\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left(\left[\frac{\mu(\tilde{P})r_{-k+h}}{l}\right]s^k\right.\right.\\
&\qquad\left.\left. + \left(\mu(\tilde{P})-1\right)s^{k+(l-1)/2} - \left[\frac{\mu(\tilde{P})r_{-k+h}}{l}\right]s^{k+(l-1)/2}\right)\right\}\\
&\qquad - \Pi_\Gamma\cdot\left(1+s^{(l-1)/2}\right)\varepsilon
\end{aligned}$$

$$
\begin{aligned}
&= 2\sum_{k=0}^{(l-3)/2}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})r_{-k+h}}{l}\right]\varepsilon_k + \Pi_\Gamma\cdot s^{k+(l-1)/2}\right)\\
&\qquad\qquad - \Pi_\Gamma\cdot\left(1+s^{(l-1)/2}\right)\varepsilon\\
&= 2\sum_{k=0}^{(l-3)/2}\left(\sum_{P\in\mathcal{P}}(-1)^{\#\tilde{P}-1}\mu(P)\left[\frac{\mu(\tilde{P})r_{-k+h}}{l}\right]\right)\varepsilon_k - \Pi_\Gamma\cdot\left(1-s^{(l-1)/2}\right)\varepsilon\\
&= 2\sum_{k=0}^{(l-3)/2} a_{kh}\varepsilon_k\,.
\end{aligned}
$$

Since the entries k_{ij} $(1\le i,j\le (l-1)/2)$ of the matrix $\mathbf{K}_\Gamma$ satisfy the identity $k_{ij} = a_{-\operatorname{ind} j,\operatorname{ind} i}$, we get from Propositions 4.2 and 4.4

$$
\begin{aligned}
\det\mathbf{K}_\Gamma &= (-1)^{(l-1)(l-3)/8}\det\mathbf{A}_\Gamma^{\mathrm{T}}\\
&= (-1)^{(l-1)(l-3)/8+(l-1)/2}\frac{\Omega(\Gamma)}{2l}h^-\\
&= (-1)^{(l^2-1)/8}\frac{\Omega(\Gamma)}{2l}h^-\,,
\end{aligned}
$$

which completes the proof of the theorem. □

We should supplement here that Hazama [H] introduced the $(0,1)$ square matrix $\mathbf{H} = [h_{ij}]_{1\le i,j\le (l-1)/2}$ of order $(l-1)/2$ defined by $h_{ij}=0$ if $\overline{ij} > l/2$ and $h_{ij}=1$ if $\overline{ij} < l/2$, and he evaluated its determinant as follows:

$$
\det\mathbf{H} = (-1)^{[(l-1)/4]}\frac{\omega(2)}{l}h^-\,.
$$

The adjustment between the formulas of $\det\mathbf{H}$ and $\det\mathbf{K}_\Gamma$ for $\Gamma=\{2\}$ has been accurately mentioned in [AS; Proposition 4.3].

The following proposition was proved in [AS; Proposition 5.6]:

PROPOSITION 4.6. *Let S' be the basis of R' stated in* Section 3 *and $\xi\in R'$. If $\mathbf{C}$ is the transition matrix from S' to the elements $s^j\xi$ $(0\le j\le (l-3)/2)$ and δ, then*

$$
\det\mathbf{C} = 2^{-(l-3)/2}\det\mathbf{C}(\xi)\,.
$$

Applying Propositions 4.2 and 4.6 we obtain:

THEOREM 4.7.
(i) *If* $\mathbf{C}_\Gamma$ *is the transition matrix from* S' *to the elements* $s^j\beta_\Gamma$ $(0 \le j \le (l-3)/2)$ *and* δ, *then*

$$\det \mathbf{C}_\Gamma = (-1)^{(l-1)/2}\frac{\Omega(\Gamma)}{l}h^- .$$

(ii) *The system* $\{s^j\beta_\Gamma \mid 0 \le j \le (l-3)/2\} \cup \{\delta\}$ *forms a basis of* $\mathcal{B}_\Gamma$ *regarded as a* $\mathbb{Z}$*-module.*

As a consequence of Theorem 4.7, one can state the following index formula for the Stickelberger subideal $\mathcal{B}_\Gamma$ of $\mathcal{I}$ in R':

THEOREM 4.8.

$$[R' : \mathcal{B}_\Gamma] = \frac{\Omega(\Gamma)}{l}h^- .$$

The next theorem follows from Iwasawa's class number formula ([I]) and it was extended by Sinnott [S] to a wider class of cyclotomic fields (see also [W; §6.4]).

THEOREM 4.9.

$$[R' : \mathcal{I}] = h^- .$$

Using Theorems 4.8 and 4.9 we may state:

COROLLARY 4.10.

$$[\mathcal{I} : \mathcal{B}_\Gamma] = \frac{\Omega(\Gamma)}{l} .$$

Next, we argue inclusion relation between the Stickelberger subideals of the above mentioned type.

PROPOSITION 4.11. *Let* Γ' *be a non-empty subset of* Γ. *Then* $\mathcal{B}_{\Gamma'} \supseteq \mathcal{B}_\Gamma$.

Proof. It is enough to prove the proposition only for the case $\Gamma = \Gamma' \cup \{M\}$, where M is a positive integer with $M \notin \Gamma'$ and $2 \le M \le l-1$. Let $\mathcal{P}'$ be the power set of Γ' and put for simplicity

$$X_i = M \sum_{P' \in \mathcal{P}'} (-1)^{\#\tilde{P}'-1}\mu(P')\left[\frac{\mu(\tilde{P}')r_{-i}}{l}\right],$$

$$Y_i = \sum_{P' \in \mathcal{P}'} (-1)^{\#\tilde{P}'-1}\mu(P')\left[\frac{\mu(\tilde{P}')Mr_{-i}}{l}\right].$$

Then we see that $\beta_\Gamma = \sum_{i=0}^{l-2}(X_i - Y_i)s^i$. Here $\sum_{i=0}^{l-2} X_i s^i = M\beta_{\Gamma'} \in \mathcal{B}_{\Gamma'}$. We now show that $\sum_{i=0}^{l-2} Y_i s^i \in \mathcal{B}_{\Gamma'}$. For a fixed primitive root r mod l, let g and m be the integers satisfying $\mu(\tilde{P}') \equiv r_g \pmod{l}$ and $M = r_m$, respectively. Then

$$\mu(\tilde{P}')Mr_{-i} = \left[\frac{\mu(\tilde{P}')Mr_{-i}}{l}\right] l + r_{g+m-i},$$

$$\mu(\tilde{P}')\overline{Mr_{-i}} = \left[\frac{\mu(\tilde{P}')\overline{Mr_{-i}}}{l}\right] l + r_{g+m-i},$$

hence

$$\left[\frac{\mu(\tilde{P}')Mr_{-i}}{l}\right] = \left[\frac{\mu(\tilde{P}')\overline{Mr_{-i}}}{l}\right] + \frac{\mu(\tilde{P}')(Mr_{-i} - \overline{Mr_{-i}})}{l}.$$

Since $\overline{Mr_{-i}} = r_{-i+m}$, we get

$$\begin{aligned} Y_i = & \sum_{P' \in \mathcal{P}'} (-1)^{\#\tilde{P}'-1} \mu(P') \left[\frac{\mu(\tilde{P}')\overline{Mr_{-i}}}{l}\right] \\ & + \frac{\mu(\Gamma)(Mr_{-i} - \overline{Mr_{-i}})}{l} \sum_{P' \in \mathcal{P}'} (-1)^{\#\tilde{P}'-1} \\ = & \sum_{P' \in \mathcal{P}'} (-1)^{\#\tilde{P}'-1} \mu(P') \left[\frac{\mu(\tilde{P}')r_{-i+m}}{l}\right]. \end{aligned}$$

Consequently, by Proposition 3.2 we see $\beta_\Gamma = M\beta_{\Gamma'} - s^m\beta_{\Gamma'} \in \mathcal{B}_{\Gamma'}$, which implies the result. □

Incidentally, we add that if $m(N)$ is the integer with $N = r_{m(N)}$, then for any $N' \in \Gamma$

$$\beta_\Gamma = \gamma_{m(N')} \prod_{N \in \Gamma \setminus \{N'\}} \left(N - s^{m(N)}\right).$$

Based on Proposition 4.11, we obtain from Theorem 4.8:

COROLLARY 4.12. *Let Γ' be as in* Proposition 4.11. *Then*

$$[\mathcal{B}_{\Gamma'} : \mathcal{B}_\Gamma] = \Omega(\Gamma \setminus \Gamma').$$

Acknowledgment

The author thanks Ladislav Skula for his careful reading of the paper and useful comments.

REFERENCES

[A_1] AGOH, T.: *On the Kummer-Mirimanoff congruences*, Acta Arith. **55** (1990), 141–156.

[A_2] AGOH, T.: *Some variations and consequences of the Kummer-Mirimanoff congruences*, Acta Arith. **62** (1992), 73–96.

[AM] AGOH, T.—MORI, K.: *Kummer type system of congruences and bases of Stickelberger subideals*, Arch. Math. (Brno) **32** (1996), 211–232.

[AS] AGOH, T.—SKULA, L.: *Kummer type congruences and Stickelberger subideals*, Acta Arith. **75** (1996), 235–250.

[B] BENNETON, G.: *Sur le dernier théorème de Fermat*, Ann. Sci. Univ. Besançon Math. **3** (1974).

[F] FUETER, R.: *Kummers Kriterium zum letzten Theorem von Fermat*, Math. Ann. **85** (1922), 11–20.

[G] GRANVILLE, A.: *Diophantine Equations with Varying Exponents* (*with Special Reference to Fermat's Last Theorem*). Ph.D. Thesis, Queen's Univ., 1989.

[H] HAZAMA, F.: *Demjanenko matrix, class number, and Hodge group*, J. Number Theory **34** (1990), 174–177.

[I] IWASAWA, K.: *A class number formula for cyclotomic fields*, Ann. of Math. **76** (1962), 171–179.

[K] KUMMER, E. E.: *Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen, für den Fall, daß die Klassenanzahl durch λ teilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, Abhandl. Königl. Akad. Wiss. Berlin (1857), 41–74 [Collected papers, Vol. I, 639–692].

[R] RIBENBOIM, P.: 13 *Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

[S] SINNOTT, W.: *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980), 181–234.

[S_1] SKULA, L.: *A remark on Mirimanoff polynomials*, Comment. Math. Univ. Sancti Pauli (Tokyo) **31** (1982), 89–97.

[S_2] SKULA, L.: *Some bases of the Stickelberger ideal*, Math. Slovaca **43** (1993), 541–571.

[S_3] SKULA, L.: *On a special ideal contained in the Stickelberger ideal*, J. Number Theory **58** (1996), 173–195.

[W] WASHINGTON, L. C.: *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

Received June 20, 1996
Revised September 11, 1996

Department of Mathematics
Science University of Tokyo
Noda, Chiba 278
JAPAN
E-mail: agoh@ma.noda.sut.ac.jp