Archivum Mathematicum

Ladislav Skula

On certain ideals of the group ring $\mathbf{Z}[G]$

Archivum Mathematicum, Vol. 15 (1979), No. 1, 53--66

Persistent URL: `http://dml.cz/dmlcz/107024`

ARCH. MATH. 1, SCRIPTA FAC. SCI. NAT. UJEP BRUNENSIS
XV: 53—66, 1979

ON CERTAIN IDEALS OF THE GROUP RING $\mathbf{Z}[G]$

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

0. INTRODUCTION

This paper deals with certain ideals $\mathfrak{J}$, $\mathfrak{J}_{Tm}$ of the group ring $\mathfrak{R} = \mathbf{Z}[G]$ of the cyclic group G of order $l - 1$ (l an odd prime) over the ring $\mathbf{Z}$ of integers and especially the inclusion $\mathfrak{J} \subseteq \mathfrak{J}_{Tm}$. 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 $\mathbf{Z}[G]$ act on this group and the elements of the ideal $\mathfrak{J}$ act trivially here. On the irregular class group of the l^{th} cyclotomic field there act the elements of the group ring $\bar{\mathfrak{R}} = \bar{\mathbf{Z}}[G]$, where $\bar{\mathbf{Z}}$ is the ring of l-adic integers. A great meaning for this irregular class group has the subring $\bar{\mathfrak{R}}^-$ of $\bar{\mathfrak{R}}$ and the ideal $\bar{\mathfrak{J}}^-$ of $\bar{\mathfrak{R}}^-$ which is derived from the ideal $\mathfrak{J}$. 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 $\mathfrak{R}^-$ in $\mathfrak{R}$ and the group $\mathfrak{J}^- = \mathfrak{J} \cap \mathfrak{R}^-$. Iwasawa proved this result in a more general form, for the $l^{n+1\text{th}}$ cyclotomic fields ($n \geqq 0$). But we attend only to the case $n = 0$ in this paper.

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

In the 5^{th} paragraph Theorem 5.3 gives some equivalent conditions for the $\bar{\mathfrak{R}}$-group H^- to be generated by a single element (over $\bar{\mathfrak{R}}$), 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
$\mathbf{Z}$	the ring of integers
$\bar{\mathbf{Z}}$	the ring of l-adic integers

r	a primitive root modulo l^n for each positive integer n
r_i	the integer ($i \in \mathbf{Z}$), $0 < r_i < l$, $r_i \equiv r^i \pmod{l}$ for $i \geqq 0$ $r_i r^{-i} \equiv 1 \pmod{l}$ for $i < 0$
G	a multiplicative cyclic group of order $l - 1$
s	a generator of G, hence $G = \{1 = s^0, s, s^2, \ldots, s^{l-2}\}$
$\sum_i \delta_i = \sum_{i=0}^{l-2} \delta_i$	for suitable symbols δ_i
$\sum_{i \in \mathscr{E}} \delta_i = 0$	for suitable symbols δ_i and $\mathscr{E} = \emptyset$
$\mathfrak{R} = \mathbf{Z}[G]$	the group ring of G over $\mathbf{Z}$, thus $\mathfrak{R} = \{\sum_i a_i s^i : a_i \in \mathbf{Z}\}$
$\overline{\mathfrak{R}} = \overline{\mathbf{Z}}[G]$	the group ring of G over $\overline{\mathbf{Z}}$, thus $\overline{\mathfrak{R}} = \{\sum_i a_i s^i : a_i \in \overline{\mathbf{Z}}\}$

$$\mathfrak{J} = \{\alpha \in \mathfrak{R} : \exists\, \varrho \in \mathfrak{R},\ \varrho \sum_i r_{-i} s^i = l\alpha\}$$

$$= \{\sum_i a_i s^i : a_i = \frac{1}{l} \sum_t x_t r_{-i+t},\ x_t \in \mathbf{Z},\ \sum_t x_t r_t \equiv 0 \pmod{l}\}$$

$$\overline{\mathfrak{J}} = \{\alpha \in \overline{\mathfrak{R}} : \exists\, \varrho \in \overline{\mathfrak{R}},\ \varrho \sum_i r_{-i} s^i = l\alpha\}$$

$$= \{\sum_i a_i s^i : a_i = \frac{1}{l} \sum_t x_t r_{-i+t},\ x_t \in \overline{\mathbf{Z}},\ \sum_t x_t r_t \equiv 0 \pmod{l}\}$$

$$\mathfrak{R}^- = \left\{\alpha \in \mathfrak{R} : \left(1 + s^{\frac{l-1}{2}}\right) \alpha = 0\right\}$$

$$= \left\{\sum_i a_i s^i : a_i \in \mathbf{Z},\ a_i + a_{i+\frac{l-1}{2}} = 0 \text{ for } 0 \leqq i \leqq \frac{l-3}{2}\right\}$$

$$\overline{\mathfrak{R}}^- = \left\{\alpha \in \overline{\mathfrak{R}} : \left(1 + s^{\frac{l-1}{2}}\right) \alpha = 0\right\} =$$

$$= \left\{\sum_i a_i s^i : a_i \in \overline{\mathbf{Z}},\ a_i + a_{i+\frac{l-1}{2}} = 0 \text{ for } 0 \leqq i \leqq \frac{l-3}{2}\right\}$$

$$\mathfrak{J}^- = \mathfrak{J} \cap \mathfrak{R}^-$$

$$\overline{\mathfrak{J}}^- = \overline{\mathfrak{J}} \cap \overline{\mathfrak{R}}^-$$

m	a positive integer,
T	an integer, $0 \leqq T < l - 1$

$$\lambda = r^{Tl^{m-1}}$$

$$\mathfrak{J} = \mathfrak{J}_T = \mathfrak{J}_{Tm} = \{\sum_i a_i s^i : a_i \in \mathbf{Z},\ \sum_i a_i \lambda^i \equiv 0 \pmod{l^m}\}$$

$$\overline{\mathfrak{J}} = \overline{\mathfrak{J}}_T = \overline{\mathfrak{J}}_{Tm} = \{\sum_i a_i s^i : a_i \in \overline{\mathbf{Z}},\ \sum_i a_i \lambda^i \equiv 0 \pmod{l^m}\}$$

$$\mathfrak{J}^- = \mathfrak{J}_T^- = \mathfrak{J}_{Tm}^- = \mathfrak{J} \cap \mathfrak{R}^-$$

$\bar{\mathfrak{J}}^- = \bar{\mathfrak{J}}_T^- = \bar{\mathfrak{J}}_{Tm}^- = \bar{\mathfrak{J}} \cap \bar{\mathfrak{R}}^-$

h^- the first factor of the class number of the l^{th} cyclotomic field over the rational field

$\bar{h}^- = l^a$, where $h^- = l^a . d$, a, d non-negative integers, $l \nmid d$

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

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

$$h^- = [\mathfrak{R}^- : \mathfrak{I}^-], \qquad \bar{h}^- = [\bar{\mathfrak{R}}^- : \bar{\mathfrak{I}}^-].$$

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

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

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

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

$$B_{l^{h(T)-1}T+1} \equiv 0 \pmod{l^{h(T)}}$$

and for integer $X > h(T)$

$$B_{l^{X-1}T+1} \not\equiv 0 \pmod{l^X}$$

is satisfied.

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

$$a = \Sigma h(T) \qquad (T \in \mathscr{T}).$$

2. THE IDEALS $\mathfrak{J}$

The following *Proposition* is easy to see.

2.1. Proposition.

$$\mathfrak{J} = \bar{\mathfrak{J}} \cap \mathfrak{R}, \qquad \mathfrak{I}^- = \bar{\mathfrak{J}} \cap \mathfrak{R}^- = \bar{\mathfrak{J}}^- \cap \mathfrak{R}^- = \mathfrak{J}^- \cap \mathfrak{R}.$$

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

(a) $\mathfrak{I} \subseteq \mathfrak{J}$,

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

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

(c) $$\mathfrak{I}^- \subseteq \mathfrak{J}^-,$$

(d) $$\bar{\mathfrak{I}}^- \subseteq \bar{\mathfrak{J}}^-.$$

Proof. I. Let (a) hold and let $\alpha \in \bar{\mathfrak{I}}$. Then there exist $x_t \in \mathbf{Z}$ such that $\sum_t x_t r_t \equiv 0 \pmod{l}$ and $\alpha = \sum_i a_i s^i$, where $a_i = \frac{1}{l} \sum_t x_t r_{-i+t}$. Put $b_i = \frac{1}{l} \sum_t y_t r_{-i+t}$, $\beta = \sum_i b_i s^i$, where $y_t \in \mathbf{Z}$, $y_t \equiv x_t \pmod{l^{m+1}}$. Then $\beta \in \mathfrak{I}$ and $b_i \equiv a_i \pmod{l^m}$. Therefore $\beta \in \mathfrak{J}$ and $0 \equiv \sum_i b_i \lambda^i \equiv \sum_i a_i \lambda^i \pmod{l^m}$. Thus $\alpha \in \bar{\mathfrak{J}}$ and the implication $(a) \to (b)$ holds.

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

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

If (d) holds, then according to 2.1, $\mathfrak{I}^- \subseteq \bar{\mathfrak{I}}^- \cap \mathfrak{R}^- \subseteq \bar{\mathfrak{J}}^- \cap \mathfrak{R}^- = \mathfrak{J}^-$ which gives the implication $(d) \to (c)$.

III. Let T be odd, $\mathfrak{I}^- \subseteq \mathfrak{J}^-$ and $\alpha = \sum_i a_i s^i \in \mathfrak{I}$ $(a_i \in \mathbf{Z})$. Then there exist integers x_t such that $\sum_t x_t r_t \equiv 0 \pmod{l}$ and $a_i = \frac{1}{l} \sum_t x_t r_{-i+t}$. Put

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

Then $\sum_t y_t r_t = \sum_t x_t r_t - \sum_t x_t r_{t+\frac{l-1}{2}} \equiv 0 \pmod{l}$.

If we put $b_i = \frac{1}{l} \sum_t y_t r_{-i+t}$ and $\beta = \sum_t b_t s^t$, we get $\beta \in \mathfrak{I}$ and

$$b_i = \begin{cases} a_i - a_{i+\frac{l-1}{2}} & \text{for } 0 \leqq i < \frac{l-1}{2} \\ a_i - a_{i-\frac{l-1}{2}} & \text{for } \frac{l-1}{2} \leqq i \leqq l-2. \end{cases}$$

From this we have $\beta \in \mathfrak{I}^-$ and according to the supposition $\beta \in \mathfrak{J}^-$, hence $0 \equiv \sum_i b_i \lambda^i \equiv 2 \sum_i a_i \lambda^i \pmod{l^m}$, whence we get $\alpha \in \mathfrak{J}$. The implication $(c) \to (a)$ is proved.

2.3. Proposition. *For even T the equalities*

$$\mathfrak{J}^- = \mathfrak{R}^-, \quad \bar{\mathfrak{J}}^- = \bar{\mathfrak{R}}^-$$

are satisfied.

Proof. Let $\alpha = \sum_i a_i s^i \in \mathfrak{R}^-, \bar{\mathfrak{R}}^-$ ($a_i \in \mathbf{Z}$, $a_i \in \bar{\mathbf{Z}}$) respectively. Then $a_i + a_{i+\frac{l-1}{2}} = 0$ for $0 \leqq i < \frac{l-1}{2}$ and according to the relation $\lambda^i \equiv \lambda^{i+\frac{l-1}{2}} \pmod{l^m}$, $0 \leqq i \leqq l-2$, we get $0 = \sum_{i=0}^{\frac{l-3}{2}} (a_i + a_{i+\frac{l-1}{2}})\, \lambda_i \equiv \sum_i a_i \lambda^i \pmod{l^m}$, thus $\alpha \in \mathfrak{J}^-, \alpha \in \bar{\mathfrak{J}}^-$, respectively.

2.4. Lemma *The following statements are equivalent:*

(a) $$\mathfrak{J} \subseteq \mathfrak{J},$$

(b) $$\sum_i (r_{-i+t} - r_{-i} r_t)\, \lambda^i \equiv 0 \pmod{l^{m+1}} \qquad \textit{for each } t \in \mathbf{Z}.$$

Proof. Let $x_t \in \mathbf{Z}$ $(0 \leqq t \leqq l-2)$, $\sum_t x_t r_t \equiv 0 \pmod{l}$, $a_i = \frac{1}{l} \sum_t x_t r_{-i+t}$ $(0 \leqq i \leqq l-2)$. Then there exists an integer y such that

$$x_0 = -\sum_{t=1}^{l-2} x_t r_t + ly.$$

From this we obtain

$$\sum_i a_i \lambda^i = y \sum_i r_{-i} \lambda^i + \frac{1}{l} \sum_{t=1}^{l-2} x_t \sum_i (r_{-i+t} - r_{-i} r_t)\, \lambda^i.$$

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

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

$$\sum_i (r_{-i+\tau} - r_{-i} r_\tau)\, \lambda^i = l \sum_i a_i s^i \equiv 0 \pmod{l^{m+1}}.$$

The Lemma is proved.

2.5. Consequence. *For $T = 0$ and $T = 1$ the relation*

$$\mathfrak{J} \nsubseteq \mathfrak{J}$$

is satisfied.

Proof. If $T = 0$, then by the proof of 2.4 we have $\sum_i (r_{-i+t} - r_{-i}r_t) \lambda^i \not\equiv 0 \pmod{l^{m+1}}$ for $t \not\equiv 0 \pmod{l-1}$. From 2.4 it follows that $\mathfrak{J} \nsubseteq \mathfrak{J}$.

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

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

Then from 2.4 we obtain the relation $\mathfrak{J} \nsubseteq \mathfrak{J}$.

3. THE INCLUSION $\mathfrak{J} \subseteq \mathfrak{J}$ 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) $\quad \binom{c}{k} l^k \equiv 0 \pmod{l^{m+1}} \qquad$ *for* $2 \leqq k \leqq c$,

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

(c) $\quad \binom{c+1}{k} l^{c+1-k} \equiv 0 \pmod{l^{m+2}} \qquad$ *for* $0 \leqq k \leqq c-2$ *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 $k \leqq c - 2$. Further put

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

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

$$v(\alpha) \geqq m - 1 + k - x,$$
$$v(\beta) \geqq m - 1 + k - y,$$
$$v(\gamma \geqq m + c - k - z.$$

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

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

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

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

The Lemma is proved.

3.2. Lemma. *If t is an integer, then*

$$s(1 - r_t^c) \equiv cr_t^{c-1} \sum_i (r_{-i+t} - r_{-i}r_t)\,\lambda^i (\text{mod } l^{m+1}).$$

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

$$r_{-i} = r^{l-1-i} + lu.$$

By 3.1(b) we have

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

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

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

For $i, t \in \mathbf{Z}$ 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

$$r_{-i+t}^c \equiv r_{-i}^c r_t^c + cr_t^{c-1} l r_{-i}^{c-1} \frac{r_{-i+t} - r_{-i}r_t}{l} (\text{mod } l^{m+1}).$$

Thus we get for each $t \in \mathbf{Z}$

$$s(1 - r_t^c) = \sum_i r_{-i+t}^c - \sum_i r_{-i}^c r_t^c \equiv$$

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

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 $\mathfrak{J} \nsubseteq \mathfrak{J}_{Tm}$ is satisfied.*
If $T \neq 0$, $T \neq 1$, then for T odd it holds

$$\mathfrak{J} \subseteq \mathfrak{J}_{Tm} \Leftrightarrow B_{l^{m-1}(l-T-1)+1} \equiv 0 (\mathrm{mod}\, l^m),$$

for T even and $m > 1$ it holds

$$\mathfrak{J} \subseteq \mathfrak{J}_{Tm} \Leftrightarrow B_{l^{m-1}(l-T-1)} \equiv 0 (\mathrm{mod}\, l^{m-1})$$

and for T even and $m = 1$ the inclusion

$$\mathfrak{J} \subseteq \mathfrak{J}_{Tm} = \mathfrak{J}_{T1}$$

is satisfied.

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

$$(c + 1)\, s = \sum_{k=0}^{c} \binom{c+1}{k} B_k l^{c+1-k} \equiv$$

$$\equiv \binom{c+1}{c-1} B_{c+1} l^2 + \binom{c+1}{c} B_c l (\mathrm{mod}\; l^{m+1}) = \frac{(c+1)\, c}{2} B_{c-1}\, l^2 + (c+1)\, B_c l,$$

thus

$$s \equiv \frac{c}{2}\, l^2 B_{c-1} + l B_c\, (\mathrm{mod}\; l^{m+1}).$$

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

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

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

It follows the Theorem.

4. THE GROUP $\bar{\mathfrak{R}}^-/\bar{\mathfrak{J}}^-$

4.1. Proposition. *The groups $\mathfrak{R}/\mathfrak{J}_{Tm}$, $\bar{\mathfrak{R}}/\bar{\mathfrak{J}}_{Tm}$ are cyclic groups of order l^m.*
If T is odd, the groups $\mathfrak{R}^-/\mathfrak{J}_{Tm}^-$, $\bar{\mathfrak{R}}^-/\bar{\mathfrak{J}}_{Tm}^-$ are cyclic groups of order l^m and if T is even, the groups are trivial.

For each element A of these groups ($A \in \mathfrak{R}/\mathfrak{J}_{Tm} \cup \bar{\mathfrak{R}}/\bar{\mathfrak{J}}_{Tm} \cup \mathfrak{R}^-/\mathfrak{J}^-_{Tm} \cup \bar{\mathfrak{R}}^-/\bar{\mathfrak{J}}^-_{Tm}$)

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

is valid.

Proof. We can easily see that $\{0, 1, 2, \ldots, l^m - 1\}$ is a complete system of representatives $\mathfrak{R}/\mathfrak{J}_{Tm}$ and $\bar{\mathfrak{R}}/\bar{\mathfrak{J}}_{Tm}$.

In case T is even we get from 2.3 that the grouds $\mathfrak{R}^-/\mathfrak{J}^-_{Tm}$ and $\bar{\mathfrak{R}}^-/\bar{\mathfrak{J}}^-_{Tm}$ are trivial.

If T is odd, then $\left\{x\left(1 - s^{\frac{l-1}{2}}\right) : x = 0, 1, 2, \ldots, l^{m-1}\right\}$ is a complete system of representatives $\mathfrak{R}^-/\mathfrak{J}^-_{Tm}$ and $\bar{\mathfrak{R}}^-/\bar{\mathfrak{J}}^-_{Tm}$.

Since $r^{Tl^{m-1}} - s \in \mathfrak{J}_{Tm}$, we have $s(A) = r^{Tl^{m-1}}A$ for each element A of given factor groups.

Thus, the proposition is proved.

From 4.1 we immediately get

4.2. Proposition. $\mathfrak{J}_{Tm} \supsetneqq \mathfrak{J}_{Tm+1}$, $\bar{\mathfrak{J}}_{Tm} \supsetneqq \bar{\mathfrak{J}}_{Tm+1}$ *and in case T is odd*

$$\mathfrak{J}^-_{Tm} \supsetneqq \mathfrak{J}^-_{Tm+1}, \bar{\mathfrak{J}}^-_{Tm} \supsetneqq \bar{\mathfrak{J}}^-_{Tm+1}.$$

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

$$\bigcap \bar{\mathfrak{J}}^-_{Tm(T)}(1 \leqq T \leqq l - 2, T \text{ odd}, T \neq \tau) + \bar{\mathfrak{J}}^-_{\tau m(\tau)} = \bar{\mathfrak{R}}^-$$

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

Proof. Let $\alpha \in \bar{\mathfrak{R}}^-$, $\alpha = \sum_i a_i s^i \left(a_i \in \bar{\mathbf{Z}},\ a_i + a_{i+\frac{l-1}{2}} = 0 \text{ for } 0 \leqq i \leqq \frac{l-3}{2}\right)$.

Put $\lambda_T = r^{Tl^{m(T)-1}}$ for $1 \leqq T \leqq l - 2$, T odd. Since $\det(\lambda^i_T)\left(0 \leqq i \leqq \frac{l-3}{2}, 1 \leqq \leqq T \leqq l - 2, T \text{ odd}\right) = \Pi(\lambda_{T'} - \lambda_T)\,(1 \leqq T < T' \leqq l - 2;\ T, T' \text{ odd}) \not\equiv 0 (\text{mod } l)$, the system of linear equations

$$\sum_{i=0}^{\frac{l-3}{2}} x_i\lambda^i_T = 0 \qquad (1 \leqq T \leqq l - 2, T \text{ odd}, T \neq \tau)$$

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

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

If we put $\beta = \sum_{i=0}^{\frac{l-3}{2}} x_i s^i\left(1 - s^{\frac{l-1}{2}}\right)$ and $\gamma = \sum_{i=0}^{\frac{l-3}{2}} (a_i - x_i)\, s^i\left(1 - s^{\frac{l-1}{2}}\right)$, we have $\beta \in \in \bigcap \bar{\mathfrak{J}}^-_{Tm(T)}(1 \leqq T \leqq l - 2, T \text{ odd}, T \neq \tau)$, $\gamma \in \bar{\mathfrak{J}}^-_{\tau m(\tau)}$ and $\alpha = \beta + \gamma$.

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

4.5. Theorem. *The $\bar{\mathfrak{R}}$-group $\bar{\mathfrak{R}}^-/\bar{\mathfrak{J}}^-$ is $\bar{\mathfrak{R}}$-isomorph to the direct sum of the $\bar{\mathfrak{R}}$-groups $\bar{\mathfrak{R}}^-/\bar{\mathfrak{J}}^-_{Tm(T)}$ (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, $\bigcap \bar{\mathfrak{J}}^-_{Tm(T)}$ (T odd) $= \bar{\mathfrak{J}}^-$.

Proof. Let S be the direct sum of the $\bar{\mathfrak{R}}$-groups $\bar{\mathfrak{R}}^-/\bar{\mathfrak{J}}^-_{Tm(T)}$, T odd. For $X = [\ldots, X_\tau, \ldots] \in S$ (τ odd, $1 \leqq \tau \leqq l-2$) there exists $a_\tau \in X_\tau \cap \bigcap \bar{\mathfrak{J}}^-_{Tm(T)}$($1 \leqq T \leqq l-2$, T odd, $T \neq \tau$) by 4.3. The mapping $X \to \Sigma a_\tau$ (τ odd, $1 \leqq \tau \leqq l-2$) $+ \bigcap \bar{\mathfrak{J}}^-_{Tm(T)}$ (T odd, $1 \leqq T \leqq l-2$) is an $\bar{\mathfrak{R}}$-isomorphism of S on the $\bar{\mathfrak{R}}$-group $\bar{\mathfrak{R}}^-/\bigcap \bar{\mathfrak{J}}^-_{Tm(T)}$, ($1 \leqq T \leqq l-2$, T odd), which has order l^μ by 4.1, where $\mu = \Sigma m(T)$ ($1 \leqq T \leqq l-2$, 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 $\bar{\mathfrak{R}}^-/\bigcap \bar{\mathfrak{J}}^-_{Tm(T)}$ ($1 \leqq T \leqq l-2$, T odd) is equal to $\bar{h}^-$, which follows the Theorem according to the *Iwasawa*'s formula 1.1.

From 4.5 and 4.1 we obtain

4.6. Theorem. *The $\bar{\mathfrak{R}}$-group $\bar{\mathfrak{R}}^-/\bar{\mathfrak{J}}^-$ is a direct sum of $\bar{\mathfrak{R}}$-groups $\mathfrak{K}_T (T \in \mathscr{T})$, where $\mathfrak{K}_T$ is a cyclic group of order $l^{h(T)}$ and for each $X \in \mathfrak{K}_T$*

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

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

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

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 Γ as homomorphisms.

From *Hilbert*'s „Zahlbericht" ([2], Kapitel XXIV) we obtain the following assertion going back to *Kummer.*

$$(1) \qquad \varphi(\gamma) = 0 \quad \text{for } \varphi \in \mathfrak{I},\ \gamma \in \Gamma.$$

The l-Sylow subgroup of the group Γ is said to be the *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 ($1 \leqq i \leqq n$) by χ_i. For each $1 \leqq i \leqq n$ there exists an integer T_i, $0 \leqq T_i < l - 1$ such that

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

Using equality $\{\varphi \in \mathfrak{R} : \varphi(\chi) = 0 \text{ for each } \chi \in H_i\} = \mathfrak{I}_{T_i m_i}$ we obtain $\mathfrak{I} \subseteq \mathfrak{I}_{T_i m_i}$ and we get from 3.3:

5.1. Theorem. *Let* $1 \leqq i \leqq n$. *Then* $0 \neq T_i \neq 1$.
If T_i *is odd, then* $B_{l^{m_i - 1}(l - T_i - 1) + 1} \equiv 0 (\bmod l^{m_i})$.
If T_i *is even and* $m_i > 1$, *then* $B_{l^{m_i - 1}(l - T_i - 1)} \equiv 0 (\bmod l^{m_i - 1})$.

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

Put

$$\mathcal{O} = \{1 \leqq i \leqq n : T_i \text{ odd}\}$$

and denote by

$$H^- = \Sigma H_i \qquad (i \in \mathcal{O})$$

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

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

$$(3) \qquad \varphi(\chi) = 0 \quad \text{for } \varphi \in \overline{\mathfrak{I}},\ \chi \in H.$$

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

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

(*a*) $\mathfrak{I}_\omega = \{\varphi \in \overline{\mathfrak{R}}^- : \varphi(\chi) = 0$ *for each* $\chi \in H^-\}$,

(*b*) $\omega = \Sigma x_i \chi_i$ ($i \in \mathcal{O}$), *where* x_i *are integers such that for each* $i \in \mathcal{O}$ *there exists* $j \in \mathcal{O}$ *with the property* $T_i = T_j$, $m_j \geqq m_i$ *and* $l \nmid x_j$.

Proof. Obviously, $\mathfrak{J}_\omega \supseteqq \{\varphi \in \overline{\mathfrak{R}}^- : \varphi(\chi) = 0$ for each $\chi \in H^-\}$. Let $0 \leqq x_i < l^{m_i}$ be integers ($i \in \mathcal{O}$) such that $\omega = \Sigma x_i \chi_i$ ($i \in \mathcal{O}$).

I. Let (b) hold and let $\varphi = \sum_k a_k s^k \in \mathfrak{J}_\omega (a_k \in \overline{\mathbf{Z}})$. For $i \in \mathcal{O}$ there exists $j \in \mathcal{O}$ such that $T_i = T_j$, $m_j \geqq m_i$ and $l \nmid x_j$. We have $x_j \varphi(\chi_j) = 0$, which follows

$$\sum_k a_k r^{kT_j l^{m_j - 1}} \equiv 0 (\operatorname{mod} l^{m_j}), \qquad \text{hence} \qquad \sum_k a_k r^{kT_i l^{m_i - 1}} \equiv 0 (\operatorname{mod} l^{m_i})$$

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

II. Let (b) not hold. Then there exists $j \in \mathcal{O}$ such that l / x_j and $m_i < m_j$ or $m_i = m_j$ and l / x_i for $i \in \mathcal{O}$, $T_i = T_j$.

For $i \in \mathcal{O}$ put

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

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 $\varphi = \left(1 - s^{\frac{l-1}{2}}\right) \Pi \varphi_i \, (i \in \mathcal{O})$ (in the case $\mathcal{O} = \emptyset$, $\Pi \varphi_i \, (i \in \mathcal{O}) = 1$). Then $\varphi(\omega) = 0$ and consequently $\varphi \in \mathfrak{J}_\omega$. But $\varphi(\chi_j) = 2 y l^{m_j - 1} \chi_j$, where y is an integer, $l \nmid y$.

Thus the Proposition is proved.

5.3. Theorem. *The following statements are equivalent:*

(a) *The $\overline{\mathfrak{R}}$-group H^- is $\overline{\mathfrak{R}}$-isomorphic to the $\overline{\mathfrak{R}}$-group $\overline{\mathfrak{R}}^-/\overline{\mathfrak{J}}^-$.*

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

(c) $\overline{\mathfrak{J}}^- = \{\varphi \in \overline{\mathfrak{R}}^- : \varphi(\chi) = 0$ *for each* $\chi \in H^-\}$.

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

(e) *If T is odd,* $3 \leqq T \leqq l - 2$, *and m is a positive integer such that* $B_{l^{m-1}(l-T-1)+1} \equiv 0 (\operatorname{mod} l^m)$, *then there exists* $1 \leqq i \leqq n$ *so that* $T = T_i$ *and* $m \leqq m_i$.

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

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 $\emptyset \neq \mathcal{O}_0 \subseteq \mathcal{O}$ and $\chi = \Sigma y_i \chi_i$ ($i \in \mathcal{O}_0$), where y_i are integers, $l \nmid y_i$. For $j \in \mathcal{O}_0$ we have $s(\chi) - r^{T_j l^{m_j - 1}} \chi = \Sigma y_i (r^{T_i l^{m_i - 1}} - r^{T_j l^{m_j - 1}}) \chi_i$ ($i \in \mathcal{O}_0$) $= \Sigma z_i \chi_i$ ($i \in \mathcal{O}_0 - \{j\}$), where z_i are integers, $l \nmid z_i$.

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

Thus, (b) holds.

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

$$\chi_j = \sum_u a_u \sum_{i \in \mathcal{O}} x_i r^{uT_i l^{m_i - 1}} \chi_i = \sum_{i \in \mathcal{O}} x_i \chi_i \sum_u a_u r^{uT_i l^{m_i - 1}}$$

we have

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

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

consequently $x_k \equiv 0 \pmod{l}$ and $x_j \not\equiv 0 \pmod{l}$. 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 ω be an element of H^- of the form from 5.2 (b). In a similar way as in [3] (p. 177) we put for $\varphi \in \bar{\mathfrak{R}}^-$

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

Obviously, f is an $\bar{\mathfrak{R}}$-homomorphism from $\bar{\mathfrak{R}}^-$ to H^- with the kernel $\mathfrak{I}_\omega = \{\varphi \in \bar{\mathfrak{R}}^- : \varphi(\chi) = 0 \text{ for each } \chi \in H^-\}$ (by 5.2). For $\varphi = z\left(1 - s^{\frac{l-1}{2}}\right)$, where z is an integer such that $2z \equiv 1 \pmod{l^{m_i}}$ $(i \in \mathcal{O})$, we have $f(\varphi) = \beta$. The factor group $\bar{\mathfrak{R}}^-/\mathfrak{I}_\omega$ is embedded into the factor group $\bar{\mathfrak{R}}^-/\bar{\mathfrak{I}}^-$ and also into H^-.

From I, 1.1. and 5.4 we obtain the equivalence of statements (a), (b), (c).

III. For $i \in \mathcal{O}$ put $U_i = l - T_i - 1$. According to 3.4 $U_i \in \mathcal{T}$ and $h(U_i) \geqq m_i$, hence $\mathcal{T} \supsetneqq \{U_i : i \in \mathcal{O}\}$. According to 1.2 Σm_i $(i \in \mathcal{O}) = \Sigma h(U)$ $(U \in \mathcal{T})$.

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

Let $j, k \in \mathcal{O}$, $j \neq k$, $T_j = T_k$. Then there exists $U \in \mathcal{T} - \{U_i : i \in \mathcal{O}\}$. The integer $T = l - U - 1$ is odd, $3 \leqq T \leqq l - 2$, $T \neq T_i$ for each $1 \leqq i \leqq n$ and $B_{l-T} \equiv 0 \pmod{l}$. Consequently, it follows from the statement (e) that

$$i, j \in \mathcal{O}, \qquad i \neq j \Rightarrow T_i \neq T_j$$

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

[1] Z. J. Borevič and J. R. Šafarevič: *Number Theory,* New York 1966.

[2] D. Hilbert: *Die Theorie der algebraischen Zahlkörper,* Jahresber. der Deutsch. Math. Ver., (1897), 175—546.

[3] K. Iwasawa: *A Class Number Formula for Cyclotomic Fields,* Annals of Mathematics, vol. 76 No. 1, July (1962), 171—179.

[4] F. Pollaczek: *Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswurzeln,* Math Zeitschrift 21 (1924), 1—38.

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