

Teorema (Existencia de bases normales) Para cualquier cuerpo finito K y cualquier extensión finita F de K existe una base normal de F sobre K .

Querramos ahora entender cuándo un conjunto dado de m elementos de F (una extensión finita de grado m de K), digamos

$$B = \{\alpha_1, \dots, \alpha_m\}$$

es una base de F sobre K .

Def: Sea $K = \mathbb{F}_q$ y $F = \mathbb{F}_{q^m}$ y sea $B = \{\alpha_1, \dots, \alpha_m\}$

un conjunto con m elementos de F . El discriminante

$$\Delta_{F/K}(\alpha_1, \dots, \alpha_m)$$

se define como

$$\Delta_{F/K}(\alpha_1, \dots, \alpha_m) =$$

$$\begin{vmatrix} \text{Tr}_{F/K}(\alpha_1 \alpha_1) & \text{Tr}_{F/K}(\alpha_1 \alpha_2) & \dots & \text{Tr}_{F/K}(\alpha_1 \alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \text{Tr}_{F/K}(\alpha_m \alpha_1) & \text{Tr}_{F/K}(\alpha_m \alpha_2) & \dots & \text{Tr}_{F/K}(\alpha_m \alpha_m) \end{vmatrix}$$

Es decir es el determinante de la matriz de $m \times m$ cuyas entradas son $a_{ij} = \text{Tr}_{F/K}(\alpha_i \alpha_j)$

De la definición, tenemos que $\Delta_{F/k}(\alpha_1, \dots, \alpha_m)$ es un elemento de k .

El siguiente resultado nos da un criterio que nos permite determinar cuando un conjunto $B = \{\alpha_1, \dots, \alpha_m\}$ es una base.

Teorema: Si $\alpha_1, \dots, \alpha_m \in F$, el conjunto $B = \{\alpha_1, \dots, \alpha_m\}$ es una base de F sobre un subcuerpo k si y solo si $\Delta_{F/k}(\alpha_1, \dots, \alpha_m) \neq 0$.

$[F:k] = m$

Demostración

$\Rightarrow$) Supongamos que $B = \{\alpha_1, \dots, \alpha_m\}$ es una base de F sobre k . Vamos a probar que las filas de la matriz que define al discriminante son l.i.

Sean $c_1, \dots, c_m \in k$ tales que

$$c_1 \begin{pmatrix} \text{Tr}_{F/k}(\alpha_1 \cdot \alpha_1) \\ \text{Tr}_{F/k}(\alpha_1 \cdot \alpha_2) \\ \vdots \\ \text{Tr}_{F/k}(\alpha_1 \cdot \alpha_m) \end{pmatrix}^t + c_2 \begin{pmatrix} \text{Tr}_{F/k}(\alpha_2 \cdot \alpha_1) \\ \text{Tr}_{F/k}(\alpha_2 \cdot \alpha_2) \\ \vdots \\ \text{Tr}_{F/k}(\alpha_2 \cdot \alpha_m) \end{pmatrix}^t + \dots + c_m \begin{pmatrix} \text{Tr}_{F/k}(\alpha_m \cdot \alpha_1) \\ \text{Tr}_{F/k}(\alpha_m \cdot \alpha_2) \\ \vdots \\ \text{Tr}_{F/k}(\alpha_m \cdot \alpha_m) \end{pmatrix}^t = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$\uparrow$
fila 1
 $\uparrow$
fila 2

$$c_1 \operatorname{Tr}_{F/K}(\alpha_1 \alpha_j) + c_2 \operatorname{Tr}_{F/K}(\alpha_2 \alpha_j) + \dots + c_m \operatorname{Tr}_{F/K}(\alpha_m \alpha_j) = 0$$

para todo $j = 1, \dots, m$.

Consideremos $\beta = c_1 \alpha_1 + \dots + c_m \alpha_m \in F$ y para este β tenemos

$$\operatorname{Tr}_{F/K}(\beta \cdot \alpha_j) = 0 \quad \text{para cualquier } j = 1, \dots, m$$

Pero entonces como α_j forman una base, si $\gamma \in F$
 $\gamma = b_1 \alpha_1 + \dots + b_m \alpha_m$

$$\begin{aligned} \operatorname{Tr}_{F/K}(\beta \cdot \gamma) &= \operatorname{Tr}_{F/K}(\beta b_1 \alpha_1 + \dots + \beta b_m \alpha_m) = \\ &= b_1 \operatorname{Tr}_{F/K}(\beta \alpha_1) + \dots + b_m \operatorname{Tr}_{F/K}(\beta \alpha_m) \\ &= 0 \quad \forall \gamma \in F. \end{aligned}$$

Esto solo es posible si $\beta \cdot \gamma = 0 \Rightarrow \boxed{\beta = 0}$

Pero entonces $0 = \beta = c_1 \alpha_1 + \dots + c_m \alpha_m$ y como $\{\alpha_1, \dots, \alpha_m\}$ es base $\Rightarrow \alpha_1, \dots, \alpha_m$ son l.i. y debe ser que $c_1 = c_2 = \dots = c_m = 0$.

Luego, las filas de la matriz que definen al $\Delta_{F/k}(\alpha_1, \dots, \alpha_m)$ son l.i. y por lo tanto $\Delta_{F/k}(\alpha_1, \dots, \alpha_m) \neq 0$

$\Leftarrow$) Supongamos ahora $\Delta_{F/k}(\alpha_1, \dots, \alpha_m) = 0$. Sean $c_1, \dots, c_m \in k$ tales que

$$c_1 \alpha_1 + \dots + c_m \alpha_m = 0.$$

Multiplicamos por α_j y aplicando lo $\text{Tr}_{F/k}$ tenemos

$$c_1 \alpha_1 \alpha_j + \dots + c_m \alpha_m \alpha_j = 0$$

$$\text{Tr}_{F/k}(\quad) = \text{Tr}_{F/k}(0)$$

$$c_1 \text{Tr}_{F/k}(\alpha_1 \alpha_j) + \dots + c_m \text{Tr}_{F/k}(\alpha_m \alpha_j) = 0 \quad j = 1, \dots, m$$

$$c_1 \begin{pmatrix} \text{Tr}_{F/k}(\alpha_1 \alpha_1) \\ \text{Tr}_{F/k}(\alpha_1 \alpha_2) \\ \vdots \\ \text{Tr}_{F/k}(\alpha_1 \alpha_m) \end{pmatrix} + \dots + c_m \begin{pmatrix} \text{Tr}_{F/k}(\alpha_m \alpha_1) \\ \text{Tr}_{F/k}(\alpha_m \alpha_2) \\ \vdots \\ \text{Tr}_{F/k}(\alpha_m \alpha_m) \end{pmatrix} = \vec{0}$$

$\uparrow$ fila 1 $\uparrow$ fila m

Como las anteriores son las filas de la matriz que define el discriminante y $\Delta_{F/k}(\alpha_1, \dots, \alpha_m) \neq 0 \Rightarrow$ las filas son l.i. $\Rightarrow c_1 = c_2 = \dots = c_m = 0$. y por lo tanto $\alpha_1, \dots, \alpha_m$ son l.i. $\Rightarrow \mathcal{B} = \{\alpha_1, \dots, \alpha_m\}$ es base. 

Corolario: Sean $\alpha_1, \dots, \alpha_m \in F$, $[F:k]=m$ entonces $B = \{\alpha_1, \dots, \alpha_m\}$ es una base de F/k si y solo si

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \alpha_1^p & \alpha_2^p & & \alpha_m^p \\ \vdots & \vdots & & \vdots \\ \alpha_1^{p^{m-1}} & \alpha_2^{p^{m-1}} & & \alpha_m^{p^{m-1}} \end{vmatrix} \neq 0$$

Demostración

Sea $A = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \alpha_1^p & \alpha_2^p & & \alpha_m^p \\ \vdots & \vdots & & \vdots \\ \alpha_1^{p^{m-1}} & \alpha_2^{p^{m-1}} & & \alpha_m^{p^{m-1}} \end{pmatrix}$

Entonces

$$\begin{aligned} A^T \cdot A &= \begin{pmatrix} \alpha_1 & \alpha_1^p & \dots & \alpha_1^{p^{m-1}} \\ \alpha_2 & \alpha_2^p & \dots & \alpha_2^{p^{m-1}} \\ \vdots & \vdots & & \vdots \\ \alpha_m & \alpha_m^p & \dots & \alpha_m^{p^{m-1}} \end{pmatrix} \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \alpha_1^p & \alpha_2^p & & \alpha_m^p \\ \vdots & \vdots & & \vdots \\ \alpha_1^{p^{m-1}} & \alpha_2^{p^{m-1}} & & \alpha_m^{p^{m-1}} \end{pmatrix} \\ &= \begin{pmatrix} \alpha_1^2 + (\alpha_1^2)^p + \dots + (\alpha_1^2)^{p^{m-1}} & \dots & \alpha_1 \alpha_m + (\alpha_1 \alpha_m)^p + \dots + (\alpha_1 \alpha_m)^{p^{m-1}} \\ \vdots & & \vdots \\ \text{Tr}_{F/k}(\alpha_i \alpha_1) & \dots & \text{Tr}_{F/k}(\alpha_i \alpha_m) \\ \vdots & & \vdots \\ \text{Tr}_{F/k}(\alpha_i \alpha_j) & & \end{pmatrix} \\ &= \begin{pmatrix} \text{Tr}_{F/k}(\alpha_i \alpha_j) \end{pmatrix} \end{aligned}$$

$$\begin{aligned}
 \Delta_{\mathbb{F}_K}(\alpha_1, \dots, \alpha_m) &= \det \left(\text{Tr}_{\mathbb{F}_K}(\alpha_i \alpha_j) \right) = \det(A^T \cdot A) \\
 &= \det(A^T) \cdot \det(A) \\
 &= \det(A) \cdot \det(A) \\
 &= \det(A)^2
 \end{aligned}$$

Ejercicio: Considera $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ con $\alpha^3 + \alpha^2 + 1 = 0$

y las bases polinómicas $\{1, \alpha, \alpha^2\}$ y normal

$\{\alpha, \alpha^2, \alpha^4\} = \{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$ y calcula

el discriminante en ambos casos.

$$\Delta_{\mathbb{F}_8/\mathbb{F}_2}(1, \alpha, \alpha^2) = \begin{vmatrix} \text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(1 \cdot 1) & \text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(1 \cdot \alpha) & \text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(1 \cdot \alpha^2) \\ \text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha \cdot 1) & \text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha \cdot \alpha) & \text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha \cdot \alpha^2) \\ \text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha^2 \cdot 1) & \text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha^2 \cdot \alpha) & \text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha^2 \cdot \alpha^2) \end{vmatrix}$$

Ejercicio: Calcular todas las bases normales de $\mathbb{F}_8$ sobre $\mathbb{F}_2$, donde

$$\mathbb{F}_8 = \mathbb{F}_2(\alpha)$$

$$[\mathbb{F}_8 : \mathbb{F}_2] = 3$$

$$\alpha^3 + \alpha^2 + 1 = 0.$$

Raíces de la unidad

Para un positivo n , el polinomio $x^n - 1$ tiene muchas propiedades especiales, por ejemplo: $x^n - 1$ es el polinomio mínimo del automorfismo de Frobenius que genera el grupo de Galois de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Queremos investigar el cuerpo de descomposición de este polinomio sobre un cuerpo k , denotado por $k^{(n)}$ que se llama el n -ésimo cuerpo ciclotómico sobre k .

$$k = \mathbb{F}_q$$

Definición: Los raíces $\alpha_1, \dots, \alpha_n \in k^{(n)} \subset \mathbb{F}_{q^n}$ del polinomio $x^n - 1 \in k[x]$ se llaman n -ésimas raíces de la unidad sobre k .

$$\mathbb{F} = \mathbb{F}_q^n$$

Sea U_n (en el libro $\mathbb{F}^{(n)}$) el conjunto formado por todas las raíces n -ésimas de la unidad sobre k .

$$k^{(n)} = \mathbb{F}_q^{(n)}$$

$$k = \mathbb{F}_q$$

Ejercicio: Probar que U_n es un grupo multiplicativo.

Teorema: Sea n un entero positivo y $K = \mathbb{F}_q$ un cuerpo de característica p .

(1) si p no divide a n , entonces U_n es un grupo multiplicativo cíclico (con la multiplicación en $\mathbb{F}_q^*$) de orden n .

(2) si p divide a n y $n = m \cdot p^e$ con $\text{mcd}(m, p) = 1$ entonces

$$x^n - 1 = (x^m - 1)^{p^e}$$

y los raíces n -ésimas de la unidad son raíces m -ésimas de la unidad con multiplicidad p^e .

Def: Si p no divide a n y α es un generador del grupo cíclico U_n , es decir, $U_n = \langle \alpha \rangle$ entonces α se llama una raíz n -ésima primitiva de la unidad.

Ejercicios de la página 71 del libro de Lidl y Niederreiter:

2.9 (Ayuda: mirar la prueba del Teorema 2.8: $\mathbb{F}_q^*$ es cíclico)

2.12

2.13.

$$\mathbb{F}/\mathbb{K}$$

$$[\mathbb{F} : \mathbb{K}] = m$$

$$\alpha^3 + \alpha^2 + 1 = 0$$

$$\text{Tr}_{\mathbb{F}/\mathbb{K}}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \dots + \alpha^{q^{m-1}}$$

$$\mathbb{F}_8/\mathbb{F}_2$$

$$[\mathbb{F}_{2^3} : \mathbb{F}_2] = 3$$

$$q=2 \quad m=3$$

$$\text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} = \alpha + \alpha^2 + \alpha^4$$

$$\text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(1) = 1$$

$$\alpha^3 = \alpha^2 + 1$$

$$\alpha^4 = \alpha^3 + \alpha$$

$$\alpha^4 = \alpha^2 + 1 + \alpha$$

$$\text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha) = \alpha + \alpha^2 + \alpha^4 = \alpha + \alpha^2 + \cancel{\alpha^2} + \cancel{\alpha} + 1 = 1.$$

$$\text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha^2) = \text{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha) = 1.$$

$$\alpha \in \mathbb{F} = \mathbb{F}_{q^m}$$

$$\alpha^{q^m} = \alpha$$

$$\text{Tr}_{\mathbb{F}/\mathbb{K}}(\alpha) = \underbrace{\alpha + \alpha^q + \dots + \alpha^{q^{m-1}}}_{\alpha^{q^m}} = (\alpha^q) + \dots + (\alpha^q)^{q^{m-2}} + (\alpha^q)^{q^{m-1}} = \text{Tr}_{\mathbb{F}/\mathbb{K}}(\alpha^q)$$