A note on polynomial cycles

Michal Vavroš

Abstract. The paper deals with correspondence between polynomial cycles for a polynomial $f \in Z[x]$ in the ring of integers of p-th cyclotomic field and polynomial cycles for f in the ring $\mathbb{C}_p$ of integral circulant matrices of degree p, p is prime number. As a corollary it follows that integral polynomials over $Q(\zeta_{p^k})$ have polynomial cycles in ring $\mathbb{C}_p$ of only of lengths $n = p_1 p_2 \dots p_s$, where $p_i \leqq p$.

The paper deals with correspondence between polynomial cycles for a polynomial $f \in Z[x]$ in the ring of integers of p-th cyclotomic field $Q(\zeta_p)$ and polynomial cycles for f in the ring $\mathbb{C}_p$ of integral circulant matrices of degree p, p is prime number.

First we recall some notions.

Notation

ζ_n is a n-th primitive root of unity (for example $\zeta_n = e^{2\pi i/n}$)
$Z[\zeta_n]$ - ring of integers of the n-th cyclotomic field $Q(\zeta_n)$
$\mathbb{C}_n$ - the ring of circulant matrices over Z of degree n
A^* is the conjugate transpose of matrix A

Definition 1 Let R be a ring. A finite subset $\{x_0, x_1, \dots, x_{n-1}\}$ of the ring R is called a cycle, n-cycle or polynomial cycle for polynomial f,$f \in R[x]$, if for $i = 0, 1, \dots, n-2$ 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 polynomial cycle in the situation that S, R are rings and R is an S-module:

Received: January 10, 20022.
1991 *Mathematics Subject Classification:* Primary 11R18 , 11C08, 11C20.
Key words and phrases: Circulant matrix,polynomial cycle, cyclotomic field.
This research was supported by GA of the Czech Academy of Sciences Grant A1187101/01.

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

In the above cases, polynomial cycles were investigated over a field. The results hold for any polynomial $f \in R[x]$. In this situation it is not interesting to investigate possible lengths of polynomial cycles for all polynomials over R. The answer is trivial. Any length is available.

It follows for example by the fact that for any m there is the Lagrange interpolation polynomial

$$f(x) = \sum_{i=0}^{m-1} x_{i+1} \frac{\prod_{j=0 j\neq i}^{m-1}(x - x_j)}{\prod_{j=0 j\neq i}^{m-1}(x_i - x_j)}$$

with polynomial cycle $\{x_0, x_1, \dots, x_{m-1}\}$ of length m in the field R (we put $x_m = x_0$ in polynomial f).

The situation is rather different if R is not a field.

In the case $R = Z$, Narkiewicz [7] proved that a polynomial with rational integral coefficients can have in Z only cycles of length 1 or 2.

In the case $R = Z_K$ is a ring of integers of quadratic number field K, Boduch [1] and G.Baron (letter to Narkiewicz) determined independently possible lengths of polynomial cycles (see e.g. Narkiewicz [7]).

For fields K of greater degree the problem of determining of all cycle-lengths in their rings of integers Z_K is still open (Problem XXI of [7]).

In the above results it is very important that R is domain. We will be interested in lengths of polynomial cycles in rings of circulant matrices which are not domains, but in our investigation it will be important that rings of integers of corresponding cyclotomic fields are domains.

Definition 3 By circulant matrix of order n it is meant a square matrix of the form

$$C = circ_n(c_0, c_1, \dots, c_{n-1}) = \begin{pmatrix} c_0 & c_1 & \dots & c_{n-1} \\ c_{n-1} & c_0 & \dots & c_{n-2} \\ \dots & \dots & \dots & \dots \\ c_1 & c_2 & \dots & c_0 \end{pmatrix}.$$

The elements of each row of C are identical to those of previous row, but are moved one position to the right and wraped around. We can also write a circulant matrix in the form

$$C = (c_{jk}) = (c_{k-j+1})$$

subscripts mod n. If all $c_i \in Z$ then C is called integral rational circulant matrix.

Remark 1 All integral rational circulant matrices of rank n form a ring which we denote by $\mathbb{C}_n$. This ring is also a Z-module and so it is posible for us to investigate polynomial cycles for polynomial $f \in Z[x]$ in rings of integral rational circulant matrices $\mathbb{C}_n$.

In the next we will interesting only in the cases when order of circulant matrices $n = p$ is prime number. Let $C = circ_p(c_0, c_1, \ldots, c_{p-1})$ be a circulant over Z. Associate with the p-tuple $\gamma = (c_0, c_1, \ldots, c_{p-1})$ the polynomial $p_\gamma(\lambda) = c_0 + c_1\lambda + \cdots + c_{p-1}\lambda^{p-1}$. The polynomial $p_\gamma(\lambda)$ be called the representer of the circulant matrix C. The determinant of the matrix C is given by the formula

$$det\ C = p(1) \cdot p(\zeta_p) \cdots p(\zeta_p^{p-1}) = \prod_{j=1}^{p} p(\zeta_p^{j-1}).$$

By the above formula the correspondence between circulant matrices from the ring $\mathbb{C}_p$ and elements of p-th cyclotomic field $\mathbb{Q}(\zeta_p)$ is established.

The correspondence between the ring $\mathbb{C}_p$ of integral circulant rational matrices and the ring of integers of cyclotomic field $Z[\zeta_p]$ is given by the following relation

$$circ_p(c_0, c_1, \ldots, c_{p-1}) \longleftrightarrow \alpha = c_0 + c_1\zeta_p + \cdots + c_p\zeta_p^{p-1},\ \alpha \in Z[\zeta_p].$$

The set $\{1, \zeta_p, \ldots, \zeta_p^{p-1}\}$ is a set of generators but it is not a basis of the field $Q(\zeta_p)$ over Q. So an element $\alpha \in Z[\zeta_p]$ corresponds to the whole class of circulant matrices from $\mathbb{C}_p$.

The following theorems 1 and 2 describe the connection between possible lengths of polynomial cycles of a polynomial $f \in Z[x]$ in $\mathbb{C}_p$ and $Z[\zeta_p]$.

Theorem 1 *Let $f \in Z[x]$ have a cycle of length n in the ring of integral rational circulant matrices $\mathbb{C}_p$ over Z, where p is prime. Then*

1. If $2 \nmid n$ or $4|n$, then f has a cycle of length n in $Z[\zeta_p]$.

2. If $2|n$ and $4 \nmid n$, then f has a cycle of length n or $\frac{n}{2}$ in $Z[\zeta_p]$.

Theorem 2 *Let $f \in Z[x]$ have a cycle $\{x_0 = \varepsilon, x_1, \ldots, x_{n-1}\}$ of a length n in $Z[\zeta_p]$.*

1. Let n be even. Then f has a cycle of length n in the ring $\mathbb{C}_p$, which contains some of representations of ε in $\mathbb{C}_p$ if and only if there exists cycle $\{k_0, k_1\} \in Z$ for f, where $k_0 \equiv \varepsilon \mod (1 - \zeta_p)$.

2. Let n be odd. Then f has a cycle of length n in the ring $\mathbb{C}_p$, which contains some of representations of ε in $\mathbb{C}_p$ if and only if there exists fixpoint $k_0 \in Z$ of f, where $k_0 \equiv \varepsilon \mod (1 - \zeta_p)$.

3. If n is odd. Then f has a cycle of length 2n in the ring $\mathbb{C}_p$, which contains some of representations of ε in $\mathbb{C}_p$ if and only if there exists cycle $\{k_0, k_1\} \in Z$ for f, where $k_0 \equiv k_1 \equiv \varepsilon \mod (1 - \zeta_p)$.

For proofs of Theorems 1 and 2 we recall the way of diagonalization for circulant matrices Davis [2].

The Fourier matrix F_n of degree n is the matrix conjugate transpose to the matrix

$$F_n^* = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \zeta_n & \zeta_n^2 & \ldots & \zeta_n^{n-1} \\ 1 & \zeta_n^2 & \zeta_n^4 & \ldots & \zeta_n^{2(n-1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \zeta_n^{n-1} & \zeta_n^{2(n-1)} & \ldots & \zeta_n^{(n-1)(n-1)} \end{pmatrix}.$$

It holds $F_n^* = F_n^{-1}$.

A procedure of diagonalization for circulant matrices is given by the following Lemma 1, Davis [2].

Lemma 1 *If C is circulant of order p, it is diagonalized by F_p. More precisely*

$$C = F_p^* \Lambda F_p$$

where

$$\Lambda = \Lambda_C = diag(p_\gamma(1), p_\gamma(\zeta_p), \dots, p_\gamma(\zeta_p^{p-1})).$$

In this case the product $F_p \cdot C \cdot F_p^* = diag(p(1), p(\zeta_p), \dots, p(\zeta_p^{p-1})) = D_C$ is a diagonal matrix whose diagonal elements are the eigenvalues of the matrix C.

The Fourier matrix F_p transforms any circulant matrix C of the order p to diagonal matrix D_C.

Diagonal matrix D_C has a form

$$D_C = \begin{pmatrix} k & 0 & 0 & \dots & 0 \\ 0 & \varepsilon_1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \varepsilon_{p-1} \end{pmatrix},$$

where $k = p(1) = \sum_{i=0}^{p-1} c_i,\ k \in Z$; elements $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{p-1}$ are conjugate elements from cyclotomic field $Q(\zeta_p)$ over Q.

So we can substitute the problem with polynomial cycles in the ring of circulants for the problem with polynomial cycles in the set of special diagonal matrices, then

$$F_p \cdot g(C) \cdot F_p^* = \sum_{i=0}^{n} a_i F_p C^i F_p^* = g(F_p \cdot C \cdot F_p^*) = g(D_C),\ g \in Z[x].$$

So, the set C_p forms the set Δ_p of diagonal matrices of the form D_C. Δ_p is a ring which is isomorphic to a subring of the direct sum $Z \oplus Z[\zeta_p]$. The sets of cycles lengths in C_p and Δ_p coincide. Hence, we shall consider only cycles in ring Δ_p.

For the next we will need the following Lemma 2 (G.Baron[7, Theorem 12.9])

Lemma 2 *Polynomial $f \in Z[x]$ over Z has this possibility for lengths of cycles*

i) f has no cycle;

ii) f has 1 cycle of length 1 and $k \geq 0$ cycles of length 2;

iii) f has $k \geq 1$ cycles of the same length (1 or 2).

Proof of Theorem 1 Let $f \in Z[x]$ and let the set $\{C_0, C_1, \dots, C_{n-1}\}$ be polynomial cycle for f in $\mathbb{C}_p$. By the above the set $\{D_{C_0}, D_{C_1}, \dots, D_{C_{n-1}}\}$ is corresponding polynomial cycle for f in diagonal matrices. By the form of diagonal matrices

$$D_{C_i} = \begin{pmatrix} k_i & 0 & 0 & \dots & 0 \\ 0 & \varepsilon_{1,i} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \varepsilon_{p-1,i} \end{pmatrix},$$

it follows that the length of polynomial cycle $\{D_{C_0}, D_{C_1}, \dots, D_{C_{n-1}}\}$ and so also for $\{C_0, C_1, \dots, C_{n-1}\}$ is the least common multiple of the lengths of polynomial cycles of diagonal elements

$$k_i, \varepsilon_{1,i}, \varepsilon_{2,i}, \dots, \varepsilon_{p-1,i}.$$

By the Lemma 2 the numbers $k_i \in Z$ generate the cycle of length r, r is 1 or 2. All of the another diagonal elements generate cycle of the same length s for $f \in Z$ because the elements $\varepsilon_{1,i}, \varepsilon_{2,i}, \dots, \varepsilon_{p-1,i}$ are conjugated. Then n equals the least common multiple of r and s. Since there are only cycles of lengths 1 and 2 in Z, hence

$$n = \begin{cases} s & \text{for } r = 1 \text{ or } r = 2, 2|s \\ 2s & \text{for } r = 2, 2 \not| s. \end{cases}$$

Now the assertion of Theorem 1 follows immediately.

Proof of Theorem 2 Let $f \in Z[x]$ have a cycle $\{x_0 = \varepsilon, x_1, \dots, x_{n-1}\}$ of a length n in $Z[\zeta_p]$. Let one of representations ε in the $\mathbb{C}_p$ be a circulant matrix

$$circ_p(c_0, c_1, \dots, c_{p-1}),$$

where

$$\sum_{i=0}^{p-1} c_i = k.$$

By the correspondence between $Z[\zeta_p]$ and $\mathbb{C}_p$ which was described above a circulant matrix is a representation of ε in $\mathbb{C}_p$ if and only if it has a form

$$C_t = circ_p(c_0 + t, c_1 + t, \dots, c_{p-1} + t),$$

where $t \in Z$. Such a circulant matrix is an element of polynomial cycle of length n for polynomial f if and only if the diagonal matrix is in the form

$$D_{C_t} = \begin{pmatrix} k + pt & 0 & 0 & \dots & 0 \\ 0 & \varepsilon_1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \varepsilon_{p-1} \end{pmatrix},$$

where $\varepsilon_1, \varepsilon_2 \dots \varepsilon_{p-1}$ are all conjugations of ε. So C_t is a element of polynomial cycle of length n for polynomial f if and only if $k_0 = k + pt$ is a cyclic element of f of order m which divides n. By Lemma 2 we have only two possibilities for m, m is equal to 1 or 2. It is equivalent to the existence of cycle $\{k_0, k_1\} \in Z$ for f, where $k_0 \equiv \varepsilon \mod (1 - \zeta_p)$. If n is odd , then $k_0 = k_1$.

If n is odd and $k_0 \neq k_1$ then length of polynomial cycle in $\mathbb{C}_p$ is $2n$ (the least common multiply of lengths of cycles for k_0 and ε) and the n-th iteration $f_n(C_t) \neq C_t$. But both C_t and $f_n(C_t)$ are representations of the same element ε in $\mathbb{C}_p$. We have

$$D_{C_t} = \begin{pmatrix} k_0 & 0 & 0 & \dots & 0 \\ 0 & \varepsilon_1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \varepsilon_{p-1} \end{pmatrix}$$

and

$$D_{f_n(C_t)} = \begin{pmatrix} k_1 & 0 & 0 & \dots & 0 \\ 0 & \varepsilon_1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \varepsilon_{p-1} \end{pmatrix}.$$

So $k_0 \equiv k_1 \equiv \varepsilon \pmod{1-\zeta_p}$ and also $k_0 \equiv k_1 \pmod{p}$.

As a corollary we obtain the following theorem.

Theorem 3 *Let p be a prime and let n be a length of polynomial cycle of f in $\mathbb{C}_p$. Then*

$$n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s},$$

where $p_1, p_2, \dots p_s$ are primes with the property $p_i \leq p$ for all $1 \leq i \leq s$.

Proof The Lenstra constant L of ring $Z[\zeta_p]$ does not exceed p, the principal ideal $I = (1 - \zeta_p)$ in the ring $Z[\zeta_p]$ is of norm p, $L(Z[\zeta_p]) \leq p$. Now it remains to apply the Corollary 2 [7, p. 104].

Remark 2 Let a polynomial $f \in Z[x]$ have a polynomial cycle of length n in $Q(\zeta_p)$

$$\{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}\}.$$

By the above theorems for such a polynomial f there exists a polynomial cycle in the ring of circulant matrices $\mathbb{C}_p$ if and only if polynomial f has a fixpoint

$$k_0 \in Z$$

or polynomial cycle of length 2

$$k_0, k_1 \in Z.$$

In the other cases, polynomial f does not have a polynomial cycle in the ring of circulant matrices $\mathbb{C}_p$.

So, in the special case for monic quadratic polynomial, there is the following situation. We have a monic polynomial f in the form

$$f(x) = x^2 + bx + c, \quad b, c \in Z.$$

Let $k_0 \in Z$ it holds

$$f(k_0) = k_0,$$

then k_0 is a root of equation $x^2 + (b-1)x + c = 0$ and so

$$c \leq \frac{(b-1)^2}{4}, \quad k_0 = \frac{1 - b \pm \sqrt{D}}{2} \in Z.$$

The equation $x^2 + bx + c$ has exactly one fixpoint k_0 in Z if and only if

$$b = 2k_0 + 1, \; c = k_0^2, \; k_0 \in Z.$$

The equation $x^2 + bx + c$ has two fixpoints $k_0, k_0 - d$ if and only if

$$b = 1 - 2k_0 + d, \ c = k_0^2 - k_0 d, \ \ k_0 \in Z,$$

or $k_0, k_0 + d$ if and only if

$$b = 1 - 2k_0 - d, \ c = k_0^2 + k_0 d, \ \ k_0 \in Z.$$

Let $f(x) = x^2 + bx + c, \ f \in Z[x]$ and

$$c > \frac{(b-1)^2}{4},$$

then by above and by the inequality $f(x) > x$ for all $x \in Z$ there is no cycle for f in Z and so there is no polynomial cycle for f in $\mathbb{C}_n$ for all positive $n \in Z$.

References

[1] Boduch, J *Polynomial cycles in rings of algebraic integer,* (Polish) MA thesis Wroclaw University, 1990.

[2] Davis,P.J. *Circulant Matrices.* Wiley-Interscience publishers, John Wiley and sons, New York-Chichester-Brisbane-Toronto, 1979.

[3] Divišová, Z *On cycles of polynomials with integral rational coefficients,* Mathematica Slovaca, (to appear 2002).

[4] Halter-Koch,F and Konečná, P *Polynomial cycles in finite extension fields,* Mathematica Slovaca, (to appear 2002).

[5] Kostra, J. *A note on representation of cyclotomic fields,* Acta Mathematica et Informatica Universitatis Ostraviensis 4, 29–35, 1996.

[6] Kostra, J. *On orbits in ambiguons ideals,* Acta Acad. Paed. Agriensis, Section Mathematical, (to appear 2002).

[7] Narkiewicz, W. *Polynomial Mappings.* Lecture Notes in Mathematics, 1600, Springer-Verlag, Berlin, Heidelberg, 1995.

[8] Pomp, M., Havelek, R., *On representation of cyclotomic fields* $\mathbb{Q}(\zeta_{pq})$, Acta Mathematica et Informatica Universitatis Ostraviensis, 7, 71–78, 1999.

Michal Vavroš, University of Ostrava, Department of Mathematics of the Faculty of Sciences, 30.Dubna 22, 701 03 Ostrava, Czech Republic
E-mail address: michal.vavros@osu.cz