AMPLIACIÓN DE MATEMÁTICAS

OTROS RESULTADOS SOBRE CUERPOS FINITOS.

El grupo multiplicativo de un cuerpo finito es como hemos visto un grupo **cíclico**. Lo cuál nos permite encontrar propiedades especiales de los cuerpos finitos.

Corolario 1. *Sea $\mathbb{F}$ un cuerpo finito de q elementos. Sea $\alpha \in \mathbb{F}^*$ un elemento* ***primitivo*** *(es decir un generador del grupo multiplicativo). Entonces*

$$\mathbb{F} = \{\, 0, 1, \alpha, \alpha^2, ..., \alpha^{q-2} \,\}$$

donde $\alpha^{q-1} = 1$. Además, α^k es otro elemento primitivo de $\mathbb{F}$ si y solo si $m.c.d(k, q-1) = 1$.

Demostración: $(\mathbb{F}^*, \times)$ es un cíclico y α por definición es un generador del grupo. Luego sus potencias recorren todos los elementos de $\mathbb{F}^*$ (ver el Tema de Grupos). Si añadimos a $\mathbb{F}^*$ el 0 ya tenemos todos los elementos del cuerpo $\mathbb{F}$.

Por otro lado si $m.c.d.(k, q-1) = 1$, se tiene que $m.c.m.(k, q-1) = k(q-1)$. Luego

$$(\alpha^k)^r = 1 \qquad \Leftrightarrow \qquad q - 1 \,|\, kr.$$

Como k y $q-1$ no tienen divisores comunes, se tiene que $q - 1 \,|\, r$, lo que prueba que α^k es un generador de $\mathbb{F}^*$ $\square$

Observación 1.

$$Card\{k \in \mathbb{Z}_{q-1} \;:\; m.c.d.(k, q-1)\,\} = \varphi(q-1),$$

donde φ es la función de Euler.

Teorema 1. *Sea $\mathbb{F}$ un cuerpo finito y sean $\alpha_1, ..., \alpha_k$ elementos* ***algebraicos*** *sobre $\mathbb{F}$ (pertenecientes a alguna extensión del cuerpo $\mathbb{F}$).*

Entonces existe algún $\alpha \in \mathbb{F}(\alpha_1, ..., \alpha_k)$ *de modo que*

$$\mathbb{F}(\alpha) = \mathbb{F}(\alpha_1, ..., \alpha_k).$$

Demostración: Como sabemos $\mathbb{F}(\alpha_1, ..., \alpha_k)$ es el menor cuerpo $\mathbb{K}$ que contiene a $\mathbb{F}$ y a los elementos $\alpha_1, ..., \alpha_k$ (ver el capítulo de Cuerpos de Descomposición, en el apéndice anterior). $\mathbb{K}$ es un extensión finita de $\mathbb{F}$ (ya que cada α_j es un elemento algebraico sobre $\mathbb{F}$), $\mathbb{F}$ es un cuerpo finito, por tanto $\mathbb{K}$ también es un cuerpo finito. Existe en $\mathbb{K}$ un elemento primitivo $\alpha \in \mathbb{K}$. $\mathbb{F}(\alpha)$ es el menor cuerpo que contiene al cuerpo $\mathbb{F}$ y a α, por tanto $\mathbb{F}(\alpha) \subseteq \mathbb{K}$. Como α genera todo el grupo multiplicativo de $\mathbb{K}$, es claro que $\mathbb{F}(\alpha) = \mathbb{K}$ $\square$

Corolario 2. *Sea* $\mathbb{F}$ *un cuerpo finito de característica* p *y sea* $[\mathbb{F} : \mathbb{Z}_p] = n$ *(*n *es la dimensión de* $\mathbb{F}$ *como espacio vectorial sobre* $\mathbb{Z}_p$*). Entonces existe* $\alpha \in \mathbb{F}$*, algebraico de grado* n *sobre* $\mathbb{Z}_p$*, de modo que* $\mathbb{F} = \mathbb{Z}_p(\alpha)$*.*

Demostración: $\mathbb{F}$ es un espacio vectorial sobre $\mathbb{Z}_p$ de dimensión n. Sea $1, \alpha_1, ..., \alpha_{n-1} \in \mathbb{F}$ una base de $\mathbb{F}$. Así,

$$\mathbb{F} = \{\, a_0 + a_1\alpha_1 + ... + a_{n-1}\alpha_{n-1} : a_0, ..., a_{n-1} \in \mathbb{Z}_p \,\} = \mathbb{Z}_p(1, \alpha_1, ..., \alpha_{n-1}) = \mathbb{Z}_p(\alpha)$$

donde la última igualda nos viene dada por el teorema anterior.

Sea ahora f el polinomio mínimo de α con respecto a $\mathbb{Z}_p$. Vimos que $\mathbb{Z}_p(\alpha)$ es isomorfo a $\mathbb{Z}_p[x]/f$ (ver capítulo de Extensiones Finitas y Polinomio Mínimo). Para que esto sea así claramente el grado de f tiene que ser n

$$(n = [\mathbb{F} : \mathbb{Z}_p] = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = [\mathbb{Z}_p[x]/f : \mathbb{Z}_p] = grad.f) \ \square$$

Teorema 2. **a:** *Todo cuerpo finito* $\mathbb{F}$ *tiene cardinal igual a* p^n *(*$|\mathbb{F}| = p^n$*), donde* p *es la característica de* $\mathbb{F}$ *(*$Char.\mathbb{F} = p$*) y* n *es algún número natural (*$n \in \mathbb{N}$*).*

b: *Para todo* p *primo y para todo* $n \in \mathbb{N}$*, existe un cuerpo* $\mathbb{F}$ *con cardinal igual a* p^n*.*

c: *Todo cuerpo finito de orden (o cardinal)* p^n *es, salvo isomorfismo, el* ***cuerpo de descomposición*** *del polinomio* $x^{p^n} - x \in \mathbb{Z}_p[x]$ *(y también del polinomio* $x^{p^n-1} - 1 \in \mathbb{Z}_p[x]$*).*

d: *Dos cuerpos finitos de orden* p^n *son isomorfos.*

Demostración: **a)** Ya lo hemos visto en el primer capítulo sobre cuerpos finitos.

b) Consideremos el polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$. Sea $\mathbb{K}$ el cuerpo finito donde se descompone el polinomio anterior; así

$$x^{p^n} - x = \Pi_{i=1}^{p^n}(x - \alpha_i)$$

con $\alpha_i \in \mathbb{K}$ para todo $i = 1, 2, ..., p^n$ ($\mathbb{K}$ sabemos que existe, que es finito y de característica p por el Teorema de Kronecker). Sea

$$A = \{\alpha_i \in \mathbb{K} : i = 1, 2, ..., p^n\} \subseteq \mathbb{K},$$

el conjunto de todas las raíces del polinomio $x^{p^n} - x$. Veamos que $(A, +, \times)$ es un cuerpo. Como $\mathbb{K}$ tiene característica p,

$$(\alpha_i+\alpha_j)^{p^n} - (\alpha_i+\alpha_j) = \alpha_i^{p^n} + \alpha_j^{p^n} - (\alpha_i+\alpha_j) = \alpha_i^{p^n} - \alpha_i + \alpha_j^{p^n} - \alpha_j = 0,$$

luego $\alpha_i + \alpha_j \in A$. Además, como $\alpha_j^{p^n} = \alpha_j$ se sigue que

$$(\alpha_i\alpha_j)^{p^n} - \alpha_i\alpha_j = \alpha_i\alpha_j(\alpha^{p^n-1} - 1) = 0,$$

ya que si $\alpha_i = 0$, es clara la último igualdad; y si no se tiene que $\alpha^{p^n-1} - 1 = 0$. Por tanto $\alpha_i\alpha_j \in A$. Hemos visto que la suma y el producto son **cerrados** en A. Solo nos queda ver que los opuestos e inversos de los elementos de A están tanbién en A para concluir que A es un cuerpo.

Como p es impar (es un primo) se tiene que p^n también es impar, y así

$$(-\alpha_i)^{p^n} - (-\alpha_i) = (-1)^{p^n}(\alpha_i)^{p^n} - (-\alpha_i) = -(\alpha_i^{p^n} - \alpha_i) = 0,$$

lo que prueba que $-\alpha_i \in A$.

Por otro lado si $\alpha_i \neq 0$, entonces

$$0 = \alpha_i^{p^n-1} - 1 \qquad \Rightarrow \qquad \alpha_i\alpha_i^{p^n-2} = 1,$$

lo que muestra que $\alpha_i^{-1} = \alpha_i^{p^n-2}$. Ahora

$$(\alpha_i^{p^n-2})^{p^n-1} = (\alpha_i^{p^n-1})^{p^n-2} = 1,$$

lo que prueba que $\alpha_i^{-1} \in A$.

Hemos visto que A es un cuerpo y como en él se descompone $x^{p^n} - x$, se tiene que $A = \mathbb{K}$. Además, como estamos en característica p,

$$m.c.d.(x^{p^n} - x, p^n x^{p^n-1} - 1) = m.c.d.(x^{p^n} - x, -1) = 1.$$

Lo anterior prueba que todas las raíces de $x^{p^n} - x$ son simples (ver el tema de Polinomios), lo que nos dice que el cardinal de A es exactamente p^n ($|A| = Card.A = p^n$).

c) y d) Sea $\mathbb{K}'$ un cuerpo de cardinal p^n, con p primo y $n \in \mathbb{N}$. Así la característica del cuerpo es p y tenemos que

$$\mathbb{Z}_p \hookrightarrow \mathbb{K}'.$$

Sea ahora A el cuerpo de descomposición del polinomio $x^{p^n} - x$ (ver el apartado anterior **b)**). Tenemos que

$$[\mathbb{K}' : \mathbb{Z}_p] = [A : \mathbb{Z}_p] = n.$$

Por el corolario anterior existen $\alpha \in \mathbb{K}'$ y $\alpha' \in A$ de modo que

$$\mathbb{Z}_p(\alpha) = \mathbb{K}' \qquad \text{y} \qquad \mathbb{Z}_p(\alpha') = A.$$

Por el último teorema del capítulo de Extensiones Finitas. Polinomio Mínimo sabemos que

$$\mathbb{Z}_p(\alpha) = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \ : \ a_0, a_1, ..., a_{n-1} \in \mathbb{Z}_p \ \}$$

y que

$$\mathbb{Z}_p(\alpha') = \{a_0 + a_1\alpha' + ... + a_{n-1}\alpha'^{n-1} \ : \ a_0, a_1, ..., a_{n-1} \in \mathbb{Z}_p \ \}.$$

Luego identificando α con α' se llega a que $\mathbb{K}'$ y A son isomorfos $\square$

Observación 2. *En un cuerpo finito $\mathbb{F}$ de característica p todo elemento $a \in \mathbb{F}$ tiene una raíz p-ésima (existe $\sqrt[p]{a}$).*

Claro, salvo isomororfismo, $\mathbb{F}$ es el cuerpo de todas las raíces del polinomio $x^{p^n} - x$, donde $p^n = card.\mathbb{F}$. Luego

$$(a^{p^{n-1}})^p = a \qquad \Rightarrow \qquad \sqrt[p]{a} = a^{p^{n-1}}.$$

Recordemos que la existencia de la raíz p-ésima de un elemento del cuerpo se utiliza para ver la forma de los polinomios con raíces múltiples (ver el capítulo de Raíces Múltiples, en el tema de Polinomios) $\square$

Observación 3. *Sea $\mathbb{F}$ un cuerpo finito de característica p y sea $f \in \mathbb{F}[x]$ un polinomio irreducible sobre $\mathbb{F}$. Todas las raíces de f son simples.*

Claro, vimos que un polinomio irreducible tenía raíces simples si y solo si su derivada no era nula ($f' \neq 0$). Si $f' = 0$ y $\mathbb{F}$ es finito, entonces vimos que existe $g \in \mathbb{F}[x]$ de modo que $f = g^p$, luego f no sería irreducible $\square$

Corolario 3. *Sea $\mathbb{F}$ un cuerpo finito y sea $f \in \mathbb{F}[x]$ un polinomio irreducible de grado mayor que* 1. *El cuerpo de descomposición de f es precisamente $\mathbb{F}[x]/f$.*

Demostracción: Supongamos que $grad.f = n$. Por la Observación anterior f tiene n raíces distintas en su cuerpo de descomposición. Si éstas son $\alpha_1, \alpha_2, .., \alpha_n$, el cuerpo de descomposición de f es

$$\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, .., \alpha_n)$$

(ver el capítulo de Cuerpos de Descomposición). Por ser $\mathbb{F}$ finito y las raíces α_j claramente algebraicas sobre $\mathbb{F}$, el cuerpo de descomposición es una extensión finita de $\mathbb{F}$ (por tanto también algebraica). Supongamos que $[\mathbb{K} : \mathbb{F}] = k$. Como los cuerpos finitos de igual orden son isomorfos, sea una raíz de f para la cuál $\alpha \in \mathbb{F}_{\mathbb{F}^k} \backslash \mathbb{F}_{\mathbb{F}^{k-1}}$ (donde notamos por $\mathbb{F}_{p^r}$ el cuerpo finito de orden p^r). α tiene que existir, de otro modo $\mathbb{F}_{\mathbb{F}^{k-1}}$ sería el cuerpo de descomposición.

El polinomio mínimo de α sobre $\mathbb{F}$ es f. Veámoslo. Si hubiese otro de grado menor, pongamos g, como $\mathbb{F}(\alpha)$ es isomorfo a $\mathbb{F}[x]/g$ (ver capítulo de Extensiones Finita. Polinomio Mínimo), se tendría que $\alpha \in \mathbb{F}_{\mathbb{F}^{k-1}}$ ya que

$$\mathbb{F}[x]/g \subsetneq \mathbb{F}[x]/f \subsetneqq \mathbb{K}.$$

Por lo tanto $\mathbb{F}(\alpha)$ es isomorfo a $\mathbb{F}[x]/f$. Por otro lado $\mathbb{F}(\alpha) \subsetneqq \mathbb{K}$ y $\alpha \in \mathbb{F}_{\mathbb{F}^k} \backslash \mathbb{F}_{\mathbb{F}^{k-1}}$, luego el orden de $\mathbb{F}(\alpha)$ será

$$|\mathbb{F}(\alpha)| \geq |\mathbb{F}|^k > |\mathbb{F}|^{k-1}.$$

Por tanto $\mathbb{F}(\alpha) = \mathbb{K}$ □

Ejemplo 1. *Los cuerpos* $\mathbb{Z}_2[x]/x^3 + x + 1$ *y* $\mathbb{Z}_2[x]/x^3 + x^2 + 1$ *son iguales, salvo isomorfismo.*

Los polinomios $x^3 + x + 1$ y $x^3 + x^2 + 1$ no tienen raíces en $\mathbb{Z}_2$ y como son de grado tres ambos son irreducibles. Por tanto los cocientes $\mathbb{Z}_2[x]/x^3+x+1$ y $\mathbb{Z}_2[x]/x^3+x^2+1$ son cuerpos de orden $2^3 = 8$ (Teorema de Kronecker). Sabemos que dos cuerpos finitos de igual orden son isomorfo, lo cuál termina la prueba □

Corolario 4. *Para todo* $n \in \mathbb{N}$ *y para todo* p *primo, el cuerpo finito de* p^n *elementos* ($\mathbb{F}_{p^n}$) *es el cuerpo de descomposición de un polinomio irreducible de grado* n *en* $\mathbb{Z}_p[x]$. *En particular, siempro podemos encontrar polinomios irreducible de grado* n *en* $\mathbb{Z}_p[x]$ *para todo* $n \in \mathbb{N}$.

Demostracción: Sea $\mathbb{F}$ un cuerpo finito con $|\mathbb{F}| = p^n$. Como $(\mathbb{F}^*, \times)$ es un grupo cíclico, existe un **elemento primario** $\alpha \in \mathbb{F}$ (es decir α

genera $\mathbb{F}^* = \{1, \alpha, ..., \alpha^{p^n-2}\}$ y $\alpha^{p^n-1} = 1$). Sea $f \in \mathbb{Z}_p[x]$ el polinomio mínimo de α con respecto a $\mathbb{Z}_p[x]$ (es decir el **polinomio primitivo** de α). Ahora se tiene que

$$\mathbb{F} = \mathbb{Z}_p(\alpha) \qquad \text{isomorfo a} \qquad \mathbb{Z}_p[x]/f.$$

Así

$$n = [\mathbb{F} : \mathbb{Z}_p] = [\mathbb{Z}_p[x]/f : \mathbb{Z}_p] = grad.f.$$

Luego f es el polinomio que buscábamos $\square$

Este resultado es propio de los cuerpos finitos, como muestra el siguiente ejemplo.

Ejemplo 2. *En* $\mathbb{R}[x]$ *los polinomios irreducibles solo pueden tener grado* 1 *o* 2.

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

E-mail address: Cesar_Ruiz@mat.ucm.es