COLLOQUIUM MATHEMATICUM
VOL. LVIII 1989 FASC. 1

POLYNOMIAL CYCLES IN ALGEBRAIC NUMBER FIELDS

BY

W. NARKIEWICZ (WROCŁAW)

1. Let K be a field, let P be a K-polynomial, and let L be an extension of K. A sequence $x_0,\dots,x_{n-1}$ of distinct elements of L is called an *n-cycle* for P provided $P(x_{n-1}) = x_0$ and for $i = 0, 1, 2, \dots, n-2$ one has $P(x_i) = x_{i+1}$.

Baker [2] proved in 1964 that every non-constant and non-linear polynomial with complex coefficients has n-cycles lying in the complex field for every $n \neq 2$ and he described all polynomials without a 2-cycle as those which are linearly conjugated with $x^2 - x$. (Two functions f, g are *linearly conjugated* if there exists a linear polynomial L such that $L(f) = g(L)$.) A similar result holds, more generally, for entire functions: in [1] Baker proved that every entire function which is not a constant nor a linear polynomial has cycles of every length except possibly one.

It follows from [6] that a polynomial with coefficients in an algebraic number field K can have only a finite number of cycles lying in K, and Lagrange's formula makes it clear that one can construct polynomials over such fields having a given finite number of cycles of prescribed length. If one restricts attention to monic polynomials with integral coefficients, then the situation is different and, in fact, we shall prove below (Corollary to Theorem I) that in this case the cycle lengths are bounded by a constant depending only on the degree of the field in question but not on the polynomial nor on the field itself. This is a special case of a more general result which we now state:

Let P be a polynomial with coefficients in K, let $A(P)$ be its leading coefficient, and denote by $S_1(P)$ the set of all prime ideals p of Z_K, the ring of integers of K, for which at least one coefficient of P is not p-integral. Let $S_2(P)$ be the set of all prime ideals p for which $1/A(P)$ is not p-integral and let

$$S(P) = S_0(P) \cup S_1(P) \cup S_\infty,$$

where S_∞ is the set of all infinite primes of K. Let $w(P)$ be the cardinality of $S(P)$, and finally let $t(P)$ denote the smallest norm of a prime ideal of Z_K not belonging to $S(P)$. Note that from the Prime Ideal Theorem one obtains the evaluation

$$t(P) = O(w(P)\log w(P)).$$

2. THEOREM I. *For all pairs M, w of positive integers there exists a number*

$B(M, w)$ with the property that if K is an algebraic number field of degree M, P is a K-polynomial with $w(P) = w$, then every n-cycle of P lying in K satisfies

$$n \leqslant B(M, w);$$

more precisely,

$$n \leqslant (6 \cdot 7^{M+2w(P)})^{\pi(t(P))},$$

where $\pi(u)$ denotes the number of prime ideals of Z_K with norms not exceeding u.

COROLLARY. *If P is a monic polynomial with coefficients in Z_K, then the length of its cycles lying in K is bounded by a constant, depending only on the degree of K, but not on the polynomial nor on K itself. This constant does not exceed $\exp(C \cdot 2^M)$ with a suitable absolute constant C.*

Proof. Let R be the set of all S-integral elements of K. Note that all coefficients of P lie in R and $A(P)$ is invertible in R. We shall work in R, and hence in the sequel divisibility, units and associated elements will be considered in this ring. (Of course, units of R are exactly the S-units of K.)

Let

$$x_0 = P(x_{n-1}), \quad x_1 = P(x_0), \quad \ldots, \quad x_{n-1} = P(x_{n-2})$$

be an n-cycle for P lying in K. Since every x_i is a fixpoint of the n-th iterate of P and R is integrally closed in K, all elements of the cycle lie in R. Without restricting the generality we may thus assume that $x_0 = 0$, replacing if necessary $P(x)$ by $P_1(x) = P(x+x_0)-x_0$, which evidently has the same cycle structure and satisfies $S(P_1) = S(P)$. The following lemma gives us some insight in the structure of cycles of P:

LEMMA 1. *The numbers x_i $(i = 1, 2, \ldots, n-1)$ are all divisible (in R) by x_1 and if we put $t_i = x_i/x_1$ $(i = 0, 1, \ldots, n-1)$ and $t_i = t_{i(\mathrm{mod}n)}$ for $i \geqslant n$, then the following holds:*

(i) *For any fixed $k = 1, 2, \ldots$ the differences $t_{j+k}-t_j$ are associated in R (i.e., differ by a factor which is an S-unit).*

(ii) *For $i = 0, 1, \ldots, n-1$ the differences $t_{i+1}-t_i$ are S-units.*

Proof. Let N be the degree of P and let

$$P(x) = \sum_{i=0}^{N} a_i x^i$$

with $a_i \in R$. Since $x_1 = P(0) = a_0$ and $x_2 = P(x_1)$, we obtain the divisibility of x_2 by x_1 and the divisibility of the x_i's by x_1 follows now by recurrence. This shows that the t_i's lie in R.

Now fix a positive integer k. Since

$$x_{i+k}-x_i = P(x_{i+k-1})-P(x_{i-1}),$$

we get

$$(x_{i+k-1}-x_{i-1}) \mid (x_{i+k}-x_i).$$

Thus for $i = 0, 1, 2, \ldots$

$$(t_{i+k-1}-t_{i-1})|(t_{i+k}-t_i)$$

holds, and this leads to

$$t_k = (t_k-t_0)|(t_{k+1}-t_1)| \ \ldots \ |(t_{k+n}-t_n) = t_k,$$

proving (i). Finally, (ii) results from (i) and the observation that $t_1-t_0 = 1$.

COROLLARY 1. *For $k = 1, 2, \ldots, n-1$ and all m the number t_k divides t_{km}.*

Proof. By (i) the numbers t_k, $t_{2k}-t_k, \ldots$ are associated, and hence they all are divisible by t_k. This immediately implies the assertion.

COROLLARY 2. *If $(k, n) = 1$, then t_k is an S-unit. In particular, t_{n-1} is an S-unit.*

Proof. Choose m so that $km \equiv 1 (\mathrm{mod} n)$. According to Corollary 1, $t_k|t_1 = 1$.

COROLLARY 3. *If n is a prime, then $t_1, \ldots, t_{n-1}$ as well as all differences t_i-t_j $(i, j = 1, 2, \ldots, n-1;\ i \neq j)$ are S-units.*

Proof. The first assertion is a special case of Corollary 2 and the second results from the observation that due to the part (i) of Lemma 1 the numbers t_i-t_j and $t_{i-j}-t_0 = t_{i-j}$ are associated.

Recall that the *Lenstra constant* $L(A)$ of a ring A (see [4] and [5]) is defined as the maximal length of a sequence $b_1, \ldots, b_r$ of elements of A with the property that all non-zero differences b_i-b_j are units. If A has a finite homomorphic image A', then this constant is finite since it clearly cannot exceed the cardinality of A'. Hence in our case, with $A = R$, we see that $L(R)$ does not exceed $t(P)$, defined above as the smallest norm of a prime ideal p of Z_K not belonging to $S(P)$.

LEMMA 2. *If n is a prime number, then $n \leqslant L(R) \leqslant t(P)$.*

Proof. The assertion follows from Corollary 3 and the definition of the Lenstra constant.

LEMMA 3. *If $n = p^a$ is a prime power, then p^a cannot exceed*

$$6 \cdot 7^{M+2w(P)}.$$

Proof. If $0 < k < p^a$ and $p \nmid k$, then Lemma 2 shows that t_k is an S-unit and by Lemma 1 (ii) we infer that for every j the difference $c_{j,k} = t_{k+j}-t_j$ is associated with $t_k-t_0 = t_k$, hence is an S-unit. If $s = p^a-p$, then evidently for every k not divisible by p and satisfying $0 < k < p^a$ we have

$$t_s = t_{s-k}+c_{s-k,k}$$

and one sees that both summands on the right are S-units, because $p \nmid s-k$. Since all t_i's are distinct, the equation

$$t_s = u_1+u_2$$

has at least $\varphi(p^a) = p^{a-1}(p-1)$ solutions in S-units. It has been proved in [3] that this equation can have at most $3 \cdot 7^{M+2w(P)}$ solutions in a field of degree M, and hence, using Lemma 2, we arrive at

$$p^a \leqslant 2\varphi(p^a) \leqslant 6 \cdot 7^{M+2w(P)},$$

as asserted.

Now we can conclude the proof of the theorem. Let p be one of prime divisors of n and let $s = n/p$. Considering the s-th iterate P_s of the polynomial P we see that P_s has a p-cycle in K, namely

$$\{0, x_s, x_{2s}, \ldots, x_{(p-1)s}\},$$

and since p is prime, we obtain, in view of $S(P) = S(P_s)$,

$$p \leqslant t(P_s) = t(P).$$

Let now p^a be the highest power of p dividing n. Then, with $s = n/p^a$, the sequence

$$0, x_s, x_{2s}, \ldots, x_{(p^a-1)s}$$

is a p^a-cycle for the s-th iterate of P. It suffices now to apply Lemma 3 to obtain the first assertion of the theorem, and the asserted bound for $B(M, w)$ follows now from Lemmas 2 and 3.

The corollary results immediately, since in this case $R = Z_K$, $w(P) \leqslant M$ and $t(P) \leqslant 2^M$.

3. In certain cases one can get a more precise bound for $B(M)$ and in the case where the only units of K are 1 and -1 (i.e., either $K = Q$ or K is an imaginary quadratic field without non-real roots of unity) one gets the best possible value for it.

THEOREM II. *If K is either the field of rationals or a quadratic imaginary field, not generated by roots of unity, and P is a monic polynomial whose coefficients are integers of K, then P cannot have an n-cycle lying in K with $n > 2$. On the other hand, there exist such polynomials having 2-cycles in Q.*

Proof. Without restricting the generality we may assume that P has an n-cycle $\{0, x_1, \ldots, x_{n-1}\}$ with $n > 2$ consisting of integers of K and define the t_i's as in Lemma 1. Then by that lemma we obtain $t_i - t_{i-1} = 1$ or -1 for all i and, utilizing Corollary 2 and $n > 2$, $t_{n-1} = -1$. Now one has to get from $t_1 = 1$ to $t_{n-1} = -1$ by steps equal to 1 or -1 without passing through 0, but this is clearly impossible and the obtained contradiction shows that n cannot exceed 2.

The second assertion is a triviality. It suffices to look at the polynomial $P(x) = (x-1)^2$ which has a 2-cycle $\{0, 1\}$.

REFERENCES

[1] I. N. Baker, *The existence of fixpoints of entire functions*, Math. Z. 73 (1960), pp. 280–284.
[2] — *Fixpoints of polynomials and rational functions*, J. London Math. Soc. 39 (1964), pp. 615–622.
[3] J. H. Evertse, *On equations in S-units and the Thue–Mahler equation*, Invent. Math. 75 (1984), pp. 561–584.
[4] H. W. Lenstra, Jr., *Euclidean number fields of large degree*, ibidem 38 (1977), pp. 237–254.
[5] A. Leutbecher and G. Niklasch, *On cliques of exceptional units and Lenstra's construction of Euclidean fields*, preprint TUM-M8705, TU München 1987.
[6] W. Narkiewicz, *On polynomial transformations*, Acta Arith. 7 (1961–1962), pp. 241–249.

INSTITUTE OF MATHEMATICS
WROCŁAW UNIVERSITY

Reçu par la Rédaction le 28.9.1988