Czechoslovak Mathematical Journal

Štefan Schwarz

Construction of normal bases in cyclic extensions of a field

Czechoslovak Mathematical Journal, Vol. 38 (1988), No. 2, 291–312

Persistent URL: http://dml.cz/dmlcz/102225

Terms of use:

© Institute of Mathematics AS CR, 1988

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

Czechoslovak Mathematical Journal, 38 (113) 1988, Praha

CONSTRUCTION OF NORMAL BASES IN CYCLIC EXTENSIONS OF A FIELD

ŠTEFAN SCHWARZ, Bratislava

(Received July, 14 1986)

Let F be a field and K a separable normal extension of F of degree n. Let $G = \{g_1, g_2, \ldots, g_n\}$ be the Galois group of K/F. It is known that there exists an element $\omega \in K$ such that $g_1\omega, g_2\omega, \ldots, g_n\omega$ are linearly independent, hence they form a basis of K/F. Such a basis is called a normal basis of K over F.

Various proofs of the existence of a normal basis are given in several textbooks. The proofs always distinguish two cases: F is infinite and F is finite. In this last case both F and K are finite fields. For example Van der Waerden ([9], Russian edition pp. 239–243) proves the case F is infinite, the case F is finite is rather sketched. A thorough discussion of the case F finite given in L. Rédei ([6], pp. 552–558) is certainly not short. The proof of the case F finite (more generally K cyclic over F) given in N. Jacobson ([3], pp. 57 and 61) is short but it is based on several previously proved not quite elementary results. An analogous situation is in the book A. A. Albert ([1], p. 120).

In this paper we first give a new short and transparent proof of the normal basis theorem for cyclic extensions over any field F. In section 2 we give a method how to find effectively all normal bases. As far as I can decide the systematic method developed in this paper is new. In section 3 we illustrate this method on several examples.

1

Theorem 1. *Any cyclic extension K/F has a normal basis over F.*

Proof. Write $K = F(\alpha)$, where α satisfies $f(\alpha) = 0$ and $f(x)$ is an irreducible cyclic polynomial of degree n over F. Let $G = \{g, g^2, \ldots, g^{n-1}, g^n = 1\}$ be the Galois group of K/F. The roots of $f(x) = 0$ will be written in the form

$$\alpha_1 = \alpha\,, \quad \alpha_2 = g\alpha\,, \quad \alpha_3 = g^2\alpha, \ldots, \alpha_n = g^{n-1}\alpha\,.$$

Introduce the following $n \times n$ matrices:

$$\varDelta = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & & & \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{pmatrix} \qquad N = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & & & \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix},$$

and (T denotes the transpose)

$$N^T = N^{-1} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ & & & & & \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

Construct finally the $n \times n$ matrix $C = (c_{ij})$ defined by

$$\begin{aligned} g1 &= c_{00} + c_{01}\alpha + \dots + c_{0,n-1}\alpha^{n-1}, \\ g\alpha &= c_{10} + c_{11}\alpha + \dots + c_{1,n-1}\alpha^{n-1}, \\ g\alpha^2 &= c_{20} + c_{21}\alpha + \dots + c_{2,n-1}\alpha^{n-1}, \\ &\vdots \\ g\alpha^{n-1} &= c_{n-1,0} + c_{n-1,1}\alpha + \dots + c_{n-1,n-1}\alpha^{n-1}, \end{aligned} \tag{1}$$

$(c_{00} = 1, c_{01} = \dots = c_{0,n-1} = 0)$. Otherwise written

$$(1, \alpha_2, \alpha_2^2, \dots, \alpha_2^{n-1})^T = C(1, \alpha_1, \alpha_1^2, \dots, \alpha_1^{n-1})^T.$$

By applying g^{i-1} $(i \geqq 2)$ to both sides we obtain (with the convention $\alpha_{n+1} = \alpha_1$)

$$(1, \alpha_{i+1}, \alpha_{i+1}^2, \dots, \alpha_{i+1}^{n-1})^T = C(1, \alpha_i, \alpha_i^2, \dots, \alpha_i^{n-1})^T.$$

Hence the matrix $C\varDelta$ is equal to the matrix arising from $\varDelta$ by (cyclicly) shifting the columns of $\varDelta$ to the right (i.e. we replace the first column in $\varDelta$ by the last column, the second by the first column, and so on). Therefore $C\varDelta = \varDelta N^T$ and (since the determinant $|\varDelta| \neq 0$)

$$\varDelta^{-1} C \varDelta = N^T. \tag{2}$$

We have proved that the matrices C and N^T are similar in $K = F(\alpha)$. Now since all elements of the matrices C and N^T are in F, they are similar in F. [This is the unique not quite elementary statement from the theory of matrices used in the proof. It immediately follows from the fact that (2) implies $\varDelta^{-1}(C - \lambda E)\varDelta = N^T - \lambda E$ and the λ-matrices $C - \lambda E$ and $N^T - \lambda E$ have the same invariant factors. Hereby E is the $n \times n$ unit matrix.]

Hence there exists a non-singular matrix P with elements in F such that $PCP^{-1} = N^T$.

In the following sections it is more convenient to work with N (instead of N^T). The matrices N and N^T are similar (in F). As a matter of fact we have $N^T = SNS$, where

$$S = S^{-1} = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

We finally have: There is a non-singular matrix Q (with all element in F) such that

(3) $$QCQ^{-1} = N.$$

Denote $Q(1, \alpha, \dots, \alpha^{n-1})^T = U = (u_1, u_2, \dots, u_n)^T$. Since Q is non-singular, $(u_1, u_2, \dots, u_n)$ are linearly independent over F. We show that $(u_1, u_2, \dots, u_n)$ is a normal basis of $F(\alpha)$ over F. We have

$$gU = Q(g1, g\alpha, \dots, g\alpha^{n-1})^T = QC(1, \alpha, \dots, \alpha^{n-1})^T = QCQ^{-1}U = NU.$$

Explicitly:

$$(gu_1, gu_2, \dots, gu_n) = (u_2, u_3, \dots, u_n, u_1),$$

whence

$$u_2 = gu_1,\ u_3 = gu_2, \dots, gu_{n-1} = u_n,$$

and

$$U = (u_1, gu_1, g^2u_1, \dots, g^{n-1}u_1).$$

This proves Theorem 1.

Note for further purposes: Since $N^n = E$, the relation (3) implies $C^n = E$. Next since det $|N| = (-1)^{n-1}$, we have det $|C| = (-1)^{n-1}$.

2

We now turn to the question how to find effectively all normal bases of $F(\alpha)$ over F. This will be done by using the matrix C introduced above.

We have seen: If an $n \times n$ matrix Q satisfies (3), then the elements of the column vector $Y = Q(1, \alpha, \dots, \alpha^{n-1})^T$ form a normal basis. Conversely, suppose that the elements of the vector $Z = R(1, \alpha, \dots, \alpha^{n-1})^T$ with some non-singular matrix R form a normal basis, i.e. $gZ = NZ$. Then

$$R(g1, g\alpha, \dots, g\alpha^{n-1})^T = NZ,$$

implies $RC(1, \alpha, \dots, \alpha^{n-1})^T = NZ$ and $RCR^{-1}Z = NZ$. Hence $RCR^{-1} = N$, i.e. R satisfies (3) with $Q = R$.

To find all solutions satisfying (3) (with unknown Q) we first find all solutions of $QC = NQ$.

Denote by $\varrho_i = (r_{i1}, r_{i2}, \dots, r_{in})$ $(i = 1, 2, \dots, n)$ the rows of Q. Then

$$\begin{pmatrix} \varrho_1 \\ \varrho_2 \\ \vdots \\ \varrho_{n-1} \\ \varrho_n \end{pmatrix} C = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} \varrho_1 \\ \varrho_2 \\ \vdots \\ \varrho_{n-1} \\ \varrho_n \end{pmatrix}$$

implies $\varrho_1 C = \varrho_2, \varrho_2 C = \varrho_3, \ldots, \varrho_{n-1} C = \varrho_n$ [and $\varrho_n C = \varrho_1$]. Hence Q is necessarily of the form

(4)
$$Q = \begin{pmatrix} \varrho_1 \\ \varrho_1 C \\ \varrho_1 C^2 \\ \vdots \\ \varrho_1 C^{n-1} \end{pmatrix} .$$

Conversely, if ϱ_1 is an arbitrary row vector (with elements in F), then with respect to $C^n = E$ we obtain

$$Q, C = \begin{pmatrix} \varrho_1 C \\ \varrho_1 C^2 \\ \vdots \\ \varrho_1 C^{n-1} \\ \varrho_1 \end{pmatrix} = NQ .$$

This implies

Lemma 1. *Any normal basis $(\omega_1, \omega_2, \ldots, \ldots, \omega_n)$ of the cyclic field $F(\alpha)$ is of the form*

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = Q \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix} = \begin{pmatrix} \varrho \\ \varrho C \\ \vdots \\ \varrho C^{n-1} \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix},$$

where the row vector $\varrho = (r_1, r_2, \ldots, r_n)$ $(r_i \in F)$ is restricted by the condition det $|Q| \neq 0$.

A row vector $\varrho = (r_1, \ldots, r_n)$ will be called admissible (with respect to C) if for the corresponding matrix Q, we have dct $|Q| \neq 0$.

For a given row vector ϱ denote by $\psi_\varrho(\lambda)$ the monic λ-polynomial of smallest degree (with coefficients in F) such that $\varrho\, \psi_\varrho(C) = 0$. The polynomial $\psi_\varrho(\lambda)$ is called the minimal polynomial of ϱ with respect to C. It is well known that $\psi_\varrho(\lambda)$ is uniquely determined and $\psi_\varrho(\lambda) \mid \lambda^n - 1$.

The condition that $\varrho, \varrho C, \ldots, \varrho C^{n-1}$ are linearly independent says that the minimal polynomial of ϱ with respect to C is $\lambda^n - 1$.

We decompose the polynomial $\lambda^n - 1$ into the product of monic irreducible factors over F. This factorization is of the form

(5)
$$\lambda^n - 1 = [\varphi_1(\lambda) \, . \, \varphi_2(\lambda) \ldots \varphi_r(\lambda)]^t .$$

a) If the characteristic of the field F is zero, or a prime $p \geqq 2$ with $(n. p) = 1$, then $t = 1$.

b) If the characteristic of F is p and $n = mp^e$, $(n, m) = 1$, then $t = p^e$, $e \geqq 1$.

Construct now the polynomials

$$\phi_1(\lambda) = \frac{\lambda^n - 1}{\varphi_1(\lambda)}, \quad \phi_2(\lambda) = \frac{\lambda^n - 1}{\varphi_2(\lambda)}, \ldots, \phi_r(\lambda) = \frac{\lambda^n - 1}{\varphi_r(\lambda)} .$$

The minimal polynomial of a row vector ϱ with respect to C is $\lambda^n - 1$ if and only if ϱ is such that

$$\varrho\, \phi_1(C) \neq 0\,, \quad \varrho\, \phi_2(C) \neq 0, \ldots, \varrho\, \phi_r(C) \neq 0\,.$$

This implies:

Lemma 2. *Denote by W_i the linear space of all row vectors $\varrho = (r_1, \ldots, r_n)$ satisfying $\varrho\, \phi_i(C) = 0$ $(i = 1, 2, \ldots, r)$. Then ϱ is admissible with respect to C if and only if ϱ is not contained in the (set theoretical) union $\{W_1 \cup W_2 \cup \ldots \cup W_r\}$.*

The procedure described by Lemma 2 can be essentially simplified. In particular, it will turn out that it is not necessary to solve the system of linear equations $\varrho\, \phi_i(C) = 0$.

Lemma 3. *Any vector ϱ satisfying $\varrho\, \phi_i(C) = 0$ is contained in the linear space V_i spanned by the rows of the matrix $\varphi_i(C)$.*

Proof. a) We first give a very simple proof in the case that $\lambda^n - 1 = \varphi_1(\lambda) \ldots \ldots \varphi_r(\lambda)$, where all irreducible factors are different.

Since $\varphi_i(C) \,.\, \phi_i(C) = 0$, it is clear that any ϱ contained in V_i satisfies $\varrho\, \phi_i(C) = 0$. We show conversely that any ϱ satisfying $\varrho\, \phi_i(C) = 0$ is contained in V_i.

Since $\varphi_i(\lambda)$ and $\phi_i(\lambda)$ are relatively prime, there are two polynomials $\xi_i(\lambda)$, $\eta_i(\lambda)$ such that $\xi_i(\lambda)\, \varphi_i(\lambda) + \eta_i(\lambda)\, \phi_i(\lambda) = 1$. This implies

$$\xi_i(C)\, \varphi_i(C) + \eta_i(C)\, \phi_i(C) = E\,,$$

and multiplying by ϱ we obtain

$$\varrho = \varrho\, \xi_i(C)\, \varphi_i(C) + \varrho\, \phi_i(C)\, \eta_i(C)\,.$$

If ϱ is such that $\varrho\, \varphi_i(C) = 0$, we get $\varrho = \varrho\, \xi_i(C)\, \varphi_i(C)$. Denote $\varrho\, \xi_i(C) = (k_1^{(i)}, k_2^{(i)}, \ldots, k_n^{(i)})$ with $k_j^{(i)} \in F$. Then $\varrho = (k_1^{(i)}, \ldots, k_n^{(i)})\, \varphi_i(C)$, which says that ϱ is a linear combination of the rows of $\varphi_i(C)$, hence it is contained in V_i.

b) Suppose next the general case, i.e. the case that repeated irreducible factors may occur. Write

$$\lambda^n - 1 = [\varphi_1(\lambda) \ldots \varphi_r(\lambda)]^{p^e}\,,$$

where $n = mp^e$, $(m, n) = 1$, $e \geqq 0$. We cannot apply the argument used above since $\varphi_i(\lambda)$ and $\phi_i(\lambda)$ are not relatively prime. The proof which follows holds however also in the case a) (i.e. $e = 0$).

Again, if ϱ is in the linear space V_i spanned by the rows of $\varphi_i(C)$, then $\varrho\, \phi_i(C) = 0$. We prove conversely, if ϱ satisfies $\varrho\, \phi_i(C) = 0$, then ϱ is in V_i.

Recall that there exists a non-singular matrix Q_0 such that $Q_0 C Q_0^{-1} = N$. If $g(\lambda)$ is any polynomial over F, then $Q_0\, g(C)\, Q_0^{-1} = g(N)$.

Suppose that $\varrho = (r_1, r_2, \ldots, r_n)$ satisfies $\varrho\, \phi_i(C) = 0$. This is equivalent to $\varrho\, \phi_i(C)\, Q_0^{-1} = 0$ and $\varrho Q_0^{-1} \,.\, Q_0\, \phi_i(C)\, Q_0^{-1} = 0$. Write $\varrho' = \varrho Q_0^{-1} = (r'_1, r'_2, \ldots, r'_n)$. We then have

(6) $$\varrho'\, \phi_i(N) = 0\,.$$

If the vector ϱ' satisfies (6), then each of the rows of the matrix

$$\begin{pmatrix} \varrho' \\ \varrho' N \\ \vdots \\ \varrho' N^{n-1} \end{pmatrix} = \begin{pmatrix} r'_1 r'_2 & \dots & r'_n \\ r'_n r'_1 & \dots & r'_{n-1} \\ \vdots & & \\ r'_2 r'_3 & \dots & r'_1 \end{pmatrix}$$

satisfies (6)

The circulant to the right can be written in the form

$$r'_1 E + r'_2 N + r'_3 N^2 + \dots + r'_n N^{n-1} = \psi(N) .$$

Hence $\psi(N)\, \phi_i(N) = 0$.

Write $\psi(\lambda) = \varphi_i(\lambda)\, \chi_i(\lambda) + \chi_{io}(\lambda)$, where $\deg \chi_{io}(\lambda) < \deg \varphi_i(\lambda)$. Then $\chi_{io}(\lambda)$ is necessarily the zero polynomial, since otherwise

$$[\varphi_i(N)\, \chi_i(N) + \chi_{io}(N)]\, \phi_i(N) = \chi_{io}(N)\, \phi_i(N) = 0 ,$$

and the minimal polynomial of N would be a polynomial of degree $<n$, which is not true. Hence $\psi(N) = \chi_i(N)\, \varphi_i(N)$. The first row of $\psi(N)$ is $\varrho' = (r'_1, r'_2, \dots, r'_n)$. Hence

$$\varrho' = (1, 0, \dots, 0)\, \chi_i(N)\, \varphi_i(N) .$$

Denote $(1, 0, \dots, 0)\, \chi_i(N) = (k'_1, k'_2, \dots, k'_n)$. We have

$$\varrho' = (k'_1, k'_2, \dots, k'_n)\, \varphi_i(N) .$$

Using $NQ_0 = Q_0 C$, and $\varphi_i(N)\, Q_0 = Q_0\, \varphi_i(C)$ we have successively

$$\varrho Q_0^{-1} = (k'_1, k'_2, \dots, k'_n)\, \varphi_i(N) ,$$

$$\varrho = (k'_1, k'_2, \dots, k'_n)\, \varphi_i(N)\, Q_0 = (k'_1, k'_2, \dots, k'_n)\, Q_0\, \varphi_i(C) .$$

Denoting $(k'_1, k'_2, \dots, k'_n)\, Q_0 = (k_1, k_2, \dots, k_n)$ $(k_i \in F)$, we finally obtain $\varrho = (k_1, \dots, k_n)\, \varphi_i(C)$, i.e. ϱ is contained in the linear space spanned by the rows of $\varphi_i(C)$. This proves Lemma 3.

We have proved the following Theorem which enables to find all normal bases of cyclic extensions of any field.

Theorem 2. *Let $F(\alpha)$ be a cyclic extension of degree n of the field F and g a generator of the Galois group of $F(\alpha)/F$. Construct the matrix C defined by* (1). *Let* (5) *be the factorization of $\lambda^n - 1$ into irreducible factors over F. Denote by V_i the linear space spanned by the rows of the matrix $\varphi_i(C)$. Choose a row vector $\varrho = (r_1, r_2, \dots, r_n)$ (with elements in F) such that $\varrho \notin \{V_1 \cup \dots \cup V_n\}$.* Construct finally the column vector

$$\Omega = \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = \begin{pmatrix} \varrho \\ \varrho C \\ \vdots \\ \varrho C^{n-1} \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix} .$$

Then $(\omega_1, \omega_2, \dots, \omega_n)$ is a normal basis of $F(\alpha)$ with respect to F, and any normal basis of $F(\alpha)$ over F is obtained in this manner.

Remark. It should be noted that $V_i \cap V_j$ may be different from 0. Next two normal bases (considered as unordered n-tuples) are either identical or have no elements in common.

3. Examples

The following examples illustrate the procedure described by Theorem 2. Several supplementary observations are included in these examples.

In the case of finite fields we do not aim to construct large tables of normal bases. On the contrary, we show how such tables can be replaced by rather simple statements which enable to identify all generators of normal bases.

Example 1. Let R be the field of rational numbers and $R(\alpha)$ the extension obtained by adjoining a root α of $x^3 - 3x + 1 = 0$. $R(\alpha)$ is cyclic over R and $g: \alpha \to g\alpha = -2 + \alpha^2$ is the generator of the Galois group $\{1, g, g^2\}$.

We wish to find all normal bases of $R(\alpha)$ over R.

Here $g1 = 1$, $g\alpha = -2 + \alpha^2$, $g\alpha^2 = (-2 + \alpha^2)^2 = 4 - \alpha - \alpha^2$.

$$C = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 0 & 1 \\ 4 & -1 & -1 \end{pmatrix} \quad \text{and} \quad C^2 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & -1 & -1 \\ 2 & 1 & 0 \end{pmatrix}.$$

Since $\lambda^3 - 1 = (\lambda - 1)(\lambda^2 + \lambda + 1)$, we have

$$\varphi_1(C) = C - E = \begin{pmatrix} 0 & 0 & 0 \\ -2 & -1 & 1 \\ 4 & -1 & -2 \end{pmatrix}, \quad \varphi_2(C) = E + C + C^2 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 6 & 0 & 0 \end{pmatrix}.$$

The space V_1 spanned by the vectors $(-2, 1, 1)$ and $(4, -1, -2)$ is the set of all vectors of the form $k_1(-2, -1, 1) + k_2(0, 1, 0)$, $k_i \in R$.

A vector $\varrho = (r_1, r_2, r_3)$ belongs to V_1 if and only if

$$\begin{vmatrix} r_1 & r_2 & r_3 \\ -2 & -1 & 1 \\ 0 & 1 & 0 \end{vmatrix} = -(r_1 + 2r_3) = 0\,.$$

The space V_2 is the set of all vectors of the form $(r_1, 0, 0)$. Hence [with $r_i \in R$]

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix} = \begin{pmatrix} \varrho \\ \varrho C \\ \varrho C^2 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix} = \begin{pmatrix} r_1 & r_2 & r_3 \\ r_1 - 2r_2 + 4r_3 & -r_3 & r_2 - r_3 \\ r_1 + 2r_2 + 2r_3 & -r_2 + r_3 & -r_2 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix}$$

gives all normal bases over R provided that $\varrho = (r_1, r_2, r_3)$ is chosen in such a manner that $(r_2, r_3) \neq (0, 0)$ and $r_1 \neq -2r_3$.

Remark. The numbers $\omega_1, \omega_2, \omega_3$ satisfy an equation of degree 3 over R: $m(x) = (x - \omega_1)(x - \omega_2)(x - \omega_3) = 0$. After some calculations we obtain

$$m(x) = (x - r_1)^3 - 6r_3(x - r_1)^2 + 3(3r_3^2 - r_2^2 + r_2 r_3)(x - r_1) + \\ + (r_2^3 - 3r_2 r_3^2 - r_3^3)\,.$$

These are all monic irreducible polynomials of degree 3 over R with roots in $R(\alpha)$, where the roots are linearly independent over R. [Provided that $(r_2, r_3) \neq (0, 0)$ and $r_1 \neq -2r_3$.]

Example 2. Consider the polynomial $f(x) = x^4 - 3$ over the field $F = R(i)$. Let $f(\alpha) = 0$. We have the find all normal bases of $F(\alpha)$ over F.

Here $F(\alpha)/F$ is of degree 4. Take as the generator of the Galois group $g\colon \alpha \rightarrow i\alpha$. Then $g1 = 1$, $g\alpha = \mathrm{i}\alpha$, $g\alpha^2 = -\alpha^2$, $g\alpha^3 = -\mathrm{i}\alpha^3$. Hence

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathrm{i} & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -\mathrm{i} \end{pmatrix}.$$

Next $\lambda^4 - 1 = (\lambda - 1)(\lambda + 1)(\lambda - \mathrm{i})(\lambda + \mathrm{i})$ implies

$$\begin{aligned} \varphi_1(C) &= C - E = \operatorname{diag}(0, \mathrm{i} - 1, -2, -\mathrm{i} - 1), \\ \varphi_2(C) &= C + E = \operatorname{diag}(2, \mathrm{i} + 1, 0, -\mathrm{i} + 1), \\ \varphi_3(C) &= C - \mathrm{i}E = \operatorname{diag}(1 - \mathrm{i}, 0, -1 - \mathrm{i}, -2\mathrm{i}), \\ \varphi_4(C) &= C + \mathrm{i}E = \operatorname{diag}(1 + \mathrm{i}, 2\mathrm{i}, -1 + \mathrm{i}, 0). \end{aligned}$$

The space V_1 consists of all vectors of the form $(0, r_2, r_3, r_4)$, where r_2, r_3, r_4 run independently over all elements of $R(\mathrm{i})$. Analogously for V_2, V_3, V_4. The admissible vectors are exactly those vectors $\varrho = (r_1, r_2, r_3, r_4)$ for which $r_1r_2r_3r_4 \neq 0$.

We have $\varrho C = (r_1, \mathrm{i}r_2, -r_3, -\mathrm{i}r_4)$, $\varrho C^2 = (\varrho C)\,C = (r_1, -r_2, r_3, -r_4)$, $\varrho C^3 = (\varrho C^2)\,C = (r_1, -\mathrm{i}r_2, -r_3, \mathrm{i}r_4)$.

All normal bases are given by

$$\Omega = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 \\ r_1 & \mathrm{i}r_2 & -r_3 & -\mathrm{i}r_4 \\ r_1 & -r_2 & r_3 & -r_4 \\ r_1 & -\mathrm{i}r_2 & -r_3 & \mathrm{i}r_4 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{pmatrix}$$

provided that $r_1r_2r_3r_4 \neq 0$ $[r_j \in R(i)]$.

In the following examples we shall deal with finite fields $GF(q^n)$ as extensions of degree n over $GF(q)$ ($q = p^s$, $s \geqq 1$, p a prime). We shall occasionally write F_q instead of $GF(q)$.

Suppose that in the decomposition (5) (over F_q) the degree of $\varphi_i(\lambda)$ is d_i, so that $d_1 + \ldots + d_r = m$. In this case it is known that the number of n-tuples

$$\{\omega, \omega^q, \ldots, \omega^{q^{n-1}}\}, \quad \omega \in F_{q^n},$$

forming a normal basis is equal to the number

$$\nu(q, n) = \frac{1}{n} q^n \left(1 - \frac{1}{q^{d_1}}\right) \ldots \left(1 - \frac{1}{q^{d_r}}\right).$$

This has been proved by O. Ore [5] and reproduced in a slightly other form in [2] and [4].

Recall also the well known fact that the number of monic irreducible polynomials of degree n over F_q is given by the formula

$$J(q, n) = \frac{1}{n} \sum_{d/n} \mu \left(\frac{n}{d} \right) q^d .$$

Remark 1. If we wish to know only the number $\nu(q, n)$ it is not necessary to know the factors $\varphi_i(\lambda)$ explicitly. It is known (see [7]) that the number σ_k of irreducible factors of degree k of $\lambda^n - 1$ over F_q, $(n, q) = 1$, is given by the formula

$$\sigma_k = \frac{1}{k} \sum_{t/k} \mu \left(\frac{k}{t} \right) (n, q^t - 1) ,$$

where μ is the Moebius function. The numbers σ_k may be successively calculated from the system

$$\sum_{t/k} t\sigma_t = (n, q^k - 1) , \quad k = 1, 2, \ldots, [n/2] .$$

For instance, for the polynomial $\lambda^{15} - 1$ over F_2 we have

$$\begin{aligned} \sigma_1 &= (15, 2 - 1) , \\ 2\sigma_2 + \sigma_1 &= (15, 2^2 - 1) , \\ 3\sigma_3 + \sigma_1 &= (15, 2^3 - 1) , \\ 4\sigma_4 + 2\sigma_2 + \sigma_1 &= (15, 2^4 - 1) , \\ \ldots\ldots\ldots\ldots&\ldots\ldots\ldots\ldots \end{aligned}$$

This gives $\sigma_1 = 1$, $\sigma_2 = 1$, $\sigma_3 = 0$, $\sigma_4 = 3$. Hence in our notation $d_1 = 1$, $d_2 = 2$, $d_3 = d_4 = d_5 = 4$. Therefore

$$\nu(2, 15) = \frac{1}{15} 2^{15} \left(1 - \frac{1}{2} \right) \left(1 - \frac{1}{2^2} \right) \left(1 - \frac{1}{2^4} \right)^3 = 675 .$$

The field $GF(2^{15})$ has 675 normal bases over $GF(2)$.

For our purposes the complete factorization of $\lambda^n - 1$ over F_q is of course necessary.

Remark 2. For numerical calculations it is useful further to note. The matrix C is non-singular. As a matter of fact we have det $|C| = (-1)^{n-1}$. On the other hand $C - E$ has exactly the rank $n - 1$. Both statements follow from a general theory concerning factorization of polynomials over finite fields given by the author in [8]. (See also [2].)

For convenience we introduce the following notion. An irreducible monic polynomial $g(x)$ of degree n over F_q will be called an N-polynomial if the roots of $g(x) = 0$ form a normal basis of $G\,F(q^n)$ over $G\,F(q)$. If $(\omega, \omega^q, \ldots, \omega^{q^{n-1}})$ is a normal basis of $G\,F(q^n)$ over $G\,F(q)$, then the monic minimal polynomial $m(x)$ of all the elements $\omega, \omega^q, \ldots, \omega^{q^{n-1}}$ is the same polynomial of degree n and $m(x)$ is an N-polynomial. [The number of N-polynomial is exactly $\nu(q, n)$.]

If $G\,F(q^n)$ is represented in the form $F_q(\alpha)$, then each basis is expressed as an n-tuple of polynomials in α of degree $\leqq n - 1$. But the totality of all N-polynomials does not depend on the special choice of α.

To decide whether a given irreducible polynomial $f(x)$ is an N-polynomial is of course conceptually very simple. Let $f(\alpha) = 0$. It is sufficient to calculate $\alpha, \alpha^q, \ldots$ $\ldots, \alpha^{q^{n-1}}$ as polynomials in $\alpha, \alpha^2, \ldots, \alpha^{n-1}$ and to check the linear independence. It is advantageous to use the matrix C.

Example 3. We have decide whether the irreducible polynomial $f(x) = x^4 +$ $+ 2x^3 + x^2 + 1$ over $G\,F(3)$ is an N-polynomial.

This is the case if and only if $\varrho = (0, 1, 0, 0)$ is an admissible vector with respect to C.

Let α be defined by $f(\alpha) = 0$. We have $1 = 1$, $\alpha^3 = \alpha^3$, $\alpha^6 = 2\alpha + 2\alpha^2 + 2\alpha^3$, $\alpha^9 = 2 + 2\alpha$. Hence

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 2 & 2 & 2 \\ 2 & 2 & 0 & 0 \end{pmatrix}.$$

Now $(0, 1, 0,0)\,C = (0, 0, 0, 1)$, $(0,0,0,1)\,C = (2, 2, 0, 0)$, $(2, 2, 0, 0)\,C = (2, 0, 0, 2)$. The matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 2 & 0 & 0 \\ 2 & 0 & 0 & 2 \end{pmatrix}$$

is singular. The given polynomial is not an N-polynomial over $G\,F(3)$.

Example 4. Find all normal bases of $G\,F(7^2)$ over $G\,F(7)$ [in a given representation of $G\,F(7^2)$] and the corresponding quadratic N-polynomials.

Choose an irreducible polynomial of degree 2 over F_7, e.g., $f(x) = x^2 + 1$, and represent F_{49} as $F_7(\alpha)$, where $f(\alpha) = 0$.

We have $J(7, 2) = 21$. Since $\lambda^2 - 1 = (\lambda - 1)(\lambda + 1)$, we have $\nu(7, 2) =$ $= \frac{1}{2} \cdot 7^2(1 - \frac{1}{7})^2 = 18$.

Here $1 = 1$, $\alpha^7 = 6\alpha$, so that

$$C = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

and

$$\varphi_1(C) = C - E = \begin{pmatrix} 0 & 0 \\ 0 & 5 \end{pmatrix}, \quad \varphi_2(C) = C + E = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}.$$

The space V_1 consists of all vectors of the form $k_1(0, 1)$, $k_1 \in F_7$. The space V_2 is the set of all vectors of the form $k_2(1, 0)$, $k_2 \in F_7$. A vector (r_1, r_2) does not belong to $V_1 \cup V_2$ iff $r_1 \neq 0$ and $r_2 \neq 0$. Hence the admissible vectors are the 36 vectors $\varrho = (r_1, r_2)$, where r_1, r_2 run independently over the set $\{1, 2, \ldots, 6\}$.

Since $(r_1, r_2)\, C = (r_1, 6r_2)$, we obtain all normal bases in the form:

$$\Omega = \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \begin{pmatrix}r_1, & r_2\\ r_1, & 6r_2\end{pmatrix}\begin{pmatrix}1\\ \alpha\end{pmatrix} = \begin{pmatrix}r_1 + r_2\alpha\\ r_1 - r_2\alpha\end{pmatrix}, \quad r_1r_2 \neq 0\,.$$

Since the couples (r_1, r_2) and $(r_1, 6r_2)$ lead to the same normal basis we obtained 18 different normal bases.

In this case [and in general for $n = 2$, $n = 3$ independently of q] it is easy to find all N-polynomials. It is sufficient to calculate

$$m(x) = (x - \omega_1)(x - \omega_2) = [x - (r_1 + \alpha r_2)]\,[x - (r_1 - \alpha r_2)] =$$
$$= (x - r_1)^2 + r_2^2\,, \quad r_1r_2 \neq 0\,.$$

Since $r_2^2 (\bmod 7)$ is one of the elements 1, 2, 4, $m(x)$ gives the 18 different quadratic N-polynomials over F_7.

Remark 1. Note that knowing one irreducible polynomial (namely $x^2 + 1$) we have found "almost all" irreducible polynomils. The remaining three irreducible polynomials which are not N-polynomials are $x^2 + 1$, $x^2 + 2$, $x^2 + 4$.

Remark 2. The polynomial $f(x) = x^2 + x + 3$ is irreducible over F_7. It is primitive and moreover an N-polynomial. If we represent F_{49} as $F_7(\beta)$, where $f(\beta) = 0$, the form of the normal bases will be, of course, different (but in some sense not "simpler").

Here $\beta^7 = 6 + 6\beta$. Hence

$$C = \begin{pmatrix}1 & 0\\ 6 & 6\end{pmatrix}, \quad \varphi_1(C) = C - E = \begin{pmatrix}0 & 0\\ 6 & 5\end{pmatrix}, \quad \varphi_2(C) = C + E = \begin{pmatrix}2 & 0\\ 6 & 0\end{pmatrix}.$$

The space V_1 is the set of all vectors of the form $k_1(6, 5)$, $k_1 \in F_7$, what is the same as $k_1'(1, 2)$, $k_1' \in F_7$. The space V_2 is the set of all vectors of the form $k_2(1, 0)$, $k_2 \in F_7$.

A vector $\varrho = (r_1, r_2)$ is admissible if and only if $r_2 \neq 0$ and $r_2 \neq 2r_1$. The normal bases are now given by

$$\Omega = \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \begin{pmatrix}\varrho\\ \varrho C\end{pmatrix}\begin{pmatrix}1\\ \beta\end{pmatrix} = \begin{pmatrix}r_1, & r_2\\ r_1 + 6r_2, & 6r_2\end{pmatrix}\begin{pmatrix}1\\ \beta\end{pmatrix} = \begin{pmatrix}r_1 + r_2\beta\\ r_1 - r_2 - r_2\beta\end{pmatrix}.$$

Of course, the set of N-polynomials remains the same as above.

Example 5. Find all normal bases of $GF(7^4)$ over $GF(7^2)$ for fixed chosen representations of $GF(7^4)$ and $GF(7^2)$. Find also the set of all N-polynomials of degree 2 over $GF(7^2)$.

We represent F_{49} as $F_7(b)$, where b satisfies $b^2 + 1 = 0$. Next $x^2 + x + b$ is irreducible over $F_7(b)$. Denote by α a root of $x^2 + x + b = 0$. Then F_{2401} can be represented as $F_7(b, \alpha)$, i.e. any element of F_{2401} is of the form $u + v\alpha$, where $u, v \in F_7(b)$ and $\alpha^2 + \alpha + b = 0$.

[The fact that $x^2 + x + b$ is irreducible over $F_7(b)$ can be proved directly by showing that there is no element $\xi + b\eta$, $\xi \in F_7$, $\eta \in F_7$, satisfying $(\xi + b\eta)^2 + (\xi + b\eta) + b = 0$.]

The number of monic irreducible quadratic polynomials over F_{49} is $J(49, 2) = \frac{1}{2}[49^2 - 49] = 1176$. Since $\lambda^2 - 1 = (\lambda - 1)(\lambda + 1)$, we have for the number of different bases (or different N-polynomials) $\nu(49, 2) = \frac{1}{2} . 49^2(1 - \frac{1}{49})^2 = 1152$.

To construct the matrix C we need $\alpha^9 = \alpha^{49}$. By using $\alpha^2 = -(\alpha + b)$ we have successively $\alpha^4 = -(1 + b) + (2b - 1)\alpha$, $\alpha^6 = -3 + (2 + 4b)\alpha$, $\alpha^7 = (4 - 2b) + (2 - 4b)\alpha$ and finally $\alpha^{49} = 6 + 6\alpha$. Therefore

$$C = \begin{pmatrix} 1 & 0 \\ 6 & 6 \end{pmatrix}, \quad \varphi_1(C) = C - E = \begin{pmatrix} 0 & 0 \\ 6 & 5 \end{pmatrix}, \quad \varphi_2(C) = C + E = \begin{pmatrix} 2 & 0 \\ 6 & 0 \end{pmatrix}.$$

The space V_1 consists of all vectors of the form $k_1(1, 2)$, where $k_1 \in F_7(b)$. The space V_2 is the set of all vectors $k_2(1, 0)$, $k_2 \in F_7(b)$. Hence a vector $\varrho = (r_1, r_2)$ is admissible if and only if $r_2 \neq 0$ and $r_2 \neq 2r_1$.

This gives 48 vectors of the form $(0, r_2)$, $r_2 \neq 0$, and 48.47 vectors of the form (r_1, r_2), $r_1 \neq 0$, $r_2 \neq 2r_1$. Together there exist $48.47 + 48 = 2304$ admissible vectors [with elements from $F_7(b)$].

Now

$$\varrho C = (r_1, r_2)\begin{pmatrix} 1 & 0 \\ 6 & 6 \end{pmatrix} = (r_1 + 6r_2, 6r_2).$$

Hence all normal bases are given by

$$(7) \qquad \Omega = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} r_1 & r_2 \\ r_1 - r_2, & -r_2 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \end{pmatrix} = \begin{pmatrix} r_1 + r_2\alpha \\ r_1 - r_2 - r_2\alpha \end{pmatrix},$$

with the restriction $r_2 \neq 0$, $r_2 \neq 2r_1$.

Since again the vectors (r_1, r_2) and $(r_1 + 6r_2, 6r_2)$ lead to the same basis we obtain $\frac{1}{2} . 2304 = 1152$ different normal bases, given by (7).

To find all N-polynomials it is sufficient to form

$$m(x) = (x - \omega_1)(x - \omega_2) = [x - (r_1 + r_2\alpha)][x - (r_1 - r_2 - r_2\alpha)] =$$
$$= (x - r_1)^2 + r_2(x - r_1) + br_2^2 .$$

We have proved: All the 1152 N-polynomials are given by

$$(8) \qquad m(x) = x^2 + (r_2 - 2r_1)x + r_1^2 - r_1r_2 + br_2^2 ,$$

where $r_1, r_2 \in F_7(b)$, with the restrictions $r_2 \neq 0$, $r_2 \neq 2r_1$.

Remark. We may use the polynomial $m(x)$ to describe all irreducible polynomials of degree 2 over $F_7(b)$.

If ω_1 and $\omega_2 = \omega_1^{49}$ are different elements the polynomial $(x - \omega_1)(x - \omega_2)$ is irreducible over $F_7(b)$. Now $\omega_1 - \omega_2 = (r_1 + r_2\alpha) - (r_1 - r_2 - r_2\alpha) = r_2(1 + 2\alpha)$. Hence putting in $m(x)$ any (r_1, r_2) with $r_2 \neq 0$ we get an irreducible polynomial. The non-admissible vectors satisfying this condition are the vectors (r_1, r_2), where $r_2 = 2r_1$, $r_1 \neq 0$. Putting in (8) $r_2 = 2r_1$ we obtain $\bar{m}(x) = x^2 -$

$-\ (1 + 3b)\, r_1^2$. For $r_1 \in F_7(b)$, $r_1 \neq 0$, this gives $\frac{1}{2}(49 - 1) = 24$ different irreducible quadratic polynomials over $F_7(b)$.

Summarily: The polynomials $m(x)$ and $\overline{m}(x)$ describe all the 1176 monic irreducible quadratic polynomials over $F_7(b)$.

Example 6. We have to find all normal bases of $G\,F(7^3)$ over $G\,F(7)$ in a given representation of $G\,F(7^2)$.

There exist 112 irreducible monic polynomials of degree 3 over F_7.

We shall represent F_{343} as $F_7(\alpha)$, where $\alpha^3 + 2 = 0$. Here $\alpha^7 = 4\alpha$, $\alpha^{14} = 2\alpha^2$. so that

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Further $\lambda^3 - 1 = (\lambda - 1)(\lambda - 4)(\lambda - 2)$ over F_7, so that the number of N-polynomials is $\nu(7, 3) = \frac{1}{3} \cdot 7^3(1 - \frac{1}{7})^3 = 72$.

We have

$$\varphi_1(C) = C - E = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \varphi_2(C) = C - 4E = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5 \end{pmatrix},$$

$$\varphi_3(C) = C - 2E = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

The space V_1 consists of all vectors of the form $(0, r_2, r_3)$ Analogously for V_2 and V_3. Hence the vector $\varrho = (r_1, r_2, r_3)$ is admissible if and only if $r_1 r_2 r_3 \neq 0$.

All normal bases are of the form

$$\begin{pmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix} = \begin{pmatrix} \varrho \\ \varrho C \\ \varrho C^2 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix} = \begin{pmatrix} r_1 + r_2\alpha + r_3\alpha^2 \\ r_1 + 4r_2\alpha + 2r_3\alpha^2 \\ r_1 + 2r_2\alpha + 4r_3\alpha^2 \end{pmatrix},$$

where r_1, r_2, r_3 run independently over all elements of the set $\{1, 2, \ldots, 6\}$. The vectors (r_1, r_2, r_3), $(r_1, 4r_2, 2r_3)$ and $(r_1, 2r_2, 4r_3)$ lead always to the same basis.

This result may be formulated as follows: An element $\beta = r_1 + r_2\alpha + r_3\alpha^2 \in$ $\in F_7(\alpha)$ is a generator of a normal basis of $F_7(\alpha)$ over F_7 if and only if $r_1 r_2 r_3 \neq 0$. This immediately enables to decide whether a given element $\beta \in F_7(\alpha)$ is a generator of a normal basis or not. [For large n, $n > 3$, analogous statements make unnecessary the construction of huge tables of normal bases. See Examples 9 and 10.]

We now turn to the problem to find all N-polynomials. Any N-polynomial is of the form

$$m(x) = (x - \omega_1)(x - \omega_2)(x - \omega_3) =$$
$$= [(x - r_1) - (r_2\alpha + r_3\alpha^2)]\,[(x - r_1) - (4r_2\alpha + 2r_3\alpha)]\,.$$
$$.\,[(x - r_1) - (2r_2\alpha + 4r_3\alpha^2)]\,.$$

After some calculations we obtain

$$(9)\qquad m(x) = (x - r_1)^3 - r_2r_3(x - r_1) + 2(r_2^3 - 2r_3^3)\,.$$

If $r_2r_3 = a$, then

$$2(r_2^3 - 2r_3^3) = 2\left(r_2^3 - \frac{2a^3}{r_2^3}\right) = 2\frac{1 - 2a^3}{r_2^3}\,.$$

Since $r_2^3 \pmod 7$ is either 1 or -1, we have

$$m(x) = (x - r_1)^3 - a(x - r_1) \pm 2(1 - 2a^3)\,.$$

If here r_1 and a run independently through the elements $\{1, 2, \ldots, 6\}$, we obtain all the 72 different N-polynomials (each polynomial exactly once). Such a nice result is hardly available for $n \geqq 4$.

Remark. We may use the result (9) to describe in a condensed form all the 112 irreducible polynomials of degree 3 over F_7.

The polynomial $(x - \omega_1)(x - \omega_1^7)(x - \omega_1^{49})$ is irreducible if and only if the elements $\omega_1 = r_1 + r_2\alpha + r_3\alpha^2$, $\omega_1^7 = r_1 + 4r_2\alpha + 2r_3\alpha^2$, $\omega_1^{49} = r_1 + 2r_2\alpha + 4r_3\alpha^2$ are mutually different. This is true unless $r_2 = r_3 = 0$.

Since the N-polynomials are automatically irreducible, we have only to consider the non-admissible vectors $(0, r_2, r_3)$, $(r_1, 0, r_3)$, $(r_1, r_2, 0)$ with the exception of the case $(r_1, 0, 0)$.

a) If $r_1 = 0$, $r_2r_3 \neq 0$, we have $m^{(1)}(x) = x^3 - r_2r_3x + 2(r_2^3 - 2r_3^3)$.

b) If $r_1 \in F_7$, $r_2 = 0$, $r_3 \neq 0$, we get $m^{(2)}(x) = (x - r_1)^3 + 3r_3^3$.

c) If $r_1 \in F_7$, $r_2 \neq 0$, $r_3 = 0$, we get $m^{(3)}(x) = (x - r_1)^3 + 2r_2^3$.

This gives $12 + 14 + 14 = 40$ irreducible polynomials (which are not N-polynomials).

Example 7. Consider the field $GF(3^4)$ over $GF(3)$, if $GF(3^4)$ is represented by $F_3(\alpha)$ and $\alpha^4 + \alpha + 2 = 0$.

a) There exist 18 irreducible polynomials of degree 4 over F_3. One of them is $x^4 + x + 2$.

Since $\lambda^4 - 1 = (\lambda - 1)(\lambda + 1)(\lambda^2 + 1)$ over F_3, we have $\nu(3, 4) = \frac{1}{4} \cdot 3^4 \cdot (1 - \frac{1}{3})^2 \cdot (1 - \frac{1}{9}) = 8$. Hence there are 8 different normal bases.

Using $\alpha^4 + \alpha + 2 = 0$ we get $\alpha^6 = \alpha^2 + 2\alpha^3$, $\alpha^9 = \alpha + \alpha^2 + \alpha^3$, so that

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \qquad C^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

$$\varphi_1(C) = C - E = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \qquad \varphi_2(C) = C + E = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{pmatrix},$$

$$\varphi_3(C) = C^2 + E = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 2 & 2 \end{pmatrix}.$$

To get simple descriptions of the vector spaces V_1, V_2, V_3, we use elementary row operations. It follows that V_1, V_2, V_3 are spanned by the rows of the following matrices

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 2 \end{pmatrix}.$$

The space V_1 consists of all vectors of the form $(0, r_2, r_3, r_4)$. Hence an admissible vector is necessarily of the form (r_1, r_2, r_3, r_4), $r_1 \neq 0$. Next an admissible vector (r_1, r_2, r_3, r_4) does not belong to V_2, therefore we have necessarily

$$\begin{vmatrix} r_1 & r_2 & r_3 & r_4 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{vmatrix} = r_2 + r_3 - r_4 \neq 0\,.$$

Any vector not contained in $V_1 \cup V_2$ is of the form (r_1, r_2, r_3, r_4), where $r_1 \neq 0$, $r_4 \neq r_2 + r_3$. From these 36 vectors we have to exclude the 4 vectors contained in V_3 (with $r_1 \neq 0$):

$$(1, 1, 2, 2),\ (1, 2, 1, 1),\ (2, 1, 2, 2),\ (2, 2, 1, 1)\,,$$

(which satisfy $r_4 \neq r_2 + r_3$).

We obtained the following result: An element $\beta \in F_3(\alpha)$, $\beta = r_1 + r_2\alpha + r_3\alpha^2 + r_4\alpha^3$, is a generator of a normal basis if and only if $r_1 \neq 0$, $r_4 \neq r_2 + r_3$ and $(r_2, r_3, r_4) \neq (1, 2, 2)$, $(r_2, r_3, r_4) \neq (2, 1, 1)$.

This solves, as a matter of fact, our problem since for any $\beta \in F_3(\alpha)$ we can immediately decide whether β is a generator of a normal basis or not. E.g. $\beta_1 = 1 + \alpha + 2\alpha^2 + \alpha^3$ is a generator, while $\beta_2 = 1 + 2\alpha + 2\alpha^2 + \alpha^3$ is not a generator (since $r_2 + r_3 = r_4$).

b) In the case (as our) where the number of admissible vectors is relatively small we can write down all admissible vectors. In our case the first half of them is:

$$\begin{aligned} &(1\,0\,0\,1),\ (1\,0\,2\,0),\ (1\,2\,0\,0),\ (1\,1\,2\,1)\,,\\ &(1\,0\,0\,2),\ (1\,0\,2\,1),\ (1\,2\,0\,1),\ (1\,2\,1\,2)\,,\\ &(1\,0\,1\,0),\ (1\,1\,0\,0),\ (1\,1\,1\,0),\ (1\,2\,2\,0)\,,\\ &(1\,0\,1\,2),\ (1\,1\,0\,2),\ (1\,1\,1\,1),\ (1\,2\,2\,2)\,. \end{aligned}$$

The second half is obtained by multiplying each vector by the element 2.

The rows of the matrices $M = [\varrho, \varrho C, \varrho C^2, \varrho C^3]^T$ introduced below are calculated successively as ϱC, $(\varrho C)\,C$, $(\varrho C^2)\,C$.

Put, e.g. $\varrho = (1, 0, 0, 1)$. This gives the matrix M_1. Then choose for ϱ an admissible vector which is not a row of M_1, e.g., $\varrho = (1, 1, 0, 2)$. This gives M_2. In this manner we obtain the matrices $M_1 - M_4$. Multiplying each row by 2 we get $M_5 - M_8$.

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 1 & 0 & 2 \\ 1 & 2 & 2 & 0 \\ 1 & 0 & 2 & 0 \\ 1 & 0 & 2 & 1 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 1 & 2 & 2 & 2 \\ 1 & 2 & 1 & 2 \end{pmatrix},$$

$$M_4 = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 1 & 2 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \quad M_5 = \begin{pmatrix} 2 & 0 & 0 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 1 & 2 \\ 2 & 2 & 0 & 0 \end{pmatrix}, \quad M_6 = \begin{pmatrix} 2 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \\ 2 & 0 & 1 & 0 \\ 2 & 0 & 1 & 2 \end{pmatrix},$$

$$M_7 = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 \\ 2 & 1 & 1 & 1 \\ 2 & 1 & 2 & 1 \end{pmatrix}, \quad M_8 = \begin{pmatrix} 2 & 0 & 2 & 1 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 2 & 0 \\ 2 & 0 & 2 & 0 \end{pmatrix}.$$

The normal bases Ω_i $(i = 1, 2, \ldots, 8)$ are given by $M_i\,(1, \alpha, \alpha^2, \alpha^3)^T$. I.e.

$$\Omega_1 = \begin{pmatrix} 1 + \alpha^3 \\ 1 + \alpha + \alpha^2 + \alpha^3 \\ 1 + \alpha + 2\alpha^2 + \alpha^3 \\ 1 + \alpha \end{pmatrix}, \ \ldots, \ \Omega_8 = \begin{pmatrix} 2 + 2\alpha^2 + \alpha^3 \\ 2 + \alpha + \alpha^3 \\ 2 + 2\alpha + 2\alpha^2 \\ 2 + 2\alpha^2 \end{pmatrix}.$$

c) We now turn to the problem to describe all N-polynomials. It is easy (even for $n > 4$) to write down the matrix M corresponding to the "general form" of an admissible vector (with indeterminates r_1, r_2, r_3, r_4). This is obtained by successive multiplication of the rows by C. In our case we have

$$M = \begin{pmatrix} r_1 & r_2 & r_3 & r_4 \\ r_1 & r_4 & r_3 + r_4 & r_2 + 2r_3 + r_4 \\ r_1 & r_2 + 2r_3 + r_4 & r_2 + 2r_4 & r_2 + r_3 + r_4 \\ r_1 & r_2 + r_3 + r_4 & 2r_2 + r_3 & r_2 \end{pmatrix}$$

The elements of the matrix M are always linear forms of the r_i.

Denote $\omega_1 = r_1 + r_2\alpha + r_3\alpha^2 + r_4\alpha^3, \ldots, \omega_4 = r_1 + (r_2 + r_3 + r_4)\,\alpha + (2r_2 + r_3)\,\alpha^2 + r_2\alpha^3$. What is technically by far not easy is to calculate the product $(x - \omega_1) \ldots (x - \omega_4)$ (with indeterminates r_i).

But for any specified admissible vector (r_1, r_2, r_3, r_4) the corresponding N-polynomial can be obtained as the minimal polynomial of $\beta = r_1 + r_2\alpha + r_3\alpha^2 + r_4\alpha^3$ by a well known general procedure (see, e.g., [4]).

Consider, e.g., Ω_2 and the third row $\beta = 1 + 2\alpha^2$. (Recall that all rows of Ω_i have the same minimal polynomial.) We compute

$$\begin{aligned} 1 &= 1\,, \\ \beta &= 1 + 2\alpha^2\,, \end{aligned}$$

$$\beta^2 = 2 + 2\alpha + \alpha^2 ,$$
$$\beta^3 = 1 + 2\alpha^2 + \alpha^3 ,$$
$$\beta^4 = 2 + \alpha + 2\alpha^2 + \alpha^3 .$$

Then the coefficients of the monic minimal polynomial $m(x) = b_0 + b_1x + b_2x^2 + + b_3x^3 + x^4$ are given as the solution of

$$(b_0, b_1, b_2, b_3, 1) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 2 & 2 & 1 & 0 \\ 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 1 \end{pmatrix} = (0, 0, 0, 0) .$$

This gives $(b_0, b_1, b_2, b_3, 1) = (2, 1, 1, 2, 1)$ and $m(x) = 2 + x + x^2 + 2x^3 + x^4$.

Denote by $m_i(x)$ the minimal polynomial corresponding to the rows of M_i. In our example we obtain:

$$m_1(x) = 2 + 2x^3 + x^4 , \qquad m_5(x) = 2 + x^3 + x^4 ,$$
$$m_2(x) = 2 + x + x^2 + 2x^3 + x^4 , \qquad m_6(x) = 2 + 2x + x^2 + x^3 + x^4 ,$$
$$m_3(x) = 1 + x + 2x^3 + x^4 , \qquad m_7(x) = 1 + 2x + x^3 + x^4 ,$$
$$m_4(x) = 1 + 2x + x^2 + 2x^3 + x^4 , \qquad m_8(x) = 1 + x + x^2 + x^3 + x^4 .$$

These are the eight N-polynomials of degree 4 over F_3.

Remark 1. It is of course not necessary always to use the general method applied above to find the minimal polynomials.

Consider, e.g., the basis Ω_1 and $\beta = 1 + \alpha$. Then $\alpha^4 + \alpha + 2 = 0$ implies $(\beta - 1)^4 + (\beta - 1) + 2 = 0$, i.e. $\beta^4 + 2\beta^3 + 2 = 0$ which immediately gives $m_1(x)$.

M_5 contains the same rows as M_1 multiplicated by 2. We have $\beta = 1 + \alpha^3 \in \Omega_1$, $\beta_1 = 2\beta = 2 + 2\alpha^3 \in \Omega_5$. Now $2 + 2\beta^3 + \beta^4 = 0$ implies $2 + 2 . (\frac{1}{2}\beta_1)^3 + + (\frac{1}{2}\beta_1)^4 = 0$ which gives $m_5(x)$. Knowing $m_2(x), m_3(x), m_4(x)$ we obtain in the same manner $m_6(x), m_7(x)$ and $m_8(x)$.

Remark 2. The polynomial $x^4 + x + 2$ over $GF(3)$ is a primitive polynomial. Hence all non-zero elements of $F_3(\alpha)$ can be represented by the sequence $\{\alpha, \alpha^2, \alpha^3, \ldots \ldots, \alpha^{40} = 2, \ldots, \alpha^{79}, \alpha^{80} = 1\}$.

In the following $[u_0, u_1, u_2, u_3]$ will denote $u_0 + u_1\alpha + u_2\alpha^2 + u_3\alpha^3$, and we shall freely consider Ω as a vector as well as a set of elements.

We compute

$$\alpha = [0, 1, 0, 0] , \quad \alpha^2 = [0, 0, 1, 0] , \quad \alpha^3 = [0, 0, 0, 1] , \quad \alpha^4 = [1, 2, 0, 0] .$$

Since $\alpha^4 \in \Omega_3$, we may write $\Omega_3 = \{\alpha^4, \alpha^{12}, \alpha^{36}, \alpha^{108}\} = \{\alpha^4, \alpha^{12}, \alpha^{36}, \alpha^{28}\}$. Since $\Omega_7 = 2\Omega_3$ and $2 = \alpha^{40}$, we have $\Omega_7 = \{\alpha^{44}, \alpha^{52}, \alpha^{76}, \alpha^{68}\}$.

Further computing gives:

$$\alpha^5 = [0, 1, 2, 0]\,, \quad \alpha^6 = [0, 0, 1, 2]\,, \quad \alpha^7 = [2, 1, 0, 1]\,, \quad \alpha^8 = [1, 1, 1, 0]\,.$$

Hence $\Omega_4 = \{\alpha^8, \alpha^{24}, \alpha^{72}, \alpha^{56}\}$ and $\Omega_8 = \{\alpha^{48}, \alpha^{64}, \alpha^{32}, \alpha^{16}\}$.

Analogously we obtain: $\Omega_2 = \{\alpha^{11}, \alpha^{33}, \alpha^{19}, \alpha^{57}\}$, $\Omega_6 = \{\alpha^{51}, \alpha^{73}, \alpha^{59}, \alpha^{17}\}$, $\Omega_5 = \{\alpha^{13}, \alpha^{39}, \alpha^{37}, \alpha^{31}\}$, $\Omega_1 = \{\alpha^{53}, \alpha^{79}, \alpha^{77}, \alpha^{71}\}$.

This "multiplicative representation" of normal bases has been used in [10] (and reproduced in [4]), where of course, many other informations concerning finite fields are included.

If we are interested only in normal bases, the result obtained in a) replaces a tabulation since it enables to decide immediately whether a given $\beta \in F_{81}$ (written in its usual form) is a generator of a normal basis or not.

Example 8. Consider the field $GF(2^6)$ as extension of degree 3 over $GF(2^2)$.

a) The number of irreducible polynomials of degree 3 over F_4 is $J(4, 3) = 20$.

We represent the field F_4 by means of the irreducible polynomial $x^2 + x + 1$ over F_2. We have $F_4 = \{0, 1, b, b^2\}$, where $b^2 + b + 1 = 0$. Over F_4 the polynomial $\lambda^3 - 1$ splits into three factors: $\lambda^3 - 1 = (\lambda - 1)(\lambda - b)(\lambda - b^2)$. The number of N-polynomials is $\nu(4, 3) = \frac{1}{3} \,.\, 4^3(1 - \frac{1}{4})^3 = 9$.

We now choose an irreducible polynomial of degree 3 over F_4, e.g., $f(x) = x^3 + x + 1$, and represent F_{64} as $F_4(\alpha)$, where $\alpha^3 + \alpha + 1 = 0$. Hence all elements of $F_4(\alpha)$ are of the form $u_0 + u_1\alpha + u_2\alpha^2$, where $u_i \in F_4$.

Recall that the generator of the Galois group is now $g: \alpha \to \alpha^q = \alpha^4$. We have $\alpha^4 = \alpha + \alpha^2$ and $\alpha^8 = \alpha$ so that

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Further

$$\varphi_1(C) = C - E = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \varphi_2(C) = C - bE = \begin{pmatrix} b^2 & 0 & 0 \\ 0 & b^2 & 1 \\ 0 & 1 & b \end{pmatrix},$$

$$\varphi_3(C) = C - b^2E = \begin{pmatrix} b & 0 & 0 \\ 0 & b & 1 \\ 0 & 1 & b^2 \end{pmatrix}.$$

The spaces V_i (over F_4) are spanned by the rows of the following matrices

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & b & 1 \end{pmatrix}$$

A vector $\varrho = (r_1, r_2, r_3)$ $(r_i \in F_4)$ is admissible if and only if

$$\begin{vmatrix} r_1 & r_2 & r_3 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{vmatrix} = r_1 \neq 0\,, \quad \begin{vmatrix} r_1 & r_2 & r_2 \\ 1 & 0 & 0 \\ 0 & 1 & b \end{vmatrix} = r_3 + br_2 \neq 0\,, \quad \begin{vmatrix} r_1 & r_2 & r_3 \\ 1 & 0 & 0 \\ 0 & b & 1 \end{vmatrix} = br_3 + r_2 \neq 0\,.$$

Hence (r_1, r_2, r_3) is admissible if and only if $r_1 \neq 0$, $r_3 \neq br_2$, $r_3 \neq b^2r_2$.

This implies the following result: An element $\beta = r_1 + r_2\alpha + r_3\alpha^2$ $[r_i \in F_2(b)]$ is a generator of a normal basis of $F_4(\alpha)$ over $F_2(b)$ if and only if $r_1 \neq 0$, $r_3 \neq br_2$, $r_3 \neq b^2 r_2$.

This immediately enables to decide whether a given β is a generator of a normal basis or not. E.g., $\beta = 1 + b\alpha + b\alpha^2$ is a generator, while $\beta' = 1 + b\alpha + b^2\alpha$ is not a generator of a normal basis.

b) The admissible vectors in which $r_1 = 1$ are the following 9 vectors:

$$(10) \qquad \begin{matrix} (1,\ 0,\ 1)\,, & (1,\ 1,\ 0)\,, & (1,\ b,\ b)\,, \\ (1,\ 0,\ b)\,, & (1,\ 1,\ 1)\,, & (1,\ b^2.\ 0)\,, \\ (1,\ 0,\ b^2)\,, & (1,\ b,\ 0)\,, & (1,\ b^2,\ b^2)\,. \end{matrix}$$

The remaining 18 admissible vectors are obtained by multiplyning all the vectors in (10) by b and b^2 respectively.

The matrices $M = (\varrho, \varrho C, \varrho C^2)^T$ coresponding to the vectors in (10) are

$$M_1 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 0 & b \\ 1 & b & 0 \\ 1 & b & b \end{pmatrix}, \quad M_3 = \begin{pmatrix} 1 & 0 & b^2 \\ 1 & b^2 & 0 \\ 1 & b^2 & b^2 \end{pmatrix}.$$

Hence we obtain the normal bases

$$\Omega_1 = \begin{pmatrix} 1 + \alpha^2 \\ 1 + \alpha \\ 1 + \alpha + \alpha^2 \end{pmatrix}, \quad \Omega_2 = \begin{pmatrix} 1 + b\alpha^2 \\ 1 + b\alpha \\ 1 + b\alpha + b\alpha^2 \end{pmatrix}, \quad \Omega_3 = \begin{pmatrix} 1 + b^2\alpha^2 \\ 1 + b^2\alpha \\ 1 + b^2\alpha + b^2\alpha^2 \end{pmatrix}.$$

The remaining bases $\Omega_4 - \Omega_9$ are obtained by multiplying $\Omega_1, \Omega_2, \Omega_3$ by b and b^2 respectively.

c) To obtain the minimal polynomial $m_1(x)$ of $\beta = 1 + \alpha$ it is sufficient to insert $\alpha = \beta + 1$ into $x^3 + x + 1 = 0$. This gives $\beta^3 + \beta^2 + 1 = 0$. Hence $m_1(x) = x^3 + x^2 + 1$. Analogously we obtain $m_2(x) = x^3 + x^2 + bx + b^2$ and $m_3(x) = x^3 + x^2 + b^2x + b$.

Replacing in $m_1(x)$, $m_2(x)$, $m_3(x)$ the term x by the term bx we obtain

$$\begin{aligned} m_4(x) &= x^3 + b^2x^2 + 1\,, \\ m_5(x) &= x^2 + b^2x^2 + b^2x + b^2\,, \\ m_6(x) &= x^3 + b^2x^2 + x + b\,. \end{aligned}$$

Finally replacing in $m_1(x)$, $m_2(x)$, $m_3(x)$ the term x by b^2x we get

$$\begin{aligned} m_7(x) &= x^3 + bx^2 + 1\,, \\ m_8(x) &= x^3 + bx^2 + x + b^2\,, \\ m_9(x) &= x^3 + bx^2 + bx + b\,. \end{aligned}$$

The polynomials $m_1(x), \ldots, m_9(x)$ are all N-polynomials of degree 3 over F_4.

Example 9. Find all normal bases of $GF(3^6)$ over $GF(3)$ if $GF(3^6)$ is represented as $F_3(\alpha)$, where $\alpha^6 + \alpha + 2 = 0$.

There exist 116 irreducible polynomials of degree 6 over F_3. The polynomial $x^6 + x + 2$ is one of them.

Since $\lambda^6 - 1 = (\lambda - 1)^3 (\lambda + 1)^3$ over F_3, there exist $\nu(3, 6) = \frac{1}{6} . 3^6(1 - \frac{1}{3})^2 = 54$ normal bases of E_{729} over F_3.

We have $\alpha^0 = 1$, $\alpha^3 = \alpha^3$, $\alpha^6 = 1 + 2\alpha$, $\alpha^9 = \alpha^3 + 2\alpha^4$, $\alpha^{12} = 1 + \alpha + \alpha^2$ and $\alpha^{15} = \alpha^3 + \alpha^4 + \alpha^5$. Therefore

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

$$\varphi_1(C) = C - E = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 2 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 1 & 1 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}, \quad \varphi_2(C) = C + E = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{pmatrix}.$$

The matrix $C - E$ is of rank 5, hence V_1 has dimension 5 and it is immediately seen that V_1 consists of all vectors $\varrho = (r_1, r_2, r_3, r_4, r_5, 0)$, where $r_1, \ldots, r_5$ run independently over all elements of F_3.

By elementary row transformations we find that the vectors contained in V_2 are of the form

$$(r_1, r_2, r_3, r_4, r_4 - r_2 - r_3, r_6)$$

where r_1, r_2, r_3, r_4 and r_6 run independently over all elements of F_3. (Hence V_2 is again of dimension 5.)

The admissible row vectors are all vectors $\varrho = (r_1, r_2, \ldots, r_6)$, where $r_6 \neq 0$ and $r_5 \neq r_4 - r_2 - r_3$.

Hence an element $\beta = r_1 + r_2\alpha + r_3\alpha^2 + r_4\alpha^3 + r_5\alpha^4 + r_6\alpha^5 \in F_3(\alpha)$ is a generator of a normal basis over F_3 if and only if $r_6 \neq 0$ and $r_5 \neq r_4 - r_2 - r_3$.

This statement enables again to decide immediately whether a given $\beta \in F_3(\alpha)$ generates a normal basis or not.

The admissible vectors are the vectors

$$\varrho = (r_1, r_2, r_3, r_4, r_4 - r_2 - r_3 + a, r_6),$$

where r_1, r_2, r_3, r_4 run independently over $F_3 = \{0, 1, 2\}$ while a and r_6 run independently over the set $\{1, 2\}$. This gives $3^4 . 2^2 = 324$ admissible vectors. Since always 6 vectors give the same normal basis we obtain indeed 54 different normal bases.

If we take, e.g., $\varrho_1 = (0, 0, 0, 0, 1, 1)$, which is an admissible vector, we get (by succesive multiplication by C) the normal basis

$$\Omega_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 2 & 0 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 & 0 & 1 \\ 0 & 2 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \\ \alpha^5 \end{pmatrix}$$

The remaining 53 normal bases are obtained in the same way.

Example 10. Rather simple results are obtained if the degree is a power of the characteristic. Consider the case $GF(5^5)$ over $GF(5)$.

There are 624 irreducible polynomials of degree 5 over F_5. One of them is $f(x) = x^5 + 4x + 1$. Since $\lambda^5 - 1 \equiv (\lambda - 1)^5 \pmod 5$, there exist $\frac{1}{5} \cdot 5^5(1 - \frac{1}{5}) = 500$ normal bases. If α satisfies $f(\alpha) = 0$, we have $\alpha^0 = 1$, $\alpha^5 = 4 + \alpha$, $\alpha^{10} = 1 + 3\alpha + \alpha^2$, $\alpha^{15} = 4 + 3\alpha + 2\alpha^2 + \alpha^3$, $\alpha^{20} = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$.

Hence

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 4 & 1 & 0 & 0 & 0 \\ 1 & 3 & 1 & 0 & 0 \\ 4 & 3 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \qquad C - E = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 \\ 4 & 3 & 2 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

The vector space V spanned by the rows of $C - E$ consists of all vectors of the form $(r_1, r_2, r_3, r_4, 0)$ $(r_i \in F_5)$. The admissible vectors are the $5^4 \cdot 4 = 2500$ vectors of form $(r_1, r_2, r_3, r_4, r_5)$, where $r_5 \neq 0$. This implies:

An element $\beta = r_1 + r_2\alpha + r_3\alpha^2 + r_4\alpha^3 + r_5\alpha^4 \in F_5(\alpha)$ is a generator of a normal basis of $F_5(\alpha)$ over F_5 if and only if $r_5 \neq 0$.

It follows, e.g., that α^4 is generator of a normal basis, and this basis is $(\alpha^4, \alpha^{20}, \alpha^{100}, \alpha^{500}, \alpha^{2500})$. It is of course by far simpler to use our method and to compute $(0\ 0\ 0\ 0\ 1)\, C^i$, for $i = 1, 2, 3, 4$. We obtain

$$\Omega = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 & 1 \\ 1 & 2 & 4 & 3 & 1 \\ 0 & 4 & 1 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \end{pmatrix}.$$

The corresponding N-polynomial (i.e. the minimal polynomial of α^4) is $m(x) = 4 + x + x^2 + x^3 + x^4 + x^5$.

References

[1] *Albert, A. A.:* Fundamental Concepts of Higher Algebra, The Univ. of Chicago Press, 1956.

[2] *Berlekamp, E. R.:* Algebraic Coding Theory, Mc. Graw-Hill Company, New York, 1968.

[3] *Jacobson, N.:* Lectures in Abstract Algebra, D. Van Nostrand Comp., New York, Volume III, 1964.

[4] *Lidl, R.* and *Niederreiter, H.:* Finite Fields, Addison-Wesley Publ. Comp., Reading, Massachusetts, 1983.

[5] *Ore, O.:* Contributions to the theory of finite fields. Trans. Amer. Mat. Soc. *36* (1934), 243—274.

[6] *Rédei, L.:* Algebra, Akad. Verlagsgesellschaft, Leipzig 1959.

[7] *Schwarz, Š.:* On the reducibility of binomial congruences and the bound of the least integer belonging to a given exponent (mod p). Časopis pěst. mat. fys. *74* (1949), 1—16.

[8] *Schwarz, Š.:* On the reducibility of polynomials over a finite field. Quart. J. of Math. (Oxford) (2) *7* (1956), 110—124.

[9] *Van der Waerden, B. L.:* Algebra I (1971) and II (1967) (Russian edition, 1976).

[10] *Conway, J. H.:* A tabulation of some information concerning finite fields. Computers in Mathematical Research, pp. 37—50, North-Holland, Amsterdam, 1968.

Author's address: 814 73 Bratislava, Obrancov mieru 49, Czechoslovakia (Matematický ústav SAV).