ON ORBITS IN AMBIGUOUS IDEALS

Juraj Kostra (Ostrava, Czech Republic)

Dedicated to the memory of Professor Péter Kiss

Abstract. Let $K$ be a tamely ramified algebraic number field. The paper deals with polynomial cycles for a polynomial $f \in \mathbb{Z}[x]$ in ambiguous ideals of $Z_K$. A connection between the existence of “normal” and “power” basis and the existence of polynomial orbits is given.

AMS Classification Number: 11R18, 11C08, 12F05

1. Introduction

Let $R$ be a ring. A finite subset $\{x_0, x_1, \ldots, x_{n-1}\}$ of the ring $R$ is called a cycle, $n$-cycle or polynomial cycle for polynomial, $f \in R[x]$, if for $i = 0, 1, \ldots, n-2$ one has $f(x_i) = x_{i+1}$, $f(x_{n-1}) = x_0$ and $x_i \neq x_j$ for $i \neq j$. The number $n$ is called the length of the cycle and the $x_i$'s are called cyclic elements of order $n$ or fixpoints of $f$ of order $n$.

We can introduce a similar definition for a polynomial cycle in the situation that $S, R$ are rings and $R$ is an $S$-module.

A finite subset $\{x_0, x_1, \ldots, x_{n-1}\}$ of an $S$-module $R$ is called a cycle, $n$-cycle or polynomial cycle for polynomial $f \in S[x]$, if for $i = 0, 1, \ldots, n-2$ one has $f(x_i) = x_{i+1}$, $f(x_{n-1}) = x_0$ and $x_i \neq x_j$ for $i \neq j$.

A finite sequence $\{y_0, y_1, \ldots, y_n, y_{n+1}, \ldots, y_{m+n-1}\}$ is called an orbit of $f \in S[x]$ with the precycle $\{y_0, y_1, \ldots, y_{n-1}\}$ of length $m$ and the cycle $\{y_m, y_{m+1}, \ldots, y_{m+n-1}\}$ of length $n$ if $f(y_i) = y_{i+1}$, $f(y_{m+n-1}) = y_m$ for distinct elements $y_0, y_1, \ldots, y_{m+n-1}$ of $R$.

Let $K$ be a Galois algebraic number field and let $K/Q$ be a finite extension of rational numbers with a Galois group $G$. We will be interested in polynomial cycles generated by conjugated elements for polynomials from $Z[x]$ in the ring of integers $Z_K$ of the field $K$ and in ambiguous ideals of $Z_K$.

First we recall some general properties of ambiguous ideals according to Ulom [8]. Let $K/F$ be a Galois extension of an algebraic number field $F$ with the Galois group $G$ and $Z_K$ (resp. $Z_F$) be the ring of integers of $K$ (resp. $F$).

This research was supported by GA ČR Grant 201/01/0471.
Definition 1. An ideal $U$ of $Z_K$ is $G$-ambiguous or simply ambiguous if $U$ is invariant under action of the Galois group $G$.

Let $\mathfrak{Z}$ be a prime ideal of $F$ whose decomposition into prime ideals in $K$ is

$$\mathfrak{Z}Z_K = (\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_f)^e.$$

Let $\Psi(\mathfrak{Z}) = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_f$. It is known that

(i) $\Psi(\mathfrak{Z})$ is ambiguous and the set of all $\Psi(\mathfrak{Z})$ with $\mathfrak{Z}$ prime in $F$ is a free basis for the group of ambiguous ideals of $K$. 

(ii) An ambiguous ideal $U$ of $Z_K$ may be written in the form $U_0, T$ where $T$ is an ideal of $Z_F$ and

$$U_0 = \Psi(\mathfrak{Z}_1)^{a_1} \cdots \Psi(\mathfrak{Z}_r)^{a_r}$$

where $0 < a_i \leq e_i$ and $e_i > 1$ is the ramification index of a prime ideal of $Z_K$ dividing $\mathfrak{Z}_i$. The ideal $U$ determines $U_0$ and $T$ uniquely. The ambiguous ideal $U_0$ is called a primitive ambiguous ideal.

In our investigation we will focus a special attention to cyclic extensions $K/Q$ of prime degree $l$. In this case ambiguous ideals with normal basis were characterized in papers [3], [4] and [8].

2. Results

Let $K/Q$ be a finite normal extension of rational numbers with a Galois group $G$.

Theorem 1. Let $f \in Z[x]$ and $Y = \{y_0, y_1, \ldots\}$ be a sequence of elements of $Z_K$. Let $i < j$ such that $y_i$ and $y_j$ are conjugated over $Z$. Then $Y$ is an orbit with the precycle of length $m \leq i$.

Proof of Theorem 1. We denote by $f_k$ the $k$-iteration of polynomial $f$. Then

$$f_{j-i}(y_i) = y_j.$$

The elements $y_i$ and $y_j$ are conjugated over $Z$ and there is such an automorphism $\phi \in G$ that $\phi(y_i) = y_j$. Coefficients of $f$ are from $Z$ and it immediately follows that

$$\phi^s(y_i) = \phi^{s-1}(f(y_i)) = f(\phi^{s-1}(y_i)).$$

By induction it follows that

$$\phi^s(y_i) = y_{i+s(j-i)}.$$

The automorphism $\phi$ is of a finite order and so there is such an $s_0$ that $\phi^{s_0}(y_i) = y_i$. 
Corollary 1. Let $K/Q$ be a cyclic extension of a prime degree $l$. Let $x_0, x_1, \ldots, x_{l-1}$ be a polynomial cycle of the length $l$ for $f \in Z[x]$ in $Z_K$. Then either all $x_i$ are conjugated or $x_i$ are pairwise not conjugated.

Corollary 2. Let $K/Q$ be a cyclic extension of a prime degree $l$. Let $x_0, x_1, \ldots, x_{n-1}$ be a polynomial cycle of the length $l$ for $f \in Z[x]$ in $Z_K$. Then either $l$ divides $n$ or $x_i$ are pairwise not conjugated.

Now we will consider polynomial cycles of conjugated cyclic elements for polynomials $f \in Z[x]$ in ambiguous ideals of $Z_K$, where $K/Q$ is a tamely ramified extension with Galois group $G$.

The following theorem gives a connection between the existence of a power basis for ambiguous ideals and the existence of a polynomial cycle consisting of elements of normal basis.

Theorem 2. Let $K/Q$ be a tamely ramified cyclic algebraic number field of prime degree $l$ over $Q$. Let $\mathfrak{a}$ be an ambiguous ideal of $Z_K$ with a normal basis $\{a_0, a_1, \ldots, a_{l-1}\}$ over $Z$. There exists a polynomial $f \in Z[x]$ of degree $k \leq l$ with the polynomial cycle $\{a_0, a_1, \ldots, a_{l-1}\}$ if and only if there are $0 \leq i \neq j < l$ that

$$a_i = a_0^{i_j} + a_{l-1}^{i_j} + \cdots + a_0,$$

where $a_i \in \mathfrak{a}$.

Proof of Theorem 2. Let $\{a_0, a_1, \ldots, a_{l-1}\}$ be a polynomial cycle for $f \in Z[x]$ of degree $k \leq l$

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0.$$

Then for example

$$a_1 = f(a_0) = a_k a_0^k + a_{k-1} a_0^{k-1} + \cdots + a_0.$$

Let there are $0 \leq i \neq j < l$ such that

$$a_i = a_0^{i_j} + a_{l-1}^{i_j} + \cdots + a_0.$$

Then by Theorem 1 there is a polynomial cycle for $g(x) = a_i x^i + a_{l-1} x^{i-1} + \cdots + a_0$ which started with conjugated elements $a_j, a_i$. It is obvious that all elements of this cycle are conjugated and by Corollary 2 it follows that the polynomial cycle consists of elements $a_0, a_1, \ldots, a_{l-1}$. Because all the elements are conjugated and they have the same minimal polynomial over $Z$ of degree $l$, there exists a polynomial $f \in Z[x]$ of degree $k \leq l$ with the polynomial cycle consisting of elements $a_0, a_1, \ldots, a_{l-1}$.

Remark. In the above Theorem 2 let $f \in Z[x]$ be a polynomial with the normal basis

$$\{a_0, a_1, \ldots, a_{l-1}\}$$
as a polynomial cycle. Let
\[ f_0(x) = x^l + c_{l-1}x^{l-1} + \cdots + c_0 \]
be a minimal polynomial for \( \alpha_i \). Then for any \( i \in \{0, 1, \ldots, l-1\} \) the set
\[ \{c_0, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{l-1}\} \]
is a “power” basis of \( \mathfrak{D} \). For example let \( Q(\zeta_l) \) be the \( 7 \)-th cyclotomic field. The ideal \( \wp_7 \) lying over 7 in maximal real subfield \( K \) of \( Q(\zeta_l) \) has a normal basis
\[ \alpha_0 = 2 - \zeta_7 - \zeta_7^5, \alpha_1 = 2 - \zeta_7^2 - \zeta_7^5, \alpha_2 = 2 - \zeta_7^3 - \zeta_7^5. \]
The polynomial \( f(x) = x^2 + 4x \) has the polynomial cycle \( \alpha_0, \alpha_1, \alpha_2 \). The minimal polynomial of \( \alpha_i \) is
\[ f_0(x) = x^3 - 7x^2 - 2x - 7 = (x - \alpha_0)(x - \alpha_1)(x - \alpha_2). \]
For example a “power” basis for \( \wp_7 \) over \( Z \) is \( \{7, 2 - \zeta_7 - \zeta_7^5, (2 - \zeta_7 - \zeta_7^5)^2\} \).

Some of previous properties hold more generally.

**Theorem 3.** Let \( K/Q \) be a tamely ramified cyclic algebraic number field of prime degree \( l \) with the conductor \( m = p_1p_2\cdots p_s \). Let \( \mathfrak{D} = \wp_1^{t_1}\wp_2^{t_2}\cdots\wp_s^{t_s} \) with \( 0 \leq t_j < l \) for \( j = 1, 2, \ldots, s \) be an ideal of \( Z_K \) lying over conductor of \( K \) and let \( \{x_0, x_1, \ldots, x_{n-1}\} \) be a polynomial cycle in \( \mathfrak{D} \) for
\[ f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \quad a_i \in Z, \]
such that \( \mathfrak{D} \) is a minimal product of ideals \( \wp_j \) which contains \( x_1 \). Then \( \mathfrak{D} \) is a minimal product of ideals \( \wp_j \) which contains \( x_i \) for \( i = 0, 1, \ldots, n-1 \) and \( m \) divides \( a_0 \).

**Proof of Theorem 3.** Let \( f \in Z[x] \) and \( \{x_0, x_1, \ldots, x_{n-1}\} \) be a polynomial cycle for \( f \) in an ideal \( \mathfrak{D} \subset Z_K \). Then for all \( i \in \{0, 1, \ldots, n-1\} \) we have \( f(x_i) = x_{i+1} \) where indices are taken \( \text{mod} \ n \). Both \( x_i, x_{i+1} \in \mathfrak{D} \) and so from
\[ x_{i+1} = f(x_i) = a_nx_i^n + a_{n-1}x_i^{n-1} + \cdots + a_1x_i + a_0 \in \mathfrak{D}, \]
it follows that
\[ a_0 = x_{i+1} - (a_nx_i^n + a_{n-1}x_i^{n-1} + \cdots + a_1x_i) \in \mathfrak{D}. \]
Let \( v_j \) be a valuation corresponding to the ideal \( \wp_j \) for \( j = 1, 2, \ldots, s \). We have \( v_j(x_1) = t_j \) and \( v_j(x_i) \geq t_j \). Hence
\[ v_j(a_0) \geq \min\{v_j(x_2), v_j(a_nx_1^n), v_j(a_{n-1}x_1^{n-1}), \ldots, v_j(a_1x_1)\} \]
and so $m$ divides $a_0$. From this it follows that

$$v_j(a_0) \geq l > t_j.$$

Let $v_j(x_i) > t_j$, then

$$v_j(x_{i+1}) \geq \min\{v_j(a_0), v_j(a_n x_i^n), v_j(a_{n-1} x_i^{n-1}), \ldots, v_j(a_1 x_i)\} > t_j.$$

But it is impossible, since $f(x_{n-1}) = x_1$. Theorem 3 is proved.

References


Juraj Kostra
Department of Mathematics of the Faculty of Sciences
University of Ostrava
30.dubna 22
701 03 Ostrava, Czech Republic