

Estructuras Algebraicas: Taller 1

Universidad Nacional de Colombia

Edgar Santiago Ochoa Quiroga

Problema 1:

Las clases de conjugación de S_n corresponden a particiones de n , dadas por la longitud de los ciclos. Determine el tamaño de la clase de conjugación de en S_n que corresponde a una partición dada $n = \sum jm_j$. (m_1 elementos fijos, m_2 2-ciclos, m_3 3-ciclos. . .)

Solución:

Como el tamaño de la clase de conjugación corresponde a la partición particular de n que define el tipo de ciclo. entonces basta con ver de cuantas maneras se puede escribir ese ciclo en particular para determinar el tamaño de la clase de conjugación. Primero es claro que en los ciclos independientemente de su distribución podemos asegurar que hay $n!$ maneras de colocar los elementos de $\{1, 2, 3, \dots, n\}$. Ahora hay que ver cuantas maneras repetidas tenemos que descontar. Fijemos un tipo de ciclo específico en el cual hay una cantidad m_1 de 1-ciclos, m_2 de 2-ciclos y así sucesivamente. Observe que en un j -ciclo específico se puede escribir de j maneras diferentes desplazando los elementos una posición sin alterar su orden para cada j -ciclo, y como hay una cantidad m_j de esos ciclos, se obtiene que de momento hay j^{m_j} casos repetidos, pero falta tener en cuenta una cosa, note que los j -ciclos como hay una cantidad m_j de ellos puedo permutarlos sin alterar la permutación, entonces habrían $m_j!$ maneras de permutarlos y junto con lo anterior para un tipo de ciclo específico tendríamos que hay $m_j!j^{m_j}$ maneras distintas de escribirlo sin alterar la permutación. Luego como esto es para cada j -ciclo pues basta con multiplicar todos estos y dividir esta cantidad a $n!$. Así obtenemos que el tamaño de una clase de conjugación correspondiente a una partición es:

$$\frac{n!}{(m_1!1^{m_1})(m_2!2^{m_2}) \dots (m_n!n^{m_n})}$$

Note que en los casos que hay 0 ciclos de algún j -ciclo específico ese termino en particular se hace 1 y no afecta el resultado.

□□

Problema 2:

Pruebe que A_n es generado por 3-ciclos. Usando este hecho pruebe que A_n es simple.

Solución:

Primero probemos que A_n es generado por 3-ciclos para $n \geq 3$.

Sea X el conjunto de todos los 3-ciclos y sea $\sigma = (a, b, c)$ con $a, b, c \in \{1, 2, 3, \dots, n\}$, es claro que $(a, b, c) = (a, c)(a, b)$ por tanto $\sigma \in A_n$ y como este era arbitrario $\langle X \rangle \subseteq A_n$. Ahora sea $\sigma \in A_n$, por definición σ se puede escribir como un numero par de trasposiciones, es decir $\sigma = \tau_1 \tau_2 \dots \tau_k$ con k par y donde cada $\tau_i = (a_1, a_2)$ con $a_1, a_2 \in \{1, 2, 3, \dots, n\}$ y $a_1 \neq a_2$, note que podemos agrupar trasposiciones dos a dos. Veamos que el producto de 2 trasposiciones puede ser visto como el producto de 3-ciclos. Sean (a, b) y (c, d) dos trasposiciones tenemos dos casos posibles:

- Caso 1: $\{a, b\} \cap \{c, d\} = \emptyset$, es decir son ciclos disjuntos y por tanto tenemos que:

$$\begin{aligned} (a, b)(c, d) &= (a, b)id(c, d) \\ &= (a, b)[(b, c)(b, c)](c, d) \\ &= (a, b)(b, c)(c, d, b) \\ &= (a, b, c)(c, d, b) \end{aligned}$$

- Caso 2: $\{a, b\} \cap \{c, d\} \neq \emptyset$, es decir coinciden en algunos elementos, o en todos, veamos que posibilidades hay.

La primera es que $\{a, b\} = \{c, d\}$, es decir $(a, b) = (c, d)$ y por tanto:

$$(a, b)(c, d) = (a, b)(a, b) = id = (a, b, r)(a, b, r)(a, b, r)$$

donde r es un elemento distinto a a, b , note que esto lo podemos asegurar ya que $n \geq 3$.

Ahora como segundo caso consideremos que $a = c$ pero $b \neq d$, por tanto tenemos que:

$$(a, b)(c, d) = (a, b)(a, d) = (a, d, b)$$

Por ultimo tendríamos el caso $a = d$ y $b \neq c$ que es análogo al anterior:

$$(a, b)(c, d) = (a, b)(c, a) = (a, c, b)$$

De esta forma concluimos que cualquier producto dos a dos de trasposiciones es un producto de 3-ciclos, luego σ es un producto de tres ciclos, por lo tanto $\sigma \in \langle X \rangle$ y $A_n \subseteq \langle X \rangle$. Por la doble contención concluimos que A_n es generado por los 3-ciclos. Ahora debemos mostrar que si $N \trianglelefteq A_n$, para $n \geq 5$ y N contiene un 3-ciclo, entonces $N = A_n$. Para esto primero demostremos que todos los 3-ciclos son conjugados en S_n , por medio de la identidad $f(a, b, c)f^{-1} = (f(a), f(b), f(c))$. Sea (a, b, c) un 3-ciclo arbitrario y sea $f \in S_n$ una permutación arbitraria. Ahora como f puede ser escrita como producto de trasposiciones basta con ver que pasa en el caso de que f sea un ciclo de la forma (α, β) y nuevamente consideraremos dos casos:

- Caso 1: $\{\alpha, \beta\} \cap \{a, b, c\} = \emptyset$, quiere decir que son disyuntos y por tanto conmutan los ciclos:

$$(\alpha, \beta)(a, b, c)(\alpha, \beta) = (a, b, c)(\alpha, \beta)(\alpha, \beta) = (a, b, c)$$

Note que podemos ver $(a, b, c) = (f(a), f(b), f(c))$ ya que f no mueve estos elementos.

- Caso 2: $\{\alpha, \beta\} \cap \{a, b, c\} \neq \emptyset$, y tenemos dos casos, el primero suponga que $\alpha, \beta \in \{a, b, c\}$ y que $\alpha = a$ y $\beta = b$, tenemos que:

$$(\alpha, \beta)(a, b, c)(\alpha, \beta) = (a, b)(a, b, c)(a, b) = (b, a, c) = (f(a), f(b), f(c))$$

y en caso de que $\alpha = a$ y $\beta = c$:

$$(\alpha, \beta)(a, b, c)(\alpha, \beta) = (a, c)(a, b, c)(a, c) = (c, b, a) = (f(a), f(b), f(c))$$

Esto agota las posibilidades y por tanto muestra que los 3-ciclos son conjugados en S_n . Ahora para probar esto en A_n basta con ver que la permutación f siempre la podemos tomar par. Si f es par no hay nada que probar. Consideremos f impar, como $n \geq 5$ existen i, j diferentes a a, b, c y por tanto sus ciclos conmutaran, luego planteemos que la permutación par que conjuga es $\pi = f(i, j)$, de esta manera:

$$(f(i, j))(a, b, c)(f(i, j))^{-1} = f(i, j)(a, b, c)(i, j)f^{-1} = f(a, b, c)(i, j)(i, j)f^{-1} = f(a, b, c)f^{-1}$$

y que por lo anterior podemos concluir que todos los 3-ciclos son conjugados en A_n para $n \geq 5$. Ahora volvamos a lo que realmente nos interesaba probar. Como N contiene un 3-ciclo y es normal, los conjugados de ese 3-ciclo pertenecen a N , es decir N contiene todos los 3-ciclos y como A_n es generado por estos no queda de otra que $N = A_n$.

Con todo esto ya podemos probar lo que nos interesa, A_n es simple para todo $n \geq 5$. Sea $N \trianglelefteq A_n$ y supongamos que $N \neq \{id\}$, es decir hay un $\tau \in N$ distinto a la identidad. Vamos a mostrar que la existencia de tal elemento implica que en N hay un 3-ciclo y por tanto que es todo A_n , esto sera por casos:

- Caso 1: En la descomposición en ciclos disyuntos de τ hay al menos un r -ciclo con $r \geq 4$, es decir $\tau = (a_1, a_2, a_3, a_4, \dots, a_r) \cdots$ donde los puntos suspensivos indican la existencia de otros ciclos. Consideremos $\sigma = (a_1, a_2, a_3) \in A_n$ como N es un subgrupo normal $\sigma\tau\sigma^{-1}\tau^{-1} \in N$ pero note que esto es:

$$\begin{aligned} \sigma\tau\sigma^{-1}\tau^{-1} &= (a_1, a_2, a_3)(a_1, a_2, a_3, a_4, \dots, a_r) \cdots (a_3, a_2, a_1) \cdots (a_r, \dots, a_4, a_3, a_2, a_1) \\ &= (a_1, a_2, a_4) \in N \end{aligned}$$

De esta manera N contiene un 3-ciclo y por lo anterior $N = A_n$

- Caso 2: τ contiene al menos un 3-ciclo y los demás son de longitud menor o igual a 3. Es decir $\tau = (a_1, a_2, a_3)(a_4, a_5, \dots) \dots$, y consideremos $\sigma = (a_1, a_2, a_4) \in A_n$ igual que en el anterior $\sigma\tau\sigma^{-1}\tau^{-1} \in N$ y:

$$\begin{aligned}\sigma\tau\sigma^{-1}\tau^{-1} &= (a_1, a_2, a_4)(a_1, a_2, a_3)(a_4, a_5, \dots) \dots (a_4, a_2, a_1) \dots (\dots, a_5, a_4)(a_3, a_2, a_1) \\ &= (a_1, a_2, a_5, a_3, a_4) \in N\end{aligned}$$

y por el Caso 1, tenemos que hay un 3-ciclo en N y nuevamente concluimos que $N = A_n$

- Caso 3: τ es exactamente un 3-ciclo y por tanto no hay nada que probar ya que N ya tendría un 3-ciclo y por tanto $N = A_n$
- Caso 4: En τ todos los ciclos son de longitud menor o igual a 2, es decir $\tau = (a_1, a_2)(a_3, a_4) \dots$. Considere $\sigma = (a_1, a_2, a_3) \in A_n$, nuevamente $\sigma\tau\sigma^{-1}\tau^{-1} \in N$ y:

$$\begin{aligned}\sigma\tau\sigma^{-1}\tau^{-1} &= (a_1, a_2, a_3)(a_1, a_2)(a_3, a_4) \dots (a_3, a_2, a_1)(a_1, a_2)(a_3, a_4) \dots \\ &= (a_1, a_3)(a_2, a_4) \in N\end{aligned}$$

Ahora como $n \geq 5$ tenemos que:

$$(a_1, a_2, a_5, a_3, a_4) = (a_1, a_4)(a_1, a_3)(a_1, a_5)(a_1, a_2) \in A_n$$

y como N es normal:

$$(a_1, a_2, a_5, a_3, a_4)(a_1, a_3)(a_2, a_4)(a_4, a_3, a_5, a_2, a_1) = (a_1, a_5)(a_2, a_4) \in N$$

y por ultimo al hacer el producto de esos dos elementos de N obtenemos:

$$(a_1, a_3)(a_2, a_4)(a_1, a_5)(a_2, a_4) = (a_1, a_5, a_3) \in N$$

Por lo que hay un 3-ciclo en N y así concluimos que $N = A_n$

Como hemos agotado todas las posibilidades concluimos que A_n para $n \geq 5$ es simple. Cabe aclarar que los casos con $n = 1, 2, 3$ también determinan a A_n simple de manera trivial y que el caso $n = 4$ vimos en clase como no era simple.

□□

Problema 3:

Clasifique los grupos de orden 12.

Solución:

Primero por el Teorema de Clasificación (o estructura) de los Grupos abelianos finitos tenemos que si $|G| = 12$ y G es abeliano entonces:

$$G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12} \quad \text{ó} \quad G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_6$$

Ahora veamos que ocurre cuando G es no abeliano.

Tomemos H un 3-subgrupo de Sylow de G , es decir $H = \langle c \rangle$ para algún $c \in G$ y $|H| = 3$, Ahora definamos el siguiente homomorfismo (Generalización del teorema de Cayley presentada en los cuadernos de álgebra del profesor Lezama):

$$\varphi : G \longrightarrow \text{Sym}(G/H)$$

De tal manera que $\varphi(x) = \varphi_x$ donde:

$$\varphi_x : G/H \longrightarrow G/H$$

tal que $\varphi_x(gH) = xgH$. Observe que $|G/H| = 4$ y por tanto $\text{Sym}(G/H) \cong S_4$. Ahora note que el $\ker(\varphi) \subseteq H$ y por tanto $\ker(\varphi) = \{e\}$ o $\ker(\varphi) = H$. en el primer caso tendríamos que G es isomorfo a un subgrupo de S_4 de orden 12, llamémoslo K , Note que $[S_4 : K] = 2$ por tanto K es normal, Ya conocemos que A_4 tiene orden 12 toca ver que nuestro K es igual a A_4 . en este caso tenemos dos posibilidades K tiene un 3-ciclo o no lo tiene. Si lo tiene por el punto anterior concluimos que $K = A_4$, Ahora veamos que no es posible lo segundo. Sea $\sigma \notin K$ un 3-ciclo, Note que las clases $K, \sigma K, \sigma^{-1}K$ son distintas eso nos daría que $[S_4 : K] \geq 3$ una contradicción. Así concluimos que en este caso tenemos que $G \cong A_4$. Ahora supongamos que $\ker(\varphi) = H$, luego H es normal en G y por tanto es el único 3 subgrupo de Sylow, entonces solo hay dos elementos de orden 3, c, c^2 . Ahora como los elementos conjugados tienen el mismo orden y H es normal entonces $|O(c)| \in \{1, 2\}$, donde la orbita esta definida por la conjugación de elementos, de esto tenemos por la ecuación de clases que $|C_G(c)| \in \{6, 12\}$, pero en cualquiera de los dos casos existe un elemento d de orden 2, y como $cd = dc$, digamos que $a := cd$, note que $|a| = 6$, luego $[G : \langle a \rangle] = 2$ y por tanto $\langle a \rangle \trianglelefteq G$. Consideremos $b \in G$ tal que $b \notin \langle a \rangle$, note que $b^2 \in \langle a \rangle$, además como este es normal $bab^{-1} \in \langle a \rangle$. Observemos los posibles casos:

- $bab^{-1} = e$ por tanto $a = e$, lo cual es falso
- $bab^{-1} = a$ por tanto $ba = ab$, pero $\langle a, b \rangle$ posee 12 elementos y por tanto G seria abeliano, lo cual es falso.
- $bab^{-1} = a^2$, así $(bab^{-1})^3 = a^6 = 1$, luego $ba^3b^{-1} = 1$ y por tanto $a^3 = 1$, lo cual es falso.

- $bab^{-1} = a^3$, así $(bab^{-1})^2 = a^6 = 1$, luego $ba^2b^{-1} = 1$ y por tanto $a^2 = 1$, lo cual es falso.
- $bab^{-1} = a^4$ así $(bab^{-1})^3 = a^{12} = 1$, luego $ba^3b^{-1} = 1$ y por tanto $a^3 = 1$, lo cual es falso.
- $bab^{-1} = a^5 = a^{-1}$, como esta es la única posibilidad restante se vuelve una condición necesaria.

Ahora veamos los casos de valores para b^2 :

- $b^2 = 1$ es una posibilidad
- $b^2 = a$ implica que $b^12 = a^6 = 1$ por tanto $|b| \mid 12$
 - $|b| = 1$, entonces $b = e$, es falso.
 - $|b| = 2$ entonces $e = b^2 = a$, es falso.
 - $|b| = 3$ entonces $e = b^2b = ab$ por lo que $b \in \langle a \rangle$ lo cual es falso.
 - $|b| = 4$ entonces $e = b^4 = a^2$, es falso.
 - $|b| = 6$ entonces $e = b^6 = a^3$, es falso.
 - $|b| = 12$ entonces $\langle b \rangle = G$, G es no abeliano por tanto es falso.
- $b^2 = a^2$, note que $a^{-2} = (bab^{-1})^2 = ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ por tanto $a^4 = 1$, es falso.
- $b^2 = a^3$ es una posibilidad.
- $b^2 = a^4$, note que $a^{-4} = (bab^{-1})^4 = ba^4b^{-1} = bb^2b^{-1} = b^2 = a^4$ por tanto $a^8 = 1$ y $6 \nmid 8$, es falso.
- $b^2 = a^5$ note que $a^{-5} = (bab^{-1})^5 = ba^5b^{-1} = bb^2b^{-1} = b^2 = a^5$ por tanto $a^{10} = 1$ y $6 \nmid 10$, es falso.

Ahora antes de establecer las condiciones finales veamos que el conjunto:

$$C := \{a^k b^m \mid 0 \leq k \leq 5, 0 \leq m \leq 1\}$$

tiene 12 elementos. Tome k_1, k_2 y m_1, m_2 tales que $a^{k_1} b^{m_1} = a^{k_2} b^{m_2}$, de aquí tenemos que $a^{k_1 - k_2} = b^{m_2 - m_1}$, supongamos que $m_2 > m_1$ luego $b = a^{k_1 - k_2} \in \langle a \rangle$ lo cual es falso. De aquí concluimos que $m_1 = m_2$ y $k_1 = k_2$. Así C tiene 12 elementos. por tanto $\langle a, b \rangle \cong G$. Para finalizar según todo lo anterior determinamos que si G es no abeliano tenemos alguno de los siguientes casos:

- $G \cong A_4$
- $G \cong \langle a, b \mid a^6 = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle$
- $G \cong \langle a, b \mid a^6 = 1, b^2 = a^3, bab^{-1} = a^{-1} \rangle$

Así concluimos que para los grupos de orden 12 hay 2 abelianos y 3 no abelianos.



Problema 4:

Sea $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$. Muestre que $PSL_2(\mathbb{Z}) \simeq \langle SR, S^2, R^3 \rangle$ donde

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ y } R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

Solución:

Esta proposición es falsa, veamos por que. Primero observe que:

$$S^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

y además:

$$R^3 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Es decir que $S^2 = R^3 = -I$, Además:

$$SR = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} = -1 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Llamemos $SR = T$ ahora podemos probar por inducción que:

$$(T)^n = (-1)^n \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

Observe que para $n = 1$ se tiene el resultado, Ahora supóngalo para n y veamos que ocurre con $n + 1$

$$(T)^{n+1} = T^n T = (-1)^n \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} (-1) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = (-1)^{n+1} \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$$

Entonces tenemos que:

$$\langle SR, S^2, R^3 \rangle = \left\langle (-1)^{n+1} \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}, -I \right\rangle$$

Ahora note que $S, R \in PSL_2(\mathbb{Z})$ por definición, pero ni S ni R pueden ser generadas por $\langle SR, -I \rangle$ por lo que no pueden ser isomorfas.

□□