Ladislav Skula

Some bases of the Stickelberger ideal

Mathematica Slovaca, Vol. 43 (1993), No. 5, 541--571

Persistent URL: `http://dml.cz/dmlcz/136590`

Math. Slovaca, 43 (1993), No. 5, 541–571

SOME BASES OF THE STICKELBERGER IDEAL

LADISLAV SKULA [1)]

Dedicated to Professor Helmut Koch on the occasion of his 60th birthday.

ABSTRACT. In this paper various bases of the Stickelberger ideal (considered as a $\mathbb{Z}$-module) in the group ring $R = \mathbb{Z}[G]$ of the Galois group G of p^{n+1}th cyclotomic field ($n \geq 0$, p an odd prime) over the ring of rational integers are introduced. One special basis is used for the computation of the index of the Stickelberger ideal in a subring of R (Sinnott's result (1980)).

Some bases are used to show "equivalence" of known systems of congruences (Fueter (1992), Le Lidec (1967)) to the Kummer system of congruences. In case $n = 0$, Kummer operated with special elements from the Stickelberger ideal, and it is shown here that these elements form a basis of the Stickelberger ideal. The "π-adic" situation is also investigated.

Sinnott's class number formula is added by a formula where the ring of rational integers is substituted for the ring of congruence classes modulo p. Here the index of the Stickelberger ideal equals $p^{\mathrm{i}(p)}$, where $\mathrm{i}(p)$ means the index of irregularity of the prime p.

0. Introduction

The background of this paper is formed by *Kummer's system of congruences*

$$\varphi_{p-2j}(t)\, B_{2j} \equiv 0 \pmod{p}, \qquad 1 \leq j \leq \frac{p-3}{2}, \tag{K}$$

where B_{2j} are the Bernoulli numbers and $\varphi_i(t)$ are the Mirimanoff polynomials. Here always p will designate a fixed odd prime.

These congruences (K) were introduced by Kummer ([8], 1857) when trying to solve the *First Case of Fermat's Last Theorem*. Many authors have

AMS Subject Classification (1991): Primary 16S34, 11R29, 11R18, 11R68.

Key words: Stickelberger ideal, Kummer (Fueter, Le Lidec, Benneton) system of congruences, Iwasawa's (Sinnott's) class number formula, Index of irregularity.

1) The results of this paper were delivered in the 10th Czechoslovak Number Theory Conference held in Mýto pod Ďumbierom (the Low Tatras), Slovakia, 2–7 September 1991.

used various systems of congruences for this reason since. In the paper [17] a new system (S) of congruences depending on the Stickelberger ideal was introduced and it was shown that (S) and (K) are "equivalent" in a certain sense (6.1). This result can be obtained by means of a special basis of the Stickelberger ideal mod p considered as a vector space over the Galois field $\mathbb{Z}/p\mathbb{Z}$ (5.4).

If we use the basis of the Stickelberger ideal I considered as a $\mathbb{Z}$-module consisting of Kummer's elements, then we obtain "equivalence" (6.3) of the system (S) and the system (L) formed by the Le Lidec polynomials ([10], [11]). The equivalence of Fueter's system of congruences (F_1) ([3, VI]) and (S) can be obtained by the choice of another special basis of I. By means of another choice of elements from I we get the statement that each solution of (S) is a solution of the other system of congruences (F_2) using the Fermat quotients introduced by Fueter [3, VII] (6.4). Another choice of elements from I (6.5) gives the Benneton system of congruences ([2]).

For these reasons various bases of the Stickelberger ideal considered as a module over the ring of rational integers $\mathbb{Z}$ or π-adic integers $\mathbb{Z}_\pi$ (π a prime) are studied in this paper.

In Section 2 the group ring $R = \mathbb{Z}[G]$ and the Stickelberger ideal I in R are investigated, where G is the Galois group of the p^{n+1}th cyclotomic field ($n \geq 0$). The study of the quotient-ring R/I was begun by Iwasawa ([5], 1962), who proved the following class number formula:

0.1. Iwasawa.

$$[R^- : I^-] = h_n^- .$$

R^- means a special subring of R, $I^- = I \cap R^-$ and h_n^- is the first factor of the class number of the p^{n+1}th cyclotomic field.

Sinnott [13] extended this formula to a general cyclotomic field and in [14] he transferred it for the case of the Stickelberger ideal I (Theorem 2.1):

0.2. Sinnott (*For the p^{n+1}th cyclotomic field*).

$$[R^\star : I] = h_n^- .$$

$R^\star$ means a special subring of R containing R^- (denoted by A in [11]*).*

Although Sinnott's case is more general, I am working only (like Iwasawa) with the p^{n+1}th cyclotomic field since the applications I am interested in concern only the case of the pth cyclotomic field (Sections 4, 5, 6). The case of a general cyclotomic field is investigated in this direction by Kučera [6].

In Main Theorem 2.7 some bases of the $\mathbb{Z}$-module I are given and we obtain Sinnott's formula 0.2 in another way by the computation of the absolute value of the determinant of the transition matrix from a special basis of R to some of these bases of I.

Iwasawa ([2], [5]) also formulated the class number formula for the subring R_π^- of the group ring $R_\pi = \mathbb{Z}_\pi[G]$ of G over the ring of π-adic integers generated by R^- as follows:

0.3. Iwasawa.

$$[R_\pi^- : I_\pi^-] = (h_n^-)_\pi .$$

Here I_π^- means the Stickelberger ideal in the ring R_π^- and $(h_n^-)_\pi$ is the π-part of h_n^-.

This π-adic situation is investigated in Section 3 and Iwasawa's formula 0.3 is transferred for the Stickelberger ideal I_π in the subring $R_\pi^\star$ of R_π generated by R (3.7(b)):

0.4.

$$[R_\pi^\star : I_\pi] = (h_n^-)_\pi .$$

Section 4 deals with special elements κ_ρ from the Stickelberger ideal I (for the pth cyclotomic field, the case $n = 0$) which were used by Kummer ([7], 1847), and the main result (4.8) states that these elements of Kummer form a basis of the $\mathbb{Z}$-module I.

The author ([19, 2.2]) showed the following addition to Iwasawa's class number formula.

0.5. Skula.

$$\left[R^-(p) : I^-(p)\right] = p^{\mathrm{i}(p)} .$$

Here $R^-(p)$, $I^-(p)$ are the former notions considered $\bmod p$ *and* $\mathrm{i}(p)$ *means the index of irregularity of the prime p.*

In Section 5 we obtain (5.2) a similar addition to Sinnott's class number formula:

0.6.

$$\left[R^\star(p) : I(p)\right] = p^{\mathrm{i}(p)} .$$

1. Notation and basic assertions

Through this paper we denote by:

p an odd prime,
n a non-negative integer,
h_n^- the first factor of the class number of the cyclotomic field generated by the p^{n+1}th roots of unity over the rational field,
$\mathbb{Z}$ the ring of rational integers,

$$q = p^{n+1}\,, \qquad M = p^n(p-1)\,, \qquad N = \frac{M}{2}\,,$$

r a primitive root modulo q,
$\operatorname{ind} x$ index of x relative to the primitive root r of x ($x \in \mathbb{Z},\ p \nmid x$),
r_j the integer ($j \in \mathbb{Z}$), $0 < r_j < q$, $r_j \equiv r^j \pmod q$,

hence we have:

1.1. *For each $j \in \mathbb{Z}$ we have:*

$$r_j + r_{j+N} = q\,.$$

$\sum\limits_i \delta_i = \sum\limits_{i=0}^{M-1} \delta_i$ for suitable symbols δ_i,
G a multiplicative cyclic group of order M,
s a generator of G; thus $G = \{1, s, s^2, \dots, s^{M-1}\}$,
$R = \mathbb{Z}[G]$ the group ring of G over the ring $\mathbb{Z}$; thus $R = \sum\limits_i a_i s^i :\ a_i \in \mathbb{Z}$;
$a_j = a_i$ for $\alpha = \sum\limits_i a_i s^i \in R$ and $j \in \mathbb{Z}$, $i \equiv j \pmod M$,

$$\begin{aligned} R^\star &= \Big\{\alpha = \sum_i a_i s^i \in R:\ a_k + a_{k+N} = a_l + a_{l+N} \text{ for each } k, l \in \mathbb{Z}\Big\} \\ &= \Big\{\alpha \in R:\ (1+s^N)\alpha \in \mathbb{Z}\cdot\sum_i s^i\Big\}\,, \end{aligned}$$

$$\begin{aligned} R^- &= \Big\{\alpha = \sum_i a_i s^i \in R:\ a_k + a_{k+N} = 0 \text{ for each } k \in \mathbb{Z}\Big\} \\ &= (1-s^N)R = \{\alpha \in R:\ \alpha(1+s^N) = 0\}\,, \end{aligned}$$

$$I = \left\{ \alpha \in R : \ \exists \rho \in R, \ \rho \cdot \sum_i r_{-i} s^i = q \cdot \alpha \right\}$$
$$= \left\{ \alpha = \sum_i a_i s^i \in R : \ \exists x_t \in \mathbb{Z} \ (0 \le t \le M-1), \ \sum_t x_t r_t \equiv 0 \ (\mathrm{mod}\ q), \right.$$
$$\left. a_i = \frac{1}{q} \sum_t x_t r_{-i+t} \text{ for each } 0 \le i \le M-1 \right\}$$

([16, Section 4, (4)]).
I is an ideal of the ring R which is called the *Stickelberger ideal of the ring* R. $I^- = I \cap R^-$ is an ideal of the ring R^- which is called the *Stickelberger ideal of the ring* R^-.

Ideals of the ring R are often considered as $\mathbb{Z}$-modules.

Since $\frac{1}{q} \sum_t x_t r_{i+t} + \frac{1}{q} \sum_t x_t r_{i+N+t} = \sum_t x_t$ for each $i \in \mathbb{Z}$ and each $x_t \in \mathbb{Z}$ $(0 \leqq t \leqq M-1)$, we have

1.2.
$$I \subseteq R^\star .$$

Further we can state

1.3. $R \neq R^\star$ *unless* $p = 3$ *and* $n = 0$, $R = R^\star = I$ *for* $p = 3$ *and* $n = 0$.

Proof. The relations $R \neq R^\star$, $R = R^\star$ are obvious. Let $p = 3$, $n = 0$ and $\alpha = a + bs \in R$. Put

$$x_0 = -a + 2b,$$
$$x_1 = 2a - b.$$

The equalities $\sum_t x_t r_t = 3a$ and $\sum_t x_t r_{-1+t} = 3b$ conclude the proof.

1.4. Lemma.
$$R^\star = I + R^- .$$

Proof. For $0 \le t \le M-1$ put

$$x_t = \begin{cases} 2 & \text{for } t = 0, \\ -1 & \text{for } t = \operatorname{ind} 2, \\ 0 & \text{otherwise}, \end{cases}$$

and $a_i = \frac{1}{q} \sum_t x_t r_{-i+t} = \frac{1}{q}(2r_{-i} - r_{-i+\operatorname{ind} 2})$. Then $\alpha = \sum_i a_i s^i \in I$ and $a_i + a_{i+N} = 1$, the results follow.

Applying this lemma we get:

1.5. THEOREM. *The quotient-rings $R^\star/I$ and R^-/I^- are isomorphic (canonically).*

Put

$$\begin{aligned}
b_{00} &= q-2\,, \\
b_{0j} &= 1-r_j\,, && 1 \leqq j \leqq N-1\,, \\
b_{i0} &= 1-r_i\,, && 1 \leqq i \leqq N-1\,, \\
b_{ij} &= \frac{1}{q}(r_i r_j - r_{i+j})\,, && 1 \leqq i,\ j \leqq N-1\,, \\
B &= (b_{ij})_{0\le i,\,j\le N-1}.
\end{aligned}$$

For $n=0$ this matrix B was introduced and $|\det B|$ was computed in [12], in general case in [16]:

1.6.

$$|\det B| = h_n^-\,.$$

Further put for $1 \le k \le N-1$, $0 \le l \le N-1$:

$$\begin{aligned}
g_{0l} &= r_{-l} - q\,, \quad g_{0N} = q\,, \quad g_{kN} = r_k - 1\,, \quad g_{Nl} = -1\,, \quad g_{NN} = 2\,, \\
g_{kl} &= \frac{1}{q}(r_{-l} r_k - r_{-l+k}) - r_k + 1\,.
\end{aligned}$$

Denote by C the following matrix:

$$C = (g_{kh})_{0\le k,\,h\le N}\,.$$

1.7. PROPOSITION.

$$|\det C| = h_n^-\,.$$

P r o o f. Perform the following operations on C:

a) Interchange the columns with indices l and $N-1$ $(1 \le l \le N-1)$.
b) Multiply by (-1) the columns with indices $1, 2, \ldots, N-1$.
c) Add the column with index 0 to the column with index N.
d) Subtract the row with index N from the row with index 0.
e) Multiply the row with index 0 by (-1).

Then it is easy to see $|\det C| = |\det B|$ and the assertion follows from 1.6.

2. Some bases of the $\mathbb{Z}$-Module I

2.1. Notation. *For $k \in \mathbb{Z}$ put*

$$\gamma_k = \sum_i \frac{1}{q}(r_{-i}r_k - r_{-i+k})s^i = \sum_i \left[\frac{r_{-i}r_k}{q}\right] s^i ,$$
$$\varepsilon_k = s^k(1 - s^N) ,$$

and further put

$$\gamma = \sum_i r_{-i}s^i ,$$
$$\delta = \sum_i s^i = 1 + s + s^2 + \cdots + s^{M-1} ,$$
$$\varepsilon = \sum_{i=0}^{N-1} s^i = 1 + s + s^2 + \cdots + s^{N-1} .$$

If we consider instead of the group ring $\mathbb{Z}[G]$ the group ring $\mathbb{Q}[G]$, then the element $\frac{1}{q}\gamma$ is often called the *Stickelberger element.* The element δ acts on the class group of the qth cyclotomic field as the norm. Clearly,

$$\gamma_k,\ \varepsilon_k,\ \gamma,\ \delta,\ \varepsilon \qquad \text{are elements of the ring} \quad R .$$

2.2. Definition. *Let $X \subseteq \{0, 1, \ldots, M-1\}$. The set X is said to have the basis property if it has the following property:*

$$\xi \in X , \quad \xi' \in \mathbb{Z}, \quad \xi' \equiv \xi + N \pmod M \implies \xi' \notin X .$$

It is easy to see the following:

2.3. Proposition. *Let $L \subseteq \{0, 1, \ldots, M-1\}$ have the basis property and let $|L| = N$. Then the system*

$$\mathcal{S}^\star(L) = \{\varepsilon_l :\ l \in L\} \cup \{\varepsilon\}$$

forms a basis of the $\mathbb{Z}$-module $R^\star$. (Symbol $|L|$ denotes the cardinal of the set L.)

2.4. PROPOSITION. *We have*

$$\gamma \in I\,, \quad \delta \in I\,, \qquad \textit{and} \quad \gamma_k \in I \quad \textit{for each} \quad k \in \mathbb{Z}\,.$$

P r o o f.

a) We can assume $k \in \mathbb{Z},\ 1 \le k \le M-1$. Put for each $t \in \mathbb{Z},\ 0 \le t \le M-1$:

$$x_t = \begin{cases} r_k & \text{for } t = 0\,, \\ -1 & \text{for } t = k\,, \\ 0 & \text{otherwise.} \end{cases}$$

Then for $0 \le i \le M-1$ we have

$$\frac{1}{q}\sum_t x_t r_{-i+t} = \frac{1}{q}(r_{-i}r_k - r_{-i+k})\,,$$

hence $\gamma_k \in I$.

b) If we put for $0 \le t \le M-1$

$$x_t = \begin{cases} q & \text{for } t = 0\,, \\ 0 & \text{otherwise,} \end{cases}$$

then $\frac{1}{q}\sum_t x_t r_{-i+t} = r_{-i}$ and hence $\gamma \in I$. (Or we can see the relation $\gamma \in I$ immediately from the first definition of I putting $\rho = q \in R$.)

c) If we put for $0 \le t \le M-1$

$$x_t = \begin{cases} 1 & \text{for } t = 0 \text{ or } t = N\,, \\ 0 & \text{otherwise,} \end{cases}$$

then $\frac{1}{q}\sum_t x_t r_{-i+t} = \frac{1}{q}(r_{-i} + r_{-i+N}) = 1$. Thus $\delta \in I$.

2.5. LEMMA.

(a) *For each $j, k \in \mathbb{Z}$ we have*

$$\frac{1}{q}(r_j r_k - r_{j+k}) + \frac{1}{q}(r_j r_{k+N} - r_{j+k+N}) = r_j - 1\,.$$

(b) *For each $k \in \mathbb{Z}$ we have*

$$\gamma_k + \gamma_{k+N} = \gamma - \delta\,.$$

P r o o f. (a) follows from 1.1 and (b) follows from (a).

2.6. Proposition. *Let $K \subseteq \{1, 2, \ldots, M-1\}$ have the basis property and let $|K| = N-1$, $N \notin K$. Then the system*

$$\mathcal{S}(K) = \{\gamma_k : k \in K\} \cup \{\gamma, \delta\}$$

forms a system of generators of the $\mathbb{Z}$-module I.

Proof. According to 2.5 (b) we can suppose $K = \{1, 2, \ldots, N-1\}$, hence

$$\mathcal{S}(K) = \{\gamma_1, \gamma_2, \ldots, \gamma_{N-1}, \gamma, \delta\}.$$

Let $\alpha = \sum_i a_i s^i \in I$. Then there exist integers $x_t \in \mathbb{Z}$ ($0 \leqq t \leqq M-1$) such that $\sum_t x_t r_t \equiv 0 \pmod q$ and

$$a_i = \frac{1}{q} \sum_t x_t r_{-i+t} \qquad \text{for each} \quad 0 \leq i \leq M-1.$$

Put

$$x = \frac{1}{q} \sum_t x_t r_t, \qquad d = \sum_{t=N}^{M-1} x_t, \qquad c = x - d,$$

$$c_k = x_{k+N} - x_k \qquad \text{for each} \quad 1 \leq k \leq N-1.$$

We have for each $i \in \mathbb{Z}$, $0 \leq i \leq M-1$:

$$\begin{aligned}
&\sum_{k=1}^{N-1} c_k (r_{-i} r_k - r_{-i+k}) \\
&= r_{-i} \sum_{l=N+1}^{M-1} x_l r_{l+N} - r_{-i} \sum_{l=1}^{N-1} x_l r_l - \sum_{l=N+1}^{M-1} x_l r_{-i+l+N} + \sum_{l=1}^{N-1} x_l r_{-i+l} \\
&= q r_{-i} \sum_{l=N+1}^{M-1} x_l - r_{-i} \sum_{l=N+1}^{M-1} x_l r_l - r_{-i} \sum_{l=1}^{N-1} x_l r_l \\
&\qquad\qquad - q \sum_{l=N+1}^{M-1} x_l + \sum_{l=N+1}^{M-1} x_l r_{-i+l} + \sum_{l=1}^{N-1} x_l r_{-i+1} \\
&= q r_{-i} d - q r_{-i} x_N - r_{-i} \sum_l x_l r_l + r_{-i} x_N r_N + r_{-i} x_0 \\
&\qquad\qquad - qd + q x_N + \sum_l x_l r_{-i+1} - x_0 r_{-i} - x_N r_{-i+N} \\
&= q r_{-i} d - q r_{-i} x_N - q x r_{-i} + r_{-i} q x_N - r_{-i} x_N - qd \\
&\qquad\qquad + q x_N + q a_i - q x_N + x_N r_{-i} \\
&= q a_i - q c r_{-i} - qd.
\end{aligned}$$

It follows that

$$\alpha = \sum_{k=1}^{N-1} c_k\gamma_k + c\gamma + d\delta\,,$$

and we are done.

2.7. Main Theorem. *Let $K, L \subseteq \{0,1,2,\dots,M-1\}$ have the basis property, $|K| = N-1$, $|L| = N$, $0 \notin K$, $N \notin K$.*

Then the system $\mathcal{S}(K) = \{\gamma_k : k \in K\} \cup \{\gamma, \delta\}$ forms a basis of the $\mathbb{Z}$-module I and for the determinant Δ of the transition matrix from the basis $\mathcal{S}^\star(L) = \{\varepsilon_l : l \in L\} \cup \{\varepsilon\}$ of the $\mathbb{Z}$-module $R^\star$ to the basis $\mathcal{S}(K)$ of the $\mathbb{Z}$-module I we have

$$|\Delta| = h_n^-\,.$$

Therefore the Stickelberger ideal I has a finite index in the ring $R^\star$, for which the following relation holds

$$[R^\star : I] = h_n^-\,.$$

Proof. Without loss of generality we can suppose $L = \{0,1,\dots \dots,N-1\}$ and $K = \{1,2,\dots,N-1\}$, thus $\mathbf{S}^\star(L) = \{\varepsilon_0,\varepsilon_1,\dots,\varepsilon_{N-1},\varepsilon\}$ and $\mathcal{S}(K) = \{\gamma,\gamma_1,\gamma_2,\dots,\gamma_{N-1},\delta\}$.

Using 1.1 and 2.5 (a) ($-l \to k$, $k \to j$) we get

$$\gamma = \sum_{l=0}^{N-1}(r_{-l} - q)\varepsilon_l + q\varepsilon\,,$$

$$\gamma_k = \sum_{l=0}^{N-1}\left[\frac{1}{q}(r_{-l}r_k - r_{-l+k}) - r_k + 1\right]\varepsilon_l + (r_k - 1)\varepsilon \qquad (1 \le k \le N-1)\,,$$

$$\delta = \sum_{l=0}^{N-1}(-1)\varepsilon_l + 2\varepsilon\,.$$

The transition matrix from the basis $\mathcal{S}^\star(L)$ to the system of generators $\mathcal{S}(K)$ of the $\mathbb{Z}$-module I is the matrix C from Section 1 and according to 1.7 we have $|\Delta| = |\det C| = h_n^-$. This completes the proof.

2.8. Remark. The assertion of 2.7 concerning the index of the Stickelberger ideal I in the ring $R^\star$ is a special case of *Sinnott's Theorem* 0.2 for the p^{n+1}th cyclotomic field. Here, this special case was derived by presenting a special basis $\mathcal{S}(K)$ of the Stickelberger ideal (as a $\mathbb{Z}$-module) and by the computation of the absolute value of the determinant of the transition matrix from the basis $\mathbf{S}^\star(L)$ of $R^\star$ to $\mathbf{S}(K)$.

If we use *Iwasawa's class number formula* 0.1, we can prove 2.7 from 1.5, 2.3 and 2.6.

On the other hand, we can show from *Sinnott's relation* $[R^\star : I] = h_n^-$ that a system of generators of the $\mathbb{Z}$-module I^- forms a basis of I^- and compute the absolute value of the determinant of the transition matrix from a basis of R^- to the given system if we use the isomorphism between $R^\star/I$ and R^-/I^-. (see 2.9.2.)

2.9. Notation. *Put* $K^0 = \{1 \le k \le M-1 :\ r_k \text{ odd}\}$. *Then the set* K^0 *has the basis property,* $|K^0| = N-1$, $0 \notin K^0$.

According to 2.7:

2.9.1. *The system* $\mathcal{S}(K^0) = \{\gamma_k :\ k \in K^0\} \cup \{\gamma, \delta\}$ *forms a basis of the* $\mathbb{Z}$*-module* I.

Put

$$\alpha_k = \sum_i \left[\frac{1}{q}(r_{-i}r_k - r_{-i+k}) + \frac{1-r_k}{2}\right] s^i \qquad (k \in K^0),$$

$$\alpha_0 = \sum_i (2r_{-i} - q)s^i .$$

It was proved in [16, Theorem]:

2.9.2. *The system* $\{\alpha_k :\ k \in K^0\} \cup \{\alpha_0\}$ *forms a basis of the* $\mathbb{Z}$*-module* I^- *and for the determinant* Δ *of the transition matrix from the basis* $s^j(1-s^N)$ $(0 \le j < N)$ *of the* $\mathbb{Z}$*-module* R^- *to this basis we have*

$$|\Delta| = h_n^- .$$

Therefore $[R^- : I^-] = h_n^-$. (Iwasawa 0.1.)

Clearly, the following holds.

2.9.3.

$$\alpha_k = \gamma_k + \frac{1-r_k}{2}\delta \qquad (k \in K^0),$$

$$\alpha_0 = 2\gamma - q\delta .$$

We can see easily from these assertions that $\delta \cdot \mathbb{Z} \cap I^- = \{0\}$. We denote by I^0 the sum of the $\mathbb{Z}$-modules $\delta\mathbb{Z}$ and I^-. This sum is the direct sum of these $\mathbb{Z}$-modules. (Since $\delta\mathbb{Z} = \delta R$, I^0 is also an ideal of the ring R.) Summarizing we have

2.9.4.

$$I^0 = I^- \oplus \delta\mathbb{Z} \subseteq I\,.$$

2.10. PROPOSITION. *The systems* $\{\alpha_k : k \in K^0\} \cup \{\alpha_0, \delta\}$, $\{\gamma_k : k \in K^0\} \cup \{2\gamma, \delta\}$ *form bases for the* $\mathbb{Z}$*-module* I^0.

P r o o f. Immediately from 2.9.2 and 2.9.4 we get the fact that the former system is a basis of the $\mathbb{Z}$-module I^0. Since the second system is a system of generators of the $\mathbb{Z}$-module I^0 according to 2.9.3 and has the same number of elements (namely $N+1$), the results follow.

According to 2.9.1 and 2.10 we get

2.11. THEOREM. *For the index of the ideal* I^0 *in the Stickelberger ideal* I *the following relation is valid:*

$$[I : I^0] = 2\,.$$

For the quotient $\mathbb{Z}$*-module* I/I^0 *we have*

$$I/I^0 = \{I^0, \gamma + I^0\}\,.$$

3. The Stickelberger ideal of the ring R_π

3.1. Notation. In this Section we will denote by

π	a prime,
$\mathbb{Q}$	the field of rational numbers,
$\mathbb{Q}_\pi$	the field of π-adic numbers,
$\mathbb{Z}_\pi$	the ring of π-adic integers,
$S = \mathbb{Q}[G]$	the group rings of the group G over $\mathbb{Q}$,
$S_\pi = \mathbb{Q}_\pi[G]$	the group rings of the group G over $\mathbb{Q}_\pi$,
$R_\pi = \mathbb{Z}_\pi[G]$	the group rings of the group G over $\mathbb{Z}_\pi$.

Thus $S_\pi = \left\{\sum\limits_i a_i s^i : a_i \in \mathbb{Q}_\pi\right\}$ and for $\alpha = \sum\limits_i a_i s^i \in S_\pi$ we put again $a_j = a_i$, where $j, i \in \mathbb{Z}$, $0 \le i \le M-1$, $j \equiv i \pmod{M}$.

S, S_π are considered as $\mathbb{Z}$-module and $\mathbb{Z}_\pi$-module (respectively).

We will consider (as in [2, Section 2]) the natural π-adic topology in the ring S_π: if $\alpha^{(\nu)} = \sum\limits_i a_i^{(\nu)} S^i \in S_\pi$ and $\lim\limits_{\nu\to\infty} a_i^{(\nu)} = a_i \in \mathbb{Q}_\pi$ (lim denotes the π-adic limit) for each $0 \le i \le M-1$, then $\lim\limits_{\nu\to\infty} \alpha^{(\nu)} = \alpha = \sum\limits_i a_i\, s^i \in S_\pi$.

For $\mathcal{M} \subseteq S_\pi$ let $\mathcal{M}_\pi$ denote closure in this topology:

$$\mathcal{M}_\pi = \{\alpha \in S_\pi :\ \exists \alpha^{(\nu)} \in \mathcal{M},\ \lim_{\nu\to\infty} \alpha^{(\nu)} = \alpha\}.$$

The former notation S_π, R_π, $\mathbb{Q}_\pi$ and $\mathbb{Z}_\pi$ is in accordance with this one. Obviously,

$$R_\pi^- = \Big\{\alpha = \sum_i a_i s^i \in R_\pi :\ a_i + a_{i+N} = 0 \text{ for each } i \in \mathbb{Z}\Big\},$$

$$R_\pi^\star = \Big\{\alpha = \sum_i a_i s^i \in R_\pi :\ a_i + a_{i+N} = a_j + a_{j+N} \text{ for each } i, j \in \mathbb{Z}\Big\}.$$

Ideals of the ring R_π will often be considered as $\mathbb{Z}_\pi$-modules in the natural way.

The *Stickelberger ideals* I_π and I_π^- of the rings R_π and R_π^- are defined as the closures of I and I^- in the natural π-adic topology, respectively. (see [5, Section 2])

Obviously,

$$I_\pi \subseteq R_\pi^\star.$$

3.2. Theorem. *Let $\mathcal{M} \subseteq S$ be a $\mathbb{Z}$-submodule of the $\mathbb{Z}$-module S with a basis $\mu_1, \dots, \mu_m$ $(1 \le m \le M)$. Then $\mathcal{M}_\pi$ is a $\mathbb{Z}_\pi$-submodule of the $\mathbb{Z}_\pi$-module S_π with the basis $\mu_1, \dots, \mu_m$.*

Proof. Put $\overline{\mathcal{M}} = \Big\{\sum_{j=1}^m m_j\mu_j :\ m_j \in \mathbb{Z}_\pi\Big\}$. Clearly, $\overline{\mathcal{M}} \subseteq \mathcal{M}_\pi$. For each $1 \le j \le m$ there exist $d_{ji} \in \mathbb{Q}$ such that $\mu_j = \sum_i d_{ji}s^i$. Since $\mu_1, \dots, \mu_m$ are linearly independent over $\mathbb{Q}$, rank of the matrix $D = (d_{ji})$ $(1 \le j \le m$, $0 \le i \le M-1)$ equals m. Therefore $\mu_1, \dots, \mu_m$ are also linearly independent over $\mathbb{Q}_\pi$, and then they form a basis of the $\mathbb{Z}_\pi$-module $\overline{\mathcal{M}}$.

Let $\mu \in \mathcal{M}_\pi$, $\mu = \sum_i b_i s^i$ $(b_i \in \mathbb{Q}_\pi)$. Then there exist $\mu^{(\nu)} \in \mathcal{M}$ $(\nu \geqq 1)$ such that $\mu = \lim_{\nu\to\infty} \mu^{(\nu)}$.

We have $\mu^{(\nu)} = \sum_{j=1}^m m_j^{(\nu)}\mu_j$, where $m_j^{(\nu)} \in \mathbb{Z}$. Put

$$b_i^{(\nu)} = \sum_{j=1}^m m_j^{(\nu)} d_{ji} \qquad (0 \leqq i \leqq M-1,\ \ \nu = 1, 2, \dots).$$

Then $\mu^{(\nu)} = \sum_i s^i \sum_{j=1}^{m} m_j^{(\nu)} d_{ji} = \sum_i b_i^{(\nu)} s^i$, hence $b_i = \lim_{\nu\to\infty} b_i^{(\nu)}$ $(0 \le i \le M-1)$.

Since the sequences $\left\{m_j^{(\nu)}\right\}_{\nu=1}^{\infty}$ $(1 \le j \le m)$ are bounded, there exist positive integers $k_1 < k_2 < \dots$ such that the sequences $\left\{m_j^{(\nu_k)}\right\}_{k=1}^{\infty}$ are convergent.

If we put $m_j = \lim_{k\to\infty} m_j^{(\nu_k)}$ $(\in \mathbb{Z}_\pi)$, we get $b_i = \sum_{j=1}^{m} m_j d_{ji}$, hence $\mu = \sum_{j=1} m_j \mu_j \in \overline{\mathcal{M}}$. The proof is complete.

3.3. Proposition. *Put*

$$J = \left\{\alpha \in R_\pi :\ \exists \rho \in R_\pi,\ \rho \cdot \sum_i r_{-i} s^i = q \cdot \alpha\right\},$$

$$K = \left\{\alpha = \sum_i a_i s^i \in R_\pi :\ \exists x_t \in \mathbb{Z}_\pi \ \ (0 \le t \le M-1),\right.$$
$$\left. q / \sum_t x_t r_t \ \ (\text{in } \mathbb{Z}_\pi),\ \ a_i = \frac{1}{q} \sum_t x_t r_{-i+t} \ \text{for each } i \in \mathbb{Z}\right\}.$$

Then

$$I_\pi = J = K.$$

Proof.

I. Let $\alpha = \sum_i a_i s^i \in J$, $\rho = \sum_t x_t s^t \in R_\pi$, $\rho \cdot \sum_i r_{-i} s^i = q \cdot \alpha$. We have $\sum_i q a_i s^i = \sum_i \Big(\sum_t x_t r_{-i+t}\Big) s^i$, hence $a_i = \frac{1}{q} \sum_t x_t r_{-i+t}$, from which $J \subseteq K$ follows.

II. Let $\alpha = \sum_i a_i s^i \in K$. Then there exist $x_t \in \mathbb{Z}_\pi$ $(0 \leqq t \leqq M-1)$ such that $q / \sum_t x_t r_t$ in the ring $\mathbb{Z}_\pi$ and $a_i = \frac{1}{q} \sum_t x_t r_{-i+t}$ for each $t \in \mathbb{Z}$. There exist $z_t^{(\nu)} \in \mathbb{Z}$ $(0 \leqq t \leqq M-1,\ \nu = 1, 2, \dots)$ such that $\lim_{\nu\to\infty} z_t^{(\nu)} = x_t$. Since $\frac{1}{q} \sum_t x_t r_t \in \mathbb{Z}_\pi$, there exist $y^{(\nu)} \in \mathbb{Z}$ $(\nu \geqq 1)$ such that $\lim_{\nu\to\infty} y^{(\nu)} = \frac{1}{q} \sum_t x_t r_t$ $= a_0$. For $0 \leqq t \leqq M-1$ and $\nu = 1, 2, \dots$ put

$$x_t^{(\nu)} = \begin{cases} q \cdot y^{(\nu)} - \sum_{v=1}^{M-1} z_v^{(\nu)} r_v & \text{for } t = 0, \\ z_t^{(\nu)} & \text{for } 1 \leqq t \leqq M-1. \end{cases}$$

Then we have $x_t^{(\nu)} \in \mathbb{Z}$ and $\sum_t x_t^{(\nu)} r_t = qy^{(\nu)} \equiv 0 \pmod{q}$ (in $\mathbb{Z}$). Hence $\alpha^{(\nu)} = \sum_t a_i^{(\nu)} s^i \in I$ for each $\nu = 1, 2, \dots$, where $a_i^{(\nu)} = \frac{1}{q} \sum_t x_t^{(\nu)} r_{-i+t}$.

Since $\lim_{\nu\to\infty} q \cdot y^{(\nu)} = \sum_t x_t r_t$, we have $\lim_{\nu\to\infty} x_0^{(\nu)} = \lim_{\nu\to\infty} q \cdot y^{(\nu)} - \sum_{v=1}^{M-1} x_v r_v = x_0$, hence $\lim_{\nu\to\infty} x_t^{(\nu)} = x_t$ for each $0 \le t \le M-1$, which implies $\lim_{\nu\to\infty} a_i^{(\nu)} = a_i$, $\lim_{\nu\to\infty} \alpha^{(\nu)} = \alpha$ and $\alpha \in I_\pi$. The inclusion $K \subseteq I_\pi$ follows.

III. According to 2.7 there exists a basis $\{\beta_1, \dots, \beta_{N+1}\}$ of the $\mathbb{Z}$-module I and according to 3.2 it forms a basis of the $\mathbb{Z}_\pi$-module I_π. There exist $\rho_k \in R$ such that $\rho_k \sum_i r_{-i} s^i = q \cdot \beta_k$ $(1 \leqq k \leqq N+1)$.

Let $\alpha \in I_\pi$. Then there exist $b_k \in \mathbb{Z}_\pi$ such that

$$\alpha = \sum_{k=1}^{N+1} b_k \beta_k .$$

Put $\rho = \sum_{k=1}^{N+1} b_k \rho_k$. Then $\rho \in R_\pi$ and we have $\rho \cdot \sum_i r_{-i} s^i = \sum_{k=1}^{N+1} b_k \rho_k \sum_i r_{-i} s^i = q \cdot \alpha$. The inclusion $I_\pi \subseteq J$ follows immediately.

3.4. Proposition. *We have*

$$I_\pi^- = I_\pi \cap R_\pi^- .$$

Proof. The inclusion $I_\pi^- \subseteq I_\pi \cap R_\pi^-$ follows immediately from the equality $I^- = I \cap R^-$. Let $\alpha \in I_\pi \cap R_\pi^-$ and put as in 2.9 $K_0 = \{1 \le k \le M-1 : r_k \text{ odd}\}$. According to 2.7 and 3.3 the system $\mathcal{S}(K^0) = \{\gamma_k : k \in K^0\} \cup \{\gamma, \delta\}$ forms a basis of the $\mathbb{Z}$-module I_π. Hence there exist $c_k, c, d \in \mathbb{Z}_\pi$ $(k \in K^0)$ such that

$$\alpha = \sum_{k \in K^0} c_k \gamma_k + c\gamma + d\gamma .$$

Then

$$\alpha = \sum_i s^i \left(\frac{1}{q} \sum_{k \in K^0} c_k (r_{-i} r_k - r_{-i+k}) + c r_{-i} + d \right).$$

Since $\alpha \in R_\pi^-$, we have for each $i \in \mathbb{Z}$:

$$\frac{1}{q} \sum_{k \in K^0} c_k (r_{-i} r_k - r_{-i+k}) + c r_{-i} + d + \frac{1}{q} \sum_{k \in K^0} c_k (r_{-i+N} r_k - r_{-i+N+k}) + c r_{-i+N} + d = 0 .$$

According to 1.1

$$\sum_{k\in K^0} c_k(r_k-1)+cq+2d=0\,.$$

Therefore $c=2c'$ for an π-adic integer c' and

$$\sum_{k\in K^0} c_k\frac{1-r_k}{2}=c'q+d\,.$$

Then according to 2.9.3

$$\begin{aligned}\sum_{k\in K^0} c_k\alpha_k \;+c'\alpha_0 &= \sum_{k\in K^0} c_k\gamma_k+(c'q+d)\delta+c\gamma-c'q\delta\\ &= \sum_{k\in K^0} c_k\gamma_k+c\gamma+d\delta=\alpha\,.\end{aligned}$$

The proposition follows from 2.9.2 and 3.2.

3.5. Remark. (Iwasawa [5, Section 2]) makes a mention of the formula in 3.4 but his proof is based on other facts. Another proof of the equality $I_\pi=J$ from 3.3 and Proposition 3.4 is also given in Washington's book [21, §6.4, Lemma 6.2].

3.6. THEOREM. *Let $\mathcal{N}\subseteq\mathcal{M}$ be $\mathbb{Z}$-submodules of the $\mathbb{Z}$-module S with finite bases possessing the same number of elements (thus the index $[\mathcal{M}:\mathcal{N}]$ of the $\mathbb{Z}$-module $\mathcal{N}$ in $\mathbb{Z}$-module $\mathcal{M}$ is finite). Let $(\mathcal{M}/\mathcal{N})_\pi$ denote the π-Sylow subgroup of the factor group $(\mathcal{M}/\mathcal{N},+)$ considered as a $\mathbb{Z}_\pi$-module in the natural way.*

Then the $\mathbb{Z}_\pi$-module $(\mathcal{M}/\mathcal{N})_\pi$ and the $\mathbb{Z}_\pi$-quotient module $\mathcal{M}_\pi/\mathcal{N}_\pi$ are isomorphic (canonically). The $\mathbb{Z}_\pi$-module $\mathcal{N}_\pi$ has a finite index in $\mathbb{Z}_\pi$-module $\mathcal{M}_\pi$, which equals the π-part $[\mathcal{M}:\mathcal{N}]_\pi$ of the index $[\mathcal{M}:\mathcal{N}]$. Hence

$$(\mathcal{M}/\mathcal{N})_\pi\cong\mathcal{M}_\pi/\mathcal{N}_\pi\,,\qquad [\mathcal{M}_\pi:\mathcal{N}_\pi]=[\mathcal{M}:\mathcal{N}]_\pi\,.$$

Proof.

I. We have $[\mathcal{M}:\mathcal{N}]_\pi=\pi^a$, where a is a non-negative integer. Then $\pi^a\cdot\mathcal{M}\subseteq\mathcal{N}_\pi$.

Let $\mu_1,\dots,\mu_m$ be a basis of the $\mathbb{Z}_\pi$-module $\mathcal{M}$. According to 3.2 $\mu_1,\dots,\mu_m$ is a basis of the $\mathbb{Z}_\pi$-module $\mathcal{M}_\pi$. For $\alpha\in\mathcal{M}_\pi$, there exist $a_1,\dots,a_m\in\mathbb{Z}_\pi$ such that

$$\alpha=a_1\mu_1+\cdots+a_m\mu_m\,.$$

Each integer a_i has the form: $a_i = x_i + \pi^a y_i$, where $x_i \in \mathbb{Z}$, $0 \leqq x_i \leqq \pi^a$ and $y_i \in \mathbb{Z}_\pi$. Put

$$\chi(\alpha) = x_1\mu_1 + \cdots + x_m\mu_m .$$

Then $\chi(\alpha) \in \mathcal{M}$, χ is a mapping from $\mathcal{M}_\pi$ into $\mathcal{M}$, $\alpha - \chi(\alpha) \in \mathcal{N}_\pi$ and for $\alpha, \beta \in \mathcal{M}_\pi$, $c \in \mathbb{Z}_\pi$, $\bar{c} \in \mathbb{Z}$, $c \equiv \bar{c} \pmod{\pi^a}$ we have

$$\chi(\alpha+\beta) \equiv \chi(\alpha) + \chi(\beta) \ \ (\pi^a \cdot \mathcal{M}), \qquad \chi(c\alpha) \equiv \bar{c}\chi(\alpha) \ \ (\pi^a \cdot \mathcal{M}).$$

Let ϕ be the projection from $\mathcal{M}/\mathcal{N}$ on the π-Sylow subgroup $(\mathcal{M}/\mathcal{N})_\pi$ of the additive group $\mathcal{M}/\mathcal{N}$. Denote by ψ the canonical mapping from $\mathcal{M}$ on $\mathcal{M}/\mathcal{N}$ and put $\sigma \doteq \phi \circ \psi \circ \chi$. Then σ is a homomorphism from the $\mathbb{Z}_\pi$-module $\mathcal{M}_\pi$ into the $\mathbb{Z}_\pi$-module $(\mathcal{M}/\mathcal{N})_\pi$.

II. We show that

$$\mathcal{M} \cap \mathcal{N}_\pi = \{\alpha \in \mathcal{M} : \text{ order of } \alpha + \mathcal{N} \text{ in } \mathcal{M}/\mathcal{N} \text{ is not divisible by } \pi\}.$$

Let $\alpha \in \mathcal{M} \cap \mathcal{N}_\pi$ and let $\pi^x \cdot y$ be the order of $\alpha + N$ in $\mathcal{M}/\mathcal{N}$ $(x, y \in \mathbb{Z})$, $x \geq 0$, $y > 0$, $\pi \nmid y$. If $\nu_1, \ldots, \nu_m$ is a basis of the $\mathbb{Z}$-module $\mathcal{N}$, then according to 3.2 $\nu_1, \ldots, \nu_m$ is a basis of the $\mathbb{Z}_\pi$-module $\mathcal{N}_\pi$, hence there exist $c_1, \ldots, c_m \in \mathbb{Z}_\pi$ such that $\alpha = \sum_{j=1}^{m} c_j\gamma_j$. If $y \cdot c_j \in \mathbb{Z}$ for each $1 \leq j \leq m$, then $y \cdot \alpha \in \mathcal{N}$, thus $x = 0$. If there exists $1 \leq j \leq m$ such that $y \cdot c_j \notin \mathbb{Z}$, then $\pi^x \cdot y \cdot c_j \notin \mathbb{Z}$, hence $\pi^x \cdot y \cdot \alpha \notin \mathcal{N}$, which is a contradiction. The converse inclusion is obvious.

III. From the formula in II we get that the kernel of $\phi \circ \psi$ equals $\mathcal{M} \cap \mathcal{N}_\pi$. Since $\alpha - \chi(\alpha) \in \mathcal{N}_\pi$ $(\alpha \in \mathcal{M}_\pi)$, it holds that $\chi^{-1}(\mathcal{M} \cap \mathcal{N}_\pi) = \mathcal{N}_\pi$. It follows that the kernel of σ is equal to $\mathcal{N}_\pi$.

The mapping $\phi \circ \psi$ is surjective. For $\mu \in \mathcal{M}$ we have $\mu - \chi(\mu) \in \mathcal{M} \cap \mathcal{N}_\pi$, hence $\phi \circ \psi(\mu) = \sigma(\mu)$, which implies that σ is surjective as well. This completes the proof.

We obtain from this theorem and from 2.9.2, 2.7 and 2.11

3.7. THEOREM. *We have*

(a) $[R_\pi^- : I_\pi^-] = (h_n^-)_\pi$ (I w a s a w a),

(b) $[R_\pi^\star : I_\pi] = (h_n^-)_\pi$,

(c) $$[I_\pi : I_\pi^0] = \begin{cases} 1 & \textit{for } \pi \neq 2, \\ 2 & \textit{for } \pi = 2. \end{cases}$$

The part (a) is due to I w a s a w a [5, (5)].

We obtain in a similar way as in 1.4 $R_\pi^\star = I_\pi + R_\pi^-$, which implies:

3.8 THEOREM. *The quotient-rings* $R_\pi^\star/I_\pi$ *and* R_π^-/I_π^- *are isomorphic (canonically).*

This theorem can be proved by means of 3.7 (a), (b) as well or from 1.5 and 3.6.

3.9. PROPOSITION. *Let* M , N *be* $\mathbb{Z}$*-submodels of the* $\mathbb{Z}$*-module* S *with finite bases and let* $M \cap N = 0$ *. Then*

$$(M \oplus N)_\pi = M_\pi \oplus N_\pi \,.$$

P r o o f . The results follow easily from 3.2.

We obtain from this proposition and from 2.9.4 and 3.7 (c):

3.10. PROPOSITION. *For* $\pi \neq 2$ *we have*

$$I_\pi = I_\pi^- \oplus \delta\mathbb{Z}_\pi \,.$$

(*Note* $\delta\mathbb{Z}_\pi = \delta R_\pi$.)

4. Kummer's elements

In the last three Sections we will assume $n = 0$, hence

$$q = p\,, \qquad M = p - 1\,, \qquad N = \frac{p-1}{2}\,,$$

the group G has order $p - 1$, etc. For the sake of simplicity we put

$$h^- = h_0^- \,.$$

4.1. DEFINITION. *For* $i, \rho \in \mathbb{Z}$ *put*

$$\kappa_{i\rho} = \begin{cases} 1 & \text{for } r_i + r_{i+\rho} \geq p\,, \\ 0 & \text{for } r_i + r_{i+\rho} < p\,, \end{cases}$$

$$\kappa_\rho = \sum_i \kappa_{-i\rho} s^i \in R\,.$$

4.2. Proposition. *Let $i, \rho \in \mathbb{Z}$.*

(a) *If $\rho \equiv N \pmod{M}$, then $\kappa_{i\rho} = 1$ and $\kappa_\rho = \kappa_N = \delta$.*

(b) *Let $\rho \not\equiv N \pmod{M}$. Then*

(b1) $\kappa_{i\rho} + \kappa_{i+N\rho} = 1$,

(b2) $\kappa_{i\rho} = \frac{1}{p}(r_i + r_{i+\rho} - r_{i+\sigma})$, *where* $\sigma = \operatorname{ind}(r_\rho + 1)$,

(b3) $\kappa_{i\rho} = \left[\frac{1}{p}(r_i + r_{i+p})\right]$,

(b4) $\kappa_{i\rho} = \left[\frac{1}{p} r_i(1 + r_\rho)\right] - \left[\frac{1}{p} r_i r_\rho\right]$.

P r o o f. The assertions (a), (b1), (b2) and (b3) are obvious. We get (b4) from the relation $r_{i+\rho} = r_i r_\rho - p\left[\frac{1}{p} r_i r_\rho\right]$ and (b3):

$$\kappa_{i\rho} = \left[\frac{1}{p} r_i(1 + r_\rho) - \left[\frac{1}{p} r_i r_\rho\right]\right] = \left[\frac{1}{p} r_i(1 + r_\rho)\right] - \left[\frac{1}{p} r_i r_\rho\right].$$

4.3. Proposition. *For each $\rho \in \mathbb{Z}$ we have $\kappa_\rho \in I$.*

P r o o f. Since $\kappa_N = \delta \in I$ (2.4), we can assume $0 \le \rho \le p-2$, $\rho \ne N$. Put $\operatorname{ind}(r_\rho + 1) = \sigma$ and

$$x_t = \begin{cases} 1 & \text{for } t = 0 \text{ or } t = \rho \text{ in case } \rho \ne 0, \\ 2 & \text{for } t = 0 \text{ in case } \rho = 0, \\ -1 & \text{for } t = \sigma, \\ 0 & \text{for } 0 \le t \le p-2,\ t \notin \{0, \rho, \sigma\}. \end{cases}$$

Then $\sum_t x_t r_t = 0$ and for each $i \in \mathbb{Z}$ we have $\frac{1}{p}\sum_t x_t r_{-i+t} = \frac{1}{p}(r_{-i} + r_{-i+\rho} - r_{-i+\sigma}) = \kappa_{-i\rho}$ according to 4.3 (b2). This concludes the proof. (Note that it follows also from 4.9.)

4.4. R e m a r k. K u m m e r [7, §11, §12] operated with these elements κ_ρ $(0 \le \rho \le p-2,\ \rho \ne N)$ and proved that these elements annihilate on the class group Γ of the pth cyclotomic field. For this reason we call the elements κ_ρ $(\rho \in \mathbb{Z})$ *Kummer's elements*.

In [15] the following elements from R^- were considered:

$$\phi_j = \sum_i \alpha_{-i\ \operatorname{ind}(j+1)} s^i \qquad (0 \le j \le N-1),$$

where for $i, \rho \in \mathbb{Z}$

$$\alpha_{i\rho} = \begin{cases} 1 & \text{for } r_i + r_{i+\rho} < p\,, \\ -1 & \text{for } r_i + r_{i+\rho} \geq p\,. \end{cases}$$

The following proposition was shown in [15, Theorem 3.3, Consequence 3.4 and conclusion of the proof of Theorem 3.6].

4.5. PROPOSITION.

(a) $|\det(\alpha_{i\,\mathrm{ind}(j+1)})|_{0\leq i,\,j\leq N-1} = 2^{N-1}h^-$.

(b) *For integers* $\rho \not\equiv N \not\equiv \sigma \pmod M$ *the equality*

$$\alpha_{i\rho} = \alpha_{i\sigma} \qquad \textit{for each} \quad i \in \mathbb{Z}$$

is satisfied if and only if $\sigma \equiv \rho \pmod M$ *or* $\sigma \equiv \mathrm{ind}(p-1-r_\rho) \pmod M$.

(c) *The elements* ϕ_j $(0 \leq j \leq N-1)$ *form a basis of the* $\mathbb{Z}_p$*-module* I_p^- .

Since $\alpha_{i+N\rho} = -\alpha_{i\rho}$ $(\rho \not\equiv N \pmod M)$, we have

$$\begin{aligned} &|\det(\alpha_{-i\,\mathrm{ind}(j+1)})|_{0\leq i,\,j\leq N-1} \\ &= |\det(\alpha_{i+N\,\mathrm{ind}\,(j+1)})|_{0\leq i,\,j\leq N-1} \\ &= |\det(\alpha_{i\,\mathrm{ind}\,(j+1)})|_{0\leq i,\,j\leq N-1} = 2^{N-1}h^- \end{aligned}$$

according to 4.5 (a). This determinant is the determinant of the transition matrix from the basis $\varepsilon_i = s^i(1-s^N)$ $(0 \leq i \leq N-1)$ of the $\mathbb{Z}$-module R^- to the elements ϕ_j $(0 \leq j \leq N-1)$. Thus we get from 3.2, 3.6 and 3.7 (a):

4.6. PROPOSITION.

(a) $|\det(\alpha_{-i\,\mathrm{ind}(j+1)})|_{0\leq i,\,j\leq N-1} = 2^{N-1}h^-$.

(b) *The elements* ϕ_j $(0 \leq j \leq N-1)$ *form a basis of the* $\mathbb{Z}$*-module* I_π^- *for each odd prime* π .

The parts (a) and (b) of the following proposition are obvious and the part (c) follows from 4.5 (b).

4.7. PROPOSITION. *Let* $i, j, \rho, \sigma \in \mathbb{Z}$. *Then we have*

(a) $\alpha_{i\rho} = 1 - 2\kappa_{i\rho}$.

(b) $\phi_j = \delta - 2\kappa_{\mathrm{ind}(j+1)}$ $(0 \leq j \leq N-1)$.

(c) *For* $\rho \not\equiv N \not\equiv \sigma \pmod M$ *the equality* $\kappa_{i\rho} = \kappa_{i\sigma}$ *for each* $i \in \mathbb{Z}$ *is satisfied if and only if* $\sigma \equiv \rho \pmod M$ *or* $\sigma \equiv \mathrm{ind}(p-1-r_\rho) \pmod M$. *Hence* $\kappa_\rho = \kappa_\sigma$ *if and only if* $\sigma \equiv \rho \pmod M$ *or* $\sigma \equiv \mathrm{ind}(p-1-r_\rho) \pmod M$.

4.8. THEOREM. *Kummer's elements*

$$\kappa_{\operatorname{ind}(j+1)} \quad (0 \le j \le N-1), \qquad \kappa_N = \delta$$

form a basis of the $\mathbb{Z}$-module I.

Proof. According to 2.3 the elements $\varepsilon_l = s^l(1-s^N)$ $(0 \le l \le N-1)$ and $\varepsilon = \sum_{i=0}^{N-1} s^i$ form a basis $\mathcal{S}^\star$ of the $\mathbb{Z}$-module $R^\star$. For 4.2 (b1) we have for $\rho \in \mathbb{Z}$:

$$\kappa_\rho = \sum_{l=0}^{N-1} (\kappa_{-l\rho} - 1)\varepsilon_l + \varepsilon \qquad (\rho \not\equiv N \pmod{M}),$$

$$\kappa_\rho = \kappa_N = \delta = \sum_{l=0}^{N-1} (-1)\varepsilon_l + 2\varepsilon \qquad (\rho \equiv N \pmod{M}).$$

Thus the transition matrix C from the basis $\mathcal{S}^\star$ to Kummer's elements $K = \{\kappa_{\operatorname{ind}(j+1)} : 0 \le j \le N-1\} \cup \{\kappa_N\}$ has form $C^T = (c_{ij})$ $(0 \le i,\ j \le N)$, where

$$c_{ij} = \begin{cases} \kappa_{-i\operatorname{ind}(j+1)} - 1 & \text{for } 0 \le i,\ j \le N-1, \\ 1 & \text{for } i = N,\ 0 \le j \le N-1, \\ -1 & \text{for } 0 \le i \le N-1,\ j = N, \\ 2 & \text{for } i = j = N. \end{cases}$$

According to 4.7(a) $\kappa_{-i\operatorname{ind}(j+1)} = \frac{1}{2}(1 - \alpha_{-i\operatorname{ind}(j+1)})$, hence

$$\det C = \frac{(-1)^N}{2^N} \cdot \det D,$$

where $D = (d_{ij})$ $(0 \le i,\ j \le N)$ and

$$d_{ij} = \begin{cases} 1 + \alpha_{-i\operatorname{ind}(j+1)} & \text{for } 0 \le i,\ j \le N-1, \\ 1 & \text{for } i = N,\ 0 \le j \le N-1, \\ 2 & \text{for } 0 \le i \le N,\ j = N. \end{cases}$$

If we subtract the last row of the determinant of D from the others, we get

$$\det D = 2\det(\alpha_{-i\operatorname{ind}(j+1)}) \qquad (0 \le i,\ j \le N-1).$$

Proposition 4.6 (a) gives then

$$|\det C| = h^-,$$

and Main Theorem 2.7 completes the proof.

Using 4.2 (b4) we obtain the following relation between *Kummer's elements* and elements γ's.

4.9. PROPOSITION. *We have for* $1 \le j \le p-2$:

(a) $\kappa_{\mathrm{ind}j} = \gamma_{\mathrm{ind}(j+1)} - \gamma_{\mathrm{ind}j}$,

(b) $\sum_{\nu=1}^{j} \kappa_{\mathrm{ind}\nu} = \gamma_{\mathrm{ind}(j+1)}$.

4.10. Remarks.

To show the decomposition of the Lagrange resolvent Kummer ([7, p. 363]) used in fact the following equality:

4.10.1.

$$\sum_{\nu=1}^{p-2} \kappa_{\mathrm{ind}\nu} = \gamma_{\mathrm{ind}(p-1)} = \gamma - \delta .$$

Vandiver [20, Section 1] himself was interested in transformations of *Kummer's elements* κ_ρ $\left(0 \le \rho \le p-2,\ \rho \ne \frac{p-1}{2}\right)$ and he obtained, using 4.9 (b), in fact the equality ([20, (3)]):

4.10.2.

$$s^{\frac{p-1}{2}} \sum_{\nu=1}^{j} \kappa_{\mathrm{ind}\,\nu} = j\delta - \gamma_{\mathrm{ind}(j+1)} \qquad (1 \le j \le p-2)$$

since $s^{\frac{p-1}{2}} \gamma_{\mathrm{ind}(j+1)} = j\delta - \gamma_{\mathrm{ind}(j+1)}$ (2.5 (a)).

When operating with *Fermat's equation*, Fueter [3, (V)] showed in essence 4.9 (a).

Denote $q_i = \dfrac{rr_i - r_{i+1}}{p}$ for $i \in \mathbb{Z}$. Then

$$\gamma_1 = \sum_i q_{-i} s^i = \sum_i q_i s^{-i}, \qquad s^k \gamma_1 = \sum_i q_{-i+k} s^i = \sum_i q_{i+k} s^{-i} \quad (k \in \mathbb{Z}).$$

We have

$$\begin{aligned} q_{i+k} &= \left[\frac{rr_{i+k}}{p}\right] = \left[\frac{rr_i r_k}{p}\right] - r\left[\frac{r_i r_k}{p}\right] \\ &= \left[\frac{r_i r_{k+1}}{p}\right] + \left(\left[\frac{r^{k+1}}{p}\right] - r\left[\frac{r^k}{p}\right]\right) r_i - r\left[\frac{r_i r_k}{p}\right], \end{aligned}$$

since $r_i r_k = r_{i+k} + p\left[\dfrac{r_i r_k}{p}\right]$ and $r^k = r_k + p\left[\dfrac{r^k}{p}\right]$.

It follows

4.10.3. $s^k\gamma_1 = \gamma_{k+1} - r\gamma_k + \left(\left[\frac{r^{k+1}}{p}\right] - r\left[\frac{r^k}{p}\right]\right)\gamma$ $(0 \le k \le p-2)$, which is a slight modification of F u e t e r 's proof of (IV) in [3].

We can obtain from 2.7 and the relation $q_{i+N} = r - 1 - q_i$ on the basis of 4.10.3:

4.10.4. PROPOSITION. *Let $K \subseteq \{0, 1, \dots, p-3\}$ have the basis property, $|K| = N - 1$ and $N - 1 \notin K$. Then the system*

$$\left\{s^k\gamma_1 = \sum_i q_{-i+k}s^i : \ k \in K\right\} \cup \{\gamma, \delta\}$$

forms a basis of the $\mathbb{Z}$-module I.

For $a \in \mathbb{Z}$, $p \nmid a$ denote $q(a)$ the *Fermat quotient* with base a (with respect to the prime p), thus

$$q(a) = \frac{a^{p-1} - 1}{p}.$$

By L e r c h [9, (8)] we have

$$q(a) \equiv \sum_{x=1}^{p-1} (xa)^{p-2}\left[\frac{xa}{p}\right] \pmod{p}. \tag{L}$$

From the considerations of F u e t e r [3] leading to his formula (VII) we can formulate the following:

4.10.5. *For $0 \le h \le p-2$ there exists $\beta_h \in R$ such that*

$$\omega_h = \sum_i r_{-i}\, q(r_{-i+h})s^i + p\beta_h,$$

where $\omega_h = r_{-h}s^h \sum_k r_{-k}\,\gamma_k \in I$.

P r o o f . We have

$$\omega_h = \sum_k r_{-h}r_{-k} \sum_i \left[\frac{r_{-i}r_k}{p}\right] s^{i+h} = \sum_i s^i \sum_k r_{-h}r_{-k}\left[\frac{r_{-i+h}r_k}{p}\right].$$

According to L e r c h 's Theorem (L) the following holds

$$\begin{aligned} r_{-i}q(r_{-i+h}) &\equiv r_{-i}\sum_k r_{i-h}r_{-k}\left[\frac{r_{-i+h}r_k}{p}\right] \pmod{p} \\ &\equiv \sum_k r_{-h}r_{-k}\left[\frac{r_{-i+h}r_k}{p}\right] \pmod{p}, \end{aligned}$$

which concludes the proof.

5. The Stickelberger ideal $\mod p$

Remind that we assume $n = 0$, thus

$$q = p, \qquad M = p - 1, \qquad N = \frac{p-1}{2}, \qquad \text{etc.}$$

Denote further by:

$\mathbb{Z}(p)$ the ring of residue classes $\mod p$, thus $\mathbb{Z}(p) = \mathbb{Z}/p\mathbb{Z}$; the elements from $\mathbb{Z}$ are often considered as the elements from $\mathbb{Z}(p)$,

$R(p)$ $= \mathbb{Z}(p)[G]$ the group ring of G over the ring $\mathbb{Z}(p)$; thus $R(p) = \left\{ \sum\limits_i a_i s^i : a_i \in \mathbb{Z}(p) \right\}$ for $\alpha = \sum\limits_i a_i s^i \in R(p)$ we put $a_j = a_i$, where $j, i \in \mathbb{Z}$, $0 \le i \le M - 1$, $j \equiv i \pmod M$,

$R^\star(p)$ $= \left\{ \alpha = \sum\limits_i a_i s^i \in R(p) : a_k + a_{k+N} = a_l + a_{l+N} \text{ for each } k, l \in \mathbb{Z} \right\}$,

$R^-(p)$ $= \left\{ \alpha = \sum\limits_i a_i s^i \in R(p) : a_k + a_{k+N} = 0 \text{ for each } k \in \mathbb{Z} \right\}$,

$i(p)$ index of irregularity of p; thus $i(p) = \operatorname{card}\left\{ 1 \le a \le \frac{p-3}{2} : p/B_{2a} \right\}$, where B_{2a} mean the *Bernoulli numbers*,

ψ the canonical mapping from $\mathbb{Z}$ onto $\mathbb{Z}(p)$ ($\psi(a) = a + p\mathbb{Z}$, $a \in \mathbb{Z}$). The mapping ψ will also be considered as the mapping from R onto $R(p)$ in this way:
For $\alpha = \sum\limits_i a_i s^i \in R$ we have $\psi(\alpha) = \sum\limits_i \psi(a_i) s^i \in R(p)$.
Obviously, $\psi(R^\star) = R^\star(p)$, $\psi(R^-) = R^-(p)$.

$I(p)$ $= \psi(I)$ the *Stickelberger ideal* of the ring $R(p)$,

$I^-(p)$ $= \psi(I^-)$ the *Stickelberger ideal* of the ring $R^-(p)$.

$R(p)$, $R^\star(p)$, $R^-(p)$, $I(p)$, $I^-(p)$ are considered as $\mathbb{Z}(p)$-modules (hence vector spaces over the field $\mathbb{Z}(p)$).

The following addition to *Iwasawa's class number formula* (0.1) was shown in [19, 2.2]:

5.1. Theorem. (Skula)

$$\left[R^-(p) : I^-(p)\right] = p^{i(p)}.$$

We show a similar addition to Sinnott's formula (0.2):

5.2. Theorem.

$$\left[R^\star(p) : I(p)\right] = p^{i(p)}.$$

First we prove the following lemma:

5.3. LEMMA. *For $\mathbb{Z}(p)$-modules $R^\star(p)$, $R^-(p)$, $I(p)$ and $I^-(p)$ we have*

(a) $R^\star(p) = R^-(p) \oplus \varepsilon\mathbb{Z}(p) = R^-(p) \oplus \delta R(p)$,

(b) $I(p) = I^-(p) \oplus \delta R(p)$.

(The elements ε, δ are considered to be elements from $R(p)$. Note $\delta R(p) = \delta\mathbb{Z}(p)$.)

Proof. The assertion (a) is obvious. According to 2.11 we have $[I : I^0] = 2$, where $I^0 = I^- \oplus \delta R$. Thus $I(p) = \psi(I^0) = \psi(I^-) + \delta R(p)$. The lemma follows by noting that $\delta \notin R^-(p)$.

Proof of Theorem 5.2. According to 5.3 we have

$$\left[R^\star(p) : R^-(p)\right] = p, \qquad \left[I(p) : I^-(p)\right] = p.$$

Using 5.1 we get

$$\begin{aligned} p^{\mathrm{i}(p)+1} &= \left[R^\star(p) : R^-(p)\right] \cdot \left[R^-(p) : I^-(p)\right] = \left[R^\star(p) : I^-(p)\right] \\ &= \left[R^\star(p) : I(p)\right] \cdot \left[I(p) : I^-(p)\right] = \left[R^\star(p) : I(p)\right] \cdot p. \end{aligned}$$

The theorem follows.

Let $1 \le L \le p-2$, L odd. Put

$$\sigma_L = \sum_i r_{-iL} s^i \in R^-(p).$$

It was shown in [18, 3.3, 6.4] (the element σ_L is designated by α_L) that the system $\left\{\sigma_L :\ 3 \le L \le p-2,\ L \text{ odd},\ B_{p-L} \not\equiv 0 \pmod p\right\} \cup \{\sigma_1 = \gamma\}$ forms a basis of the vector space $I^-(p)$ over the field $\mathbb{Z}(p)$. Together with 5.3 (b) we get

5.4. PROPOSITION. *The system*

$$\left\{\sigma_L :\ 3 \le L \le p-2,\ L \text{ odd},\ B_{p-L} \not\equiv 0 \pmod p\right\} \cup \{\gamma, \delta\}$$

forms a basis of the vector space $I(p)$ over the field $\mathbb{Z}(p)$.

6. Kummer's system of congruences

Considering the first case of Fermat's Last Theorem, Kummer [8] introduced a certain system of congruences, which can be transformed in the following form:

$$\varphi_{p-2j}(t) B_{2j} \equiv 0 \pmod p, \qquad 1 \le j \le \frac{p-3}{2}, \tag{K}$$

where $\varphi_i(t) = \sum\limits_{v=1}^{p-1} (-1)^{v-1} v^{i-1} t^v$ $(1 \le i \le p-1)$ are *Mirimanoff polynomials.*

Kummer [8] also proved:

If (x, y, z) is a solution of the first case of Fermat's Last Theorem $(x^p + y^p + z^p = 0,\ p \nmid xyz)$, then the numbers $\frac{x}{y}, \frac{y}{x}, \dots$ must fulfil the congruences (K) *and the congruence*

$$\varphi_{p-1}(t) \equiv 0 \pmod{p}.$$

In [17] we introduced the following system of congruences depending on the *Stickelberger ideal* I_p^- :

$$\begin{aligned} f_\alpha(t) &\equiv 0 \pmod{p} \qquad (\alpha \in I_p^-), \\ \varphi_{p-1}(-t) &\equiv 0 \pmod{p}, \end{aligned} \tag{S}$$

where for $\alpha = \sum_i a_i s^i \in R_p$ (or $\alpha \in R(p)$) put

$$f_\alpha(t) = \sum_{v=1}^{p-1} a_{-\operatorname{ind} v} \bar{v} t^v \qquad (\bar{v} \in \mathbb{Z},\ 0 < \bar{v} < p,\ v\bar{v} \equiv 1 \pmod{p}).$$

From the results of [17] we can find that the system (S) and (K) are equivalent in the following sense:

6.1. Proposition. *Let $\tau \in \mathbb{Z}$, $\tau \not\equiv -1 \pmod{p}$. Then τ is a solution of the system* (K) *and the congruence $\varphi_{p-1}(t) \equiv 0 \pmod{p}$ if and only if $-\tau$ is a solution of* (S).

The polynomial $\varphi_{p-1}(t)$ does indeed occur among the polynomials $f_\alpha(t)$ since we have $f_\delta(t) \equiv -\varphi_{p-1}(-t) \pmod{p}$. Then we get from 5.3 (b):

6.2. Proposition. *The system* (S) *is equivalent to the following system of congruences or equations:*

$$f_\alpha(t) \equiv 0 \pmod{p} \qquad (\alpha \in J),$$

where J means I_p or I, or

$$f_\alpha(t) = 0 \qquad (\alpha \in I(p)).$$

Note that $f_{\sigma_L}(t) \equiv -\varphi_L(-t) \pmod{p}$ for elements σ_L $(1 \le L \le p-2)$ and the "equivalence" between (K) and (S) can be obtained by the choice of the basis

$$\{\sigma_L :\ 3 \le L \le p-2,\ L \text{ odd},\ B_{p-L} \not\equiv 0 \pmod{p}\} \cup \{\gamma, \delta\}$$

of the vector space $I(p)$ (5.4).

Le Lidec ([10], [11]) introduced and investigated for $1 \le n \le p-2$ the following polynomials:

$$L_n(t) = \sum_{v=1}^{p-1} \bar{v} t^{p-1-v} \qquad (\, \overline{\langle n+1 \rangle \cdot n \cdot v} < v \,),$$

where the inequality $\overline{(n+1) \cdot n \cdot v} < v$ means that $m < v$ for $1 \le m \le p-1$, $m \equiv \overline{(n+1)} \cdot n \cdot v \pmod{p}$.

Consider the following system of congruences:

$$\begin{gathered} L_n(t) \equiv 0 \pmod{p} \qquad (\, 1 \le n \le p-2 \,), \\ \varphi_{p-1}\Big(-\frac{1}{t}\Big) \equiv 0 \pmod{p}. \end{gathered} \tag{L}$$

In [17, (1.4)] it was shown that the system (S) and (L) are "equivalent" in the following sense:

6.3. Proposition. *Let λ, σ be integers with the property $\lambda \cdot \sigma \equiv 1 \pmod{p}$. Then λ is a solution of the system* (L) *if and only if σ is a solution of the system* (S).

We can obtain a proof of this proposition by choice of the basis from *Kummer's elements*

$$\{\kappa_{\mathrm{ind}(j+1)} : \ 0 \le j \le N-1\} \cup \{\kappa_N = \delta\}$$

(4.8) of the $\mathbb{Z}$-module I. We have namely for $1 \le n \le p-2$, $0 \le \rho \le p-2$, $\rho \ne \frac{p-1}{2}$, $r_\rho \equiv -\overline{(n+1)}n \pmod{p}$

$$f_{\kappa_\rho}(t) \equiv L_n\Big(\frac{1}{t}\Big) \pmod{p}.$$

Fueter, solving the first case of Fermat's Last Theorem, derived the following system of congruences ([3, (VI), (VII)]):

$$\begin{gathered} \sum_{n=1}^{p-1} \frac{1}{n}\Big[\frac{an}{p}\Big] t^n \equiv 0 \pmod{p} \qquad (\, 1 \le a \le p-1 \,), \\ \sum_{n=1}^{p-1} \frac{1}{n} t^n \equiv 0 \pmod{p}, \end{gathered} \tag{F$_1$}$$

$$\sum_i \mathrm{q}(r_{i+h}) t^{r_i} \equiv 0 \pmod{p} \qquad (\, 0 \le h \le p-2 \,). \tag{F$_2$}$$

If we put $a = r_k$ $(1 \le a \le p-1,\ 0 \le k \le p-2)$, we get

$$f_{\gamma_k}(t) \equiv \sum_{n=1}^{p-1} \frac{1}{n}\left[\frac{an}{p}\right] t^n \pmod{p}.$$

Further $f_\delta(t) \equiv \sum_{n=1}^{p-1} \frac{1}{n} t^n \pmod{p}$, $f_\gamma(t) \equiv \sum_{v=1}^{p-1} t^v \pmod{p}$ and $f_{\omega_h}(t) \equiv \sum_i \mathrm{q}(r_{i+h}) t^{r_i} \pmod{p}$. (Note that 1 is no solution of (F_1) $(a = p-1.)$)
This follows from

6.4. Proposition. *The system congruences* (F_1) *and* (S) *are equivalent. Each solution of* (S) *is also a solution of the system of congruences* (F_2).

Remark. Suppose $0 \le h \le p-2$. Put $a = r_h$ and $n = r_{-i}$ for $0 \le i \le p-2$. Then

$$a^{p-1} n^{p-1} - r_{-i+h}^{p-1} \equiv -p r_{-i+h}^{p-2}\left[\frac{an}{p}\right] \pmod{p^2}$$

since $an = p\left[\frac{an}{p}\right] + r_{-i+h}$. Hence

$$a^{p-1} - 1 + a^{p-1}\bigl(n^{p-1} - 1\bigr) - \bigl(r_{-i+h}^{p-1} - 1\bigr) \equiv -p r_{-i+h}^{p-2}\left[\frac{an}{p}\right] \pmod{p^2},$$

which implies

$$q(r_h) + q(r_{-i}) - q(r_{-i+h}) \equiv -r_{-i+h}^{p-2}\left[\frac{an}{p}\right] \pmod{p}.$$

Multiplying by $r_h r_{-i}$ we get

$$r_h\bigl(r_{-i} q(r_h) + r_{-i} q(r_{-i}) - r_{-i} q(r_{-i+h})\bigr) \equiv -\frac{1}{p}(r_{-i} r_h - r_{-i+h}) \pmod{p}.$$

Therefore according to 4.10.5 there exists $\nu_h \in R$ such that

$$r_h\bigl(q(r_h)\gamma + \omega_0 - p\beta_0 - \omega_h + p\beta_h\bigr) = -\gamma_h + p\nu_h,$$

which implies existence of an element $\mu_h \in R$ such that

$$\gamma_h = r_h\omega_h - r_h\omega_0 - r_h q(r_h)\gamma + p\mu_h \qquad (0 \le h \le p-2). \tag{A}$$

We get from (A):
each solution τ *of the system* (F_2), $\tau \not\equiv 1 \pmod p$ *and the congruence* $f_\delta(t) \equiv \sum_{n=1}^{p-1} \frac{1}{n} t^n \pmod p$ *is a solution of the system* (S).

A c k n o w l e d g e m e n t . T . A g o h called my attention to this implication ($(F_2) \implies (S)$), which was proved by him. The equality (A) is a translation of Agoh's formulas using polynomials to the language of the group ring R.

B e n n e t o n [2] considered the following system of congruences

$$\sum_{\substack{v=1 \\ \widetilde{vn} > \frac{p}{2}}}^{p-1} \bar{v} t^v \equiv 0 \pmod p \qquad (1 \le n \le p-1), \tag{B}$$

where $\widetilde{vn}$ means the least positive residue of $vn \bmod p$. (Quotation from [4, Theorem L3 (h)].) He proved that for each solution t of (K) ($t \not\equiv -1 \pmod p$) $-t$ is a solution of (B), therefore *each solution of* (S) *is a solution of* (B).

For $i, \rho \in \mathbb{Z}$ *put*

$$\beta_{i\rho} = \begin{cases} 1 & \textit{for } r_{i+\rho} > \frac{p}{2}, \\ 0 & \textit{for } r_{i+\rho} < \frac{p}{2}, \end{cases}$$

$$\beta_\rho = \sum_i \beta_{-i\rho} s^i \in R.$$

Then we have

6.5. Proposition.

(a) $\beta_\rho = \kappa_0 s^\rho \in I$ *for each integer* ρ (κ_0 *is Kummer's element*),

(b) $f_{\beta_\rho}(t) = \sum_{v=1}^{p-1} \bar{v} t^v$ ($\widetilde{vn} > \frac{p}{2}$),
where $1 \le n \le p-1$ *and* $\rho = \operatorname{ind} n$, *hence*

(c) *each solution of* (S) *is a solution of* (B).

Note that A g o h [1] proved in fact *both systems* (S) *and* (B) *are equivalent in case* 2 *is a primitive root* $\bmod p$.

REFERENCES

[1] AGOH, T.: *On Fermat's last theorem*, C.R. Math. Rep. Acad. Sci. Canada **VII** (1990), 11–15.

[2] BENNETON, G.: *Sur le dernier théorème de Fermat*, Ann. Sci. Univ. Besançon Math. **3** (1974), 15pp.

[3] FUETER, R.: *Kummers Kriterium zum letzten Theorem von Fermat*, Math. Ann. **85** (1922), 11–20.

[4] GRANVILLE, A. J.: *Diophantine Equations with Varying Exponents (with Special Reference to Fermat's Last Theorem)*, Ph. D. thesis, Queen's University, 1987.

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

[6] KUČERA, R.: *On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic fields*, J. Number Theory **40** (1992), 284–316.

[7] KUMMER, E. E.: *Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren*, J. Reine Angew. Math. **35** (1847), 327–367, (Coll. Papers I, 211–251).

[8] KUMMER, E. E.: *Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen, für den Fall, daß die Klassenanzahl durch λ theilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, Abh. Königl. Akad. Wiss., Berlin (1857), 41–74, (Coll. Papers I, 639–692).

[9] LERCH, M.: *Zur Theorie des Fermatschen Quotienten $(a^{p-1}-1)/p = q(a)$*, Math. Ann. **60** (1905), 471–490.

[10] LE LIDEC, P.: *Sur une forme nouvelle des congruences de Kummer-Mirimanoff*, C.R. Acad. Sci. Paris Sér. A **265** (1967), 89–90.

[11] LE LIDEC, P.: *Nouvelle forme des congruences de Kummer-Mirimanoff pour le premier cas du théorème de Fermat*, Bull. Soc. Math. France **97** (1969), 321–328.

[12] NEWMAN, M.: *A table of the first factor for prime cyclotomic fields*, Math. Comp. **24(109)** (1970), 215–219.

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

[14] SINNOTT, W.: *On the Stickelberger ideal and the circular units of an abelian field.* In: Invent. Math. 62, Springer, Berlin-New York, 1980, pp. 181–234.

[15] SKULA, L.: *Index of irregularity of a prime*, J. Reine Angew. Math. **315** (1980), 92–106.

[16] SKULA, L.: *Another proof of Iwasawa's class number formula*, Acta Arith. **XXXIX** (1981), 1–6.

[17] SKULA, L.: *A remark on Mirimanoff polynomials*, Comment. Math. Univ. St. Paul. **31** (1982), 89–97.

[18] SKULA, L.: *Systems of equations depending on certain ideals*, Arch. Math. (Brno) **21** (1985), 23–38.

[19] SKULA, L.: *A note on the index of irregularity*, J. Number Theory **22** (1986), 125–138.

[20] VANDIVER, H. S.: *A property of cyclotomic integers and its relation to Fermat's last theorem*, Ann. of Math. **21** (1919-20), 73–80.

[21] WASHINGTON, L. C.: *Introduction to Cyclotomic Fields*, Springer-Verlag, New York-Heidelberg-Berlin, 1982.

Received May 22, 1992

Department of Mathematics
Faculty of Science
Masaryk University
Janáčkovo nám. 2a
662 95 Brno
Czech Republic