

Caracterización de los cuerpos finitos

Nuestro siguiente objetivo es probar que todo cuerpo finito tiene orden potencia de un número primo.

Y recíprocamente, que para cada potencia de un primo p existe un cuerpo finito con exactamente esa cantidad de elementos.

Lema: K subcuerpo de F y $|K|=q \Rightarrow F$ tiene q^r elementos $r=[F:K]$.

Teorema: Si F es un cuerpo finito entonces F tiene p^n elementos donde p es la característica de F y n es el grado de extensión de F sobre su cuerpo primo.

Demostación

Como F es un cuerpo finito, su característica es un número primo p . Entonces, el subcuerpo primo K de F es isomorfo a $\mathbb{F}_p$ y por lo tanto tiene p elementos.

Además podemos considerar a F como espacio vectorial sobre K , más aún F es de dimensión finita sobre K , digamos $n=[F:K]$.

Entonces existe una base $\{\beta_1, \dots, \beta_n\}$ de F sobre K y cada $\alpha \in F$ se puede escribir como

$$\alpha = a_1 \beta_1 + \dots + a_n \beta_n \quad \text{donde } a_1, \dots, a_n \in K.$$

Luego como cada $a_i \in k$ y $|k| = p$ tenemos en $\mathbb{F}$ p^n elementos. 

Empezando con $\mathbb{F}_p$, p primo, vemos que podemos construir un cuerpo finito con p^n elementos con el proceso de adjuntar una raíz de un polinomio irreducible $f \in \mathbb{F}_p[x]$. Sin embargo no sabemos aún, si podemos garantizar que siempre existe un polinomio irreducible sobre $\mathbb{F}_p$ y de grado n para cualquier n . Antes de probar que esto es cierto necesitamos algunos resultados previos.

Recordemos que del Teorema de Lagrange para grupos finitos se desprende que si G es un grupo finito el orden de cualquier subgrupo H de G divide al orden de G , y el orden de cualquier elemento $a \in G$ divide al orden de G .

En particular, si $\mathbb{F}$ es un cuerpo ^{finito de orden q} podemos considerar $\mathbb{F}^*$ el grupo multiplicativo formado por los elementos no nulos de $\mathbb{F}$, que tiene orden $q-1$ y por lo tanto si $a \in \mathbb{F}^*$ y $n = \text{ord}(a)$ entonces $n \mid q-1$ o lo que es lo mismo $q-1 = k \cdot n$.

Pero entonces

$$a^{q-1} = a^{u \cdot n} = (a^n)^u = 1^u = 1 \quad \text{en } \mathbb{F}^*.$$

Entonces tenemos el siguiente Lema

Lema: Si $\mathbb{F}$ es un cuerpo finito con q elementos entonces para todo $a \in \mathbb{F}$ se cumple
 $a^q = a.$

Lema: Si $\mathbb{F}$ es un cuerpo finito con q elementos y k es un subcuerpo de $\mathbb{F}$, entonces el polinomio $X^q - X$ en $k[X]$ se factoriza en $\mathbb{F}[X]$ como

$$X^q - X = \prod_{a \in \mathbb{F}} (X - a)$$

Demostración

El polinomio $X^q - X$ tiene grado q y por lo tanto tiene a lo sumo q raíces distintas en $\mathbb{F}$, pero por el lema anterior todos los elementos de $\mathbb{F}$ son raíces de ese polinomio. Luego $X^q - X$ se factoriza de la forma indicada y no puede descomponerse linealmente en ningún subcuerpo menor



Ahora sí podemos demostrar el teorema principal que caracteriza los cuerpos finitos

Teorema (Existencia y unicidad de los cuerpos finitos)

Para todo primo p y todo entero positivo n existe un cuerpo finito con p^n elementos. Cualquier cuerpo finito con p^n elementos es isomorfo al cuerpo de descomposición de $x^{p^n} - x$ sobre $\mathbb{F}_p$.

Demostración

(Existencia) Para $q = p^n$ consideremos el polinomio $f(x) = x^q - x$ en $\mathbb{F}_p[x]$

y sea F el cuerpo de descomposición de $f(x)$ sobre $\mathbb{F}_p$.

Este polinomio tiene todas sus raíces simples pues

$$f'(x) = qx^{q-1} - 1 = -1 \text{ en } \mathbb{F}_p$$

Luego f y f' no tienen raíces en común y por lo tanto f tiene q raíces simples.

Sea

$$S = \{a \in F : a^q - a = 0\} \Rightarrow S \text{ es un subcuerpo de } F \text{ y tiene } q \text{ elementos.}$$

- S tiene dos elementos: $0, 1$

- si $a, b \in S$ entonces

$$(a-b)^q = a^q - b^q = a - b \Rightarrow a-b \in S$$

$\uparrow$ $q = \text{char}(\mathbb{F}_p)^n$ $\uparrow$ $a, b \in S$

- si $a, b \in S$, $b \neq 0$ entonces $(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1} \Rightarrow ab^{-1} \in S.$

Por ejercicio 1.56 $\Rightarrow S$ es un subcuerpo de F .
Entonces como todos los raíces de $x^8 - x$ están
en S , $x^8 - x$ se descompone en S y por lo
tanto $F = S$. Luego F es un cuerpo con 8
elementos.

(Unicidad) Sea F es un cuerpo finito con $q = p^n$
elementos $\Rightarrow \text{char}(F) = p$ y por lo tanto
 $\mathbb{F}_p$ es un subcuerpo de F y por el lema
anterior es el cuerpo de descomposición de
 $x^q - x$ y por el teorema de unicidad de
los cuerpos de descomp. se obtiene la unicidad
de F (salvo isomorfismos). 

El teorema anterior garantiza, por ejemplo,
que existe un cuerpo finito con 8 elementos
y como $8 = 2^3$ y ese cuerpo es de característica
2. Ese cuerpo es isomorfo al cuerpo de
descomposición de $x^8 - x$ sobre $\mathbb{F}_2$, y para
construirlo necesitamos un polinomio irreducible
de grado 3 sobre $\mathbb{F}_2$.

Ya habíamos visto en un ejemplo anterior que

$$\mathbb{F}_2[x] / (x^3 + x^2 + 1)$$

$$\mathbb{F}_8 = \{ 0, \underbrace{1}_{\alpha^0}, \alpha, \underbrace{\alpha+1}_{\alpha^5}, \alpha^2, \underbrace{\alpha^2+1}_{\alpha^3}, \underbrace{\alpha^2+\alpha}_{\alpha^6}, \underbrace{\alpha^2+\alpha+1}_{\alpha^4} \}$$

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

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

$$\alpha^4 = \alpha \cdot \alpha^3 = \alpha(\alpha^2 + 1)$$

$$x^8 - x = x(x-1)(x-\alpha)(x-(\alpha+1))(x-\alpha^2) \dots = \alpha^3 + \alpha$$

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

$$(\alpha^2)^8 = \alpha$$

$$\alpha^5 = \alpha \cdot \alpha^4 =$$

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

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

$$(\alpha^2 + \alpha)^8 = \alpha^2 + \alpha$$

$$\alpha^6 = \alpha \cdot \alpha^5 = \alpha(\alpha+1) = \alpha^2 + \alpha$$

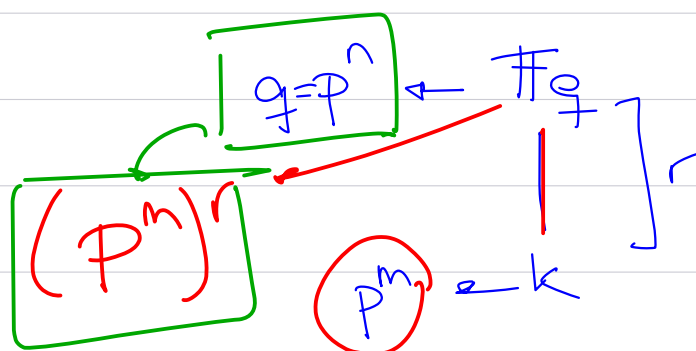
La unicidad del teorema anterior justifica que hablemos de "el cuerpo finito" (o el cuerpo de Galois) de orden q o con q elementos y lo vamos a denotar $\mathbb{F}_q$, donde q siempre es una potencia de un primo p . La notación $\text{GF}(q)$ es a veces usada para denotar a $\mathbb{F}_q$.

Teorema Sea $\mathbb{F}_q$ el cuerpo finito con $q=p^n$ elementos. Entonces cada subcuerpo de $\mathbb{F}_q$ tiene orden p^m elementos donde m es un divisor positivo de n . Recíprocamente, si m es un divisor positivo de n existe exactamente un subcuerpo de $\mathbb{F}_q$ con p^m elementos.

Demostación

Sea k un subcuerpo de $\mathbb{F}_q$. Entonces como es finito debe ser que el orden de k es p^m para algún $m \leq n$.

Además cualquier extensión $\mathbb{F}$ de grado r de k



tiene $(p^m)^r$ elementos donde $r = [\mathbb{F}:k]$ y $|k| = p^m$. Como $\mathbb{F}_q$ es una extensión finita de k , tenemos que $\mathbb{F}_q$ debe tener $(p^m)^r$ elementos, y como $q=p^n$ entonces $n = m \cdot r$ y por lo tanto m es un divisor positivo de n .

Recíprocamente, si m es un divisor positivo de n entonces

$$p^m - 1 \text{ divide a } p^n - 1$$

En efecto, si $n = m \cdot r$ entonces

$$p^n - 1 = p^{m \cdot r} - 1 = (p^m)^r - 1$$

pero para cualquier a

$$a^r - 1 = (a - 1)(a^{r-1} + a^{r-2} + \dots + a + 1)$$

con $a = p^m$

$$p^n - 1 = (p^m)^r - 1 = (p^m - 1)((p^m)^{r-1} + \dots + p^m + 1)$$

entonces $X^{p^m - 1} - 1$ divide al $X^{p^n - 1} - 1$, en

consecuencia

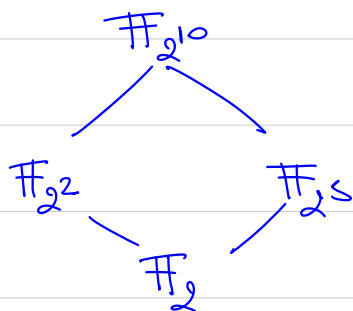
$$X^{p^m} - X \text{ divide } X^{p^n} - X = X^q - X$$

y el cuerpo de descomposición de $X^{p^m} - X$ es el subcuerpo de $\mathbb{F}_q$ con p^m elementos. $\Rightarrow$

De la prueba del teorema anterior tenemos que el único subcuerpo de $\mathbb{F}_{p^n}$ de orden p^m donde m es un divisor positivo de n , es el que contiene exactamente a las raíces del polinomio $x^{p^m} - x \in \mathbb{F}_p[x]$ en $\mathbb{F}_{p^n}$.

Por ejemplo,

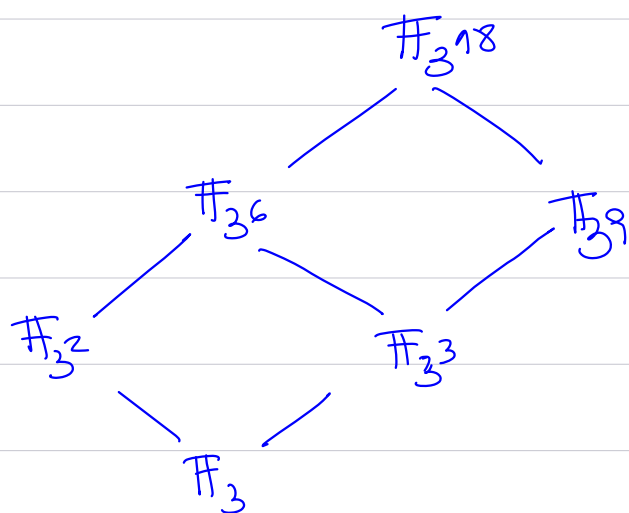
① $\mathbb{F}_{2^{10}}$ tiene como subcuerpos a $\mathbb{F}_{2^2}$ y $\mathbb{F}_{2^5}$



② $\mathbb{F}_{3^{18}}$

$$18 = 2 \cdot 3^2$$

divisores: 1, 2, 3, 6, 9, ~~18~~



③ Qo! $\mathbb{F}_8 = \mathbb{F}_{2^3}$ no es subcuerpo de $\mathbb{F}_{16} = 2^4$

pues $3 \nmid 4$.

$$30 = 2 \cdot 15 = 2 \cdot 3 \cdot 5$$

$\mathbb{F}_{2^{30}}$

divisores $1, 2, 3, 5, 6, 10, 15, 30$

