Polynomial imaginary decompositions
for finite extensions of fields
of characteristic zero

Andrzej Nowicki and Stanisław Spodzieja*

December 27, 2001

Abstract

Let $k$ be a field of characteristic zero, $L = k[\xi]$ a finite field extension of degree $m > 1$, and $f(z)$ a polynomial in one variable $z$ over $L$. Then there exist unique polynomials $u_0, \ldots, u_{m-1}$ belonging to $k[x_0, \ldots, x_{m-1}]$ such that $f(x_0 + \xi x_1 + \cdots + \xi^{m-1} x_{m-1}) = u_0 + \xi u_1 + \cdots + \xi^{m-1} u_{m-1}$. We prove that if $f(z) \notin L$, then the polynomials $u_0, \ldots, u_{m-1}$ are algebraically independent over $k$ and they have no common divisors in $k[x_0, \ldots, x_{m-1}]$ of positive degrees. Some other properties of polynomials $u_0, \ldots, u_{m-1}$ are also given.

1 Introduction

If $z, x, y$ are variables and $f(z)$ is a polynomial from $\mathbb{C}[z]$, then there exist unique polynomials $u(x, y), v(x, y)$ belonging to $\mathbb{R}[x, y]$ such that $f(x + iy) = u(x, y) + iv(x, y)$. We will show that if $f$ is nonzero, then the polynomials $u(x, y)$ and $v(x, y)$ are coprime. We will also show that the same is true if instead of the extension $\mathbb{R} \subset \mathbb{C}$ we consider a finite field extension of characteristic zero.

More exactly, assume that $k$ is a field and $L = k[\xi]$ is a finite field extension of degree $m > 1$. Let $z$ and $x_0, \ldots, x_{m-1}$ be variables and let $f(z)$ be a polynomial from $L[z]$. Then there exist unique polynomials $u_0, \ldots, u_{m-1}$, belonging to $k[x] := k[x_0, \ldots, x_{m-1}]$, such that

$$f(x_0 + \xi x_1 + \cdots + \xi^{m-1} x_{m-1}) = u_0 + \xi u_1 + \cdots + \xi^{m-1} u_{m-1}.$$
This representation we call the *imaginary decomposition* of \( f \), and the polynomials \( u_0, \ldots, u_{m-1} \) we call the *imaginary parts* of \( f \). We will show that if \( f \) is nonzero, then the imaginary parts of \( f \) have no common divisors in \( k[x] \) of positive degrees. Moreover, we prove that a sequence \((u_0, \ldots, u_{m-1})\) of polynomials from \( k[x] \) forms imaginary parts of a polynomial \( f(z) \in L[z] \) if and only if the polynomials \( u_0, \ldots, u_{m-1} \) satisfy some generalizations of Cauchy-Riemann equations. Some other properties concerning the divisibility of imaginary parts are also given.

## 2 Notations and preliminaries

Throughout the paper \( k \) is a field of characteristic zero and \( L = k[\xi] \) is a finite field extension of degree \( m > 1 \). Assume that

\[
\varphi(t) = t^m - a_{m-1}t^{m-1} - \cdots - a_1t - a_0
\]

(with \( a_0, \ldots, a_{m-1} \in k \)) is the minimal polynomial of \( \xi \) over \( k \). Let \( x = (x_0, x_1, \ldots, x_{m-1}) \), where \( x_0, \ldots, x_{m-1} \) are variables, and let \( k[x] := k[x_0, \ldots, x_{m-1}] \), \( L[x] := L[x_0, \ldots, x_{m-1}] \) be the polynomial rings. We denote by \( M \) the set \( k[X]^m \), that is,

\[
M := \{(u_0, u_1, \ldots, u_{m-1}); u_0, \ldots, u_{m-1} \in k[x]\}.
\]

Let \( u = (u_0, \ldots, u_{m-1}) \in M \). We use the following notations. We denote by \( \overline{u} = (\overline{u}_0, \ldots, \overline{u}_{m-1}) \) the element from \( M \) defined by:

\[
\overline{u}_0 = a_0u_{m-1}, \quad \overline{u}_1 = u_0 + a_1u_{m-1}, \quad \overline{u}_2 = u_1 + a_2u_{m-1}, \quad \vdots \quad \overline{u}_{m-1} = u_{m-2} + a_{m-1}u_{m-1}.
\]

Moreover, we denote by \([u]\) the polynomial from \( L[x] \) defined as

\[
[u] := u_0 + \xi u_1 + \cdots + \xi^{m-1} u_{m-1}.
\]

In particular, \([x] := x_0 + \xi x_1 + \cdots + \xi^{m-1} x_{m-1} \). If the polynomials \( u_0, \ldots, u_{m-1} \) are imaginary parts of a polynomial \( f(z) \in L[z] \), then \( f([x]) = [u] \). Observe that the equality \( \xi^m = a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1} \) implies that \([u]\xi = [\overline{u}]\).

If \( i \in \{0, \ldots, m-1\} \), then we denote by \( \frac{\partial u}{\partial x_i} \) the element from \( M \) defined as

\[
\frac{\partial u}{\partial x_i} := \left( \frac{\partial u_0}{\partial x_i}, \ldots, \frac{\partial u_{m-1}}{\partial x_i} \right).
\]
Lemma 2.1. If $u_0, \ldots, u_{m-1}$ are imaginary parts of a polynomial $f(z) \in L[z]$, then
\[
\left[ \frac{\partial u}{\partial x_i} \right] = f'([x]) \xi^i
\]
for $i \in \{0, \ldots, m-1\}$, where $f'(z)$ means the ordinary derivative of $f$ with respect to $z$.

Proof. \[
\left[ \frac{\partial u}{\partial x_i} \right] = \frac{\partial}{\partial x_i} [u] = \frac{\partial}{\partial x_i} f([x]) = f'([x]) \frac{\partial}{\partial x_i} [x] = f'([x]) \xi^i. \]
As a consequence of this lemma we obtain the following proposition.

Proposition 2.2. If $u_0, \ldots, u_{m-1} \in \mathbb{k}[x]$ are imaginary parts of a polynomial $f(z) \in L[z] \setminus L$, then $u_0, \ldots, u_{m-1}$ are algebraically independent over $\mathbb{k}$.

Proof. Assume that $f([x]) = [u]$, where $u := (u_0, \ldots, u_{m-1})$ and $f(z) \in L[z] \setminus L$. Suppose that $u_0, \ldots, u_{m-1}$ are algebraically dependent over $\mathbb{k}$. Then the vectors $\frac{\partial u}{\partial x_0}, \ldots, \frac{\partial u}{\partial x_{m-1}}$ are linearly dependent over the field $\mathbb{k}(x) := \mathbb{k}(x_0, \ldots, x_{m-1})$. Hence, there exist a nonzero sequence $\alpha = (\alpha_0, \ldots, \alpha_{m-1})$ of polynomials from $\mathbb{k}[x]$ such that $\sum_{i=0}^{m-1} \alpha_i \frac{\partial u}{\partial x_i} = 0$, that is, $\sum_{i=0}^{m-1} \alpha_i \left[ \frac{\partial u}{\partial x_i} \right] = 0$. Now, by Lemma 2.1 we get:
\[
0 = \sum_{i=0}^{m-1} \alpha_i \left[ \frac{\partial u}{\partial x_i} \right] = \sum_{i=0}^{m-1} \alpha_i f'([x]) \xi^i = f'([x]) \left( \sum_{i=0}^{m-1} \alpha_i \xi^i \right) = f'([x]) [\alpha].
\]
Hence, in the polynomial ring $L[x]$ we have the equality $f'([x]) [\alpha] = 0$. But $f'([x]) \neq 0$ and $[\alpha] \neq 0$. So, we have a contradiction. □

3 Generalization of the Cauchy-Riemann equation

We introduce the following generalization of the Cauchy - Riemann equation.

Definition 3.1. Let $u \in M$. We say that $u$ is a $\xi$-sequence if
\[
\frac{\partial u}{\partial x_i} = \frac{\partial u}{\partial x_{i-1}},
\]
for all $i = 1, 2, \ldots, m - 1$.

The following proposition show that the imaginary parts of a polynomial from $L[z]$ form a $\xi$-sequence.
Proposition 3.2. Let \( f(z) \in L[z] \) and let \( u \) be the element from \( M \) such that
\[
f([x]) = [u].
\]

Then \( u \) is a \( \xi \)-sequence.

Proof. If \( i \in \{1, \ldots, m-1\} \) then, by Lemma 2.1, we have:
\[
\left[ \frac{\partial u}{\partial x_i} \right] = f'([x]) \xi^i = f'([x]) \xi^{i-1} \cdot \xi = \left[ \frac{\partial u}{\partial x_{i-1}} \right] \cdot \xi = \left[ \frac{\partial u}{\partial x_{i-1}} \right] = \left[ \frac{\partial u}{\partial x_{i-1}} \right],
\]
and hence \( \frac{\partial u}{\partial x_i} = \frac{\partial u}{\partial x_{i-1}} \). \( \Box \)

We will show that the converse of the above proposition is also true. For a proof of this fact we need several lemmas.

Lemma 3.3. If \( u \in M \) is a \( \xi \)-sequence, then each partial derivative \( \frac{\partial u}{\partial x_j} \), for \( j = 0, \ldots, m-1 \), is also a \( \xi \)-sequence.

Proof. Let \( j \in \{0, \ldots, m-1\} \) and put \( w := \frac{\partial u}{\partial x_j} = \left( \frac{\partial u}{\partial x_0}, \ldots, \frac{\partial u}{\partial x_{m-1}} \right) \).
Then for every \( i \in \{1, \ldots, m-1\} \) we have:
\[
\frac{\partial w}{\partial x_i} = \frac{\partial^2 u}{\partial x_i \partial x_j} = \frac{\partial}{\partial x_j} \frac{\partial u}{\partial x_i} = \frac{\partial}{\partial x_j} \frac{\partial u}{\partial x_{i-1}} \frac{\partial u}{\partial x_{i-1}} = \frac{\partial u}{\partial x_{i-1}} \frac{\partial u}{\partial x_j} = \frac{\partial w}{\partial x_{i-1}};
\]
and hence, \( w \) is a \( \xi \)-sequence. \( \Box \)

Lemma 3.4. If \( u \in M \) is a \( \xi \)-sequence, then
\[
\left[ \frac{\partial u}{\partial x_i} \right] \xi^i = \left[ \frac{\partial u}{\partial x_{i+1}} \right],
\]
for \( i = 0, 1, \ldots, m-2 \). In particular,
\[
\left[ \frac{\partial u}{\partial x_0} \right] \xi = \left[ \frac{\partial u}{\partial x_1} \right], \quad \left[ \frac{\partial u}{\partial x_1} \right] \xi^2 = \left[ \frac{\partial u}{\partial x_2} \right], \quad \ldots, \quad \left[ \frac{\partial u}{\partial x_0} \right] \xi^{m-1} = \left[ \frac{\partial u}{\partial x_{m-1}} \right].
\]

Proof. \( \left[ \frac{\partial u}{\partial x_i} \right] \xi = \left[ \frac{\partial u}{\partial x_{i+1}} \right] = \left[ \frac{\partial u}{\partial x_{i+1}} \right] \). \( \Box \)

Consider the usual gradation \( k[x] = \bigoplus_{s \geq 0} k[x]_s \), where each \( k[x]_s \) is the subgroup of \( k[x] \) containing zero and all homogeneous polynomials from \( k[x] \) of degree \( s \). We say that an element \( u = (u_0, \ldots, u_{m-1}) \) from \( M \) is homogeneous of degree \( s \), if all the polynomials \( u_0, \ldots, u_{m-1} \) belong to \( k[x]_s \).

Every polynomial \( h \in k[x] \) has a presentation of the form \( h = h^{(0)} + h^{(1)} + \cdots + h^{(r)} \), where each \( h^{(j)} \), for \( j = 0, \ldots, r \), is a unique homogeneous polynomial belonging to \( k[x]_j \).

4
Let \( u = (u_0, \ldots, u_{m-1}) \in M \). Then there exists a common integer \( r \geq 0 \) such that
\[
u_i = u_i^{(0)} + u_i^{(1)} + \cdots + u_i^{(r)},
\]
for all \( i = 0, \ldots, m-1 \), and we have
\[
u = u^{(0)} + u^{(1)} + \cdots + u^{(r)},
\]
where \( u^{(j)} = (u_0^{(j)}, u_1^{(j)}, \ldots, u_{m-1}^{(j)}) \) for \( j = 0, 1, \ldots, r \). Then each \( u^{(j)} \), for \( j = 0, \ldots, r \), is a homogeneous element of \( M \) of degree \( j \). We call it the \textit{homogeneous component} of \( u \) of degree \( j \). Since
\[
\frac{\partial}{\partial x_i} (k[x]_s) \subseteq k[x]_{s-1},
\]
for every \( s \geq 0 \) and \( i = 0, 1, \ldots, m-1 \) (where \( k[x]_{-1} = 0 \)), we obtain the following lemma.

\textbf{Lemma 3.5.} Let \( u \in M \). If \( u \) is a \( \xi \)-sequence, then each homogeneous component of \( u \) is also a \( \xi \)-sequence. □

Note also:

\textbf{Lemma 3.6.} Let \( u \) be a homogeneous element of \( M \) of degree \( s \geq 0 \). If \( u \) is a \( \xi \)-sequence, then
\[
[x] \left[ \frac{\partial u}{\partial x_0} \right] = s[u].
\]

\textbf{Proof.} As a consequence of Lemma 3.4 we have:
\[
[x] \left[ \frac{\partial u}{\partial x_0} \right] = (x_0 + \xi x_1 + \xi^2 x_2 + \cdots + \xi^{m-1} x_{m-1}) \left[ \frac{\partial u}{\partial x_0} \right]
\]
\[
= x_0 \left[ \frac{\partial u}{\partial x_0} \right] + x_1 \left[ \frac{\partial u}{\partial x_1} \right] \xi + x_2 \left[ \frac{\partial u}{\partial x_0} \right] \xi^2 + \cdots + x_{m-1} \left[ \frac{\partial u}{\partial x_{m-1}} \right] \xi^{m-1}
\]
\[
= x_0 \left[ \frac{\partial u}{\partial x_0} \right] + x_1 \left[ \frac{\partial u}{\partial x_1} \right] + x_2 \left[ \frac{\partial u}{\partial x_2} \right] + \cdots + x_{m-1} \left[ \frac{\partial u}{\partial x_{m-1}} \right]
\]
\[
= x_0 \frac{\partial u}{\partial x_0} + x_1 \frac{\partial u}{\partial x_1} + x_2 \frac{\partial u}{\partial x_2} + \cdots + x_{m-1} \frac{\partial u}{\partial x_{m-1}}
\]
\[
= [su] = s[u].
\]
We used also the well-known Euler equality. □

\textbf{Lemma 3.7.} Let \( u \) be a homogeneous element of \( M \) of degree \( s \geq 0 \). If \( u \) is a \( \xi \)-sequence, then there exists a unique \( b \in L \) such that \([u] = b[x]_s\).
Proof. We use an induction with respect to $s$. It is obvious for $s = 0$. Let $s > 0$ and assume that it is true for all homogeneous $\xi$-sequences of degree $s - 1$.

Let $u$ be a homogeneous $\xi$-sequence of degree $s$. Then, by Lemma 3.3, the partial derivative $\frac{\partial u}{\partial x_0}$ is a homogeneous $\xi$-sequence of degree $s - 1$ and hence, by induction, there exists an element $c \in L$ such that

$$\left[ \frac{\partial u}{\partial x_0} \right] = c[x]^{s-1}. $$

Put $b := \frac{1}{s}c$. Then, by Lemma 3.6, we have:

$$b[x]^s = \frac{1}{s}c[x]^{s-1}[x] = \frac{1}{s} \left[ \frac{\partial u}{\partial x_0} \right] [x] = \frac{1}{s} s[u] = [u]. $$

The uniqueness is obvious. □

Now we are ready to prove the following theorem.

**Theorem 3.8.** Let $k$ be a field of characteristic zero and let $L = k[\xi]$ be a finite field extension of degree $m > 1$. Let $z, x_0, x_1, \ldots, x_{m-1}$ be variables and let $u = (u_0, \ldots, u_{m-1})$ be a sequence of polynomials belonging to $k[x] := k[x_0, \ldots, x_{m-1}]$. Then the following two conditions are equivalent.

1. $u$ is a $\xi$-sequence.
2. There exists a polynomial $f(z) \in L[z]$ such that the polynomials $u_0, \ldots, u_{m-1}$ are the imaginary parts of $f(z)$, that is,

$$f(x_0 + \xi x_1 + \cdots + \xi^{m-1} x_{m-1}) = u_0 + \xi u_1 + \cdots + \xi^{m-1} u_{m-1}. $$

**Proof.** The implication (2) $\Rightarrow$ (1) we already proved (see Proposition 3.2). Assume now that $u$ is a $\xi$-sequence. Let $u = u^{(0)} + u^{(1)} + \cdots + u^{(r)}$ be the homogeneous decomposition of $u$. Then each $u^{(j)}$, for $j = 0, \ldots, r$, is (by Lemma 3.5) a homogeneous $\xi$-sequence of degree $j$ and so, by Lemma 3.7, there exists $b_j \in L$ such that $[u^{(j)}] = b_j[x]^j$. Put $f(z) := b_0 + b_1 z + \cdots + b_r z^r$. Then

$$f([x]) = b_0[x]^0 + b_1[x]^1 + \cdots + b_r[x]^r = \left[ u^{(0)} \right] + \left[ u^{(1)} \right] + \cdots + \left[ u^{(r)} \right] = \left[ u \right].$$

This completes the proof. □

**Corollary 3.9.** If $u \in M$ is a $\xi$-sequence, then $\overline{u}$ is also a $\xi$-sequence.

**Proof.** By Theorem 3.8 there exists a polynomial $f(z) \in L[z]$ such that $f([x]) = [u]$. Consider the polynomial $g(z) := \xi f(z) \in L[z]$. Since $g([x]) = \xi f(z) = \xi[u] = [\overline{u}]$, the sequence $\overline{u}$ is, again by Theorem 3.8, a $\xi$-sequence. □
4 Divisibility

In this section we use the same notations as in the previous sections.

Proposition 4.1. Let \( u = (u_0, \ldots, u_{m-1}) \) be a \( \xi \)-sequence. Assume that the polynomials \( u_1, u_2, \ldots, u_{m-1} \) belong to \( k \). Then \( u_0 \in k \).

Proof. Since \( \frac{\partial u}{\partial x_i} = \frac{\partial u}{\partial x_{i-1}} \) for all \( i = 1, \ldots, m-1 \) (see Definition 3.1), we have
\[
\frac{\partial u_0}{\partial x_i} = \frac{\partial u_0}{\partial x_{i-1}} = \frac{\partial u_0 u_{m-1}}{\partial x_{i-1}} = 0,
\]
(for \( i = 1, \ldots, m-1 \)) and moreover,
\[
0 = \frac{\partial u_1}{\partial x_1} = \frac{\partial u_0}{\partial x_0} = \frac{\partial (u_0 + a_1 u_{m-1})}{\partial x_0} = \frac{\partial u_0}{\partial x_0} + a_1 \frac{\partial u_{m-1}}{\partial x_0} = \frac{\partial u_0}{\partial x_0}.
\]
Therefore, \( \frac{\partial u_0}{\partial x_0} = \frac{\partial u_0}{\partial x_1} = \cdots = \frac{\partial u_0}{\partial x_{m-1}} = 0 \) and hence, since \( \text{char}(k) = 0 \), the polynomial \( u_0 \) belongs to \( k \). □

Proposition 4.2. Let \( u = (u_0, \ldots, u_{m-1}) \) be a nonzero homogeneous \( \xi \)-sequence. Then \( \gcd(u_0, \ldots, u_{m-1}) = 1 \).

Proof. We know, by Lemma 3.7, that \( [u] = b[x]^s \) for some \( b \in L \) and \( s \geq 0 \). Let \( 0 \neq h \in k[x] := k[x_0, \ldots, x_{m-1}] \) be a common divisor of all the polynomials \( u_0, \ldots, u_{m-1} \). We will show that \( h \in k \).

Put \( u_0 = v_0 h, \ldots, u_{m-1} = v_{m-1} h \) with \( v_0, \ldots, v_{m-1} \in k[x] \). Then in the polynomial ring \( L[x] := L[x_0, \ldots, x_{m-1}] \) we have the equality
\[
b[x]^s = [v]h.
\]
But \( L[x] \) is a UFD and \( [x] = x_0 + \xi x_1 + \cdots + \xi^{m-1} x_{m-1} \) is an irreducible polynomial in \( L[x] \), so \( h = c[x]^r \) for some nonzero \( c \in L \) and \( 0 \leq r \leq s \). This means (by Theorem 3.8) that \( (h, 0, 0, \ldots, 0) \) is a \( \xi \)-sequence. Now Proposition 4.1 implies that \( h \in k \). □

Theorem 4.3. Let \( k \) be a field of characteristic zero and let \( L = k[\xi] \) be a finite field extension of degree \( m > 1 \). Let \( z, x_0, x_1, \ldots, x_{m-1} \) be variables and let \( u = (u_0, \ldots, u_{m-1}) \) be a sequence of polynomials belonging to \( k[x] := k[x_0, \ldots, x_{m-1}] \). If the polynomials \( u_0, \ldots, u_{m-1} \) are the imaginary parts of a nonzero polynomial \( f(z) \in L[z] \), then \( \gcd(u_0, \ldots, u_{m-1}) = 1 \).
Proof. Let \( 0 \neq h \in k[x] := k[x_0, \ldots, x_{m-1}] \) be a common divisor of all the polynomials \( u_0, \ldots, u_{m-1} \). Denote by \( h^* \) the homogeneous component of highest degree of \( h \), and let \( u_0^*, \ldots, u_{m-1}^* \) be the homogeneous components of highest degree of \( u_0, \ldots, u_{m-1} \), respectively. Then \( 0 \neq h^* \) is a common divisor of all the polynomials \( u_0^*, \ldots, u_{m-1}^* \) and moreover, by Lemma 3.5, \( (u_0^*, \ldots, u_{m-1}^*) \) is a homogeneous \( \xi \)-sequence. This implies, by Proposition 4.2, that \( h^* \in k \). Therefore, \( h \in k \) and so, \( \gcd(u_0, \ldots, u_{m-1}) = 1 \). □

As a consequence of theorems 3.8 and 4.3 we have:

**Theorem 4.4.** Let \( k \) be a field of characteristic zero and let \( k \subset L \) be a finite field extension. If \( (u_0, \ldots, u_{m-1}) \) is a nonzero \( \xi \)-sequence, then the polynomials \( u_0, \ldots, u_{m-1} \) have no common divisors of positive degrees. □

5 Quadratic extensions

Throughout this section \( L = k[\xi] \) is a quadratic field extension of \( k \). We assume that \( \xi^2 = r \), where \( r \) is a nonzero element from \( k \) such that the polynomial \( t^2 - r \) is irreducible in \( k[t] \). Every element of \( L \) has a unique presentation of the form \( a + b\xi \) with \( a, b \in k \).

Let \( x, y, z \) be variables. If \( w \in k[x, y] \), then we denote by \( w_x \) and \( w_y \) the partial derivatives \( \frac{\partial w}{\partial x} \) and \( \frac{\partial w}{\partial y} \), respectively. In this case a pair \( (u, v) \) of polynomials from \( k[x, y] \) is a \( \xi \)-sequence iff \( u_y = rv_x \) and \( v_y = u_x \). Such a pair we will call a \( \xi \)-pair. By Theorem 3.8 we have:

**Proposition 5.1.** Let \( (u, v) \) be a pair of polynomials from \( k[x, y] \). The following two conditions are equivalent.

1. There exists a polynomial \( f(z) \in L[z] \) such that \( f(x + \xi y) = u + \xi v \).
2. \( u_y = rv_x \) and \( v_y = u_x \). □

Let \( \Delta : k[x, y] \to k[x, y] \) be a generalization of the Laplace operator defined by

\[
\Delta := r \frac{\partial^2}{\partial x^2} - \frac{\partial^2}{\partial y^2},
\]

that is, \( \Delta(w) = rw_{xx} - w_{yy} \) for \( w \in k[x, y] \). It is easy to check that if \( (u, v) \) is a \( \xi \)-pair, then \( \Delta(u) = \Delta(v) = 0 \). Note the following observation.

**Proposition 5.2.** Let \( u \in k[x, y] \). The following two conditions are equivalent.

1. There exists a polynomial \( v \in k[x, y] \) such that \( (u, v) \) is a \( \xi \)-pair.
2. \( \Delta(u) = 0 \).
Proof. The implication (1) ⇒ (2) is obvious. We prove the implication (2) ⇒ (1). Let $f := \frac{1}{r} u_y$ and $g := u_x$. Since $f_y = g_x$ and char$(k) = 0$, there exists a polynomial $v \in k[x, y]$ such that $v_x = f$ and $v_y = g$. Then $u_y = rv_x$ and $v_y = u_x$ and hence, by Proposition 5.1, $(u, v)$ is a ξ-pair. □

Consider two sequences $(p_n)$ and $(q_n)$ of polynomials from $k[x, y]$ defined as follows:

$$
\begin{align*}
  p_0 &= 1, & q_0 &= 0, \\
  p_{n+1} &= xp_n + ryq_n, & q_{n+1} &= yp_n + xq_n.
\end{align*}
$$

In particular, $p_1 = x$, $p_2 = x^2 + ry^2$, $p_3 = x(x^2 + 3ry^2)$, $p_4 = x^4 + 6rx^2y^2 + r^2y^4$, $q_1 = y$, $q_2 = 2xy$, $q_3 = y(3x^2 + ry^2)$, $q_4 = 4xy(x^2 + ry^2)$. Note the following matrix presentation of these sequences.

**Proposition 5.3.** If $A = \begin{bmatrix} x & ry \\ y & x \end{bmatrix}$, then $A^n = \begin{bmatrix} p_n & rq_n \\ q_n & p_n \end{bmatrix}$, for all $n \geq 0$. □

It is easy to check that, for any nonnegative $n$, the pair $(p_n, q_n)$ is a ξ-pair such that

$$(*) \quad p_n + \xi q_n = (x + \xi y)^n.$$

We present some observations concerning the sequence $(p_n)$ and $(q_n)$.

As a consequence of $(*)$ and Proposition 2.2 we obtain

**Proposition 5.4.** If $n \geq 1$, then the polynomials $p_n$ and $q_n$ are algebraically independent over $k$. □

As a consequence of $(*)$ and Theorem 4.3 we obtain

**Proposition 5.5.** $\gcd(p_n, q_n) = 1$. □

The equality $(*)$ implies the following proposition.

**Proposition 5.6.** If $n$ and $m$ are nonnegative integers, then

$$p_{n+m} = p_np_m + rq_nq_m \quad \text{and} \quad q_{n+m} = p_nq_m + p_mq_n.$$  □

In particular, for $n = m$, we get

**Proposition 5.7.** $p_{2n} = p_n^2 + rq_n^2$ and $q_{2n} = 2p_nq_n$. □

Using a simple induction and the above propositions it is easy to prove the next proposition.
Proposition 5.8.

1. \( y \mid q_n \), for \( n \in \mathbb{N} \).
2. If \( n \mid m \), then \( q_n \mid q_m \).
3. \( p_n \mid q_{2kn} \), for \( n, k \in \mathbb{N} \).
4. \( p_n \mid p_{(2k+1)n} \), for \( n, k \in \mathbb{N} \).
5. \( \gcd(p_{kn}, q_n) = 1 \), for \( n, k \in \mathbb{N} \).
6. \( \gcd(q_{kn+r}, q_n) = \gcd(q_r, q_n) \), for \( n, k, r \in \mathbb{N} \). □

Now, by Proposition 5.8 and the Euclid algorithm, we have:

Proposition 5.9. If \( n, m \in \mathbb{N} \), then

\[ \gcd(q_n, q_m) = q_{\gcd(n,m)}. \] □

Note that a similar proposition is well known for some classical sequences of integers. Such a property have the sequences of Fibonacci numbers, Mersenne numbers and others (see for example, [1], [2]).

References


Faculty of Mathematics and Computer Science, Nicolaus Copernicus University, 87-100 Toruń, Poland
e-mail: anow@mat.uni.torun.pl

Faculty of Mathematics
University of Łódź
S. Banacha 22
90-238 Łódź, Poland
e-mail: spodziej@imul.uni.lodz.pl