

Universidad Nacional Autónoma de México
Facultad de Ciencias
Álgebra Moderna I

Tarea 1

Ángel Iván Gladín García
No. cuenta: 313112470
angelgladin@ciencias.unam.mx

5 de Febrero 2019

Ejercicio 1.

- a) Sea $\alpha = (i_0 \ i_1 \ \cdots \ i_{r-1})$ un r -ciclo. Para cualquier $i, k \geq 0$, pruebe que $\alpha^k(i_j) = i_{k+j}$.

Demostración. Notemos que α^k es la composición de α k -veces. Haciendo la siguiente observación de que $i_{j+1} = \alpha(i_j)$, $i_{j+2} = \alpha(i_{j+1}) = \alpha(\alpha(i_j)) = \alpha^2(i_j)$, $i_{j+3} = \alpha(i_{j+2}) = \alpha(\alpha^2(i_j)) = \alpha^3(i_j)$ y así para toda $k \leq r-1$, (cabe hacer la observación de que el subíndice de i , que es $j+l$ para algún l se toma $j+l$ módulo r) construyendo así hasta k se sigue que,

$$i_{j+k} = \alpha^k(i_j)$$

Como $\alpha(i_{j-1}) = i_j$, se puede ver que $i_{j+k} = \alpha^k(i_j)$ si el subíndice $j+k$ de i es tomado módulo r . \square

- b) Pruebe que si α es un r -ciclo, entonces $\alpha^r = 1$, pero que $\alpha^k \neq 1$ para cualquier entero positivo $k < r$.

Demostración. Sea α una permutación de la forma $\alpha = (i_0 \ i_1 \ \cdots \ i_{r-1})$, tenemos por el inciso anterior previamente demostrado que dada una premutación β se tiene que $\beta^k(i_j) = i_{k+j}$. Entonces si tomamos un j tal que $0 \leq j < r$, se sigue que $\alpha^r(i_j) = i_{r+j} = i_j$ (esto pasa porque $r+j = j$ en \mathbb{Z}_r), lo que significa que α deja fijos a los elementos. Ergo $\alpha^r = 1$.

Para demostrar que $\alpha^k \neq 1$ para cualquier entero positivo $k < r$, tomemos un j tal que $0 \leq j < r$, entonces $\alpha^k(i_j) = i_{j+k}$, y como por hipótesis $k < r$ entonces $i_k \neq i_{j+k}$. Por tanto $\alpha^k \neq 1$. \square

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

Demostración. Como por hipótesis los β_i son disjuntos, podemos usar el hecho de que conmutan para poder hacer lo siguiente,

$$\alpha^n = (\beta_1 \beta_2 \cdots \beta_m)^n = \beta_1^n \beta_2^n \cdots \beta_m^n$$

para toda $n \in \mathbb{Z}$. Supongamos que $\alpha^n = 1$ si y sólo si $\beta_i^n = 1$ para $1 \leq i \leq m$, Como α es un n -ciclo y β_i es un r_i -ciclo, se sigue que que todo r_i divide a n , y éso a su vez implica que el $m.c.m.(r_1, r_2, \dots, r_m) \mid n$. Como $\beta_i^n = 1$ para $1 \leq i \leq m$ justo aseguramos que n es el entero más pequeño. Renombrando a $m.c.m.(r_1, r_2, \dots, r_m) = l = n$, se sigue que l es el entero mas pequeño positivo tal que $\alpha^l = 1$. \square

Ejercicio 2.

Sea p un primo y sea $\alpha \in S_n$. Si $\alpha^p = 1$, entonces o bien $\alpha = 1$, α es un p -ciclo, o α es un producto de p -ciclos disjuntos. En particular, si $\alpha^2 = 1$, entonces o bien $\alpha = 1$, α es una transposición o α es un producto de transposiciones disjuntas.

Demostración. Por casos. Si $\alpha^p = 1$ entonces,

1. $\alpha = 1$.

Si descomponemos a α como producto de dos ciclos disjuntos (esto porque como p es primo) quedando así como $\alpha = \beta_1 \beta_2$ donde $\beta_1 = id$ y $\beta_2 = (1 \ 2 \ \cdots \ p) = \alpha$, entonces $\alpha^p = (\beta_1 \beta_2)^p = \beta_1^p \alpha^p = id \alpha^p$, por el inciso 1.2) podemos expresar a la identidad como α^p , entonces se sigue que $\alpha^p = \alpha \cdot \alpha^p = \alpha^{p+1}$ y multiplicando por α^{-p} la igualdad se sigue que $\alpha^{-p} \cdot \alpha^p = \alpha^{-p} \cdot \alpha^{p+1}$ teniendo así que $id = \alpha^p$.

2. α es un p -ciclo.

Análogo al anterior.

3. α es un producto de p -ciclos disjuntos.

Por el inciso 1.a) sabemos que $\alpha^p(i_k) = i_{k+p} = i_k$ lo que significa que lo deja fijos a todos los elementos, también podemos expresar p -ciclos disjuntos de la forma $id = (1)(2) \cdots (p)$, y ambos los dejan fijos a los i 's, por lo que ambos son la tienen la misma regla de correspondencia.

□

