Revista INTEGRACION
Departamento de Matemáticas UIS
Vol. 4. No. 2. julio-diciembre 1986

El grupo $\langle Z'_n, \cdot, 1 \rangle$

CARLOS LEZAMA*
FRANCISCO ACEVEDO**
ENRIQUE AVENDAÑO**

1. INTRODUCCION

Uno de los temas que se estudian en un curso elemental de Algebra a nivel de Licenciatura en Matemática es el de los grupos cíclicos. Puesto que todo grupo cíclico finito de orden n es isomorfo con el grupo aditivo de los enteros módulo n, $\langle Z_n, +, 0 \rangle$, éste es uno de los ejemplos iniciales del tema mencionado.

Una pregunta que formulan algunos estudiantes luego de introducir el anterior ejemplo es la siguiente:

¿Es cíclico el grupo multiplicativo de los enteros módulo n?

En otros términos, ¿Es cíclico el grupo $\langle Z'_n, \cdot, 1 \rangle$, donde

$Z'_n = \{k \in Z_n / (n,k) = 1\}$?

Cuando surgió tal pregunta en clase, fueron propuestos los siguientes ejercicios:

1. Averiguar si $\langle Z'_8, ., 1 \rangle$ es cíclico
2. Averigurar si $\langle Z'_{10}, ., 1 \rangle$ es cíclico
3. ¿Para qué valores de n es cíclico el grupo $\langle Z'_n, ., 1 \rangle$?

* Prof. Asistente. Departamento de Matemáticas. Universidad Industrial de Santander. Bucaramanga, Colombia.

** Estudiantes V Semestre Licenciatura en Matemáticas. Universidad Industrial de Santander, Bucaramanga, Colombia.

2. UN PRIMER ENFOQUE

Por la forma como son planteados los ejercicios, es de esperarse que para los dos primeros se busque la respuesta por «ensayo directo», esto es, a partir de la definición misma de grupo cíclico.

Procediendo así, tenemos:

Para $Z'_8 = \{1,3,5,7\}$, $|3| = |5| = |7| = 2$. Por tanto, $\langle Z'_8, ., 1\rangle$ no es cíclico.

Para $Z'_{10} = \{1,3,7,9\}$, $|3| = 4$. Por tanto, $\langle Z'_{10}, \cdot, 1\rangle$ es cíclico. Un generador es 3.

En cuanto al tercer ejercicio, de las catorce obras consultadas (ver referencias) sólo seis contienen algo al respecto:

En [4], p. 150, aparece propuesto el siguiente ejercicio:

¿Es cíclico el grupo multiplicativo de 1,2,...,6, mód. 7?
¿Y el de 1,3,5,7, mód. 8? ¿Y el de 1,2,4,5,7,8, mód. 9?

En [12], p. 158, se propone el siguiente ejercicio:

Se puede demostrar que para todo primo p, el grupo multiplicativo del campo Z_p es cíclico. Verificarlo para p = 7,11 y 13.

En [3], p. 134, se demuestra lo siguiente:

Si $|G| = pq$, donde p y q son primos y $p < q$, entonces G tiene un subgrupo, y solamente uno, de orden q, por ejemplo $\langle Z'_{14}, \cdot, 1\rangle$. Más aún, si $q \not\equiv 1 + kp$ para todo entero k, entonces G es el grupo cíclico de orden pq.

Además, en [1], p. 263, se demuestra el siguiente teorema:

«Dado $m \geq 1$ en donde m no es de la forma $m = 1,2,4,p^e$ ó $2p^e$, en donde p es un primo impar, entonces para todo a con (a,m) = 1 tenemos $a^{(\phi(m)/2)} \equiv 1$ (mód m), luego no existen raíces primitivas mód m».

En [13], p. 92, aparece demostrado el siguiente teorema de Gauss:

«Z'_n es cíclico si y sólo si n es uno de los siguientes:

$n = 2,4,p^m$, ó $2p^m$ donde p es un primo impar y $m \geq 1$».

El teorema anterior responde completamente la cuestión planteada en 1. Sin embargo, con este artículo se pretende mostrar otro enfoque.

3. UN SEGUNDO ENFOQUE

Dado que la relación de congruencia módulo n es la que determina los elementos del conjunto Z'_n, y que tal relación se estudia con detalle en Teoría de Números, se le dio un nuevo enfoque al ejercicio. «Traducir» al lenguaje de la teoría de Grupos resultados ya establecidos de Teoría de Números. Para tal fin se consultó el capítulo sexto, numerales 1,2 y 3, de [14].

4. PROPOSICIONES Y EJEMPLOS

En lo que sigue, Φ representa la función de Euler. Por tanto, $\Phi(n)$ representa el número de enteros positivos primos relativos con n y menores que n, para $n > 1$ y $\Phi(1) = 1$.

4.1 Proposición

Existe $g \in Z'_p$ tal que $|g| = \Phi(p)$, siendo p primo impar.

Dem. Sean $\delta_1, \delta_2, ..., \delta_r$ los distintos órdenes de los elementos de Z'_p.

Sea τ el mínimo común múltiplo de $\delta_1, \delta_2, ..., \delta_r$,

Sea $\tau = q_1^{\alpha_1} q_2^{\alpha_2} ... q_k^{\alpha_k}$ la descomposición canónica de τ. Cada factor $q_s^{\alpha_s}$ de esta descomposición divide al menos a uno de los órdenes δ_i, el cual, por consiguiente, puede ser expresado en la forma $\delta_i = a_i q_s^{\alpha_s}$

Sea g_i uno de los elementos de Z'_p cuyo orden es δ_i. Se tiene entonces que

$$g_i^{\delta_i} = g_i^{a_i q_s^{\alpha_s}} = (g_i^{a_i})^{q_s^{\alpha_s}} = 1.$$

Además,

$(g_1^{a_1} g_2^{a_2} ... g_k^{a_k})^{q_1^{\alpha_1} q_2^{\alpha_2} ... q_k^{\alpha_k}} = 1$, por ser $q_1^{\alpha_1}, q_2^{\alpha_2}, ..., q_k^{\alpha_2}$ primos relativos dos a dos.

Puesto que cada δ_i/τ, cada elemento de Z'_p satisface la igualdad $x^{\tau} = 1$. Por tanto, $\tau \geq p - 1$. Pero $\tau/\Phi(p)$, luego $\tau = \Phi(p)$.

Haciendo

$g = g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_k^{\alpha_k}$, se tiene que $|g| = \Phi(p)$. ■

Ejemplo:

Sea $G = \langle Z'_{13}, \cdot, 1 \rangle$. Entonces $|G| = 12 = 2^2.3$;
$|5| = 4 = 1.2^2$; $|4| = 6 = 2.3$.

Por tanto, $5.4 = 7$ es un generador, como puede comprobarlo el lector.

4.2 Proposición

Sea p un primo impar. Sea $\alpha > 1$. Entonces existe $h \in Z'_{p^\alpha}$ tal que $|h| = \Phi(p^\alpha)$; $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Dem:

La proposición anterior garantiza que existe $g \in Z'_p$ tal que $|g| = \Phi(p)$. Así, $g^{p-1} = 1 + pT_0$. Además,

$$(g + pt)^{p-1} = 1 + p(T_0 - g^{p-2} t + pT) = 1 + pu, \qquad (1)$$

donde $0 \leqslant u, t \leqslant p - 1$. Existe entonces un valor de t que no divide a u. Sea t_1 uno de estos valores. Por (1), tenemos:

$$\left.\begin{aligned} g + pt_1)^{p(p-1)} &= (1 + pu)^p = 1 + p^2 u_2 \\ (g + pt_1)^{p^2 (p-1)} &= (1 + p^2 u_2)^p = 1 + p^3 u_3 \end{aligned}\right\} \qquad (2)$$

donde $p \nmid u_i$.

Supongamos que $|g + pt_1| = \delta$, como elemento de Z'_{p^α}. Así, $(g + pt_1)^\delta = 1$, como elemento de Z'_{p^α}. También se tiene entonces que

$(g + pt_1)^\delta = 1$, como elemento de Z'_p. (3)

Por tanto, $(p-1)/\delta$. Pero $\delta/(p^\alpha - p^{\alpha-1}) = \Phi(p^\alpha)$. Por tanto, $\delta = p^{r-1}(p-1)$, donde r es uno de los números 1,2,..., α. Reemplazando en (3), según (1) y (2), tenemos:

$(1 + p^r u_r) \equiv 1$ (mód p^α), esto es, $p^r u_r \equiv 0$ (mód p^α). Así, $r = \alpha$, y por tanto, $\delta = \Phi(p^\alpha)$. Haciendo $h = g + pt_1$, se tiene que $|h| = \Phi(p^\alpha)$. ■

Ejemplo:

Un generador de Z'_5 es 2. Hallemos un generador para Z'_{25}.

Buscamos un valor de t tal que $(2 + 5t)^4 = 1 + 5u$, $5 \nmid u$. Para $t = 0$, tenemos que $16 = 1 + 5.3$. Puesto que $5 \nmid 3$, $2 + 5.0 = 2$ es un generador para Z_{25}, y en general, es un generador para Z'_{5^α}, $\alpha > 1$ •

4.3 **Proposición**

Sea p un primo diferente de 2; sea $\alpha \geq 1$; sea $g \in Z'_{p^\alpha}$. Entonces $\langle g \rangle = Z'_{p^\alpha}$ si y sólo si para cada divisor primo q de $\Phi(p^\alpha)$ se tiene que $g^{\Phi(p^\alpha)/q} \neq 1$.

Dem:

→) Puesto que $|g| = \Phi(p^\alpha)$, el resultado es obvio.
←) Supongamos que existe β, $1 \leq \beta \leq \Phi(p^\alpha) - 1$ tal que $g^\beta = 1$. Puesto que $\beta/\Phi(p^\alpha)$, existe algún divisor primo q de $\Phi(p^\alpha)$ tal que $\Phi(p^\alpha) = q\beta u$. Por tanto, $g^{\frac{\Phi(p^\alpha)}{q}} = g^{\beta u} = 1$, lo cual contradice la hipótesis.

Es así que $\beta = \Phi(p^\alpha)$. Luego $\langle g \rangle = Z'_{p^\alpha}$. ■

Ejemplo 1:

Hallar todos los generadores de $\langle Z'_9, ., 1 \rangle$.

Aquí, $p = 3$, $\alpha = 2$;
$\Phi(9) = \Phi(3^2) = 3^2 - 3^1 = 6 = 2.3$.
¿Qué elementos g verifican $g^3 \neq 1$, $g^2 \neq 1$?
Como puede comprobarlo el lector, tales elementos son 2 y 5;
por tanto, $\langle 2 \rangle = \langle 5 \rangle = Z'_9$ •

Ejemplo 2:

Hallar todos los generadores de $\langle Z'_{11}, . , 1\rangle$.

Aquí, $p = 11$;
$\Phi(11) = 11 - 1 = 10 = 2.5$.
¿Qué elementos g verifican $g^5 \neq 1, g^2 \neq 1$?
Tales elementos son 2, 6, 7 y 8.

Por tanto, $\langle 2\rangle = \langle 6\rangle = \langle 7\rangle = \langle 8\rangle = Z'_{11}$ •

4.4 Proposición:

Sea p un primo impar. Sea $\alpha \geq 1$. Entonces existe $g \in Z'_{2p^\alpha}$ tal que $|g| = \Phi(2p^\alpha)$.

Dem.

Las dos proposiciones anteriores garantizan que existe $g \in Z'_{p^\alpha}$ tal que $|g| = \Phi(p^\alpha)$.
Por tanto $g^{\Phi(p^\alpha)} = 1$. Consideremos dos casos:

(i) g es impar. En tal caso, $g \in Z'_{2p^\alpha}$ ya que $(g, 2p^\alpha) = 1$.
Puesto que $\Phi(p^\alpha) = \Phi(2p^\alpha)$, se tiene que $\langle g\rangle = \langle Z'_{2p^\alpha}, . , 1\rangle$.

(ii) g es par. En tal caso, $g + p^\alpha$ es impar, y por tanto, $g + p^\alpha \in Z'_{2p^\alpha}$.
Puesto que $|g + p^\alpha| = |g| = \Phi(p^\alpha) = \Phi(2p^\alpha)$, $\langle g + p^\alpha\rangle = \langle Z'_{2p^\alpha}, . , 1\rangle$. ■

Con el fin de ilustrar la proposición que se acaba de demostrar se elaboró un programa en BASIC para el caso particular de $\alpha = 1$. Tal programa dio, para los cien primeros primos impares, todos los generadores de los grupos del tipo Z'_{2p}.

4.5 Corolario

Si g es un generador de $\langle Z'_{p^\alpha}, . , 1\rangle$, entonces el impar entre g y $g + p^\alpha$ es un generador de $\langle Z'_{2p^\alpha}, . , 1\rangle$. Entonces el impar entre g y $g + p^\alpha$ es un generador de $\langle Z'_{2p^\alpha}, . , 1\rangle$ ■

Ejemplo:

Hallar generadores para $\langle Z'_{22}, . , 1\rangle$.

Según el ejemplo 2 de la proposición 4.3,
7, $2 + 11 = 13$, $8 + 11 = 19$, $6 + 11 = 17$, son generadores para dicho grupo•

REFERENCIAS

[1] APOSTOL T.M. Introducción a la Teoría Analítica de Números. Editorial Reverté, Barcelona, 1980.

[2] AYRES FRANK, J.R. Algebra Moderna. Mc Graw-Hill, México, 1975.

[3] BAUMSLAG B. , CHANDLER B. Teoría de Grupos. Mc Graw-Hill, méxico, 1972.

[4] BIRKHOFF GARRET , MAC LANE SAUNDERS. Algebra Moderna. Editorial Teide, Barcelona, 1954.

[5] CLARK A. Elementos de Algebra Abstracta. Editorial Alhambra, Madrid, 1974.

[6] DEAN R.A. Elements of Abstract Algebra. Wiley International, New York, 1967.

[7] FRALEIGH John B. A First Course in Abstract Algebra. Addison-Wesley, Amsterdam, 1974.

[8] HALL MARSHALL, J.R. Teoría de los Grupos. Editorial Trillas, México, 1979.

[9] HERSTEIN I.N. Algebra Moderna. Editorial Trillas, México, 1974.

[10] LANG SERGE. Algebra. Editorial Aguilar, Madrid, 1971.

[11] LENTIN A. , RIVAUD J. Algebra Moderna. Editorial Aguilar, Madrid, 1969.

[12] Mc COY NEAL H. Fundamentals of Abstract Algebra. Allyn and Bacon, Boston, 1974.

[13] SHANKS DANIEL. Solved and Unsolved Problemas in Number Theory. Chelsea, New York, 1978.

[14] VINOGRADOV I.M. Fundamentos de la Teoría de los Números. Editorial MIR. Moscú 1977.