DIDACTICA MATHEMATICA, Vol. 37 (2019) , pp. 45–55

A GENERALIZATION OF THE CIRCULANT MATRIX, AND THE IRREDUCIBILITY OF THE POLYNOMIAL $X^n - a$

Andrei MĂRCUŞ şi Paul Răzvan ŢAPOŞ

Abstract. We study in an elementary way the irreducibility over $\mathbb{Q}$ of the polynomial $X^n - a \in \mathbb{Q}[X]$, by using the properties of an $n \times n$ matrix with rational entries associated to a polynomial of degree less that n.

MSC 2000. 12F05.

Key words. irreducible polynomial, minimal polynomial, circulant matrix, field extension.

1. INTRODUCTION

One of the often encountered exercises in high school exams is the following:

Prove that if a, b, c are rational numbers such that $a + b\sqrt[3]{2} + c\sqrt[3]{4} = 0$, then $a = b = c = 0$.

A usual elementary argument leads to the equality

$$a^3 + 2b^3 + 4c^3 + 6abc = 0.$$

Note that the left hand side is just the determinant of the matrix

$$\begin{pmatrix} a & b & c \\ 2c & a & b \\ 2b & 2c & a \end{pmatrix},$$

which we denote here by $C_2(a, b, c)$, and we regard it as a modification of the cyclic matrix $C(a, b, c)$.

In this paper, to a polynomial f of degree $< n$ and a rational number a we associate an $n \times n$ matrix $C_a(f)$, and we investigate the connection between $\det C_a(f)$ and the irreducibility of the polynomial $X^n - a \in \mathbb{Q}[X]$.

Readers familiar with the theory of field extensions (see [4, Chapters 5, 6]) may recognize that we are talking about the field norm $N_{\mathbb{Q}(\sqrt[n]{a})/\mathbb{Q}}(f(\sqrt[n]{a}))$ (see [4, Section 6.5]). But our approach intends to be as elementary as possible, being inspired by Toma Albu's papers [1, 2, 3].We obtain the properties of the matrix $C_a(f)$ by using the properties of the cyclic matrix $C(f)$.

The paper is organized as follows. In Section 2 we recall some basic facts about simple extensions of the field $\mathbb{Q}$ of rational numbers, in the form we need them. For any other unexplained notions we refer to [5]. In Section 3 we introduce the matrix $C_a(f)$, we calculate its characteristic polynomial, and we obtain a matrix representation over $\mathbb{Q}$ of the field $\mathbb{Q}(\sqrt[n]{a})$. Finally, in Section 4 we discuss the irreducibility over $\mathbb{Q}$ of the polynomial $X^n - a$, in terms of the determinant of $C_a(f)$.

2. PRELIMINARIES ON FIELD EXTENSIONS

Definition 1. A polynomial is called *irreducible* over the field K if it cannot be expressed as a product of lower degree polynomials with coefficients in K.

Definition 2. Let K be a subfield of L. The dimension of the vector space L over K is called the *degree of the field extension* $K \leq L$, and it is denoted by $[L : K]$.

Let $n \geq 1$, let $f = a_0 + a_1X + a_2X^2 + \ldots + a_{n-1}X^{n-1} + X^n \in \mathbb{Q}[X]$, and let $\alpha \in \mathbb{C}$ a root of f. Denote by

$$\mathbb{Q}(\alpha) = \{b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_{n-1}\alpha^{n-1} \mid b_i \in \mathbb{Q},\ i = 0, \ldots, n-1\}$$

the $\mathbb{Q}$-vector space generated by the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

The following result is well-known, but we include a complete proof, for convenience.

Proposition 1. *The following statements are equivalent:*

(i) f *is irreducible over* $\mathbb{Q}$;
(ii) $g \in \mathbb{Q}[X]$, $g(\alpha) = 0 \implies f \mid g$;
(iii) *the quotient ring* $\mathbb{Q}[X]/(f)$ *is a field;*
(iv) *the quotient ring* $\mathbb{Q}[X]/(f)$ *is an integral domain;*
(v) $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ *are linearly independent over* $\mathbb{Q}$.
(vi) α *is not a root of a non-zero polynomial of degree less than* n.

In this case

a) $\mathbb{Q}(\alpha)$ *is a subfield of* $\mathbb{C}$;
b) $\mathbb{Q}[X]/(f) \simeq \mathbb{Q}(\alpha)$.

Proof. (i) $\implies$ (ii) Suppose by contradiction that $f \nmid g$. Since f is irreducible, we have that the greatest common divisor of f and g is 1. Therefore, there exist $u, v \in \mathbb{Q}[X]$ such that $fu + gv = 1$. Hence $1 = f(\alpha)u(\alpha) + g(\alpha)v(\alpha) = 0 \cdot u(\alpha) + 0 \cdot v(\alpha) = 0$, contradiction.

(ii) $\implies$ (i) Suppose by contradiction that f is reducible over $\mathbb{Q}$. Then there exist $f_1, f_2 \in \mathbb{Q}[X]$, such that $f_1, f_2 \neq 0$, $\deg(f_1) < \deg(f)$, $\deg(f_2) < \deg(f)$ and $f = f_1f_2$. Thus, $f(\alpha) = f_1(\alpha)f_2(\alpha) = 0$, which means that $f_1(\alpha) = 0$ or $f_2(\alpha) = 0$. Assume, without loss of generality, that $f_1(\alpha) = 0$. Then $f \mid f_1$, which means that $\deg(f) \leq \deg(f_1)$, contradiction.

(i) $\implies$ (iii) For any $g \in \mathbb{Q}[X]$, we use the notation $\hat{g} = g + (f)$, hence $\hat{g} \in \mathbb{Q}[X]/(f)$. Let $\hat{g} \in \mathbb{Q}[X]/(f)$, $\hat{g} \neq \hat{0}$. Then $g \in \mathbb{Q}[X]$ is a polynomial which is not divisible by f. Since f is irreducible and $f \nmid g$, we have that the greatest common divisor of f and g is 1. Then there exist $u, v \in \mathbb{Q}[X]$ such that $fu + gv = 1$. Since $fu \in (f)$, we have $\hat{fu} = \hat{0}$ and $\hat{g} \cdot \hat{v} = \hat{gv} = \hat{1}$, which shows that $\hat{g}$ is invertible, thus $\mathbb{Q}[X]/(f)$ is a field.

(iii) $\implies$ (i) Assume that f is not irreducible. If $f = f_1f_2$, where f_1 and f_2 are non-constant polynomials, then $\deg(f_1) < \deg(f)$ and $\deg(f_2) < \deg(f)$, so f_1 and f_2 are not multiples of f, and therefore $\hat{f_1} \neq \hat{0}$ and $\hat{f_2} \neq \hat{0}$. However,

$\hat{f}_1 \hat{f}_2 = \widehat{f_1 f_2} = \hat{f} = \hat{0}$. Therefore, $\mathbb{Q}[X]/(f)$ has a zero divisor hence is not a field.

(iii) $\Longrightarrow$ (iv) is obvious.

(iv) $\Longrightarrow$ (iii) $\mathbb{Q}[X]/(f)$ is a $\mathbb{Q}$-algebra with basis $\{\hat{1}, \hat{X}, \hat{X}^2, \ldots, \hat{X}^{n-1}\}$. Let $a \in \mathbb{Q}[X]/(f), a \neq 0$. We define the function

$$F : \mathbb{Q}[X]/(f) \to \mathbb{Q}[X]/(f), \qquad F(x) = ax.$$

Let $x, y \in \mathbb{Q}[X]/(f)$ such that $F(x) = F(y)$. Therefore, $ax = ay$ and $a(x - y) = 0$. But, we are in an integral domain and $a \neq 0$, hence $x - y = 0$. Thus F is injective. Moreover, $\dim(\mathbb{Q}[X]/(f)) < \infty$, so F is a bijection. We conclude that there exists $b \in \mathbb{Q}[X]/(f)$ such that $F(b) = 1$, so b is the inverse of a. It follows that $\mathbb{Q}[X]/(f)$ is a field.

(ii) $\Longrightarrow$ (v) Let $b_0, b_1, \ldots, b_{n-1} \in \mathbb{Q}$ such that

$$b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_{n-1}\alpha^{n-1} = 0.$$

We define the polynomial

$$g = b_0 + b_1 X + b_2 X^2 + \ldots + b_{n-1} X^{n-1} \in \mathbb{Q}[X].$$

Therefore, $g(\alpha) = 0$ and, using ii), we have that $f \mid g$. However, deg $(g)<$deg(f) and this implies that $g = 0$, hence $b_0 = \ldots = b_{n-1} = 0$ and $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are linearly independent over $\mathbb{Q}$.

(v) $\Longrightarrow$ (i) Suppose that f is not irreducible. Then there exists $f_1, f_2 \in \mathbb{Q}[X]$ such that $\deg(f_1) \leq n - 1$, $\deg(f_2) \leq n - 1$, f_1 is irreducible, $f_1(\alpha) = 0$ and $f = f_1 f_2$. Let k be the degree of f_1, where $k \leq n - 1$. Therefore we may write

$$f_1 = b_k X^k + b_{k-1} X^{k-1} + \ldots + b_1 X + b_0,$$

where $b_k \neq 0$. Since $f_1(\alpha) = 0$, we conclude that $1, \alpha, \ldots, \alpha^{n-1}, \alpha^n$ are linearly dependent over $\mathbb{Q}$.

(v) $\Longleftrightarrow$ (vi) is obvious.

a) We have that $\mathbb{Q}(\alpha) \subset \mathbb{C}$ and $0, 1 \in \mathbb{Q}(\alpha)$. Let

$$u = b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_{n-1}\alpha^{n-1} \in \mathbb{Q}(\alpha),$$

$$v = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1} \in \mathbb{Q}(\alpha).$$

Clearly, $u - v \in \mathbb{Q}(\alpha)$. Let

$$g = b_0 + b_1 X + b_2 X^2 + \ldots + b_{n-1} X^{n-1} \in \mathbb{Q}[X],$$

$$h = c_0 + c_1 X + c_2 X^2 + \ldots + c_{n-1} X^{n-1} \in \mathbb{Q}[X].$$

Hence, $uv = g(\alpha)h(\alpha) = (gh)(\alpha)$. But there exists $q, r \in \mathbb{Q}[X]$, deg$(r)<$deg(f) such that $gh = fq + r$. Thus,

$$uv = gh(\alpha) = fq(\alpha) + r(\alpha) = r(\alpha) \in \mathbb{Q}(\alpha),$$

because deg$(r) \leq n - 1$.

Now, if $u \neq 0$, then $g(\alpha) \neq 0$. But f is irreducible, so the greatest common divisor of f and g is 1 and, therefore, there exist $z, w \in \mathbb{Q}[X]$ such that

$fz + gw = 1$. Thus, $f(\alpha)z(\alpha) + g(\alpha)w(\alpha) = 1$ and $u \cdot w(\alpha) = 1$, which means that u is invertible in $\mathbb{Q}(\alpha)$, hence $\mathbb{Q}(\alpha)$ is a field.

b) Let $\varphi : \mathbb{Q}[X] \to \mathbb{Q}(\alpha)$, $\varphi(g) = g(\alpha)$ for all $g \in \mathbb{Q}[X]$. Then $\mathrm{Im}(\varphi) = \{g(\alpha) \mid g \in \mathbb{Q}[X]\} = \mathbb{Q}(\alpha)$, and $\mathrm{Ker}(\varphi) = \{g \in \mathbb{Q}[X] \mid g(\alpha) = 0\} = (f)$. By the first isomorphism theorem we have that $\mathbb{Q}[X]/(f) \simeq \mathbb{Q}(\alpha)$. □

Definition 3. The polynomial f satisfying one of the equivalent statements of Proposition 1 is unique and is called the *minimal polynomial* of α.

3. A GENERALIZATION OF THE CIRCULANT MATRIX

Let $n \geq 1$. We fix the polynomial

$$f = a_0 + a_1X + a_2X^2 + \ldots + a_{n-1}X^{n-1} \in \mathbb{Q}[X].$$

We also fix the element $a \in \mathbb{Q}^*$, and let $\alpha \in \mathbb{C}$ such that $\alpha^n = a$..

By using the element a and the coefficients of f, we define the matrix

$$C_a(f) = C_a(a_0, a_1, \ldots, a_{n-1}) := \begin{bmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-2} & a_{n-1} \\ aa_{n-1} & a_0 & a_1 & \ldots & a_{n-3} & a_{n-2} \\ aa_{n-2} & aa_{n-1} & a_0 & \ldots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ aa_2 & aa_3 & aa_4 & \ldots & a_0 & a_1 \\ aa_1 & aa_2 & aa_3 & \ldots & aa_{n-1} & a_0 \end{bmatrix}$$

belonging to $\mathcal{M}_n(\mathbf{Q})$. In this section we study the properties of $C_a(f)$.

Observe that in the particular case $a = 1$, we obtain the *circulant matrix*

$$C(f) = C(a_0, a_1, \ldots, a_{n-1})$$

of elements $a_0, a_1, \ldots, a_{n-1}$. The following result is well-known (and note that it is valid for any complex coefficients). Denote by

$$\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

a primitive n-th root of unity.

Lemma 1. *The determinant of the circulant matrix is given by*

$$\det C(a_0, a_1, \ldots, a_{n-1}) = \prod_{j=0}^{n-1} f(\omega^j).$$

The next result shows that the calculation of $\det C_a(f)$ reduces to the determinant of a circulant matrix.

Lemma 2. *We have*

$$\det C(a_0, a_1\alpha, \ldots, a_{n-1}\alpha^{n-1}) = \det C_a(a_0, a_1, \ldots, a_{n-1}).$$

Proof. By using elementary row and column trasformations, we have that

$$\det C(a_0, a_1\alpha, \ldots, a_{n-1}\alpha^{n-1})$$

$$= \begin{vmatrix} a_0 & a_1\alpha & a_2\alpha^2 & \ldots & a_{n-1}\alpha^{n-1} \\ a_{n-1}\alpha^{n-1} & a_0 & a_1\alpha & \ldots & a_{n-2}\alpha^{n-2} \\ a_{n-2}\alpha^{n-2} & a_{n-1}\alpha^{n-1} & a_0 & \ldots & a_{n-3}\alpha^{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2\alpha^2 & a_3\alpha^3 & a_4\alpha^4 & \ldots & a_1\alpha \\ a_1\alpha & a_2\alpha^2 & a_3\alpha^3 & \ldots & a_0 \end{vmatrix}$$

$$= \frac{1}{\alpha\cdots\alpha^{n-1}} \begin{vmatrix} a_0 & a_1\alpha & a_2\alpha^2 & \ldots & a_{n-1}\alpha^{n-1} \\ \alpha a_{n-1}\alpha^{n-1} & \alpha a_0 & \alpha a_1\alpha & \ldots & \alpha a_{n-2}\alpha^{n-2} \\ \alpha^2 a_{n-2}\alpha^{n-2} & \alpha^2 a_{n-1}\alpha^{n-1} & \alpha^2 a_0 & \ldots & \alpha^2 a_{n-3}\alpha^{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{n-1}a_1\alpha & \alpha^{n-1}a_2\alpha^2 & \alpha^{n-1}a_3\alpha^3 & \ldots & \alpha^{n-1}a_0 \end{vmatrix}$$

$$= \frac{1}{\alpha\cdots\alpha^{n-1}} \begin{vmatrix} a_0 & a_1\alpha & a_2\alpha^2 & \ldots & a_{n-2}\alpha^{n-2} & a_{n-1}\alpha^{n-1} \\ a_{n-1}a & a_0\alpha & a_1\alpha^2 & \ldots & a_{n-3}\alpha^{n-2} & a_{n-2}\alpha^{n-1} \\ a_{n-2}a & aa_{n-1}\alpha & a_0\alpha^2 & \ldots & a_{n-4}\alpha^{n-2} & a_{n-3}\alpha^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2a & aa_3\alpha & aa_4\alpha^2 & \ldots & a_0\alpha^{n-2} & a_1\alpha^{n-1} \\ a_1a & aa_2\alpha & aa_3\alpha^2 & \ldots & aa_{n-1}\alpha^{n-2} & a_0\alpha^{n-1} \end{vmatrix}$$

$$= \frac{\alpha\cdot\alpha^2\cdot\ldots\cdot\alpha^{n-1}}{\alpha\cdot\alpha^2\cdot\ldots\cdot\alpha^{n-1}} \begin{vmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-2} & a_{n-1} \\ aa_{n-1} & a_0 & a_1 & \ldots & a_{n-3} & a_{n-2} \\ aa_{n-2} & aa_{n-1} & a_0 & \ldots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ aa_2 & aa_3 & aa_4 & \ldots & a_0 & a_1 \\ aa_1 & aa_2 & aa_3 & \ldots & aa_{n-1} & a_0 \end{vmatrix}$$

$$= \det C_a(a_0, a_1, \ldots, a_{n-1}),$$

so the statement is proved. □

Remark 1. By the above lemma we get that $\det C(a_0, a_1\alpha, \ldots, a_{n-1}\alpha^{n-1}) \in \mathbb{Q}$, even if α does not necessarily belong to $\mathbb{Q}$.

Corollary 1. *We have that*

$$\det C(a_0, a_1\alpha, \ldots, a_{n-1}\alpha^{n-1}) = \prod_{j=0}^{n-1} g(\omega^j),$$

where

$$g(X) = f(\alpha X) = a_0 + a_1\alpha X + a_2\alpha^2 X^2 + \ldots + a_{n-1}\alpha^{n-1}X^{n-1} \in \mathbb{C}[X].$$

Next we want to discuss some other properties of the matrix $C_a(f)$.

PROPOSITION 2. 1) *$C_a(a_0, a_1, \ldots, a_{n-1})$ and $C(a_0, \alpha a_1, \ldots, \alpha^{n-1}a_{n-1})$ have the same characteristic polynomial.*

2) *The characteristic polynomial of $C_a(f)$ is given by*

$$P_{C_a(f)}(X) = \prod_{j=0}^{n-1}(X - f(\alpha\omega^j)).$$

Proof. We have that

$$\begin{aligned}
P_{C_a}(X) &= \det(XI_n - C_a(a_0, a_1, \ldots, a_{n-1}))\\
&= \begin{vmatrix} X-a_0 & -a_1 & -a_2 & \ldots & -a_{n-2} & -a_{n-1}\\ -aa_{n-1} & X-a_0 & -a_1 & \ldots & -a_{n-3} & -a_{n-2}\\ -aa_{n-2} & -aa_{n-1} & X-a_0 & \ldots & -a_{n-4} & -a_{n-3}\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ -aa_2 & -aa_3 & -aa_4 & \ldots & X-a_0 & -a_1\\ -aa_1 & -aa_2 & -aa_3 & \ldots & -aa_{n-1} & X-a_0 \end{vmatrix}\\
&= \det C_a(X - a_0, -a_1, -a_2, \ldots, -a_{n-1})\\
&= \det C(X - a_0, -a_1\alpha, -a_2\alpha^2, \ldots, -a_{n-1}\alpha^{n-1})\\
&= \begin{vmatrix} X-a_0 & -a_1\alpha & -a_2\alpha^2 & \ldots & -a_{n-1}\alpha^{n-1}\\ -a_{n-1}\alpha^{n-1} & X-a_0 & -a_1\alpha & \ldots & -a_{n-2}\alpha^{n-2}\\ -a_{n-2}\alpha^{n-2} & -a_{n-1}\alpha^{n-1} & X-a_0 & \ldots & -a_{n-3}\alpha^{n-3}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ -a_1\alpha & -a_2\alpha^2 & -a_3\alpha^3 & \ldots & X-a_0 \end{vmatrix}\\
&= P_{C(a_0, a_1\alpha, \ldots, \alpha^{n-1}a_{n-1})}(X).
\end{aligned}$$

2) We have that

$$\begin{aligned}
P_{C_a(f)}(X) &= P_{C(a_0, a_1\alpha, \ldots, \alpha^{n-1}a_{n-1})}(X)\\
&= \det(XI_n - C(a_0, a_1\alpha, \ldots, \alpha^{n-1}a_{n-1}))\\
&= \det C(X - a_0, -a_1\alpha, -a_2\alpha^2, \ldots, -a_{n-1}\alpha^{n-1}).
\end{aligned}$$

By Lemma 1, we have that

$$\det C(X - a_0, -a_1\alpha, -a_2\alpha^2, \ldots, -a_{n-1}\alpha^{n-1}) = \prod_{j=0}^{n-1} g(\omega^j),$$

where $g(Y) = X - a_0 - a_1\alpha Y - a_2\alpha^2Y^2 - \ldots - a_{n-1}\alpha^{n-1}Y^{n-1}$. Therefore,

$$g(\omega^j) = X - f(\alpha\omega^j),$$

and the statement follows. □

We now consider the matrix $M_a = (m_{ij}) \in \mathcal{M}_n(\mathbb{Q})$, where $m_{i,i+1} = 1$ for all $i = 1, \ldots, n-1$, $m_{n,1} = a$, and $m_{ij} = 0$ otherwise. This means that

$$M_a := \begin{bmatrix} 0 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 0 & 1 \\ a & 0 & 0 & 0 & \ldots & 0 & 0 \end{bmatrix}$$

is just the companion matrix of the polynomial $X^n - a$.

Theorem 1. *The following statements hold:*
1) $C_a(f) = f(M_a)$.
2) $M_a^n = aI_n$, *and* $X^n - a$ *is the minimal polynomial of* M_a.

Proof. 1) We compute the powers of M_a. We find that

$$M_a^2 := \begin{bmatrix} 0 & 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 0 & 1 \\ a & 0 & 0 & 0 & \ldots & 0 & 0 \\ 0 & a & 0 & 0 & \ldots & 0 & 0 \end{bmatrix},$$

and then

$$M_a^3 := \begin{bmatrix} 0 & 0 & 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a & 0 & 0 & 0 & \ldots & 0 & 0 \\ 0 & a & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & a & 0 & \ldots & 0 & 0 \end{bmatrix}.$$

Similarly, for all $k \in \{1, \ldots, n-1\}$, we have that $M_a^k = (m_{ij})$, where $m_{i,i+k} = 1$ for all $i = 1, \ldots, n-k$, $m_{n-k+i,i} = a$ for all $i = 1, \ldots, k$, and $m_{i,j} = 0$ otherwise.

Now,

$$C_a(f) = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-2} & a_{n-1} \\ aa_{n-1} & a_0 & a_1 & \dots & a_{n-3} & a_{n-2} \\ aa_{n-2} & aa_{n-1} & a_0 & \dots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ aa_2 & aa_3 & aa_4 & \dots & a_0 & a_1 \\ aa_1 & aa_2 & aa_3 & \dots & aa_{n-1} & a_0 \end{bmatrix}$$

$$= \begin{bmatrix} a_0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & a_0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & a_0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & a_0 & 0 \\ a & 0 & 0 & 0 & \dots & 0 & a_0 \end{bmatrix} + \begin{bmatrix} 0 & a_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & a_1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & a_1 \\ aa_1 & 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

$$+ \begin{bmatrix} 0 & 0 & a_2 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & a_2 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & a_2 \\ aa_2 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & aa_2 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

$$+ \dots + \begin{bmatrix} 0 & 0 & 0 & 0 & \dots & 0 & a_{n-1} \\ aa_{n-1} & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & aa_{n-1} & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & aa_{n-1} & 0 \end{bmatrix}$$

$$= a_0 I_n + a_1 M_a + a_2 M_a^2 + \dots + a_{n-1} M_a^{n-1} = f(M_a).$$

2) We similarly compute that

$$M_a^n = M_a^{n-1} \cdot M_a = \begin{bmatrix} a & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & a & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & a & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & a & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & a \end{bmatrix} = aI_n.$$

These calculations show that $X^n - a$ is the minimal polynomial of M_a. $\square$

Proposition 3. *Let $n \in \mathbf{N}^*$ and $a \in \mathbb{Q}$. Let $\mathbb{Q}_n[X]$ denote the $\mathbb{Q}$-vector space comprising the polynomials with degree smaller than n and $f, g \in \mathbb{Q}_n[X]$. Then:*

a) $C_a(f) + C_a(g) = C_a(f+g)$;

b) $C_a(f) \cdot C_a(g) = C_a(fg \ mod \ (X^n - a))$.

More precisely, the correspondence $f \mapsto C_a(f)$ induces an injective homomorphism of $\mathbb{Q}$-algebras

$$\mathbb{Q}[X]/(X^n - a) \to \mathcal{M}_n(\mathbb{Q}).$$

Proof. Let

$$\Phi : \mathbb{Q}_n[X] \to \mathcal{M}_n(\mathbb{Q}), \qquad \Phi(f) = C_a(f).$$

Then Φ is a $\mathbb{Q}$-linear map. Moreover, using Theorem 1, we have that

$$C_a(f) = f(M_a) \implies \Phi(fg) = (fg)(M_a) = f(M_a)g(M_a) = \Phi(f)\Phi(g).$$

Therefore, Φ is an algebra homomorphism.

Due to the fact that $X^n - a$ is the minimal polynomial of M_a, we must have that $\operatorname{Ker}\Phi = (X^n - a)$. Moreover, $\mathbb{Q}[X]/(X^n - a)$ can be identified with $\mathbb{Q}_n[X]$, regarded as Q-vector spaces. We conclude that Φ is an injective homomorphism, hence statements a) and b) hold. □

4. THE IRREDUCIBILITY OF THE POLYNOMIAL $X^n - a$

We keep the notations of the preceding section. Next, we want to discuss the irreducibility of the polynomial $X^n - a$ over $\mathbb{Q}$, with the aid of the matrix $C_a(f)$. It turns out that we need to work in the subfield $\mathbb{Q}(\omega)$ of $\mathbb{C}$, generated by $\mathbb{Q}$ and the primitive n-th root of unity ω. Recall that $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$, where φ is Euler's totient function.

Theorem 2. *Assume that $X^n - a$ is irreducible over $\mathbb{Q}$ if and only if $X^n - a$ is irreducible over $\mathbb{Q}(\omega)$. The following statements are equivalent:*

(1) *$X^n - a$ is irreducible over $\mathbb{Q}$.*

(2) *For all $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$, $\det C_a(a_0, a_1, \ldots, a_{n-1}) = 0 \implies a_i = 0$ for all $i = 0, \ldots, n-1$.*

Proof. "(1) ⇒ (2) Assume that $X^n - a$ is irreducible over $\mathbb{Q}$. Then, by assumption, $X^n - a$ is irreducible over $\mathbb{Q}(\omega)$. Let $\alpha \in \mathbb{C}$ be a root of $X^n - a$. By using Lemma 1 and Lemma 2, we have that

$$\begin{aligned} 0 &= \det\, C_a(a_0, a_1, \ldots, a_{n-1}) \\ &= \det\, C(a_0, a_1\alpha, \ldots, a_{n-1}\alpha^{n-1}) \\ &= \prod_{j=0}^{n-1} (a_0 + a_1\alpha\omega^j + a_2\alpha^2\omega^{2j} + \ldots + a_{n-1}\alpha^{n-1}\omega^{(n-1)j}). \end{aligned}$$

Therefore, there exists $j \in \{0, 1, \ldots, n-1\}$ such that

$$a_0 + a_1\alpha\omega^j + a_2\alpha^2\omega^{2j} + \ldots + a_{n-1}\alpha^{n-1}\omega^{(n-1)\cdot j} = 0.$$

Since $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent over $\mathbb{Q}(\omega)$, we conclude that

$$a_0 = a_1 = \ldots = a_{n-1} = 0.$$

"(2) $\Rightarrow$ (1)" We argue by contradiction. Assume that $X^n - a$ is reducible over $\mathbb{Q}$. Then $1, \alpha, \ldots, \alpha^{n-1}$ are linearly dependent over $\mathbb{Q}$, so there exist $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$, not all zero, such that

$$\sum_{k=0}^{n-1} a_k \alpha^k = 0.$$

By Corollary 1, we find that $\det C_a(a_0, a_1, \ldots, a_{n-1}) = 0$, but we also know that $a_0, a_1, \ldots, a_{n-1}$ are not all zero, contradiction. □

The assumption of the theorem is satisfied when n is a prime number.

PROPOSITION 4. *Let p be a prime number, $a \in \mathbf{Q}^*$ and $\alpha \in \mathbb{C}$ such that $\alpha^p = a$. Then*

$$X^p - a \text{ is irreducible over } \mathbb{Q} \iff X^p - a \text{ is irreducible over } \mathbb{Q}(\omega).$$

Proof. "$\Rightarrow$" We argue by contradiction. Assume that $X^p - a$ is reducible over $\mathbb{Q}(\omega)$. Hence, there exist non-constant polynomials $g, h \in \mathbb{Q}(\omega)[X]$ such that $\deg(f)$, $\deg(g) < p$ and

$$X^p - a = g \cdot h.$$

Let $1 \leq r \leq p-1$ be the degree of g. Therefore,

$$X^p - a = \prod_{k=0}^{p-1}(X - \omega^k \alpha) = gh = (X^r + \ldots + \omega^l \alpha^r)(X^{p-r} + \ldots + \omega^s \alpha^{p-r}),$$

for some $l, s \in \mathbf{N}$. Since $g, h \in \mathbb{Q}(\omega)[X]$, we have that $\alpha^r, \alpha^{p-r} \in \mathbb{Q}(\omega)$. Let d be the greatest common divisor of r and $p - r$. Thus, there are $u, v \in \mathbb{Z}$ such that $d = r \cdot u + (p-r) \cdot v$. Moreover,

$$\alpha^d = \alpha^{r \cdot u + (p-r) \cdot v} = (\alpha^r)^u \cdot (\alpha^{p-r})^v.$$

Since $\alpha^r, \alpha^{p-r} \in \mathbb{Q}(\omega)$, we find that $\alpha^d \in \mathbb{Q}(\omega)$. Also, $d \mid r$ and $d \mid p-r$, hence $d \mid r + p - r = p$. Due to the fact that $r < p$, $d \mid r$ and $d \mid p$, we must have $d = 1$. Therefore, $\alpha^d = \alpha \in \mathbb{Q}(\omega)$ and, because $Q(\omega)$ is a field, we conclude that

$$\mathbb{Q}(\alpha) \leq \mathbb{Q}(\omega).$$

Thus,

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}].$$

But we know that

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(p) = p - 1 \text{ and } [\mathbb{Q}(\alpha) : \mathbb{Q}] = p,$$

hence $p \mid p - 1$, contradiction.

The converse is obvious, since $\mathbb{Q} \leq \mathbb{Q}(\omega)$. □

EXEMPLE 1. Let $n = 6$ and $f = X^6 + 3$. Then f is irreducible over $\mathbb{Q}$, but f is reducible over $\mathbb{Q}(\omega) = \mathbb{Q}(i\sqrt{3})$, because

$$f = X^6 + 3 = (X^3 + i\sqrt{3})(X^3 - i\sqrt{3}) = (X^3 + 2\omega - 1)(X^3 - 2\omega + 1).$$

We will discuss the irreducibility over $\mathbb{Q}(\omega)$ of the polynomial $X^n - a$ in a subsequent paper.

REFERENCES

[1] ALBU, T., *Construcţii elementare de inele şi corpuri comutative (I)*, Gazeta Matematică **93** (1988), 305–311.
[2] ALBU, T., *Construcţii elementare de inele şi corpuri (II)*, Gazeta Matematică **93** (1988), 337–346.
[3] ALBU, T., *Construcţii elementare de inele şi corpuri (III)*, Gazeta Matematică **93** (1988), 386–396.
[4] LANG, S., *Algebra*. Revised Third Edition. Springer-Verlag, New-York, 2005.
[5] MARCUS, A., *Polinoame şi ecuaţii algebrice*, Casa Carţii de Ştiinţă, Cluj-Napoca, 2020.

Faculty of Mathematics and Computer Science
"Babeş-Bolyai" University
Str. Kogălniceanu, no. 1
400084 Cluj-Napoca, Romania
e-mail: marcus@math.ubbcluj.ro
razvantapos@gmail.com