

Teorema: Para $\beta \in F$ sea L_β la aplicación que manda $\alpha \mapsto \text{Tr}_{F/K}(\beta \cdot \alpha)$ es decir

$$L_\beta: F \longrightarrow K \\ \alpha \mapsto \text{Tr}_{F/K}(\beta \cdot \alpha)$$

es una transformación lineal que satisface que $L_\beta \neq L_\gamma$ si $\beta \neq \gamma$. Mas aún, todas las transformaciones lineales sobre K de F a K son exactamente los L_β donde β varía en F .

Demostración

Por el teorema anterior tenemos que L_β es una transformación lineal de F en K , para cualquier $\beta \in F$.

Si β y γ son dos elementos distintos de F , entonces

$$\begin{aligned} L_\beta(\alpha) - L_\gamma(\alpha) &= \text{Tr}_{F/K}(\beta \cdot \alpha) - \text{Tr}_{F/K}(\gamma \cdot \alpha) = \text{Tr}_{F/K}(\beta\alpha - \gamma\alpha) \\ &= \text{Tr}_{F/K}((\beta - \gamma) \cdot \alpha) \neq 0 \quad \text{por algún} \end{aligned}$$

α adecuado. Entonces L_β y L_γ son distintos si $\beta \neq \gamma$

Ahora para ver que son todos, si $k = \mathbb{F}_q$ y $F = \mathbb{F}_{q^m}$ entonces tenemos q^m transformaciones L_β , $\beta \in F$.
distintos.

Por otro lado, cada T.L. de F en k puede obtenerse asignando elementos arbitrarios de k a los m elementos de una base dada de F sobre k . y como esto puede hacerse de q^m maneras, entonces $\hookrightarrow L_\beta$ ya son todos. 

Teorema: Sea F una extensión finita de $k = \mathbb{F}_q$.

Entonces para $\alpha \in F$ tenemos que

$$\text{Tr}_{F/k}(\alpha) = 0 \text{ si y solo si } \alpha = \beta^q - \beta \text{ para algún } \beta \in F.$$

Demostración

$\Leftarrow$) Si $\alpha = \beta^q - \beta$ entonces

$$\text{Tr}_{F/k}(\alpha) = \text{Tr}_{F/k}(\beta^q - \beta) = \underbrace{\text{Tr}_{F/k}(\beta^q)}_{\text{"Tr}_{F/k}(\beta)" } - \text{Tr}_{F/k}(\beta) = 0$$

$\Rightarrow$) Supongamos que $\alpha \in F = \mathbb{F}_{q^m}$ tal que $\text{Tr}_{F/k}(\alpha) = 0$

y sea β una raíz de $X^q - X - \alpha$ en alguna extensión de F . Entonces $\beta^q - \beta - \alpha = 0$
 $\alpha = \beta^q - \beta$

$$\begin{aligned}
0 &= \text{Tr}_{\mathbb{F}/k}(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{m-1}} = \\
&= (\beta^p - \beta) + (\beta^p - \beta)^p + \dots + (\beta^p - \beta)^{p^{m-1}} = \\
&= \cancel{\beta^p} - \beta + \cancel{\beta^{p^2}} - \cancel{\beta^p} + \dots + \cancel{\beta^{p^m}} - \cancel{\beta^{p^{m-1}}} \\
&= \beta^{p^m} - \beta \Rightarrow \beta^{p^m} = \beta \quad \therefore \beta \in \mathbb{F} = \mathbb{F}_q^m.
\end{aligned}$$

Teorema (Transitividad de la Traza) Sea k es un cuerpo finito, F es una extensión finita de k y E es una extensión finita de F entonces

$$\text{Tr}_{E/k}(\alpha) = \text{Tr}_{F/k}(\text{Tr}_{E/F}(\alpha))$$

$$\begin{array}{l}
E = \mathbb{F}_{q^{n \cdot m}} \\
|_n \\
F = \mathbb{F}_{q^m} \\
|_m \\
K = \mathbb{F}_q
\end{array}$$

Demostración

$$\begin{aligned}
\alpha \in E \quad \text{Tr}_{F/k}(\text{Tr}_{E/F}(\alpha)) &= \\
&= \text{Tr}_{E/F}(\alpha) + (\text{Tr}_{E/F}(\alpha))^p + \dots + (\text{Tr}_{E/F}(\alpha))^{q^{m-1}} \\
&= (\alpha + \alpha^{p^m} + \alpha^{p^{m^2}} + \dots + \alpha^{p^{m^{n-1}}}) + (\alpha + \alpha^{p^m} + \alpha^{p^{m^2}} + \dots + \alpha^{p^{m^{n-1}}})^p \\
&\quad + \dots + (\alpha + \alpha^{p^m} + \alpha^{p^{m^2}} + \dots + \alpha^{p^{m^{n-1}}})^{q^{m-1}}
\end{aligned}$$

$$\begin{aligned}
&= \sum_{i=0}^{m-1} (\text{Tr}_{E/F}(\alpha))^{q^i} = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{n-1} \alpha^{q^{m \cdot j}} \right)^{q^i} = \\
&= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{m \cdot j + i}} = \sum_{k=0}^{n \cdot m - 1} \alpha^{q^k} = \text{Tr}_{E/K}(\alpha)
\end{aligned}$$

Ejercicio



Ahora definimos el producto de los conjugados de un elemento con respecto a un subcuerpo:

Def. Para $\alpha \in F = \mathbb{F}_{q^m}$ y $K = \mathbb{F}_q$, lo norma $N_{F/K}(\alpha)$ de α sobre K se define como

$$\begin{aligned}
N_{F/K}(\alpha) &= \alpha \cdot \alpha^q \cdots \alpha^{q^{m-1}} \\
&= \alpha^{1+q+q^2+\dots+q^{m-1}} \\
&= \alpha^{\frac{q^m-1}{q-1}}
\end{aligned}$$

Como vimos cuando definimos el polinomio característico de un $\alpha \in F$ sobre K , tenemos que

$$N_{F/K}(\alpha) = (-1)^m a_0$$

Si $g(x) = x^m + \underline{a_{m-1}}x^{m-1} + \dots + a_0$ es el pol. caract. de α en F sobre K

En particular tenemos que $N_{F/k}(\alpha) \in k$.

Teorema: Sea $k = \mathbb{F}_q$ y $F = \mathbb{F}_{q^m}$ entonces:

$$(1) \quad N_{F/k}(\alpha \cdot \beta) = N_{F/k}(\alpha) \cdot N_{F/k}(\beta)$$

$$(2) \quad N_{F/k} \text{ lleva } \mathbb{F} \text{ sobre } k \text{ y } \mathbb{F}^* \xrightarrow{\text{sobre}} k^*$$

$$(3) \quad N_{F/k}(a) = a^m, \quad a \in k = \mathbb{F}_q$$

$$(4) \quad N_{F/k}(\alpha^q) = N_{F/k}(\alpha) \quad \forall \alpha \in \mathbb{F}$$

Demostración

(1), (3), (4) derivan de la definición (Ejercicio)

Para ver (2) ya sabemos que $N_{F/k}: \mathbb{F} \rightarrow k$ y como $\mathbb{F}$ es cuerpo

$$N_{F/k}(\alpha) = 0 \iff \alpha = 0.$$

$$\text{Por lo tanto } N_{F/k}(\mathbb{F}^*) \subseteq k^*$$

Para ver que es sobreyectiva mostraremos que $N_{F/k}(\alpha)$ es un generador del grupo cíclico k^* si α genera F^* .

Sea α un generador del grupo cíclico F^* entonces

$$\left(N_{F/k}(\alpha)\right)^{q-1} = \left(\alpha^{\frac{q^m-1}{q-1}}\right)^{q-1} = \alpha^{q^m-1} = 1$$

y no puede haber ningún otro $d < q-1$

$$\left(N_{F/k}(\alpha)\right)^d = 1 \quad \text{por en ese caso} \quad \alpha^d = 1 \quad \text{no} \\ \uparrow \\ \text{ord}(\alpha) = q^m - 1.$$

$$\beta \in k^* \Rightarrow \beta = \left(N_{F/k}(\alpha)\right)^j = N_{F/k}(\alpha^j) \quad \text{con } j \in F.$$

Teorema (Transitividad de la norma): Sea k un cuerpo finito, F una extensión finita de k y E una extensión finita de F entonces

$$N_{E/k}(\alpha) = N_{F/k}\left(N_{E/F}(\alpha)\right) \quad \forall \alpha \in E.$$

Demonstración

$$\alpha \in E$$

$$N_{F/K} (N_{E/F} (\alpha)) =$$

$$= N_{F/K} \left(\alpha^{\frac{q^{n \cdot m} - 1}{q^m - 1}} \right) =$$

$$= \left(\alpha^{\frac{q^{n \cdot m} - 1}{q^m - 1}} \right)^{\frac{q^m - 1}{q - 1}} = \alpha^{\frac{q^{n \cdot m} - 1}{q - 1}} = N_{E/K} (\alpha)$$



Bases

$$F/K$$

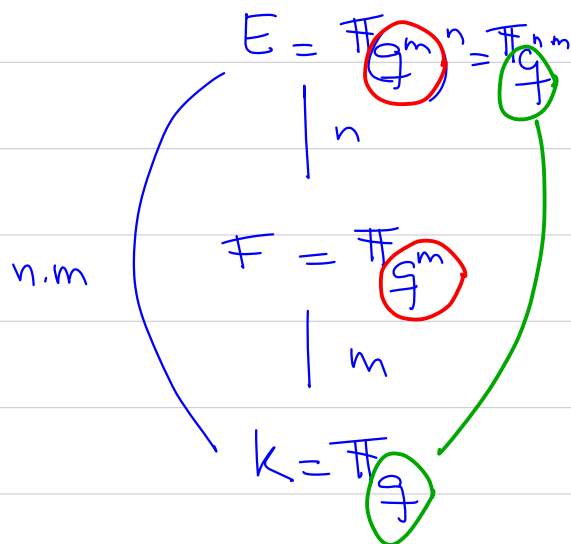
$$[F:K] = m$$

$\{\alpha_1, \dots, \alpha_m\}$ es una base

$$\alpha \in F$$

$$\alpha = c_1 \alpha_1 + \dots + c_m \alpha_m$$

$$c_1, \dots, c_m \in K.$$



Si $\{\alpha_1, \dots, \alpha_m\}$ es una base un cuerpo finito F sobre un subcuerpo k , una pregunta de interés es cómo calcular los coeficientes para un $\alpha \in F$, es decir $c_1, \dots, c_m \in k$ tales que

$$\alpha = c_1 \alpha_1 + \dots + c_m \alpha_m$$

y otra es determinar/elegir que base es más adecuada para las operaciones que debe realizar.

Con algunas bases calcular potencias e inversos es fácil, mientras que otras operaciones pueden ser más complicadas y con otras bases se pueden calcular rápidamente productos o sumas pero pagando un pagando un precio (en cantidad de operaciones) para calcular inversos.

Cuando consideramos una ext. finita F de un cuerpo finito k hay dos bases que son particularmente importantes:

La primera es la base polinomial $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$ formado por las potencias de α un elemento de definición de F sobre k . $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$

Otra base importante es la base normal

Def.: Sea $k = \mathbb{F}_q$ y $F = \mathbb{F}_{q^m}$ entonces una base de F sobre k de la forma $\{\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}\}$

formada por un elemento adecuado $\alpha \in F$ y sus conjugados respecto de k se llame base normal de F sobre k .

Ejemplo: $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ α es raíz $X^3 + X^2 + 1 \in \mathbb{F}_2[X]$.

$$\mathbb{F}_8 = \{0, 1, \underbrace{\alpha}_\alpha, \alpha+1, \underbrace{\alpha^2}_{\alpha^2}, \underbrace{\alpha^2+1}_{\alpha^3}, \alpha^2+\alpha, \underbrace{\alpha^2+\alpha+1}_{\alpha^4 = \alpha^4}\}$$

$$F = \mathbb{F}_8 = \mathbb{F}_{2^3}$$

3

$$K = \mathbb{F}_2$$

Base polinomial $\{1, \alpha, \alpha^2\}$

Base normal

$$\{\alpha, \alpha^2, \alpha^4\}$$

$$= \{\alpha, \alpha^2, \alpha^2+\alpha+1\}$$

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

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

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

$$\begin{aligned}\alpha^4 &= \alpha \cdot \alpha^3 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha = \\ &= \alpha^2 + 1 + \alpha\end{aligned}$$

