<table>
<thead>
<tr>
<th>Title</th>
<th>THE STICKELBERGER IDEAL OF THE FIELD OF 2N-TH ROOTS OF UNITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Kobayashi, Midori</td>
</tr>
<tr>
<td>Citation</td>
<td>経営と経済, 61(1), pp.129-136; 1981</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1981-06-25</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10069/28127">http://hdl.handle.net/10069/28127</a></td>
</tr>
</tbody>
</table>

NAOSITE: Nagasaki University's Academic Output SITE
http://naosite.lb.nagasaki-u.ac.jp
THE STICKELBERGER IDEAL OF THE FIELD
OF $2^N$-TH ROOTS OF UNITY

By Midori Kobayashi

§ 1. Introduction

Let $Q$ be the rational number field and $Z$ the rational integer ring. For any rational integer $m > 2$, let $\zeta_m$ be a primitive $m$-th root of unity and $K = Q(\zeta_m)$ the cyclotomic field generated by $\zeta_m$ over $Q$. We denote by $G$ the Galois group of $K$ over $Q$, by $R$ the group ring of $G$ over $Z$, and by $S$ the Stickelberger ideal of $K$. Let $h$ be the class number of $K$ and $h^+$ the class number of the maximal real subfield $K^+$ of $K$. We put $h^- = h/h^+$, then $h^-$ is the so-called first factor of $h$. Iwasawa ([1]) proved the class number formula: $h^- = [R^- : S^-]$ when $m$ is an odd prime power, and Sinnott ([5]) extended this formula for any cyclotomic field. Let $S_k$ be the Stickelberger ideal of $K$, generalizing $S$ for $k = 1$ to arbitrary odd integer $k > 0$. Lang determined the index of $S_k$ of odd prime power level and Kitahara ([2]) worked out the index of $S_k$ in the composite level.

On the other hand, Skula ([6]) has presented a special basis of $S^-$ when $m$ is an odd prime power, and he gives an another proof of Iwasawa's formula by the calculation of the determinant of the transition matrix from a certain basis of $R^-$ to this basis of $S^-$. In this paper, we extend Skula's method to the case when $m$ is a power of 2.

§ 2. Notation and terminology

Let $p$ be a prime number and $n$ a natural number. For $p=2$ let $n>1$. Put $q = p^n$. We let $\zeta_q$ be a primitive $q$-th root of unity, $K = Q(\zeta_q)$ the cyclotomic field generated by $\zeta_q$ over $Q$, and $G$ the
Galois group of $K$ over $Q$. Let $\sigma_t$ denote the element of $G$ such that $\sigma_t(\zeta_q) = \zeta_q^t$ for any integer $t$ prime to $q$, and the mapping $t \mapsto \sigma_t$, for $t$ prime to $m$, induces an isomorphism 

$$(Z/qZ)\times \cong G$$

of the multiplicative group $(Z/qZ)\times$ of rational integers mod $q$ with $G$. We then identify the group $(Z/qZ)\times$ and $G$ through this isomorphism. Let $\chi$ be a character of $G$, i.e. a homomorphism of $G$ into $\mathbb{C}^\times$. $\chi$ is said to be an odd character if $\chi(\sigma_t) = -1$. We denote by $G^*$ the character group of $G$.

$R = \mathbb{Z}[G]$ and $Q[G]$ denote the group ring of $G$ over $\mathbb{Z}$ and $Q$, respectively. We define the element $\theta$ in $Q[G]$:

$$\theta = \frac{1}{q} \sum_{t=1 \atop (t,q)=1}^q \sigma_t^{-1}$$

and put $I = \theta R \cap R$, then $I$ is an ideal of $R$. $I$ is the Stickelbelger ideal in this case. For any ideal $A$ of $R$, we define

$$A^- = \{a \in A; \sigma_a a = -a\}.$$ 

Furthermore we shall use the followings symbols. For any real number $r$, let $<r>$ denote the unique real number $r'$, $0 \leq r' < 1$, such that $r - r'$ is an integer. For any $a \in \mathbb{Z}$, we denote by $[a]$ the unique integer $a'$, $0 \leq a' < q$, such that $a' \equiv a \pmod{q}$. Then $[a]$ is the smallest integer $\geq 0$ in the residue class of $a$ mod $q$.

§ 3. The expressing of $h^-$ as a determinant

Put $q = 2^n$ $(n>2)$ and $K = Q(\zeta_q)$. We identify $G = G(K/Q)$ with $(Z/qZ)\times$ as described in § 2. We have

$$G = (Z/qZ)\times = A \times B \ (\text{direct product}),$$

where $A$ is the cyclic subgroup generated by $-1$ with order 2 and $B$ the cyclic subgroup generated by 5 with order $2^{n-2}$.

As is well-known, the first factor $h^-$ is given by the formula:

$$h^- = q\left(\frac{1}{2}\right)^{2^{n-2}} \prod_{x \text{odd}} \sum_{a=1 \atop (a,q) = 1}^q \chi(a) < \frac{a}{q} >,$$
where \( \chi \) ranges over all odd characters of \( G \) and \( a \) over all integers with \( 1 \leq a < q \), \((a, q) = 1\).

Now we let \( \omega \) be the odd character of \( G \) satisfying \( \omega(B) = 1 \). Then \( \chi = \omega \psi \) ranges over all odd characters of \( G \) when \( \psi \) ranges over all even characters of \( G \), hence we have

\[
h^- = q \left( \frac{1}{2} \right)^{2^{n-2}} \prod_{\psi \text{ even } a = 1}^{\sum_{a \equiv 1}^{q} \omega \psi(a) < \frac{a}{q} >} \]

\[
= q \left( \frac{1}{2} \right)^{2^{n-2}} \prod_{\psi \text{ even } a \in B}^{\sum_{a \equiv 1}^{\omega(a) \psi(a) \left( < \frac{a}{q} > - < \frac{-a}{q} > \right)}}
\]

\[
= q \left( \frac{1}{2} \right)^{2^{n-2}} \prod_{\psi \in B^* a \in B}^{\omega(a) \psi(a) \left( < \frac{a}{q} > - < \frac{-a}{q} > \right)},
\]

where \( B^* \) is the character group of \( B \). From the Dedekind determinant relation (cf. Lang [4], p. 89), we get

\[
h^- = q \left( \frac{1}{2} \right)^{2^{n-2}} \left| \det \left( \omega(ab) \left( < \frac{ab}{q} > - < \frac{-ab}{q} > \right) \right)_{a, b \in B} \right|.
\]

The size of the determinant is \( 2^{n-2} \). Since we have \( \omega(ab) = 1 \)

\[
\left( \frac{ab}{q} > + \frac{-ab}{q} > = 1 \right) \text{ for any } a, b \in B,
\]

\[
h^- = q \left( \frac{1}{2} \right)^{2^{n-2}} \left| \det \left( 2 < \frac{ab}{q} > - 1 \right)_{a, b \in B} \right|
\]

\[
= q \left( \frac{1}{2} \right)^{2^{n-2}} \left( \frac{1}{q} \right)^{2^{n-2}} \left| \det \left( 2 \left[ \frac{ab}{q} \right] - q \right)_{a, b \in B} \right|.
\]
If we subtract row 1 from every other row, we obtain

\[
D = \begin{vmatrix}
q-2 & q-2[b] \\
q-2[a] & q-2[ab] \\
2-2[a] & 2[b] - 2[ab] \\
\end{vmatrix}
= 2^{n-1} - 1
\]

If we subtract \([b]\)-times column 1 from column \(b\) \((b \neq 1)\), we get

\[
D = 2^{n-1} - 1
\]

Therefore we have

\[
h^{-} = \frac{1}{2}
\left|
\begin{array}{c}
q-2 \\
1-[a] \\
\end{array}
\begin{array}{c}
1-b \\\n[a][b] - [ab] \\\n\end{array}
\right|
\]

\[
b
\]

\[
h^{-} = \frac{1}{2}
\left|
\begin{array}{c}
q-2 \\
1-[a] \\
\end{array}
\begin{array}{c}
1-[b] \\\n[a][b] - [ab] / q \\\n\end{array}
\right|
\]

\[
< a
\]

\(a, b \in \mathbb{B}\)
§ 4. The basis of $I^-$

Let $\alpha = \sum_{t=1}^{q} a_t \sigma_t$ be any element of $I^-$. Since $\alpha \in R$, then there exist $x_t \in Z$ such that $a_t = \frac{1}{q} \sum_{k=1}^{q} [kt^{-1}] x_k$, for any $t \in Z$ with $(t, q) = 1$, $1 \leq t < q$, where $t^{-1}$ means the integer $t'$ satisfying $t't \equiv 1 \pmod{q}$, $1 \leq t' < q$. Since $\alpha \in R$, we have $\sum_{k=1}^{q} k x_k \equiv 0 \pmod{q}$, and since $\sigma \cdot \alpha = -\alpha$, it follows $\sum_{k=1}^{q} x_k = 0$. The converse is immediate, thus it holds

$$I^- = \{ \alpha = \sum_{t=1}^{q} a_t \sigma_t; \exists x_t \in Z, a_t = \frac{1}{q} \sum_{k=1}^{q} [kt^{-1}] x_k, \sum_{k=1}^{q} k x_k \equiv 0 \pmod{q}, \sum_{k=1}^{q} x_k = 0 \}.$$ 

For $1 \leq t < q$, $(t, q) = 1$ and $i \in B$, put

$$a_{i, t} = [t^{-1}] - \frac{q}{2}$$

$$a_{i, t} = \frac{1}{q} ([t^{-1}] [i] - [t^{-1} i]) + \frac{1}{2} (1 - [i]), \text{ if } i \neq 1.$$

Further put for $i \in B$

$$\alpha_i = \sum_{t=1}^{q} a_{i, t} \sigma_t$$

$$(i, q) = 1$$
If we put
\[
x_i = \begin{cases} 
  -q/2 & \text{for } t = 1 \\
  -q/2 & \text{for } t = q - 1 \\
  0 & \text{for } t \neq 1, q - 1 
\end{cases}
\]
we get \(\alpha_i \in I^-\). Suppose that \(i \in B, \ i \neq 1\) and put
\[
x_i = \begin{cases} 
  (1 + i)/2 & \text{for } t = 1 \\
  -1 & \text{for } t = i \\
  (1 - i)/2 & \text{for } t = q - 1 \\
  0 & \text{for } t \neq 1, i, q - 1 
\end{cases}
\]
then we see that \(\alpha_i \in I^-\).

Let \(\beta = \sum_{t=1}^{q} b_t \sigma_i \in I^-\). There exist \(x_i \in Z\) such that
\[
b_t = \frac{1}{q} \sum_{t} \left[ t^{-1} \right] x_i, \quad \sum_{i} i x_i \equiv 0 \pmod{q}, \quad \sum_{i} x_i = 0.
\]
For any \(i \in B\), we put \(y_i = x_i - x_{-i}\) and \(c = \sum_{i \in B} (x_i - x_{-i})\), then it holds \(c \equiv 0 \pmod{q}\). By computation we obtain that
\[
\beta = - \sum_{i \in B, i \neq 1} y_i \alpha_i + \frac{c}{q} \alpha_1.
\]
Hence \(\{\alpha_i, i \in B\}\) is a system of generators of the additive group \(I^-\).

Since we have \(R^- = (1 - \sigma_{-i}) R\), we see \(R^-\) is a free abelian group with \(Z\)-basis
\[
\{\sigma_i - \sigma_{-i}, (t, q) = 1, 1 \leq t < \frac{q}{2}, t \in Z\}
\]
of rank \(2^{n-1}\). Therefore the index of \(I^-\) in \(R^-\) is given by
THE STICKELBERGER IDEAL OF THE FIELD OF $2^n$-TH ROOTS OF UNITY

$$(R^- : I^-) = |\det((a_{it}), \ i, \ t \in B)|.$$ 

$$E = |\det(a_{it}), \ i, \ t \in B| = \left| \begin{array}{c} q \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \end{array} \right| < i$$

If we subtract the column 1 from every other column, we have

$$E = \frac{1}{2} \left| \begin{array}{c} q - 2 \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \\ \frac{1}{q} \\ \frac{1}{2} \end{array} \right| < i , \ t \in B$$

Hence we have $h^- = (R^- : I^-)$, and from $h^- \not= 0$, it follows that $\{\alpha_i, \ i \in B\}$ is a basis of $I^-$ over $Z$.

Therefore we obtain the following theorem.
THEOREM. Let $q=2^n$ and $K=\mathbb{Q}(\xi_q)$. The system $\{\alpha_i, \ i \in B\}$ is a basis of the additive group $I^-$ and for the determinant $\Delta$ of the transition matrix from the basis $\{\sigma_t - \sigma_{-t}, \ (t, q) = 1, \ 1 \leq t < \frac{q}{2}, \ t \in \mathbb{Z}\}$ of $R^-$ to the basis $\{\alpha_i, \ i \in B\}$ of $I^-$ there holds $h^- = |\Delta|$. Therefore $h^- = (R^- : I^-)$.

REFERENCES