Radan Kučera

On a certain subideal of the Stickelberger ideal of a cyclotomic field

*Archivum Mathematicum*, Vol. 22 (1986), No. 1, 7--19

Persistent URL: [http://dml.cz/dmlcz/107242](http://dml.cz/dmlcz/107242)

**Terms of use:**

© Masaryk University, 1986

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use.*

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* [http://project.dml.cz](http://project.dml.cz)
ON A CERTAIN SUBIDEAL OF THE STICKELBERGER IDEAL OF A CYCLOTOMIC FIELD

RADAN KUČERA

(Received June 27, 1984)

Abstract. In this paper we compare ideals $S^- = S \cap R^-$ and $I^- = I \cap R^-$, where $S$ means the Stickelberger ideal from Sinnott's paper [4] and $I$ means the Stickelberger ideal from Washington's book [7] for the case of arbitrary cyclotomic field. There is found the basis of $I^-$ (as a $\mathbb{Z}$-module), the group index $[R^- : I^-]$ is determined and it is shown that the ideals $I^-$ and $S^-$ are not identical in a general case.

Key words. Cyclotomic field, Stickelberger ideal, class number.

1. INTRODUCTION

In this paper we shall mean by a cyclotomic field a subfield of the complex numbers $\mathbb{C}$ generated over the rational numbers $\mathbb{Q}$ by a root of unity. Let $k$ be an imaginary cyclotomic field. Let $\xi_n = e^{2\pi i/n}$ for any integer $n \geq 1$. There is then a unique integer $m > 2$, $m \equiv 2 \pmod{4}$, such that $k = \mathbb{Q}(\xi_m)$. Let $G$ be the Galois group of $k$ over $\mathbb{Q}$, and let $R = \mathbb{Z}[G]$ be a group ring of $G$ over the rational integers $\mathbb{Z}$. Let $h$ denote the class number of $k$, $h^+$ the class number of $k^+$ (the maximal totally real subfield of $k$), and let $h^- = \frac{h}{h^+}$.

We shall consider certain subring $R^-$ of $R$ and the Stickelberger ideal $S$ of $R$. Let $S^-$ be the intersection of $S$ and $R^-$. Iwasawa [3] has proved that in the special case $m = p^{n+1}$ ($p$ is an odd prime and $n \geq 0$ an integer) $h^-$ is equal to the group index $[R^- : S^-]$. Iwasawa's proof is based on the representations of a semi-simple algebra. Another proof, based on the presentation of a special basis of $S^-$, has been given by Skula [5].

The result of Iwasawa has been generalized by Sinnott [4] to the case of any cyclotomic field. He has shown that

$$[R^- : S^-] = 2^a h^-,$$
where \( a \) is an integer defined as follows. Let \( r \) be the number of distinct primes dividing \( m \). Then \( a = 0 \) if \( r = 1 \), and

\[
a = 2^{r-2} - 1
\]

if \( r > 1 \).

Sinnott defined \( S \) as the intersection of \( R \) and \( S' \), where \( S' \) is the subgroup of \( \mathbb{Q}[G] \) generated by the elements

\[
\Theta(a) = \sum_{t \mod m \atop (t,m) = 1} \left\langle -\frac{at}{m} \right\rangle \sigma_t^{-1}, \quad a \in \mathbb{Z},
\]

where the sum is taken over complete set of integers \( t \) prime to \( m \) and distinct modulo \( m \), \( \sigma_t \) denotes the automorphism \( k \) over \( \mathbb{Q} \) sending \( \xi_m \) to \( \xi_m^t \). For any real number \( x \) the symbol \( \langle x \rangle \) denotes the fractional part of \( x \); so \( x - \langle x \rangle \in \mathbb{Z} \) and \( 0 \leq \langle x \rangle < 1 \). Since

\[
\Theta(a) = \Theta(a + m)
\]

for any integer \( a \), \( S \) is generated by the elements \( \Theta(a) \), for all \( a \) from the complete set of integers distinct modulo \( m \).

I have been interested in changing the group index \([R^{-} : S^{-}]\) in the case of replacing \( S' \) by the subgroup \( I' \) of the group \( \mathbb{Q}[G] \) generated by the elements \( \Theta(a) \), for all \( a \) from the complete set of integers prime to \( m \) and distinct modulo \( m \). Since

\[
\Theta(a) = \sigma_a \Theta(-1)
\]

for any integer \( a \) prime to \( m \), \( I' \) is an \( R \)-module and

\[
I' = (\Theta(-1)) R.
\]

Hence

\[
I = I' \cap R
\]

is an ideal of \( R \). Since \( I \subseteq S' \), \([4]\) follows that the elements of \( I \) annihilate the ideal class group of \( k \). Let \( I^{-} = I \cap R \). (This ideal has been considered by Washington \([7]\), § 6.2. In the general case \( I^{-} \) is not equal to \( S^{-} \) (see Proposition 4.3.), so in \([7]\), Remark after Theorem 6.19, we have to take \( S^{-} \) instead of \( I^{-} \).) A question of finiteness of the group \( R^{-}/I^{-} \) is fully solved in theorem 4.1 and order \( R^{-}/I^{-} \) in case of finiteness is given by theorem 4.2. The proof of these theorems will be based on the presentation of a special basis of \( I^{-} \) and the calculation of the determinant of the transition matrix from a certain basis of \( R^{-} \) to this basis of \( I^{-} \), like Skula’s proof \([5]\).

2. NOTATION

In this paper the following symbols are used:

\[
\begin{align*}
Z_n^* & \text{ the multiplicative group of } \mathbb{Z}/n\mathbb{Z} \\
m & \text{ an integer, } m > 2, m \not\equiv 2 \pmod{4}
\end{align*}
\]
STICKELBERGER IDEAL

\[ m = p_1^{s_1} \ldots p_r^{s_r} \] prime decomposition, \( p_1, \ldots, p_r \) are distinct primes

\[ m_i = \frac{m}{p_i^{s_i}} \quad \text{(for } i = 1, \ldots, m) \]

\( s_i \) order of \( p_i \) of the group \( \mathbb{Z}_{m_i}^* \) (for \( i = 1, \ldots, m \))

\[ N = \frac{1}{\varphi(m)} \quad \text{(} \varphi \text{ is the Euler function)} \]

\[ \xi_m = e^m \]

\( G \) the Galois group of \( \mathbb{Q}(\xi_m) \) over \( \mathbb{Q} \)

\( j \) the element of \( G \) induced by complex conjugation

\[ \mapsto: G \to \{ t \mid t \in \mathbb{Z}, 0 \leq t < m, (t, m) = 1 \} \text{ the canonical mapping, defined in this way, that for any } \sigma \in G \]

\[ \sigma(\xi_m) = \xi_m^\sigma \]

\[ w = \begin{cases} 
  m & \text{if } m \text{ is even} \\
  2m & \text{if } m \text{ is odd}
\end{cases} \]

\[ \hat{\sigma} = \begin{cases} 
  \bar{\sigma} & \text{if } \bar{\sigma} \text{ is odd} \\
  \bar{\sigma} + m & \text{if } \bar{\sigma} \text{ is even}
\end{cases} \]

\( X^- \) the set of all odd characters \( \chi \) of \( G \) (i.e., \( \chi(f) = -1 \))

\[ F_\chi = \sum_{k \in G} \chi(k) \cdot k \quad \text{(for } \chi \in X^-) \]

\[ \langle x \rangle \text{ the fractional part of the real number } x; \text{ so } x - \langle x \rangle \in \mathbb{Z} \text{ and } 0 \leq \langle x \rangle < 1 \]

\( R = Z[G] \) the group ring of \( G \) over the integers \( Z \)

\( R^- = (1 - j)R \) a subring, often considered as a \( Z \)-module

\[ \Theta(a) = \sum_{\sigma \in G} \left\langle -\frac{a \bar{\sigma}}{m} \right\rangle \sigma^{-1} \in \mathbb{Q}[G] \quad (a \text{ is an integer}) \]

\( I' = (\Theta(-1)) R \)

\( I = I' \cap R \) an ideal in \( R \)

\( I^- = I \cap R^- \) an ideal in \( R^- \), often considered as \( Z \)-module

**Definition.** A subset \( \Xi \) of the set \( G \) is called a choice from \( G \), if the following conditions are satisfied

(i) \( 1 \in \Xi \)

(ii) \( x \in \Xi \iff jx \notin \Xi \text{ for any } x \in G \)

Clearly, a choice from \( G \) is for example the set

\[ \left\{ x; \ x \in G \land 1 \leq \bar{x} < \frac{m}{2} \right\} \]

3. THE BASIS OF \( R^- \) AND THE SYSTEM OF GENERATORS OF \( I^- \)

3.1. Theorem. *The system \( \{ \beta_\sigma; \sigma \in \Xi \}, \text{ where } \beta_\sigma = (1 - j) \sigma \text{ and } \Xi \text{ is any choice from } G, \text{ is a basis of } R^-.*
Proof. Clearly \( \{ \beta_\sigma; \sigma \in \Xi \} \subset R^- \). Let \( \gamma \) be any element of \( R^- \). Then there is \( \delta = \sum_{\sigma \in G} \delta_\sigma \sigma \in R \) such that \( \gamma = (1 - j) \delta \). Thus

\[
\gamma = (1 - j) \sum_{\sigma \in G} \delta_\sigma \sigma = (1 - j) \left( \sum_{\sigma \in \Xi} \delta_\sigma + \sum_{\sigma \in G - \Xi} \delta_\sigma \sigma \right) = (1 - j) \sum_{\sigma \in \Xi} (\delta_\sigma + \delta_{ja}) \sigma = \sum_{\sigma \in \Xi} (\delta_\sigma - \delta_{ja}) (1 - j) \sigma = \sum_{\sigma \in \Xi} (\delta_\sigma - \delta_{ja}) \beta_\sigma.
\]

Now we have to show linear independence. Let us assume, that

\[
0 = \sum_{\sigma \in \Xi} c_\sigma \beta_\sigma = \sum_{\sigma \in \Xi} c_\sigma (1 - j) \sigma = \sum_{\sigma \in \Xi} c_\sigma \sigma - \sum_{\sigma \in \Xi} c_\sigma j \sigma = \sum_{\sigma \in \Xi} c_\sigma \sigma - \sum_{\sigma \in G - \Xi} c_{ja} \sigma = \sum_{\sigma \in G} d_\sigma \sigma,
\]

where

\[
d_\sigma = \begin{cases} 
c_\sigma & \text{for } \sigma \in \Xi, 
-c_{ja} & \text{for } \sigma \in G - \Xi.
\end{cases}
\]

It follows that \( d_\sigma = 0 \) for any \( \sigma \in G \). Hence \( c_\sigma = 0 \) for any \( \sigma \in \Xi \).

3.2. Theorem. The system \( \{ \alpha_k; k \in \Xi \} \), where

\[
\alpha_k = \begin{cases} 
\frac{w}{2} (1 - j) \Theta (-1) & \text{for } k = 1, \\
\left( \frac{1 + k}{2} + \frac{1 - k}{2} j - k \right) \Theta (-1) & \text{for } k \in \Xi - \{1\}
\end{cases}
\]

and \( \Xi \) is any choice, is the system of generators of \( I^- \).

Proof. Clearly \( \alpha_k \in I' \) for any \( k \in \Xi \), because \( k \) is an odd integer. We prove that also \( \alpha_k \in R^- \):

\[
\alpha_k = \frac{w}{2} (1 - j) \frac{1}{m} \sum_{\sigma \in \Xi} \sigma^{-1} \sigma = \frac{w}{2m} (1 - j) \left[ \sum_{\sigma \in \Xi} \sigma^{-1} \sigma + \sum_{\sigma \in \Xi} j \sigma^{-1} j \sigma \right] = \frac{w}{2m} (1 - j) \sum_{\sigma \in \Xi} \left( \sigma^{-1} + j \sigma^{-1} \right) \sigma = (1 - j) \sum_{\sigma \in \Xi} \frac{w}{2m} (2 \sigma^{-1} - m) \sigma,
\]

(3.1)

where we have used the identity \( \sigma^{-1} + j \sigma^{-1} = m \). Let us notice that

\[
\frac{w}{2m} (2 \sigma^{-1} - m) \in \mathbb{Z}
\]

for any \( \sigma \in G \) regardless of if \( m \) is odd or even, and thus \( \alpha_1 \in R^- \). Let \( k \) be any element in \( \Xi - \{1\} \). Then
STICKELBERGER IDEAL

\[ \alpha_k = \left( \frac{1 + k}{2} + \frac{1 - k}{2} j - k \right) \cdot \frac{1}{m} \sum_{\sigma \in \mathbb{S}} \sigma^{-1} \sigma = \]

\[ = \frac{1}{m} \left( \frac{1 + k}{2} \sum_{\sigma \in \mathbb{S}} \sigma^{-1} \sigma + \frac{1 - k}{2} \sum_{\sigma \in \mathbb{S}} j \sigma^{-1} \sigma - \sum_{\sigma \in \mathbb{S}} k \sigma^{-1} \sigma \right) = \]

\[ = \frac{1}{m} \sum_{\sigma \in \mathbb{S}} \left( \frac{1 + k}{2} \sigma^{-1} + \frac{1 - k}{2} j \sigma^{-1} - k \sigma^{-1} \right) \sigma + \]

\[ + \frac{1}{m} \sum_{\sigma \in \mathbb{S}} \left( \frac{1 + k}{2} j \sigma^{-1} + \frac{1 - k}{2} \sigma^{-1} - j k \sigma^{-1} \right) j \sigma. \]

Considering that \( j x = m - x \) for any \( x \in G \)

\[ \alpha_k = \frac{1}{m} \sum_{\sigma \in \mathbb{S}} (k(1 - j) \sigma^{-1} - (1 - j) k \sigma^{-1}) \sigma + \sum_{\sigma \in \mathbb{S}} \frac{1 - k}{2} (1 - j) \sigma = \]

\[ = (1 - j) \sum_{\sigma \in \mathbb{S}} \left( \frac{k \sigma^{-1} - k \sigma^{-1}}{m} + \frac{1 - k}{2} \right) \sigma. \]

(3.2)

Since \( \bar{x} \cdot \bar{y} \equiv xy \pmod{m} \) for any \( x, y \in G \), we have

\[ k \sigma^{-1} - k \sigma^{-1} \equiv k \sigma^{-1} - k \sigma^{-1} \equiv 0 \pmod{m}. \]

It follows that

\[ \frac{k \sigma^{-1} - k \sigma^{-1}}{m} + \frac{1 - k}{2} \in \mathbb{Z}, \]

because \( k \) is an odd integer. Hence \( \alpha_k \in R^- \) and then \( \{ \alpha_k; k \in \mathbb{S} \} \subseteq I^- \).

Now, let \( \gamma \) be any element in \( I^- \). Then there are \( \xi, \eta \in R \) so that

(3.3) \[ \gamma = \xi \cdot \Theta(-1), \]

(3.4) \[ \gamma = (1 - j) \eta. \]

Thus

(3.5) \[ \gamma = (1 - j) \eta = \frac{1}{2} (1 - j)^2 \eta = \frac{1}{2} (1 - j) \gamma = \frac{1}{2} (1 - j) \zeta \cdot \Theta(-1). \]

Let us denote

\[ \gamma = \sum_{y \in \mathbb{G}} \gamma_y y, \]

\[ \zeta = \sum_{y \in \mathbb{G}} \zeta_y y, \]

\[ \eta = \sum_{y \in \mathbb{G}} \eta_y y, \]

\[ t_y = \xi_y - \xi_j, \quad \text{for any } y \in \mathbb{S}, \]

\[ t = \frac{1}{w} \sum_{y \in \mathbb{S}} t_y y. \]

We prove that \( t \) is an integer. Using (3.4), we get

\[ \gamma_1 + \gamma_j = \eta_1 - \eta_j + \eta_j - \eta_1 = 0. \]

By (3.3),

\[ \gamma_1 + \gamma_j = \eta_1 - \eta_j + \eta_j - \eta_1 = 0. \]

By (3.3),
\[ \gamma = \zeta \cdot \Theta(-1) = \sum_{y \in G} \zeta_y y \cdot \frac{1}{m} \sum_{\sigma \in G} \sigma^{-1} \sigma = \frac{1}{m} \sum_{\sigma \in G} \left( \sum_{y \in G} \zeta_y y \sigma^{-1} \right) \sigma. \]

It follows that
\[ \gamma_1 = \frac{1}{m} \sum_{y \in G} \zeta_y y \]
\[ \gamma_j = \frac{1}{m} \sum_{y \in G} \zeta_y j y = \sum_{y \in G} \zeta_y - \frac{1}{m} \sum_{y \in G} \zeta_y y. \]

Hence
\[ 0 = \gamma_1 + \gamma_j = \sum_{y \in G} \zeta_y. \]

To prove \( t \in \mathbb{Z} \), it is enough to verify, that
\[ \sum_{y \in S} t_y \bar{y} \equiv 0 \pmod{w}. \]

Since \( w \) is the least common multiple of the numbers 2 and \( m \), we verify this congruence modulo \( m \) and modulo 2:
\[ \sum_{y \in S} t_y \bar{y} \equiv \sum_{y \in S} t_y \bar{y} = \sum_{y \in S} (\zeta_y - \zeta_{yj}) \bar{y} = \]
\[ = \sum_{y \in S} \zeta_y \bar{y} - \sum_{y \in G - S} \zeta_y (m - \bar{y}) \equiv \sum_{y \in G} \zeta_y \bar{y} = m\gamma_1 \equiv 0 \pmod{m}, \]
\[ \sum_{y \in S} t_y \bar{y} \equiv \sum_{y \in S} t_y = \sum_{y \in G} (\zeta_y - \zeta_{yj}) \equiv \sum_{y \in G} \zeta_y \equiv 0 \pmod{2}. \]

Thus \( t \in \mathbb{Z} \). The theorem will be proved, if we show
\[ \gamma = t\alpha_1 - \sum_{y \in S - \{1\}} t_y \alpha_y. \]

By (3.1) and (3.2),
\[ t\alpha_1 - \sum_{y \in S - \{1\}} t_y \alpha_y = \frac{1}{w} \sum_{y \in S} t_y \bar{y} \cdot (1 - j) \sum_{\sigma \in S} w \left( 2\sigma^{-1} - m \right) \sigma - \]
\[ - \sum_{y \in S - \{1\}} t_y (1 - j) \sum_{\sigma \in S} \left( \frac{y \sigma^{-1} - y \sigma^{-1}}{m} + \frac{1 - \bar{y}}{2} \right) \sigma. \]

Let us notice that we get zero in the second sum for \( y = 1 \). Consequently, we can take this sum over the whole choice \( S \).
\[ t\alpha_1 - \sum_{y \in S - \{1\}} t_y = \]
\[ = \frac{1}{2m} (1 - j) \sum_{y \in S} t_y \sum_{\sigma \in S} (2\sigma^{-1} - m\bar{y} - 2y\sigma^{-1} + 2y\sigma^{-1} - m + m\bar{y}) \sigma = \]
\[ = \frac{1}{2m} (1 - j) \sum_{y \in S} \sum_{\sigma \in S} (\sigma^{-1} - jy\sigma^{-1}) \sigma = \]
\[ = \frac{1}{2m} (1 - j) \sum_{y \in S} (\zeta_y - \zeta_{yj}) \sum_{\sigma \in G} \sigma^{-1} y \sigma = \]
STICKELBERGER IDEAL

\[ \frac{1}{2} (1 - j) \cdot \Theta(-1) \cdot \sum_{\gamma \in \mathbb{Z}} (\zeta_{\gamma} + j \zeta_{j\gamma}) y = \]

\[ = \frac{1}{2} (1 - j) \cdot \Theta(-1) \cdot \zeta = \gamma \]

according to (3.5). The theorem is proved.

4. THE GROUP INDEX \([I^- : I^-]\)

Let \(A\) denote the absolute value of the determinant of the transition matrix from the basis \(\{\beta_{\sigma}; \sigma \in \mathbb{Z}\}\) to the system of generators \(\{\alpha_{\sigma}; \sigma \in \mathbb{Z}\}\). Clearly

\[ \alpha_{1} = (1 - j) \sum_{\sigma \in \mathbb{Z}} \frac{w}{2m} (2 \sigma^{-1} - m) \sigma = \sum_{\sigma \in \mathbb{Z}} \frac{w}{2m} (2 \sigma^{-1} - m) \beta_{\sigma} \]

and for any \(k \in \mathbb{Z} - \{1\}\)

\[ \alpha_{k} = (1 - j) \sum_{\sigma \in \mathbb{Z}} \left( \frac{k \sigma^{-1} - k \sigma^{-1}}{m} + \frac{1 - k}{2} \right) \sigma = \sum_{\sigma \in \mathbb{Z}} \left( \frac{k \sigma^{-1} - k \sigma^{-1}}{m} + \frac{1 - k}{2} \right) \beta_{\sigma}. \]

Hence

\[
A = \left| \begin{array}{cccc}
\frac{w}{2m} (2 - m) & \ldots & \frac{w}{2m} (2 \sigma^{-1} - m) & \ldots \\
\vdots & \ddots & \vdots & \ddots \\
\frac{k - k}{m} + \frac{1 - k}{2} & \ldots & \frac{k \sigma^{-1} - k \sigma^{-1}}{m} + \frac{1 - k}{2} & \ldots \\
\vdots & \ddots & \vdots & \ddots \\
\end{array} \right|.
\]

If we multiply the first row by the number \(-\frac{2m}{w}\) and the other rows by the number \(2m\) and if we add the first row multiplied by the number \(k\) to the \(k\) th row for each \(k \in \mathbb{Z} - \{1\}\), we obtain

\[
A = \frac{w}{(2m)^n} \cdot \left| \begin{array}{cccc}
m - 2 & \ldots & m - 2 \sigma^{-1} & \ldots \\
\vdots & \ddots & \vdots & \ddots \\
m - 2 k & \ldots & m - 2 k \sigma^{-1} & \ldots \\
\vdots & \ddots & \vdots & \ddots \\
\end{array} \right|.
\]

Let us consider a mapping \(f: \mathbb{Z} \rightarrow \mathbb{Z}\), defined in this way:

\[ f(x) = \begin{cases} 
x^{-1} & \text{if } x^{-1} \in \mathbb{Z}, \\
jx^{-1} & \text{if } x^{-1} \notin \mathbb{Z}. 
\end{cases} \]

It is easy to show that \(f\) is the bijective mapping. With the help of \(f\) we permute the columns in the determinant (if \(\sigma^{-1} \notin \mathbb{Z}\), we must multiple \(\sigma\)th column by \(-1\):
Let 

\[ A = (m - 2\overline{k}\sigma)_{k,\sigma \in \mathbb{Z}}, \quad C = (\chi(k))_{\chi \in X^{-}, k \in \mathbb{Z}}, \]

\[ D = C \cdot A = (d_{x,\sigma})_{x \in X^{-}, \sigma \in \mathbb{Z}}. \]

Then 

\[ d_{x,\sigma} = \sum_{k \in \mathbb{Z}} \chi(k)(jk\overline{\sigma} - \overline{k}\sigma) = \sum_{k \in G - \mathbb{Z}} \chi(jk)\overline{k}\sigma - \sum_{k \in \mathbb{Z}} \chi(k)\overline{k}\sigma = -\sum_{k \in G} \chi(k)\overline{k}\sigma = -\sum_{k \in G} \chi(k)\overline{k}\sigma \overline{E} = -(\chi(\sigma))^{-1} \sum_{k \in G} \chi(k) E = -(\chi(\sigma))^{-1} \cdot F_{x}. \]

In the following lines a vinculum denotes a complex conjugation.

\[ |\det D| = |\det (-\overline{\chi(\sigma)} \cdot F_{x})_{x \in X^{-}, \sigma \in \mathbb{Z}}| = | \prod_{x \in X^{-}} F_{x} | \cdot |\det (\chi(\sigma))_{x \in X^{-}, \sigma \in \mathbb{Z}}| = | \prod_{x \in X^{-}} F_{x} | \cdot |\det (\chi(\sigma))_{x \in X^{-}, \sigma \in \mathbb{Z}}| = | \prod_{x \in X^{-}} F_{x} | \cdot |\det C| = | \det C | \cdot |\det A|. \]

Let us assumed, that the matrix \( C \) is a singular matrix. Then there exist complex numbers \( c_{x} (\chi \in X^{-}) \), from which at least one is non-zero, such that

\[ \sum_{x \in X^{-}} c_{x}\chi(k) = 0 \]

for any \( k \in \mathbb{Z} \). The same fact holds also for any \( k \in G - \mathbb{Z} \):

\[ \sum_{x \in X^{-}} c_{x}\chi(k) = \sum_{x \in X^{-}} \chi(j) c_{x}\chi(jk) = -\sum_{x \in X^{-}} c_{x}\chi(jk) = 0, \]

because \( jk \in \mathbb{Z} \). Hence, the characters \( \chi, \chi \in X^{-} \) are linearly dependent. But any finite system of distinct characters of any group is linearly independent ([6], § 54, Unabhängigkeitssatz). Thus, the matrix \( C \) is regular and by (4.2)

\[ |\det A| = | \prod_{x \in X^{-}} F_{x} |. \]

Consequently, by substitution to (4.1)

\[ (4.3) \quad A = \frac{w}{(2m)^{N}} \cdot | \prod_{x \in X^{-}} F_{x} |. \]
Let us consider, that

\[ G \cong \mathbb{Z}_m^* \]

(this isomorphism assigns to \( \sigma \in G \) the class containing \( \sigma \)). If \( \chi \) is any character of \( G \), we denote also by \( \chi \) the Dirichlet character modulo \( m \) associated to \( \chi \) by means of this isomorphism. Hence, \( X^- \) is also the set of all odd Dirichlet characters modulo \( m \) (i.e. such that \( \chi(-1) = -1 \)). Then

\[ F_{\chi} = \sum_{k \in G} \chi(k) \overline{k} = \sum_{i=1}^{m} \chi(i) i \]

for any \( \chi \in X^- \). With the help of [4], lemma 2.1:

\[-\frac{1}{m} \sum_{i=1}^{m} \chi(i) i = \left( \prod_{p|m} (1 - \chi^*(p)) \right) \left( -\frac{1}{f(\chi)} \sum_{i=1}^{f(\chi)} \chi^*(i) i \right),\]

where \( \chi^* \) denotes the primitive character inducing \( \chi \), \( f(\chi) \) its conductor and the product is taken over all primes dividing \( m \). Thus

\[ F_{\chi} = \left( \prod_{p|m} (1 - \chi^*(p)) \right) \left( \frac{m}{f(\chi)} \sum_{i=1}^{f(\chi)} \chi^*(i) i \right). \tag{4.4} \]

We use the analytic class number formula (see, for example [2]):

\[ h^- = 2Qw \prod_{\chi \in X^-} \frac{1}{2f(\chi)} \sum_{i=1}^{f(\chi)} (-\chi^*(i) i), \tag{4.5} \]

where \( Q \) is 1 if \( m \) is a prime power, and \( Q \) is 2 otherwise. The formulas (4.3), (4.4) and (4.5) imply

\[ \Delta = w \left| \prod_{\chi \in X^-} \frac{1}{2m} F_{\chi} \right| = \]

\[ = w \left| \prod_{\chi \in X^-} \left( \frac{1}{2f(\chi)} \sum_{i=1}^{f(\chi)} \chi^*(i) i \right) \prod_{p|m} (1 - \chi^*(p)) \right| = \]

\[ = \frac{1}{Q} h^- \prod_{\chi \in X^-} \prod_{p|m} |1 - \chi^*(p)|. \tag{4.6} \]

4.1. Theorem. The group \( R^-/I^- \) is finite if and only if \( s_i \) is even and \( p_i^2 \equiv -1 \pmod{m_i} \) for each \( i = 1, \ldots, r \), or if \( r = 1 \).

Proof. If \( r = 1 \), then \( m = p_1^{s_1} \) and \( p_1 \mid f(\chi) \) for any character \( \chi \in X^- \). Hence \( \chi^*(p_1) = 0 \) and from (4.6)

\[ \Delta = h^- \prod_{\chi \in X^-} (1 - \chi^*(p_1)) = h^- \neq 0 \tag{4.7} \]

and the group \( R^-/I^- \) is finite.
Hereafter let us suppose, that \( r \geq 2 \). Clearly \( R^\sim/I^- \) is finite if and only if \( \Delta \neq 0 \). From (4.6) \( \Delta \neq 0 \) if and only if there does not exist an odd character \( \chi \) modulo \( m \) and \( i \in \{1, \ldots, r\} \) such, that \( \chi^*(p_i) = 1 \).

We shall show that it is right if and only if \(-1\) is an element of the subgroup \( H \) of \( \mathbb{Z}^*_{m_i} \) generated by \( p_i \).

Indeed, if \( \chi^*(p_i) = 1 \) for an odd character \( \chi \) modulo \( m \), then \( p_i \not\equiv 0(\chi) \) and \( \chi \) is induced by any character \( \chi' \) modulo \( m_i \). Since \( \chi'(p_i) = 1 \), the character \( \chi' \) is unit on the whole subgroup \( H \) generated by \( p_i \). Since \( \chi'(-1) = -1 \), \(-1\) is not an element of \( H \).

On the other hand, if \(-1 \notin H \), then there exists a character \( \chi' \) modulo \( m_i \) such that \( \chi'(-1) \neq 1 \) and \( \chi'(x) = 1 \) for any \( x \in H \) (see, for example [1]). Thus specially \( \chi'(p_i) = 1 \) and \( \chi'(-1) = -1 \), because the order of \(-1\) of the group \( \mathbb{Z}^*_{m_i} \) is 2 and it implies that \( \chi'(-1) \) is 1 or \(-1\). Let \( \chi \) be the character modulo \( m \) induced by \( \chi' \).

Then \( \chi(-1) = -1 \) and \( \chi^*(p_i) = 1 \).

For completing of the proof of the theorem it is enough to notice that if \( s_i \) is even and

\[
p_i^2 \equiv -1(\text{mod } m_i),
\]

then really \(-1 \in H \) and on the contrary \(-1 \in H \) implies that \( s_i \) is even (the order of the element \(-1\) divides the order of the group \( H \)) and

\[
p_i^2 \equiv -1(\text{mod } m_i),
\]

(there is only one element such that its order is 2 in the cyclic group of even order).

4.2. Theorem. If the group \( R^\sim/I^- \) is finite, then

\[
[R^- : I^-] = 2^b \cdot h^-,
\]

where \( b = 0 \) if \( r = 1 \) and

\[
b = -1 + \sum_{i=1}^{r} \frac{\varphi(m_i)}{s_i}
\]

if \( r \geq 2 \).

Proof. Let us notice that if \( R^\sim/I^- \) is finite, then

\[
[R^- : I^-] = \Delta.
\]

If \( r = 1 \) then by (4.7)

\[
\Delta = h^- = 2^b \cdot h^-.
\]

Hereafter let us suppose, that \( r \geq 2 \). For \( l \in \mathbb{Z} \) let \( X^+_l \) or \( X^-_l \) denote the set of all even or odd characters modulo \( l \), respectively. It is easy to show that if \( l_1, l_2 \) are a relative prime integers then for any character \( \chi \in X_{l_1}^+ \) there exist the unique characters \( \chi_1, \chi_2 \), where \( \chi_1 \in X_{l_1}^+ \) and \( \chi_2 \in X_{l_2}^- \) or \( \chi_1 \in X_{l_1}^- \) and \( \chi_2 \in X_{l_2}^+ \), such that

\[
\chi(y) = \chi_1(y) \cdot \chi_2(y)
\]
STICKELBERGER IDEAL

for any integer \( y \). Besides that,

\[ \chi^*(y) = \chi_1^*(y) \cdot \chi_2^*(y) \]

for any integer \( y \), too. Hence

\[ \prod_{i=1}^{r} \prod_{x \in X^*} |1 - \chi^*(p_i)| = \prod_{i=1}^{r} \left( \prod_{x_1 \in X^{-q_i}, x_2 \in X^{-m_i}} \prod_{x \in X^*} |1 - \chi_1^*(p_i) \chi_2^*(p_i)| \right) \]

where \( q_i = p_i^{r_i} \). Let us notice that \( \chi_2^*(p_i) = \chi_2(p_i) \), because \( p_i \not\mid m_i \). If \( p_i \mid f(\chi_1) \) then \( \chi_1^*(p_i) = 0 \). Moreover \( p_i \mid f(\chi_1) \) if and only if \( \chi_1 \) is not the unit character. Consequently

(4.8) \[ \prod_{i=1}^{r} \prod_{x \in X^*} |1 - \chi^*(p_i)| = \prod_{i=1}^{r} \prod_{x \in X^{-m_i}} |1 - \chi(p_i)|. \]

Since the group \( R^*/I^- \) is finite, we have \( 1 - \chi(p_i) \neq 0 \). Hence, there exists a logarithm

\[ \ln (1 - \chi(p_i)). \]

Since

\[ \ln (1 - z) = -\sum_{n=1}^{\infty} \frac{z^n}{n}, \]

for \( |z| < 1 \) and \( |\chi(p_i)| = 1 \), by Abel’s theorem on continuity up to the circle of convergence

\[ \ln (1 - \chi(p_i)) = -\sum_{n=1}^{\infty} \frac{(\chi(p_i))^n}{n}, \]

considering that the sum on the right side converges by Dirichlet’s test. Thus

\[ 1 - \chi(p_i) = \exp \left( -\sum_{n=1}^{\infty} \frac{(\chi(p_i))^n}{n} \right). \]

By (4.6) with the help of (4.8)

\[ A = \frac{1}{2} h^{-r} \prod_{i=1}^{r} \prod_{x \in X^{-m_i}} \left| \exp \left( -\sum_{n=1}^{\infty} \frac{\chi(p_i^n)}{n} \right) \right| = \]

(4.9) \[ = \frac{1}{2} h^{-r} \left| \prod_{i=1}^{r} \exp \left( -\sum_{i=1}^{\infty} \frac{1}{n} \sum_{x \in X^{-m_i}} \chi(p_i^n) \right) \right|. \]

It is easy to show
By the proof of the theorem 4.1,

\[ p_i^n \equiv 1 \pmod{m_i} \]

if and only if

\[ n \equiv 0 \pmod{s_i} \]

and

\[ p_i^n \equiv -1 \pmod{m_i} \]

if and only if

\[ n \equiv s_i \pmod{2} \]

Thus

\[ \sum_{n=1}^{\infty} \frac{1}{n} \sum_{x \in \mathcal{X}_{m_i}} \chi(n) = \sum_{i=1}^{\infty} \frac{1}{\frac{1}{2}} \frac{\varphi(m_i)}{t} (-1)^t \frac{\varphi(m_i)}{2} = \]

\[ = \frac{\varphi(m_i)}{s_i} \sum_{i=1}^{\infty} \frac{(-1)^t}{t} = \frac{\varphi(m_i)}{s_i} \ln 2. \]

By (4.9),

\[ \Delta = \frac{1}{2} h^{-1} \prod_{i=1}^{r} \left| \exp \left( \frac{\varphi(m_i)}{s_i} \ln 2 \right) \right| = \]

\[ = \frac{1}{2} h^{-1} \prod_{i=1}^{r} 2^{\frac{\varphi(m_i)}{s_i}} = h^{-1} 2^{-1 + \sum_{i=1}^{r} \frac{\varphi(m_i)}{s_i}} = 2^bh^{-1}. \]

Since \( \Delta = [R^+ : I^+] \), the theorem follows.

The following proposition solves the problem, when the ideals \( I^- \) and \( S^- \) are identical.

4.3. Proposition. If \( r = 1 \) then \( I^- = S^- \), if \( r \geq 2 \) then \( I^- \neq S^- \).

Proof. If \( r = 1 \) then the groups \( R^-/I^- \) and \( R^-/S^- \) are finite and have the same order. By their definitions \( I^- \geq S^- \). Hence \( I^- = S^- \).

Hereafter let us suppose that \( r \geq 2 \). If the group \( R^-/I^- \) is not finite then \( I^- \neq S^- \) because \( R^-/S^- \) is finite. Let us assume that \( R^-/I^- \) is finite. It is easy to show that

\[ Z_{m_i}^x \approx \prod_{k=1}^{r} Z_{m_i}^x, \]
where $\prod$ denotes the direct product of groups and $q_k = \mathbb{Z}^*_{p_k}$. Therefore an order of any element of $\mathbb{Z}^*_{m_i}$ has to divide the least common multiple of $\varphi(p_k^{n_k})$, $k \in \{1, \ldots, r\} - \{i\}$. Considering that these numbers are all even, their common multiple is also

$$2 \prod_{k=1, \ldots, r, k \neq i} \frac{\varphi(p_k^{n_k})}{2} = 2^{2r-2} \varphi(m_i).$$

Consequently

$$s_i \leq 2^{2r-2} \varphi(m_i)$$

and then

$$b = -1 + \sum_{i=1}^r \frac{\varphi(m_i)}{s_i} \geq -1 + r 2^{r-2} > 2^{r-2} - 1.$$ 

That follows that $[R^- : S^-] \neq [R^- : I^-]$. Therefore $I^- \neq S^-.$

REFERENCES


R. Kučera
Department of Mathematics
Faculty of Science, J. E. Purkyně University
Janáčkovo nám. 2a,
662 95 Brno
Czechoslovakia