Franz Halter-Koch; Petra Konečná

Polynomial cycles in finite extension fields

Mathematica Slovaca, Vol. 52 (2002), No. 5, 531--535

Persistent URL: http://dml.cz/dmlcz/129059

Mathematica Slovaca

Math. Slovaca, **52** (2002), No. 5, 531–535

POLYNOMIAL CYCLES IN FINITE EXTENSION FIELDS

FRANZ HALTER-KOCH* — PETRA KONEČNÁ**

(*Communicated by Stanislav Jakubec*)

ABSTRACT. Let K/F be an algebraic field extension. We characterize finite orbits of polynomial mappings of K which are induced by polynomials from F. As an application we determine all possible cycle lengths of such orbits in the case of a finite field 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

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

If R is a field, $k \in \mathbb{N}_0$ and $(x_1, x_2, \dots, x_{k+l})$ is any finite sequence of distinct elements of R, then it follows by Lagrange interpolation that there exists a polynomial $f \in R[X]$ (of degree $\deg(f) < k + l$) such that $(x_1, x_2, \dots, x_{k+l})$ is a finite orbit of f with precycle length k and cycle length l.

In contrast, if R is an integral domain of characteristic zero which is finitely generated (over $\mathbb{Z}$) with integral closure $\overline{R}$ such that $\left(\overline{R}^\times : R^\times\right) < \infty$, then in R there are (up to trivial cases) only finitely many equivalence classes of finite orbits of polynomials $f \in R[X]$, see [2; Theorem 5].

For a survey concerning finite polynomial orbits in integral domains, the reader should consult [6] and the survey articles [7] and [8]. For more recent results and problems, see [1], [3] and [9].

In this paper, we return to polynomial cycles in fields. We consider an algebraic field extension K/F and we determine the structure of finite orbits of polynomials $f \in F[X]$ in K. For a finite field F, we obtain as a corollary all possible lengths of cycles of polynomials from $F[X]$ in K.

2000 Mathematics Subject Classification: Primary 11C08, 11T06.
Keywords: polynomial cycle, finite field.

The research of the second author was supported by GA of the Czech Academy of Sciences Grant A1187101/01.

THEOREM. *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 with 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) *We have $F(x_1) \supset F(x_2) \supset \cdots \supset F(x_{k+1}) = \cdots = F(x_{k+l})$, there exist $d, m \in \mathbb{N}$, and there exists some $\tau \in \mathrm{Aut}_F(F(x_{k+1}))$ such that $l = dm$, $\mathrm{ord}(\tau) = m$, the elements $x_1, \dots, x_{k+d}$ are pairwise not conjugate over F, and*

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

For the proof we need the Chinese Remainder Theorem for polynomials, which we state for the convenience of the reader.

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

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

Proof. This follows immediately from well-known isomorphism

$$F[X]/f_1 \cdot \dots \cdot f_m F[X] \xrightarrow{\sim} \prod_{j=1}^{m} F[X]/f_j F[X]$$

(induced by the identity on $F[X]$). □

Proof of Theorem.

a) $\Longrightarrow$ b): Obvious.

b) $\Longrightarrow$ c): Let $(x_1, x_2, \dots, x_{k+l})$ be a finite orbit of $f \in F[X]$ with precycle length k and cycle length l, and set $x_{k+l+1} = x_{k+1}$. Now $f(x_i) = x_{i+1} \in F(x_i)$ implies $F(x_{i+1}) \subset F(x_i)$ for all $i \in \{1, \dots, k+l\}$. Since $F(x_{k+l+1}) = F(x_{k+1})$ it follows that

$$F(x_1) \supset F(x_2) \supset \cdots \supset F(x_{k+1}) = \cdots = F(x_{k+l}) ,$$

and there exist uniquely determined indices $0 \le e < q \le k+l$ such that $x_1, \ldots, x_q$ are pairwise not conjugate, and x_{q+1} is conjugate to x_{e+1} over F. But now $F(x_{e+1}) \supset F(x_{q+1})$ implies $F(x_{e+1}) = F(x_{q+1})$, and there is an automorphism $\tau \in \mathrm{Aut}_F(F(x_{e+1}))$ such that $x_{q+1} = \tau(x_{e+1})$, and we denote by $m = \mathrm{ord}(\tau)$ the order of τ in $\mathrm{Aut}_F(F(x_{e+1}))$.

Now we assert that

$$(x_1, \ldots, x_e, x_{e+1}, \ldots, x_q, \tau(x_{e+1}), \ldots, \tau(x_q), \ldots, \tau^{m-1}(x_{e+1}), \ldots, \tau^{m-1}(x_q))$$

is a finite orbit of f with precycle length e and cycle length $m(q-e)$. Once this is done, the assertion follows with $d = q-e$ and $k = e$, since every finite orbit is uniquely determined by its first element.

By definition, we have

$$f(\tau^\mu(x_{e+j})) = \tau^\mu(f(x_{e+j})) = \tau^\mu(x_{e+j+1})$$

for all $\mu \in \{0, \ldots, m-1\}$ and $j \in \{1, \ldots, q-e-1\}$, and

$$f(\tau^\mu(x_q)) = \tau^\mu(f(x_q)) = \tau^\mu(x_{q+1}) = \tau^{\mu+1}(x_{e+1})$$

for all $\mu \in \{0, \ldots, m-1\}$. In particular, it follows that $f(\tau^{m-1}(x_q)) = \tau^m(x_{e+1}) = x_{e+1}$, and since

$$F(x_q) \subset F(x_{q-1}) \subset \cdots \subset F(x_{e+1}) \subset F(\tau^{m-1}(x_q)) = F(x_q),$$

all these fields are equal.

It remains to prove that the $m(q-e)$ elements

$$\tau^\mu(x_{e+j}) \qquad \text{for} \quad \mu \in \{0, \ldots, m-1\} \text{ and } j \in \{1, \ldots, q-e\}$$

are distinct. Suppose that $i, j \in \{1, \ldots, q-e\}$ and $\nu, \mu \in \{0, \ldots, m-1\}$ are such that $\tau^\nu(x_{e+i}) = \tau^\mu(x_{e+j})$. Then the elements x_{e+i} and x_{e+j} are conjugate over F, and by the choice of q we obtain $i = j$. Since $F(x_{e+i}) = F(x_{e+1})$, we get $\tau^\nu = \tau^\mu$ and therefore finally $\nu = \mu$.

c) $\Longrightarrow$ **a)**: Let $g_1, \ldots, g_{k+d} \in F[X]$ be the minimal polynomials of $x_1, \ldots, x_{k+d}$ over F. By assumption, they are distinct and hence coprime in pairs. For every $j \in \{1, \ldots, k+d-1\}$, we have $x_{j+1} \in F(x_j)$, and therefore there exists a polynomial $f_j \in F[X]$ such that $x_{j+1} = f_j(x_j)$.

By the lemma, there exists some polynomial $f \in F[X]$ such that

$$\deg f < \prod_{i=1}^{k+d} \deg_F(x_i) \qquad \text{and} \qquad f \equiv f_j \mod g_j \quad \text{for all } j \in \{1, \ldots, k+d\}.$$

Then we obtain

$$f(x_j) = f_j(x_j) = x_{j+1} \qquad \text{for all} \quad j \in \{1, \ldots, k+d\},$$

and if $\mu \in \{0,\dots,m-1\}$ and $j \in \{1,\dots,d\}$, then

$$f(x_{k+\mu d+j}) = f\big(\tau^{\mu}(x_{k+j})\big) = \tau^{\mu}\big(f(x_{k+j})\big) = \tau^{\mu}(x_{k+j+1}) = x_{k+\mu d+j+1}\,.$$

Consequently, $(x_1,\dots,x_{k+l})$ is a finite orbit of f with precycle length k and cycle length l.

It remains to prove the uniqueness of f. Suppose that $(x_1,\dots,x_{k+l})$ is also a finite orbit with precycle length k and cycle length l of some polynomial $f^* \in F[X]$. Now $f^*(x_j) = f(x_j)$ implies $f^* \equiv f \mod g_j$ for all $j \in \{1,\dots,k+d\}$. Hence it follows by the uniqueness statement of the lemma that

$$f^* = f\,, \qquad \text{provided that} \quad \deg(f^*) < \prod_{i=1}^{k+d} \deg_F(x_i)\,.$$

□

COROLLARY. *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*

$$\operatorname{Cycl}(K/F) = \big\{dm:\ 1 \le d \le N,\ 1 \le m \,|\, n\big\}\,.$$

Proof. By part **c**) of Theorem, an integer $c \in \mathbb{N}$ lies in $\operatorname{Cycl}(K/F)$ if and only if $c = md$, where m is the order of some $\tau \in \operatorname{Aut}_F(K)$, and there exist d elements of K which are pairwise not conjugate over F. Since $\operatorname{Aut}_F(K)$ is cyclic of order n, m is the order of some $\tau \in \operatorname{Aut}_F(K)$ if and only if $m \mid n$. By the very definition of N, there exist d elements in K which are pairwise not conjugate over F if and only if $d \le N$. □

REFERENCES

[1] DIVIŠOVÁ, Z.: *On cycles of polynomials with integral rational coefficients*, Math. Slovaca **52** (2002), 537–540.

[2] HALTER-KOCH, F.—NARKIEWICZ, W.: *Scarcity of finite polynomial orbits*, Publ. Math. Debrecen **56** (2000), 405–414.

[3] KOSTRA, J.: *On orbits in ambiguous ideals*, Acta Acad. Paed. Agriensis, Sect. Math. **29** (2002) (To appear).

[4] LANG, S.: *Algebra*, Addison-Wesley, New York, 1993.

[5] LIDL, R.—NIEDERREITER, H.: *Finite Fields.* Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, Cambridge, 1997.

[6] NARKIEWICZ, W.: *Polynomial Mappings.* Lecture Notes in Mathematics 1600, Springer, New York, 1995.

[7] NARKIEWICZ, W.: *Arithmetics of dynamical systems: A survey*, Tatra Mt. Math. Publ. **11** (1997), 69–75.

[8] NARKIEWICZ, W.: *Finite polynomial orbits: A survey.* In: Algebraic Number Theory and Diophantine Analysis. (F. Halter-Koch, R Tichy, eds.), Proceedings of the International Conference, Graz, Austria, August 30-September, Walter de Gruyter, Berlin, 2000, pp. 331–338.

[9] NARKIEWICZ, W.: *Problem 9 in The Problem Session on The 3rd Czech and Polish Conference on Number Theory*, Acta Math. Inform. Univ. Ostraviensis **8** (2000), 9.

Received December 19, 2001
Revised April 22, 2002

* *Mathematisches Institut der Universität*
Heinrichstraße 36
A-8010 Graz
AUSTRIA
E-mail: franz.halterkoch@kfunigraz.ac.at

** *Department of Mathematics*
Faculty of Sciences
University of Ostrava
30. Dubna 22
CZ-701 03 Ostrava
CZECH REPUBLIC
E-mail: petra.konecna@osu.cz