Tercera serie de ejercicios de Álgebra Moderna

Akiyuki Shinbou

Mayo 2018

Problema 1. Encuentra todos los generadores de Z_6, Z_8, Z_{20}

Solución:
Para Z_6: $\{1, 5\}$

Para Z_8: $\{1, 3, 5, 7\}$

Para Z_{20}: $\{1, 3, 5, 7, 11, 13, 17, 19\}$

Problema 2. Suponga que $\langle a\rangle$, $\langle b\rangle$ y $\langle c\rangle$ son grupos ciclicos de orden 6, 8 y 20 respectivamente. Encuentra todos los generadores de $\langle a\rangle$, $\langle b\rangle$ y $\langle c\rangle$.

Para $\langle a\rangle$, los generadores son $\{a^1, a^5\}$

Para $\langle b\rangle$, los generadores son $\{b^1, b^3, b^5, b^7\}$

Para $\langle c\rangle$, los generadores son $\{c^1, c^3, c^5, c^7, c^{11}, c^{13}, c^{17}, c^{19}\}$

Problema 3. Enlista los elementos de los subgrupos $\langle 20\rangle$ y $\langle 10\rangle$ en Z_{30}. Sea a el elemento del grupo de orden 30. Enlista los elementos de los subgrupos a^{20} y a^{10}.

$$\langle 20\rangle = \{0, 10, 20\}$$
$$\langle 10\rangle = \{0, 10, 20\}$$

Para a

$$
\begin{aligned}
|a| = |\langle a \rangle| &= 30 \\
mcd(30, 20) &= mcd(30, 10) \\
&= 10 \\
|\langle a^{10} \rangle| &= |\langle a^{20} \rangle| \\
&= 30/10 = 3 \\
\langle a^{10} \rangle = \langle a^{20} \rangle &= \langle a^{mcd(30,10)} \rangle \\
&= \langle a^{mcd(30,20)} \rangle \\
&= \langle a^{10} \rangle \\
\langle a^{10} \rangle &= \{e, a^{10}, a^{20}\}
\end{aligned}
$$

Problema 4. Enlista los elementos de los subgrupos $\langle 3 \rangle$ y $\langle 15 \rangle$ en Z_{18}. Sea a un elemento de grupo de orden 18. Enlista los elementos de los subgrupos $\langle a^3 \rangle$ y $\langle a^{15} \rangle$.

Solución:

$$
\begin{aligned}
\langle 3 \rangle &= \{3, 6, 9, 12, 15, 0\} \\
\langle 15 \rangle &= \{15, 12, 9, 6, 3, 0\} \\
\langle a^3 \rangle &= \{a3, a6, a9, a12, a15, a0\} \\
\langle a^{15} \rangle &= \{a15, a12, a9, a6, a3, a0\}
\end{aligned}
$$

Problema 5. Enlista los elementos de los subgrupos $\langle 3 \rangle$ y $\langle 7 \rangle$ en $U(20)$

Solución:

$$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$$

$3^1 = 3$

$3^2 = 9$

$3^3 = 27 \mod 20 = 7$

$3^4 = 7 \cdot 3 \mod 20 = 1$

$3^5 = 3 \cdot 1$

$\langle 3 \rangle = \{3, 7, 9, 1\}$

$7^1 = 7$

$7^2 = 49 \mod 20 = 9$

$7^3 = 9 \cdot 7 \mod 20 = 3$

$7^4 = 3 \cdot 7 \mod 20 = 1$

$\langle 7 \rangle = \{1, 3, 7, 9\}$

Problema 6. ¿Qué tienen en comun los ejercicios 3, 4 y 5? Intenta realizar una generalización que incluya los 3 casos.

Solución:
En cualquier grupo, $\langle a \rangle = \langle a^{-1} \rangle$.

Problema 7. Encuentra un ejemplo de un grupo no ciclico cuyos subgrupos propios son ciclicos.

Solución:
$U(8)$.

Problema 8. Sea a un elemento de un grupo y sea $|a| = 15$. Computa el orden de los siguientes elementos de G.

a. a^3, a^6, a^9, a^{12}

b. a^5, a^{10}

c. a^2, a^4, a^8, a^{14}

Solución:

a. 5

b. 3

c. 15

Problema 9. ¿Cuantos subgrupos tiene Z_{20}? Enlista los generadores de cada uno de estos subgrupos. Suponga que $G = \langle a \rangle$ y $|a| = 20$. ¿Cuantos de estos subrupos tiene G? Enlista los generadores de estos subgrupos.

Solución:
Usando la propiedad de los grupos, $\langle a \rangle$ es sugrupo de G, entonces contamos con 20 subgrupos de G, donde el generador es obvio. De igual manera, ya que el orden de a es 20, eso significa que para obtener la identidad se tuvo que operar y resultar en otros 19 elementos, donde cada uno de estos es generador de otro subgrupo de G. Es decir, que también existen 20 subgrupos y cada potencia de a es un generador.

Problema 10. En Z_{24}, enlista todos los generadores para el subgrupo de orden 8. Sea $G = \langle a \rangle$ y sea $|a| = 24$. Enlista todos los generadores del subgrupo de orden 8.

Solución:

$$Z_{24} = \{0, 1, \ldots, 23\}$$
$$\langle 24/8 \rangle = \langle 3 \rangle = 0, 3, 6, 9, 12, 15, 18, 21$$
$$|3| = |\langle 3 \rangle| = 8$$

Generadores para Z_{24} considerando el producto mod 24: $\{3, 9, 15, 21\}$ obtenidos a partir de la fórmula: $|a| = \frac{n}{mdc(n,k)}$ recorriendo los números desde 0 a 24 donde 24 es el orden de Z_{24}

Ahora

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{23}\}$$

Subgrupo de orden 8

$$\langle a^{\frac{24}{8}} \rangle = \langle a^3 \rangle$$
$$\langle a^3 \rangle = \{e, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}\}$$

Generadores

$$\langle a^3 \rangle = \{a^3, a^9, a^{15}, a^{21}\}$$

Obtenidos de la misma forma que el inciso anterior

Problema 11. Sea G un grupo y $a \in G$. Demuestre que $\langle a^{-1} \rangle = \langle a \rangle$.

Solución:
$a^{-1} \in \langle a \rangle$ por definicion, asi que $\langle a^{-1} \subseteq \langle a \rangle$. Por otro lado, $a = (a^{-1})^{-1} \in \langle a^{-1} \rangle$, por lo que $\langle a \rangle \subseteq \langle a^{-1} \rangle$. Con estas dos relaciones ya tenemos que $\langle a \rangle = \langle a^{-1} \rangle$.

Problema 12. En Z encuentra todos los generadores del subgrupo $\langle 3 \rangle$. Si a tiene orden infinito, encuentra todos los generadores del subgrupo $\langle a^3 \rangle$.

Solución:
En Z, los generadores de $\langle 3 \rangle$ son $\{3, -3\}$

Si a tiene orden infinito entonces $\langle a^3 \rangle$ tiene dos generadores $\{a^3, a^{-3}\}$.

Problema 14. Supón que un grupo ciclico G tiene exactamete tres subgrupos: el mismo G, $\{e\}$ y un subgrupo de orden 7. ¿Cual es $|G|$? ¿Qué puedes decir si 7 es reemplazado por p donde p es primo?

Solución:
Para poder tener exactamente 3 subgrupos, $|G|$ solo puede ser dividido por tres números: 1, 7 y $|G|$. Tambien sabemos que $|G|/7$ tambien es divisor de G, y que este numero debe ser 7 para que solo haya 3 subgrupos, por lo que $|G| = 7 \cdot 7 = 49$.

Problema 15. Sea G un grupo Abeliano y sea $H = \{g \in G | |g| \text{ divide a } 12\}$. Demuestra que H es un subgrupo de G. ¿Hay algo especial sobre el 12 aqui? ¿Tu demostración sería valida si 12 fuera reemplazada por algun otro entero positivo? Enuncia el resultado general.

Solución:
Si $|g|$ es dividido por 12, entonces $g^{12} = e$. Sean a y b en H. Vemos que $(ab^-1)^{12} = a^{12}(b^{12})^{-1} = ee^{-1} = e$, por tanto, H es subgrupo de G.

Problema 16. Encuentra una colección de subgrupos distintos $\langle a_1 \rangle, \langle a_2 \rangle, \ldots, \langle a_n \rangle$ of $_{240}$ con la propiedad que $\langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots \subset \langle a_n \rangle$ con la n mas grande posible.

Solución:

$$\langle a_2 \rangle, \langle a_4 \rangle, \langle a_8 \rangle, \langle a_{16} \rangle \cdots \langle a_{240} \rangle$$

Problema 17. Completa el siguiente enunciado: $|a| = |a^2|$ si y solo si $|a| \ldots$

Solución:
$\ldots$ es impar o infinito.

Dado que $k = 2$

$$|a^2| = \frac{n}{mdc(n,2)} = n$$

Para ello se necesita que n sea impar o infinito.

Problema 18. Si un grupo ciclico tiene un elemento de orden infinito, ¿cuantos elementos de orden finito tiene?

Solución:
Uno, la identidad.

Problema 19. Enlista los subgrupos ciclicos de $U(30)$.

Solución:

$$U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$$

$$\begin{aligned}
\langle 1\rangle &= \{1, 7, 19, 13\}\\
\langle 7\rangle &= \{1, 11\}\\
\langle 13\rangle &= \{1, 13, 19, 7\}\\
\langle 17\rangle &= \{1, 17, 19, 23\}\\
\langle 19\rangle &= \{1, 19\}\\
\langle 23\rangle &= \{1, 23, 19, 17\}\\
\langle 29\rangle &= \{1, 29\}
\end{aligned}$$

Problema 22. Demuestra que un grupo de orden 3 debe ser ciclico.

Solución:
Sea $G = \{e, a, b\}$. ab debe estar en G. ab no puede ser a o b porque implicaria que $a = e$ o $b = e$. Por tanto, $ab = e$ y $b = a^{-1}$, dejando el grupo como $\{e, a, a^{-1}\}$, un grupo ciclico.

Problema 24. Para cada elemento a en cualquier grupo G, demuestra que $\langle a\rangle$ es un subgrupo de $C(a)$.

Solución:
Dado que $\langle a\rangle$ se compone de los elementos de la forma a^n entonces $a \cdot a^n = a^{1+n}$ $= a^{n+1} = a^n \cdot a$ por lo que a^n està en el centrizador de a y como fue elegido al azar $< a > \subset C(a)$ y como ambos estàn en G entonces es un subgrupo de $C(a)$.

Problema 26. Encuentra todos los generadores de Z. Sea a un elemento de grupo con orden infinito. Encuentra todos los generadores de $\langle a\rangle$.

Solución:
Los generadores de Z son $\{-1, 1\}$.

Si $a \in G$ y $|a| = \infty$, entonces los generadores de a son $\{a^{-1}, a^1\}$.

Problema 29. Enlista los elementos de orden 8 en $Z_{8000000}$. ¿Como sabes que tu lista esta completa? Sea a un elemento del grupo tal que $|a| = 8000000$. Enlista todos los elementos de orden 8 en $\langle a \rangle$.

Solución:
Por el teorema 4.3, sabemos que $\langle 1000000 \rangle$ es el unico subgrupo de orden 8, asi que sus elementos son los unicos de orden 8: 1000000, 2000000, 3000000, 4000000, 5000000, 6000000, 7000000.

Problema 30. Supón que a y b pertenecen a un grupo, a tiene orden impar y $aba^-1 = b^{-1}$. Demuestra que $b^2 = e$.

$$\begin{aligned} aba^{-1} &= b^{-1} \\ ab &= b^{-1}a \\ baba^{-1} &= e \\ a &= baba \\ a^{-1} &= b^{-2}a^{-2} \\ a &= b^{-2} \\ ab &= b^{-1} \\ a &= e \\ b &= e = b^2 \end{aligned}$$

Problema 31. Sea G un grupo finito. Muestra que existe un numero fijo de enteros positivos n tales que $a^n = e$ para todo a en G.

Solución:
G es $\{e, a_1, a_2, \ldots, a_k\}$, entonces $|a_i| = n_i$. Para encontrar la n general calculamos $n = lcm(n_1, n_2, \ldots, n_k)$. Ahora $a^n = a^{kn} = e$, $\forall a \in G$.

Problema 34. Determine la cuadricula de subgrupos para Z_8

Solución:
Orden 8: $\langle 1 \rangle = 0, 1, 2, 3, 4, 5, 6, 7$

Orden 4: $\langle 2 \rangle = 0, 2, 4, 6$

Orden 2: $\langle 4 \rangle = 0, 4$

Orden 1: $\langle 8 \rangle = 0$

Problema 36. Demuestra que un grupo finito es la union de subgrupos propios si y solo si el grupo no es ciclico.

Solución:
Supongamos que el grupo es la union de grupos propios. Si $G = \langle a \rangle$, entonces a pertenece a algun subgrupo propio H_i de G y por tanto $\langle a \rangle = G$ debe ser un subgrupo de H_i, lo cual es una contradicción.

Por otro lado, asumimos que G no es ciclico. Tomamos un elemento a cualquiera de G. Como G no es ciclico, $\langle a \rangle$ es un subgrupo propio de G. Podemos repetir este proceso para todos los elementos a y al unir estos subgrupos propios obtenemos todo G.

Problema 37. Demuestra que el grupo de numeros enteros racionales bajo la multiplicación no es ciclica.

Solución:
Supongamos que existe un generador para el grupo, y ese es de la forma $\frac{a}{b}$. Para que este sea generador, debe generar todo el grupo a partir de potencias, lo cual sería imposible en el grupo de los racionales positivos, ya que una fracción de la forma $\frac{a}{b}^n$ va a tender hacia infinito o hacia 0, pero todo con una tendencia muy marcada. Es decir, siempre sus potencias van a ser múltiplos de este o de su inverso.

Problema 38. Considera el conjunto $\{4, 8, 12, 16\}$. Demuestra que este conjunto es un grupo bajo la multiplicación modulo 20 construyendo su tabla de Cayley. ¿Cual es el elemento identidad? ¿El grupo es ciclico? Si lo es, encuentra los generadores.

Solución:

	4	8	12	16
4	16	12	8	4
8	12	4	16	8
12	8	16	4	12
16	4	8	12	16

La identidad es 16. El grupo es ciclico pues $\langle 8, 12 \rangle = \{4, 8, 12, 16\}$

Problema 40. Sean m y n elementos del grupo Z. Encuentra los generadores del grupo $\langle m \rangle \cap \langle n \rangle$.

Solución:
$m, n \in Z$.

Suponiendo que $\langle m\rangle \cap \langle n\rangle = \langle lcm(m,n)\rangle$

$\langle m\rangle \cap \langle n\rangle \leq Z \Rightarrow \langle m\rangle \cap \langle n\rangle = \langle k\rangle$ para alguna $k \in Z$
$\Rightarrow k = m \cdot k_1$, y $k = n \cdot k_2$ para alguna $k_1, k_2 \in Z$
$\Rightarrow lcm(m,n)$ divide a k
Sea $lcm(m,n) \in \langle m\rangle \cap \langle n\rangle$, y desde que m, n divide a $lcm(m,n)$
$\rightarrow lcm(m,n) \in \langle k\rangle$
$\rightarrow lcm(m,n) = k \cdot q$ para alguna $q \in Z$
$\rightarrow k$ divide a $lcm(m,n)$
Entonces $k = lcm(m,n)$ y esto es que $\langle m\rangle \cap \langle n\rangle = \langle lcm(m,n)\rangle$.

Problema 41. Suponga que a y b son elementos de grupo que conmutan y tienen ordenes m y n. Si $\langle a\rangle \cap \langle b\rangle = e$, demuestra que el grupo contiene un elemento cuyo orden es al menos el minimo comun multiplo de m y n. Demuestra que esto no necesita ser verdad si a y b no conmutan.

Solución:
Suppose that a and b are group elements that commute and have orders m and n. If $\langle a\rangle \cap \langle b\rangle = e$, prove that the group contains an element whose order is the least common multiple of m and n. Show that this need not be true if a and b do not commute.

De la hipotesis, el orden de ab es lcm(m, n).

Si consideramos $|ab| = r$ entonces:

$$\begin{aligned} (ab)^r &= a^r b^r = e \\ a^r &= b^{-r} \in \langle b\rangle \\ a^r \in \langle a\rangle \cap \langle b\rangle &= e \\ a^r &= e \\ b^r &= e \end{aligned}$$

Por estos resultados, $m|r$ y $n|r$ y por lo tanto $lcm(m,n)|r$, y en particular, $r \geq lcm(m,n)$

Ahora consideremos $q = lcm(m,n)$. Por lo tanto q se puede descomponer en mq_1 y nq_2 para q_1, q_2 positivos.

Revisitando una de las formulas anteriores tenemos:

$$\begin{aligned} (ab)^q &= a^q b^q \\ a^q b^q &= a^{mq_1} b^{nq_2} \\ a^{mq_1} b^{nq_2} &= (a^m)^{q_1} (b^n)^{q_2} \\ (a^m)^{q_1} (b^n)^{q_2} &= e^{q_1} e^{q_2} = e \end{aligned}$$

Asi que $r = |ab| \leq q = lcm(m, n)$. Por lo tanto $r = lcm(m, n)$.

Ahora veamos el caso en el que a y b no conmutan. En este caso, no necesariamente existe r que cumpla lo que se quiere y se puede ver con un ejemplo. Veamos el caso de S_3. Si $a = (12)$ y $b = (123)$ entonces $|a| = 2$ y $|b| = 3$ pero porque S_3 no es abeliano, no es un grupo ciclico y no existe un elemento de grado $lcm(2, 3) = 6$.

Problema 43. Sea p un primo. Si un grupo tiene mas de $p - 1$ elementos de orden p, ¿Por qué el grupo no puede ser ciclico?

Solución:
Supongamos un grupo ciclico finito. Si tenemos un subgrupo de orden p, este tendra $\phi(p) = p - 1$ elementos de orden p por el teorema 4.4. Si existiera otro elemento de orden p, tendria que existir otro subgrupo de orden p, lo cual contradice la propiedad de los subgrupos finitos establecida en el teorema 4.3.

Problema 45. Enlista todos los elementos de Z_{40} de orden 10. Sea $|x| = 40$. Enlista todos los elementos de x que tienen orden 10.

Solución:

1. Los de orden 10 en $Z_{40} = \{4, 12, 28, 36\}$
   Obtenidos a partir de la fórmula $|a| = \frac{n}{mcd(n,k)}$ se seleccionan aquellos números en Z_{40} tales que $mcd(40, x) = 4$ desde 0 a 39.
2. Los de orden 10 en $< x > = \{1, 3, 7, 9\}$ donde $|x| = 10$
   Similar al anterior pero ahora se seleccionan sólo aquellos $mcd(10, x) = 1$ desde 0 a 9

Problema 47. Determina los ordenes de los elementos de D_{33} y cuantos hay de cada uno.

Solución:
D_{33} tiene 33 ejes de simetria que forman 33 permutaciones de orden 2. Tambien hay 33 rotationes, los cuales forman un grupo ciclico. Sabemos que por cada divisor d de 33 tenemos $\phi(d)$ rotaciones de orden d en el grupo. Asi obtenemos $\phi(1) = 1$ elemento de orden 1, $\phi(3) = 2$ elementos de orden 3, $\phi(11) = 10$ elementos de orden 11 y $\phi(33) = 20$ elementos de orden 33.

Problema 50. Si G es un grupo Abeliano y contiene subgrupos ciclicos de ordenes 4 y 6, ¿Qué otros tamaños de subgrupos ciclicos estan contenidos en G? Generalice.

Solución:
Tomamos dos grupos ciclicos $|\langle a \rangle| = 4$ y $|\langle b \rangle| = 6$. Sabemos que $(a^4)^3(b^6)^2 =$

$ee = e$, asi que sabemos que 12 divide a $|ab|$. Tambien sabemos que $(ab)^4 = a^4 = e$, por lo tanto, $|ab| \neq 1, 2$ o 4. Conversamente, vemos que $(ab)^6 = a^6 \neq e$, asi que $|ab| \neq 1, 2, 3, 6$. Por tanto, debe en existir subgrupos de orden $1, 2, 3, 4, 6$ y 12.

Problema 54. Sean a y b en un grupo. Si $|a|$ y $|b|$ son primos relativos, demuestra que $\langle a \rangle \cap \langle b \rangle = \{e\}$

Solución:
Sea $a, b \in G$

Suponiendo que $\langle a \rangle \cap \langle b \rangle \leq \langle a \rangle$ y $\langle a \rangle \cap \langle b \rangle \leq \langle b \rangle$.

Si $x \in \langle a \rangle \cap \langle b \rangle$
entonces $|x||a|$ y $|x||b|$,
$|x| = \gcd(|a|, |b|)$.
$|x| = 1$ porque $gcd(|a|, |b|) = 1$
$\{x\} = \{e\}$.
$\langle a \rangle \cap \langle b \rangle = \{e\}$

Problema 57. Supón que un grupo G tiene al menos nueve elmentos x tales que $x^8 = e$. ¿Puedes concluir que G no es ciclico? ¿Y si G tiene al menos cinco elementos x tales que $x^4 = e$? Generalice.

Solución:
Sabemos que $|x|$ divide a 8. Si G fuese ciclico, entonces habria exactamente $\phi(8) + \phi(4) + \phi(2) + \phi(1) = 4 + 2 + 1 + 1 = 8$ elementos con ordenes que dividan a 8 en G, asi que G no es ciclico. Igual en el otro caso, habria $\phi(4) + \phi(2) + \phi(1) = 2 + 1 + 1 = 4$ elementos con ordenes que dividan a 4, por lo que G tampoco seria ciclico.

Problema 61. Supon que a es un elemento de grupo tal que $|a^{28}| = 10$ y $|a^{22}| = 20$. Determine $|a|$.

Solución:
$|a^{28}| = 10 \Rightarrow a^{280} = e$
$|a^{22}| = 20 \Rightarrow a^{440} = e$

$|a|$ divide a 280 y $|a|$ divide a 440.
$|a|$ divide a $\gcd(280, 440)$.
$|a|$ divide a 40.
$|a| = 40$.

Problema 64. Demuestre que $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} | n \in Z \right\}$ es un subgrupo ciclico

de $GL(2, R)$

Solución:
Observamos que $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n$, que pertenece a $GL(2, R)$, por lo que H es un subgrupo de este.

Problema 68. Sean r_1 y r_2 numeros racionales. Demuestre que el grupo $G = \{n_1 r_1 + n_2 r_2 | n_1, n_2 \in Z\}$ bajo la suma es ciclico. Generalice al caso donde tienes r_1, r_2, ..., r_k rationals.

Problema 71. Demuestra que para cualquier primo p y entero positivo n, $\phi(p^n) = p^n - p^{n-1}$.