Petra Konečná

Polynomial orbits in finite commutative rings

Czechoslovak Mathematical Journal, Vol. 56 (2006), No. 2, 711–719

Persistent URL: `http://dml.cz/dmlcz/128099`

Czechoslovak Mathematical Journal, 56 (131) (2006), 711–719

POLYNOMIAL ORBITS IN FINITE COMMUTATIVE RINGS

Petra Konečná, Ostrava

(Received January 9, 2004)

Abstract. Let R be a finite commutative ring with unity. We determine the set of all possible cycle lengths in the ring of polynomials with rational integral coefficients.

Keywords: polynomial cycles, finite rings

MSC 2000: 11C08, 13M05, 13M10

1. Introduction

Let R be a commutative ring with unity, $k \in \mathbb{N}_0$, $l \in \mathbb{N}$ and let f be a polynomial over the ring R. By a *finite orbit of f in R with precycle length k and cycle length l* we mean a sequence $(x_1, x_2, \ldots, x_{k+l})$ of distinct elements of R such that

$$f(x_i) = x_{i+1} \quad \text{for all } i \in \{1, 2, \ldots, k+l-1\}, \quad \text{and} \quad f(x_{k+l}) = x_{k+1}.$$

The elements $x_{k+1}, \ldots, x_{k+l}$ are called *fixpoints of f of order l*. Let $j \in \mathbb{N}_0$. By the *j-iterate of f in R* we mean the polynomial $f_0(x) = x$ if $j = 0$ or the polynomial $f_j(x) = f(f_{j-1}(x))$ if $j > 0$.

The following lemma shows useful properties of cycles and iterations.

Lemma 1 ([6]). *Let R be a ring. If $a \in R$, $f_n(a) = a$ and j is the smallest integer satisfying $f_j(a) = a$, then j divides n. Cyclic elements of order n of f coincide with those fixpoints of f_n which are not fixpoints of f_d, where d runs over all proper divisors of n.*

In the study of polynomial orbits we are especially interested in their lengths, more precisely in their cycle lengths. In this paper we shall determine the set of all

The research of the author was supported by the grant No. A1187101/01 of the Grant Agency of the Academy of Sciences of the Czech Republic.

possible cycle lengths in finite commutative rings with unity. First, we make this determination for some special rings, specifically for the ring of circulant matrices over a finite field and for semisimple rings. In the last part we will solve this problem for the general case of an arbitrary finite commutative ring with unity. The set of all possible cycle lengths in a finite commutative ring with unity R of polynomials with rational integral coefficients is denoted by the symbol $\operatorname{Cycl}(R/\mathbb{Z})$.

In our investigation we will make use of the following three propositions. The first proposition gives the set of all possible cycle lengths of polynomials over some finite field F in a finite extension K of F. This set is denoted by the symbol $\operatorname{Cycl}(K/F)$.

Proposition 1 ([4]). *Let F be a finite field, $n \in \mathbb{N}$ and N the number of irreducible monic polynomials of degree n over F. Let K/F be a field extension of degree n. Then the set of all possible cycle lengths in K of polynomials over F is given by*

$$\operatorname{Cycl}(K/F) = \{dm\colon\ 1 \leqslant d \leqslant N,\ 1 \leqslant m \mid n\}.$$

The following propositions determine the set of all possible cycle lengths in the direct sum of finite extensions of a finite field F that are induced by polynomials over F. Proposition 2 gives this determination for the special case when the direct sum is given by the k-th power of a finite field and Proposition 3 solves this problem for an arbitrary direct sum of finite fields.

Proposition 2 ([5]). *Let F be a finite field, K its algebraic extension of degree n, N the number of irreducible monic polynomials of degree n over F and $s \in \mathbb{N}$. Then the set of all possible cycle lengths of polynomials over F in the direct sum K^s with the property that elements of these cycles do not belong to any proper subfield of K is given by* $\operatorname{Cycl}(K^s/F) = \{m\cdot\operatorname{lcm}(d_1,\dots,d_t)\colon\ t \leqslant s,\ d_1,\dots,d_t$ *are different,* $d_1+\ldots+d_t \leqslant N$ *and* $m \mid n\}$.

Proposition 3 ([5]). *Let $K_1, K_2, \dots, K_r$ be finite extensions of a finite field F, $s_1, \dots, s_r$, $r \in \mathbb{N}$. Then*

$$\operatorname{Cycl}(K_1^{s_1} \oplus \ldots \oplus K_r^{s_r}/F) = \{\operatorname{lcm}(l_i)\colon\ l_i \in \operatorname{Cycl}(K_i^{s_i}/F)\ \ \text{for } i = 1,\dots,r\}.$$

2. Polynomial cycles in the ring of circulant matrices

We determine the set of all possible cycle lengths in the ring of circulant matrices over a finite field F of polynomials from $F[x]$. We have to observe that this ring is very important in the coding theory.

Definition ([1]). By a *circulant matrix* of order r is meant a square matrix of the form

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & \dots & c_{r-1} \\ c_{r-1} & c_0 & c_1 & \dots & c_{r-2} \\ c_{r-2} & c_{r-1} & c_0 & \dots & c_{r-3} \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ c_1 & c_2 & c_3 & \dots & c_0 \end{pmatrix}.$$

It is denoted by $C = \operatorname{circ}(c_0, \dots, c_{r-1})$.

The following lemma is a well known fact.

Lemma 2. *Circulant matrices of order r over a finite field F form a ring R which is isomorphic to the ring of polynomials $F[x]/(x^r - 1)$.*

Theorem 1. *Let F be a finite field of characteristic p, and R a ring of circulant matrices of order r over F, where p is a prime and r is a positive integer such that $\gcd(p, r) = 1$. Then the set of all possible cycle lengths of polynomials over F in the ring R is given by*

$$\operatorname{Cycl}(R/F) = \operatorname{Cycl}\Big(\bigoplus_{i=1}^{k} F(x_i)/F\Big),$$

where k is a positive integer such that $k \leqslant r$ and

$$\sum_{i=1}^{k} [F(x_i) : F] = r.$$

Proof. Consider a finite field F of characteristic p and a positive integer r such that $\gcd(r, p) = 1$.

By Lemma 2 we know that the ring R of circulant matrices of order r over the finite field F is isomorphic to the finite polynomial algebra

$$\mathrm{GF}(q)[x]/(x^r - 1).$$

For every $i \in \{1, \ldots, k\}$, where $k \leqslant r$, denote by $g^{(i)} \in F[x]$ the irreducible polynomial of degree δ_i over F such that

$$(x^r - 1) = \prod_{i=1}^{k} g^{(i)}.$$

Then

$$R \simeq \mathrm{GF}(q)[x]/(x^r - 1) = \mathrm{GF}(q) \Big/ \prod_{i=1}^{k} g^{(i)}.$$

Owing to the fact that r is coprime with the characteristic p of the field F, the polynomial $x^r - 1$ does not have multiple roots and thus

$$R \simeq \bigoplus_{i=1}^{k} \mathrm{GF}(q^{\delta_i}).$$

Using Proposition 2 and Proposition 3, we obtain our assertion

$$\mathrm{Cycl}(R/F) = \mathrm{Cycl}\left(\bigoplus_{i=1}^{k} F(x_i)/F\right).$$

□

Example. Consider the ring R of circulant matrices over a finite field $\mathrm{GF}(2^3)$ of degree 3. Then it is isomorphic to the ring $\mathrm{GF}(2^3)[x]/(x^3 - 1)$. The decomposition of the polynomial $x^3 - 1$ into irreducible polynomials over $\mathrm{GF}(2^3)$ is

$$(x^3 - 1) = (x - 1)(x^2 + x + 1),$$

so if we use the notation of Theorem 1, we obtain

$$k = 2, \quad g^{(1)}(x) = (x - 1), \quad \delta_1 = 1, \quad g^{(2)}(x) = (x^2 + x + 1), \quad \delta_2 = 2.$$

Then

$$\mathrm{Cycl}(R/\,\mathrm{GF}(2)) = \mathrm{Cycl}(\mathrm{GF}(2^3) \oplus \mathrm{GF}(2^6)/\,\mathrm{GF}(2))$$

and this set is given by

$$\{\mathrm{lcm}(l_1, l_2)\colon\ l_1 \in \mathrm{Cycl}(\mathrm{GF}(2^3)/\,\mathrm{GF}(2)),\ l_2 \in \mathrm{Cycl}(\mathrm{GF}(2^6)/\,\mathrm{GF}(2))\}.$$

We have

$$\mathrm{Cycl}(\mathrm{GF}(2^3)/\,\mathrm{GF}(2)) = \{1, 2, 3, 6\}$$

and

$$\operatorname{Cycl}(\mathrm{GF}(2^6)/\,\mathrm{GF}(2)) = \{1,2,3,4,5,6,7,8,9,10,12,14,15,16,18,21,\\ 24,27,30,36,42,48,54\}.$$

Clearly

$$\operatorname{Cycl}(\mathrm{GF}(2^3)/\,\mathrm{GF}(2)) \subseteq \operatorname{Cycl}(\mathrm{GF}(2^6)/\,\mathrm{GF}(2)).$$

Therefore

$$\operatorname{Cycl}(R/\,\mathrm{GF}(2)) = \operatorname{Cycl}(\mathrm{GF}(2^6)/\,\mathrm{GF}(2)).$$

3. Polynomial cycles in semisimple finite commutative rings

Definition. A finite ring R is called *semisimple* iff it has zero radical, i.e., iff

$$\operatorname{Rad}(R) = \bigcap_{I\in\max(R)} I = 0,$$

where $\max(R)$ is the set of all maximal ideals of the ring R.

Recall that two ideals I and J of a ring R are *coprime* iff $I + J = R$. Then we can formulate the Chinese remainder theorem for ideals as the following lemma.

Lemma 3. *Let R be a commutative ring with unity, $P_i \lhd R$, $i = 1,\ldots,k$, be coprime ideals of the ring R. Then $\bigcap\limits_{i=1}^{k} P_i = \prod\limits_{i=1}^{k} P_i$ and there exists an isomorphism*

$$R\Big/\prod_{i=1}^{k} P_i \to \prod_{i=1}^{k} R/P_i$$

such that for all $x \in R$

$$x + \prod_{i=1}^{k} P_i \mapsto (x + P_1, \ldots, x + P_k).$$

Theorem 2. *Let R be a finite commutative semisimple ring. Then the set of all possible cycle lengths in the ring R of polynomials with rational integral coefficients is given by*

$$\mathrm{Cycl}(R/\mathbb{Z}) = \mathrm{Cycl}\Bigl(\bigoplus_{i=1}^{k} R/P_i\Bigr),$$

where $P_1, \dots P_k$ are prime ideals of the ring R.

Proof. Let R be a finite commutative ring. Then for every $i = 1, \dots k$ the prime ideal P_i of R satisfies that R/P_i is a finite integral domain, thus it must be a finite field. So, every ideal P_i is maximal. Prime ideals $P_1, \dots, P_k$ are pairwise coprime, thus $\mathrm{Rad}(R) = \bigcap\limits_{i=1}^{k} P_i = \prod\limits_{i=1}^{k} P_i$.

The ring R is semisimple, thus $\mathrm{Rad}(R) = 0$ and by Lemma 3 it is isomorphic to the direct sum of finite fields R/P_i

$$R = R\Big/\prod_{i=1}^{n} P_i \simeq \bigoplus_{i=1}^{n} R/P_i.$$

Therefore we get

$$\mathrm{Cycl}(R/\mathbb{Z}) = \mathrm{Cycl}\Bigl(\bigoplus_{i=1}^{k} R/P_i\Bigr).$$

□

Example. Consider the ring of residue classes modulo 6 $R = \mathbb{Z}/6\mathbb{Z}$. This ring has two maximal ideals $M_1 = \{0, 2, 4\}$ and $M_2 = \{0, 3\}$, whose intersection is the zero. Therefore R is semisimple. The following holds

$$R \simeq \mathrm{GF}(2) \oplus \mathrm{GF}(3).$$

Thus

$$\mathrm{Cycl}(R/\mathbb{Z}) = \mathrm{Cycl}(\mathrm{GF}(2) \oplus \mathrm{GF}(3)/\mathbb{Z}) = \{1, 2, 3, 6\}.$$

4. Polynomial cycles in finite commutative rings

Definition. A finite commutative ring R with unity is called *local* iff it has only one maximal ideal.

Lemma 4 ([2])**.** *Let R be a finite commutative ring. Then R decomposes (up to order of summands) uniquely as a direct sum of local rings.*

Theorem 3. *Let R be a finite commutative local ring, P its prime ideal. Let p be the characteristic of the ring R/P with p^n elements. Then cycle lengths of polynomials with rational integral coefficients in the ring R can be from the set*

$$\operatorname{Cycl}(R/\mathbb{Z}) \subseteq \Big\{kl^*, \text{where } k \leqslant \frac{|R|}{p^n},\ l^* \in \operatorname{Cycl}(\operatorname{GF}(p^n)/\operatorname{GF}(p))\Big\}.$$

Proof. Let R be a local finite ring with $|R|$ elements. We know that this ring has only one maximal ideal, denote it by P. Then the factor ring R/P is a finite field with $q = |R|/|P|$ elements and so it is isomorphic to the Galois field $\operatorname{GF}(q)$ with the same number of elements $q = p^n$, where p is the characteristic of this field. Then there is an epimorphism $\psi\colon\ R \to \operatorname{GF}(q)$.

Let $(x_1, \ldots, x_l)$ be a cycle of the length l in R of a polynomial $f \in \mathbb{Z}[x]$. Then by definition

$$f_l(x_j) = x_j \quad \text{for every } \ j = 1, \ldots, l.$$

Consider the image of this cycle in the field $\operatorname{GF}(q)$, which is isomorphic to the factor ring R/P. We have

$$\psi((x_1, \ldots, x_l)) = (\psi(x_1), \ldots, \psi(x_l)).$$

Then this image is a cycle in the field $\operatorname{GF}(q)$ Let l^* be the least positive integer such that

$$f_{l^*}(\psi(x_j)) = \psi(x_j) \quad \text{for every } \ j = 1, \ldots, l.$$

Then by Lemma 1

$$l^* \mid l \ \text{ with } \ l^* \in \operatorname{Cycl}((R/P)/\mathbb{Z}) = \operatorname{Cycl}(\operatorname{GF}(q)/\operatorname{GF}(p)).$$

Therefore, with utilization of Proposition 1, for every $l \in \operatorname{Cycl}(R/\mathbb{Z})$

$$l = kl^* = kmd, \ \text{ where } \ \frac{|R|}{p^n} \geqslant k \in \mathbb{N}, \quad m \mid n, \ \ 1 \leqslant d \leqslant N.$$

□

Corollary. *Let R be a finite commutative ring. Let $P_1,\dots,P_k$ be maximal ideals of this ring and let m be a positive integer such that $\bigcap\limits_{i=1}^{k} P^m = 0$.*

Then the set of all possible cycle lengths of polynomials with rational integral coefficients is given by the set $\operatorname{Cycl}(R/\mathbb{Z})$ *which is equal to the set*

$$\operatorname{Cycl}\biggl(\Bigl(\bigoplus_{i=1}^{k} R/P_i^m\Bigr)/\mathbb{Z}\biggr) \subseteq \{\operatorname{lcm}(l_i),\ \textit{where } l_i \in \operatorname{Cycl}((R/P_i^m)/\mathbb{Z})\ \textit{ for } i=1,\dots,k\}.$$

Proof. By Lemma 4 the finite ring R is isomorphic to the direct sum of local rings $\bigoplus\limits_{i=1}^{k} R/P_i^m$ with maximal ideals P_i/P_i^m, where $P_1,\dots,P_k$ are maximal ideals of the ring R and m is a positive integer such that $\bigcap\limits_{i=1}^{k} P^m = 0$. Let l be a cycle length of a polynomial with rational integral coefficients in the ring R. This is possible if and only if there exists a cycle $(\bar{x}_1,\dots,\bar{x}_l)$ of that polynomial, where $\bar{x}_j \in \bigoplus\limits_{i=1}^{k} R/P_i^m$, that can be decomposed to basic cycles of the polynomial f

$$(x_1^{(i)},\dots,x_{l_i}^{(i)}),\ \text{ where } i=1,\dots,k,\ x_j^{(i)} \in R/P_i^m \ \text{ and } \ l_i \in \operatorname{Cycl}((R/P_i^m)/\mathbb{Z}).$$

From Lemma 1 it follows that for every $i = 1,\dots,k$ there holds $l_i \mid l$, therefore $l = \operatorname{lcm}(l_i)$. □

Example. Consider the ring $R = \mathbb{Z}/8\mathbb{Z}$ of residue classes modulo 8. The maximal ideal is $M = (2)$. Thus the factor ring $R/(2)$ is a finite field with two elements, that is

$$R \to R/(2) \simeq \mathrm{GF}(2).$$

Thence cycle lengths of polynomials with rational integral coefficients belong to the set

$$\operatorname{Cycl}(R/\mathbb{Z}) \subseteq \{1,2,3,4,6,8\}.$$

Above that it was shown in [3] that in this particular case $\operatorname{Cycl}(R/\mathbb{Z}) = \{1,2,4,8\}$.

References

[1] *P. J. Davis*: Circulant Matrices. J. Wiley and Sons, NewYork-Chichester-Brisbane-Toronto, 1979. Zbl 0418.15017

[2] *B. R. McDonald*: Finite Rings with Identity. M. Dekker, New York, 1974. Zbl 0294.16012

[3] *V. Dubovský*: Polynomial cycles. Master Thesis. Department of Mathematics, Faculty of Science, University of Ostrava, 2003. (In Czech.)

[4] *F. Halter-Koch and P. Konečná*: Polynomial cycles in finite extension fields. Mathematica Slovaca *52* (2002), 531–535. Zbl 1028.11014

[5] *P. Konečná*: Polynomial orbits in direct sum of finite extension fields. Studia Universitatis "Babes-Bolyai" Mathematica, Vol. XLVIII. June 2003, pp. 73–77.

[6] *W. Narkiewicz*: Polynomial Mappings. Lecture Notes in Mathematics Vol. 1600. Springer-Verlag, Berlin, 1995. Zbl 0829.11002

Author's address: Department of Mathematics, Faculty of Science, University of Ostrava, 30. dubna 22, CZ-701 03 Ostrava, Czech Republic, e-mail: `petra.konecna@osu.cz`.