Para el cuerpo finito $\mathbb{F}_q$ denotamos por $\mathbb{F}_q^*$ al grupo multiplicativo formado por los elementos no nulos de $\mathbb{F}_q$. Vamos a probar que $\mathbb{F}_q^*$ es cíclico.

Recordemos que un grupo multiplicativo G se dice <u>cíclico</u> si existe un elemento $a \in G$ tal que para cualquier $b \in G$ existe un entero j tal que $b = a^j$. El elemento a se llama <u>generador</u> del grupo cíclico y escribimos $G = \langle a \rangle$.

<u>Teorema</u>: El grupo multiplicativo $\mathbb{F}_q^*$ es cíclico.

<u>Demostración</u>

- Para $q = 2$ el resultado es trivial.
- Sea $q \geq 3$, y escribimos $h = q-1 = p_1^{r_1} \cdots p_m^{r_m}$ la descomposición en primos de $q-1 = |\mathbb{F}_q^*|$ es decir $p_1, \ldots, p_m$ son primos distintos y $r_1, \ldots, r_m \in \mathbb{N}$.

Para cada $1 \leq i \leq m$ consideramos el polinomio

$$X^{h/p_i} - 1$$

que es de grado $h/p_i < h = q-1$, y por lo tanto existen elementos en $\mathbb{F}_q^*$ que no son raíces del polinomio.

Sea $a_i \in \mathbb{F}_q^*$ tal que $a_i^{h/p_i} \neq 1$, y consideremos

$$b_i = a_i^{h/p_i^{r_i}}$$

Entonces el orden de b_i es $p_i^{r_i}$. En efecto, como

$$b_i^{p_i^{r_i}} = a_i^{h} = a_i^{q-1} = 1 \quad \text{y}$$

$$b_i^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1.$$

Consideremos ahora $b = b_1 \cdots b_m$. Este elemento tiene orden $q-1$, y por lo tanto es el generador del grupo.

Si eso no fuera cierto y el orden de b fuera un k menor a $q-1$, entonces k debería ser un divisor de $q-1=h$ entonces debe dividir a algun h/p_i
(digamos por ejemplo k divide a h/p_1)

Entonces $h/p_1 = k \cdot s \quad s \in \mathbb{N}$

$$b_1^{h/p_1} \cdots b_m^{h/p_1} = b^{h/p_1} = b^{u \cdot s} = (b^u)^s = 1$$

Además $p_i^{r_i}$ divide a h/p_1 para $i = 2, \ldots, m$, y por lo tanto

$$b_i^{h/p_1} = 1 \qquad i = 2, \ldots, m$$

$\Rightarrow$ $b_1^{h/p_1} = 1$, y esto no puede ser pues $\text{ord}(b_1) = p_1^{r_1}$

y ahora consigo un orden que divide a h/p_1 con potencia $p_1^{r_1-1}$.

$\frac{h}{p_1} = p_1^{r_1-1} \cdot p_2^{r_2} \cdots p_m^{r_m}$

$\text{ord}(b) \mid h/p_1 \rightarrow p_1^{r_1-1}$ ⊗ Absurdo.

$\text{ord}(b) = p_1^{r_1}$

Def: Un generador del grupo cíclico $\mathbb{F}_q^*$ se llama elemento primitivo de $\mathbb{F}_q$.

Ejemplo: Si consideramos $\mathbb{F}_7 \Rightarrow \mathbb{F}_7^* = \{1, 2, \ldots, 6\} \Rightarrow$

- 2 no es un elemento primitivo pues $2^2 = 4$ $2^3 = 8 = 1$
- 3 sí lo es

$3^2 = 9 = 2$ $3^3 = 3 \cdot 3^2 = 3 \cdot 2 = 6$ $3^4 = 3 \cdot 6 = 18 = 4$

$3^5 = 3 \cdot 4 = 12 = 5$ $3^6 = 3 \cdot 5 = 15 = 1$

$\mathbb{F}_7^* = \{1, 2, 3, 4, 5, 6\}$

$= \{3^6, 3^2, 3^1, 3^4, 3^5, 3^3\}$

Ejemplo: $\mathbb{F}_q = \mathbb{F}_3(\theta)$ $\theta^2 + \theta + 2 = 0 \rightarrow \theta^2 = -\theta - 2$ $\rightarrow \theta^2 = 2\theta + 1$

$\mathbb{F}_3(\theta)^* = \{\underbrace{1}_{\theta^8}, \underbrace{2}_{\theta^4}, \theta, \underbrace{\theta+1}_{\theta^7}, \underbrace{\theta+2}_{\theta^6}, \underbrace{2\theta}_{\theta^5}, \underbrace{2\theta+1}_{\theta^2}, \underbrace{2\theta+2}_{\theta^3}\}$.

$\theta^3 = \theta\,\theta^2 = \theta(2\theta+1) = 2\theta^2 + \theta = 2(2\theta+1) + \theta = 2\theta + 2$.

Teorema: Sea $\mathbb{F}_q$ un cuerpo finito y $\mathbb{F}_r$ una extensión finita de $\mathbb{F}_q$. Entonces $\mathbb{F}_r$ es una extensión algebraica simple de $\mathbb{F}_q$ y cualquier elemento primitivo de $\mathbb{F}_r$ sirve como elemento de definición de $\mathbb{F}_r$ sobre $\mathbb{F}_q$.

Demostración

Sea S un elemento primitivo de $\mathbb{F}_r$. Consideramos $\mathbb{F}_q(S) \subseteq \mathbb{F}_r$. Pero además $0 \in \mathbb{F}_q(S)$ y todos los elementos de $\mathbb{F}_r^*$ se escriben como potencias de S y por lo tanto $\mathbb{F}_r = \mathbb{F}_q(S)$. ∎

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

Demostración

Sea $\mathbb{F}_r$ una extensión de $\mathbb{F}_q$ de orden q^n es decir $[\mathbb{F}_r : \mathbb{F}_q] = n$. Por el teorema anterior

$$\mathbb{F}_r = \mathbb{F}_q(S)$$

para algún S elemento primitivo de $\mathbb{F}_r$ sobre $\mathbb{F}_q$. Luego el polinomio mínimo de S es un polinomio irreducible de grado n con coeficientes en $\mathbb{F}_q$. ∎

Raíces de polinomios irreducibles

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

Demostración

Sea a el coef. líder de f y $g(x) = a^{-1} f(x)$. Entonces g es un polinomio mónico e irreducible en $\mathbb{F}_q[x]$ y $g(\alpha) = 0$, por lo tanto g es el polinomio mínimo de α sobre $\mathbb{F}_q$. El resultado se obtiene de las propiedades del polinomio mínimo. ∎

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

Demostración:

⇒) Supongamos que f divide a $x^{q^n} - x$ (y probemos que m divide a n).

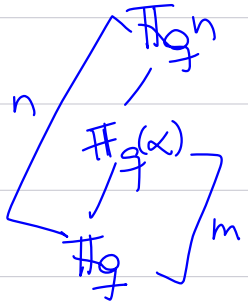
Sea α una raíz de f en el cuerpo de descomposición de f sobre $\mathbb{F}_q$. Entonces como $f(\alpha) = 0$ y f divide a $x^{q^n} - x$, tenemos que

$$\alpha^{q^n} = \alpha \quad \text{y por lo tanto} \quad \alpha \in \mathbb{F}_{q^n}.$$

Entonces $\mathbb{F}_q(\alpha)$ es un subcuerpo de $\mathbb{F}_{q^n}$; pero como

$$[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg(f) = m \quad \text{y}$$

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = n.$$



Entonces $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = \underbrace{[\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)]}_{s} \underbrace{[\mathbb{F}_q(\alpha) : \mathbb{F}_q]}_{m} = s.m.$

$\deg f$

$\Leftarrow$) Supongamos que m divide a n. Por un teorema anterior que caracteriza los subcuerpos, tenemos que $\mathbb{F}_{q^n}$ contiene a $\mathbb{F}_{q^m}$ como subcuerpo.

Si α es una raíz de f en ~~un~~ cuerpo de descomposición de f sobre $\mathbb{F}_q$ tenemos

$$\left.\begin{array}{l} [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m = \deg(f) \quad \text{y} \\ [\mathbb{F}_{q^m} : \mathbb{F}_q] = m \end{array}\right\} \Rightarrow \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$$

Por lo tanto $\alpha \in \mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ y entonces $\alpha^{q^n} = \alpha$, es decir α es una raíz de $X^{q^n} - X \in \mathbb{F}_q(X)$.

Finalmente, por el lema anterior como α es raíz de $x^{p^n} - x$, debe pasar que f divide a $x^{p^n} - x$. ∎

Teorema: Si f es un polinomio irreducible en $\mathbb{F}_p[x]$ de grado m, entonces f tiene una raíz α en $\mathbb{F}_{p^m}$. Más aun, todas las raíces de f son simples y están dadas por los elementos diferentes

$$\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{m-1}} \text{ de } \mathbb{F}_{p^m}.$$