Tarea 2. Álgebra Moderna

Estudiante: Juan Armando Parra Flores **Fecha:** 18 de febrero de 2021

Parte 1. t2-P.

1.12. (I) Sea $\alpha = (i_0 \quad i_1 \quad \cdots \quad i_{r-1})$ un r-ciclo. Para cada $j, k \geq 0$, demuestra que $\alpha^k(i_j) = i_{k+j}$ si los subíndices se leen módulo r.

Demostración. Podemos identificar al conjunto de $\{0, \ldots, r-1\}$ con $\mathbb{Z}_r$ para así decir que $i_j = i_{\overline{t}}$ siempre que $j \in \overline{t}$, donde $j \in \{1, \ldots, r-1\}$ y $\overline{t} \in \mathbb{Z}_r$, es decir, $j \equiv t \mod r$.

Procederemos por inducción sobre $k \geq 0$. Para $k = 0$ tenemos que $\alpha^k = \text{id}$. Por lo tanto, para toda $j \geq 0$ se tiene $\alpha^k\left(i_{\overline{j}}\right) = i_{\overline{j}} = i_{\overline{j+k}}$. Así que nuestra base inductiva con $k = 0$ es cierta.

Supongamos que para alguna $k \geq 0$ se tiene que para toda $\overline{j} \in \mathbb{Z}_r$, $\alpha^k\left(i_{\overline{j}}\right) = i_{\overline{j+k}}$. Al aplicar nuevamente α obtenemos que para toda $\overline{t} \in \mathbb{Z}_r$

$$\begin{aligned} \alpha^{k+1}(i_{\overline{t}}) &= \alpha\left(\alpha^k(i_{\overline{t}})\right) \\ &= \alpha\left(i_{\overline{t+k}}\right), \quad \text{por la hipótesis de inducción,} \end{aligned}$$

Sin embargo, como α es un ciclo, tenemos $\alpha\left(i_{\overline{t+k}}\right) = i_{\overline{t+k}+\overline{1}} = i_{\overline{t+k+1}}$. Por lo tanto $\alpha^{k+1}\left(i_{\overline{j}}\right) = i_{\overline{j+k+1}}$. Por el principio de inducción, se satisface lo anterior para cada $k \geq 0$.

■

(II) Demuestra que si α es un r-ciclo, entonces $\alpha^r = 1$, pero que $\alpha^k \neq 1$ para cada entero positivo $k < r$.

Demostración. Sea $i_{\overline{j}}$ un elemento que se mueve por el ciclo α. Por el inciso anterior

$$\alpha^r\left(i_{\overline{j}}\right) = i_{\overline{j+r}} = i_{\overline{j}+\overline{r}} = i_{\overline{j}+\overline{0}} = i_{\overline{j}}.$$

Para cualquier $i_{\overline{j}}$ que se queda fijo por α, para toda $k \geq 0$ también se queda fijo por α^k, en particular para $k = r$. De esta manera α^r es la función identidad porque fija a todos los elementos en su dominio.

Sin embargo, si $0 < k < r$, por lo anterior $\alpha^k(i_{\overline{0}}) = i_{\overline{k}}$, pero $\overline{k} \neq \overline{0}$, y entonces $\alpha^k(i_{\overline{0}}) \neq i_{\overline{0}}$. Así que α^k no es la identidad.

■

(III) Si $\alpha = \beta_1\beta_2\cdots\beta_m$ es un producto de r_i-ciclos disuntos β_i, entonces el entero positivo más pequeño l con $\alpha^l = 1$ es el mínimo común múltiplo de $\{r_1, r_2, \ldots, r_m\}$.

Demostración. Por inducción se puede probar que $\alpha^n = \beta_1^n \cdots \beta_m^n$ para toda $n \in \mathbb{Z}$, como una generalización del ejercicio en la tarea 1, pues es el producto de permutaciones disjuntas.

De esta manera tenemos $1 = \alpha^l = \beta_1^l \cdots \beta_m^l$. Si algún β_i mueve a x, entonces β_j lo fija si $i \neq j$. Por lo tanto β_j^l también lo deja fijo, ya que $\beta^l(x) = \beta^{l-1}(\beta(x)) = \beta^{l-1}(x)$, e inductivamente se tiene que $\beta^{l-1}(x) = x$.
Informalmente... $\beta_i^l(x) = 1$. Entonces l es un múltiplo de r_i por incisos anteriores, pues esto se mantiene para toda x que sea movida por β_i. Por tanto l es un común múltiplo de $r_1, \ldots, r_m$.
Si el mínimo común múltiplo lo satisface entonces terminamos. Pero sí lo hace porque se elevan cada una de las betas al mcm de las r_i's. Lo cual las hace identidades.

■

1.14. (I) Sea $\alpha = \beta\gamma$ en S_n, donde β y γ son disjuntas. Si β mueve i, entonces $\alpha^k(i) = \beta^k(i)$ para toda $k \geq 0$. El lema siguiente será de utilidad.

Lema 1.1. *Sea $\beta \in S_n$, y sea i tal que β mueve a i. Entonces β mueve a $\beta^k(i)$ para toda $k \geq 0$.*

Demostración. Por inducción sobre $k \geq 0$. Para $k = 0$ tenemos que $\beta^k = \mathrm{id}$, por lo que β mueve a $i = \mathrm{id}(i) = \beta^k(i)$, por hipótesis.
Supongamos que para alguna $k \geq 0$, β mueve a $\beta^k(i)$. Si suponemos que $\beta\left(\beta^{k+1}(i)\right) = \beta^{k+1}(i)$ aplicando β^{-1} por la izquierda concluiríamos que

$$\beta^{k+1}(i) = \beta^k(i).$$

Es decir, tendríamos que $\beta\left(\beta^k(i)\right) = \beta^k(i)$, lo cual contradice la hipótesis de inducción, en la que β mueve a $\beta^k(i)$. Por lo tanto, debe suceder que β mueva a $\beta^{k+1}(i)$.
Lo anterior, por el principio de inducción implica que β mueve a $\beta^k(i)$, para toda $k \geq 0$.

■

Continuamos con la demostración del inciso.

Demostración. Cuando $k = 0$, el resultado es claro, porque $\alpha^0 = \beta^0 = \mathrm{id}$. Sea i tal que $\beta(i) \neq i$. Cuando $k = 1$, como β mueve a i y es disjunta con γ, se tiene que γ fija a i. Entonces

$$\alpha(i) = \beta(\gamma(i)) = \beta(i).$$

Por lo tanto $\alpha^1(i) = \beta^1(i)$, para cada i que sea movido por β.
Supongamos que para algún $k \geq 0$ se tiene que si β mueve a i entonces $\alpha^k(i) = \beta^k(i)$. Por el Lemma 1.1 tenemos que β mueve a $\beta^k(i)$. Entonces usando la base inductiva (caso $k = 1$) tenemos que

$$\begin{aligned} \beta^{k+1}(i) &= \beta\left(\beta^k(i)\right) \\ &= \alpha\left(\beta^k(i)\right). \end{aligned}$$

Pero por la hipótesis de inducción $\alpha^k(i) = \beta^k(i)$, por lo que

$$\begin{aligned} \beta^{k+1}(i) &= \alpha\left(\beta^k(i)\right) \\ &= \alpha\left(\alpha^k(i)\right) \\ &= \alpha^{k+1}(i). \end{aligned}$$

Por el principio de inducción concluimos que $\alpha^k(i) = \beta^k(i)$, para toda $k \geq 0$.

$\blacksquare$

(II) Sean α y β ciclos en S_n (no suponemos que tienen la misma longitud). Si existe i_1 que se mueve por ambas α y β, y $\alpha^k(i_1) = \beta^k(i_1)$ para todo entero positivo k, entonces $\alpha = \beta$.

Demostración. Supongamos que la longitud de α es s. Tenemos que α mueve únicamente a los elementos del conjunto $\left\{i_1, \alpha(i_1), \ldots, \alpha^{s-1}(i_1)\right\}$, porque α es un ciclo. Más aún, el primer inciso del Ejercicio 1.12 implica que para toda $k \geq 0$, tenemos que $\alpha^k(i_1) \in \left\{i_1, \alpha(i_1), \ldots, \alpha^{k-1}(i_1)\right\}$. Lo mismo podemos decir de β. Usando módulos el tamaño de los ciclos podemos probar que

$$\left\{i_1, \alpha(i_1), \ldots, \alpha^{s-1}(i_1)\right\} = \left\{i_1, \beta(i_1), \ldots, \beta^{r-1}(i_1)\right\}.$$

Donde r es el tamaño de β. Como son ciclos son los únicos a los que mueven, y la hipótesis dice que son iguales.

$\blacksquare$

Parte 2. t2-H.

2. Si $\varphi : G \to H$ es un isomorfismo, demuestra que $|\varphi(x)| = |x|$ para toda $x \in G$. Deduce que cualquier par de grupos isomorfos tienen la misma cantidad de elementos de orden n para cada $n \in \mathbb{Z}^+$. ¿El resultado es cierto si φ sólo es homomorfismo?

Antes de demostrar lo que pide este ejercicio, demostraremos el siguiente lema.

Lema 2.2. *Sea $\varphi : G \to H$ un isomorfismo de grupos. Para todo $n \in \mathbb{Z}$ y todo $g \in G$ se tiene $\varphi(g^n) = (\varphi(g))^n$.*

Demostración. Probémoslo por inducción sobre $n \geq 0$. Para $n = 0$ es un resultado de homomorfismos que

$$\varphi\left(g^0\right) = \varphi(1_G) = 1_H = (\varphi(g))^0.$$

Supongamos que es cierto para algún $k \geq 0$. Entonces debe tenerse para cualquier $g \in G$ que $\varphi\left(g^k\right) = (\varphi(g))^k$. Multiplicando por $\varphi(g)$

$$\begin{aligned}
\varphi^{k+1}(g) &= (\varphi(g))^k \varphi(g) \\
&= \varphi\left(g^k\right)\varphi(g), \quad \text{por hipótesis de inducción,} \\
&= \varphi\left(g^k g\right), \quad \text{por ser } \varphi \text{ un homomorfismo,} \\
&= \varphi\left(g^{k+1}\right).
\end{aligned}$$

Por inducción se concluye que el resultado es cierto para toda $n \geq 0$. Sin embargo, también se sabe que $\varphi\left(g^{-1}\right) = (\varphi(g))^{-1}$. Por lo tanto, si $n \geq 0$ se tiene

$$\begin{aligned}
\varphi\left(g^{-n}\right) &= \varphi\left(\left(g^{-1}\right)^n\right) \\
&= \left(\varphi\left(g^{-1}\right)\right)^n, \quad \text{pues es lo que acabamos de probar,} \\
&= \left(\varphi(g)^{-1}\right)^n \\
&= \varphi(g)^{-n}.
\end{aligned}$$

Por lo tanto, se extiende el resultado para toda $n \in \mathbb{Z}$.

■

También nos será de utilidad el siguiente resultado.

Lema 2.3. *Sea $f : G \to H$ un isomorfismo. Su inversa f^{-1} también es un homomorfismo de H a G.*

Demostración. Sean $h_1, h_2 \in H$, y notemos que $f^{-1}(h_1), f^{-1}(h_2) \in G$. Por ser f un homomorfismo, al aplicarla en estos elementos se tiene

$$\begin{aligned} f\left(f^{-1}(h_1)f^{-1}(h_2)\right) &= f\left(f^{-1}(h_1)\right) f\left(f^{-1}(h_2)\right) \\ &= h_1h_2. \end{aligned}$$

Aplicando f^{-1} obtenemos

$$f^{-1}(h_1)f^{-1}(h_2) = f^{-1}(h_1h_2).$$

Esto implica que f^{-1} también es un homomorfismo.

■

Ahora sí, procedemos a demostrar que $|\varphi(x)| = |x|$ para toda $x \in G$, cuando φ es un isomorfismo.

Demostración. Sea $x \in G$. Por el Lema 2.2 se tiene

$$1_H = \varphi\left(1_G\right) = \varphi\left(x^{|x|}\right) = \varphi(x)^{|x|}.$$

Entonces $|\varphi(x)| \leq |x|$. Por otro lado se tiene también que

$$1_H = \varphi(x)^{|\varphi(x)|} = \varphi\left(x^{|\varphi(x)|}\right).$$

Tomando inversos se llega a que

$$\begin{aligned} x^{|\varphi(x)|} &= \varphi^{-1}\left(1_H\right) \\ &= 1_G. \end{aligned}$$

El último paso se debe a que φ^{-1} es un homomorfismos, y los homomorfismos envían los neutros a neutros. De aquí podemos concluir que $|\varphi(x)| \geq |x|$, y por lo tanto $|x| = |\varphi(x)|$.

■

1.49. Describe todos los homomorfismos de $\mathbb{Z}_{12}$ en sí mismo. ¿Cuáles de estos son isomorfismos?

Solución. Cada homomorfismo es determinado por el valor que le asigna al $\overline{1}$, ya que si φ es un homomorfismo, para cada $1 \leq i \leq 12$, se cumple que $\varphi\left(\overline{i}\right) = \sum_{j=1}^{i} \varphi\left(\overline{1}\right)$. A continuación escribiremos en una tabla todas las posibles funciones dependiendo del valor que le asignen al $\overline{1}$.

La columna cuyo nombre es "Valores" corresponde a elementos de $\mathbb{Z}_{12}$ a los que se les aplicará cada función φ_i. Por ejemplo, en la columna de φ_2 en el primer renglón (correspondiente al valor $\overline{1}$) tenemos el $\overline{2}$ ya que le asignamos $\varphi_2\left(\overline{1}\right) = \overline{3}$. De esto se deduce que $\varphi_2\left(\overline{2}\right) = \varphi_2\left(\overline{1}\right) + \varphi_2\left(\overline{1}\right) = \overline{2} + \overline{2} = \overline{4}$. Por eso en el renglón del valor $\overline{2}$ en la columna correspondiente a φ_2 está el valor de $\overline{4}$.

Valores	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6	φ_7	φ_8	φ_9	φ_{10}	φ_{11}	φ_{12}
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$	$\overline{0}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{0}$
$\overline{4}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$
$\overline{5}$	$\overline{5}$	$\overline{10}$	$\overline{3}$	$\overline{8}$	$\overline{1}$	$\overline{6}$	$\overline{11}$	$\overline{4}$	$\overline{9}$	$\overline{2}$	$\overline{7}$	$\overline{0}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$
$\overline{7}$	$\overline{7}$	$\overline{2}$	$\overline{9}$	$\overline{4}$	$\overline{11}$	$\overline{6}$	$\overline{1}$	$\overline{8}$	$\overline{3}$	$\overline{10}$	$\overline{5}$	$\overline{0}$
$\overline{8}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$
$\overline{9}$	$\overline{9}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$	$\overline{0}$
$\overline{10}$	$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$
$\overline{11}$	$\overline{11}$	$\overline{10}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	$\overline{0}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$

$\blacksquare$