Tema 11.-. Cuerpos finitos. Grupo de automorfismos.

11.1. Cuerpos finitos.

DEFINICIÓN 11.1.1.– Un cuerpo finito es un cuerpo con un número finito de elementos. Solemos escribir $\mathbb{F}_q$ para indicar un cuerpo finito con q elementos.

Observando que cualquier cuerpo finito es un espacio vectorial sobre un cierto $\mathbb{Z}/\mathbb{Z}p$, se tiene el siguiente resultado.

PROPOSICIÓN 11.1.2.– Si k es un cuerpo finito, tiene característica positiva p. En ese caso el cardinal de k es p^n, para cierto $n > 0$.

Demostración. Si k es un cuerpo finito con t elementos, entonces φ no puede tomar siempre valores diferentes. Por tanto, la característica es positiva, y k contiene un subcuerpo isomorfo a $\mathbb{F}_p = \mathbb{Z}/\mathbb{Z}p$ para algún $p \in \mathbb{Z}$ primo. Si $[k : \mathbb{F}_p] = n$ entonces existe una base $v_1, \ldots, v_n$ y $k = \{\alpha_1 v_1 + \ldots + \alpha_n v_n : \alpha_i \in \mathbb{F}_p\}$, y hay t^n elementos diferentes. □

LEMA 11.1.3.– Sea G un grupo multiplicativo y $\alpha = a^k$ con $o(a) = n$. Entonces $o(\alpha) = \frac{n}{\text{mcd}(n,k)}$.

Demostración. Sea $s = o(\alpha)$. Como $1 = \alpha^s = a^{ks}$ se deduce que $n|ks$. Escribamos $nn_1 = ks$. Sea $d = \text{mcd}(n, k)$. Entonces $\frac{k}{d}s = \frac{n}{d}n_1$, y como $\text{mcd}(n/d, k/d) = 1$ se tiene que n/d divide a s. Por otro lado, $\alpha^{n/d} = a^{kn/d} = 1$ de donde s divide a n/d. □

LEMA 11.1.4.– Sea G un grupo multiplicativo, $a, b \in G$ tales que

$$ab = ba \text{ y } \text{mcd}(o(a), o(b)) = 1.$$

Entonces $o(ab) = o(a)o(b)$.

Demostración. Sea $n = o(a), m = o(b)$. Entonces $\text{mcm}(m, n) = mn$. Es claro que $(ab)^{mn} = a^{mn}b^{mn} = 1$, de donde $o(ab)|mn$. Por la identidad de Bezout, existen $p, q \in \mathbb{Z}$ tales que $pm + qn = 1$. Entonces

$$a = ab^{pm} = a^{pm}a^{qn}b^{pm} = (ab)^{pm}$$

de donde $a \in \langle ab \rangle$. De igual forma se tiene que $b \in \langle ab \rangle$. Por tanto, $o(a), o(b)$ dividen a $o(ab)$ y por ser primos entre sí $o(a)o(b)|o(ab)$. □

LEMA 11.1.5.– Sea G un grupo abeliano multiplicativo y finito, y $x \in G$ un elemento de orden máximo. Entonces para todo $y \in G$, $o(y)|o(x)$.

Demostración. Sea $n = o(x), m = o(y)$. Si m no divide a n, en la factorización de ambos como producto de primos aparece un factor primo p más veces en m que en n, esto es,

$$m = p^k a, k \geq 1, a \text{ no múltiplo de } p, n = p^h b, k > h \geq 0, b \text{ no múltiplo de } p.$$

Entonces

$$o(x^{p^h}) = n/p^h = b, o(y^a) = m/a = p^k.$$

Como G es abeliano y $\text{mcd}(b, p^k) = 1$, el orden de $z = x^{p^h} y^a$ es $o(x^{p^h})o(y^a) = bp^k > bp^h = n = o(x)$, lo que es contradictorio con la elección de x. □

Teorema 11.1.6.– Sea k un cuerpo. Entonces cualquier subgrupo finito de k^* es cíclico. En particular, k^* es cíclico de orden $|k| - 1$.

Demostración. Sea G un subgrupo finito de k^*. Escojamos $x \in G$ de orden maximal $a = o(x)$. Entonces todos los elementos de G son raíces de $X^a - 1$. Si $m = |G|$ tenemos entonces que $m \leq a$. Por otro lado, para cada $z \in G$, el orden de z divide a m, en particular $z = x$. Luego $a \leq m$, y tenemos la igualdad. □

Corolario 11.1.7.– Teorema del elemento primitivo, caso finito. Toda extensión finita $K|k$ de un cuerpo finito k es simple.

Demostración. El cuerpo K es también finito, pues es isomorfo como espacio vectorial a k^n, con $n = [K : k]$. Por el teorema anterior, existe $a \in K^*$ que lo genera como grupo multiplicativo. Por tanto, todo elemento $x \in K^*$ es de la forma a^k, con $k \in \mathbb{Z}$ y se sigue que $K \subset k(a)$. El recíproco es inmediato. □

Proposición 11.1.8.– Si k es un cuerpo finito, con p^n elementos, entonces k es cuerpo de descomposición del polinomio $X^{p^n} - X$ sobre $\mathbb{Z}/\mathbb{Z}p$.

Demostración. Como k^* es cíclico de orden $p^n - 1$, todos los elementos de k^* son raíces del polinomio $X^{p^n-1} - 1$. Si añadimos el cero, todos los elementos de k son raíces del polinomio $X^{p^n} - X$. □

Proposición 11.1.9.– Dos cuerpos finitos con el mismo número de elementos son isomorfos

Demostración. Es consecuencia trivial de la unicidad de los cuerpos de descomposición. □

11.2. Grupo de automorfismos.

LEMA 11.2.1.– Sea k un cuerpo de característica p. Entonces para cualesquiera $a, b \in k$ se tiene que

$$(a+b)^p = a^p + b^p, (ab)^p = a^p b^p.$$

En otras palabras, la aplicación

$$\varphi : k \to k, \varphi(a) = a^p$$

es un homomorfismo inyectivo de cuerpos.

Demostración. Por el teorema del binomio,

$$(a+b)^p = a^p + \left(\begin{array}{c} p \\ 1 \end{array} \right) a^{p-1}b + \ldots + \left(\begin{array}{c} p \\ i \end{array} \right) + \ldots + b^p$$

y debemos probar que si p es primo entonces el coeficiente binomial $\left(\begin{array}{c} p \\ i \end{array} \right)$ es divisible por p para $i = 1, 2, \ldots, p-1$. Pero como

$$\left(\begin{array}{c} p \\ i \end{array} \right) = \frac{p!}{i!(p-i)!}$$

es un entero y en el denominador no aparece el factor p del numerador, tiene que ser divisible por p. □

DEFINICIÓN 11.2.2.– La aplicación definida en el lema anterior se denomina endomorfismo de Frobenius del cuerpo k.

COROLARIO 11.2.3.– Supongamos que k es un cuerpo finito de característica p. Entonces todo elemento de k es una potencia p-ésima de un elemento de k. O bien, el endomorfismo de Frobenius es automorfismo.

Demostración. Si k es finito, la inyectividad del endomorfismo de Frobenius implica su carácter sobreyectivo. □

TEOREMA 11.2.4.– Para cada primo $p > 0$ y cada entero $n > 0$ existe un cuerpo de p^n elementos, (único salvo isomorfismo), que es una extensión normal de $\mathbb{Z}/\mathbb{Z}p$.

Demostración. Sea k el cuerpo de descomposición de $f(X) = X^{p^n-1} - 1$ sobre $\mathbb{Z}/\mathbb{Z}p$. El cuerpo k es finito porque es una extensión finita de un cuerpo finito. Como la derivada de f respecto de X sólo tiene la raíz nula, que no lo es de f, todas las raíces de f son simples. Así k tiene, al menos, p^n elementos. Luego $|k| = p^m$ con $m \geq n$.

Por otra parte, las $p^n - 1$ raíces de $X^{p^n-1} - 1 = 0$ forman un subgrupo $G \in k^*$, y además $G_0 = G \cup \{0\}$ tiene estructura de cuerpo. Observemos que G_0 es cerrado por la suma, porque

$$(x+y)^{p^n} = x^{p^n} + y^{p^n} = x + y$$

para cada $x, y \in G$. También es cerrado por el producto y contiene al 1. Como sus elementos no nulos tiene inverso, tenemos que $G_0 = \mathbb{F}_{p^n}$, subcuerpo de k con p^n elementos.

En realidad, $G_0 = k$ porque $\mathbb{F}_{p^n}$ es un cuerpo de descomposición de $X^{p^n-1} - 1$. □

Teorema 11.2.5.– Sea q una potencia de un primo cualquiera y $r > 0$ un entero cualquiera. Entonces el grupo de Galois

$$\mathrm{Gal}(\mathbb{F}_{q^r}|\mathbb{F}_q) \simeq \mathbb{Z}/\mathbb{Z}r,$$

el grupo cíclico de r elementos, que está generado por el automorfismo de Fröbenius $\varphi : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$, dado por $\varphi(x) = x^q$, para todo $x \in \mathbb{F}_{q^r}$.

Demostración. Por el teorema de Artin

$$|\,\mathrm{Gal}(\mathbb{F}_{q^r}|\mathbb{F}_q)| = [\mathbb{F}_{q^r} : \mathbb{F}_q] = r.$$

Además si $x \in \mathbb{F}_q$, $\varphi(x) = x^q = x$, luego $\varphi \in \mathrm{Gal}(\mathbb{F}_{q^r}|\mathbb{F}_q)$. Sin embargo, si x es un generador del grupo cíclico multiplicativo $\mathbb{F}_{q^r}^*$, entonces $\varphi^j(x) = x^{q^j}$ que no es igual a 1 si $1 \leq j \leq r-1$. Luego φ genera el grupo de Galois. □