Miscelánea Matemática **53** (2011) 33–37 SMM

Otra caracterización de los grupos cíclicos finitos

Juan Morales Rodríguez

jmorales@unam.mx

Departamento de Matemáticas
Facultad de Ciencias
Universidad Nacional Autónoma de México
04510 México, D. F., México

Cuando el antagonismo, esto es, el egoísmo, no reine más en la ciencia, cuando se formen sociedades para estudiar, en lugar de enviar a las Academias paquetes sellados, se apresurarán a publicar sus mínimas observaciones por poco que tengan de novedad, y se agregará "lo demás no lo sé"
Evariste Galois.

Este trabajo es un pequeño tributo a la memoria del genial matemático Évariste Galois, en el segundo centenario de su nacimiento.

En mil ochocientos treinta, con sólo diez y nueve años de edad, Galois logró establecer criterios con base en los cuales, dada una ecuación algebraica, se está en posibilidad de establecer si es, o no, soluble por radicales. Concretamente, demostró que una ecuación algebraica con coeficientes racionales es soluble por radicales si y sólo si su grupo tiene una serie de composición con todos sus factores de orden primo. Lo que es equivalente a que éste tenga una serie subnormal con todos sus factores cíclicos.

El objetivo principal de esta nota es presentar una caracterización original de los grupos cíclicos finitos.

Parece ocioso hacer notar que en cada grupo cíclico finito, existe un elemento g de orden máximo, necesariamente en su centro, tal que el subgrupo generado por cada elemento diferente del idéntico tiene intersección no trivial con el subgrupo generado por g. Demostraremos que esta propiedad caracteriza a los grupos cíclicos finitos y la usaremos para probar dos conocidos resultados, primero, que en un grupo abeliano finito G, si $g \in G$ es de orden máximo, G es producto directo

del subgrupo generado por g con un subgrupo M, y segundo, que un grupo finito es cíclico si y sólo si es abeliano y por cada primo p que divide a su orden, el grupo tiene sólo un subgrupo de orden p.

En primer lugar demostraremos un lema, de carácter en buena medida técnico.

Lema 1 *Sea G un grupo finito y $g \in G$ de orden máximo. Si g está contenido en el centro de G ($Z(G)$), entonces, para todo $y \in G$, el orden de y ($o(y)$) divide al orden de g.*

Demostración. Es suficiente probar que si $y \in G$ y $o(y) = p^k l$ con p un primo y $(p, l) = 1$, p^k divide a $o(g)$.

Se tiene que $o(g) = p^\alpha \beta$ con $(p, \beta) = 1$; $c = y^l$ es de orden p^k, $d = g^{p^\alpha}$ es de orden β; como $d \in Z(G)$ y $(p^k, \beta) = 1$, el orden de cd es $p^k\beta$, de donde se sigue que $p^k\beta \leq p^\alpha\beta$, lo que implica que $k \leq \alpha$, por consiguiente p^k divide a p^α y p^k divide a $p^\alpha\beta$, esto es, p^k divide a $o(g)$.

Presentaremos ahora la anunciada caracterización de los grupos cíclicos finitos.

Teorema 2 *Sea G un grupo finito. G es cíclico si y sólo si existe $g \in G$ de orden máximo, tal que $g \in Z(G)$ y para todo $b \in G$, $b \neq 1$, la intersección del subgrupo generado por b ($\langle b \rangle$) con el subgrupo generado por g no es trivial.*

Demostración. Sólo es necesario probar la suficiencia.

Sea $A = \langle g \rangle$, demostraremos que $G = A$.

Supóngase que $G - A \neq \emptyset$.

Si $x \in G - A$, el orden de x no es primo, porque $\mathbf{1} \neq \langle x \rangle \cap A \lneqq \langle x \rangle$, lo que implica que $o(\langle x \rangle \cap A)$ es un divisor de $o(x)$ diferente de 1 y de $o(x)$.

Sea $b \in G - A$ de orden mínimo y p un primo que divide a $o(b)$, digamos que $o(b) = pl$. Como $o(b^p) < o(b)$, $b^p \in A$, es decir $b^p = g^r$ para alguna $1 \leq r < o(g)$.

Por el lema 1, $o(b)$ divide a $o(g)$, pongamos $o(g) = pls$; $1 = b^{o(g)} = b^{pls} = (b^p)^{ls} = g^{rls}$, de donde se tiene que pls divide a rls, y por ello p divide a r; sea $r = pt$, así, $b^p = g^r = g^{pt}$, $b^p g^{-pt} = 1$, $(bg^{-t})^p = 1$, lo que implica que $bg^{-t} \in A$, y por consiguiente $b \in A$, lo que es una contradicción.

Por lo tanto $G - A = \emptyset$ y G es cíclico.

Utilizando esta caracterización de los grupos cíclicos demostraremos la siguiente afirmación.

Lema 3 *Sea G un grupo abeliano finito y $g \in G$ de orden máximo. Si A es el subgrupo generado por g, existe un subgrupo M de G tal que G es el producto directo de A y M.*

Demostración. Procederemos por inducción sobre el orden de G.

Podemos suponer que G no es cíclico.

Por el Teorema 1 existe $b \in G$, $b \neq 1$, tal que $\langle b \rangle \cap A = \mathbf{1}$.

Sea $Q = \langle b \rangle$ y $\bar{G} = G/Q$. Por el lema 1, $o(b)$ divide a $o(g)$ y como $1 < o(b) \leq o(g) < o(G)$, $\bar{G}$ es un grupo abeliano no trivial de orden menor que $o(G)$.

Probaremos que $\bar{g} = gQ \in \bar{G}$ es un elemento de orden mximo.

Es conocido que $s = o(\bar{g})$ divide a $o(g)$; ahora, $Q = \bar{g}^s = (gQ)^s = g^sQ$, por lo que $g^s \in Q \cap A$ y como $Q \cap A = \mathbf{1}$, se tiene que $g^s = 1$, lo que muestra que $o(g)$ divide a $o(\bar{g})$, y por consiguiente $o(\bar{g}) = o(g)$, lo que implica que $\bar{g} = gQ$ es un elemento de orden mximo, ya que si $xQ \in \bar{G}$, $o(xQ) \leq o(x) \leq o(g) = o(\bar{g})$.

Por hipótesis de inducción, si $\bar{A} = \langle \bar{g} \rangle$, existe un subgrupo $\bar{M}$ de $\bar{G}$ tal que $\bar{G}$ es el producto directo de $\bar{A}$ y $\bar{M}$.

Se tiene que $\bar{M} = M/Q$ para algn un subgrupo M de G tal que $Q < M$. Probaremos que G es el producto directo de A y M.

Si $x \in G$, $xQ = (gQ)^r mQ$ con $m \in M$, por lo que $x = g^r q_1 m q_2$ con q_1, $q_2 \in Q$ y se tiene que $x \in AM$, esto es $G = AM$.

Si $x \in A \cap M$, $xQ \in \bar{A} \cap \bar{M}$, de donde se sigue que $xQ = Q$, y $x \in Q = \langle b \rangle$, de donde se tiene que $x \in \langle b \rangle \cap A$, y entonces $x = 1$. Por lo tanto G es el producto directo de A y M.

Usando el lema anterior y por consiguiente la caracterización de los grupos cíclicos finitos que se da en el teorema 1, demostraremos el siguiente resultado.

Teorema 4 *Todo grupo abeliano finito G es producto directo de subgrupos cíclicos A_1, A_2, ..., A_s con $s \geq 1$, tales que $o(A_{i+1})$ divide a $o(A_i)$ para toda $i = 1, ..., s-1$.*

Demostración. Se har por inducción sobre el orden de G.

Podemos suponer que G no es cíclico.

Sea $g \in G$ de orden mximo, si $A_1 = \langle g \rangle$, por el lema anterior existe un subgrupo M de G tal que G es el producto directo de A_1 y M.

Como $o(M) < o(G)$, por hipótesis de inducción existen A_2, ..., A_s subgrupos cíclicos de M tales que M es el producto directo de A_2, ..., A_s y $o(A_{j+1})$ divide a $o(A_j)$ para toda $2 \leq j \leq s-1$.

$G = A_1M = A_1(A_2...A_s) = A_1A_2...A_s$, adems:

$$\begin{aligned} A_{s-1} \cap A_s &= \mathbf{1} \\ A_{s-2} \cap (A_{s-1}A_s) &= \mathbf{1} \\ &\vdots \\ A_2 \cap (A_3A_4...A_{s-1}A_s) &= \mathbf{1} \\ A_1 \cap (A_2...A_s) = A_1 \cap M &= \mathbf{1} \end{aligned}$$

Por lo tanto, G es el producto directo de A_1, A_2, ..., A_s.

Para terminar la demostración del teorema, sólo hace falta hacer notar que $o(A_2)$ divide a $o(A_1)$, pero esto se sigue del lema 1.

Teorema 5 *Si G es un grupo abeliano finito y m es un divisor de su orden, G tiene un subgrupo de orden m*

Demostración. Como diría Galois, se hace sola.

Se puede probar que si el grupo finito G es producto directo de los grupos cíclicos A_1, ..., A_s con $o(A_{i+1})$ divisor de $o(A_i)$ para toda $i = 1, ..., s-1$ y el grupo finito H es el producto directo de los subgrupos cíclicos B_1, ..., B_r con $o(B_{j+1})$ divisor de $o(B_j)$ para toda $j = 1, ..., r-1$, se tiene que G y H son isomorfos si y sólo si $s = r$ y para toda $1 \leq i \leq s$, los grupos A_i y B_i son isomorfos.

Este hecho se conoce como el teorema fundamental de los grupos abelianos finitos. Una demostración sencilla de éste se puede ver en [1].

Utilizando de nuevo el teorema 1, daremos esta otra conocida caracterización de los grupos cíclicos finitos.

Teorema 6 *Sea G un grupo finito. G es cíclico si y sólo si G es abeliano y para cada primo p que divide a $o(G)$, G tiene sólo un subgrupo de orden p.*

Demostración. Sólo es necesario demostrar la suficiencia.

Sea $g \in G$ de orden mximo y $A = \langle g \rangle$.

Si $x \in G$, $x \neq 1$ y el primo p divide a $o(x)$, $\langle x \rangle$ tiene un subgrupo H de orden p; en virtud del lema 1, se tiene que p divide a $o(A)$ y por lo tanto A tambin tiene un subgrupo K de orden p. Por hipótesis G sólo tiene un subgrupo de orden p, por lo tanto $H = K$ y se tiene que $H < \langle x \rangle \cap \langle g \rangle$ de donde se sigue, por el Teorema 1, que G es cíclico.

Colorario *Sea P un $p-$grupo finito. Si P es abeliano y sólo tiene un subgrupo de orden p, P es cíclico.*

Observaciones.

1. Si en el enunciado del corolario anterior se suprime la hipótesis de ser abeliano, el grupo P no necesariamente es cíclico. El grupo Q de los cuaternios es un grupo de orden 8 con sólo un subgrupo de orden 2 y no es cíclico.

2. Se prueba (por ejemplo en [**3**]) que si P es un $p-$grupo finito, P tiene sólo un subgrupo de orden p si y sólo si P es cíclico ó $p = 2$ y P es un grupo cuaternio generalizado.

Bibliografía

1. M. A. Armstrong, *Groups and Symmetry*, Springer-Verlag, 1988.
2. J. M. Rodríguez, Una caracterización de los grupos cíclicos finitos, *Aportaciones Matemáticas, SMM, Serie Comunicaciones* **25** (1999) 79–82.
3. G. Zappa, *Fondamenti di Teoria dei Gruppi, volume secondo*, Edizioni Cremonese, Roma, 1970.