ACTA ARITHMETICA
LI (1988)

A note on power series representations in local fields

by

TUTOMU SHIMADA (Yokohama)

Introduction. Let p be a prime number and Q_p the field of p-adic numbers. Every element $\alpha \in Q_p$ has a unique representation as a power series in p,

$$\alpha = \sum_{-\infty < i} a_i p^i, \quad a_i \in \{0, 1, \ldots, p-1\}.$$

It is well known that a p-adic number $\alpha = \sum_{-\infty < i} a_i p^i$ is rational if and only if the sequence of coefficients a_i is periodic from some index i on. This equivalence relation is a characterization of the field of rational numbers Q in Q_p. It is natural to ask whether or not a similar relation holds for an algebraic number field of finite degree over Q. The purpose of this paper is to investigate this question.

1. Sufficient conditions. Now we introduce the following notation. Let k and $\mathfrak{O}$ be an algebraic number field of finite degree over Q and the ring of algebraic integers of k respectively. Throughout the present paper, $\mathfrak{p}$ denotes a fixed prime ideal in $\mathfrak{O}$. By $| \ |_{\mathfrak{q}}$ we shall denote a so-called normalized multiplicative valuation corresponding to a divisor $\mathfrak{q}$ of k. If $\mathfrak{q}$ is a prime ideal, $| \ |_{\mathfrak{q}}$ is non-archimedean; if $\mathfrak{q}$ is one of the archimedean divisors $\mathfrak{p}_{\infty,i}$ ($i = 1, 2, \ldots, r_1+r_2$), $| \ |_{\mathfrak{q}}$ is archimedean. Here, r_1 and r_2 denote the number of real archimedean divisors and that of complex archimedean divisors respectively. By a residue system we mean a complete residue system, containing 0, of the ring $\mathfrak{O}$ modulo $\mathfrak{p}$, and by a prime element we mean an element ω of k such that $|\omega|_{\mathfrak{p}} = N_{\mathfrak{p}}^{-1}$, here, $N_{\mathfrak{p}}$ denotes the index $[\mathfrak{O}:\mathfrak{p}]$. Let $k_{\mathfrak{p}}$ be the completion of k with respect to $| \ |_{\mathfrak{p}}$. If we choose a residue system S and a prime element ω, every element α of $k_{\mathfrak{p}}$ has a unique representation as a power series in ω, $\alpha = \sum_{-\infty \ll i} a_i \omega^i$, $a_i \in S$. We say that the power series has periodic coefficients when there exist integers $\gamma > 0$ and ν such that $a_i = a_{i+\gamma}$ for all $i \geqslant \nu$. If $\gamma_0 > 0$ is the smallest integer such that $a_i = a_{i+\gamma_0}$ for all $i \geqslant \nu$, then we call γ_0 the period of α. We say that the equivalence relation $E_{\mathfrak{p}}(\omega, S)$

holds when, for any $\alpha \in k_{\mathfrak{p}}$ ($\alpha = \sum_{-\infty \leqslant i} a_i \omega^i$, $a_i \in S$), α belongs to k if and only if the sequence of coefficients a_i is periodic. When the sequence of coefficients a_i is periodic, then α belongs to k clearly. So we shall study whether or not the representation of any element $\alpha = \sum_{-\infty \leqslant i} a_i \omega^i \in k$ has periodic coefficients.

THEOREM 1. *Suppose that there exists a prime element ω satisfying $|\omega|_{\mathfrak{q}} \geqslant 1$ for all non-archimedean $\mathfrak{q} \neq \mathfrak{p}$ and $|\omega|_{\mathfrak{p}_{\infty,i}} > 1$ for all $i = 1, 2, \ldots, r_1 + r_2$. Then $E_{\mathfrak{p}}(\omega, S)$ holds for all S.*

Proof. It is sufficient to prove that the series representation of any $\alpha \in k$ has periodic coefficients. Take a residue system S. Without loss of generality, we may assume that $\alpha \in k$ is a $\mathfrak{p}$-unit, $\alpha = \sum_{i=0} a_i \omega^i$ ($a_i \in S$, $a_0 \neq 0$). Let $\{\alpha_n\}$ ($n = 1, 2, 3, \ldots$) be the sequence defined by

$$\alpha_n = \{\alpha - (a_0 + a_1 \omega + \ldots + a_{n-1} \omega^{n-1})\} \omega^{-n} \in k.$$

If $\mathfrak{q}$ is a non-archimedean divisor such that $|\omega|_{\mathfrak{q}} = 1$, then

$$\begin{aligned} |\alpha_n|_{\mathfrak{q}} &= |\alpha - (a_0 + a_1 \omega + \ldots + a_{n-1} \omega^{n-1})|_{\mathfrak{q}} \\ &\leqslant \max \{|\alpha|_{\mathfrak{q}}, |a_0|_{\mathfrak{q}}, |a_1 \omega|_{\mathfrak{q}}, \ldots, |a_{n-1} \omega^{n-1}|_{\mathfrak{q}}\} \\ &\leqslant \max \{|\alpha|_{\mathfrak{q}}, 1\}, \quad \text{for all } n \geqslant 1. \end{aligned}$$

If $\mathfrak{q}$ is a non-archimedean divisor such that $|\omega|_{\mathfrak{q}} > 1$, then

$$\begin{aligned} |\alpha_n|_{\mathfrak{q}} &\leqslant \max \{|\alpha \omega^{-n}|_{\mathfrak{q}}, |a_0 \omega^{-n}|_{\mathfrak{q}}, |a_1 \omega^{-n+1}|_{\mathfrak{q}}, \ldots, |a_{n-1} \omega^{-1}|_{\mathfrak{q}}\} \\ &\leqslant \max \{|\alpha \omega^{-n}|_{\mathfrak{q}}, |\omega^{-n}|_{\mathfrak{q}}, |\omega^{-n+1}|_{\mathfrak{q}}, \ldots, |\omega^{-1}|_{\mathfrak{q}}\} \\ &= \max \{|\alpha \omega^{-n}|_{\mathfrak{q}}, |\omega|_{\mathfrak{q}}^{-1}\} \quad \text{for all } n \geqslant 1. \end{aligned}$$

Now let Ms denotes the real number $\max \{|a|_{\mathfrak{p}_{\infty,i}} | a \in S, i = 1, 2, \ldots, r_1 + r_2\}$. If $\mathfrak{q}$ is an archimedean divisor, then

$$\begin{aligned} |\alpha_n|_{\mathfrak{q}} &\leqslant |\alpha \omega^{-n}|_{\mathfrak{q}} + |a_0 \omega^{-n}|_{\mathfrak{q}} + |a_1 \omega^{-n+1}|_{\mathfrak{q}} + \ldots + |a_{n-1} \omega^{-1}|_{\mathfrak{q}} \\ &\leqslant |\alpha \omega^{-n}|_{\mathfrak{q}} + Ms |\omega|_{\mathfrak{q}}^{-1} (|\omega|_{\mathfrak{q}}^{-n+1} + \ldots + |\omega|_{\mathfrak{q}}^{-1} + 1) \\ &< |\alpha \omega^{-n}|_{\mathfrak{q}} + Ms |\omega|_{\mathfrak{q}}^{-1} (1 - |\omega|_{\mathfrak{q}}^{-1})^{-1} \\ &= |\alpha \omega^{-n}|_{\mathfrak{q}} + Ms (|\omega|_{\mathfrak{q}} - 1)^{-1} \quad \text{for all } n \geqslant 1. \end{aligned}$$

In case $\mathfrak{q} = \mathfrak{p}$, as every α_n $\mathfrak{p}$-integer, we have $|\alpha_n|_{\mathfrak{p}} \leqslant 1$ for all $n \geqslant 1$. Therefore every α_n is included in some compact subset of the adele ring $R(k)$ of k. Since k is a discrete subset of $R(k)$, we have $\alpha_\mu = \alpha_\lambda$ for some natural numbers μ, λ such that $\mu < \lambda$. Then

$$\begin{aligned} \alpha &= a_0 + a_1 \omega + \ldots + a_{\mu-1} \omega^{\mu-1} + \alpha_\mu \omega^\mu \\ &= a_0 + a_1 \omega + \ldots + a_{\mu-1} \omega^{\mu-1} + a_\mu \omega^\mu + \ldots + a_{\lambda-1} \omega^{\lambda-1} + \alpha_\lambda \omega^\lambda, \end{aligned}$$

so that the series $\alpha = \sum_{i=0} a_i \omega^i$ has periodic coefficients from μ on. This proves our theorem.

Now we define a real valued function φ of divisors in k such that $\varphi(\mathfrak{q}) > 0$ for all divisors and $\varphi(\mathfrak{q}) = 1$ for all but a finite number of divisors. Let $V(\varphi)$ be a parallelotope in $R(k)$ with respect to φ, i.e.

$$V(\varphi) = \{(x_{\mathfrak{q}}) \in R(k) |\ |x_{\mathfrak{q}}|_{\mathfrak{q}} \leqslant \varphi(\mathfrak{q}) \text{ for all } \mathfrak{q}\},$$

and let $\|\varphi\| = \prod_{\mathfrak{q}} \varphi(\mathfrak{q})$.

COROLLARY TO THEOREM 1. *Let ω be a prime element satisfying the same conditions as in Theorem 1 and let S be a residue system. Then the period of each $\alpha \in \mathfrak{O}$ is bounded.*

Proof. From the proof of Theorem 1 we have following inequalities:

(1) If $\mathfrak{q}$ is non-archimedean and $|\omega|_{\mathfrak{q}} = 1$, then $|\alpha_n|_{\mathfrak{q}} \leqslant \max \{|\alpha|_{\mathfrak{q}}, 1\}$ for all $n \geqslant 1$;

(2) If $\mathfrak{q}$ is non-archimedean and $|\omega|_{\mathfrak{q}} > 1$, then $|\alpha_n|_{\mathfrak{q}} \leqslant \max \{|\alpha|_{\mathfrak{q}} |\omega|_{\mathfrak{q}}^{-n}, |\omega|_{\mathfrak{q}}^{-1}\}$ for all $n \geqslant 1$;

(3) If $\mathfrak{q}$ is archimedean, then $|\alpha_n|_{\mathfrak{q}} < |\alpha|_{\mathfrak{q}} |\omega|_{\mathfrak{q}}^{-n} + Ms(|\omega|_{\mathfrak{q}} - 1)^{-1}$ for all $n \geqslant 1$;

(4) If $\mathfrak{q} = \mathfrak{p}$, then $|\alpha_n|_{\mathfrak{q}} \leqslant 1$ for all $n \geqslant 1$.

Therefore, if $\alpha \in \mathfrak{O}$ then we have

(I) $|\alpha_n|_{\mathfrak{q}} \leqslant 1$ for all non-archimedean $\mathfrak{q}$ and $n \geqslant 1$,

(II) $|\alpha_n|_{\mathfrak{q}} < |\alpha|_{\mathfrak{q}} |\omega|_{\mathfrak{q}}^{-n} + Ms(|\omega|_{\mathfrak{q}} - 1)^{-1}$ for all archimedean $\mathfrak{q}$ and $n \geqslant 1$.

We define

$$\varphi(\mathfrak{q}) = \begin{cases} 1 & \text{if } \mathfrak{q} \text{ is non-archimedean,} \\ Ms(|\omega|_{\mathfrak{q}} - 1) & \text{if } \mathfrak{q} \text{ is archimedean.} \end{cases}$$

It is clear that φ depends only on ω, S and is independent of α. By inequalities (I) and (II), we can see that α_n belongs to $V(\varphi)$ for all sufficiently large n. Therefore the period of each $\alpha \in \mathfrak{O}$ is bounded by the number of elements of $V(\varphi) \cap k$. This completes the proof.

The following lemma is well known.

LEMMA (S. Iyanaga [3]). *If $\|\varphi\| > 2^{r_2} \pi^{-r_2} |d_k|^{1/2}$, then there exists a non-zero element in $V(\varphi) \cap k$.*

Here $|d_k|$ is the ordinary absolute value of the discriminant of k. We then have the following theorem.

THEOREM 2. *Assume that $N_{\mathfrak{p}} > 2^{r_2} \pi^{-r_2} |d_k|^{1/2}$. Then, there is a prime element ω such that $E_{\mathfrak{p}}(\omega, S)$ holds for all S.*

Proof. Let ε be a real number such that $0<\varepsilon<1$ and $N_\mathfrak{p}\times\varepsilon^{[k:\mathbf{Q}]}>2^{r_2}\pi^{-r_2}|d_k|^{1/2}$. We define φ as follows

$$\varphi(\mathfrak{q})=\begin{cases}N_\mathfrak{p} & \text{if } \mathfrak{q}=\mathfrak{p},\\ 1 & \text{if } \mathfrak{q}\neq\mathfrak{p} \text{ is non-archimedean},\\ \varepsilon^{\delta_i} & \text{if } \mathfrak{q}=\mathfrak{p}_{\infty,i}\ (1\leqslant i\leqslant r_1+r_2).\end{cases}$$

Here δ_i is 1 if $\mathfrak{p}_{\infty,i}$ is real, and 2 if $\mathfrak{p}_{\infty,i}$ is complex. Since $\|\varphi\|=N_\mathfrak{p}\times\varepsilon^{[k:\mathbf{Q}]}>2^{r_2}\pi^{-r_2}|d_k|^{1/2}$, by the Lemma, there exists an element $\varrho\neq 0$ in $V(\varphi)\cap k$. Put $\omega=\varrho^{-1}$, then we have $|\omega|_\mathfrak{p}\geqslant N_\mathfrak{p}^{-1}$, $|\omega|_\mathfrak{q}\geqslant 1$ for all non-archimedean divisors $\mathfrak{q}\neq\mathfrak{p}$ and $|\omega|_{\mathfrak{p}_{\infty,i}}>1$ for all $i=1,\ldots,r_1+r_2$. Since $\prod_\mathfrak{q}|\omega|_\mathfrak{q}=1$, we have $|\omega|_\mathfrak{p}=N_\mathfrak{p}^{-1}$, therefore by Theorem 1 our theorem is proved.

2. A necessary condition. Next, we study a necessary condition for the equivalence relation.

THEOREM 3. *Suppose that $E_\mathfrak{p}(\omega, S)$ holds, then we have $|\omega|_\mathfrak{q}\geqslant 1$ for all divisors $\mathfrak{q}\neq\mathfrak{p}$.*

Proof. Let $\alpha\in k$ be a $\mathfrak{p}$-unit, that is, $\alpha=\sum_{i=0} a_i\omega^i$ $(a_i\in S,\ a_0\neq 0)$. In our case, the sequence $\{\alpha_n\}$ $(n=1,2,\ldots)$ defined similarly to in the proof of Theorem 1 is periodic from some index on. Therefore, $\max\{|\alpha_n|_\mathfrak{q}|\ n=1,2,\ldots\}$ is bounded for all $\mathfrak{q}$. Now assume that $\mathfrak{q}\neq\mathfrak{p}$ is a non-archimedean divisor such that $|\omega|_\mathfrak{q}<1$. Then

$$\begin{aligned}|\alpha_n|_\mathfrak{q} &\geqslant |\alpha\omega^{-n}|_\mathfrak{q}-|a_0\omega^{-n}+a_1\omega^{-n+1}+\ldots+a_{n-1}\omega^{-1}|_\mathfrak{q}\\ &\geqslant |\alpha\omega^{-n}|_\mathfrak{q}-\max\{|a_0\omega^{-n}|_\mathfrak{q}, |a_1\omega^{-n+1}|_\mathfrak{q},\ldots,|a_{n-1}\omega^{-1}|_\mathfrak{q}\}\\ &\geqslant |\alpha\omega^{-n}|_\mathfrak{q}-|\omega^{-n}|_\mathfrak{q}=(|\alpha|_\mathfrak{q}-1)|\omega|_\mathfrak{q}^{-n}.\end{aligned}$$

If we take an element $\alpha\in k$ such that $|\alpha|_\mathfrak{q}-1>0$, then $|\alpha_n|_\mathfrak{q}\to\infty$ $(n\to\infty)$ that is a contradiction. Consequently $|\omega|_\mathfrak{q}\geqslant 1$ for all non-archimedean divisors $\mathfrak{q}\neq\mathfrak{p}$. Next, assume that $\mathfrak{q}$ is an archimedean divisor such that $|\omega|_\mathfrak{q}<1$. Then

$$\begin{aligned}|\alpha_n|_\mathfrak{q} &\geqslant |\omega|_\mathfrak{q}^{-n}\{|\alpha|_\mathfrak{q}-(|a_0|_\mathfrak{q}+|a_1\omega|_\mathfrak{q}+\ldots+|a_{n-1}\omega^{n-1}|_\mathfrak{q})\}\\ &\geqslant |\omega|_\mathfrak{q}^{-n}\{|\alpha|_\mathfrak{q}-Ms(1+|\omega|_\mathfrak{q}+\ldots+|\omega|_\mathfrak{q}^{n-1})\}\\ &> |\omega|_\mathfrak{q}^{-n}\{|\alpha|_\mathfrak{q}-Ms(1-|\omega|_\mathfrak{q})^{-1}\},\end{aligned}$$

where Ms is the same as in the proof of Theorem 1. If we take α to be a sufficiently large natural number which is prime to p, we may assume that $|\alpha|_\mathfrak{q}-Ms(1-|\omega|_\mathfrak{q})^{-1}>0$. Then, $|\alpha_n|_\mathfrak{q}\to\infty$ $(n\to\infty)$ that is a contradiction and our theorem is proved.

This theorem shows us that the number of prime elements ω such that $E_\mathfrak{p}(\omega, S)$ holds for all S is only finite.

Now let $E_\mathfrak{p}(\omega, S)$ hold and let m_1 be a natural number $\geqslant 2$ which is prime to p and $|\omega m_1|_\mathfrak{q}<1$ for some non-archimedean divisor $\mathfrak{q}$ and let m_2 be a natural number prime to p such that $|\omega m_2^{-1}|_\mathfrak{q}<1$ for some archimedean divisor $\mathfrak{q}$. Then although ωm_1 and ωm_2^{-1} are prime elements, neither $E_\mathfrak{p}(\omega m_1, S)$ nor $E_\mathfrak{p}(\omega m_2^{-1}, S)$ holds for any S. In case of $k=\mathbf{Q}$, let m_1 be as above, there is a rational number which is never represented as a power series in pm_1 with periodic coefficients. In fact, from the proof of Theorem 3, m_1^{-1} is such a rational number.

If k is totally real, then the condition for ω in Theorem 1 is necessary and sufficient for $E_\mathfrak{p}(\omega, S)$ to be valid. If k is imaginary quadratic and $\mathfrak{p}$ is principal, then a generator of $\mathfrak{p}$ satisfies inequalities for ω in Theorem 1.

Now we let

$$q=\begin{cases}p & \text{if } p\neq 2,\\ 4 & \text{if } p=2,\end{cases}$$

and let ζ_q and $\mathfrak{p}$ be a primitive qth root of unity and the unique prime ideal in $k=\mathbf{Q}(\zeta_q)$ lying above p respectively. Then $\omega=1-\zeta_q$ is a prime element. By Theorem 1 and Theorem 3, we can see that, for all S, if $q\leqslant 5$ then $E_\mathfrak{p}(\omega, S)$ holds and if $q>5$ then $E_\mathfrak{p}(\omega, S)$ never holds.

3. Counterexamples. Lastly, we shall prove a theorem concerning counterexamples.

THEOREM 4. *Assume that the ideal (2) ramifies completely for $k/\mathbf{Q}$, and the prime ideal $\mathfrak{p}$ of $\mathfrak{O}$ lying above (2) is not principal. Then $E_\mathfrak{p}(\omega, S)$ does not hold for any ω and S.*

Proof. Suppose that $E_\mathfrak{p}(\omega, S)$ holds. The assumption and the previous theorem show that $|\omega|_\mathfrak{p}=2^{-1}$, $|\omega|_\mathfrak{q}=1$ or $\geqslant 3$ for all non-archimedean $\mathfrak{q}\neq\mathfrak{p}$ and $|\omega|_\mathfrak{q}\geqslant 1$ for all archimedean $\mathfrak{q}$. From the product formula $\prod_\mathfrak{q}|\omega|_\mathfrak{q}=1$ we have $|\omega|_\mathfrak{q}=1$ for all non-archimedean $\mathfrak{q}\neq\mathfrak{p}$, therefore $\mathfrak{p}$ must be principal. This is a contradiction and proves our theorem.

EXAMPLE. Let m be a square-free rational integer $\equiv 5 \pmod 8$ and let $k=\mathbf{Q}(\sqrt{-4m})$, $\mathbf{Q}(\sqrt{-8m})$ or $\mathbf{Q}(\sqrt{8m})$. Then k satisfies the assumption of Theorem 4.

4. The case of characteristic $p>0$. In the rest of this paper we shall treat the case of characteristic $p>0$. Let F be a finite field of characteristic $p>0$ and k a finitely generated extension of F, of degree of transcendence 1 over F. We assume that F is algebraically closed in k. Under the same notation as in previous sections, we have

THEOREM 5. *$E_{\mathfrak{p}}(\omega, S)$ holds if and only if $|\omega|_{\mathfrak{q}} \geqslant 1$ for all $\mathfrak{q} \neq \mathfrak{p}$.*

Proof. As Theorems 1 and 3.

We define

$$\varphi(\mathfrak{q}) = \begin{cases} 1 & \text{if } \mathfrak{q} \neq \mathfrak{p}, \\ N_{\mathfrak{p}} & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

When $E_{\mathfrak{p}}(\omega, S)$ holds, by Theorem 5, ω^{-1} belongs to $V(\varphi) \cap k$ which is a vector space with finite dimension over F. Let $\dim \mathfrak{p}$ be the dimension of $V(\varphi) \cap k$. As

$$F = \{(x_{\mathfrak{q}}) \in R(k) \mid |x_{\mathfrak{q}}|_{\mathfrak{q}} = 1 \text{ for all } \mathfrak{q}\} \cap k,$$

we have

COROLLARY 1 TO THEOREM 5. *There exists a prime element ω satisfying $|\omega|_{\mathfrak{q}} \geqslant 1$ for all $\mathfrak{q} \neq \mathfrak{p}$ if and only if $\dim \mathfrak{p} \geqslant 2$.*

Furthermore, we can see easily a following corollary.

COROLLARY 2 TO THEOREM 5. *Let $E_{\mathfrak{p}}(\omega, S)$ holds. Then the period of each $\alpha \in \mathfrak{O}$ is bounded.*

References

[1] E. Artin and G. Whaples, *Axiomatic characterization of fields by the product formula for valuations*, Bull. Amer. Math. Soc. 164 (1931), 1–11.

[2] H. Hasse, *Zahlentheorie*, Berlin 1963.

[3] S. Iyanaga (ed.), *Theory of numbers*, North-Holland, 1975.

[4] S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, MA, 1970.

22-4 M kigahara, Asahi-ku
Yokohama, 241 Japan

Received on 17. 6. 1986 (1651)

ACTA ARITHMETICA
LI (1988)

Über ganzzahlige Vertauschbarkeitsketten ungeraden Grades *

von

WINFRIED B. MÜLLER und RUPERT NÖBAUER (Klagenfurt)

1. Einleitung. Motiviert durch Anwendungen in der Kryptologie haben sich in den letzten Jahren mehrere Arbeiten mit der Kette der Potenzen $x, x^2, x^3, \ldots$ sowie mit den beiden Ketten der Dicksonpolynome $g_1(d, x)$, $g_2(d, x)$, $g_3(d, x), \ldots, d = \pm 1$, über den ganzen Zahlen $\boldsymbol{Z}$ (vgl. [2]) und mit den davon induzierten Permutationen auf Restklassenringen $\boldsymbol{Z}/(m)$ beschäftigt. Insbesondere wird in [5], [6] und [7] die Fixpunktanzahl der von den Polynomen dieser Ketten dargestellten Permutationen von $\boldsymbol{Z}/(m)$ berechnet, und in [8], [1] und [4] die Gruppenstruktur der von diesen Ketten induzierten Permutationsgruppen von $\boldsymbol{Z}/(m)$ ermittelt.

In [2] (vgl. Chapter 3, Prop. 3.51) wurde bewiesen, daß für ein lineares Polynom $l = ax+b$ mit reellen Koeffizienten a und b die konjugierte Kette $\{l^{-1} \circ x^k \circ l \mid k \in \boldsymbol{N}\}$ bzw. $\{l^{-1} \circ g_k(d, x) \circ l \mid k \in \boldsymbol{N}\}$, $d = +1$, nur dann ganzzahlig ist, wenn $l = ax+b$ ganzzahlig ist. Daher lassen sich Eigenschaften der von den ganzzahligen konjugierten Ketten induzierten Permutationen von $\boldsymbol{Z}/(m)$ (z.B. Fixpunktanzahl, Zyklenlänge und Struktur der gebildeten Gruppen) unmittelbar aus den entsprechenden Eigenschaften der von den ursprünglichen Ketten induzierten Permutationen von $\boldsymbol{Z}/(m)$ herleiten.

Lidl und Müller haben in [3] die ungerade Kette der Potenzen $x, x^3, x^5, \ldots$ und die ungerade Kette der Dicksonpolynome $g_1(d, x)$, $g_3(d, x)$, $g_5(d, x), \ldots, d = \pm 1$, betrachtet. In der vorliegenden Arbeit wird gezeigt, daß konjugierte Ketten dieser Ketten auch dann ganzzahlig sein können, wenn das transformierende Polynom $l = ax+b$ nicht ganzzahlig ist.

Es werden alle konjugierten Ketten der ungeraden Kette der Potenzen sowie der Dicksonpolynome mit $d = +1$ bestimmt, welche ganzzahlig sind. Weiters werden Kriterien dafür angegeben, wann die Elemente der ganzzahligen konjugierten Ketten Permutationen von $\boldsymbol{Z}/(m)$ induzieren, und im Fall der Potenzen auch die Anzahl der Fixpunkte dieser Permutationen sowie

* Die vorliegende Arbeit wurde vom Österreichischen Fonds zur Förderung der wissenschaftlichen Forschung unter dem FWF-Projekt Nr. 5452 wesentlich unterstützt.