Álgebra III
Semana 9

Alejandro García Montoro
agarciamontoro@correo.ugr.es

22 de diciembre de 2015

Ejercicio 1. *Sea q una potencia de un entero primo positivo.*

1. *Demostrar que un polinomio irreducible de grado r sobre $\mathbb{F}_q$ es un factor de $X^{q^n} - X$ si, y sólo si, $r|n$.*

2. *Deducir que*
$$X^{q^n} - X = \prod_i f_i(X)$$
donde f_i varía sobre todos los polinomios irreducibles cuyo grado divide a n.

3. *Demostrar que si t_r es el número de tales polinomios, entonces*
$$\sum rt_r = q^n$$
y deducir una fórmula para t_r, en términos de q, r y la función de Möbius.

Solución.

Apartado 1.1. Llamamos $P(X) = X^{q^n} - X$.

Sea K un cuerpo con q^n elementos. Sabemos que, si $\alpha \in \mathbb{K}^x$, entonces $\alpha^{q^n-1} = \alpha$. Es claro entonces que todos los elementos de K son raíces de $P(X)$; de hecho, *todas* las raíces del polinomio están en K, pues no puede tener más de q^n raíces.

Sea ahora $Q(X) \in \mathbb{F}_q$ un factor irreducible de $P(X)$. Como todas las raíces de $P(X)$ están en K, también lo están las de Q. Sea entonces $\beta \in K$ una raíz de Q.

Tenemos entonces la torre de cuerpos
$$\mathbb{F}_q \subset \mathbb{F}_q(\beta) \subset K$$
donde $[\mathbb{F}_q(\beta) : \mathbb{F}_q]$ es el grado del polinomio Q. Es claro entonces que el grado de Q es un divisor de n.

Sea ahora $Q(X)$ un irreducible de grado r, divisor de n. Usando el corolario 12.5 y teniendo en cuenta que la característica de $\mathbb{F}_q$ es p, es claro que $Q(X)$ es factor de $P(X)$.

Apartado 1.2. Este resultado se deduce directamente de 1.

Todos los factores de $P(X)$ tienen grado divisor de n y cualquier irreducible con grado divisior de n es factor, luego el conjunto de todos los factores de $P(X)$ es exactamente igual al de todos los irreducibles de grado divisor de n; es decir:

$$X^{q^n} - X = \prod_i f_i(X)$$

donde f_i varía sobre todos los polinomios irreducibles cuyo grado divide a n.

Apartado 1.3. Dada la finitud de elementos en $\mathbb{F}_q$, este resultado es claro contando las raíces de $P(X)$.

Sabemos que $P(X)$ tiene q^n raíces por ser este el grado del polinomio. Para cada r divisor de n, los irreducibles de las raíces con ese grado son factores de $P(X)$ y, por tanto, hay rt_r de ellos.

La suma de todos nos da la igualdad buscada:

$$\sum_{r \in Div(n)} rt_r = q^n$$

De la definición de la definición de Möbius,

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ es el producto de } r \text{ enteros primos distintos} \\ 0 & \text{si } n \text{ es divisible por el cuadrado de un entero primo} \end{cases}$$

y del resultado que acabamos de ver, es directo deducir la fórmula para t_r:

$$t_r = \frac{1}{r} \sum_{d \in Div(r)} \mu(d) q^{\frac{r}{d}}$$