Zuzana Divišová

On cycles of polynomials with integral rational coefficients

Mathematica Slovaca, Vol. 52 (2002), No. 5, 537--540

Persistent URL: http://dml.cz/dmlcz/136871

Mathematica Slovaca
©2002
Mathematical Institute
Slovak Academy of Sciences

Math. Slovaca, **52** (2002), No. 5, 537–540

ON CYCLES OF POLYNOMIALS WITH INTEGRAL RATIONAL COEFFICIENTS

ZUZANA DIVIŠOVÁ

(*Communicated by Stanislav Jakubec*)

ABSTRACT. The paper deals with polynomial cycles in the rings of integers of cyclic algebraic number fields for polynomials with integral rational coefficients. In the first part, a connection between the existence of cycles and the existence of power basis is shown. In the second part, properties of cycles for quadratic polynomials with rational integral coefficients are described.

Let K be a ring. Recall that a finite subset $\{x_1, x_2, \ldots, x_n\}$ of K is called a *cycle for a polynomial* $f(x)$ if for $i = 1, 2, \ldots, n-1$ one has $f(x_i) = x_{i+1}$, $f(x_n) = x_1$ and $x_i \neq x_j$ for $i \neq j$. The number n will be called the *length of the cycle*, and x_i's, *cyclic elements of order* n. Denote by f_i the ith iterate of f for $i = 1, 2, \ldots$, i.e. $f_1 = f$ and $f_{i+1} = f(f_i)$ for $i = 1, 2, \ldots$. Let K be an algebraic number field; denote by $\mathbb{Z}_K$ the ring of integers of K.

The possible cycle-lengths in the rings of integers in quadratic number fields were determined independently by J. Boduch and by G. Baron. The result can be found in [6].

For fields K of larger degrees, the problem of determining all cycle-lengths in their rings of integers $\mathbb{Z}_K$ is still open. Cycles of quadratic polynomials were recently studied by P. Morton [5] and P. Russo, R. Walde [11].

In this paper, only cycle-lengths for polynomials with rational integral coefficients in the rings of integers $\mathbb{Z}_K$ of an algebraic number field K will be studied. First, a connection between the existence of power basis for $\mathbb{Z}_K$ over rational integers $\mathbb{Z}$ and polynomial cycles for a polynomial $f(x) \in \mathbb{Z}[x]$ will be investigated.

Recall the definition of an order.

2000 Mathematics Subject Classification: Primary 11R04, 11C08.
Keywords: polynomial cycle, ring of integers of algebraic number field.

This research was supported by GA of the Czech Academy of Sciences, Grant A1187101/01.

DEFINITION 1. Let $K/\mathbb{Q}$ be an algebraic number field of degree n. An *order* of K is a subring of $\mathbb{Z}_K$ which contains an integral basis of length n.

THEOREM 1. *Let $K/\mathbb{Q}$ be a cyclic algebraic number field of degree n and let σ be a generator of its Galois group G. There exists a polynomial $f(x) \in \mathbb{Z}[x]$ of degree less than n with a cycle $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ in $\mathbb{Z}_K$, where $\alpha_i = \alpha^{\sigma^{i-1}}$ for $i = 1, 2, \ldots, n$, if and only if there exists an order of K with a power basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ which is a G-module.*

Proof. Let $f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$, $a_i \in \mathbb{Z}$, be a polynomial with a cycle $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ in $\mathbb{Z}_K$ where $\alpha_i = \alpha^{\sigma^{i-1}}$. So $\alpha_{i+1} = f(\alpha_i)$. Clearly, any $\alpha_i \in \mathbb{Z}[1, \alpha_1, \alpha_1^2, \ldots, \alpha_1^{n-1}]$, and so $\mathbb{Z}[1, \alpha_1, \alpha_1^2, \ldots, \alpha_1^{n-1}]$ is a G-module. Now let the order $\mathbb{Z}[1, \alpha, \alpha^2, \ldots, \alpha^{n-1}]$ be a G-module. Denote $\alpha_i = \alpha^{\sigma^{i-1}}$. So $\alpha_{i+1} = a_{n-1}\alpha_i^{n-1} + a_{n-2}\alpha_i^{n-2} + \cdots + a_1\alpha_i + a_0$ where $a_i \in \mathbb{Z}$. From above it follows that $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a cycle for the polynomial $f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0$. □

Remark. If the assumption of Theorem 1 holds, then for any d such that $d \mid n$, there exists a polynomial $g(x) \in \mathbb{Z}[x]$ of degree less then n with a cycle length d in $\mathbb{Z}_K$. It is $\frac{n}{d}$th iteration of $f(x)$ modulo a minimal polynomial of α_i.

EXAMPLE 1. Let ζ be a primitive 7th root of unity and let $K = \mathbb{Q}(\zeta)$ be the 7th cyclotomic field. The degree of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is $n = 6$. Let $\mathbb{Z}_{\mathbb{Q}(\zeta)}$ be the ring of integers of $\mathbb{Q}(\zeta)$. Then $\mathbb{Z}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta, \zeta^2, \ldots, \zeta^6] = \mathbb{Z}[1, \zeta, \zeta^2, \ldots, \zeta^5]$. Using the fact that $\sigma\colon \zeta \to \zeta^3$ is a generator of the Galois group $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ it follows that a polynomial $f(x) = x^3$ has the cycle $\{\zeta, \zeta^3, \zeta^2, \zeta^6, \zeta^4, \zeta^5\}$. Put $g(x)$ equal to the second and $h(x)$ the third iteration of $f(x)$ modulo the minimal polynomial of ζ, so $g(x) = x^2$ and $h(x) = -x^5 - x^4 - x^3 - x^2 - x - 1$. Then $\{\zeta, \zeta^2, \zeta^4\}$ is the cycle of length 3 for $g(x)$ and $\{\zeta, \zeta^6\}$ is a cycle of length 2 for $h(x)$.

EXAMPLE 2. Let K be a cyclic algebraic number field of degree 3 over $\mathbb{Q}$ with the conductor 31. With regard to the fact (shown by Kostra) that for a cyclic algebraic number field of an odd prime degree l with the conductor which is a power q^s of Mersenne prime $q = 2^r - 1$, where l and rq are coprime numbers, there is no power basis for any G-submodule of the ring of integers, we can say that in the field K there is no power basis for any G-submodule of $\mathbb{Z}_K$, so by Theorem 1 there is no polynomial cycle for $f(x) \in \mathbb{Z}[x]$ in the ring of integers $\mathbb{Z}_K$, the elements of which are conjugated.

The following Theorem 2 will show that if a quadratic polynomial of $\mathbb{Z}[x]$ has a cycle of length 3 in a cubic algebraic number field, then it is the case of Theorem 1.

THEOREM 2. *Let K be a cubic algebraic number field and let the quadratic polynomial $f(x) \in \mathbb{Z}[x]$ have a cycle $\{\alpha_1, \alpha_2, \alpha_3\}$ of length 3 in $\mathbb{Z}_K$. Then K is normal and α_1, α_2, α_3 are conjugated.*

Proof. By [6; Lemma 12.1.(v)], $f_3(x) = x + \big(f(x) - x\big)g(x)$ and with regard to the fact that $f(x)$ is quadratic, it follows that $g(x)$ is of degree 6. By $f_3(\alpha_i) = \alpha_i$ we have $g(x) \equiv 0 \mod f_{\alpha_i}$, where f_{α_i} is a minimal polynomial for α_i for $i = 1, 2, 3$. By [6; Lemma 12.9], the degree of f_{α_i} cannot be 1, so it has to be 3. So at least two of f_{α_i} are the same. Without loss of generality, put $f_{\alpha_1} = f_{\alpha_2}$. So there exists an isomorphism σ from $\mathbb{Q}(\alpha_1)$ to $\mathbb{Q}(\alpha_2)$ over $\mathbb{Q}$ such that $\alpha_1^\sigma = \alpha_2$. We have $\alpha_2 = \alpha_1^\sigma = f(\alpha_1)$ and $\alpha_2^\sigma = f(\alpha_1)^\sigma = f(\alpha_1^\sigma) = f(\alpha_2) = \alpha_3$. Hence $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_K$ and they are conjugated. □

COROLLARY 1. *Let K be an algebraic number field, let $f(x) \in \mathbb{Z}[x]$ be a quadratic polynomial and let $\{\alpha_1, \alpha_2, \alpha_3\}$ be its polynomial cycle of length 3 in $\mathbb{Z}_K$. Then $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_M$, where M is a subfield of K such that $[M : \mathbb{Q}] = 3$ or 6 and α_i are conjugated.*

Proof. If $f(x)$ is a quadratic polynomial over $\mathbb{Z}$, then $f_3(x) - x = \big(f(x) - x\big)g(x)$ and the degree of $g(x)$ is 6. By [6; Lemma 12.9], $g(x)$ cannot have a linear factor, and by [5; Theorem 3], $f(x)$ does not have a quadratic factor. So if $f_\alpha(x)$ is an irreducible factor of $g(x)$, then the degree of $f_\alpha(x)$ is 3 or 6. Now the result follows immediately. □

COROLLARY 2. *Let K be an algebraic number field of degree n over $\mathbb{Q}$ and $3 \nmid n$. Then there is no quadratic polynomial with cycle of length 3 with conjugated elements.*

Acknowledgement

My thanks belong to Juraj Kostra for his help and encouragement.

REFERENCES

[1] BODUCH, J.: *Polynomial Cycles in Rings of Algebraic Integers.* MA Thesis, Wroclaw University, 1990.

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

[3] HALTER-KOCH, F.—KONEČNÁ, P.: *Polynomial cycles in finite extension fields*, Math. Slovaca **52** (2002), 531–535.

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

[5] MORTON, P.: *Arithmetic properties of periodic points of quadratic maps*, Acta Arith. **62** (1992), 343–372.

[6] NARKIEWICZ, W.: *Polynomial Mappings*. Lecture Notes in Math. 1600, Springer-Verlag, Berlin-Heidelberg, 1995.

[7] NARKIEWICZ, W.: *Polynomial cycles in algebraic number fields*, Colloq. Math. **58** (1989), 151–155.

[8] PEZDA, T.: *Cycles of polynomials in algebraically closed fields of positive characteristics*, Colloq. Math. **67** (1994), 187–195.

[9] PEZDA, T.: *Cycles of polynomials in algebraically closed fields of positive characteristics II*, Colloq. Math. **71** (1996), 23–30.

[10] PEZDA, T.: *Polynomial cycles in certain local domains*, Acta Arith. **66** (1994), 11–22.

[11] RUSSO, P.—WALDE, R.: *Rational periodic points of the quadratic function* $Q_c(x) = x^2 + c$, Amer. Math. Monthly **101** (1994), 318–331.

[12] VAVROŠ, M.: *A note on polynomial cycles* (Submitted).

Received November 6, 2001
Revised March 5, 2002

Faculty of Sciences
Department of Mathematics
University of Ostrava
30. dubna 22
CZ–701 03 Ostrava
CZECH REPUBLIC
E-mail: zuzana.divisova@osu.cz