Cuerpos Finitos

XXVII Escuela Venezolana de Matemáticas – EMALCA

Edgar Martínez-Moro

Sept. 2014

imUVa Instituto de Investigación en Matemáticas

Universidad de Valladolid

Cuerpos y extensiones de cuerpos

Un cuerpo $(\mathbb{F}, +, \cdot)$ es un conjunto no vacío en el que se han definido dos operaciones binarias: la adición, denotada por $+$, y el producto, denotado por $\cdot$. Los conjuntos $(\mathbb{F}, +)$ y $(\mathbb{F}\backslash\{0\}, \cdot)$ son grupos abelianos y además, el producto es distributivo con respecto a la adición. Los elementos neutros de ambas operaciones son diferentes y se denotan, respectivamente, como 0 y 1.

Adoptaremos la notación $\mathbb{F}^*$ para el conjunto de elementos no nulos de $\mathbb{F}$. Un cuerpo se llama primo si no contiene ningún subcuerpo propio.

Todo cuerpo $\mathbb{F}$ contiene un cuerpo primo que es, o bien $\mathbb{Q}$, o bien $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ para algún primo p.

Cuerpos y extensiones de cuerpos

Un cuerpo $(\mathbb{F}, +, \cdot)$ es un conjunto no vacío en el que se han definido dos operaciones binarias: la adición, denotada por $+$, y el producto, denotado por $\cdot$. Los conjuntos $(\mathbb{F}, +)$ y $(\mathbb{F}\backslash\{0\}, \cdot)$ son grupos abelianos y además, el producto es distributivo con respecto a la adición. Los elementos neutros de ambas operaciones son diferentes y se denotan, respectivamente, como 0 y 1.

Adoptaremos la notación $\mathbb{F}^*$ para el conjunto de elementos no nulos de $\mathbb{F}$. Un cuerpo se llama primo si no contiene ningún subcuerpo propio.

Todo cuerpo $\mathbb{F}$ contiene un cuerpo primo que es, o bien $\mathbb{Q}$, o bien $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ para algún primo p.

Cuerpos y extensiones de cuerpos

Un cuerpo $(\mathbb{F}, +, \cdot)$ es un conjunto no vacío en el que se han definido dos operaciones binarias: la adición, denotada por $+$, y el producto, denotado por $\cdot$. Los conjuntos $(\mathbb{F}, +)$ y $(\mathbb{F}\backslash\{0\}, \cdot)$ son grupos abelianos y además, el producto es distributivo con respecto a la adición. Los elementos neutros de ambas operaciones son diferentes y se denotan, respectivamente, como 0 y 1.

Adoptaremos la notación $\mathbb{F}^*$ para el conjunto de elementos no nulos de $\mathbb{F}$. Un cuerpo se llama primo si no contiene ningún subcuerpo propio.

Todo cuerpo $\mathbb{F}$ contiene un cuerpo primo que es, o bien $\mathbb{Q}$, o bien $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ para algún primo p.

Un cuerpo $\mathbb{F}$ tiene característica cero si $\mathbb{Q} \leq \mathbb{F}$, y tiene característica p si $\mathbb{Z}_p \leq \mathbb{F}$. Cualquier cuerpo de característica cero, como $\mathbb{R}$ o $\mathbb{C}$, contiene el cuerpo primo $\mathbb{Q}$, por tanto tiene un número infinito de elementos. A su vez, un cuerpo finito tiene necesariamente característica p. Sin embargo, existen cuerpos de característica p que no son finitos.

Un par de cuerpos $\mathbb{K}$ y $\mathbb{F}$ con $\mathbb{F} \subseteq \mathbb{K}$ se llama extensión de cuerpos y se denota por $\mathbb{K}|\mathbb{F}$. Dada una extensión $\mathbb{K}|\mathbb{F}$ de cuerpos,

es fácil ver que $\mathbb{K}$ es un $\mathbb{F}$-espacio vectorial

de donde se llama grado de la extensión $\mathbb{K}|\mathbb{F}$ a la dimensión del $\mathbb{F}$-espacio vectorial $\mathbb{K}$. Se denota por $[\mathbb{K} : \mathbb{F}]$. La extensión se dice finita si su grado es finito, e infinita en caso contrario.

Un par de cuerpos $\mathbb{K}$ y $\mathbb{F}$ con $\mathbb{F} \subseteq \mathbb{K}$ se llama extensión de cuerpos y se denota por $\mathbb{K}|\mathbb{F}$. Dada una extensión $\mathbb{K}|\mathbb{F}$ de cuerpos,

es fácil ver que $\mathbb{K}$ es un $\mathbb{F}$-espacio vectorial

de donde se llama grado de la extensión $\mathbb{K}|\mathbb{F}$ a la dimensión del $\mathbb{F}$-espacio vectorial $\mathbb{K}$. Se denota por $[\mathbb{K} : \mathbb{F}]$. La extensión se dice finita si su grado es finito, e infinita en caso contrario.

Un par de cuerpos $\mathbb{K}$ y $\mathbb{F}$ con $\mathbb{F} \subseteq \mathbb{K}$ se llama extensión de cuerpos y se denota por $\mathbb{K}|\mathbb{F}$. Dada una extensión $\mathbb{K}|\mathbb{F}$ de cuerpos,

es fácil ver que $\mathbb{K}$ es un $\mathbb{F}$-espacio vectorial

de donde se llama grado de la extensión $\mathbb{K}|\mathbb{F}$ a la dimensión del $\mathbb{F}$-espacio vectorial $\mathbb{K}$. Se denota por $[\mathbb{K} : \mathbb{F}]$. La extensión se dice finita si su grado es finito, e infinita en caso contrario.

Un par de cuerpos $\mathbb{K}$ y $\mathbb{F}$ con $\mathbb{F} \subseteq \mathbb{K}$ se llama extensión de cuerpos y se denota por $\mathbb{K}|\mathbb{F}$. Dada una extensión $\mathbb{K}|\mathbb{F}$ de cuerpos,

es fácil ver que $\mathbb{K}$ es un $\mathbb{F}$-espacio vectorial

de donde se llama grado de la extensión $\mathbb{K}|\mathbb{F}$ a la dimensión del $\mathbb{F}$-espacio vectorial $\mathbb{K}$. Se denota por $[\mathbb{K} : \mathbb{F}]$. La extensión se dice finita si su grado es finito, e infinita en caso contrario.

Si $\mathbb{K}|\mathbb{F}$ es una extensión de cuerpos y $S \subseteq \mathbb{K}$, el cuerpo obtenido a partir de $\mathbb{F}$ por la adjunción de S es $\mathbb{F}(S) = \bigcap\{\mathbb{L} \leq \mathbb{K} \,|\, \mathbb{F} \cup S \subseteq \mathbb{L}\}$. Es claro que $\mathbb{F}(S)|\mathbb{F}$ es la menor extensión de $\mathbb{F}$ que contiene a S. En el caso en que $S = \{a\}$, la extensión $\mathbb{F}(a)|\mathbb{F}$ se dice simple y

se puede probar que $\mathbb{F}(a) = \left\{ \frac{f(a)}{g(a)} \mid f, g \in \mathbb{F}[x], g(a) \neq 0 \right\}$.

Dada una extensión de cuerpos $\mathbb{K}|\mathbb{F}$, un elemento $a \in \mathbb{K}$ se dice algebraico sobre $\mathbb{F}$ si existe un polinomio no nulo $f(x) \in \mathbb{F}[x]$ tal que $f(a) = 0$. En caso contrario, el elemento se dice trascendente.

La extensión $\mathbb{K}|\mathbb{F}$ se dice algebraica si todos los elementos de $\mathbb{K}$ son algebraicos sobre $\mathbb{F}$. En caso contrario, se dice trascendente.

Dada una extensión de cuerpos $\mathbb{K}|\mathbb{F}$, un elemento $a \in \mathbb{K}$ se dice algebraico sobre $\mathbb{F}$ si existe un polinomio no nulo $f(x) \in \mathbb{F}[x]$ tal que $f(a) = 0$. En caso contrario, el elemento se dice trascendente.

La extensión $\mathbb{K}|\mathbb{F}$ se dice algebraica si todos los elementos de $\mathbb{K}$ son algebraicos sobre $\mathbb{F}$. En caso contrario, se dice trascendente.

– Teorema –

Sean $\mathbb{K}|\mathbb{F}$ una extensión y $a \in \mathbb{K}$ un elemento algebraico sobre $\mathbb{F}$. Entonces:

1. Existe un único polinomio mónico irreducible $p(x) \in \mathbb{F}[x]$ tal que $p(a) = 0$.
2. Si $g(x) \in \mathbb{F}[x]$, entonces $g(a) = 0$ si y sólo si $p(x)|g(x)$ en $\mathbb{F}[x]$.
3. $\mathbb{F}(a) = \mathbb{F}[a] = \{f(a) \mid f(x) \in \mathbb{F}[x]\}$. Además, todo elemento de $\mathbb{F}(a)$ admite una expresión única de la forma $r(a)$, con $r = 0$ o con $\mathrm{gr}(r) < \mathrm{gr}(p)$. Así pues, si $n = \mathrm{gr}(f)$, el conjunto $\{1, a, \ldots, a^{n-1}\}$ es una $\mathbb{F}$-base de $\mathbb{F}(a)$.

Dados un cuerpo $\mathbb{F}$ y un polinomio $f(x) \in \mathbb{F}[x]$, se llama cuerpo de descomposición de $f(x)$ sobre $\mathbb{F}$ a un cuerpo $\mathbb{K}$ extensión de $\mathbb{F}$ que cumple estas dos propiedades:

1. $f(x)$ tiene todas las raíces en $\mathbb{K}$, por tanto, existen $\lambda \in \mathbb{K}$ y $a_1, \ldots, a_n \in \mathbb{K}$ tales que

$$f(x) = \lambda(x - a_1) \cdots (x - a_n) \in \mathbb{K}[x].$$

2. $\mathbb{K}$ es la menor extensión de $\mathbb{F}$ con esta propiedad, esto es,

$$\mathbb{K} = \mathbb{F}(a_1 \ldots, a_n).$$

– Teorema –

Para cada polinomio $f(x) \in \mathbb{F}[x]$ de grado $n \geq 1$ existe un cuerpo de descomposición sobre $\mathbb{F}$. Este cuerpo de descomposición es único salvo isomorfismo.

Anillos de polinomios sobre c. finitos

$\mathbb{K}$ representará un cuerpo finito de caracteristica p. Su cuerpo primo será $\mathbb{Z}_p$ y si el grado de la extensión $[\mathbb{K} : \mathbb{Z}_p] = n$, entonces $|\mathbb{K}| = p^n$.

– Teorema –

Sea $\mathbb{K}$ un cuerpo, no necesariamente finito, y G un subgrupo del grupo multiplicativo $(\mathbb{K}^*, \cdot)$. Si G es finito, entonces G es un grupo cíclico. En particular, si $\mathbb{K}$ es finito, $(\mathbb{K}^*, \cdot)$ es un grupo cíclico.

Anillos de polinomios sobre c. finitos

$\mathbb{K}$ representará un cuerpo finito de caracteristica p. Su cuerpo primo será $\mathbb{Z}_p$ y si el grado de la extensión $[\mathbb{K} : \mathbb{Z}_p] = n$, entonces $|\mathbb{K}| = p^n$.

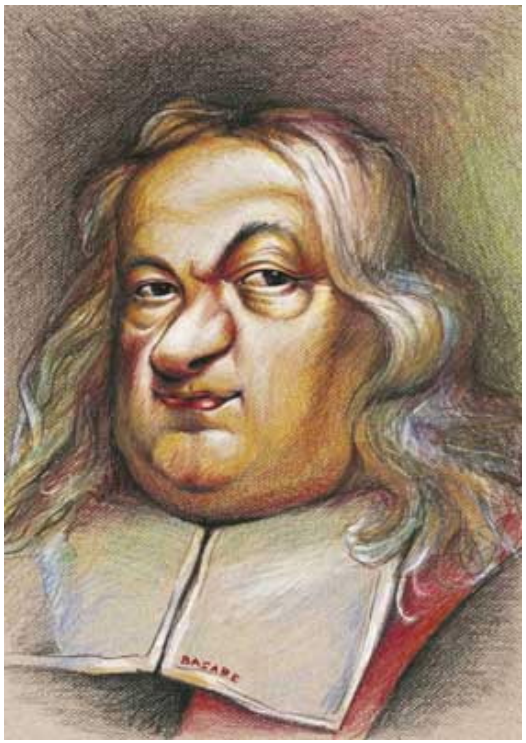
– Teorema –

Sea $\mathbb{K}$ un cuerpo, no necesariamente finito, y G un subgrupo del grupo multiplicativo $(\mathbb{K}^*, \cdot)$. Si G es finito, entonces G es un grupo cíclico. En particular, si $\mathbb{K}$ es finito, $(\mathbb{K}^*, \cdot)$ es un grupo cíclico.

Si $\mathbb{K}$ es un cuerpo finito, entonces $(\mathbb{K}^*, \cdot) \cong C_{p^n-1}$ con $|\mathbb{K}| = p^n$. Por otra parte,

$$(\mathbb{K}, +) \cong C_p \oplus \cdots \oplus C_p,$$

por tanto, el grupo aditivo $(\mathbb{K}, +)$ tiene exponente p.



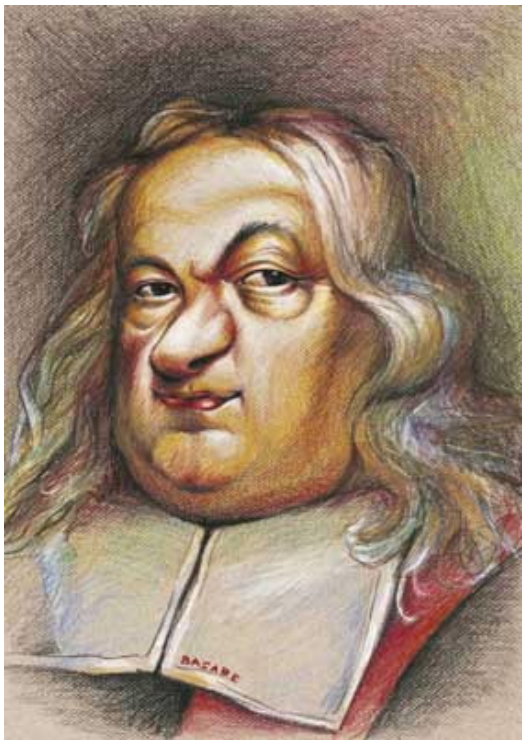
– Pequeño teorema de Fermat –

Para todo $n \in \mathbb{Z}$ y p primo, $n^p \equiv n$ mód p. Si $(n, p) = 1$, entonces $n^{p-1} \equiv 1$ mód p.

Si $\mathbb{K}$ es un cuerpo finito, entonces $(\mathbb{K}^*, \cdot) \cong C_{p^n-1}$ con $|\mathbb{K}| = p^n$. Por otra parte,

$$(\mathbb{K}, +) \cong C_p \oplus \cdots \oplus C_p,$$

por tanto, el grupo aditivo $(\mathbb{K}, +)$ tiene exponente p.



– Pequeño teorema de Fermat –

Para todo $n \in \mathbb{Z}$ y p primo, $n^p \equiv n$ mód p. Si $(n, p) = 1$, entonces $n^{p-1} \equiv 1$ mód p.

– Teorema del elemento primitivo –

Sean $\mathbb{F}$ un cuerpo finito y $\mathbb{K}|\mathbb{F}$ una extensión finita. Entonces la extensión es simple, es decir, existe un elemento $u \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{F}(u)$.

Si u es un generador del grupo multiplicativo $\mathbb{K}^*$, esto es, $\mathbb{K}^* = \langle u \rangle$, entonces $\mathbb{K} = \mathbb{Z}_p(u) = \mathbb{F}(u)$ para cualquier cuerpo intermedio $\mathbb{Z}_p \leq \mathbb{F} \leq \mathbb{K}$. Sin embargo, el recíproco no es cierto, pues si $\mathbb{K} = \mathbb{Z}_p(u)$, no necesariamente, $\mathbb{K}^* = \langle u \rangle$.

– Teorema del elemento primitivo –

Sean $\mathbb{F}$ un cuerpo finito y $\mathbb{K}|\mathbb{F}$ una extensión finita. Entonces la extensión es simple, es decir, existe un elemento $u \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{F}(u)$.

Si u es un generador del grupo multiplicativo $\mathbb{K}^*$, esto es, $\mathbb{K}^* = \langle u \rangle$, entonces $\mathbb{K} = \mathbb{Z}_p(u) = \mathbb{F}(u)$ para cualquier cuerpo intermedio $\mathbb{Z}_p \leq \mathbb{F} \leq \mathbb{K}$. Sin embargo, el recíproco no es cierto, pues si $\mathbb{K} = \mathbb{Z}_p(u)$, no necesariamente, $\mathbb{K}^* = \langle u \rangle$.

– Proposición –

Sea $\mathbb{K}$ un cuerpo con característica p diferente de cero. Si $r \geq 1$, entonces la aplicación

$$\begin{array}{rccc} \varphi : & \mathbb{K} & \longrightarrow & \mathbb{K} \\ & a & \longrightarrow & a^{p^r} \end{array}$$

es un $\mathbb{Z}_p$-homomorfismo de $\mathbb{K}$ en $\mathbb{K}$. Si $\mathbb{K}$ es finito, entonces φ es un automorfismo de cuerpos.

– Teorema de existencia y unicidad de cuerpos finitos –

Si $p > 0$ es primo y $n \geq 1$ es un número cualquiera, entonces existe un cuerpo $\mathbb{K}$ con orden $|\mathbb{K}| = p^n$. Si $\mathbb{K}_1$ y $\mathbb{K}_2$ son cuerpos y $|\mathbb{K}_1| = |\mathbb{K}_2| = p^n$, entonces $\mathbb{K}_1$ y $\mathbb{K}_2$ son $\mathbb{Z}_p$ isomorfos.

– Corolario –

Si $\mathbb{K}$ es un cuerpo finito tal que $|\mathbb{K}| = p^n$ y $\mathbb{F}$ es un subcuerpo de $\mathbb{K}$, entonces $x^{p^n} - x \in \mathbb{Z}_p[x] \subseteq \mathbb{F}[x]$ se escinde en $\mathbb{K}$, esto es, $x^{p^n} - x = \prod_{a \in \mathbb{K}} (x - a)$.

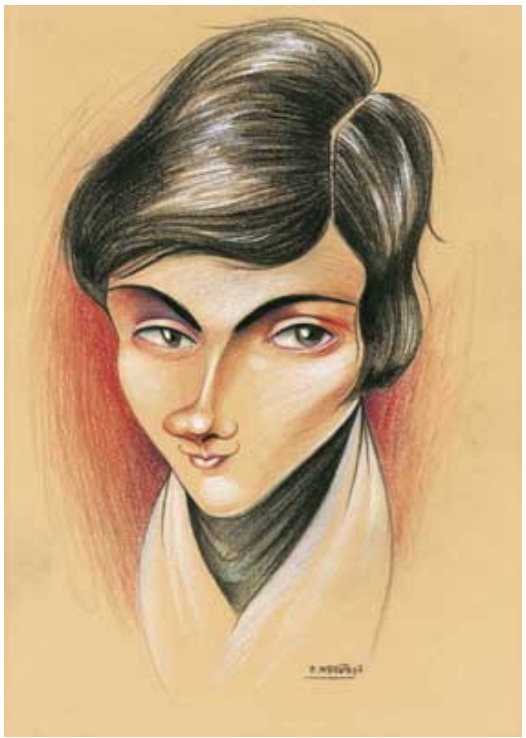
– Teorema de existencia y unicidad de cuerpos finitos –

Si $p > 0$ es primo y $n \geq 1$ es un número cualquiera, entonces existe un cuerpo $\mathbb{K}$ con orden $|\mathbb{K}| = p^n$. Si $\mathbb{K}_1$ y $\mathbb{K}_2$ son cuerpos y $|\mathbb{K}_1| = |\mathbb{K}_2| = p^n$, entonces $\mathbb{K}_1$ y $\mathbb{K}_2$ son $\mathbb{Z}_p$ isomorfos.

– Corolario –

Si $\mathbb{K}$ es un cuerpo finito tal que $|\mathbb{K}| = p^n$ y $\mathbb{F}$ es un subcuerpo de $\mathbb{K}$, entonces $x^{p^n} - x \in \mathbb{Z}_p[x] \subseteq \mathbb{F}[x]$ se escinde en $\mathbb{K}$, esto es, $x^{p^n} - x = \prod_{a \in \mathbb{K}} (x - a)$.

Introducción a la Teoría de Galois



Determinaremos ahora el grupo de $\mathbb{F}$-automorfismos de una extensión $\mathbb{K}|\mathbb{F}$ de cuerpos finitos. Este grupo se conoce como grupo de Galois de la extensión $\mathbb{K}|\mathbb{F}$.

Un polinomio irreducible $f(x) \in \mathbb{F}[x]$ se dice separable sobre $\mathbb{F}$ si todas las raíces de $f(x)$ en un cuerpo de descomposición $\mathbb{K}$ sobre $\mathbb{F}$ son simples. En caso contrario, el polinomio se dice inseparable.

Sea $\mathbb{K}|\mathbb{F}$ una extensión algebraica. Un elemento $a \in \mathbb{K}$ se dice separable sobre $\mathbb{F}$ si su polinomio irreducible asociado es separable sobre $\mathbb{F}$. La extensión $\mathbb{K}|\mathbb{F}$ se dice separable si todo elemento $a \in \mathbb{K}$ es separable sobre $\mathbb{F}$.

Un polinomio irreducible $f(x) \in \mathbb{F}[x]$ se dice separable sobre $\mathbb{F}$ si todas las raíces de $f(x)$ en un cuerpo de descomposición $\mathbb{K}$ sobre $\mathbb{F}$ son simples. En caso contrario, el polinomio se dice inseparable.

Sea $\mathbb{K}|\mathbb{F}$ una extensión algebraica. Un elemento $a \in \mathbb{K}$ se dice separable sobre $\mathbb{F}$ si su polinomio irreducible asociado es separable sobre $\mathbb{F}$. La extensión $\mathbb{K}|\mathbb{F}$ se dice separable si todo elemento $a \in \mathbb{K}$ es separable sobre $\mathbb{F}$.

– Teorema (Automorfismo de Frobenius) –

Sea $\mathbb{K}$ un cuerpo finito. Entonces $\mathbb{K}$ es una extensión separable de $\mathbb{Z}_p$ y, por tanto, de cualquier $\mathbb{F}$ con $\mathbb{Z}_p \subseteq \mathbb{F} \subseteq \mathbb{K}$. El grupo de $\mathbb{F}$-automorfismos de $\mathbb{K}$, $Aut_{\mathbb{F}}(\mathbb{K})$, es un grupo cíclico generado por el automorfismo de Frobenius $\phi(a) = a^q$ con $q = |\mathbb{F}|$. El orden de ϕ es $n = [\mathbb{K} : \mathbb{F}]$.

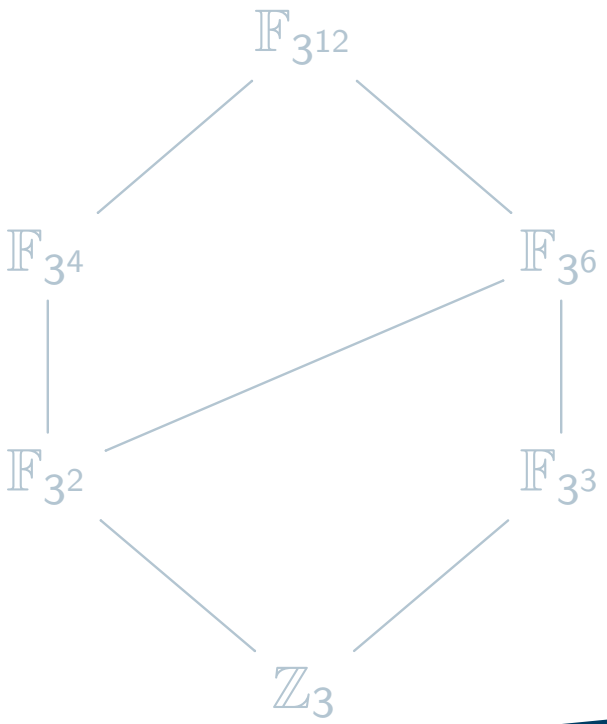
– Corolario –

Sea f un polinomio irreducible de grado n en $\mathbb{F}_q[x]$. El cuerpo de descomposición de f sobre $\mathbb{F}_q$ es $\mathbb{K} = \mathbb{F}_{q^n}$.

Subcuerpos, traza y norma. Bases

– Teorema del subcuerpo –

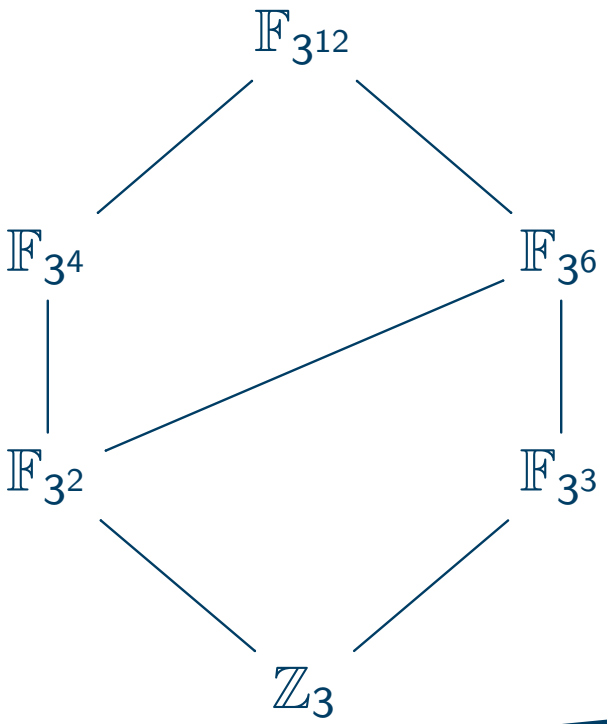
Sean $\mathbb{K}$ y $\mathbb{F}$ cuerpos finitos tales que $|\mathbb{K}| = p^n$ y $|\mathbb{F}| = p^m$. Entonces $\mathbb{F}$ es un subcuerpo de $\mathbb{K}$ si y sólo si $m|n$.



Subcuerpos, traza y norma. Bases

– Teorema del subcuerpo –

Sean $\mathbb{K}$ y $\mathbb{F}$ cuerpos finitos tales que $|\mathbb{K}| = p^n$ y $|\mathbb{F}| = p^m$. Entonces $\mathbb{F}$ es un subcuerpo de $\mathbb{K}$ si y sólo si $m|n$.



– Corolario –

1. Sean $\mathbb{K}$ un cuerpo finito tal que $|\mathbb{K}| = q = p^m$ y $n \geq 1$ un número natural. Entonces, existe una extensión simple de $\mathbb{K}$, $\mathbb{K}(a)$, con $|\mathbb{K}(a) : \mathbb{K}| = n$.
2. Si $\mathbb{K}_1$ y $\mathbb{K}_2$ son extensiones de $\mathbb{K}$ y $[\mathbb{K}_1 : \mathbb{K}] = n = [\mathbb{K}_2 : \mathbb{K}]$, entonces $\mathbb{K}_1$ y $\mathbb{K}_2$ son $\mathbb{K}$-isomorfas.
3. Para todo natural $n \geq 1$ existe un polinomio irreducible de grado n sobre $\mathbb{K}$.

Sean $\mathbb{F} = \mathbb{F}_q$ un cuerpo finito y $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. Para cada elemento $a \in \mathbb{K}$, la traza de a, $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ se define como

$$\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a) = a + a^q + \cdots + a^{q^{n-1}}.$$

Si $\mathbb{F}$ es el cuerpo primo de $\mathbb{K}$, entonces $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ se llama traza absoluta de a y se denota por $\mathrm{Tr}_{\mathbb{K}}(a)$.

Dado un elemento $a \in \mathbb{K}$, su traza es la suma de todas las imágenes de a por las diferentes potencias del automorfismo de Frobenius, ϕ. Por ello, $\phi(\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)) = \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ para todo $a \in \mathbb{K}$. Y entonces, $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a) \in \mathbb{F}$ para todo $a \in \mathbb{K}$.

Sean $\mathbb{F} = \mathbb{F}_q$ un cuerpo finito y $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. Para cada elemento $a \in \mathbb{K}$, la traza de a, $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ se define como

$$\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a) = a + a^q + \cdots + a^{q^{n-1}}.$$

Si $\mathbb{F}$ es el cuerpo primo de $\mathbb{K}$, entonces $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ se llama traza absoluta de a y se denota por $\mathrm{Tr}_{\mathbb{K}}(a)$.

Dado un elemento $a \in \mathbb{K}$, su traza es la suma de todas las imágenes de a por las diferentes potencias del automorfismo de Frobenius, ϕ. Por ello, $\phi(\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)) = \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ para todo $a \in \mathbb{K}$. Y entonces, $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a) \in \mathbb{F}$ para todo $a \in \mathbb{K}$.

– Teorema (propiedades de la traza) –

Sea $\mathbb{F} = \mathbb{F}_q$ y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. La función traza satisface las siguientes propiedades:

1. $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a+b) = \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a) + \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(b)$ para todo $a, b \in \mathbb{K}$.
2. $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(ca) = c\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ para todo $c \in \mathbb{F}$ y $a \in \mathbb{K}$.
3. $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}$ es una transformación lineal suprayectiva de $\mathbb{K}$ en $\mathbb{F}$.
4. $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a) = na$ para todo $a \in \mathbb{F}$.
5. $\mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a^q) = \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(a)$ para todo $a \in \mathbb{K}$.

– Teorema –

Sea $\mathbb{F}$ un cuerpo finito. Sean $\mathbb{K}$ una extensión finita de $\mathbb{F}$ y $\mathbb{L}$ una extensión finita de $\mathbb{K}$. Entonces, para todo $a \in \mathbb{L}$,

$$\mathrm{Tr}_{\mathbb{L}|\mathbb{F}}(a) = \mathrm{Tr}_{\mathbb{K}|\mathbb{F}}(\mathrm{Tr}_{\mathbb{L}|\mathbb{K}}(a)).$$

Sea $\mathbb{F} = \mathbb{F}_q$ un cuerpo finito y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. La norma $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a)$ de un elemento $a \in \mathbb{K}$ sobre $\mathbb{F}$ se define como

$$\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a) = a \cdot a^q \cdot \cdots \cdot a^{q^{n-1}}.$$

La imagen de $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a)$, para todo $a \in \mathbb{K}$ es invariante por el automorfismo de Frobenius. Por ello, $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a) \in \mathbb{F}$ para todo $a \in \mathbb{K}$.

Sea $\mathbb{F} = \mathbb{F}_q$ un cuerpo finito y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. La norma $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a)$ de un elemento $a \in \mathbb{K}$ sobre $\mathbb{F}$ se define como

$$\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a) = a \cdot a^q \cdot \cdots \cdot a^{q^{n-1}}.$$

La imagen de $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a)$, para todo $a \in \mathbb{K}$ es invariante por el automorfismo de Frobenius. Por ello, $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a) \in \mathbb{F}$ para todo $a \in \mathbb{K}$.

– Teorema (propiedades de la norma) –

Sea $\mathbb{F} = \mathbb{F}_q$ y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. La función norma satisface las siguientes propiedades:

1. $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(ab) = \mathrm{N}_{\mathbb{K}|\mathbb{F}}(a)\mathrm{N}_{\mathbb{K}|\mathbb{F}}(b)$ para todo $a, b \in \mathbb{K}$.
2. $N_{\mathbb{K}|\mathbb{F}}$ es una transformación lineal suprayectiva de $\mathbb{K}$ en $\mathbb{F}$ y de $\mathbb{K}^*$ en $\mathbb{F}^*$.
3. $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a) = a^n$ para todo $a \in \mathbb{F}$.
4. $\mathrm{N}_{\mathbb{K}|\mathbb{F}}(a^q) = \mathrm{N}_{\mathbb{K}|\mathbb{F}}(a)$ para todo $a \in \mathbb{K}$.

– Teorema –

Sea $\mathbb{F}$ un cuerpo finito. Sean $\mathbb{K}$ una extensión finita de $\mathbb{F}$ y $\mathbb{L}$ una extensión finita de $\mathbb{K}$. Entonces, para todo $a \in \mathbb{L}$,

$$\mathrm{N}_{\mathbb{L}|\mathbb{F}}(a) = \mathrm{N}_{\mathbb{K}|\mathbb{F}}(\mathrm{N}_{\mathbb{L}|\mathbb{K}}(a)).$$

Nota:
Sea $\mathbb{F}$ un cuerpo finito y $\mathbb{K}$ una extensión finita de $\mathbb{F}$. Si consideramos para cada $\alpha \in \mathbb{K}$ el endomorfismo de $\mathbb{F}$-espacios vectoriales

$$x \in \mathbb{K} \mapsto \alpha x$$

entonces la norma y la traza son los dos coeficientes correspondientes del polinomio característico del endomorfismo.

Sea $\mathbb{F} = \mathbb{F}_q$ y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. Una $\mathbb{F}$-base de $\mathbb{K}$ de la forma $\{a, a^q \ldots, a^{q^{n-1}}\}$, que consiste en un elemento a adecuado y todos sus $\mathbb{F}$-conjugados, recibe el nombre de base normal de $\mathbb{K}$ sobre $\mathbb{F}$.

– Teorema –

Sea $\mathbb{F} = \mathbb{F}_q$ un cuerpo finito y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. El conjunto $\{a_1, \ldots, a_n\}$ es una $\mathbb{F}$-base de $\mathbb{K}$ si y sólo si

$$\begin{vmatrix} a_1 & a_2 & \cdots & a_n \\ a_1^q & a_2^q & \cdots & a_n^q \\ \vdots & \vdots & & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_n^{q^{n-1}} \end{vmatrix} \neq 0$$

Sea $\mathbb{F} = \mathbb{F}_q$ y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. Una $\mathbb{F}$-base de $\mathbb{K}$ de la forma $\{a, a^q \ldots, a^{q^{n-1}}\}$, que consiste en un elemento a adecuado y todos sus $\mathbb{F}$-conjugados, recibe el nombre de base normal de $\mathbb{K}$ sobre $\mathbb{F}$.

– Teorema –

Sea $\mathbb{F} = \mathbb{F}_q$ un cuerpo finito y sea $\mathbb{K} = \mathbb{F}_{q^n}$ una extensión suya. El conjunto $\{a_1, \ldots, a_n\}$ es una $\mathbb{F}$-base de $\mathbb{K}$ si y sólo si

$$\begin{vmatrix} a_1 & a_2 & \cdots & a_n \\ a_1^q & a_2^q & \cdots & a_n^q \\ \vdots & \vdots & & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_n^{q^{n-1}} \end{vmatrix} \neq 0$$

Estructura multiplicativa

Sea $\mathbb{K}$ un cuerpo de característica $p \geq 0$ y sea n un número natural. Se llama n-simo cuerpo ciclotómico sobre $\mathbb{K}$, denotado por $\mathbb{K}^{(n)}$, al cuerpo de descomposición sobre $\mathbb{K}$ del polinomio $x^n - 1 \in \mathbb{K}[x]$. El conjunto de raíces de ese polinomio en $\mathbb{K}^{(n)}$ se llama conjunto de n-raíces de la unidad sobre $\mathbb{K}$ y se denota por $E^{(n)}$.

– Proposición –

1. $E^{(n)}$ es un subgrupo cíclico finito del grupo multiplicativo $\mathbb{K}^{(n)} \setminus \{0\}$. Si $p \nmid n$ (en particular si $p = 0$), entonces $E^{(n)}$ es un grupo cíclico de orden n.
2. Si $E^{(n)} = \langle \xi \rangle$, entonces $\mathbb{K}^{(n)} = \mathbb{K}(\xi)$.
3. Si $n = mp^a$ con $(m, p) = 1$, entonces se tiene que $E^{(m)} = E^{(n)}$ y $\mathbb{K}^{(m)} = \mathbb{K}^{(n)}$.

Sea $\mathbb{K}$ un cuerpo de característica $p \geq 0$. Sea $n \in \mathbb{N}$ tal que $(n, p) = 1$. Se llama n-raíz primitiva de la unidad, ξ, a cualquier generador de $E^{(n)}$. El polinomio que tiene como raíces todas las n-raíces primitivas de la unidad recibe el nombre de n-simo polinomio ciclotómico y se representa por $\phi_n(x)$.

Si ξ es una n-raíz primitiva de la unidad, entonces $\xi^n = 1$ mientras que $\xi^m \neq 1$ para cualquier $m < n$. Por otra parte, es fácil ver que ξ^s es n-raíz primitiva para todo s relativamente primo con n. Así pues, el n-simo polinomio ciclotómico se puede escribir como

$$\phi_n(x) = \prod_{(s,n)=1, s<n} (x - \xi^s) \in \mathbb{K}^{(n)}[x].$$

Por tanto, si φ representa la función de Euler, el grado de $\phi_n(x)$ será $\varphi(n)$.

Sea $\mathbb{K}$ un cuerpo de característica $p \geq 0$. Sea $n \in \mathbb{N}$ tal que $(n, p) = 1$. Se llama n-raíz primitiva de la unidad, ξ, a cualquier generador de $E^{(n)}$. El polinomio que tiene como raíces todas las n-raíces primitivas de la unidad recibe el nombre de n-simo polinomio ciclotómico y se representa por $\phi_n(x)$.

Si ξ es una n-raíz primitiva de la unidad, entonces $\xi^n = 1$ mientras que $\xi^m \neq 1$ para cualquier $m < n$. Por otra parte, es fácil ver que ξ^s es n-raíz primitiva para todo s relativamente primo con n. Así pues, el n-simo polinomio ciclotómico se puede escribir como

$$\phi_n(x) = \prod_{(s,n)=1, s<n} (x - \xi^s) \in \mathbb{K}^{(n)}[x].$$

Por tanto, si φ representa la función de Euler, el grado de $\phi_n(x)$ será $\varphi(n)$.

Sea $\mathbb{K} = \mathbb{Q}$ y $n = 4$. En ese caso,

$$E^{(4)} = \{1, -1, i, -i\} = \langle i \rangle = \langle -i = i^3 \rangle.$$

Así pues, las 4-raíces primitivas de la unidad son $\{i, -i\}$ y el cuarto polinomio ciclotómico

$$\phi_4(x) = (x - i)(x + i) = x^2 + 1.$$

– Proposición –

1. $x^n - 1 = \prod_{d|n} \phi_d(x)$.
2. Si $\mathbb{F}$ es el cuerpo primo de $\mathbb{K}$, entonces $\phi_n(x) \in \mathbb{F}[x]$. Si la característica de $\mathbb{F}$ es cero, entonces $\phi_n(x) \in \mathbb{Z}[x]$.

La proposición anterior permite calcular los polinomios ciclotómicos de forma recursiva. Es fácil ver que $\phi_1(x) = x-1$ y que $\phi_2(x) = x+1$, pues 1 y -1 son, respectivamente, 1-raíces y 2-raíces primitivas de la unidad. Ahora bien, utilizando la proposición anterior podemos ver que

$$\phi_3(x) = \frac{x^3-1}{\phi_1(x)} = \frac{x^3-1}{x-1} = x^2+x+1,$$
$$\phi_4(x) = \frac{x^4-1}{\phi_1(x)\phi_2(x)} = \frac{x^4-1}{(x-1)(x+1)} = x^2+1.$$

Y así sucesivamente.

– Proposición –

Sea $\mathbb{K} = \mathbb{F}_q$. Entonces $\mathbb{K}$ es el $(q-1)$-simo cuerpo ciclotómico sobre cualquier subcuerpo suyo $\mathbb{F}$.

– Proposición –

Sea $d \neq n$ un divisor de n. Entonces, el n-simo polinomio ciclotómico $\phi_n(x)$ divide al cociente $\frac{x^n-1}{x^d-1}$ en $\Pi[x]$, donde Π representa el cuerpo primo.

– Proposición –

Sea $\mathbb{K} = \mathbb{F}_q$. Entonces $\mathbb{K}$ es el $(q-1)$-simo cuerpo ciclotómico sobre cualquier subcuerpo suyo $\mathbb{F}$.

– Proposición –

Sea $d \neq n$ un divisor de n. Entonces, el n-simo polinomio ciclotómico $\phi_n(x)$ divide al cociente $\frac{x^n-1}{x^d-1}$ en $\Pi[x]$, donde Π representa el cuerpo primo.

– Teorema –

Sea $\mathbb{K} = \mathbb{F}_q$. Entonces $\phi_n(x)$ se factoriza como producto de $\frac{\phi(n)}{d}$ factores irreducibles del mismo grado d. Además, d es el menor nmero natural que cumple $q^d \equiv 1 (\text{mod } n)$. Si la característica de $\mathbb{K}$ es cero, entonces $\phi_n(x)$ es irreducible en $\mathbb{Q}[x]$ y, por tanto, en $\mathbb{Z}[x]$.

Ejemplo:

Sea $\phi_{12}(x) = x^4 - x^2 + 1$ el 12-polinomio ciclotómico. Por el resultado anterior, este polinomio es irreducible en $\mathbb{Q}[x]$ y, por tanto, sobre $\mathbb{Z}[x]$. Si ahora trabajamos sobre $\mathbb{F}_7[x]$, puesto que $7^2 \equiv 1 (\text{mod } 12)$, el polinomio $\phi_{12}(x)$ se factoriza como producto de dos polinomios irreducibles de grado 2. Esto es,

$$\phi_{12}(x) = x^4 - x^2 + 1 = (x^2 + 2)(x^2 + 4).$$

Lo mismo sucede sobre $\mathbb{F}_{11}[x]$. En este caso, $11^2 \equiv 1 (\text{mod } 12)$ y entonces

$$\phi_{12}(x) = x^4 - x^2 + 1 = (x^2 + 6x + 1)(x^2 + 5x + 1).$$

Por ltimo, puesto que $\mathbb{F}_{13}$ es cuerpo de descomposición del polinomio $x^{12} - 1$, el polinomio $\phi_{12}(x)$ deberá escindirse sobre él y factorizarse como producto de cuatro polinomios de grado uno. Esto es,

$$\phi_{12}(x) = x^4 - x^2 + 1 = (x + 2)(x + 6)(x + 7)(x + 11).$$