STUDIA UNIV. "BABEŞ–BOLYAI", MATHEMATICA, Volume **XLVIII**, Number 2, June 2003

POLYNOMIAL ORBITS IN DIRECT SUM OF FINITE EXTENSION FIELDS

PETRA KONEČNÁ

Abstract. Let $K_1, \dots, K_n$ be a finite extensions of the field F. We describe the structure of finite orbits and determine its precycle and cycle lengths in the direct sum $K_1 \oplus \dots \oplus K_n$ which are induced by polynomials from F.

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

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

Elements $x_i, i = k+1, \dots, l$ are called *fixpoints of f of order l*. Let $k \in \mathbb{N}_0$. By a *k-iterate of f in R* we mean a polynomial f_k such that

$$f_0(x) = (x), f_1(x) = f(x), f_{k+1}(x) = f(f_k(x))$$

Let K/F be an algebraic field extension. Then Cycl(K/F) is the set of all possible cycle lengths in K of polynomials over F. Consider an algebraic field extension K/F. The following proposition determine the structure of finite orbits in K of polynomials $f \in F[X]$.

Proposition 1. [1] *Let K/F be an algebraic field extension, $k \in \mathbb{N}_0$, $l \in \mathbb{N}$, and let $(x_1, x_2, \dots, x_{k+l})$ be a sequence of distinct elements of K. Then the following assertions are equivalent:*

a): *$(x_1, x_2, \dots, x_{k+l})$ is a finite orbit of a unique polynomial $f \in F[X]$ with precycle length k and cycle length l such that for a certain d*

$$\deg f < \prod_{i=1}^{k+d} \deg_F(x_i).$$

b): *$(x_1, x_2, \dots, x_{k+l})$ is a finite orbit of a polynomial $f \in F[X]$ with precycle length k and cycle length l.*

c): *There holds $F(x_1) \supset F(x_2) \supset \dots \supset F(x_{k+1}) = \dots = F(x_{k+l})$, there exist $d, m \in \mathbb{N}$ and $\tau \in Aut_F\big(F(x_{k+1})\big)$ such that $l = dm$, $\mathrm{ord}(\tau) = \mathrm{m}$, the elements $x_1, \dots, x_{k+d}$ are pairwise not conjugate over F, and*

$$x_{k+\mu d+j} = \tau^{\mu}(x_{k+j}) \quad \textit{for all} \quad j \in \{1, \dots, d\} \quad \textit{and} \quad \mu \in \{1, \dots, m-1\}.$$

Received by the editors: 27.03.2003.
2000 *Mathematics Subject Classification.* 11C08, 11T06.
Key words and phrases. polynomial cycles, finite extension field.
The research was supported by GA of the Czech Academy of Sciences Grant A1187101/01.

By proposition, let K/F be an algebraic field extension of degree n and N the number of irreducible monic polynomials of degree n over F. Then the set of all possible cycle lengths in K of polynomials over F is given by

$$\mathrm{Cycl(K/F)} = \left\{\mathrm{dm} \;\middle|\; 1 \leq \mathrm{d} \leq \mathrm{N},\ 1 \leq \mathrm{m|n}\right\}.$$

In the present paper we shall describe the structure of finite polynomial orbits and determine the set of all possible cycle lengths of polynomials over F in the direct sum of finite extension fields $K_1, \ldots, K_n$ which is given by

$$\bigcup_{K_i' \subseteq K_i} \mathrm{Cycl}(\mathrm{K}_1^{'} \oplus \ldots \oplus \mathrm{K}_\mathrm{n}^{'}/\mathrm{F}),$$

over all n-tuple $(K_1^{'} \oplus \ldots \oplus K_n^{'})$ with $\mathrm{Cycl}(\mathrm{K}_1^{'} \oplus \ldots \oplus \mathrm{K}_\mathrm{n}^{'}/\mathrm{F})$ are different.

As an application of this general case we can obtain the set of all cycle lengths for special rings which are direct sum of finite extension fields, for example ring of circulant matrices over a finite field which is very important in the coding theory.

First we recall some properties of cycles and polynomials in the following lemmas.

Lemma 1. [1] *Let F be a field, let $f_1, \ldots, f_m \in F[X]$, $m \in \mathbb{N}$ be pairwise coprime polynomials, and let $g_1, \ldots, g_m \in F[X]$ be any polynomials. Then there exists a unique polynomial $f \in F[X]$ such that*

$$\mathrm{deg(f)} < \prod_{\mathrm{j=1}}^{\mathrm{m}} \mathrm{deg(f_j)} \quad \textit{and} \quad \mathrm{f \equiv g_j \mod f_j} \quad \textit{for all} \quad \mathrm{j} \in \{1, \ldots, \mathrm{m}\}.$$

Lemma 2. [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.*

Lemma 3. *All conjugated elements in the finite extension of the field F have the same cycle length of a polynomial $f \in F$.*

Proof. This follows immediately from properties of any automorphism of the algebraic closure of K. □

Theorem 1. *Let K/F be an algebraic field 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 f in the direct sum K^s is given by*
$Cycl(K^s/F) = \{m \cdot \mathrm{lcm}(\mathrm{d}_1, \ldots, \mathrm{d}_\mathrm{t}) \mid \mathrm{t} \leq \mathrm{s}, \mathrm{d}_1, \ldots, \mathrm{d}_\mathrm{t}$ are distinct, $d_1 + \cdots + d_t \leq N$ and $m|n\}$.

Proof. Let $(\bar{x}_1, \ldots, \bar{x}_l)$ be a cycle of polynomial f in K^s with length l, where $\bar{x}_i = (x_i^{(1)}, \ldots, x_i^{(s)})$ and $x_i^{(j)} \in K$.

Then $f_l(\bar{x}_i) = \bar{x}_i$ and $f_l(x_i^{(j)}) = x_i^{(j)}$ for any $i = 1, \ldots, l, j = 1, \ldots, s$.

For any $j = 1, \ldots, s$ consider the least positive integers $l_j \leq l$ with $f_{l_j}(x_i^{(j)}) = x_i^{(j)}$. By Lemma 2 we have that l_j divides l and l_j is a cycle length of f in K. Hence by Proposition, l_j can be written in the form $l_j = d_j m_j$, where $d_j = 1, \ldots, N$ and $m_j|n$, whence $l = m \cdot \mathrm{lcm}(\mathrm{d}_1, \ldots, \mathrm{d}_\mathrm{s})$, where m is a positive integer which divides n.

From the set $\{d_1,\dots,d_s\}$ choose t elements $d_1,\dots,d_t$, which are different. Assume to the contrary that $d_1+\cdots+d_t > N$. Then there are positive integers $j_1, j_2 = 1,\dots,s, i_1, i_2 = 1,\dots,l, j_1 \neq j_2, i_1 \neq i_2$ such that elements $x_{i_1}^{j_1}, x_{i_2}^{j_2}$ are conjugated. Lemma 3 implies that cycles $(x_1^{j_1},\dots,x_{l_1}^{j_1}), (x_1^{j_2},\dots,x_{l_2}^{j_2})$ must have the same cycle length of the type $d\cdot m$, it means $d_{j_1} = d_{j_2}$. Contradiction.

Let $m, d_1,\dots,d_t$ be positive integers such that $m|n, d_j \leq N,$ and $d_1+\cdots+d_t \leq N, j=1,\dots,t\leq s$. Then there is a unique t-tuple of polynomials $f^{(1)},\dots,f^{(t)}$ over F with cycles $(x_1^{(j)},\dots,x_{d_j}^{(j)},\dots,x_{md_j}^{(j)})$, such that $x_1^{(j)},\dots,x_{d_j}^{(j)}$ are pairwise non conjugated elements. Let $p_i^{(j)}$ be the minimal polynomials of elements x_i^j. Then by Lemma 1 there is a unique polynomial $f\in F[x]$ such that

$$\mathrm{deg(f)} < \prod_{\mathrm{j=1}}^{\mathrm{t}}\prod_{\mathrm{i=1}}^{\mathrm{d_j}} \mathrm{deg(p_i^{(j)})} \quad \text{and} \quad \mathrm{f \equiv f^{(j)} \mod \prod_{i=1}^{d_j} p_i^{(j)}} \quad \text{for all} \quad \mathrm{j\in\{1,\dots,t\}}$$

and

$$f_{md_j}(x_i^{(j)}) = x_i^{(j)}.$$

Put $l = m\cdot \mathrm{lcm(d_1,\dots,d_s)} = \mathrm{m\cdot lcm(d_1,\dots,d_t)}$, then $f_l(\bar{x}_i) = \bar{x}_i$ and so $l \in Cycl(K^s/F)$. □

Theorem 2. *Let $K_1, K_2,\dots,K_r$ be finite extensions of the field F, $s_1,\dots,s_r, r\in\mathbb{N}$. Then*

$$\mathrm{Cycl(K_1^{s_1}\oplus\cdots\oplus K_r^{s_r}/F) = \{lcm(l_i) \mid l_i \in Cycl(K_i^{s_i}/F)\}}.$$

Proof. Let $l\in \mathrm{Cycl(K_1^{s_1}\oplus\cdots\oplus K_r^{s_r}/F)}$. Then there is a polynomial $f\in F[x]$ with the cycle $\big((\bar{x}_1^{(1)},\dots,\bar{x}_1^{(r)}),\dots,(\bar{x}_l^{(1)},\dots,\bar{x}_l^{(r)})\big)$, where $\bar{x}_j^{(i)}\in K_i^{s_i}$ for $i=1,\dots,r, j=1,\dots,l$. Then

$$(\bar{x}_j^{(1)},\dots,\bar{x}_j^{(r)}) = f_l\big((\bar{x}_j^{(1)},\dots,\bar{x}_j^{(r)})\big) = \big(f_l(\bar{x}_j^{(1)}),\dots,f_l(\bar{x}_j^{(r)})\big).$$

Consider the least positive integers $l_i\leq l$ with $f_{l_i}(\bar{x}_j^{(i)}) = \bar{x}_j^{(i)}$. By lemma 2 we have $l_i|l$, therefore $l_i\in\mathrm{Cycl(K_i^{s_i}/F)}$ and $l = \mathrm{lcm(l_i)}$.

Let $l_i\in\mathrm{Cycl(K_i^{s_i}/F)}$ for $i=1,\dots,r$. Then there are polynomials $f^{(i)}$ over F with cycles $(\bar{x}_1^{(i)},\dots,\bar{x}_{l_i}^{(i)})$ such that $f_{l_i}^{(i)}(\bar{x}_j^{(i)}) = \bar{x}_j^{(i)}$ for $j=1,\dots,l_i$. Consider polynomials p_i over F as products of minimal polynomials of non conjugated elements in the cycle $(\bar{x}_1^{(i)},\dots,\bar{x}_{l_i}^{(i)})$. Now the fact, that different l_i-tuples $(\bar{x}_1^{(i)},\dots,\bar{x}_{l_i}^{(i)})$ don't consist conjugated elements for $i=1,\dots,r$, implies that these polynomials are pairwise coprime and by Lemma 1 we have a polynomial $f\in F[x]$ such that

$$f\equiv f^{(i)} \mod p_i \quad \text{for all} \quad j\in\{1,\dots,r\}.$$

Hence $f_{l_i}(\bar{x}_j^{(i)}) = \bar{x}_j^{(i)}$ and if $l = \mathrm{lcm(l_i)}$, then $l\in\mathrm{Cycl(K_1^{s_1}\oplus\cdots\oplus K_r^{s_r}/F)}$. □

Theorem 3. *Let $L_1,\dots,L_n$ are algebraic extensions of a field F, $L_1^{'},\dots,L_n^{'}$ are any subfields such that $F\subseteq L_i^{'}\subseteq L_i$ for $i=1,\dots,n$.*
Let $\bar{x}_1 = \langle x_1^{(1)},\dots,x_1^{(n)}\rangle,\dots,\bar{x}_{k+l} = \langle x_{k+l}^{(1)},\dots,x_{k+l}^{(n)}\rangle$ are different elements of the direct sum $L_1\oplus\cdots\oplus L_n$.
Let $d(L_i^{'}), t(L_i^{'}), N(L_i^{'})$ are nonnegative integers such that
$d(L_i^{'})$ is the number of non-conjugated elements of $L_i^{'}$ in the set $\{x_{k+1}^{(i)},\dots,x_{k+l}^{(i)}\}$,
$t(L_i^{i})$ is the number of non-conjugated elements of $L_i^{'}$ in the set $\{x_1^{(j)},\dots,x_k^{(j)}\}-$

$-\{x_{k+1}^{(j*)},\ldots,x_{k+l}^{(j*)}\}$ for $j=1,\ldots,n$ and some $j*\in\{1,\ldots,n\}$ such that $L_{j*}^{'}=L_i^{'}$, $N(L_i^{'})$ is the number of irreducible polynomials in $F[X]$ of degree $[L_i^{'}:F]$.

Then following assertions are equivalent:

a): *The sequence $(\bar{x}_1,\ldots,\bar{x}_{k+l})$ is a finite orbit of a polynomial $f\in F[X]$ in the direct sum $L_1\oplus\cdots\oplus L_n$ with precycle length k and cycle of the length l in the direct sum $L_1^{'}\oplus\cdots\oplus L_n^{'}$.*

b): *For $i=1,\ldots,n$, there are sequences of fields*

$$L_i\supseteq F(x_1^{(i)})\supseteq\cdots\supseteq F(x_{k_i}^{(i)})\supseteq F(x_{k_i+1}^{(i)})=\cdots=F(x_{k_i+l_i}^{(i)})=\cdots=F(x_{k+l}^{(i)})=L_i^{'}$$

where $k_i\in\mathbb{N}_0, l_i\in\mathbb{N}, k=\max(\mathrm{k_i})$ and
$l\in\mathrm{Cycl}(\mathrm{K_1^{s_1}}\oplus\cdots\oplus\mathrm{K_r^{s_r}}/\mathrm{F})=\mathrm{Cycl}(\mathrm{L_1^{'}}\oplus\cdots\oplus\mathrm{L_n^{'}}/\mathrm{F})$ and for every $i=1,\ldots,n$ it holds

$$t(L_i^{'})+\sum_{L_j^{'}=L_i^{'},d(L_j^{'})\ are\ distinct}d(L_j^{'})\le N(L_i^{'}).$$

Proof. Let $(\bar{x}_1,\ldots,\bar{x}_{k+l})$ is a finite orbit of a polynomial $f\in F[X]$ in the direct sum of algebraic field extensions $L_1\oplus\cdots\oplus L_n$ with precycle length k and cycle in the direct sum $L_1^{'}\oplus\cdots\oplus L_n^{'}$ of the length l.
Then by definition for $j=1,\ldots,k+l-1$ it holds

$$f(\bar{x}_j)=f(\langle x_j^{(1)},\ldots,x_j^{(n)}\rangle)=\langle f(x_j^{(1)}),\ldots,f(x_j^{(n)})\rangle=\langle x_{j+1}^{(1)},\ldots,x_{j+1}^{(n)}\rangle=\bar{x}_{j+1}$$

and for $j=k+1,\ldots,k+l$

$$f_l(\bar{x}_j)=f_l(\langle x_j^{(1)},\ldots,x_j^{(n)}\rangle)=\langle f_l(x_j^{(1)}),\ldots,f_l(x_j^{(n)})\rangle=\langle x_j^{(1)},\ldots,x_j^{(n)}\rangle=\bar{x}_j.$$

Then for every $i=1,\ldots,n$ there is a finite orbit $(x_1^{(i)},\ldots,x_{k+l}^{(i)})$ of the polynomial $f\in F[X]$ in the field L_i.

Consider least positive integers $k_i\in\mathbb{N}_0, l_i\in\mathbb{N}$ such that $f_{l_i}(x_j^{(i)})=x_j^{(i)}$ for every $j>k_i$. Then by definition and lemma2 l_i is the cycle length of i-th finite orbit, k_i is the precycle length of i-th orbit and $k=\max(\mathrm{k_i})$.

By proposition we obtain sequences of fields

$$L_i\supseteq F(x_1^{(i)})\supseteq\cdots\supseteq F(x_{k_i}^{(i)})\supseteq F(x_{k_i+1}^{(i)})=\cdots=F(x_{k+l}^{(i)})=L_i^{'}.$$

Let $K_1,\ldots,K_r$ be distinct fields such that $\{K_1,\ldots,K_r\}=\{L_1^{'},\ldots,L_n^{'}\}$ and suppose that K_i appears s_i times, so

$$L_1^{'}\oplus\cdots\oplus L_n^{'}=K_1^{s_1}\oplus\cdots\oplus K_r^{s_r}.$$

Now assume to the contrary that

$$t(L_i^{'})+\sum_{L_j^{'}=L_i^{'},d(L_j^{'})\text{ are distinct}}d(L_j^{'})>N(L_i^{'}).$$

Then there is a pair of conjugated elements such that one of them is in some precycle and the second one in some other cycle and it is in contradiction with lemma3. From b) to a) it follows immediately from Lemma1 and Theorem2.

□

References

[1] Halter-Koch, F., Konečná, P. Polynomial cycles in finite extension fields. *Mathematica Slovaca*, 52:531 – 535, 2002.

[2] Jakubec, S., Kostra, J., Nemoga, K. On the existence of an integral normal basis generated by a unit in prime extension of rational numbers.*Mathematics of Computation*, 56 :809 – 815, 1991.

[3] Jakubec, S., Kostra J., A note of normal basis of ideals. *Math. Slovaca*, 42 :677 – 684, 1992 .

[4] Jakubec, S., Kostra, J. On the existence of a normal basis for ambiguous ideal. *Atti del Seminario Matematico e Fisico dell Universita di Modena*, 46(1):125–129, 1998.

[5] Kostra, J. On orbits in ambiguous ideals. *Acta Acad. Paed. Agriensis, Sectio Mathematicae* , 29:35–39, 2002.

[6] Narkiewicz, W. Polynomial Mappings. Lecture Notes in Mathematics 1600, Springer, 1995.

Department of Mathematics, Faculty of Science, University of Ostrava, 30.Dubna 22, 701 03 Ostrava, Czech Republic

E-mail address: petra.konecna@osu.cz