Functiones et Approximatio
42.2 (2010), 163–168

CYCLE-LENGTHS OF A CLASS OF MONIC BINOMIALS

Władysław Narkiewicz

Abstract: Let K be an algebraic field of degree N and let p be an odd prime. It is shown that if K does not contain p-th primitive roots of unity and $f(X) = X^{p^k} + c$ with $k \geqslant 1$ and non-zero $c \in K$, then the length of cycles of f in K is bounded by a value depending only on K and p. If $p > 2^N$, then this bound depends only on N.

Keywords: polynomial cycles, algebraic number fields.

1. Let F be a polynomial with coefficients in a field K. A sequence $a_1, a_2, \ldots, a_k$ of distinct elements of K is said to be a cycle of length k for F provided one has $F(a_i) = a_{i+1}$ for $i = 1, 2, \ldots, k-1$ and $F(a_k) = a_1$.

It has been conjectured by P.Russo and R.Walde in [RW] that the length of a cycle for a quadratic polynomial in the rational number field is bounded by an absolute constant. One expects this constant to be equal to 3. P.Morton ([Mo]) proved that quadratic polynomials cannot have a cycle of length four in the rational field, and T.Erkama ([Er]) showed that the same happens in the field $\mathbf{Q}(i)$. The impossibility of a cycle of length five in the rational case has been established by E.V.Flynn, B.Poonen and E.F.Schaefer ([FPS]), and M.Stoll ([S]) showed that the conjecture of Birch and Swinnerton-Dyer implies the non-existence of 6-cycles. The Russo-Walde conjecture was later extended by P.Morton and J.Silverman ([MS]), who conjectured that there is a constant $B(n, d)$ such that the union of all finite orbits of polynomials of degree d in an algebraic number field K of degree n cannot have more than $B(n, d)$ elements.

In this note we shall consider binomials $F(X) = X^n + c$ with $n = p^r$, where p is an odd prime. If K is a real field, then F is increasing hence it cannot have in K cycles longer than 1. This argument is not applicable to totally complex algebraic number fields but we shall show that if K does not contain primitive p-th roots of unity, then the lengths of cycles of F in K are bounded by a value depending

2010 Mathematics Subject Classification: primary: 11R09; secondary: 37C25, 37E15, 37F10.

on K and p, and if $p > 2^{[K:\mathbf{Q}]}$, then this bound depends only on the degree of K. Note that the assumption about roots of unity implies that every finite orbit of F forms necessarily a cycle.

Theorem. *Let K be a totally complex extension of the rationals of degree $N > 1$, denote by R its ring of integers and let D be the maximal order of a primitive root of unity contained in K. Let p be a prime not dividing D, and put $F(X) = X^n + c \in K[X]$ with n being a power of p and $c \neq 0$. Then the lengths of cycles of F in K are bounded by a constant depending only on K and p. If $p > 2^N$, then this constant can be taken to be $N2^{N+1}(2^N - 1)$.*

2. In this section R will be an arbitrary Dedekind domain, and K its field of fractions. For a prime ideal $\mathfrak{p}$ we denote by $\nu_\mathfrak{p}$ the corresponding additive valuation of K. We shall deal with polynomials $F(X) = X^n + c$ with $c \in K \setminus R$. This implies that there exist prime ideals $\mathfrak{p}$ with $\nu_\mathfrak{p}(c) < 0$. We shall denote the m-th iterate of polynomial F by F_m.

We start with a simple observation:

Lemma 1. *Let $n \geqslant 2$, $F(X) = X^n + c$ with $c \in K \setminus R$, let*

$$r_1 \mapsto r_2 \mapsto \ldots \mapsto r_k \mapsto r_1$$

be a cycle of F, lying in K, and prolong this cycle periodically by putting $r_{m+k} = r_m$ for $m = 1, 2, \ldots$. Then all r_j's are non-zero, and if $\mathfrak{p}$ is a prime ideal of R with $\nu_\mathfrak{p}(r_j) < 0$ for some j, then $\nu_\mathfrak{p}(c) < 0$.

Proof. Let $\mathfrak{p}$ be a prime ideal with $\lambda = \nu_\mathfrak{p}(c) < 0$ and assume $r_i = 0$ for some i. We may assume $i = k$. Then $r_1 = F(r_k) = F(0) = c$, hence $\nu_\mathfrak{p}(r_1) = \lambda$, and in view of $r_2 = F(r_1) = F(c) = c^n + c$ and $\nu_\mathfrak{p}(c^n) = n\lambda < \lambda$ we get

$$\nu_\mathfrak{p}(r_2) = \nu_\mathfrak{p}(c^n) = n\lambda < \lambda.$$

An easy induction leads now to

$$\nu_\mathfrak{p}(r_j) = n^{j-1}\lambda$$

for $j = 2, 3, \ldots$, hence $\nu_\mathfrak{p}(r_k) = n^{k-1}\lambda$, contradicting $r_k = 0$.

To prove the second assertion observe that if $\nu_\mathfrak{p}(c) \geqslant 0$, then $F \in R_\mathfrak{p}[X]$, $R_\mathfrak{p}$ being the closure of R in the completion $K_\mathfrak{p}$ of K. Since $R_\mathfrak{p}$ is integrally closed and F is monic, all elements of its cycle in K, being roots of the monic polynomial $F_k(X) - X$ lie in $R_\mathfrak{p}$. ∎

Note, that the assumption $c \notin R$ is essential, as the example $K = \mathbb{Q}(i)$, $f(X) = X^3 + i$, with $0 \mapsto i \mapsto 0$ shows.

The following lemma generalizes slightly the results obtained in [RW] and [CG] (Corollary 6.7), where the case $n = 2$ has been considered.

Lemma 2. *Let $n \geqslant 2$, $F(X) = X^n + c$ with $c \in K \setminus R$, and assume that*

$$r_1 \mapsto r_2 \mapsto \ldots \mapsto r_k \mapsto r_1$$

is a cycle of length $k \geqslant 3$ for F, lying in K. Put $I_0 = cR$, $I_j = r_jR$ $(j = 1, 2, \ldots, k)$, and define the fractional ideals A_j, B_j by

$$I_j = A_j B_j^{-1} \qquad (j = 0, 1, \ldots, k),$$

where $A_0, A_1, \ldots, A_k, B_0, B_1, \ldots, B_k$ are ideals of R satisfying $(A_j, B_j) = R$ for $j = 0, 1, \ldots, k$. Then the ideal B_0 is an n-th power, say $B_0 = B^n$, and for $j = 1, 2, \ldots, k$ one has $B_j = B$.

Proof. It follows from Lemma 1 that none of the r_j's vanishes, hence the ideals A_j,B_j are well-defined. Note also that in view of $c \notin R$ we have $B_0 \neq R$. Let $\mathfrak{p}$ be a prime ideal dividing B_0 and denote, for shortness, $\nu_{\mathfrak{p}}(x)$ by $\nu(x)$. Putting $r_{k+1} = r_1$ we have $r_{j+1} = r_j^n + c$ for $j = 1, 2, \ldots, k$, hence

$$\nu(r_{j+1}) \geqslant \min\{n\nu(r_j), \nu(c)\}, \tag{1}$$

with equality in the case $n\nu(r_j) \neq \nu(c)$. Observe first that we must have

$$\nu(c) \leqslant n\nu(r_j) \tag{2}$$

for all j. Indeed, if for some i one would have

$$\nu(c) > n\nu(r_i), \tag{4}$$

then (1) would imply

$$\nu(r_{i+1}) = n\nu(r_i). \tag{3}$$

Since $\nu(c) < 0$ we get $\nu(r_i) < 0$, and (3) leads to $\nu(r_{i+1}) < \nu(r_i)$, hence

$$n\nu(r_{i+1}) = n^2\nu(r_i) < n\nu(r_i) < \nu(c),$$

so we may repeat this argument to obtain that the sequence $\nu(r_j)$ decreases indefinitely, contradiction.

If for a certain i we would have $n\nu(r_i) > \nu(c)$, then $\nu(r_{i+1}) = \nu(c) < 0$, hence $n\nu(r_{i+1}) = n\nu(c) < \nu(c)$, contradicting (2). Finally we see that for all prime ideals $\mathfrak{p}$ dividing B_0 and all j one has

$$\nu_{\mathfrak{p}}(c) = n\nu_{\mathfrak{p}}(r_j). \tag{4}$$

This shows that if a prime ideal divides B_0, then it divides $B_1, \ldots, B_k$. On the other hand Lemma 1 implies that every prime ideal dividing B_j divides B_0, and therefore (4) holds for all $\mathfrak{p}|B_j$, showing that the ideal B_0 is an n-th power of an ideal, say B, and for all j one has $B_j = B$, as asserted. ∎

Lemma 3. *Let $F(X) = X^n + c$ with $n \geqslant 2$ and $c \in K \setminus R$, and assume that $r_1 \mapsto \ldots \mapsto r_k \mapsto r_1$ is a cycle of length $k \geqslant 3$ for F lying in K.*

Then there is a class $\mathcal{X}$ in the class-group of ideals of R such that if the ideal I lies in $\mathcal{X}$ and is prime to B, then there exist $a, b, N_1, \ldots, N_k \in R$ such that

$$c = \frac{a}{b^n}, \quad r_j = \frac{N_j}{b}, \quad (aR, b^n R) = I^n, \quad (N_j R, bR) = I, \qquad (j = 1, 2, \ldots, k).$$

If we extend the sequence N_j be periodicity, putting $N_{j+k} = N_j$ for $j \geqslant 1$, then the following holds:

(i) *The sequence N_j satisfies the recurrence $b^{n-1} N_{j+1} = N_j^n + a$,*

(ii) *One has*

$$\prod_{i=1}^{k} (N_{i+1}^{n-1} + N_{i+1}^{n-2} N_i + \cdots + N_i^{n-1}) = b^{k(n-1)},$$

(iii) *For $i = 1, 2, \ldots, k$ one has $(N_i R, B) = R$.*

Note that in case $n = 2$ and $R = \mathbb{Z}$ the equality (ii) is a simple consequence of Theorem 1 in [Be].

Proof. Let A_i, B_i be as in Lemma 2, let $\mathcal{Y}$ be the ideal class containing B, let $\mathcal{X} = \mathcal{Y}^{-1}$, and choose an ideal $I \in \mathcal{X}$ with $(I, B) = R$. Then with some $b \in R$ we have $IB = bR$. If we now put $a = cb^n$ and $N_j = r_j b$ for $j = 1, 2, \ldots, k$, then

$$N_j R = r_j bR = r_j IB = I_j IB = A_j B^{-1} IB = A_j I \subset R,$$

hence $N_j \in R$, and we obtain

$$(N_j R, bR) = (A_j I, BI) = I.$$

In view of $B_0 = B^n$ we get

$$(aR, b^n R) = (cb^n R, b^n R) = (A_0 B_0^{-1} I^n B^n, I^n B^n) = (A_0 I^n, B^n I^n) = I^n.$$

Now (i) results from

$$\frac{N_{j+1}}{b} = r_{j+1} = r_j^n + c = \left(\frac{N_j}{b}\right)^n + \frac{a}{b^n},$$

and to obtain (ii) multiply for $i = 1, \ldots, k$ the equalities

$$b^{n-1}(N_{i+2} - N_{i+1}) = (N_{i+1} - N_i)(N_{i+1}^{n-1} + N_{i+1}^{n-2} N_i + \cdots + N_i^{n-1})$$

which follow from (i). Finally (iii) follows from the equality $N_i R = A_i I$ and $(A_i, B) = (I, B) = R$. ∎

3. Now let R be the ring of integers of an algebraic number field K of degree N over the rationals.

We shall need three auxiliary results. The first is well-known, the second has been proved by T.Pezda ([Pe], Theorem 1 (ii)), and the third is a theorem of Bauer ([Ba]), of which a proof can be found in [Na] (Corollary 1 to Theorem 7.38):

Lemma 4.

(i) *If R is the ring of integers of a finite extension of the rationals, $a \neq b$ are non-zero elements of R and n is a power of an odd prime p, then for every prime ideal $\mathfrak{p}$ of R containing $(a^n - b^n)/(a-b)$ either $\mathfrak{p}$ divides both aR and bR, or $\mathfrak{p}|pR$ and $a \equiv b \pmod{\mathfrak{p}}$, or, finally, one has $N\mathfrak{p} \equiv 1 \pmod{p}$, $N\mathfrak{p}$ denoting the norm of $\mathfrak{p}$.*

(ii) *Let q be a prime, let L be a finite extension of the q-adic field $\mathbb{Q}_q$ and let $\mathbb{Z}_L$ be its ring of integers. The lengths of cycles in $\mathbb{Z}_L$ of any polynomial $f \in \mathbb{Z}_L[X]$ are bounded by a constant $B(L)$, depending only on L. More precisely, one has*

$$B(L) = N(\mathfrak{Q})(N(\mathfrak{Q}) - 1)q^{1+\log_2 e},$$

where $\mathfrak{Q}$ is the the unique prime ideal of $\mathbb{Z}_L$ and e is the ramification index of the extension $L/\mathbb{Q}_q$.

(iii) *If K is an algebraic number field, p is a rational prime and for all except finitely many prime ideals $\mathfrak{p}$ of the first degree one has*

$$N(\mathfrak{p}) \equiv 1 \pmod{p},$$

then K contains p-th primitive roots of unity.

4. Proof of the Theorem: In the proof we may assume $c \notin R$, as otherwise all assertions of Theorem 3 are direct consequences of results of Pezda ([Pe]).

Observe first that to establish our assertion it suffices to find a prime ideal $\mathfrak{P}$ not dividing B whose norm is bounded in terms of K and p. Indeed, if $K_{\mathfrak{P}}$ is the completion of K at $\mathfrak{P}$ and $R_{\mathfrak{P}}$ is its ring of integers, then $F(X) \in R_{\mathfrak{P}}[X]$ and as every cycle of F in K lies in $R_{\mathfrak{P}}$ the Theorem will follow from Lemma 4 (ii).

We shall use now the notation of Lemma 3. Let $\mathfrak{p}$ be a prime ideal dividing B. Since $\mathfrak{p}|bR$ it follows from part (ii) of Lemma 3 that $\mathfrak{p}$ contains an integer of the form $(N_{i+1}^n - N_i^n)/(N_{i+1} - N_i)$. Lemma 4 (i) implies now that one has either

(i) $\mathfrak{p}|(N_iR, N_{i+1}R)$, or
(ii) $\mathfrak{p}|pR$, or
(iii) $N\mathfrak{p} \equiv 1 \pmod{p}$.

Observe that (i) is impossible due Lemma 3 (iii). This shows that every prime ideal $\mathfrak{P}$ with $\mathfrak{P} \nmid pR$, and $N(\mathfrak{P}) \not\equiv 1 \pmod{p}$ does not divide B, thus satisfies our needs. It remains thus to find such $\mathfrak{P}$ with bounded norm.

First assume $p > 2^N$. In that case if $\mathfrak{p}_2$ is a prime ideal containing 2, then its norm does not exceed 2^N, hence $N(\mathfrak{p}_2) \leqslant 2^N < p$, violating (iii). Since $p \neq 2$

condition (ii) is also impossible. Therefore $\mathfrak{p}_2 \nmid B$, and Lemma 4 (ii) gives the bound $N2^{N+1}(2^N-1)$ for any cycle of F in K.

If $p \leqslant 2^N$, then recall that K does not contain p-th roots of unity, hence by Lemma 4 (iii) there exist $N+1$ prime ideals, say $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_{N+1}$ with $N(\mathfrak{P}_j) \not\equiv 1 \pmod{p}$. Since the prime p can lie in at most N distinct prime ideals, hence at least one $\mathfrak{P}_i$ does not not divide pR. Therefore $\mathfrak{P}_i \nmid B$ and the application of Lemma 4 (ii) bounds the length of any cycle of F in K by a number depending only on K and p. ■

References

[Ba] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*, Math. Ann., **77**, 1916, 353–356.

[Be] R.L. Benedetto, *An elementary product identity in polynomial dynamics*, Amer. Math. Monthly, **108**, 2001, 860–864.

[CG] G.S. Call, S.W. Goldstine, *Canonical heights on projective space*, J. Number Theory, **63**, 1997, 211–243.

[Er] T. Erkama, *Periodic orbits of quadratic polynomials*, Bull. London Math. Soc., **38**, 2006, 804–814.

[FPS] E.V. Flynn, B. Poonen, E.F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus* 2*-curve*, Duke Math.J., **90**, 1997, 435–463.

[Mo] P. Morton, *Arithmetic properties of periodic points of quadratic maps*, Acta Arith., **62**, 1992, 343–372.

[MS] P. Morton, J.H. Silverman, *Rational periodic points of rational functions*, Intern. Math. Res. Notices, 1994, 97–109.

[N] W. Narkiewicz, *Polynomial Mappings*, Lecture Notes in Math., **1600**, Springer 1989.

[Na] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer 2004.

[Pe] T. Pezda, *Polynomial cycles in certain local domains*, Acta Arith., **66**, 1994, 11–22.

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

[S] M. Stoll, *Rational* 6*-cycles under iteration of quadratic polynomials*, LMS Journal of Comput. Math., **11**, 2008, 367–380.

Address: Institute of Mathematics, Wrocław University, Poland.

E-mail: narkiew@math.uni.wroc.pl

Received: 27 July 2009; **revised:** 17 November 2009