

Exemples d'éléments normaux et de polynômes normaux

1 Le cas de l'extension \mathbb{F}_{16} de \mathbb{F}_2

Le nombre de polynômes à coefficients dans \mathbb{F}_2 , irréductibles de degré 4 est

$$I_2(4) = 3.$$

Le nombre de polynômes primitifs est

$$J_2(4) = 2.$$

Le nombre de polynômes normaux est

$$V_2(4) = 2.$$

Pour faire les calculs on utilisera comme polynôme minimal le polynôme $P(X) = X^4 + X^3 + 1$. On note α la classe de X .

Les 4 polynômes irréductibles sont

1.1 $R_1(X) = X^4 + X^3 + X^2 + X + 1$

dont les racines sont

$$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9.$$

Ces racines sont linéairement indépendantes. Donc $R_1(X)$ est normal (mais pas primitif).

1.2 $R_2(X) = X^4 + X^3 + 1$

dont les racines sont

$$\alpha, \alpha^2, \alpha^4, \alpha^8.$$

Ces racines sont linéairement indépendantes. Donc $R_2(X)$ est normal (et primitif).

1.3 $R_3(X) = X^4 + X + 1$

dont les racines sont

$$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}.$$

Ces racines ne sont pas linéairement indépendantes. Donc $R_3(X)$ n'est pas normal (mais primitif).

1.4 Matrice de la multiplication

Considérons la base normale $\alpha, \alpha^2, \alpha^4, \alpha^8$ et écrivons la matrice de la multiplication par α dans cette base.

$$M_\alpha = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

On a $C_N = 9$.

Considérons maintenant la base normale

$$\beta = \alpha^3, \beta^2 = \alpha^6, \beta^4 = \alpha^{12}, \beta^8 = \alpha^9.$$

Dans cette base la matrice de la multiplication par β est

$$M_\beta = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Cette fois-ci $C_N = 7 = 2m - 1$, la base est optimale.