COLLOQUIUM MATHEMATICUM

VOL. LXVII 1994 FASC. 2

CYCLES OF POLYNOMIALS IN ALGEBRAICALLY CLOSED FIELDS OF POSITIVE CHARACTERISTIC

BY

T. PEZDA (WROCŁAW)

1. Let K be a field and f a polynomial with coefficients in K. A k-tuple $x_0, x_1, \dots, x_{k-1}$ of distinct elements of K is called a *cycle* of f if

$$f(x_i) = x_{i+1} \quad \text{for} \quad i = 0, 1, \dots, k-2 \quad \text{and} \quad f(x_{k-1}) = x_0.$$

It follows from the results of I. N. Baker ([1], [2]) that if K is an algebraically closed field of zero characteristic and f is a non-linear polynomial over K then f has in K cycles of all lengths with at most one exception. Moreover, the exceptional case may occur only when f is linearly conjugate to the polynomial $X^2 - X$. (Two polynomials f and g are called *linearly conjugate* if $f(aX + b) = ag(X) + b$ for some $a, b \in K$, $a \neq 0$.) In this exceptional case there are no cycles of length 2.

For $n = 1, 2, \dots$ denote by f_n the nth iterate of f and let $Z(n) = \{m : m \mid n,\ m < n\}$. Put also $\mathbb{N} = \{1, 2, \dots\}$, and let $\mathrm{CYCL}(f)$ denote the set of all lengths of cycles for $f \in K[X]$. Thus in algebraically closed fields of zero characteristic one has for non-linear polynomials f either $\mathrm{CYCL}(f) = \mathbb{N}$ or $\mathrm{CYCL}(f) = \mathbb{N} \setminus \{2\}$. Here we shall consider the same question in algebraically closed fields of prime characteristic. It has been established by G. Chassé [3] that in this case $\mathrm{CYCL}(f)$ is infinite for all non-linear f. We shall make this result more precise and describe this set up to finitely many elements. Since for linearly conjugate polynomials the sets of their cycle lengths coincide it is sufficient to consider f monic and vanishing at 0.

THEOREM. *Let K be an algebraically closed field of characteristic $p > 0$, let $f \in K[X]$ be monic of degree $d \geq 2$ and assume $f(0) = 0$.*

(i) *If $p \nmid d$ then* $\mathrm{CYCL}(f)$ *contains all positive integers with at most* 8 *exceptions. At most one of those exceptional integers can exceed* $\max\{4p, 12\}$.

(ii) *If $p \mid d$ and f is not of the form $\sum_{i \geq 0} \alpha_i X^{p^i}$ then* $\mathrm{CYCL}(f) = \mathbb{N}$ *or* $\mathrm{CYCL}(f) = \mathbb{N} \setminus \{2\}$.

1991 *Mathematics Subject Classification*: 11C08, 12E05.

Supported by KBN-grant No. 2-1037-91-01.

(iii) *If* $f(X)=\alpha X+\sum_{i>0}\alpha_i X^{p^i}$ *then*

(a) *if* α *is not a root of unity, then* $\mathrm{CYCL}(f)=\mathbb{N}$;

(b) *if* $\alpha=1$ *then* $\mathrm{CYCL}(f)=\mathbb{N}$ *for* $f(X)\neq X+X^d$, *and* $\mathrm{CYCL}(f)=\mathbb{N}\setminus\{p,p^2,\ldots\}$ *for* $f(X)=X+X^d$;

(c) *if* $\alpha\neq 1$ *is a root of unity of order* l *and* l *is not a prime power then* $\mathrm{CYCL}(f)=\mathbb{N}$;

(d) *if* α *is a root of unity of a prime power order* $l=q^r$ *with prime* $q\neq p$ *then* $\mathrm{CYCL}(f)=\mathbb{N}$ *unless*

$$f_{q^{r-1}(q-1)}(X)+f_{q^{r-1}(q-2)}(X)+\ldots+f_{q^{r-1}}(X)+X=X^{d^{q^{r-1}(q-1)}}.$$

In this exceptional case $\mathrm{CYCL}(f)=\mathbb{N}\setminus\{q^r,q^rp,q^rp^2,\ldots\}$.

2. Proof of (i). Assume that f has no cycles of lengths n and k, with $n>k$. We consider (following [1]) the rational function

$$T(X)=\frac{f_n(X)-X}{f_{n-k}(X)-X}=\frac{R(X)}{Q(X)},$$

where R, Q are relatively prime polynomials. Write $R=r^{p^M}$ and $Q=q^{p^M}$ with a maximal possible $M\geq 0$. Then obviously $(r/q)'\neq 0$.

Put $m=\deg Q$. Then

$$\deg R=d^n-d^{n-k}+m,\quad \deg r=p^{-M}(d^n-d^{n-k}+m),\quad \deg q=p^{-M}m. \tag{1}$$

If ξ is a zero of T then $f_n(\xi)-\xi=0$ and since f has no cycles of length n, we must have $f_l(\xi)-\xi=0$ for some $l\in Z(n)$, and this shows that the number of different zeros of T does not exceed $\sum_{l\in Z(n)}d^l$.

Similarly we estimate the number of different elements ξ satisfying $T(\xi)=1$. In this case $f_n(\xi)=f_{n-k}(\xi)$, hence $f_k(f_{n-k}(\xi))=f_{n-k}(\xi)$ and as f has no cycles of length k, we get $f_j(f_{n-k}(\xi))=f_{n-k}(\xi)$ for some $j\in Z(k)$. This shows that the number of solutions of $T(\xi)=1$ is bounded by $\sum_{j\in Z(k)}d^{n-k+j}$.

If ξ is a zero of r/q of order l then it is a zero of $(r/q)'$ of order $\geq l-1$ and the same applies to zeros of $r/q-1$.

This finally shows that the number of solutions of $r/q=0$ and $r/q=1$ counted with multiplicities is bounded by

$$\sum_{l\in Z(n)}d^l+\sum_{j\in Z(k)}d^{n-k+j}+\deg r+\deg q-1.$$

On the other hand, this number equals $2\deg r$, and thus we get

$$2\deg r\leq\sum_{l\in Z(n)}d^l+\sum_{j\in Z(k)}d^{n-k+j}+\deg r+\deg q-1.$$

Equalities (1) now lead to

$$d^n - d^{n-k} \le p^M\Big(\sum_{l\in Z(n)} d^l + \sum_{j\in Z(k)} d^{n-k+j} - 1\Big) \tag{2}$$

and

$$d^n \le p^M(2d^{n/2} + 2d^{n-k/2} - 3) + d^{n-k}. \tag{3}$$

This gives $d^n < 4p^M d^{n-k/2}$, hence

$$d^{k/2} < 4p^M, \tag{4}$$

and in view of $p^M \mid d^n - d^{n-k}$ one gets

$$p^M \mid d^k - 1. \tag{5}$$

If now $M = 0$ then (4) gives $k \le 3$ and so in this case at most three positive integers can lie outside $\mathrm{CYCL}(f)$ in view of $1 \in \mathrm{CYCL}(f)$.

In the case $M \ge 1$ denote by w_0 the order of d mod 4 if $p = 2$ and the order of d mod p otherwise.

If p is odd then (5) shows that $k = cw_0$ for some c. Now observe that the highest power of p dividing $d^k - 1$ does not exceed $c(d^{w_0} - 1)$. Indeed,

$$d^k - 1 = ((d^{w_0} - 1) + 1)^c - 1 = \sum_{r\ge 1} \binom{c}{r}(d^{w_0} - 1)^r,$$

and for $r \ge 2$ the number $\binom{c}{r}(d^{w_0} - 1)^r$ is divisible by a larger power of p than $c(d^{w_0} - 1)$.

If $p = 2$ then $d \ge 3$ so in case $M = 1$, (4) implies $k \le 3$ and in case $M \ge 1$ we find (as in the case of p odd) that the highest power of 2 dividing $d^k - 1$ does not exceed $c(d^{w_0} - 1)$, where w_0 is the smallest positive integer with $d^{w_0} \equiv 1 \bmod 4$.

From (3) and (5) we see that if $k \ge 4$ then

$$d^{cw_0/2} = d^{k/2} < 4c(d^{w_0} - 1),$$

which implies $d^{(c/2-1)w_0} < 4c$. Therefore, in case $w_0 \ge 3$ one has $c \le 4$ and so $k \in \{2, 3, w_0, 2w_0, 3w_0, 4w_0\}$, while in case $w_0 = 2$ we get $c \le 6$, hence $k \in \{2, 3, 4, 6, 8, 10, 12\}$.

Finally, if $w_0 = 1$ then $d \ge 4$, thus $4^{c/2-1} < 4c$ and $c \le 6$. Hence in this case $k \in \{2, 3, 4, 5, 6\}$.

We see that k can assume at most seven values and in view of $w_0 \le p$ they are bounded by $\max\{4p, 12\}$. This implies (i).

3. Now we deal with the case $p \mid d$.

LEMMA 1. *If n is not the length of a cycle for f then $f_n'(X) = 1$.*

P r o o f. Let $f(X)=\sum_{r\ge 1} b_r X^r$, assume that there exists $1<t<d$ with $p\nmid t$ and $b_t\neq 0$, and let a be the smallest such t. Put

$$f_j(X)=\sum_{r\ge 1} b_r^{(j)} X^r.$$

A simple recurrence shows that the highest r with $p\nmid r$ and $b_r^{(j)}\neq 0$ equals $(a-1)(1+d+\ldots+d^{j-1})+1$. From the formula

$$d^n\le \#\{\xi : f_n(\xi)=\xi\}+\deg((f_n(X)-X)')$$

we get

$$d^n\le \sum_{k\in Z(n)} d^k+(a-1)(1+d+\ldots+d^{n-1}),$$

but in view of $a\le d-1$ we have $1+1+d+\ldots+d^{n-1}\le\sum_{k\in Z(n)} d^k$, which leads to a contradiction.

If there is no t as above and our lemma is false then $f_n'-1$ is a non-zero constant and we get $d^n\le\sum_{k\in Z(n)} d^k$, which is clearly impossible. ∎

4. Proof of (ii). Assume f has no cycles of length n. So $(f_n(X)-X)'=0$ by Lemma 1 and hence $f(X)=\alpha X+\sum_r b_r X^{pr}$, with $\alpha^n=1$.

By assumption there exists $m\ge 1$ such that f contains terms of the form bX^{up^m} with u not divisible by p and exceeding 1. Let m be the smallest such integer and choose u to be the largest possible. So $f(X)=\alpha X+\sum_{0<i\le m} c_i X^{p^i}+\sum_{p\nmid k,k>1} b_k X^{kp^m}+\sum_r d_r X^{rp^{m+1}}$. By induction we get

$$f_n(X)=\alpha^n X+\sum_{0<i\le m} C_i X^{p^i}+\sum_{p\nmid k,k>1} B_k X^{kp^m}+\sum_r D_r X^{rp^{m+1}}$$

where the highest power appearing in the second sum equals $X^{(1+(u-1)d^{n-1})p^m}$. Write $f_n(X)-X=(\psi(X))^{p^M}$ with non-zero ψ' and consider two cases:

(α) $M<m$. Then ψ' is a non-zero constant and this gives $d^n\le p^M\times\sum_{l\in Z(n)} d^l$. Thus $d^n<2dd^{n/2}$, leading to $n\le 3$ and $d^n<d\cdot d$, a contradiction.

(β) $M=m$. Then $d^n\le p^m(\sum_{l\in Z(n)} d^l+(u-1)d^{n-1})$ and

$$d^{n-1}u\le\sum_{l\in Z(n)} d^l+(u-1)d^{n-1}.$$

So $d^{n-1}\le\sum_{l\in Z(n)} d^l$ and $n=2$, $d=p^m u$ follows. ∎

5. Proof of (iii). Assume that f is of the form

$$\alpha X + \sum_{i\ge 1} \alpha_i X^{p^i} \tag{6}$$

and has no cycle of length n.

LEMMA 2. *For $s = 1, 2, \ldots$ one has, with suitable $\alpha^{(s)}$, $\alpha_i^{(s)}$,*

$$f_s(X) = \alpha^{(s)} X + \sum_{i\ge 1} \alpha_i^{(s)} X^{p^i},$$

all roots of f_s have the same multiplicity and f_s defines an $\mathbb{F}_p$-linear map $K \to K$.

Proof. Easy induction. ∎

Let q be a prime and denote by $A(X)$ the divisor of $f_q(X) - X$ which is prime to $f(X) - X$ and has a maximal degree. Write $B(X) = (f_q(X) - X)/A(X)$. Since $f(X) - X$ is of the form (6), Lemma 2 implies that all zeros of $f(X) - X$ have the same multiplicity. Since the same applies to $f_q(X) - X$ we get $\deg B(X) = d^q c(f, q)$, where $c(f, q) = c_1/c_q$, c_i denoting the number of different zeros of $f_i(X) - X$.

LEMMA 3. *Let q be a prime and let f be a polynomial of the form* (6).

(i) *If $\alpha = 1$, then*

$$c(f, q) = \begin{cases} 1/d^{q-1} & \text{if } q \ne p, \\ (r/d)^{p-1} & \text{if } q = p, \end{cases}$$

where $r = r(f)$ is the smallest degree of a monomial occurring in $f(X) - X$ and $d = d(f)$ is the degree of f.

(ii) *If $\alpha \ne 1$ and $q \ne p$ then either $c(f, q) = 1$ or $c(f, q) \le p^{-\lambda}$, where λ denotes the order of $p \bmod q$.*

Proof. (i) Write $f(X) = X + aX^r + \ldots = X + h(X)$ with $a \ne 0$. Using Lemma 2 we deduce that all roots of h have multiplicity r, thus $c_1 = d/r$. Similarly one gets

$$c_q = \begin{cases} d^q/r & \text{if } q \ne p, \\ (d/r)^p & \text{if } q = p, \end{cases}$$

leading to the assertion.

(ii) In this case we have $q \ne p$. If we put $h(X) = f(X) - X$ then

$$f_q(X) - X = \binom{q}{1} h(X) + \binom{q}{2} h_2(X) + \ldots + \binom{q}{q} h_q(X).$$

Let $H = \{x : h(x) = 0\}$ and $L = \{x : f_q(x) = x\}$. Then H is a subspace of L treated as linear spaces over $\mathbb{F}_p$. Notice that $h(H) \subset H$ and $h(L) \subset L$.

Let $x \in L$. In this case $h(x), h_2(x), \ldots \in L$. Since L is finite, there exist $m \in \mathbb{N}$ and $\beta_1, \ldots, \beta_m \in \mathbb{F}_p$ with $\beta_m = 1$ such that $\beta_1 h(x) + \beta_2 h_2(x) +$

$\ldots + \beta_m h_m(x) = 0$. Choose m as small as possible and define $g_0(X) = g_0(x, X) = \beta_1 X + \ldots + \beta_m X^m$.

Consider the linear map $T : \mathbb{F}_p[X] \to \mathbb{F}_p[X]$ defined for $g(X) = \beta_0 + \beta_1 X + \ldots + \beta_w X^w$ by $T(g)(X) = \beta_0 X + \beta_1 h(X) + \ldots + \beta_w h_w(X)$. Then $T(g_1 \cdot g_2) = T(g_1) \circ T(g_2)$ and $T(g)(0) = 0$.

Put $Q(X) = \binom{q}{1} X + \ldots + \binom{q}{q} X^q$. For our x we have $T(Q)(x) = 0$ and $T(g_0)(x) = 0$. So $T(G_1 \cdot Q + G_2 \cdot g_0)(x) = 0$ for every $G_1, G_2 \in \mathbb{F}_p[X]$. Hence $T((Q, g_0))(x) = 0$ and using $(Q, g_0)(0) = 0$ and the minimality of m we arrive at $g_0 \,|\, Q$.

If $H = L$ then $c(f, q) = 1$, so consider the case $H \neq L$. Let $x \in L \setminus H$. Notice that $g_0(x, X) \neq X^m$ as $q \neq p$ and $h(x) \neq 0$. So there exists a polynomial G irreducible over $\mathbb{F}_p$ with $G \,|\, g_0$ and $G \neq cX$. Let $\deg G = s \leq m - 1$. Then $G \,|\, X^{p^s} - X$. This shows that $Q(X)$ and $X^{p^s} - X$ have a common divisor different from X, and this means that

$$((1 + X)^q - 1, X^{p^s} - X) \neq X,$$

thus $(X^q - 1, X^{p^s} - 1) \neq X - 1$ and $q \,|\, p^s - 1$ follows. Further, no non-zero linear combination of x, $h(x), \ldots, h_{m-2}(x)$ lies in H, and this shows that either $c(f, q) = 1$ or $c(f, q) \leq p^{-(m-1)} \leq p^{-s} \leq p^{-\lambda}$. ∎

Corollary. *If $c(f, q) = 1$, then either $\alpha \neq 1$ and $q \neq p$, or $\alpha = 1$, $q = p$ and $f(X) = X + X^d$.* ∎

6. We need two lemmas:

Lemma 4. *Assume that n is not the length of a cycle for $f(X) = \alpha X + \sum_{i>0} \alpha_i X^{p^i}$. Then $c(f_{n/q}, q) = 1$ for some prime $q \,|\, n$.*

Proof. Assume that $c(f_{n/q}, q) < 1$ for all primes q dividing n. In view of Lemma 1 we have $\alpha^n = 1$ and Lemma 3 shows that the following must hold:

1) If $p \,|\, n$ then $c(f_{n/p}, p) = (r/d)^{p-1} \leq 1/p^{p-1}$;

2) If $q \,|\, n$, $q \neq p$ and $\alpha^{n/q} = 1$ then $c(f_{n/q}, q) = 1/d^{n(q-1)/q} \leq 1/p^{q-1}$;

3) If $q \,|\, n$ and $\alpha^{n/q} \neq 1$, then $c(f_{n/q}, q) \leq 1/p^s$ where s satisfies $q \,|\, p^s - 1$.

Now we show that our assumption implies

$$\sum := \sum_{\substack{q \,|\, n \\ q \text{ prime}}} c(f_{n/q}, q) < 1.$$

This will give the desired contradiction, since every zero of $f_n(X) - X$ is a zero of $f_{n/q}(X) - X$ for some prime $q \,|\, n$ (otherwise f would have a cycle of length n) and thus $\sum \geq 1$.

Notice that

$$\sum \le \frac{1}{p^{p-1}} + \sum_{s\ge 1} \frac{t(s)}{p^s} = \sum(p)$$

where $t(s)$ the number of primes q for which p has order $s \mod q$. Obviously $t(s) \le s \log_2 p$ and thus for $p \ge 5$ in view of $\log_2 p < p/2$ we get

$$\sum(p) < 0.01 + \log_2 p \cdot \sum_{s\ge 1} \frac{s}{p^s} = 0.01 + \frac{p}{(p-1)^2} \log_2 p < 0.8.$$

For $p = 3$ one has $t(1) = 1$ and $t(2) = 0$, hence

$$\sum(3) \le \frac{1}{9} + \frac{1}{3} + \frac{\log 3}{\log 2} \sum_{n\ge 3} \frac{n}{3^n} < 0.76,$$

and finally

$$\sum(2) < \sum_{k=1}^{5} \frac{1}{2^k} + \sum_{k=7}^{10} \frac{1}{2^k} + \frac{2}{2048} + \frac{1}{4096} + \sum_{n\ge 13} \frac{n}{2^n} \le 0.9881. \ \blacksquare$$

LEMMA 5. *If d is a power of p, then the polynomial $f(X) = X + X^d$ has no cycles of length p^k for $k = 1, 2, \ldots$ but does have cycles of all other lengths.*

P r o o f. It is easy to check that f has no cycles of lengths $p, p^2, \ldots$ If now $1 < M \ne p^\alpha$ and f has no cycle of length M then the last lemma shows that $c(f_{M/r}, r) = 1$ for some prime divisor r of M. Since in our case $\alpha = 1$, we may invoke the Corollary to Lemma 3 to get $r = p$ and $f_m(X) = X + X^{d^m}$ with $m = M/p$. As m is not a power of p there is $1 < j < m$ with $p \nmid \binom{m}{j}$, but this implies $f_m(X) = X + \binom{m}{1} X^d + \ldots + X^{d^m} \ne X + X^{d^m}$, a contradiction. ∎

7. In view of Lemma 4 there exists a prime divisor q of n with $c(f_{n/q}, q) = 1$.

First, suppose $q = p$. Then the Corollary to Lemma 3 gives $f_{n/q}(X) = X + X^{d^{n/q}}$, showing that both $f_{n/q}(X) - X$ and $f(X) - X$ have exactly one root, which can happen only for $f(X) = X + X^d$, and the assertion follows from Lemma 5.

LEMMA 6. *If f is as in case* (iii) *of the Theorem, q is a prime and $\alpha^{n/q} \ne 1$ then the following conditions are equivalent*:

(a) $c(f_{n/q}, q) = 1$,

(b) $f_n(X) - X = (f_{n/q}(X) - X)^{d^{n(q-1)/q}}$,

(c) $f_n(X) - X = \beta X^{d^{n(q-1)/q}} +$ *higher powers of* X.

P r o o f. (a)⇒(b). If $c(f_{n/q},q)=1$ then every root of $f_n(X)-X$ is a root of $f_{n/q}(X)-X$. The last polynomial has all its roots distinct, f is monic, and all roots of $f_n(X)-X$ have the same multiplicity by Lemma 2. By comparing degrees we arrive at

$$f_n(X)-X=(f_{n/q}(X)-X)^{d^{n(q-1)/q}}.$$

(b)⇒(c). Follows immediately from $\alpha^{n/q}-1\neq 0$.

(c)⇒(a). The multiplicity of every root of $f_n(X)-X$ is $d^{n(q-1)/q}$, since that is the multiplicity of 0. So one has

$$(f_{n/q}(X)-X)^{d^{n(q-1)/q}}\mid f_n(X)-X$$

and it suffices to compare the degrees. ∎

Let l be the smallest positive integer such that $\alpha^l=1$. Then $n=mp^\beta l$ where $p\nmid m$ since $\alpha^n=1$.

Write $f_l(X)-X=\beta_1X^A+\ldots$ ($\beta_1\neq 0$) where we omitted, as we shall also do in the sequel, terms containing higher powers of X. Then with suitable non-zero β_2, β_3 we get

$$f_{lm}(X)-X=\beta_2X^A+\ldots\quad\text{and}\quad f_n(X)-X=\beta_3X^{A^{p^\beta}}+\ldots$$

Since the degree of $f_l(X)-X$ equals d^l we get $A\leq d^l$. Note that in case $A=d^l$ we would have $f(X)=X+X^d$, and since all possible cycle-lengths of this polynomial have been determined in Lemma 5, we can assume $A<d^l$.

In view of $\alpha^{n/q}-1\neq 0$ using Lemma 6 one obtains

$$A^{p^\beta}=d^{n(q-1)/q}$$

and $A=d^{lm(q-1)/q}$ follows. From $A<d^l$ one gets $m(q-1)/q<1$ and so $m=1$. Thus $n=lp^\beta$ and $A=d^{l(q-1)/q}$. Finally, using $\alpha^{l/q}\neq 1$ we get $c(f_{l/q},q)=1$ by Lemma 6 and this shows that there are no cycles of length l.

Now we show that if there are no cycles of length l then there are none of lengths $l,lp,lp^2,\ldots$ Assume, therefore, that there are no cycles of length l. Then for some prime $q\neq p$ dividing l we have $f_l(X)-X=\beta_1X^{d^{l(q-1)/q}}+\ldots$, and

$$f_{lp^\beta}(X)-X=\beta_4X^{lp^\beta(q-1)/q}+\ldots$$

Now in view of $\alpha^{lp^\beta/q}\neq 1$ and using Lemma 6 one obtains $c(f_{lp^\beta/q},q)=1$, showing that there are no cycles of length lp^β for any positive integers β.

Finally, we obtained the following assertion:

(a) if there are no cycles of length l then $\mathrm{CYCL}(f)=\mathbb{N}\setminus\{l,lp,lp^2,\ldots\}$;

(b) if there is a cycle of length l then $\mathrm{CYCL}(f)=\mathbb{N}$.

It suffices hence to consider, for some $q\mid l$, $q\neq p$, the equality

$$f_l(X)-X=(f_{l/q}(X)-X)^{d^{l(q-1)/q}}.$$

Let $f_{l/q} = G$, $d^{l/q} = D$, so that $G_q(X) - X = (G(X) - X)^{D^{q-1}}$. This is equivalent to

$$(G_{q-1}(X) + G_{q-2}(X) + \ldots + G(X) + X) \circ (G(X) - X) = (G(X) - X)^{D^{q-1}}$$

and

$$G_{q-1}(X) + G_{q-2}(X) + \ldots + G(X) + X = X^{D^{q-1}}.$$

Now we show that l must be a power of q. Suppose that there exists a prime divisor $k \neq q$ of l. Then every root of $f_{l/k}(X) - X$ would be a root of $f_l(X) - X$, $f_{l/q}(X) - X$, and $f_\delta(X) - X$ where $\delta = (l/k, l/q)$. But $\delta < l/k$ and this leads to a contradiction as $f_{l/k}(X) - X$ has all its roots distinct. ∎

EXAMPLE. If $d \equiv 3 \pmod 4$ and $\alpha^2 = -1$ then $f(X) = \alpha X + X^d$, where d is a power of p, has no cycles of lengths $\{4, 4p, \ldots\}$.

REFERENCES

[1] I. N. Baker, *The existence of fixpoints of entire functions*, Math. Z. 73 (1960), 280–284.

[2] —, *Fixpoints of polynomials and rational functions*, J. London Math. Soc. 39 (1964), 615–622.

[3] G. Chassé, *Combinatorial cycles of a polynomial map over a commutative field*, Discrete Math. 61 (1986), 21–26.

INSTITUTE OF MATHEMATICS
WROCŁAW UNIVERSITY
PL. GRUNWALDZKI 2/4
50-384 WROCŁAW, POLAND

Reçu par la Rédaction le 8.9.1993