CYCLES OF POLYNOMIALS IN ALGEBRAICALLY CLOSED
FIELDS OF POSITIVE CHARACTERISTIC (II)

by

T. PEZDA (WROCLAW)

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

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

The number $k$ is called the length of that cycle. Two polynomials $f$ and $g$ are called linearly conjugate if $f(aX + b) = ag(X) + b$ for some $a, b \in K$ with $a \neq 0$. For linearly conjugate polynomials the sets of their cycle lengths coincide.

For $n = 1, 2, \ldots$ denote by $f_n$ the $n$th iterate of $f$ and let $Z(n)$ be the set of all maximal proper divisors of $n$, i.e. $Z(n) = \{m : mq = n \text{ for some prime } q\}$. Put also $\mathbb{N} = \{1, 2, \ldots\}$, and let CYCL($f$) denote the set of all lengths of cycles for $f \in K[X]$. Define also $E(f) = \mathbb{N} \setminus \text{CYCL}(f)$.

In [3] the following theorem has been proved:

**Theorem 0.** 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 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 CYCL($f$) = $\mathbb{N}$ or CYCL($f$) = $\mathbb{N} \setminus \{2\}$.

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

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

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

1991 Mathematics Subject Classification: 11C08, 12E05.

Research supported by the KBN-grant No. 2 P03A 036 08.

[23]
(d) if \( \alpha \) is a root of unity of a prime power order \( l = q^r \) with prime \( q \neq p \) then \( \text{CYCL}(f) = \mathbb{N} \) unless
\[
f_{q^{-1}(q-1)}(X)+f_{q^{-1}(q-2)}(X)+\ldots+f_{q^{-1}}(X)+X = X^{d^{r-1}(q-1)}.
\]
In this exceptional case \( \text{CYCL}(f) = \mathbb{N} \setminus \{q^r, q^rp, q^rp^2, \ldots\} \).

In this paper we reduce the number of exceptions in part (i) of this theorem, namely we prove the following:

**Theorem 1.** Let \( K \) be an algebraically closed field of characteristic \( p > 0 \) and let \( f \in K[X] \) be of degree \( d \geq 2 \) with \( p \nmid d \). If \( p = 3 \) and \( f \) is linearly conjugate to \( X^2 \) then \( E(f) = \{2, 6\} \), and in all other cases \( \#E(f) \leq 1 \).

2. We begin with some lemmas which will be later used in the proof of Theorem 1.

In this paper \( K \) always denotes an algebraically closed field of positive characteristic \( p > 0 \).

**Lemma 1.** Let \( f \in K[X] \) be of degree \( d \geq 2 \) with \( p \nmid d \). Then \( f(X) \) is linearly conjugate to a polynomial of the form \( X^d + a_dX^{d-2} + \ldots + a_0 \).

**Proof.** Let \( f(X) = b_dX^d + b_{d-1}X^{d-1} + \ldots + b_0 \). For every \( \alpha, \beta \in K \) with \( \alpha \neq 0 \) the polynomial \( g(X) = \frac{1}{\alpha}f(\alpha X + \beta) - \beta \) is linearly conjugate to \( f \), and since a short computation gives \( g(X) = b_d\alpha^{d-1}X^d + (b_{d-1}\alpha^{d-2} + db_d\alpha^{d-2})X^{d-1} + \ldots \), the \( g(X) \) will have the needed form provided \( \alpha, \beta \) satisfy the following system of equations:
\[
b_d\alpha^{d-1} = 1, \quad b_{d-1}\alpha^{d-2} + db_d\alpha^{d-2}\beta = 0.
\]
As \( K \) is algebraically closed and \( d \geq 2 \) and \( d \neq 0 \) in \( K \), this system has a solution.

For a rational function \( \phi \in K(X) \) write \( \phi = [\phi] + \{\phi\} \), where \( [\phi] \) is a polynomial and \( \{\phi\} \) is a rational function for which the degree of the numerator is less than the degree of the denominator. Such choice of \( [\phi], \{\phi\} \) is unique.

For \( M = 1, 2, \ldots \) let also \( L_M = K(X^{p^M}) \).

**Lemma 2.** (i) A polynomial \( \phi \) lies in \( L_M \) if and only if \( \phi(X) = \sum a_jX^{b_j} \) with \( p^M | b_j \).
(ii) \( L_M \) coincides with the set of all \( p^M \)-th powers in \( K(X) \).
(iii) If \( \phi \in L_M \) and \( \phi \neq 0 \) then \( 1/\phi \in L_M \).
(iv) \( \phi \in L_M \) if and only if \( [\phi], \{\phi\} \in L_M \).

**Proof.** Every element of \( K \) is a \( p^M \)-th power, so \( \varphi : f \mapsto f^{p^M} \) is an isomorphism of the field \( K(X) \) onto its subfield \( K(X^{p^M}) \). Of course, the formula \( \varphi([f] + \{f\}) = [\varphi(f)] + \{\varphi(f)\} \) holds.
Lemma 3. (i) Let $j > j'$; assume that $j = k j' + l$, where $0 < l < j'$. Assume also that $f(X)$ is a nonlinear polynomial. Then

$$f_j(X) - X \in L_M \quad \Rightarrow \quad f_{j'}(X) - X \in L_M.$$  

(ii) Let $j > j'$. Denote by $u, v$ the last two non-zero elements resulting from the application of the Euclidean algorithm to the pair $(j, j')$. Then

$$f_j(X) - X \in L_M \quad \Rightarrow \quad f_u(X) - X \in L_M.$$  

Proof. (i) We have

$$f_j(X) - X = \left( \sum_{i=0}^{k-1} f_{j+i+1}(X) - f_{j'+i+1}(X) \right) + f_l(X) - X.$$  

Since $G(X) - H(X) | F(G(X)) - F(H(X))$ for all polynomials $F, G, H$, we obtain

$$\left\{ \frac{f_j(X) - X}{f_{j'}(X) - X} \right\} = \frac{f_l(X) - X}{f_{j'}(X) - X}.$$  

It remains to apply Lemma 2(i), (ii).

(ii) This follows by repeated application of (i). \[ \square \]

Lemma 4. Let $f(X) = X^d + a_r X^r + \ldots$, where $r \leq d - 2$, $a_r \neq 0$, $p \nmid d$ and $d \geq 2$. Then $f_m(X) = X^{d_m} + a_d d_m^{-1} X^{d_m-d_r} + \ldots$

Proof. Easy induction. \[ \square \]

Lemma 5. Let $F(X) = X^D + a_R X^R + \ldots$ where $R \leq D - 2$, $a_R \neq 0$, $p \nmid D$, $D \geq 2$ and $T \geq 2$. Assume also that

$$F_T(X) - X \in L_M.$$  

Then

(i) $p^M \mid D - 1$, hence $D \geq 3$ for $M > 0$.

(ii) If $R \neq 0, 1$ then $p^M \mid D - R$.

Proof. It suffices to consider $M > 0$.

(i) The function $(F_T(X) - X)/(F(X) - X)$ is a polynomial. Put

$$A_3(X) = \frac{F_{T-2}(F(X)) - X}{F(X) - X}.$$  

Observe that

$$F_{T}(X) - X = F_{T-1}(F(X)) - F_{T-1}(X) + A_3(X)$$  \[ (1) \]
and

(2) \[ \deg A_4 = D^{T-1} - D. \]

Lemma 4 gives \( F_{T-1}(X) = X^{D^{T-1}} + a_R D^{T-2} X^{D^{T-1} - D + R} + \ldots \), so we can write

\[ \frac{F_{T-1}(F(X)) - F_{T-1}(X)}{F(X) - X} = A_1(X) + A_2(X), \]

where

\[
A_1(X) = F(X)^{D^{T-1} - 1} + F(X)^{D^{T-1} - 2} X + F(X)^{D^{T-1} - 3} X^2 + \ldots + X^{D^{T-1} - 1},
\]

\[
A_2(X) = a_R D^{T-2} (F(X)^{D^{T-1} - D + R - 1} + \ldots + X^{D^{T-1} - D + R - 1}) + \ldots
\]

As the polynomial \( (F_T(X) - X)/(F(X) - X) \) is of degree \( D^{T} - D \), Lemma 2(i) immediately gives \( p^M | D^T - D \), and in view of \( p | D \) we get

\[ p^M | D^{T-1} - 1. \]

This implies \( F(X)^{D^{T-1} - 1} \in L_M \). Since \( L_M \) is a field, we have

(4) \[ C_1(X) = \frac{F_T(X) - X}{F(X) - X} = F(X)^{D^{T-1} - 1} \]

\[ = A_2(X) + A_3(X) + F(X)^{D^{T-1} - 2} X + F(X)^{D^{T-1} - 3} X^2 + \ldots + X^{D^{T-1} - 1} \in L_M. \]

The equality

(5) \[ \deg A_2(X) = D(D^{T-1} - D + R - 1) \]

and

(6) \[ D(D^{T-1} - 2) + 1 > \max\{D(D^{T-1} - D + R - 1), D^{T-1} - D\} \]

give

Hence Lemma 2(ii) and the formulas (4) and (6) give \( p^M | D(D^{T-1} - 2) + 1 \), and using (3) we get the assertion.

(ii) As \( X^{D(D^{T-1} - 2)+1} \in L_M \), using (4) we obtain

(7) \[ C_2(X) = C_1(X) - X^{D(D^{T-1} - 2)+1} \in L_M. \]

Let us consider more carefully the term

\[
F(X)^{D^{T-1} - 2} X = (X^D + a_R X^R + \ldots)^{D^{T-1} - 2} X
\]

appearing in (4).

As \( R \neq 0,1, R \leq D - 2 \) and \( D \geq 3 \) we have the inequalities

(8) \[ D(D^{T-1} - 3) + R + 1 > D(D^{T-1} - 3) + 2, \]

(9) \[ D(D^{T-1} - 3) + R + 1 > D(D^{T-1} - D + R - 1), \]
Lemma 5 for which in view of (i) gives the assertion (ii).

(10) \[ D(D^{T-1} - 3) + R + 1 > D(D^{T-2} - 1). \]

Using \( D^{T-1} - 2 = -1 \neq 0 \) in \( K \), we get \( \deg C_2(X) = D(D^{T-1} - 3) + R + 1 \).

Applying Lemma 2(i) and (7) we obtain

(11) \[ p^M | D(D^{T-1} - 3) + R + 1, \]

which in view of (i) gives the assertion (ii).

**Lemma 6.** Let \( f(X) = X^d + a_r X^r + \ldots \), where \( p \nmid d, d \geq 2, a_r \neq 0, r \leq d - 2, v | u \) and \( v < u \). Then

\[ \frac{f_v(X) - X}{f_c(X) - X} \in L_M \Rightarrow p^M \leq d - 1. \]

**Proof.** Lemma 4 gives \( f_v(X) = X^{d^v} + a_r d^{v-1} X^{d^v - d + r} + \ldots \). We use Lemma 5 for \( F(X) = f_v(X), T = u/v, D = d^v \) and \( R = d^v - d + r \). Its assumptions are satisfied as \( D - R = d^v - (d^v - d + r) = d - r \geq 2 \), hence we obtain

1° If \( d^v - d + r \neq 0, 1 \) then \( p^M | d^v - (d^v - d + r) = d - r \).

2° If \( d^v - d + r \in \{0, 1\} \) then \( v = 1 \) and \( p^M | d - 1 \) (as in this case \( D = d \)).

Hence \( p^M \leq \max\{d - r, d - 1\} \). In view of \( p \nmid d \) the lemma follows.

**3. Proof of Theorem 1.** Owing to Lemma 1 it suffices to consider two kinds of polynomials, namely:

1) \( f(X) = X^d + a_r X^r + \ldots \), where \( a_r \neq 0, r \leq d - 2, p \nmid d \) and \( d \geq 2 \), and
2) \( f(X) = X^d \) for \( p \nmid d \) and \( d \geq 2 \).

**3.1.** Let \( f(X) = X^d + a_r X^r + \ldots \), where \( a_r \neq 0, r \leq d - 2, p \nmid d \) and \( d \geq 2 \).

Suppose that \( \#E(f) \geq 2 \) and assume that \( f(X) \) has no cycles of lengths \( n \) and \( k \), \( n > k \). Notice that \( k > 1 \) as \( K \) is algebraically closed. In [3] the formula

\[ d^n - d^{n-k} \leq p^M \left( \sum_{l \in Z(n)} d^l + \sum_{j \in Z(k)} d^{n-k+j} - 1 \right) \]

has been established, where \( M \geq 0 \) is the largest number satisfying

\[ \frac{f_n(X) - X}{f_{n-k}(X) - X} \in L_M. \]

Lemmas 3 and 6 give \( p^M \leq d - 1 \). Hence

(12) \[ d^n - d^{n-k} \leq (d - 1) \left( \sum_{l \in Z(n)} d^l + \sum_{j \in Z(k)} d^{n-k+j} - 1 \right). \]

We are going to show that this inequality leads to a contradiction.
Let $k'$ and $n'$ be the largest elements of $Z(k)$ and $Z(n)$ respectively. As
\[
\sum_{l \in Z(n)} d^l < 1 + d + \ldots + d^{n'} < \frac{d^{n'}}{d-1}
\]
and
\[
\sum_{j \in Z(k)} d^{n-k+j} < \frac{d}{d-1} d^{n-k+k'},
\]
(12) leads to
\[
d^n < d^{n-k} + d^{n'+1} + d^{n-k+k'+1}.
\]
In view of the last inequality we have three possibilities:
1. $n - n' = 1$,
2. $n - n' - 1 = 1$ and $k - k' - 1 = 1$,
3. $k - k' = 1$.

The equality $n - n' = 1$ gives $n = 2$, contradicting $n > k > 1$.

The equations $n - n' - 1 = 1$ and $k - k' - 1 = 1$ give $n = 4$ and $k = 3$.

But for these particular values (12) gives $d^4 - d \leq (d-1)(d^2 + d^2 - 1)$, which
is clearly impossible.

The equality $k - k' = 1$ gives $k = 2$. In this case, (12) after a simple transformation leads to
\[
d^{n-2} \leq \sum_{l \in Z(n)} d^l - 1.
\]
But the sum occurring here is less than $d^{n'+1}$, and we have $n - 2 < n' + 1$.
Hence $n \in \{3, 4\}$. It is easy to check that for these values of $n$, (13) does not hold. So in our case $\#E(f) \leq 1$.

3.2. Let $f(X) = X^d$, where $p \nmid d$ and $d \geq 2$.

**Lemma 7.** Assume that the polynomial $f(X) = X^d$ has no cycle of length $j$. Let $q$ be a prime divisor of $d^j - 1$. Then either $q = p$ or $q \mid d^{j'} - 1$ for some $j' < j$.

**Proof.** We may assume that $q \neq p$. Let $\xi$ be a primitive $q\text{th}$ root of unity. So $\xi^d = \xi$ and $f_j(\xi) = \xi$ follows. But $f$ has no cycles of length $j$.

Thus there is $j' < j$ such that $f_{j'}(\xi) = \xi$, which means $\xi^{d^{j'}} = \xi$ and $\xi^{d^{j'-1}} = 1$ (as $\xi \neq 0$).

Now let us recall that a prime divisor of $a^n - b^n$ is called *primitive* if it does not divide $a^k - b^k$ for any positive $k < n$.

We have the following result of A. S. Bang [1] (for the proof see e.g. [2]).
THEOREM. If \( d > 1 \) then for every \( j \) there is at least one prime primitive divisor of \( d^j - 1 \) except in the following cases:

- (a) \( j = 1, d = 2 \),
- (b) \( j = 2, d = 2^k - 1 \),
- (c) \( j = 6, d = 2 \).

Suppose that \( f(X) \) has no cycles of lengths \( n, k \) with \( n > k \).

If both \( d^n - 1 \) and \( d^k - 1 \) have prime primitive divisors \( q_1, q_2 \) respectively then Lemma 7 gives \( q_1 = q_2 = p \), and we obtain a contradiction as \( q_2 \mid d^k - 1 \) and \( q_1 \) is a prime primitive divisor of \( d^n - 1 \).

Hence one of the numbers \( d^n - 1, d^k - 1 \) has no prime primitive divisor.

By Bang’s theorem we obtain the following possibilities:

1st possibility: \((d, k) = (2^t - 1, 2)\);
2nd possibility: \((d, k) = (2, 6)\);
3rd possibility: \((d, n) = (2, 6)\).

LEMMA 8. (i) If for \( d = 2^t - 1 \) the polynomial \( X^d \) has no cycle of length 2 then \( p \mid d^2 - 1 \).

(ii) If \( X^2 \) has no cycles of length 6 then \( p = 3 \).

Proof. (i) Every root of \( X^{d^2} - X \) is a root of \( X^d - X \). In particular, every root of \( X^{d^2 - 1} - 1 \) is a root of \( X^{d - 1} - 1 \). This in turn implies that \( X^{d^2 - 1} - 1 \) has multiple roots. Hence the polynomial \( X^{d^2 - 1} - 1 \) and its derivative \((d^2 - 1)X^{d^2 - 2}\) have a common root. So \( d^2 - 1 = 0 \) in \( K \) and \( p \mid (d^2 - 1) \) follows.

(ii) Every root of \( X^{2^6} - X \) is a root of \( X^{2^3} - X \) or of \( X^{2^2} - X \). In particular, every root of \( X^{63} - 1 \) is a root of \( X^7 - 1 \) or of \( X^3 - 1 \). This in turn implies that \( X^{63} - 1 \) has multiple roots. In the same manner as in the proof of (i) we get \( p \mid 63 \), i.e. \( p \in \{3, 7\} \).

If \( p = 7 \) then \( X^7 - 1 = (X - 1)^7 \). The polynomial \( X^9 - 1 \) divides \( X^{63} - 1 \), hence each of its roots is a root of \( X^3 - 1 \), thus it must have multiple roots, so \( 7 = p \mid 9 \), a contradiction.

Hence \( p = 3 \).

Let us finally consider the three possibilities mentioned above:

1st possibility, \((d, k) = (2^t - 1, 2)\). Bang’s theorem and Lemma 7 show that \( p \) is a primitive prime divisor of \( d^n - 1 \), so \( p \nmid d^2 - 1 \), contrary to Lemma 8(i).

2nd possibility, \((d, k) = (2, 6)\). As \( k = 6 \), Lemma 8(ii) gives \( p = 3 \). Since \( d = 2 \) and \( n > 6 \), Bang’s theorem and Lemma 7 show that \( 3 \) is a primitive prime divisor of \( 2^n - 1 \), but this is not possible in view of \( 3 \mid 2^6 - 1 \).

3rd possibility, \((d, n) = (2, 6)\). Also Lemma 8(ii) gives \( p = 3 \). Since \( X^{2^6} - X = X(X^7 - 1)^9 \) and \( X^{2^2} - X = X(X - 1)^3 \) the polynomial \( X^2 \) has
no cycles of lengths 2 and 6. As we obtained \( n = 6 \) for every \( n, k \in E(X^2) \) with \( n > k \), in this case \( \#E(f) = 2 \).

The proof of Theorem 1 is now complete. ■

4. Some examples

a) \( X^{p^n - 1} \) has no cycles of length 2.

b) \( X^2 \) has no cycles of length \( q \) if \( p = 2^q - 1 \) is a Mersenne prime.

c) \( X^2 - X \) has no cycles of length 2 in any characteristic.

REFERENCES


Institute of Mathematics
Wrocław University
Pl. Grunwaldzki 2/4
50-384 Wrocław, Poland

Received 9 April 1995;
revised 17 May 1995