Actividad II

David Fernando Armendáriz Torres[1], Daniela Márquez Campos[2], Julio Eugenio Guevara Galván[3], and Karla Andrea Palma Villanueva[4]

[1]A01570813
[2]A00833345
[3]A01704733
[4]A01754270

Abril 2024

Resuelve los siguientes problemas. La tarea deberá ser entregada en hojas blancas (digitalizadas en un solo archivo pdf). No se aceptarán tareas en hojas de libreta o de algún otro tipo de cuaderno. Trabajen con limpieza y hagan procedimientos legibles y claros, argumentando cada paso en su solución. No entreguen la tarea con portada, pero especifiquen bien sus nombres, matrícula, número de equipo, y el número de la tarea que están entregando; escriban estos datos en la parte superior de la primera hoja. Si desean entregar un documento en formato pdf generado con Latex, esto también está permitido.

1. Prueba que un grupo G es Abeliano si y solo si $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.
   Asumiendo que G es Abeliano, se quiere probar que $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$, partiendo de $(a \cdot b)^n$:

$$
\begin{aligned}
(a \cdot b)^n &= (a \cdot b)(a \cdot b)(a \cdot b) \dots (a \cdot b) && (1)\\
&= (a \cdot a \cdot a \cdot \dots a) \cdot (b \cdot b \cdot b \cdot \dots b) && (2)\\
&= (a)^n \cdot (b)^n && (3)\\
(a \cdot b)^n &= a^n \cdot b^n && (4)\\
& && (5)\\
&\therefore n = -1 \Rightarrow (a \cdot b)^{-1} = a^{-1} \cdot b^{-1} && (6)
\end{aligned}
$$

   Ahora, asumiendo que $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$ se busca probar que G es

Abeliano:

$$(a \cdot b)^{-1} = a^{-1} \cdot b^{-1} \tag{7}$$
$$(a \cdot b)(a \cdot b)^{-1} = (a \cdot b)(a^{-1} \cdot b^{-1}) \tag{8}$$
$$e = a \cdot b \cdot a^{-1} \cdot b^{-1} \tag{9}$$
$$e \cdot b = a \cdot b \cdot a^{-1} \cdot b^{-1} b \tag{10}$$
$$e \cdot b = a \cdot b \cdot a^{-1} e \tag{11}$$
$$b \cdot a = a \cdot b \cdot a^{-1} a \tag{12}$$
$$b \cdot a = a \cdot b \cdot e \tag{13}$$
$$b \cdot a = a \cdot b \tag{14}$$

Dado lo planteado anteriormente, se comprueba que G es Abeliano si y solo si $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

2. Para cualquier grupo G, prueba que para todo $a, b \in G$ se tiene que $|ab| = |ba|$. Explica por qué esto prueba que $|abab| = |baba|$. Además, ¿es verdad que $|aba| = |bab|$?
$|ab| \to (ab)^n = e$, de manera similar, $|ba| \to (ba)^m = e$. Expandiendo la primera expresión utilizando propiedades de grupos, entre ellas zapatos y medias, se puede obtener la segunda expresión.

$$(ab)^n = (ab)(ab)(ab)\dots(ab) \tag{15}$$
$$= a(ba)(ba)(ba)\dots b \tag{16}$$
$$= a(ba)^{n-1} b \tag{17}$$
$$= a(ba)^n (ba)^{-1} b \tag{18}$$
$$= a(ba)^n a^{-1} b^{-1} b \tag{19}$$
$$= a(ba)^n a^{-1} e \tag{20}$$
$$a^{-1} e = a^{-1} a (ba)^n a^{-1} \tag{21}$$
$$a^{-1} e = e(ba)^n a^{-1} \tag{22}$$
$$a^{-1} a = (ba)^n a^{-1} a \tag{23}$$
$$e = (ba)^n e \tag{24}$$
$$(ab)^n = (ba)^n \tag{25}$$
$$\therefore |ab| = |ba| \tag{26}$$

Para el segundo caso, se tiene $|abab| = (abab)^n$ y $|baba| = (baba)^m$ lo cual se puede reescribir como $(ab)^{2n}$ y $(ba)^{2m}$ respectivamente, si se toma $k = 2n$ se tiene $(ab)^k$ cuya demostración es análoga a la anterior.

Por ultimo, ya que $|aba|$ y $|bab|$ cuentan con cantidades diferentes de elementos a y b, no se puede aplicar apropiadamente la propiedad conmutativa como en las demostraciones anteriores y por ende no se puede afirmar que $\forall a, b \in G, |aba| = |bab|$.

3. Si H y K son subgrupos de G, demuestra que $H \cap K$ también es un subgrupo de G.
   Recordando las propiedades de los grupos, tenemos que contienen a la identidad, el resultado de operar a cualquier par posible de elementos y el inverso de cada elemento. Corroboramos para $H \cap K$:

   (a) Dado que H es un grupo, contiene a la identidad, e igual para K, por lo que $H \cap K$ contiene a la identidad.

   (b) Ya que H es un grupo, el resultado de operar dos elementos de éste también será un elemento del grupo, de modo que $H = \{e, h_1, h_2, h_1 \cdot h_2, \dots\}$, por lo que en caso de que h_1 y h_2 sean elementos de G, $h_1 \cdot h_2$ también lo es, debido a que se definió que G es un grupo, y al mismo tiempo, h_1, h_2 y $h_1 \cdot h_2$ serán elementos de $H \cap K$ para todo h_1, h_2. En cambio, si h_1, h_2 son elementos de H y no de K –o viceversa–, ninguno de los dos estará en $H \cap K$.

   (c) Ya que H es un grupo, el inverso de cualquiera de sus elementos será también elemento de H, de modo que $H = \{e, h_1, h_1^{-1}, \dots\}$. Por lo que si h_1 es elemento de K, también lo será h_1^{-1}, ya que K también es un grupo. Por el otro lado, si h_1 no es elemento de K, tampoco lo será de $H \cap K$.

   Con lo cual, aunado a que por definición, todos los elementos de H y K son elementos de G –y por lo tanto pasa lo mismo para $H \cap K$–, se cumple el último requisito para que $H \cap K$ sea un subgrupo de G.

4. Encuentra un grupo que no sea cíclico, pero cuyos subgrupos sí lo sean.
   Como se verá a continuación, $U(8)$ no es cíclico, pero sus subgrupos sí lo son.
   Los subgrupos de $U(8)$ son:

$$\{1\} \tag{27}$$
$$\{1, 3\} \tag{28}$$
$$\{1, 5\} \tag{29}$$
$$\{1, 7\} \tag{30}$$

   Estos cumplen que son subgrupos ya que contienen la identidad, el resultado de la operación entre cada par posible de elementos y el inverso de cada elemento gracias a que el orden de todos es igual a 2–a excepción del subgrupo trivial, sin embargo, éste siempre es cíclico por contener un sólo elemento–, lo cual también implica que los subgrupos contienen elementos con orden igual al orden del subgrupo, por lo que son cíclicos.

5. Prueba que $U(2^n)$ no es cíclico si $n \geq 3$.
   Asumiendo que el grupo es cíclico, se tiene que hay exactamente un elemento de orden 2, dado que $\phi(2) = 1$, y en un grupo cíclico de orden n el número de elementos de orden d sólo depende de d. Sin embargo,

definiendo un elemento $u \in U(2^n)$, se tiene que $u^2 \equiv 1 \mod 2^n$, por lo que $(-u)^2 \equiv 1 \mod 2^n$ dado que $u^2 = (-u)^2$. Este último se interpreta como $2^n - u$ para este grupo.
Propongamos el siguiente número, que es elemento de $U(2^n)$ para cualquier $n \geq 3$:

$$\frac{2^n}{2} + 1 = 2^{n-1} + 1 \tag{31}$$

Ya que es impar y es menor que 2^n. Para que su orden sea igual a 2 se debe cumplir que su cuadrado es congruente con $1 \mod 2^n$, por lo que calculamos dicho cuadrado.

$$(2^{n-1} + 1)^2 = (2^{n-1})^2 + 2(2^{n-1}) + 1 \tag{32}$$
$$= 2^{2n-2} + 2^n + 1 \tag{33}$$
$$= 2^n(2^{n-2} + 1) + 1 \tag{34}$$

Como se puede observar, este número es efectivamente congruente con 1 mod 2^n. Esto se debe a que 2^n siempre divide a 2^{2n-2}, dado que para todo $n \in \mathbb{Z}^+$ mayor o igual a 3, se cumple que $2n - 2 > n$; 2^n divide a 2^n; y queda como único residuo el tercer término, es decir, 1. Por lo que

$$2^n(2^{n-2} + 1) + 1 \equiv 1 \mod 2^n \tag{35}$$

Ahora bien, su negativo sería $2^n - (2^{n-1} + 1) = 2^n - 2^{n-1} - 1$. Con esto se observa que es estrictamente menor a 2^n, positivo –ya que $2^n \geq 2^{n-1} - 1$ para todo n entero positivo–, impar y entero para todo n entero positivo igual o mayor a 3, por lo que es efectivamente un elemento de $U(2^n)$. Finalmente, para comprobar que sea congruente con $1 \mod 2^n$, expandimos.

$$(2^n - 2^{n-1} - 1)^2 = 2^n - 2^{n+1} + 2^{2n-2} + 1 \tag{36}$$
$$= 2^n(2^{n-2} - 2^1 + 1) + 1 \tag{37}$$
$$= 2^n(2^{n-2} - 1) + 1 \tag{38}$$

Por lo que

$$2^n(2^{n-2} - 1) + 1 \equiv 1 \mod 2^n \tag{39}$$

Con esto, se confirma el último requisito y por lo tanto hemos comprobado que para toda n igual o mayor a 3, $U(2^n)$ tiene al menos un par de elementos de orden 2, por lo que $U(2^n)$ no es cíclico.

6. ¿Cuál es el entero positivo n más pequeño para el cual S_n tiene un elemento de orden igual a 30?
También gracias al teorema X, podemos hallar el mayor orden posible de

un elemento de S_n, ya que éste se da cuando se maximiza el mínimo común múltiplo entre las longitudes de sus ciclos disyuntivos. Con esto en mente, comenzamos obteniendo los factores primos de 30 –que son $\{2, 3, 5\}$–, ya que este conjunto es el que minimiza la suma de sus elementos mientras mantiene el mínimo común múltiplo igual a 30. Con esto obtenemos que el entero positivo n más pequeño para el cual S_n tiene un elemento de orden igual a 30 es **n=10**, o bien, la suma de los factores primos 30. Es decir, los elementos de S_{10} con orden 30, son aquellos de la forma [2][3][5].

7. Sea $\alpha = (123)(145)$. Obtén la versión de ciclos disyuntos de α y calcula α^{99}.
   Comenzamos por obtener los ciclos disyuntivos de α:

$$(145)(123) \tag{40}$$
$$1 \overset{(145)}{\to} 4 \overset{(123)}{\to} 4 \tag{41}$$
$$4 \overset{(145)}{\to} 5 \overset{(123)}{\to} 5 \tag{42}$$
$$5 \overset{(145)}{\to} 1 \overset{(123)}{\to} 2 \tag{43}$$
$$2 \overset{(145)}{\to} 2 \overset{(123)}{\to} 3 \tag{44}$$
$$3 \overset{(145)}{\to} 3 \overset{(123)}{\to} 1 \tag{45}$$
$$\alpha = (1,4,5,2,3) \tag{46}$$

   Ahora bien, para calcular α^{99}, observamos que de acuerdo al resultado previo y el teorema X, $|\alpha| = 5$, por lo que reescribimos:

$$\alpha^{99} = (\alpha^5)^{19} \cdot \alpha^4 \tag{47}$$
$$\alpha^{99} = e^{19} \cdot \alpha^4 = \alpha^4 \tag{48}$$

   Por lo que, calculando α^4, obtenemos que:

$$\alpha^{99} = (3, 5, 2, 1, 4) \tag{49}$$

8. Para cualquier grupo G y cualquier automorfismo $\phi : G \to G$, demuestra que para todo $a \in G, |a| = |\phi(a)|$.

   Partiendo de la suposición de que $|a| = n$, se tiene que $a^n = e$ de lo cual se obtiene $\phi(a^n) = \phi(e) = e$ dadas las propiedades de isomorfismos ($\phi : G \to H, e_G \in G \Rightarrow \phi(e_G) = e_H \in H$) y automorfismos ($\phi : G \to H = G$). Nuevamente, dado el automorfismo, se tiene que $\forall n, \quad \forall a \in G, \quad \phi(a^n) = (\phi(a))^n$. Dado lo planteado se obtiene $\phi(a)^n = e$ y por ende $|\phi(a)| = n = |a|$.

9. Asume que $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_{20}$ es un automorfismo y $\phi(5) = 5$. ¿A qué puede ser igual $\phi(x)$? ¿Son estas posibilidades isomórficas a algún subgrupo de $U(20)$? Si es así, ¿cuál sería ese subgrupo?

Se puede proponer $\phi(x) = 9x$ como el automorfismo, ya que es biyectiva, la identidad se mantiene como la identidad, y va de $\mathbb{Z}_{20}$ a sí misma. Ahora bien, todo grupo cíclico finito G es isomórfico con $\mathbb{Z}$ ya que se puede establecer la función biyectiva $a^k \to k \mod n$, donde a es un generador de G y $K \in \mathbb{Z}_n$. Con vista en esto se tiene que los subgrupos de $U(20)$ isomórficos a $\mathbb{Z}_{20}$ son:

(a) El generado por 1: $\{1\}$

(b) El generado por 3 o 7: $\{1, 3, 9, 7\}$

(c) El generado por 9: $\{1, 9\}$

(d) El generado por 11: $\{1, 11\}$

(e) El generado por 13: $\{1, 13, 9, 7\}$

(f) El generado por 17: $\{1, 17, 9, 13\}$

(g) El generado por 19: $\{1, 19\}$