

Teorema: Si f es un polinomio irreducible en $\mathbb{H}_f[x]$ de grado m , entonces f tiene una raíz α en $\mathbb{H}_f^m$. Más aun, todas las raíces de f son simples y están dados por los elementos diferentes

$$\alpha, \alpha^f, \alpha^{f^2}, \dots, \alpha^{f^{m-1}} \text{ de } \mathbb{H}_f^m.$$

Demostación

Sea α una raíz de f en el cuerpo de descomposición de f sobre $\mathbb{H}_f$. Entonces $[\mathbb{H}_f(\alpha) : \mathbb{H}_f] = m$ entonces como antes obtenemos $\mathbb{H}_f(\alpha) = \mathbb{H}_f^m$, y en particular $\alpha \in \mathbb{H}_f^m$.

Veamos ahora que si $\beta \in \mathbb{H}_f^m$ es una raíz del polinomio entonces β^f también es raíz.

Supongamos $f(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0$

$$a_i \in \mathbb{H}_f \rightarrow a_i^f = a_i$$

entonces

$$f(\beta^f) = a_m (\beta^f)^m + a_{m-1} (\beta^f)^{m-1} + \dots + a_1 \beta^f + a_0$$

$$= a_m^f (\beta^m)^f + a_{m-1}^f (\beta^{m-1})^f + \dots + a_1^f \beta^f + a_0^f$$

$$= (a_m \beta^m + a_{m-1} \beta^{m-1} + \dots + a_1 \beta + a_0)^f$$

$$= (f(\beta))^f = 0.$$

Entonces $\alpha, \alpha^f, \alpha^{f^2}, \dots, \alpha^{f^{m-1}}$ son raíces de f .

Para probar que son distintos supongamos por el contrario que hay 2 iguales

$$\alpha^{f^j} = \alpha^{f^k} \quad \text{con } 0 \leq j < k \leq m-1$$

Elevando a la potencia f^{m-k}

$$\alpha^{f^{m-k+j}} = \alpha^{f^m} = \alpha$$

$\alpha \in \mathbb{F}_{f^m}$

Entonces α es raíz del polinomio

$$h(x) = x^{f^{m-k+j}} - x$$

Entonces usando los dos lemas previos como α es raíz de $h(x)$ tenemos que f divide a h y también que $m = \deg(f)$ divide a $m-k+j$

Abuso pues $0 \leq m-k+j < m$.



Corolario: Si $f \in \mathbb{F}_f[x]$ es un polinomio irreducible de grado m , entonces el cuerpo de descomposición de f sobre $\mathbb{F}_f$ es $\mathbb{F}_{f^m}$.

Dem

f se descompone en $\mathbb{F}_{f^m}$ y $\mathbb{F}_f(\alpha, \alpha^f, \dots, \alpha^{f^{m-1}}) = \mathbb{F}_f(\alpha) = \mathbb{F}_{f^m}$.



Corolario: Dos polinomios irreducibles en $\mathbb{H}_f[x]$ del mismo grado tienen cuerpos de descomposición isomorfos.

Def: Sea $\mathbb{H}_f^m$ una extensión de $\mathbb{H}_f$ y sea $\alpha \in \mathbb{H}_f^m$. Entonces los elementos

$$\alpha, \alpha^f, \dots, \alpha^{f^{m-1}}$$

se llaman conjugados de α con respecto a $\mathbb{H}_f$.

Los conjugados de $\alpha \in \mathbb{H}_f^m$ con respecto a $\mathbb{H}_f$ son distintos si y solo si el polinomio mínimo de α sobre $\mathbb{H}_f$ es de grado m . Si el polinomio mínimo de α sobre $\mathbb{H}_f$ es de grado menor a m , digamos d , entonces d es un divisor propio de m y los conjugados distintos son

$$\alpha, \alpha^f, \dots, \alpha^{f^{d-1}}$$

y en el conjunto anterior se repiten m/d veces cada uno.

$$x^2 + x + 2$$

Ejemplo: Consideremos $\mathbb{F}_9 = \mathbb{F}_{3^2} = \mathbb{F}_3(\theta)$ $\theta^2 = 2\theta + 1$

$$\mathbb{F}_{3^2} = \{0, 1, 2, \underbrace{\theta}_{\theta^3}, \underbrace{\theta+1}_{\theta^7}, \underbrace{\theta+2}_{\theta^6}, \underbrace{2\theta}_{\theta^5}, \underbrace{2\theta+1}_{\theta^2}, \underbrace{2\theta+2}_{\theta^4}\}$$

Entonces por $\beta = \theta$, hay un único conjugado diferente de θ que es
 $\theta^{q^{n-1}} = \theta^3 = 2\theta + 2$

Luego θ y $2\theta + 2$ son conjugados, con respecto a $\mathbb{F}_3$.

Si $\alpha = 2\theta + 1 = \theta^2$ entonces su conjugado es

$$\alpha^3 = (2\theta + 1)^3 = (\theta^2)^3 = \theta^6 = \theta + 2$$

$$\alpha^{3^2} = (\theta^2)^9 = \theta^{18} = \underbrace{(\theta^8)}_1 \cdot \theta^2 = \theta^2$$

$$\theta^8 = 1 \quad \theta^9 = \theta$$

Hay una relación entre los conjugados y los automorfismos de un cuerpo finito. Cuando hablemos de un automorfismo de $\mathbb{F}_{q^m}/\mathbb{F}_q$ (o de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$) nos referiremos a

un automorfismo de $\mathbb{F}_{q^m}$ que fije los elementos de $\mathbb{F}_q$, es decir σ es un automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ si es un mapeo^{1a} de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_{q^m}$ que satisface

$$\begin{aligned} \sigma(\alpha + \beta) &= \sigma(\alpha) + \sigma(\beta) \\ \sigma(\alpha \cdot \beta) &= \sigma(\alpha) \cdot \sigma(\beta) \\ \sigma(a) &= a \end{aligned} \quad \left\{ \begin{array}{l} \forall \alpha, \beta \in \mathbb{F}_{q^m} \\ \forall a \in \mathbb{F}_q. \end{array} \right.$$

Teorema: Los automorfismos distintos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ son las funciones $\sigma_0, \sigma_1, \dots, \sigma_{m-1}$ definidas por

$$\sigma_j(\alpha) = \alpha^{q^j} \quad 0 \leq j \leq m-1 \\ \forall \alpha \in \mathbb{F}_{q^m}.$$

Demostración

Es fácil ver que σ_j es un automorfismo de $\mathbb{F}_{q^m}$ (Ejercicio, usar $(\alpha + \beta)^{q^j} = \alpha^{q^j} + \beta^{q^j}$
 $\sigma_j(0) = 0 \Rightarrow \alpha = 0$
 $a \in \mathbb{F}_q \Rightarrow a^{q^j} = a.$)

Además son todos diferentes pues si elegimos un elemento primitivo β , los $\sigma_j(\beta)$ serán todos distintos. $\hookrightarrow$ de $\mathbb{F}_q^m$.

Supongamos que σ es un automorfismo arbitrario de $\mathbb{F}_q^m$ sobre $\mathbb{F}_q$. Sea β un elemento primitivo de $\mathbb{F}_q^m$ y sea

$$f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0 \in \mathbb{F}_q[x]$$

su polinomio mínimo sobre $\mathbb{F}_q$.

$$0 = f(\beta) = \sigma(f(\beta)) = \sigma(\beta^m + a_{m-1}\beta^{m-1} + \dots + a_1\beta + a_0)$$

$$= \sigma(\beta)^m + \sigma(a_{m-1})\sigma(\beta)^{m-1} + \dots + \sigma(a_1)\sigma(\beta) + \sigma(a_0)$$

$$= \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + \dots + a_1\sigma(\beta) + a_0 = f(\sigma(\beta))$$

Entonces $\sigma(\beta)$ es una raíz del polinomio mínimo de β sobre $\mathbb{F}_q$ y por un teorema anterior tenemos que f tiene todas raíces simples distintas y en particular

$$\sigma(\beta) = \beta^{\beta^j} \quad \text{para algún } 0 \leq j \leq m-1.$$

Luego $\sigma(\alpha) = \alpha^{\beta^j} \quad \forall \alpha \in \mathbb{F}_q^m \mid$ pues σ es automorfismo y β es primitivo.

El conjunto de automorfismos de $\mathbb{F}_q^m$ sobre $\mathbb{F}_q$ forme un grupo con la composición que se llame grupo de Galois de $\mathbb{F}_q^m$ sobre $\mathbb{F}_q$. Este grupo es un grupo cíclico generado

$$\sigma_1: \mathbb{F}_q^m \rightarrow \mathbb{F}_q^m \\ \alpha \rightarrow \alpha^q$$

automorfismo de
Frobenius.

Los conjugados de α son entonces los elementos a los cuales α es enviado aplicando iterativamente el automorfismo de Frobenius.

Trazas, Normas y Bases

Def Para cada $\alpha \in F = \mathbb{F}_q^m$, la traza de α sobre $k = \mathbb{F}_q$ es definido por

$$\text{Tr}_{F/k}(\alpha) = \alpha + \alpha^q + \dots + \alpha^{q^{m-1}} \in k.$$

Si k es el subcuerpo primo de F entonces $\text{Tr}_{F/k}$ se llama traza absoluta de α y escribimos

$$\text{Tr}_F(\alpha).$$

Nota que si $\alpha \in F = \mathbb{F}_q^m$ y f es un polinomio mínimo sobre $k = \mathbb{F}_q$ y $\deg(f) = d$ entonces d divide m y el polinomio

$$g(x) = (f(x))^{m/d} \in k[x]$$

se llama el polinomio característico de α sobre k .

Como las raíces de f están dadas por

$$\alpha, \alpha^q, \dots, \alpha^{q^{d-1}}$$

entonces los conjugados de α  son las raíces de $g(x)$ y podemos escribir

$$g(x) = x^m + \overbrace{a_{m-1}} x^{m-1} + \dots + a_1 x + a_0 \in K[x]$$

$$= (x - \alpha)(x - \alpha^p) \dots (x - \alpha^{p^{m-1}})$$

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

Entonces $\text{Tr}_{F/K}(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{m-1}} = -a_{m-1} \in K$.

en particular $\text{Tr}_{F/K}(\alpha)$ es siempre un elemento de K .

Lo traza tiene varias propiedades interesantes reunidas en el siguiente teorema:

Teorema: Sea $K = \mathbb{F}_q$ y $F = \mathbb{F}_{q^m}$. Entonces

- (1) $\text{Tr}_{F/K}(\alpha + \beta) = \text{Tr}_{F/K}(\alpha) + \text{Tr}_{F/K}(\beta) \quad \forall \alpha, \beta \in \overline{\mathbb{F}_q}^m$
- (2) $\text{Tr}_{F/K}(c \cdot \alpha) = c \text{Tr}_{F/K}(\alpha) \quad \forall c \in \overline{\mathbb{F}_q}^k, \alpha \in \overline{\mathbb{F}_q}^m$
- (3) $\text{Tr}_{F/K}$ es una transformación lineal de F sobre K .
- (4) $\text{Tr}_{F/K}(a) = m \cdot a \quad \forall a \in K$
- (5) $\text{Tr}_{F/K}(\alpha^p) = \text{Tr}_{F/K}(\alpha) \quad \forall \alpha \in F$

Demostración

Ejercicio (1), (2), (4), (5).

(3) Las propiedades (1) y (2) junto con el hecho $\text{Tr}_{F/K}(\alpha) \in K \quad \forall \alpha \in F$ muestran que es una transformación lineal de F sobre K .

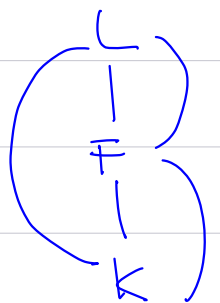
Para completar la prueba y ver que es sobre vamos a mostrar que existe $\alpha \in F$ tal que $\text{Tr}_{F/K}(\alpha) \neq 0$.

$$\text{Pero } \text{Tr}_{F/K}(\alpha) = 0 \Leftrightarrow \alpha^{f^{m-1}} + \alpha^{f^{m-2}} + \dots + \alpha^f + \alpha = 0$$

$$\Leftrightarrow \alpha \text{ es raíz del polinomio } \underbrace{X^{f^{m-1}} + \dots + X^f + X}_{\in K[X]} = p(x)$$

Pero $p(x)$ es un polinomio de grado f^{m-1} y por lo tanto tiene como máximo f^{m-1} raíces en F , y como F tiene f^m elementos hay algún $\beta \in F$ que no sea raíz, es decir

$$\text{Tr}_{F/K}(\beta) \neq 0.$$



$$\mathbb{F}_9 = \{0\} \cup \mathbb{F}_9^*$$

$$0 + 0^2 + \dots + \underbrace{0^{p-1}}_1$$

$$\left\{ \underbrace{1}_{0^{p-1}}, \sigma, \dots, \sigma^{p-2} \right\}$$

$$\alpha \in \mathbb{F}_9 \Rightarrow \alpha^9 = \alpha$$

$$0 = \alpha^9 - \alpha$$

$$(x^9 - x)$$

$$\mathbb{F}_4 = \{0, 1, \sigma, \sigma+1\}$$

$$\sigma^2 = \sigma + 1$$

$$1 + \sigma + \sigma + 1 = 2\sigma + 2 = 0.$$

24

$$S = \sum_{\alpha \in \mathbb{F}_9^*} \alpha \quad (2\sigma)^2 \quad (2\sigma)^3$$

$$\mathbb{F}_9^* \rightarrow \mathbb{F}_9^* \\ \alpha \rightarrow -\alpha$$

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

$$a + b\sigma \\ a, b \in \mathbb{F}_5.$$

$$\{1, \sigma\}$$

$$x^2 + x + 1 = 0.$$

$$\sigma^2 + \sigma + 1 = 0$$

$$\mathbb{F}_{p^2} \mathbb{F}_{p^3} = 1$$

$$\mathbb{F}_{25} = \mathbb{F}_{5^2} = \mathbb{F}_5(\sigma) = \{0, 1, 2, 3, 4, \sigma, 2\sigma, 3\sigma, 4\sigma, \dots\}$$

$$\sigma^2 = -\sigma - 1$$

$$\sigma^2 = 4\sigma + 4.$$

$$4\sigma + 4$$