Caracterización de cuerpos finitos

Kevin Velez

Universidad del Valle

Febrero 7, 2023

Caracterización de cuerpos finitos

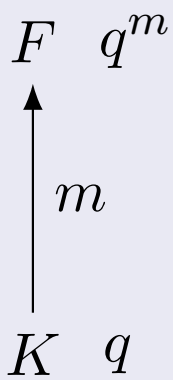
Ejemplos conocidos de cuerpos finitos

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

Es un cuerpo finito con p elementos para todo p primo.

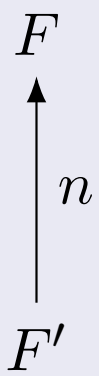
Lema 1

Sea F un cuerpo finito conteniendo un subcuerpo K con q elementos. Entonces F tiene q^m elementos, donde $m = [F : K]$



Teorema 2

Sea F un cuerpo finito, entonces F tiene p^n elementos, donde el primo p es la característica de F y n es el grado de F sobre su cuerpo primo.



$$\mathrm{ch}(F) = p$$

Construcción de nuevos cuerpos finitos

Si $f \in \mathbb{F}_p[x]$ es un polinomio irreducible de grado n, entonces $\mathbb{F}_p[x]/(f)$ es un cuerpo finito de p^n elementos.

¿Siempre es posible encontrar un polinomio irreducible en $\mathbb{F}_p$ de grado n para todo entero positivo n?

Lema 3

Si F es un cuerpo finito con q elementos, entonces cada $a \in F$ satisface $a^q = a$.

Lema 3

Si F es un cuerpo finito con q elementos, entonces cada $a \in F$ satisface $a^q = a$.

Lema 4

Si F es un cuerpo finito con q elementos, y K es un subcuerpo de F, entonces el polinomio $x^q - x \in K[x]$ se factoriza en $F[x]$ como

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

y F es un cuerpo de descomposición de $x^q - x$ sobre K.

Teorema 5 (Existencia y unicidad de cuerpos finitos)

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

Teorema 5 (Existencia y unicidad de cuerpos finitos)

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

Cuerpos de Galois

Ahora, podemos hablar de cuerpos finitos o cuerpos de Galois de orden q, denotados $\mathbb{F}_q$, donde $q = p^n$ con p primo.

Ejemplos

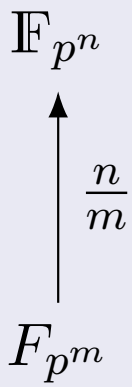
- Consideremos $f(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$, el cual es un polinomio irreducible de grado 2 sobre $\mathbb{F}_3$. Sea θ una raíz de $f(x)$ en algún cuerpo. Construimos entonces el cuerpo
  $\mathbb{F}_3(\theta) = \{a + b\theta : a, b \in \mathbb{F}_3\}$ un cuerpo con 9 elementos, y entonces $\mathbb{F}_3(\theta) = \mathbb{F}_9$.

Ejemplos

- Consideremos $f(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$, el cual es un polinomio irreducible de grado 2 sobre $\mathbb{F}_3$. Sea θ una raíz de $f(x)$ en algún cuerpo. Construimos entonces el cuerpo $\mathbb{F}_3(\theta) = \{a + b\theta : a, b \in \mathbb{F}_3\}$ un cuerpo con 9 elementos, y entonces $\mathbb{F}_3(\theta) = \mathbb{F}_9$.
- Del mismo modo, consideremos $f(x) = x^2 + x + 1 \in \mathbb{F}_2[X]$ irreducible, y θ una raíz, entonces $\mathbb{F}_2(\theta) = \mathbb{F}_4$.

Teorema 6 (Criterio de subcuerpos)

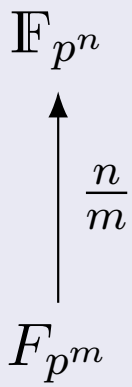
Sea $\mathbb{F}_q$ un cuerpo finito con $q = p^n$ elementos. Entonces cada subcuerpo de $\mathbb{F}_q$ tiene orden p^m donde m es un divisor positivo de n. Recíprocamente, si m es un divisor positivo de n, entonces hay exactamente un subcuerpo de $\mathbb{F}_q$ con p^m elementos.



m divisor de n

Teorema 6 (Criterio de subcuerpos)

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



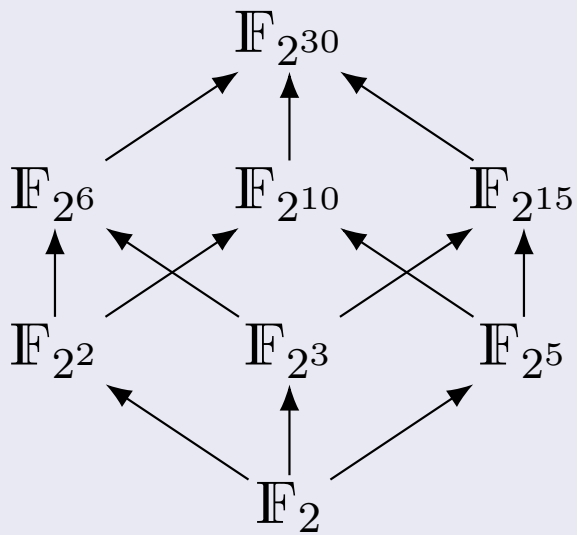
m divisor de n

Observación

El único subcuerpo de $\mathbb{F}_{p^n}$ de orden p^m donde m es un divisor positivo de n, consiste de las raíces del polinomio $x^{p^m} - x \in \mathbb{F}_p[x]$ en $\mathbb{F}_{p^n}$.

Ejemplo 7

Los subcuerpos del cuerpo finito $\mathbb{F}_{2^{30}}$ pueden ser determinados listando todos los posibles divisores positivos de 30. La relación de contenencia entre estos subcuerpos es equivalente a la relación de divisibilidad entre los divisores de 30.



Teorema 8

para cada cuerpo finito $\mathbb{F}_q$, el grupo multiplicativo ${\mathbb{F}_q}^*$ de elementos no cero de $\mathbb{F}_q$ es cíclico.

Teorema 8

para cada cuerpo finito $\mathbb{F}_q$, el grupo multiplicativo ${\mathbb{F}_q}^*$ de elementos no cero de $\mathbb{F}_q$ es cíclico.

Definición 9

Un generador del grupo cíclico ${\mathbb{F}_q}^*$ es llamado un elemento primitivo de $\mathbb{F}_q$.

Teorema 8

para cada cuerpo finito $\mathbb{F}_q$, el grupo multiplicativo ${\mathbb{F}_q}^*$ de elementos no cero de $\mathbb{F}_q$ es cíclico.

Definición 9

Un generador del grupo cíclico ${\mathbb{F}_q}^*$ es llamado un elemento primitivo de $\mathbb{F}_q$.

${\mathbb{F}_q}^*$ tiene $\phi(q-1)$ elementos primitivos.

Ejemplo

- $\mathbb{F}_5$ tiene $\phi(4) = 2$ elementos primitivos, estos son 2 y 3.

Ejemplo

- $\mathbb{F}_5$ tiene $\phi(4) = 2$ elementos primitivos, estos son 2 y 3.
- $\mathbb{F}_4$ tiene $\phi(3) = 2$ elementos primitivos. Expresando $\mathbb{F}_4$ como $\mathbb{F}_2(\theta) = \{0, 1, \theta, \theta + 1\}$, donde $\theta^2 + \theta + 1 = 0$, encontramos que θ y $\theta + 1$ son los elementos primitivos de $\mathbb{F}_4$.

Teorema 10

Sea $\mathbb{F}_q$ un cuerpo finito y $\mathbb{F}_r$ una extensión finita. Entonces $\mathbb{F}_r$ es una extensión algebraica simple de $\mathbb{F}_q$.

$$\begin{array}{c} \mathbb{F}_r = \mathbb{F}_q(\zeta) \\ \uparrow \\ \mathbb{F}_q \end{array}$$

Teorema 10

Sea $\mathbb{F}_q$ un cuerpo finito y $\mathbb{F}_r$ una extensión finita. Entonces $\mathbb{F}_r$ es una extensión algebraica simple de $\mathbb{F}_q$.

$$\begin{array}{c} \mathbb{F}_r = \mathbb{F}_q(\zeta) \\ \uparrow \\ \mathbb{F}_q \end{array}$$

Corolario 11

Para cada cuerpo finito $\mathbb{F}_q$ y cada entero positivo n, existe un polinomio irreducible $\mathbb{F}_q[x]$ de grado n.

Ejemplo

Consideremos el cuerpo finito $\mathbb{F}_9$, lo podemos expresar en la forma $\mathbb{F}_3(\beta)$, donde β es una raíz del polinomio x^2+1, irreducible sobre $\mathbb{F}_3$,. Sin embargo, como $\beta^4 = 1$, β no es un generador de $\mathbb{F}_9{}^*$. Por lo tanto, β no es un elemento primitivo de $\mathbb{F}_9$.

Raíces de polinomios irredubles sobre cuerpos finitos

Lema 12

Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible sobre un cuerpo finito $\mathbb{F}_q$ y sea α una raíz de f es una extensión de cuerpo de $\mathbb{F}_q$. Entonces para un polinomio $h \in \mathbb{F}_q[x]$ tenemos que $h(\alpha) = 0$ si y solo si f divide a h.

Raíces de polinomios irredubles sobre cuerpos finitos

Lema 12

Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible sobre un cuerpo finito $\mathbb{F}_q$ y sea α una raíz de f es una extensión de cuerpo de $\mathbb{F}_q$. Entonces para un polinomio $h \in \mathbb{F}_q[x]$ tenemos que $h(\alpha) = 0$ si y solo si f divide a h.

Lema 13

Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado m. Entonces $f(x)$ divide a $x^{q^m} - x$ si y solo si m divide a n.

Teorema 14

Si f es un polinomio irreducible en $\mathbb{F}_q[x]$ de grado m, entonces f tiene una raíz α en $\mathbb{F}_{q^m}$. Más aún, todas las raíces de f son simples y están dadas por los m distintos elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.

Teorema 14

Si f es un polinomio irreducible en $\mathbb{F}_q[x]$ de grado m, entonces f tiene una raíz α en $\mathbb{F}_{q^m}$. Más aún, todas las raíces de f son simples y están dadas por los m distintos elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.

Corolario 15

Sea f un polinomio irreducible en $\mathbb{F}_q[x]$ de grado m. Entonces el cuerpo de descomposición de f sobre $\mathbb{F}_q$ es $\mathbb{F}_{q^m}$.

Teorema 14

Si f es un polinomio irreducible en $\mathbb{F}_q[x]$ de grado m, entonces f tiene una raíz α en $\mathbb{F}_{q^m}$. Más aún, todas las raíces de f son simples y están dadas por los m distintos elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.

Corolario 15

Sea f un polinomio irreducible en $\mathbb{F}_q[x]$ de grado m. Entonces el cuerpo de descomposición de f sobre $\mathbb{F}_q$ es $\mathbb{F}_{q^m}$.

Corolario 16

Cualesquier dos polinomios irreducibles en $\mathbb{F}_q[x]$ del mismo grado tienen cuerpos de descomposición isomorfos.

Definición 17

Sea $\mathbb{F}_{q^m}$ una extensión de $\mathbb{F}_q$ y sea $\alpha \in \mathbb{F}_{q^m}$, entonces los elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ son llamados conjugados de α respecto a $\mathbb{F}_q$.

Definición 17

Sea $\mathbb{F}_{q^m}$ una extensión de $\mathbb{F}_q$ y sea $\alpha \in \mathbb{F}_{q^m}$, entonces los elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ son llamados conjugados de α respecto a $\mathbb{F}_q$.

Los conjugados de $\alpha \in \mathbb{F}_{q^m}$ con respecto a $\mathbb{F}_q$ son distintos si y solo si el polinomio minimal de α en $\mathbb{F}_q[x]$ es de grado m. En otro caso, el grado d de este polinomio minimal es un divisor propio de m y los conjugados de α con respecto a $\mathbb{F}_q$ son los elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$. repetidos cada uno $\frac{m}{d}$ veces.

Teorema 18

Los conjugados de $\alpha \in {\mathbb{F}_q}^*$ con respecto a cualquier subcuerpo de $\mathbb{F}_q$ tienen el mismo orden en el grupo ${\mathbb{F}_q}^* = \langle \zeta \rangle$

Teorema 18

Los conjugados de $\alpha \in \mathbb{F}_q{}^*$ con respecto a cualquier subcuerpo de $\mathbb{F}_q$ tienen el mismo orden en el grupo $\mathbb{F}_q{}^* = \langle \zeta \rangle$

Corolario 19

Si α es un elemento primitivo de $\mathbb{F}_q$, entonces también lo son todos sus conjugados con respecto a cualquier subcuerpo de $\mathbb{F}_q$.

Ejemplo 20

Sea $\alpha \in \mathbb{F}_{16}$ una raíz de $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Entonces los conjugados de α respecto a $\mathbb{F}_2$ son $\alpha, \alpha^2, \alpha^4 = \alpha + 1$ y $\alpha^8 = \alpha^2 + 1$. Siendo cada uno de ellos un elemento primitivo de $\mathbb{F}_{16}$.

Los conjugados de α respecto a $\mathbb{F}_4$ son α y $\alpha^4 = \alpha + 1$.

Teorema 21

Los distintos automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ son exactamente los automorfismos $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ definidos por $\sigma_j(\alpha) = \alpha^{q^j}$ con $\alpha \in \mathbb{F}_{q^m}$ y $0 \leq j \leq m-1$. Estos automorfismos son reciben el nombre de *Automorfismos de Frobenius*

Con base en el teorema 21, resulta evidente que los conjugados de $\alpha \in \mathbb{F}_{q^m}$ con respecto a $\mathbb{F}_q$ son obtenidos mediante la aplicación de todos los automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ al elemento α.

Los automorfismos de F_{q^m} sobre $\mathbb{F}_q$ forman un grupo con la operación usual de composición. Por el teorema 21, este grupos es cíclico de orden m, generado por σ_1.

Como $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m$, entonces $\mathbb{F}_{q^m}$ es de Galois sobre $\mathbb{F}_q$, entonces

$$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \sigma_1 \rangle \cong \mathbb{Z}/m\mathbb{Z}$$

Referencias

David Steven Dummit and Richard M Foote.
Abstract algebra, volume 3.
Wiley Hoboken, 2004.

Rudolf Lidl.
Finite fields.
Encyclopedia of Mathematics and its Applications, 20, 1983.