Def: Un elemento $b \in F$ se llama raíz o cero de un polinomio $f \in F[x]$ si $f(b) = 0$.

Teorema: Un elemento $b \in F$ es una raíz de un polinomio $f \in F[x]$ si y sólo si $(x-b)$ divide a $f(x)$.

Dem

Por el algoritmo de la división existen $q(x), r(x) \in F[x]$ tales que

$$f(x) = q(x)\cdot(x-b) + r(x) \quad \text{donde } \deg r < 1$$

entonces $r(x) = c \in F$ constante.

Pero $f(b) = q(b)\underbrace{(b-b)}_{0} + \underbrace{r(b)}_{c} \Rightarrow r(x) = c = f(b)$

Luego $f(x) = q(x)(x-b) + f(b)$

$\Rightarrow$)

Si b es raíz $\Rightarrow f(b) = 0 \Rightarrow f(x) = q(x)(x-b) \Rightarrow$

$(x-b)$ divide a $f(x)$.

$\Leftarrow$) Si $(x-b)$ divide a $f(x) \Rightarrow f(x) = s(x)\cdot(x-b)$

$$0 = \underbrace{(s(x)-q(x))}_{=0}\underbrace{(x-b)}_{\deg=1} = \underbrace{f(b)}_{\deg<1}$$

b es raíz de f. ∎

Def: Sea $b \in F$ una raíz de un polinomio $f \in F[x]$. Si k es un entero positivo tal que $f(x)$ es divisible por $(x-b)^k$ pero no es divisible por $(x-b)^{k+1}$ entonces k se llama la multiplicidad de b. En el caso en que $k=1$ decimos que b es una raíz simple o cero simple de f, y si $k \geq 2$ entonces b es una raíz o cero múltiple

Teorema: Sea $f \in F[x]$ de grado $\deg(f) = n \geq 0$. Si $b_1, \dots, b_m \in F$ son raíces distintas de f con multiplicidades $k_1, \dots, k_m$ respectivamente, entonces

$$(x-b_1)^{k_1} \cdot (x-b_2)^{k_2} \cdots (x-b_m)^{k_m}$$

divide a $f(x)$ y en consecuencia $k_1 + \dots + k_m \leq n$ y f puede tener a lo sumo n raíces distintas en F.

Dem

Como $(x-b_j)$ es irreducible en F $(\deg(x-b_j)=1)$ entonces $(x-b_j)^{k_j}$ es uno de los factores que aparecen en la descomposición en irreducibles de f. Como lo mismo es cierto para todos los $j = 1, \dots, m$ entonces $(x-b_1)^{k_1} \cdots (x-b_m)^{k_m}$ divide a f pues aparecen en la factorización.

Comparando los grados el resultado sigue. ∎

Def: Si $f(x) = a_0 + a_1 x + \dots + a_n x^n \in F[x]$ entonces la derivada $f'(x)$ de $f(x)$ es el polinomio

$$f'(x) = a_1 + 2 \cdot a_2 x + \dots + n a_n x^{n-1} \in F[x]$$

Teorema: Un elemento $b \in F$ es una raíz múltiple de $f \in F[x]$ si y sólo si es una raíz de f y de f'.

Hay una relación entre la no existencia de raíces y la irreducibilidad de un polinomio f en $F[x]$.

Si f es un polinomio irreducible de grado ≥ 2 entonces no puede ser divisible por $(x-b)$ para ningún $b \in F$, y por lo tanto ningún $b \in F$ satisface $f(b) = 0$.

→ Si f es irreducible de grado $\geq 2 \Rightarrow$ no tiene raíces.

Teorema: Un polinomio $f(x) \in F[x]$ de grado 2 o 3 es irreducible en $F[x]$ si y sólo si f no tiene raíces en F.

Dem

$\Rightarrow$) ✓

$\Leftarrow$) Supongamos f tiene grado 2 o 3 y que no

tiene raíces en F. Si suponemos que f es reducible en $F[x]$ entonces podemos escribir

$$f(x) = g(x) \cdot h(x)$$

donde $g, h \in F[x]$ y $1 \leq \deg(g) \leq \deg(h)$.

Pero $3 \geq \deg f = \deg(g \cdot h) = \underbrace{\deg g}_{\geq 1} + \underbrace{\deg h}_{\geq \deg g}$.

entonces

$$\deg g = 1 \Rightarrow g(x) = ax + b \quad a, b \in F.$$

Pero entonces $-a^{-1}b \in F$ es una raíz de g y por lo tanto de f. $\lightning$ contradicción.

Notar que no es cierto para grados mayores, ver contraejemplo.

El siguiente teorema permite construir un polinomio que tome ciertos valores asignados a ciertos valores de la indeterminada.

Teorema (Interpolación de Lagrange)

Para $n \geq 0$ sean $a_0, \dots, a_n$ $n+1$ elementos diferentes de $\mathbb{F}$ y sean $b_0, \dots, b_n$ $n+1$ elementos arbitrarios de $\mathbb{F}$. Entonces existe exactamente un polinomio $f \in \mathbb{F}[x]$ de grado $\leq n$ tal que $f(a_i) = b_i \quad \forall i = 0, \dots, n$.

Este polinomio está dado por

$$f(x) = \sum_{i=0}^{n} b_i \prod_{\substack{k=0 \\ k \neq i}}^{n} (a_i - a_k)^{-1} (x - a_k)$$

Ejemplo: Buscamos un polinomio en $\mathbb{F}_3[x]$ tal que

$f(0)=1 \qquad f(1)=2 \qquad f(2)=2$

$a_0=0 \quad a_1=1 \quad a_2=2 \qquad b_0=1 \quad b_1=2 \quad b_2=2$

$$f(x)=\sum_{i=0}^{n} b_i \prod_{\substack{k=0 \\ k\neq i}}^{n} (a_i-a_k)^{-1}(x-a_k)$$

$-1 \equiv 2 \ (3)$

$-2 \equiv 1 \ (3)$

$$f(x)= b_0\Big(\underbrace{(a_0-a_1)^{-1}(x-a_1)}_{k=1}\ \underbrace{(a_0-a_2)^{-1}(x-a_2)}_{k=2}\Big) +$$

$$+ b_1\Big(\underbrace{(a_1-a_0)^{-1}(x-a_0)}_{k=0}\ \underbrace{(a_1-a_2)^{-1}(x-a_2)}_{k=2}\Big) +$$

$$+ b_2\Big(\underbrace{(a_2-a_0)^{-1}(x-a_0)}_{k=0}\ \underbrace{(a_2-a_1)^{-1}(x-a_1)}_{k=1}\Big)$$

$$= 1\Big((2)^{-1}(x-1)\ (1)^{-1}(x-2)\Big)$$
$$+ 2\Big(1^{-1}(x-0)\ 2^{-1}(x-2)\Big)$$
$$+ 2\Big(2^{-1}(x-0)\ 1^{-1}(x-1)\Big)$$

$2-2=4=1 \ (3)$

$2^{-1}=2$ en $\mathbb{F}_3$.

$$= 2(x-1)(x-2)+x(x-2)+x(x-1)$$
$$= 2(x^2-x-2x+2)+x^2-2x+x^2-x$$
$$= 2x^2+1+2x^2 = x^2+1.$$

$f(0)=1 \quad f(1)=2 \quad f(2)=2$ ✓

Cada aplicación de $\mathbb{F}_q$ en sí mismo puede expresarse como un polinomio:

Si $\phi : \mathbb{F}_q \to \mathbb{F}_q$, por el teorema anterior existe un único polinomio $f \in \mathbb{F}_q[x]$ de grado $\leq q-1$ tal que $f(c) = \phi(c) \quad \forall c \in \mathbb{F}_q$.

Hasta el momento vimos que para un número primo p

① $\mathbb{F}_p$ (enteros módulo p) es un cuerpo finito con p elementos

② $\mathbb{F}_p[x]/(f)$ es un cuerpo finito sii f es irreducible sobre $\mathbb{F}_p$

③ Si $\deg f = n$ (f irreducible) entonces $\mathbb{F}_p[x]/(f)$ tiene p^n elementos.

¿Son los anteriores los únicos posibles opciones para construir cuerpos finitos?

Lo que deseamos es justamente caracterizar a todos los cuerpos finitos.

Extensiones de cuerpos

Sea F un cuerpo. Un subconjunto K de F que es él mismo un cuerpo con las operaciones de F se llama un subcuerpo de F. Si $K \neq F$ decimos que K es un subcuerpo propio.

Notar que $K \subseteq \mathbb{F}_p$ que sea un subcuerpo entonces K debe contener al menos a 0 y a 1. y como es un cuerpo (cerrado bajo suma) y por lo tanto contiene a todos los elementos de $\mathbb{F}_p$. $\Rightarrow K = \mathbb{F}_p$. Luego, $\mathbb{F}_p$ no contiene subcuerpos propios.

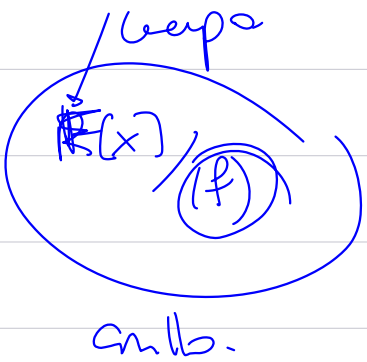
Def: Un cuerpo que no tiene subcuerpos propios se llama cuerpo primo.

Otro ejemplo de un cuerpo primo es $\mathbb{Q}$ con la suma y productos usuales. ← Ejercicio.

La intersección de cualquier colección no vacía de subcuerpos de un cuerpo es nuevamente un subcuerpo de F. La intersección de todos los subcuerpos de F es un cuerpo primo llamado subcuerpo primo de F

Teorema: el subcuerpo primo de un cuerpo F es isomorfo a $\mathbb{F}_p$ o $\mathbb{Q}$ dependiendo si la característica es prima o es cero.

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



$x \cdot (x^2+x+1) = 0$

$\mathbb{F}[x]$.

(1.36) $x^4+x^3+x+1 = (x+1)(x^3+1)$ R

$=$

$R[x]/(x^4+x^3+x+1)$

$f(x)$

x^4+x^3+x+1

$e \cdot x^4 + e \cdot x^3 + e \cdot x + e$

1.35) $(x^4+x^3+x^2+1)\, f(x) \equiv (x^2+1)^{(x+1)^2} \bmod (x^3+1)$

$f(x)$ $\qquad$ $F_2(x)$

$$\gcd(x^4+x^3+x^2+1 \;;\; x^3+1) = x^3+1$$

1.33) F un cuerpo $\quad a, b, g \in F(x) \quad g \neq 0$

$af \equiv b \bmod g \iff (a, g)$ divide a b

$$\underbrace{x^4+x^3+x^2+1}_{f} = (x+1)(x^3+1)$$

$$= (x+1)(x^3+x+1)$$

	1	1	1	0	1
1		1	0	1	1
	1	0	1	1	0

$$\underbrace{(x^3+1)}_{g} = (x+1)(x^2+x+1)$$

$$\gcd(f, g) = (x+1)$$

$(x+1) = q(x)\cdot f(x) + r(x)\cdot g(x)$ ($f(x) \to x^4+x^3+x^2+1$, $g(x) \to x^3+1$)

$x^4+x^3+x^2+1 = q_1(x)(x^3+1) + r_1(x)$

$$\begin{array}{r|l} x^4+x^3+x^2+1 & x^3+1 \\ -x^4+\quad x & x+1 \\ \hline x^3+x^2+x+1 & \\ x^3+1 & \\ \hline x^2+x & \end{array} \qquad \begin{array}{r|l} x^3+1 & x^2+x \\ x^3+x^2 & x+1 \\ \hline x^2+1 & \\ x^2+x & \\ \hline x+1 & \end{array}$$

$f = g(x+1) + (x^2+x)$

$x^3+1 = (x+1)(x^2+x) + (x+1)$

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

$= x^2\cdot g + (x+1) f.$

$x+1 = (x^3+1) + (x+1)(x^2+x)$

$= s + (x+1)[f + (x+1) g]$

$= g + (x+1)^2 \cdot g + (x+1) f$

$(x+1) = x^2 \cdot g + (x+1) f$.

$f \cdot h \equiv \underbrace{x^2+1}_{(x+1)^2} \mod g = x^3+1$.

$h(x)$

$(x+1)^2 = \underbrace{(x+1)x^2 \cdot g}_{} + (x+1)^2 \cdot f$.

$x^2+1 = + h(x) \cdot f(x)$.

$(x^4+x^3+x^2+1)(x^2+1) \equiv x^2+1 \quad (x^3+1)$

$(x+1)(x^3+x+1) \cdot h(x) \equiv (x+1)^2 \quad (x^3+1)$

$(x+1)(x^3+x+1) h(x) \equiv (x+1)^2 \quad (x^2+x+1) \quad (x+1)(x^2+x+1)$

$h(x) = (x+1)^2$

$$(x^4+x^3+x^2+1)\cdot h(x) \equiv x^2+1 \mod (x^3+1) \quad \mathbb{F}_2[x]$$

$$h(x) = x^2+1.$$