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`

ARCHIVUM MATHEMATICUM (BRNO)
Vol. 22, No. 1 (1986) 7–20

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 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 C generated over the rational numbers Q by a root of unity. Let k be an imaginary cyclotomic field. Let $\zeta_n = e^{\frac{2\pi i}{n}}$ for any integer $n \geqq 1$. There is then a unique integer $m > 2$, $m \not\equiv 2 \pmod 4$, such that $k = Q(\zeta_m)$. Let G be the Galois group of k over Q, and let $R = Z[G]$ be a group ring of G over the rational integers Z. Let h denote the class number of k, h^+ the class number of k^+ (the maximal totally real subfield of k), and let $h^- = \dfrac{h}{h^+}$.

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 $n \geqq 0$ 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 $Q[G]$ generated by the elements

$$\Theta(a) = \sum_{\substack{t \bmod m \\ (t,m)=1}} \left\langle -\frac{at}{m} \right\rangle \sigma_t^{-1}, \qquad a \in Z,$$

where the sum is taken over complete set of integers t prime to m and distinct modulo m, σ_t denotes the automorphism k over Q sending ξ_m to ξ_m^t. For any real number x the symbol $\langle x \rangle$ denotes the fractional part of x; so $x - \langle x \rangle \in Z$ and $0 \leqq \langle x \rangle < 1$. Since

$$\Theta(a) = \Theta(a + m)$$

for any integer a, S_t 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 $Q[G]$ 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:

Z_n^x the multiplicative group of Z/nZ

m an integer, $m > 2$, $m \not\equiv 2 \pmod 4$

$m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ prime decomposition, $p_1, \dots, p_r$ are distinct primes

$m_i = \dfrac{m}{p_i^{\alpha_i}}$ (for $i = 1, \dots, m$)

s_i order of p_i of the group $Z_{m_i}^x$ (for $i = 1, \dots, m$)

$N = \frac{1}{2}\varphi(m)$ (φ is the Euler function)

$\xi_m = e^{\frac{2\pi i}{m}}$

G the Galois group of $Q(\xi_m)$ over Q

j the element of G induced by complex conjugation

$\bar{\ }: G \to \{t \mid t \in Z, 0 \leqq t < m, (t, m) = 1\}$ the canonical mapping, defined in this way, that for any $\sigma \in G$

$$\sigma(\xi_m) = \xi_m^{\bar{\sigma}}$$

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

$\hat{\ }: G \to \{t \mid t \in Z, 0 \leqq t < w, (t, w) = 1\}$ the mapping, for any $\sigma \in G$ is

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

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

$F_\chi = \sum_{k \in G} \chi(k) \cdot \bar{k}$ (for $\chi \in X^-$)

$\langle x \rangle$ the fractional part of the real number x; so $x - \langle x \rangle \in Z$ and $0 \leqq \langle x \rangle < 1$

$R = Z[G]$ the group ring of G over the integers Z

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

$\Theta(a) = \sum_{\sigma \in G} \left\langle -\dfrac{a\bar{\sigma}}{m} \right\rangle \sigma^{-1} \in Q[G]$ (a 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 Ξ of the set G is called a choice from G, if the following conditions are satisfied

(i) $1 \in \Xi$

(ii) $x \in \Xi \Leftrightarrow jx \notin \Xi$ for any $x \in G$

Clearly, a choice from G is for example the set

$$\left\{x;\ x \in G \wedge 1 \leqq \bar{x} < \frac{m}{2}\right\}.$$

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

3.1. Theorem. *The system $\{\beta_\sigma; \sigma \in \Xi\}$, where $\beta_\sigma = (1 - j)\, \sigma$ and Ξ is any choice from G, is a basis of R^-.*

Proof. Clearly $\{\beta_\sigma; \sigma \in \Xi\} \subset R^-$. Let γ 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

$$\gamma = (1 - j) \sum_{\sigma \in G} \delta_\sigma \sigma = (1 - j) \Big(\sum_{\sigma \in \Xi} \delta_\sigma \sigma + \sum_{\sigma \in G - \Xi} \delta_\sigma \sigma \Big) =$$
$$= (1 - j) \sum_{\sigma \in \Xi} (\delta_\sigma \sigma + \delta_{j\sigma} j\sigma) = \sum_{\sigma \in \Xi} (1 - j)(\delta_\sigma + \delta_{j\sigma} j)\, \sigma =$$
$$= \sum_{\sigma \in \Xi} (\delta_\sigma - \delta_{j\sigma})(1 - j)\, \sigma = \sum_{\sigma \in \Xi} (\delta_\sigma - \delta_{j\sigma})\, \beta_\sigma.$$

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

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

where

$$d_\sigma = \begin{cases} c_\sigma & \text{for } \sigma \in \Xi, \\ -c_{j\sigma} & \text{for } \sigma \in G - \Xi. \end{cases}$$

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*

$$\alpha_k = \begin{cases} \dfrac{w}{2}(1 - j)\, \Theta(-1) & \textit{for } k = 1, \\ \left(\dfrac{1 + \hat{k}}{2} + \dfrac{1 - \hat{k}}{2} j - k \right) \Theta(-1) & \textit{for } k \in \Xi - \{1\} \end{cases}$$

and Ξ *is any choice, is the system of generators of* I^-.

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

$$\alpha_1 = \frac{w}{2}(1 - j) \frac{1}{m} \sum_{\sigma \in G} \overline{\sigma^{-1}}\, \sigma = \frac{w}{2m}(1 - j) \Big[\sum_{\sigma \in \Xi} \overline{\sigma^{-1}}\, \sigma + \sum_{\sigma \in \Xi} \overline{j\sigma^{-1}}\, j\sigma \Big] =$$
$$= \frac{w}{2m}(1 - j) \sum_{\sigma \in \Xi} (\overline{\sigma^{-1}} + j \,.\, \overline{j\sigma^{-1}})\, \sigma = (1 - j) \sum_{\sigma \in \Xi} \frac{w}{2m} (\overline{\sigma^{-1}} - \overline{j\sigma^{-1}})\, \sigma =$$
$$= (1 - j) \sum_{\sigma \in \Xi} \frac{w}{2m} (2\overline{\sigma^{-1}} - m)\, \sigma, \tag{3.1}$$

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

$$\frac{w}{2m}(2\overline{\sigma^{-1}} - m) \in Z$$

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

$$\alpha_k = \left(\frac{1+\bar{k}}{2} + \frac{1-\bar{k}}{2} j - k\right) \cdot \frac{1}{m} \sum_{\sigma \in G} \overline{\sigma^{-1}} \sigma =$$

$$= \frac{1}{m}\left(\frac{1+\bar{k}}{2} \sum_{\sigma \in G} \overline{\sigma^{-1}} \sigma + \frac{1-\bar{k}}{2} \sum_{\sigma \in G} \overline{j\sigma^{-1}} \sigma - \sum_{\sigma \in G} \overline{k\sigma^{-1}} \sigma\right) =$$

$$= \frac{1}{m} \sum_{\sigma \in \Xi} \left(\frac{1+\bar{k}}{2} \overline{\sigma^{-1}} + \frac{1-\bar{k}}{2} \overline{j\sigma^{-1}} - \overline{k\sigma^{-1}}\right) \sigma +$$

$$+ \frac{1}{m} \sum_{\sigma \in \Xi} \left(\frac{1+\bar{k}}{2} \overline{j\sigma^{-1}} + \frac{1-\bar{k}}{2} \overline{\sigma^{-1}} - \overline{jk\sigma^{-1}}\right) j\sigma.$$

Considering that $\overline{jx} = m - \bar{x}$ for any $x \in G$

$$\alpha_k = \frac{1}{m} \sum_{\sigma \in \Xi} (\bar{k}(1-j)\overline{\sigma^{-1}} - (1-j)\overline{k\sigma^{-1}})\sigma + \sum_{\sigma \in \Xi} \frac{1-\bar{k}}{2}(1-j)\sigma =$$

$$= (1-j) \sum_{\sigma \in \Xi} \left(\frac{\bar{k}\overline{\sigma^{-1}} - \overline{k\sigma^{-1}}}{m} + \frac{1-\bar{k}}{2}\right)\sigma. \tag{3.2}$$

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

$$\bar{k}\overline{\sigma^{-1}} - \overline{k\sigma^{-1}} \equiv \bar{k}\,\overline{\sigma^{-1}} - \overline{k\sigma^{-1}} \equiv 0 \pmod{m}.$$

It follows that

$$\frac{\bar{k}\overline{\sigma^{-1}} - \overline{k\sigma^{-1}}}{m} + \frac{1-\bar{k}}{2} \in Z,$$

because $\bar{k}$ is an odd integer. Hence $\alpha_k \in R^-$ and then $\{\alpha_k;\, k \in \Xi\} \subseteq I^-$. Now, let γ be any element in I^-. Then there are $\zeta, \eta \in R$ so, that

$$\gamma = \zeta \,.\, \Theta(-1), \tag{3.3}$$

$$\gamma = (1-j)\,\eta. \tag{3.4}$$

Thus

$$\gamma = (1-j)\eta = \frac{1}{2}(1-j)^2\eta = \frac{1}{2}(1-j)\gamma = \frac{1}{2}(1-j)\zeta \,.\, \Theta(-1). \tag{3.5}$$

Let us denote

$$\gamma = \sum_{y \in G} \gamma_y y,$$

$$\zeta = \sum_{y \in G} \zeta_y y,$$

$$\eta = \sum_{y \in G} \eta_y y,$$

$$t_y = \zeta_y - \zeta_{jy} \qquad \text{for any } y \in \Xi,$$

$$t = \frac{1}{w} \sum_{y \in \Xi} t_y \bar{y}.$$

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),

$$\gamma = \zeta \,.\, \Theta(-1) = \sum_{y \in G} \zeta_y y \,.\, \frac{1}{m} \sum_{\sigma \in G} \overline{\sigma^{-1}} \sigma = \frac{1}{m} \sum_{\sigma \in G} \Big(\sum_{y \in G} \zeta_y \overline{y\sigma^{-1}} \Big) \sigma .$$

It follows that

$$\gamma_1 = \frac{1}{m} \sum_{y \in G} \zeta_y \bar{y}$$

$$\gamma_j = \frac{1}{m} \sum_{y \in G} \zeta_y \overline{jy} = \sum_{y \in G} \zeta_y - \frac{1}{m} \sum_{y \in G} \zeta_y \bar{y}.$$

Hence

$$0 = \gamma_1 + \gamma_j = \sum_{y \in G} \zeta_y .$$

To prove $t \in Z$, it is enough to verify, that

$$\sum_{y \in \Xi} t_y \hat{y} \equiv 0 \qquad (\text{mod } w).$$

Since w is the least common multiple of the numbers 2 and m, we verify this congruence modulo m and modulo 2:

$$\sum_{y \in \Xi} t_y \hat{y} \equiv \sum_{y \in \Xi} t_y \bar{y} = \sum_{y \in \Xi} (\zeta_y - \zeta_{jy}) \, \bar{y} =$$

$$= \sum_{y \in \Xi} \zeta_y \bar{y} - \sum_{y \in G - \Xi} \zeta_y (m - \bar{y}) \equiv \sum_{y \in G} \zeta_y \bar{y} = m\gamma_1 \equiv 0 \qquad (\text{mod}\, m),$$

$$\sum_{y \in \Xi} t_y \hat{y} \equiv \sum_{y \in \Xi} t_y = \sum_{y \in \Xi} (\zeta_y - \zeta_{jy}) \equiv \sum_{y \in G} \zeta_y = 0 \qquad (\text{mod}\, 2).$$

Thus $t \in Z$. The theorem will be proved, if we show

$$\gamma = t\alpha_1 - \sum_{y \in \Xi - \{1\}} t_y \alpha_y .$$

By (3.1) and (3.2),

$$t\alpha_1 - \sum_{y \in \Xi - \{1\}} t_y \alpha_y = \frac{1}{w} \sum_{y \in \Xi} t_y \hat{y} \,.\, (1 - j) \sum_{\sigma \in \Xi} \frac{w}{2m} (2\overline{\sigma^{-1}} - m) \, \sigma -$$

$$- \sum_{y \in \Xi - \{1\}} t_y (1 - j) \sum_{\sigma \in \Xi} \left(\frac{\hat{y}\overline{\sigma^{-1}} - \overline{y\sigma^{-1}}}{m} + \frac{1 - \hat{y}}{2} \right) \sigma .$$

Let us notice that we get zero in the second sum for $y = 1$. Consequently, we can take this sum over the whole choice Ξ.

$$t\alpha_1 - \sum_{y \in \Xi - \{1\}} t_y =$$

$$= \frac{1}{2m} (1 - j) \sum_{y \in \Xi} t_y \sum_{\sigma \in \Xi} (2\hat{y}\overline{\sigma^{-1}} - m\hat{y} - 2\hat{y}\overline{\sigma^{-1}} + 2\overline{y\sigma^{-1}} - m + m\hat{y}) \, \sigma =$$

$$= \frac{1}{2m} (1 - j) \sum_{y \in \Xi} t_y \sum_{\sigma \in \Xi} (\overline{y\sigma^{-1}} - \overline{jy\sigma^{-1}}) \, \sigma =$$

$$= \frac{1}{2m} (1 - j) \sum_{y \in \Xi} (\zeta_y - \zeta_{jy}) \sum_{\sigma \in G} \overline{\sigma^{-1}} y\sigma =$$

$$= \frac{1}{2}(1 - j) \cdot \Theta(-1) \cdot \sum_{y \in \Xi} (\zeta_y + j\zeta_{jy}) y =$$

$$= \frac{1}{2}(1 - j)\,\Theta(-1)\,\zeta = \gamma$$

according to (3.5). The theorem is proved.

4. THE GROUP INDEX $[R^- : I^-]$

Let Δ denote the absolute value of the determinant of the transition matrix from the basis $\{\beta_\sigma;\, \sigma \in \Xi\}$ to the system of generators $\{\alpha_\sigma;\, \sigma \in \Xi\}$. Clearly

$$\alpha_1 = (1 - j) \sum_{\sigma \in \Xi} \frac{w}{2m}(2\overline{\sigma^{-1}} - m)\,\sigma = \sum_{\sigma \in \Xi} \frac{w}{2m}(2\overline{\sigma^{-1}} - m)\,\beta_\sigma$$

and for any $k \in \Xi - \{1\}$

$$\alpha_k = (1 - j) \sum_{\sigma \in \Xi} \left(\frac{\bar{k}\overline{\sigma^{-1}} - \overline{k\sigma^{-1}}}{m} + \frac{1 - \bar{k}}{2} \right) \sigma =$$

$$= \sum_{\sigma \in \Xi} \left(\frac{\bar{k}\overline{\sigma^{-1}} - \overline{k\sigma^{-1}}}{m} + \frac{1 - \bar{k}}{2} \right) \beta_\sigma .$$

Hence

$$\Delta = \left| \begin{vmatrix} \frac{w}{2m}(2 - m) & \dots & \frac{w}{2m}(2\overline{\sigma^{-1}} - m) & \dots \\ \vdots & & \vdots & \\ \frac{\bar{k} - \bar{k}}{m} + \frac{1 - \bar{k}}{2} & \dots & \frac{\bar{k}\overline{\sigma^{-1}} - \overline{k\sigma^{-1}}}{m} + \frac{1 - \bar{k}}{2} & \dots \\ \vdots & & \vdots & \end{vmatrix} \right| .$$

If we multiple 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 $\bar{k}$ to the k th row for each $k \in \Xi - \{1\}$, we obtain

$$\Delta = \frac{w}{(2m)^N} \cdot \left| \begin{vmatrix} m - 2 & \dots & m - 2\overline{\sigma^{-1}} & \dots \\ \vdots & & \vdots & \\ m - 2\bar{k} & \dots & m - 2\overline{k\sigma^{-1}} & \dots \\ \vdots & & \vdots & \end{vmatrix} \right| .$$

Let us consider a mapping $f : \Xi \to \Xi$, defined in this way:

$$f(x) = \begin{cases} x^{-1} & \text{if } x^{-1} \in \Xi, \\ jx^{-1} & \text{if } x^{-1} \notin \Xi. \end{cases}$$

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

$$\varDelta = \frac{w}{(2m)^N} \cdot \left| \begin{vmatrix} m - 2 & \dots & m - \overline{2(f(\sigma))^{-1}} & \dots \\ \vdots & & \vdots & \\ m - 2\bar{k} & \dots & m - \overline{2k(f(\sigma))^{-1}} & \dots \\ \vdots & & \vdots & \end{vmatrix} \right| =$$

(4.1)

$$= \frac{w}{(2m)^N} \cdot \left| \begin{vmatrix} m - 2 & \dots & m - 2\bar{\sigma} & \dots \\ \vdots & & \vdots & \\ m - 2\bar{k} & \dots & m - 2\overline{k\sigma} & \dots \\ \vdots & & \vdots & \end{vmatrix} \right|.$$

Let

$$A = (m - 2\overline{k\sigma})_{k,\sigma \in \Xi}, \qquad C = (\chi(k))_{\chi \in X^-, k \in \Xi},$$

$$D = C \cdot A = (d_{\chi,\sigma})_{\chi \in X^-, \sigma \in \Xi}.$$

Then

$$d_{\chi,\sigma} = \sum_{k \in \Xi} \chi(k) \cdot (\overline{jk\sigma} - \overline{k\sigma}) = \sum_{k \in G - \Xi} \chi(jk)\, \overline{k\sigma} - \sum_{k \in \Xi} \chi(k)\, \overline{k\sigma} = -\sum_{k \in G} \chi(k)\, \overline{k\sigma} =$$

$$= -\sum_{k \in G} \chi(k\sigma^{-1})\, \bar{k} = -(\chi(\sigma))^{-1} \sum_{k \in G} \chi(k)\, \bar{k} = -(\chi(\sigma))^{-1} \cdot F_\chi.$$

In the following lines a vinculum denotes a complex conjugation.

$$| \det D | = | \det (-\overline{\chi(\sigma)} \cdot F_\chi)_{\chi \in X^-, \sigma \in \Xi} | =$$

$$= | \prod_{\chi \in X^-} F_\chi | \cdot | \det (\overline{\chi(\sigma)})_{\chi \in X^-, \sigma \in \Xi} | =$$

(4.2)
$$= | \prod_{\chi \in X^-} F_\chi | \cdot | \overline{\det (\chi(\sigma))_{\chi \in X^-, \sigma \in \Xi}} | =$$

$$= | \prod_{\chi \in X^-} F_\chi | \cdot | \det C | = | \det C | \cdot | \det A |.$$

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

$$\sum_{\chi \in X^-} c_\chi \chi(k) = 0$$

for any $k \in \Xi$. The same fact holds also for any $k \in G - \Xi$:

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

because $jk \in \Xi$. Hence, the characters χ, $\chi \in X^-$ 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)

$$| \det A | = | \prod_{\chi \in X^-} F_\chi |.$$

Consequently, by substitution to (4.1)

(4.3)
$$\varDelta = \frac{w}{(2m)^N} \cdot | \prod_{\chi \in X^-} F_\chi |.$$

Let us consider, that

$$G \cong Z_m^x$$

(this isomorphism assigns to $\sigma \in G$ the class containing $\bar{\sigma}$). If χ is any character of G, we denote also by χ the Dirichlet character modulo m associated to χ 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

$$F_\chi = \sum_{k \in G} \chi(k)\, \bar{k} = \sum_{i=1}^{m} \chi(i)\, i$$

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 χ^* denotes the primitive character inducing χ, $f(\chi)$ 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]):

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

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

$$\begin{aligned} \Delta &= w \left| \prod_{\chi \in X^-} \frac{1}{2m} F_\chi \right| = \\ &= w \left| \prod_{\chi \in X^-} \left(\frac{1}{2f(\chi)} \sum_{i=1}^{f(\chi)} \chi^*(i)\, i\right) \prod_{p|m} (1 - \chi^*(p)) \right| = \\ &= \frac{1}{Q} h^- \prod_{\chi \in X^-} \prod_{p|m} |1 - \chi^*(p)|. \end{aligned} \tag{4.6}$$

4.1. Theorem. *The group R^-/I^- is finite if and only if s_i is even and*

$$p_i^{\frac{s_i}{2}} \equiv -1 (\mathrm{mod}\, m_i)$$

for each $i = 1, \ldots, r$, or if $r = 1$.

Proof. If $r = 1$, then $m = p_1^{\alpha_1}$ 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^-/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 χ 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 $Z^x_{m_i}$ generated by p_i.

Indeed, if $\chi^*(p_i) = 1$ for an odd character χ modulo m, then $p_i \nmid f(\chi)$ and χ is induced by any character χ' modulo m_i. Since $\chi'(p_i) = 1$, the character χ' 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 χ' 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 $Z^x_{m_i}$ is 2 and it implies that $\chi'(-1)$ is 1 or —1. Let χ be the character modulo m induced by χ'. 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

$$p_i^{\frac{si}{2}} \equiv -1 (\operatorname{mod} m_i),$$

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

$$p_i^{\frac{si}{2}} \equiv -1 (\operatorname{mod} m_i),$$

(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^-/I^- is finite, then*

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

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^-/I^- is finite, then

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

If $r = 1$ then by (4.7)

$$\Delta = h^- = 2^b \,.\, h^-.$$

Hereafter let us suppose, that $r \geq 2$. For $l \in Z$ 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 $\chi \in X^-_{l_1 l_2}$ there exist the unique characters χ_1, χ_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

$$\chi(y) = \chi_1(y) \cdot \chi_2(y)$$

for any integer y. Besides that,

$$\chi^*(y) = \chi_1^*(y) \cdot \chi_2^*(y)$$

for any integer y, too. Hence

$$\prod_{i=1}^{r} \prod_{\chi \in X^-} |1 - \chi^*(p_i)| =$$

$$= \prod_{i=1}^{r} \Big(\prod_{\chi_1 \in X^-_{q_i}} \prod_{\chi_2 \in X^+_{m_i}} |1 - \chi_1^*(p_i)\chi_2^*(p_i)|\Big)\Big(\prod_{\chi_1 \in X^+_{q_i}} \prod_{\chi_2 \in X^-_{m_i}} |1 - \chi_1^*(p_i)\chi_2^*(p_i)|\Big)$$

where $q_i = p_i^{\alpha_i}$. Let us notice that $\chi_2^*(p_i) = \chi_2(p_i)$, because $p_i \nmid m_i$. If $p_i \mid f(\chi_1)$ then $\chi_1^*(p_i) = 0$. Moreover $p_i \mid f(\chi_1)$ if and only of χ_1 is not the unit character. Consequently

$$\prod_{i=1}^{r} \prod_{\chi \in X^-} |1 - \chi^*(p_i)| = \prod_{i=1}^{r} \prod_{\chi \in X^-_{m_i}} |1 - \chi(p_i)|. \tag{4.8}$$

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

$$1 - \chi(p_i) = \exp\Big(-\sum_{n=1}^{\infty} \frac{(\chi(p_i))^n}{n}\Big).$$

By (4.6) with the help of (4.8)

$$\begin{aligned}
\Delta &= \frac{1}{2} h^- \prod_{i=1}^{r} \prod_{\chi \in X^-_{m_i}} \Big| \exp\Big(-\sum_{n=1}^{\infty} \frac{\chi(p_i^n)}{n}\Big)\Big| = \\
&= \frac{1}{2} h^- \prod_{i=1}^{r} \Big| \exp\Big(-\sum_{\chi \in X^-_{m_i}} \sum_{n=1}^{\infty} \frac{\chi(p_i^n)}{n}\Big)\Big| = \\
&= \frac{1}{2} h^- \prod_{i=1} \Big| \exp\Big(-\sum_{n=1}^{\infty} \frac{1}{n} \sum_{\chi \in X^-_{m_i}} \chi(p_i^n)\Big)\Big|.
\end{aligned} \tag{4.9}$$

It is easy to show

$$\sum_{\chi \in X_{m_i}^-} \chi(a) = \begin{cases} \frac{1}{2}\varphi(m_i) & \text{if } a \equiv \ \ 1 (\mathrm{mod}\ m_i), \\ -\frac{1}{2}\varphi(m_i) & \text{if } a \equiv -1 (\mathrm{mod}\ m_i), \\ 0 & \text{otherwise.} \end{cases}$$

By the proof of the theorem 4.1,

$$p_i^n \equiv 1 \ (\mathrm{mod}\ m_i)$$

if and only if

$$n \equiv 0 \ (\mathrm{mod}\ s_i)$$

and

$$p_i^n \equiv -1 \ (\mathrm{mod}\ m_i)$$

if and only if

$$n \equiv \frac{s_i}{2} (\mathrm{mod}\ s_i).$$

Thus

$$\sum_{n=1}^{\infty} \frac{1}{n} \sum_{\chi \in X_{m_i}^-} \chi(p_i^n) = \sum_{t=1}^{\infty} \frac{1}{t\frac{s_i}{2}} (-1)^t \frac{\varphi(m_i)}{2} =$$

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

By (4.9),

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

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

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 $I^- \subseteq S^-$. 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

$$Z_{m_i}^x \cong \prod_{\substack{k=1,\dots,r \\ k \neq i}} Z_{q_k}^x,$$

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

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

Consequently

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

and then

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

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

REFERENCES

[1] Z. I. Borevich and I. R. Shafarevich, *Number theory*, New York 1966.

[2] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin 1952.

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

[4] W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. 108 (1978), 107–134.

[5] L. Skula, *Another proof of Iwasawa's class number formula*, Acta Aritmetica 39 (1981), 1–6.

[6] B. L. van der Waerden, *Algebra 1*, Springer-Verlag Berlin Heidelberg New York 1971.

[7] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag New York Heidelberg Berlin 1982.

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