MONOGRAFÍAS MATEMÁTICAS

TEOREMA DE WEDDERBURN

FERNANDO REVILLA JIMÉNEZ

RESUMEN. Demostramos el teorema de Wedderburn: todo cuerpo finito es conmutativo.

Enunciado
A lo largo de éste problema la letra K designará un cuerpo finito y no necesariamente conmutativo. Si A es un conjunto, denotamos por $|A|$ al cardinal de A. Se trata de demostrar el teorema de Wedderburn i.e. que todo cuerpo finito es conmutativo.

1) Sea $k \subset K$ un subcuerpo propio y conmutativo de K.
(i) Demostrar que la dimensión de K como k-espacio vectorial es finita y mayor o igual que 2
(ii) Demostrar existe un entero $n \geq 2$ tal que $|K| = |k|^n$.
2) Sea $s \in K$. Definimos el *centralizador* de s como

$$C_s = \{x \in K : xs = sx\}$$

es decir, como el conjunto de los elementos de K que conmutan con s. Demostrar que C_s es subcuerpo de K.
3) El *centro* de K se define como

$$Z = \{a \in K : ax = xa \ \forall x \in K\}$$

es decir, es el conjunto de los elementos de K que conmutan con todos los de K. Demostrar que Z es subcuerpo conmutativo de K.
Nota. Obsérvese que el teorema de Wedderburn quedaría demostrado si demostramos que $Z = K$.
4) Sea $|Z| = q$. Demostrar que $|K| = q^n$ y que $|C_s| = q^{n_s}$ para ciertos enteros positivos n, n_s. Demostrar que si además K no es conmutativo, existe $s \in K$ tal que $n_s < n$.
5) Definimos en $K^* = K \setminus \{0\}$ la relación

$$u \sim v \Leftrightarrow u = x^{-1}vx \text{ para algún } x \in K^*.$$

Demostrar que $\sim$ es relación de equivalencia en K^* y determinar sus clases de equivalencia.
6) Demostrar que $|[s]| = 1 \Leftrightarrow s \in Z$, y que si K no es conmutativo existe al menos una clase tal que $|[s]| \geq 2$.

Key words and phrases. teorema, Wedderburn.

7) Para $s \in K^*$ denotamos $C_s^* = C_s \setminus \{0\}$ y $C_s^* x = \{zx : z \in C_s^*\}$. Se considera la aplicación

$$f_s : K^* \to [s], \quad f_s(x) = x^{-1}sx.$$

Demostrar que $f_s(x) = f_s(y)$ si y sólo si, $y \in C_s^* x$. Aplicar éste resultado para demostrar que

$$\frac{|K^*|}{|C_s^*|} = \frac{q^n - 1}{q^{n_s} - 1} = |[s]|$$

en donde q, n y n_s tienen los mismos significados que en el apartado 4.
8) Sea K no conmutativo y llamemos $Z^* = Z \setminus \{0\}$. Sean $[s_1], \ldots, [s_m]$ las clases que tienen más de un elemento (vimos que existen si K no conmutativo). Demostrar la fórmula

$$q^n - 1 = q - 1 + \sum_{k=1}^{m} \frac{q^n - 1}{q^{n_k} - 1} \ \text{ con } \ 1 < \frac{q^n - 1}{q^{n_k} - 1} \in \mathbb{N} \ \ \forall k = 1, \ldots, m.$$

9) Sea K no conmutativo. Demostrar que $n_k \mid n$ para todo $k = 1, \ldots, m$.
10) Sea $\xi = e^{2\pi i/n}$ y $U_n = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$ el grupo cíclico multiplicativo de las raíces enésimas de la unidad. Si $\lambda \in U_n$ definimos ord λ (orden de λ) como el menor entero positivo d tal que $\lambda^d = 1$. Por el teorema de Lagrange, necesariamente $d \mid n$. Para todos los divisores positivos d de n definimos los polinomios:

$$\phi_d(x) := \prod_{\text{ord } \lambda = d} (x - \lambda) \text{ con lo cual, } \ x^n - 1 = \prod_{d \mid n} \phi_d(x).$$

(i) Descomponer $x^6 - 1$ como producto de los polinomios $\phi_d(x)$ con $d \mid 6$.
(ii) Demostrar que para todo n el polinomio $\phi_n(x)$ tiene coeficientes enteros (i.e. $\phi_n(x) \in \mathbb{Z}[x]$) y que su término constante es 1 0 -1.
11) Demostrar que si K no es conmutativo, entonces $\phi_n(q) \mid q - 1$.
12) Demostrar el teorema de Wedderburn: todo cuerpo finito es conmutativo.

Solución
1) (i) Al ser k conmutativo, claramente K es espacio vectorial sobre el cuerpo k, y por ser K finito la dimensión de K es finita. Si $a \in K$ y $a \notin k$ el sistema $S = \{1, a\}$ es libre. En efecto, si $\lambda_1 1 + \lambda_2 a = 0$ con $\lambda_1, \lambda_2 \in k$ han de ser nulos los escalares λ_1 y λ_2. Si fuera $\lambda_2 \neq 0$, entonces

$$\lambda_1 1 + \lambda_2 a = 0 \Rightarrow \lambda_2 a = -\lambda_1 \Rightarrow a = \lambda_2^{-1}(-\lambda_1).$$

Entonces, $a = \lambda_2^{-1}(-\lambda_1)$ pertenecería a k en contradicción con la hipótesis. Necesariamente $\lambda_2 = 0$ y por ende, $\lambda_1 = -0a = 0$. Concluimos pues que $\dim K \geq 2$ y finita.
(ii) Sea $\dim K = n$, que según el apartado anterior es ≥ 2 y finita. Al ser K isomorfo a k^n, se verifica $|K| = |k^n| = |k|^n$.

2) Claramente 0 y 1 pertenecen a C_s. Por otra parte,

$$x, y \in C_s \Rightarrow (x - y)s = xs - ys = sx - sy = s(x - y) \Rightarrow x - y \in C_s,$$

$$x, y \in C_s \Rightarrow (xy)s = x(ys) = x(sy) = (xs)y = (sx)y = s(xy) \Rightarrow xy \in C_s,$$
$$0 \neq x \in C_s \Rightarrow xs = sx \Rightarrow s = x^{-1}sx \Rightarrow sx^{-1} = x^{-1}s \Rightarrow x^{-1} \in C_s$$

es decir, C_s es subcuerpo de K.

3) Tenemos que $Z = \bigcap_{s\in K} C_s$ y la intersección de subcuerpos es subcuerpo. Además, Z es conmutativo por su propia definición.

4) Dado que Z es subcuerpo conmutativo tanto de C_s como de K, podemos considerar a C_s y a K como espacios vectoriales sobre Z. Si $\dim C_s = n_s$ entonces, $n_s \geq 1$ por ser $\{1\}$ sistema libre y $C_s \cong Z^{n_s}$ es decir $|C_s| = q^{n_s}$. De manera análoga, si $\dim K = n$ entonces $|K| = q^n$ con $n \geq 1$. Nótese que según el apartado primero, sería $n \geq 2$ si $Z \subsetneq K$.

5) Para todo $u \in K^*$ se verifica $u = 1^{-1}u1$ es decir, $u \sim u$. Si $u \sim v$ entonces $u = x^{-1}vx$ lo cual implica $v = xux^{-1} = (x^{-1})^{-1}ux^{-1}$, luego $v \sim u$. Sean ahora $u, v, w \in K^*$. Entonces

$$\begin{cases} u \sim v \\ v \sim w \end{cases} \Rightarrow \begin{cases} u = x^{-1}vx \\ v = y^{-1}wy \end{cases} \Rightarrow u = x^{-1}y^{-1}wyx = (yx)^{-1}w(yx) \Rightarrow u \sim w.$$

Concluimos que $\sim$ es relación de equivalencia en K^*. Si $s \in K^*$, la clase de equivalencia a la que pertenece s es

$$[s] = \{u \in K^* : u \sim s\} = \{u \in K^* : u = x^{-1}sx \text{ con } x \in K^*\}$$
$$= \{x^{-1}sx : x \in K^*\}.$$

6) $\Rightarrow$) Si el cardinal de $[s]$ es 1, entonces $[s] = \{s\}$ y por tanto $s = x^{-1}sx$ para todo $x \in K^*$, luego $xs = sx$ para todo $x \in K^*$ y por supuesto para todo $x \in K$ con lo cual $s \in Z$.
$\Leftarrow$) Si $s \in Z$ entonces $sx = xs$ para todo $x \in K$, por tanto

$$[s] = \{x^{-1}sx : x \in K^*\} = \{x^{-1}xs : x \in K^*\} = \{s\} \Rightarrow |[s]| = 1.$$

Si K no es conmutativo existe $s \in K$ tal que $s \notin Z$ por tanto $\emptyset \neq [s]$ no tiene cardinal 1, es decir $|[s]| \geq 2$.

7) Para todo $x, y \in K^*$ se verifica

$$f_s(x) = f_s(y) \Leftrightarrow x^{-1}sx = y^{-1}sy \Leftrightarrow \left(yx^{-1}\right)s = s\left(yx^{-1}\right)$$
$$\Leftrightarrow yx^{-1} \in C_s^* \Leftrightarrow y \in C_s^* x.$$

Claramente $|C_s^* x| = |C_s^*|$ pues x es invertible. Cada elemento $f_s(x) = x^{-1}sx$ de $[s]$ es la imagen de los $y \in K^*$ tales que $y \in C_s^*$ es decir es la imagen de $|C_s^* x| = |C_s^*|$ elementos de K^*, luego $|K^*| = |[s]|\,|C_s^*|$. Es decir

$$\frac{|K^*|}{|C_s^*|} = \frac{q^n - 1}{q^{n_s} - 1} = |[s]| \quad \forall s \in K^*.$$

8) Tenemos $|K^*| = q^n - 1$, $|Z^*| = q - 1$ y $|C_s^*| = q^{n_s} - 1$. Las clases de equivalencia de $\sim$ en K^* forman una partición de K^* y tenemos $|K^*|$ clases

de equivalencia con un elemento y m clases $[s_1], \ldots, [s_m]$ con $q^{n_1}, \ldots, q^{n_m}$ elementos respectivamente, con lo cual $|K^*| = |Z^*| + \sum_{k=1}^{m} \left|C^*_{s_k}\right|$ y usando el apartado anterior queda

$$q^n - 1 = q - 1 + \sum_{k=1}^{m} \frac{q^n - 1}{q^{n_k} - 1}.$$

Por otra parte, para toda clase $[s_k]$ con $k = 1, \ldots, m$ se verifica $1 < |[s_k]| \in \mathbb{N}$ con lo cual,

$$1 < |[s_k]| = \frac{q^n - 1}{q^{n_k} - 1} \in \mathbb{N}.$$

9) Podemos escribir $n = an_k + r$ con $0 \leq r < n_k$ y para todo k se verifica $q^{n_k} - 1 \mid q^n - 1$. Entonces,

$$q^{n_k} - 1 \mid q^n - 1 \Rightarrow q^{n_k} - 1 \mid q^{an_k + r} - 1 \Rightarrow$$

$$q^{n_k} - 1 \mid \left(q^{an_k + r} - 1\right) - (q^{n_k} - 1) = q^{n_k}\left(q^{(a-1)n_k + r} - 1\right).$$

Dado que q^{n_k} y $q^{n_k} - 1$ son relativamente primos, se verifica $q^{n_k} - 1 \mid q^{(a-1)n_k + r} - 1$, y continuando de esta manera llegaríamos a que $q^{n_k} - 1 \mid q^r - 1$ con $0 \leq r < n_k$ que sólo puede ocurrir si $r = 0$, luego $n = an_k$. Es decir, $n_k \mid n$.

10) (i) Tenemos $U_6 = \{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5\}$. Los mínimos exponentes positivos d que corresponden a cada raíz son

$$1^1 = 1,\ \xi^6 = 1,\ (\xi^2)^3 = 1,\ (\xi^3)^2 = 1,\ (\xi^4)^3 = 1,\ (\xi^5)^6 = 1,$$

luego los polinomios $\phi_d(x)$ son

$$\begin{aligned} &\phi_1(x) = x - 1, \quad \phi_2(x) = (x - \xi^3), \\ &\phi_3(x) = (x - \xi^2)(x - \xi^4), \quad \phi_6(x) = (x - \xi)(x - \xi^5), \end{aligned}$$

y queda $x^6 - 1 = \phi_1(x)\phi_2(x)\phi_3(x)\phi_6(x)$.
(ii) Se verifica $\phi_1(x) = x - 1$ y procedamos por inducción. Supongamos que $\phi_d(x) \in \mathbb{Z}[x]$ para todo $d < n$ y que sus coeficientes constantes son 1 o -1. Por la descomposición $x^n - 1 = \prod_{d|n} \phi_d(x)$:

$$x^n - 1 = p(x)\phi_n(x) \ \text{ con } \ p(x) = \sum_{i=0}^{l} a_i x^i,\ \phi_n(x) = \sum_{j=0}^{n-l} b_j x^j$$

con los a_i enteros y $a_0 = 1$ o $a_0 = -1$. Dado que $-1 = a_0 b_0$, se verifica $b_0 = 1$ o $b_0 = -1$. Supongamos ahora que $b_0, b_1, \ldots, b_{k-1} \in \mathbb{Z}$. Igualando coeficientes de x^k en ambos miembros de $x^n - 1 = \prod_{d|n} \phi_d(x)$:

$$\sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=1}^{k} a_i b_{k-i} + a_0 b_k \in \mathbb{Z}.$$

Por hipótesis $b_0, b_1 \ldots, b_{k-1}$ son enteros, y también lo son todos los a_i. Dado que a_0 es 1 o -1, también es entero b_k.

11) Si $n_k \mid n$ es uno de los números que aparecen en el apartado 4, se verifica:

$$x^n - 1 = \prod_{d|n} \phi_d(x) = (x^{n_k} - 1)\, \phi_n(x) \prod_{d|n,\, d\nmid n_k\ d\neq n} \phi_d(x).$$

En consecuencia y para $q = |K|$ se verifican las relaciones de divisibilidad en $\mathbb{Z}$:

$$\phi_n(q) \mid q^n - 1 \quad y \quad \phi_n(q) \mid \frac{q^n - 1}{q^{n_k} - 1}.$$

Por la fórmula demostrada en el apartado 8 para todo n_k:

$$q^n - 1 = q - 1 + \sum_{k=1}^{m} \frac{q^n - 1}{q^{n_k} - 1},$$

deducimos que $\phi_n(q) \mid q - 1$.

12) Supongamos que K no es conmutativo. Entonces $Z \subsetneq K$ y por el apartado 1, $n > 1$. Sabemos que $\phi_n(x) = \prod(x - \lambda)$ en donde λ recorre todas las raíces de orden n. Al ser $n > 1$, $\lambda = a + bi \neq 1$ y la parte real a de λ claramente satisface $a < 1$. Entonces,

$$\begin{aligned} |q - \lambda|^2 = |q - a - bi|^2 = (q - a)^2 + b^2 = q^2 - 2aq + a^2 + b^2 \\ = q^2 - 2aq + 1 \underbrace{>}_{a<1} q^2 - 2q + 1 = (q - 1)^2. \end{aligned}$$

Es decir, se verifica $|q - \lambda| > q - 1$ para toda λ de orden n. Esto implica

$$|\phi_n(q)| > \prod_{\text{ord } \lambda = n} |q - \lambda| > q - 1.$$

Pero esto contradice la relación $\phi_n(q) \mid q - 1$ demostrada en el apartado anterior. Concluimos que K ha de ser necesariamente conmutativo y queda demostrado el teorema de Wedderburn. □

Fernando Revilla Jiménez. Jefe del Departamento de Matemáticas del IES Santa Teresa de Jesús de la Comunidad de Madrid y Profesor de Métodos Matemáticos de la Universidad Alfonso X El Sabio de Villanueva de la Cañada, Madrid (Hasta el curso académico 2008-2009).

E-mail address: frej0002@ficus.pntic.mec.es