Tercera serie de ejercicios de Álgebra Moderna

Akiyuki Shinbou

Mayo 2018

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

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 $\{c^1, c^3, c^5, c^7, c^{11}, c^{13}, c^{17}, c^{19}\}$

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

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

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

Solución:

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

$$\begin{aligned}
&3^1 = 3 \\
&3^2 = 9 \\
&3^3 = 27 \mod 20 = 7 \\
&3^4 = 7 \cdot 3 \mod 20 = 1 \\
&3^5 = 3 \cdot 1 \\
&\langle 3 \rangle = \{3, 7, 9, 1\}
\end{aligned}$$

$$\begin{aligned}
&7^1 = 7 \\
&7^2 = 49 \mod 20 = 9 \\
&7^3 = 9 \cdot 7 \mod 20 = 3 \\
&7^4 = 3 \cdot 7 \mod 20 = 1 \\
&\langle 7 \rangle = \{1, 3, 7, 9\}
\end{aligned}$$

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

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.

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.

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

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

$$< a > = \{e, a, a^2, ..., a^{23}\}$$

Subgrupo de orden 8

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

Generadores

$$< a^3 > = \{a^3, a^9, a^{15}, a^{21}\}$$

Obtenidos de la misma forma que el inciso anterior

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.

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.

28. 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.

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.

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.

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.

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.

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.

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

Solución:
Los numeros menores y no relativamente primos a p^n son los multiplos de p: $p, 2p, p^{n-1}p$. Hay p^{n-1} de estos numeros, y p^n numeros enteros positivos menores o iguales a p^n, llevando el numero de primos relativos a p^n a $p^n - p^{n-1}$.