Ladislav Skula
On certain ideals of the group ring $\mathbb{Z}[G]$
ON CERTAIN IDEALS OF THE GROUP RING $\mathbb{Z}[G]$

LADISLAV SKULA, (Brno)
(Received March 3, 1978)

0. INTRODUCTION

This paper deals with certain ideals $\mathfrak{I}, \mathfrak{I}_m$ of the group ring $\mathfrak{A} = \mathbb{Z}[G]$ of the cyclic group $G$ of order $l - 1$ ($l$ an odd prime) over the ring $\mathbb{Z}$ of integers and especially the inclusion $\mathfrak{I} \subseteq \mathfrak{I}_m$. An equivalent condition for this inclusion is given by means of Bernoulli numbers (Theorem 3.4).

The ground of the study of these questions is the class group of the $l^{th}$ cyclotomic field. The elements of $\mathbb{Z}[G]$ act on this group and the elements of the ideal $\mathfrak{I}$ act trivially here. On the irregular class group of the $l^{th}$ cyclotomic field there act the elements of the group ring $\mathfrak{A} = \mathbb{Z}[G]$, where $\mathbb{Z}$ is the ring of $l$-adic integers. A great meaning for this irregular class group has the subring $\mathfrak{A}^-$ of $\mathfrak{A}$ and the ideal $\mathfrak{I}^-$ of $\mathfrak{A}^-$ which is derived from the ideal $\mathfrak{I}$. An important role is played by the Iwasawa's class number formula ([3]) expressing the first factor of the $l^{th}$ cyclotomic field as a group index of certain additive group $\mathfrak{A}^-$ in $\mathfrak{A}$ and the group $\mathfrak{I}^- = \mathfrak{I} \cap \mathfrak{A}^-$. Iwasawa proved this result in a more general form, for the $l^{n+1}$th cyclotomic fields ($n \geq 0$). But we attend only to the case $n = 0$ in this paper.

In the 4th paragraph we deal with the group $\mathfrak{A}^-/\mathfrak{I}^-$ which is expressed as a direct sum of cyclic groups with special properties (Theorem 4.5 and 4.6).

In the 5th paragraph Theorem 5.3 gives some equivalent conditions for the $\mathfrak{A}$-group $H^-$ to be generated by a single element (over $\mathfrak{A}$), where $H^-$ means the so called "imaginary irregular class group" of the $l^{th}$ cyclotomic field.

1. NOTATION AND BASIC ASSERTIONS

In this paper we designate by

- $l$ an odd prime number
- $\mathbb{Z}$ the ring of integers
- $\mathbb{Z}$ the ring of $l$-adic integers
a primitive root modulo \( l^n \) for each positive integer \( n \)

the integer \( (i \in \mathbb{Z}), 0 < r_i < l \),

\[ r_i \equiv r_i^i \pmod{l} \] for \( i \geq 0 \)

\[ r_i^{p-i} \equiv 1 \pmod{l} \] for \( i < 0 \)

\( G \) a multiplicative cyclic group of order \( l - 1 \)

\( s \) a generator of \( G \), hence \( G = \{1 = s^0, s, s^2, \ldots, s^{l-2}\} \)

\[ \sum_{i=0}^{l-2} \delta_i = \sum_{i=0}^{l-2} \delta_i \] for suitable symbols \( \delta_i \)

\[ \sum_{i \in \mathbb{S}} \delta_i = 0 \] for suitable symbols \( \delta_i \) and \( \mathbb{S} = \emptyset \)

\( \mathbb{R} = \mathbb{Z}[G] \) the group ring of \( G \) over \( \mathbb{Z} \),

thus \( \mathbb{R} = \{ \sum a_i s^i : a_i \in \mathbb{Z} \} \)

\( \overline{\mathbb{R}} = \mathbb{Z}[G] \) the group ring of \( G \) over \( \mathbb{Z} \),

thus \( \overline{\mathbb{R}} = \{ \sum a_i s^i : a_i \in \mathbb{Z} \} \)

\( \mathbb{I} = \{ \alpha \in \mathbb{R} : \exists \ \varrho \in \mathbb{R}, \ \varrho \sum_{i} r_{-i} s^i = l \alpha \} \)

\[ = \{ \sum a_i s^i : a_i = \frac{1}{l} \sum x_i r_{-i+1}, x_i \in \mathbb{Z}, \sum x_i r_i \equiv 0 \pmod{l} \} \]

\( \overline{\mathbb{I}} = \{ \alpha \in \overline{\mathbb{R}} : \exists \ \varrho \in \overline{\mathbb{R}}, \ \varrho \sum_{i} r_{-i} s^i = l \alpha \} \)

\[ = \{ \sum a_i s^i : a_i = \frac{1}{l} \sum x_i r_{-i+1}, x_i \in \overline{\mathbb{Z}}, \sum x_i r_i \equiv 0 \pmod{l} \} \]

\( \mathbb{R}^- = \{ \alpha \in \mathbb{R} : (1 + s^{\frac{1}{2}}) \alpha = 0 \} \)

\[ = \{ \sum a_i s^i : a_i \in \mathbb{Z}, a_i + a_i + a_i = 0 \text{ for } 0 \leq i \leq \frac{l-3}{2} \} \]

\( \overline{\mathbb{R}}^- = \{ \alpha \in \overline{\mathbb{R}} : (1 + s^{\frac{1}{2}}) \alpha = 0 \} = \)

\[ = \{ \sum a_i s^i : a_i \in \overline{\mathbb{Z}}, a_i + a_i + a_i = 0 \text{ for } 0 \leq i \leq \frac{l-3}{2} \} \]

\( \mathbb{I}^- = \mathbb{I} \cap \mathbb{R}^- \)

\( \overline{\mathbb{I}}^- = \overline{\mathbb{I}} \cap \overline{\mathbb{R}}^- \)

\( m \) a positive integer,

\( T \) an integer, \( 0 \leq T < l - 1 \)

\( \lambda = r^{T_m-1} \)

\( \mathbb{I} = \mathbb{I}_T = \mathbb{I}_{T_m} = \{ \sum a_i s^i : a_i \in \mathbb{Z}, \sum a_i \lambda^i \equiv 0 \pmod{l^m} \} \)

\( \overline{\mathbb{I}} = \overline{\mathbb{I}}_T = \overline{\mathbb{I}}_{T_m} = \{ \sum a_i s^i : a_i \in \overline{\mathbb{Z}}, \sum a_i \lambda^i \equiv 0 \pmod{l^m} \} \)

\( \mathbb{I}^- = \mathbb{I}^- = \mathbb{I} \cap \mathbb{R}^- \)

54
\[ \mathfrak{J} = \mathfrak{J}_T = \mathfrak{J}_{Tm} = \mathfrak{J} \cap \mathfrak{R}^- \]

the first factor of the class number of the \( l \)th cyclotomic field over the rational field

\[ h^- = l^a, \quad \text{where} \quad h^- = l^a \cdot d, \quad a, \quad d \quad \text{non-negative integers}, \quad l \not\equiv d \]

Obviously, \( \mathfrak{R}^-, \mathfrak{J}, \mathfrak{J}, \mathfrak{J}^-, \mathfrak{J}^- \) are ideals in \( \mathfrak{R} \) and \( \mathfrak{R}^-, \mathfrak{J}, \mathfrak{J}, \mathfrak{J}^-, \mathfrak{J}^- \) are ideals in \( \mathfrak{R}^- \).

We consider these ideals (together with \( \mathfrak{R} \) and \( \mathfrak{R}^- \)) additive groups, sometimes \( \mathfrak{R}^- \) or \( \mathfrak{R}^- \) groups and the symbol \([ \mathcal{G} : \mathcal{H} ]\) denotes the group index for a group \( \mathcal{G} \) and its normal subgroup \( \mathcal{H} \).

**1.1. Theorem (Iwasawa [3]).**

\[ h^- = [\mathfrak{R} : \mathfrak{J}^-], \quad h^- = [\mathfrak{R}^- : \mathfrak{J}^-]. \]

For the sequence of Bernoulli numbers \( B_n \) we use the "even-index" notation, thus

\[ B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_3 = 0, \quad B_4 = -\frac{1}{30}, \ldots, \]

and we shall use their basic properties mentioned in the book [1].

By \( \mathcal{F} \) we denote the set of all odd integers \( T, \; 1 \leq T \leq l - 4 \) such that \( B_{T + 1} \equiv 0 \pmod{l} \). It is well known that for each \( T \in \mathcal{F} \) there exists a positive integer \( h(T) \) such that

\[ B_{h(T) - 1} \equiv 0 \pmod{l^{h(T)}} \]

and for integer \( X > h(T) \)

\[ B_{X - 1} \not\equiv 0 \pmod{l^X} \]

is satisfied.

**1.2. Theorem (Pollaczek [4], Satz IX).**

\[ a = \sum h(T) \quad (T \in \mathcal{F}). \]

2. **THE IDEALS \( \mathfrak{J} \)**

The following Proposition is easy to see.

**2.1. Proposition.**

\[ \mathfrak{J} = \mathfrak{J} \cap \mathfrak{R}, \quad \mathfrak{J}^- = \mathfrak{J} \cap \mathfrak{R}^- = \mathfrak{J}^- \cap \mathfrak{R}^- = \mathfrak{J}^- \cap \mathfrak{R}. \]

**2.2. Proposition.** The following statements are equivalent:

(a) \( \mathfrak{I} \subseteq \mathfrak{J} \),
(b) \( \bar{\mathfrak{I}} \subseteq \mathfrak{J} \).

55
If $T$ is odd, then we can add the statements:

(c) $\mathcal{S}^- \subseteq \mathcal{S}^-$,
(d) $\mathcal{S}^- \subseteq \mathcal{S}^-$.  

Proof. I. Let (a) hold and let $a \in \mathcal{S}$. Then there exist $x_t \in \mathbb{Z}$ such that $\sum x_t r_t \equiv 0 \pmod{l}$ and $a = \sum a_t s^t$, where $a_t = \frac{1}{l} \sum x_t r_{t-i}$. Put $b_t = \frac{1}{l} \sum y_t r_{t-i}$, $\beta = \sum b_t s^t$, where $y_t \in \mathbb{Z}$, $y_t \equiv x_t \pmod{l^{m+1}}$. Then $\beta \in \mathcal{S}$ and $b_t \equiv a_t \pmod{l^m}$. Therefore $\beta \in \mathcal{S}$ and $0 \equiv \sum b_t \lambda^t \equiv \sum a_t \lambda^t \pmod{l^m}$. Thus $\alpha \in \mathcal{S}$ and the implication (a) $\rightarrow$ (b) holds.

If (b) holds, then according to 2.1 we obtain $\mathcal{S} \subseteq \mathcal{S} \cap \mathcal{R} \subseteq \mathcal{S} \cap \mathcal{R} = \mathcal{S}$. The statements (a) and (b) are equivalent.

II. The implication (b) $\rightarrow$ (d) follows directly from the definition.

If (d) holds, then according to 2.1, $\mathcal{S}^- \subseteq \mathcal{S}^- \cap \mathcal{R}^- \subseteq \mathcal{S}^- \cap \mathcal{R}^- = \mathcal{S}^-$ which gives the implication (d) $\rightarrow$ (c).

III. Let $T$ be odd, $\mathcal{S}^- \subseteq \mathcal{S}^-$ and $a = \sum a_t s^t \in \mathcal{S}$ ($a_t \in \mathbb{Z}$). Then there exist integers $x_t$ such that $\sum x_t r_t \equiv 0 \pmod{l}$ and $a_t = \frac{1}{l} \sum x_t r_{t-i}$. Put

$$y_t = \begin{cases} x_t - x_{t+1} - 1 \frac{1}{2} & \text{for } 0 \leq t < \frac{l-1}{2} \\ x_t - x_{t-1} - 1 \frac{1}{2} & \text{for } \frac{l-1}{2} \leq t \leq l - 2. \end{cases}$$

Then $\sum y_t r_t = \sum x_t r_t - \sum x_t r_{t-1} \equiv 0 \pmod{l}$.

If we put $b_t = \frac{1}{l} \sum y_t r_{t-i}$ and $\beta = \sum b_t s^t$, we get $\beta \in \mathcal{S}$ and

$$b_t = \begin{cases} a_t - a_{i+1} - 1 \frac{1}{2} & \text{for } 0 \leq i < \frac{l-1}{2} \\ a_t - a_{i-1} - 1 \frac{1}{2} & \text{for } \frac{l-1}{2} \leq i \leq l - 2. \end{cases}$$

From this we have $\beta \in \mathcal{S}^-$ and according to the supposition $\beta \in \mathcal{S}^-$, hence $0 \equiv \sum b_t \lambda^t \equiv 2 \sum a_t \lambda^t \pmod{l^m}$, whence we get $\alpha \in \mathcal{S}$. The implication (c) $\rightarrow$ (a) is proved.

2.3. Proposition. For even $T$ the equalities

$$\mathcal{S}^- = \mathcal{R}^-, \quad \overline{\mathcal{S}^-} = \overline{\mathcal{R}^-}$$

are satisfied.
Proof. Let \( \alpha = \sum_{t} a_t s^t \in \mathfrak{R}^-, \mathfrak{R}^- (a_t \in \mathbb{Z}, a_t \in \overline{\mathbb{Z}}) \) respectively. Then \( a_t + a_{t+\frac{i-1}{2}} = 0 \) for \( 0 \leq i < \frac{l-1}{2} \) and according to the relation \( \lambda_i \equiv \lambda_{i+\frac{i-1}{2}} \) (mod \( l^m \)), \( 0 \leq i \leq l-2 \), we get 0 = \( \sum_{i=0}^{l-3} (a_t + a_{i+\frac{i-1}{2}}) \lambda_i \equiv \sum_{i} a_i \lambda_i \) (mod \( l^m \)), thus \( x \in \mathfrak{F}^-, x \in \overline{\mathfrak{F}}^- \), respectively.

2.4. Lemma The following statements are equivalent:

(a) \( \mathfrak{F} \subseteq \mathfrak{F}^- \),

(b) \( \sum_i (r_{-i+t} - r_{-i-t}) \lambda_i \equiv 0 \) (mod \( l^{m+1} \)) for each \( t \in \mathbb{Z} \).

Proof. Let \( x_t \in \mathbb{Z} \) (0 \( \leq t \leq l-2 \)), \( \sum_i x_t r_i \equiv 0 \) (mod \( l \)), \( a_i = \frac{1}{l} \sum_i x_t r_{-i+t} \) (0 \( \leq i \leq l-2 \)). Then there exists an integer \( y \) such that

\[ x_0 = -\sum_{i=1}^{l-2} x_t r_i + ly. \]

From this we obtain

\[ \sum_i a_i \lambda_i = y \sum_i r_{-i} \lambda_i + \frac{1}{l} \sum_i x_t \sum_i (r_{-i+t} - r_{-i-t}) \lambda_i. \]

If (b) holds, then \( T \neq 0 \), since otherwise for \( T = 0 \) we have \( \sum_i (r_{-i+t} - r_{-i-t}) \lambda_i = \sum_i (r_{-i+t} - r_{-i-t}) = \frac{l(l-1)}{2} (1 - r_t) \). It holds \( l \sum_i r_{-i} \lambda_i \equiv \sum_i (l r_{-i} - 1) \lambda_i = \sum_i (r_{-i} r_{i-1} - r_{-i+t-1}) \lambda_i \equiv 0 \) (mod \( l^{m+1} \)), hence \( \sum_i a_i \lambda_i \equiv 0 \) (mod \( l^m \)) and \( \alpha = \sum_i a_i s^i \in \mathfrak{F}^- \).

If (a) is satisfied, we put \( x_0 = -r_t, x_t = 1 \) and \( x_t = 0 \) (1 \( \leq t \leq l-2, t \neq \tau \)), where \( 1 \leq \tau \leq l-2 \). Since \( \alpha = \sum_i a_i s^i \in \mathfrak{F}^- \), we have \( x \in \mathfrak{F}^- \) and according to \( y = 0 \) we obtain

\[ \sum_i (r_{-i+t} - r_{-i-t}) \lambda_i = l \sum_i a_i \lambda_i \equiv 0 \) (mod \( l^{m+1} \)).

The Lemma is proved.

2.5. Consequence. For \( T = 0 \) and \( T = 1 \) the relation \( \mathfrak{F} \not\subseteq \mathfrak{F}^- \)
is satisfied.
Proof. If $T = 0$, then by the proof of 2.4 we have $\sum_i (r_{-i+t} - r_{-i}r_i) \lambda^i \not\equiv 0 \pmod{l^{m+1}}$ for $t \not\equiv 0 \pmod{l - 1}$. From 2.4 it follows that $\mathfrak{I} \not\subset \mathfrak{J}$.

If $T = 1$, then for $t = \frac{l-1}{2}$ we have

$\sum_i (r_{-i+t} - r_{-i}r_i) \lambda^i = \sum_i (1 - r_{-i}) r^{il^{-1}} \equiv -\sum_i r_{-i} r^i \pmod{l} = -(l - 1)$.

Then from 2.4 we obtain the relation $\mathfrak{I} \not\subset \mathfrak{J}$.

3. THE INCLUSION $\mathfrak{I} \subset \mathfrak{J}$ AND BERNOULLI NUMBERS

In this paragraph we designate by

$$c = l^{m-1}(l - T - 1) + 1$$
$$s = 1^c + 2^c + \ldots + (l - 1)^c.$$

3.1. Lemma. If $k$ is an integer, then

(a) $\binom{c}{k} l^k \equiv 0 \pmod{l^{m+1}}$ for $2 \leq k \leq c$,

(b) $\binom{c - 1}{k} l^k \equiv 0 \pmod{l^m}$ for $1 \leq k \leq c - 1$,

(c) $\binom{c + 1}{k} l^{c+1-k} \equiv 0 \pmod{l^{m+2}}$ for $0 \leq k \leq c - 2$ and $l > 3$.

Proof. For $m = 1$ the assertion is clear. Let $m > 1$ and let $v$ be the $l$-adic exponent.

Put $\alpha = \binom{c}{k} l^k$, $\beta = \binom{c - 1}{k} l^k$, $\gamma = \binom{c + 1}{k} l^{c+1-k}$, where $k$ is an integer in bounds from (a) – (c). We can also suppose $k \leq c - 2$. Further put

$$x = v(c - k) + v(c - k - 1),$$
$$y = v(c - k - 1),$$
$$z = v(c - k - 1) + v(c - k) + v(c + k).$$

It holds

$$\binom{c}{k} = \binom{c - 2}{k} \frac{c(c-1)}{(c-k-1)(c-k)},$$
$$\binom{c - 1}{k} = \binom{c - 2}{k} \frac{c-1}{c-k-1},$$
$$\binom{c + 1}{k} = \binom{c - 2}{k} \frac{(c+1)c(c-1)}{(c-k-1)(c-k)(c-k+1)}.$$
whence we obtain

\[ v(\alpha) \geq m - 1 + k - x, \]
\[ v(\beta) \geq m - 1 + k - y, \]
\[ v(\gamma) \geq m + c - k - z. \]

If \( x = 0 \) (\( y = 0, z = 0 \)), then (a) ((b), (c)) is satisfied.

a) If \( x \geq 1 \), then \( k = l^x \cdot X + \epsilon \), where \( X \) is a positive integer, \( l \nmid X \) and \( \epsilon = 0 \) or \( \epsilon = 1 \). Then \( v(\alpha) \geq m - 1 + 3^x - x \geq m + 1 \).

b) If \( y \geq 1 \), then \( k = l^y \cdot X \), where \( X \) is a positive integer, \( l \nmid X \). Then \( v(\beta) \geq m - 1 + 3^y - y \geq m + 1 \).

c) If \( z \geq 1 \), then \( k = l^z \cdot X + \epsilon \), where \( X \) is a positive integer, \( l \nmid X \) or \( X = 0 \) and \( \epsilon = 0, 1, 2 \). Then for \( l \geq 5 \) we obtain \( c - k \geq 5^z - 1 \), thus \( v(\gamma) \geq m + 5^z - 1 - z > m + 2 \).

The Lemma is proved.

3.2. Lemma. If \( t \) is an integer, then

\[ s(1 - r_i) \equiv cr_t^{c-1} \sum_i (r_{i+t} - r_i) \lambda^i (\text{mod } l^{m+1}). \]

Proof. For any integer \( i(0 \leq i \leq l - 2) \) there exists an integer \( u \) such that

\[ r_{-i} = r^{l-1-i} + lu. \]

By 3.1(b) we have

\[ r_{-i}^{-1} \equiv r^{(l-1-i)(c-1)} (\text{mod } l^m). \]

Since \((l - 1 - i)(c - 1) = (l - 1 - i)l^{m-1}(l - T - 1) \equiv iTl^{m-1}(\text{mod } l^{m-1}(l - 1))\),

we get

\[ r_{-i}^{-1} \equiv \lambda^i (\text{mod } l^m). \]

For \( i, t \in \mathbb{Z} \) we have

\[ r_{-i+t} = r_{-i}r_t + l \frac{r_{-i+t} - r_{-i}r_t}{l}, \]

from which, according to 3.1(a), it follows that

\[ r_{-i+t}^{-1} = r_{-i}^{-1}r_t^{-1} + cr_t^{c-1}lr_{-i}^{-1} \frac{r_{-i+t} - r_{-i}r_t}{l} (\text{mod } l^{m+1}). \]

Thus we get for each \( t \in \mathbb{Z} \)

\[ s(1 - r_i) = \sum_i r_{-i+t}^{-1} - \sum_i r_{-i}^{-1}r_t^{-1} \equiv cr_t^{c-1} \sum_i l\lambda^i \frac{r_{-i+t} - r_{-i}r_t}{l} (\text{mod } l^{m+1}) = cr_t^{c-1} \sum_i (r_{-i+t} - r_{-i}r_t) (\text{mod } l^{m+1}). \]

Thus, the Lemma is proved.
3.3. Remark. The proof of Lemma 3.2 is realized according to the model of Pollaczek [4], proof of Satz VIII).

3.4. Theorem. For \( T = 0 \) and \( T = 1 \) the relation \( \mathcal{I} \subseteq \mathcal{I}_{Tm} \) is satisfied.

If \( T \neq 0 \), \( T \neq 1 \), then for \( T \) odd it holds

\[
\mathcal{I} \subseteq \mathcal{I}_{Tm} \Leftrightarrow B_{m-1(1-T-1)+1} \equiv 0 \pmod{l^m},
\]

for \( T \) even and \( m > 1 \) it holds

\[
\mathcal{I} \subseteq \mathcal{I}_{Tm} \Leftrightarrow B_{m-1(1-T-1)} \equiv 0 \pmod{l^{m-1}}
\]

and for \( T \) even and \( m = 1 \) the inclusion

\[
\mathcal{I} \subseteq \mathcal{I}_{Tm} = \mathcal{I}_{T1}
\]

is satisfied.

Proof. By 2.5 \( \mathcal{I} \subseteq \mathcal{I}_{Tm} \) for \( T = 0 \) and \( T = 1 \). Let \( 0 \neq T \neq 1 \). Then \( 2 \leq T \leq l - 2 \) and \( l > 3 \). According to 2.4 and 3.2 the relation \( \mathcal{I} \subseteq \mathcal{I}_{Tm} \) is equivalent to the relation \( s \equiv 0 \pmod{l^{m+1}} \). Using 3.1(c), we see that

\[
(c + 1)s = \sum_{k=0}^{c} \binom{c + 1}{k} B_k l^{c+1-k} \equiv \\
= \binom{c + 1}{c - 1} B_{c+1} l^2 + \binom{c + 1}{c} B_c l \pmod{l^{m+1}} = \frac{(c + 1)c}{2} B_{c-1} l^2 + (c + 1) B_c l,
\]

thus

\[
s \equiv \frac{c}{2} l^2 B_{c-1} + l B_c \pmod{l^{m+1}}.
\]

Since \( c, c - 1 \not\equiv 0 \pmod{l - 1} \), \( B_c, B_{c-1} \) are \( l \)-integers.

In case \( c = 2 \) we have \( m = 1 \), \( T = l - 2 \), \( s \equiv \frac{1}{6} (1 - 3l) \not\equiv 0 \pmod{l^{m+1}} \) and \( B_{m-1(1-T-1)+1} = B_2 \equiv 0 \pmod{l^{m+1}} \).

If \( c > 2 \), we have, in case \( T \) is odd, \( s \equiv l B_c \pmod{l^{m+1}} \), and in case \( T \) is even, we get \( s \equiv \frac{c}{2} l^2 B_{c-1} \pmod{l^{m+1}} \).

It follows the Theorem.

4. THE GROUP \( \mathcal{R}^-/\mathcal{I}^- \)

4.1. Proposition. The groups \( \mathcal{R}/\mathcal{I}_{Tm}, \mathcal{R}^—/\mathcal{I}_{Tm} \) are cyclic groups of order \( l^m \).

If \( T \) is odd, the groups \( \mathcal{R}^-/\mathcal{I}_{Tm}^- \), \( \mathcal{R}^-/\mathcal{I}_{Tm}^- \) are cyclic groups of order \( l^m \) and if \( T \) is even, the groups are trivial.
For each element $A$ of these groups ($A \in \mathcal{H}/\mathcal{I}_{T_m} \cup \overline{\mathcal{H}}/\mathcal{I}_{T_m} \cup \mathcal{H}-/\mathcal{I}_{T_m} \cup \overline{\mathcal{H}}-/\overline{\mathcal{I}}_{T_m}$)

$$s(A) = r^{T_m-1}A$$

is valid.

Proof. We can easily see that $\{0, 1, 2, ..., l^m - 1\}$ is a complete system of representatives $\mathcal{H}/\mathcal{I}_{T_m}$ and $\overline{\mathcal{H}}/\mathcal{I}_{T_m}$.

In case $T$ is even we get from 2.3 that the groups $\mathcal{H}/\mathcal{I}_{T_m}$ and $\overline{\mathcal{H}}/\mathcal{I}_{T_m}$ are trivial.

If $T$ is odd, then $\{x(1 - s^{-\frac{1}{2}}) : x = 0, 1, 2, ..., l^m - 1\}$ is a complete system of representatives $\mathcal{H}/\mathcal{I}_{T_m}$ and $\overline{\mathcal{H}}/\overline{\mathcal{I}}_{T_m}$.

Since $r^{T_m-1} - s \in \mathcal{I}_{T_m}$, we have $s(A) = r^{T_m-1}A$ for each element $A$ of given factor groups.

Thus, the proposition is proved.

From 4.1 we immediately get

4.2. Proposition. $\mathcal{I}_{T_m} \cong \mathcal{I}_{T_m+1}$, $\overline{\mathcal{I}}_{T_m} \cong \overline{\mathcal{I}}_{T_m+1}$ and in case $T$ is odd

$$\mathcal{I}_{T_m} \cong \mathcal{I}_{T_m+1}, \overline{\mathcal{I}}_{T_m} \cong \overline{\mathcal{I}}_{T_m+1}.$$

4.3. Lemma. Let $m(T)$ be a positive integer for each $1 \leq T \leq l - 2$, $T$ odd. Then

$$\bigcap \mathcal{I}_{T_m(T)}(1 \leq T \leq l - 2, T \text{ odd}, T \neq \tau) + \mathcal{I}_{T_m(T)} = \mathcal{H}^{-}$$

for each odd integer $\tau(1 \neq \tau \leq l - 2)$.

Proof. Let $a \in \mathcal{H}^{-}$, $a = \sum_i a_i\alpha_i^i$ (with $a_i + a_{i+\frac{l-1}{2}} = 0$ for $0 \leq i \leq \frac{l-3}{2}$).

Put $\lambda_T = r^{T_m(T)-1}$ for $1 \leq T \leq l - 2$, $T$ odd. Since $\det(\lambda_T^i)\left(0 \leq i \leq \frac{l-3}{2}, 1 \leq T \leq l - 2, T \text{ odd} \right) = \prod(\lambda_T - \lambda_T)(1 \leq T < T' \leq l - 2; T, T' \text{ odd}) \equiv 0(\text{mod } l)$,

the system of linear equations

$$\frac{l-3}{2} \sum_{i=0} x_i\lambda_T^i = 0 \quad (1 \leq T \leq l - 2, T \text{ odd}, T \neq \tau)$$

$$\frac{l-3}{2} \sum_{i=0} x_i\lambda_T^i = \sum_{i=0} a_i\lambda_T^i$$

has a solution in $l$-adic integers $x_0, x_1, ..., x_{\frac{l-3}{2}}$.

If we put $\beta = \sum_{i=0} x_i\alpha^i(1 - s^{-\frac{i}{2}})$ and $\gamma = \sum_{i=0} (a_i - x_i)\alpha^i(1 - s^{-\frac{i}{2}})$, we have $\beta \in \bigcap \mathcal{I}_{T_m(T)}(1 \leq T \leq l - 2, T \text{ odd}, T \neq \tau), \gamma \in \mathcal{I}_{T_m(T)}$ and $a = \beta + \gamma$. 

61
4.4. Notation. According to the Iwasawa's class number formula (1.1) we have $[\mathfrak{R}^- : \mathfrak{3}^-] = h^-$ and therefore by 4.1 for each odd $T$ there exists a non-negative integer $m(T)$ such that $\mathfrak{3}_{Tm(T)}^- \supseteq \mathfrak{3}^-$ and $\mathfrak{3}_{Tm(T)}^- \not\subseteq \mathfrak{3}^-$, for integer $m > m(T)$, where we define $\mathfrak{3}_{T0}^- = \mathfrak{R}^-$. 

4.5. Theorem. The $\mathfrak{R}$-group $\mathfrak{R}^-/\mathfrak{3}^-$ is $\mathfrak{R}$-isomorph to the direct sum of the $\mathfrak{R}$-groups $\mathfrak{R}^-/\mathfrak{3}_{Tm(T)}^-$ ($T$ odd). For $T$ odd it is satisfied

$$m(T) = \begin{cases} h(l - 1 - T) & \text{for } T \neq 1, B_{l-T} \equiv 0 \pmod{l} \\ 0 & \text{otherwise.} \end{cases}$$

Further, $\mathfrak{3}_{Tm(T)}^- (T$ odd $) = \mathfrak{3}^-$. 

Proof. Let $S$ be the direct sum of the $\mathfrak{R}$-groups $\mathfrak{R}^-/\mathfrak{3}_{Tm(T)}^-$, $T$ odd. For $X = \ldots, X_t, \ldots \in S$ ($\tau$ odd, $1 \leq \tau \leq l - 2$) there exists $a_t \in X_t \cap \mathfrak{3}_{Tm(T)}^-$ ($1 \leq T \leq l - 2$, $T$ odd, $T \neq \tau$) by 4.3. The mapping $X \mapsto \Sigma a_t$ ($\tau$ odd, $1 \leq \tau \leq l - 2$) + $\mathfrak{3}_{Tm(T)}^-$ ($T$ odd, $1 \leq T \leq l - 2$) is an $\mathfrak{R}$-isomorphism of $S$ on the $\mathfrak{R}$-group $\mathfrak{R}^-/\mathfrak{3}_{Tm(T)}^-$, $1 \leq T \leq l - 2$, $T$ odd), which has order $l^n$ by 4.1, where $\mu = \Sigma m(T)$ ($1 \leq T \leq l - 2$, $T$ odd). From 3.4 we get for $T$ odd

$$m(T) = \begin{cases} h(l - 1 - T) & \text{in case } T \neq 1, B_{l-T} \equiv 0 \pmod{l} \\ 0 & \text{otherwise.} \end{cases}$$

From Pollaczek's result 1.2 we obtain that the order of the group $\mathfrak{R}^-/\mathfrak{3}_{Tm(T)}^-$ ($1 \leq T \leq l - 2$, $T$ odd) is equal to $h^-$, which follows the Theorem according to the Iwasawa's formula 1.1.

From 4.5 and 4.1 we obtain

4.6. Theorem. The $\mathfrak{R}$-group $\mathfrak{R}^-/\mathfrak{3}^-$ is a direct sum of $\mathfrak{R}$-groups $\mathfrak{R}_T (T \in \mathcal{T})$, where $\mathfrak{R}_T$ is a cyclic group of order $l^{\mu(T)}$ and for each $X \in \mathfrak{R}_T$

$$s(X) = r^{(l-1-T)} l^{\mu-1} X$$

is valid.

5. THE IRREGULAR CLASS GROUP
OF THE $l$TH CYCLOTOMIC FIELD

We can consider the group $G$ the Galois group of the $l$th cyclotomic field over the rational field, where $s$ is the automorphism fulfilling

$$s(e^{\frac{2\pi i}{l}}) = e^{\frac{2\pi i}{l} \tau}.$$

This automorphism $s$ acts on the divisor class group $\Gamma = (\Gamma, +)$ of the $l$th cyclotomic field in the natural way and so the elements of the group ring $\mathfrak{R} = \mathbf{Z}[G]$ act on $\Gamma$ as homomorphisms.
From Hilbert's "Zahlbericht" ([2], Kapitel XXIV) we obtain the following assertion going back to Kummer.

(1) \( \varphi(\gamma) = 0 \) for \( \varphi \in \mathfrak{J}, \gamma \in \Gamma \).

The \( l \)-Sylow subgroup of the group \( \Gamma \) is said to be the \textit{irregular divisor class group of the \( l \)-th cyclotomic field} and we shall denote it by \( H \).

By Pollaczek ([4], Satz III) the group \( H \) is the direct sum

\[
H = \sum_{i=1}^{n} H_i
\]

of cyclic groups \( H_i \) of orders \( l^{m_i} \) (\( m_i \) are positive integers). We shall denote a generator of \( H_i (1 \leq i \leq n) \) by \( \chi_i \). For each \( 1 \leq i \leq n \) there exists an integer \( T_i, 0 \leq T_i < l - 1 \) such that

(2) \( s(\chi_i) = r^{T_i l^{m_i-1}} \chi_i \).

Using equality \{\( \varphi \in \mathfrak{R} : \varphi(\chi) = 0 \) for each \( \chi \in H_i \)\} = \( \mathcal{J}_{T_i} \), we obtain \( \mathfrak{J} \subseteq \mathcal{J}_{T_i} \) and we get from 3.3:

5.1. Theorem. Let \( 1 \leq i \leq n \). Then \( 0 \neq T_i \neq 1 \).

If \( T_i \) is odd, then \( B_{l^{m_i-1}(l-T_i-1)+1} \equiv 0 \text{(mod } l^{m_i}) \).

If \( T_i \) is even and \( m_i > 1 \), then \( B_{l^{m_i-1}(l-T_i-1)} \equiv 0 \text{(mod } l^{m_i-1}) \).

5.2. Remark. The assertion of 5.1 about odd \( T \)'s is due to Pollaczek ([4], § 6) (see also Remark 3.3).

Put

\( \varnothing = \{ 1 \leq i \leq n : T_i \text{ odd} \} \)

and denote by

\( H^- = \sum_{i \in \varnothing} H_i \)

the direct sum of the groups \( H_i \) \( (i \in \varnothing) \). The subgroup \( H^- \) of \( H \) is said to be the \textit{imaginary irregular divisor class group of the \( l \)-th cyclotomic field}.

The elements of the group ring \( \mathfrak{R} = \mathbb{Z}[G] \) act on the group \( H \) in the natural way and from (1) we get

(3) \( \varphi(\chi) = 0 \) for \( \varphi \in \mathfrak{J}, \chi \in H \).

For \( \chi \in H^- \) set \( \mathfrak{J}_\chi = \{ \varphi \in \mathfrak{R}^- : \varphi(\chi) = 0 \} \).

5.2. Proposition. The following statements are equivalent for \( \omega \in H^- \):

(a) \( \mathfrak{J}_\omega = \{ \varphi \in \mathfrak{R}^- : \varphi(\chi) = 0 \text{ for each } \chi \in H^- \} \),

(b) \( \omega = \sum x_i \chi_i \) \( (i \in \varnothing) \), where \( x_i \) are integers such that for each \( i \in \varnothing \) there exists \( j \in \varnothing \) with the property \( T_i = T_j, m_j \geq m_i \) and \( l \nmid x_j \).
Proof. Obviously, \( S_\omega \supseteq \{ \varphi \in \mathcal{R}^- : \varphi(\chi) = 0 \text{ for each } \chi \in H^- \} \). Let \( 0 < l_i < l^m \) be integers \( (i \in \Theta) \) such that \( \omega = \Sigma x_i \chi_i \) \( (i \in \Theta) \).

I. Let \((b)\) hold and let \( \varphi = \sum a_k s^k \in S_\omega(a_k \in \mathbb{Z}) \). For \( i \in \Theta \) there exists \( j \in \Theta \) such that \( T_i = T_j, \ m_j \geq m_i \) and \( l \nmid x_j \). We have \( x_j \varphi(\chi_j) = 0 \), which follows

\[
\sum_k a_k r^k \prod_{T_i} t_m^{m_j-1} \equiv 0 \pmod{l^{m_j}}, \quad \text{hence} \quad \sum_k a_k r^k \prod_{T_i} t_m^{m_j-1} \equiv 0 \pmod{l^{m_j}}
\]

and consequently \( \varphi(\chi_j) = 0 \). Thus \( \varphi(\chi) = 0 \) for each \( \chi \in H^- \).

II. Let \((b)\) not hold. Then there exists \( j \in \Theta \) such that \( l \nmid x_j \) and \( m_j < m_i \) or \( m_j = m_i \) and \( l \mid x_j \) for \( i \in \Theta, \ T_i = T_j \).

For \( i \in \Theta \) put

\[
\varphi_i = \begin{cases} 
  r^{T_i} t_m^{m_i-1} - s & \text{for } T_i \neq T_j, \\
  r^{T_i} t_m^{m_j-1} + l^{m_j-1} - s & \text{for } T_i = T_j.
\end{cases}
\]

If \( T_i \neq T_j \), we have \( \varphi_i(\chi_i) = 0 \). In the case \( T_i = T_j \) we get \( \varphi_i(\chi_i) = l^{m_j-1} \chi_i \). Put

\[
\varphi = \left(1 - s^{l-1} \right) \Pi \varphi_i, (i \in \Theta) \quad \text{(in the case } \Theta = \emptyset, \Pi \varphi_i (i \in \Theta) = 1). \text{ Then } \varphi(\omega) = 0 \text{ and consequently } \varphi \in S_\omega. \text{ But } \varphi(\chi_j) = 2 \chi_j, \text{ where } y \text{ is an integer, } l \nmid y.
\]

Thus the Proposition is proved.

5.3. Theorem. The following statements are equivalent:

(a) The \( \mathcal{R} \)-group \( H^- \) is \( \mathcal{R} \)-isomorphic to the \( \mathcal{R} \)-group \( \mathcal{R}^- / \mathcal{R}^- \).

(b) The \( \mathcal{R} \)-group \( H^- \) is generated (over \( \mathcal{R} \)) by a single element.

(c) \( \mathcal{R}^- = \{ \varphi \in \mathcal{R}^- : \varphi(\chi) = 0 \text{ for each } \chi \in H^- \} \).

(d) \( 1 \leq i \neq j \leq n \Rightarrow T_i \neq T_j \).

(e) If \( T \) is odd, \( 3 \leq T \leq l - 2 \), and \( m \) is a positive integer such that \( B_{m-1} t_{l-1} = 0 \pmod{l^m} \), then there exists \( 1 \leq i \leq n \) so that \( T = T_i \) and \( m \leq m_i \).

If these conditions are satisfied, then the element \( \Sigma x_i \chi_i \) \( (i \in \Theta) \) \( (x_i \text{ integer}) \) is a generator of \( H^- \) over \( \mathcal{R} \) if an only if \( l \nmid x_i \) for each \( i \in \Theta \).

5.4. Remark. The equivalence of the statements \((a), (b)\) is due to Iwasawa [3], paragraph 4).

Proof of 5.3. I. Let \((d)\) hold. Let \( \emptyset \neq \Theta_0 \subseteq \Theta \) and \( \chi = \Sigma y_i \chi_i \) \( (i \in \Theta_0) \), where \( y_i \) are integers, \( l \nmid y_i \). For \( j \in \Theta_0 \) we have \( s(\chi) = r^{T_i} t_m^{m_j-1} \chi_i = \Sigma y_i (r^{T_i} t_m^{m_j-1} - r^{T_i} t_m^{m_i-1} - r^{T_i} t_m^{m_j-1}) \chi_i \) \( (i \in \Theta_0) = \Sigma z_i \chi_i \) \( (i \in \Theta_0 - \{j\}) \), where \( z_i \) are integers, \( l \nmid z_i \).

It follows that every element \( \omega \in H^- \) of the form \( \omega = \Sigma x_i \chi_i \) \( (i \in \Theta) \), where \( x_i \) are integers, \( l \nmid x_i \), is a generator of \( H^- \) over \( \mathcal{R} \).
Thus, (b) holds.

Let $\omega = \Sigma x_i \chi_i \ (i \in \Theta)$ be a generator of $H^-$ over $\bar{R}$, where $x_i$ are integers and let $1 \leq j < k \leq n$ so that $T_j = T_k$. Then there exist $l$-adic integers $a_u (0 \leq u \leq l - 2)$ such that $\chi_j = \sum_u a_u s^n(\omega)$. Since

$$\chi_j = \sum_u a_u \sum_{i \in \Theta} x_i r^n T_i u m_i - 1 \chi_i = \sum_{i \in \Theta} x_i \chi_i \sum_u a_u r^n T_i u m_i - 1$$

we have

$$1 \equiv x_j \sum_u a_u r^n T_j (\text{mod } l),$$

$$0 \equiv x_k \sum_u a_u r^n T_k (\text{mod } l),$$

consequently $x_k \equiv 0 \ (\text{mod } l)$ and $x_j \not\equiv 0 \ (\text{mod } l)$. On the other hand we can also show the contrary relation, which is a contradiction.

Thus, (d) holds.

The statements (b) and (d) are equivalent and according to 5.2 the assertion about the form of a generator of $H^-$ holds, too.

II. Let $\omega$ be an element of $H^-$ of the form from 5.2 (b). In a similar way as in [3] (p. 177) we put for $\varphi \in \bar{R}^-$

$$f(\varphi) = \varphi(\beta).$$

Obviously, $f$ is an $\bar{R}$-homomorphism from $\bar{R}^-$ to $H^-$ with the kernel $\mathfrak{I}_\omega = \{ \varphi \in \bar{R}^- : \varphi(\chi) = 0 \text{ for each } \chi \in H^- \}$ (by 5.2). For $\varphi = z \left( 1 - s \frac{l - 1}{2} \right)$, where $z$ is an integer such that $2z \equiv 1 \ (\text{mod } l^m) \ (i \in \Theta)$, we have $f(\varphi) = \beta$. The factor group $\bar{R}^\sim / \mathfrak{I}_\omega$ is embedded into the factor group $\bar{R}^\sim / \mathfrak{I}^\sim$ and also into $H^-$. From I, 1.1. and 5.4 we obtain the equivalence of statements (a), (b), (c).

III. For $i \in \Theta$ put $U_i = l - T_i - 1$. According to 3.4 $U_i \in \mathcal{S}$ and $h(U) \geq m_i$, hence $\mathcal{S} \supseteq \{ U_i : i \in \Theta \}$. According to 1.2 $\Sigma m_i \ (i \in \Theta) = \Sigma h(U) \ (U \in \mathcal{S})$.

If (d) holds, we have $\mathcal{S} = \{ U_i : i \in \Theta \}$ so that (e) holds, too.

Let $j, k \in \Theta, j \neq k, T_j = T_k$. Then there exists $U \in \mathcal{S} - \{ U_i : i \in \Theta \}$. The integer $T = l - U - 1$ is odd, $3 \leq T \leq l - 2, T \not\equiv T_i$ for each $1 \leq i \leq n$ and $B_{i-T} \equiv 0 \ (\text{mod } l)$. Consequently, it follows from the statement (e) that

$$i, j \in \Theta, \quad i \neq j \Rightarrow T_i \neq T_j$$

and according to the well-known Theorem of Pollaczek ([4], Satz VI) the statement (d) holds. Thus, the statements (d) and (e) are equivalent.

The Theorem is proved.
REFERENCES


L. Skula
662 95 Brno, Jandčkovo nám. 2a
Czechoslovakia