

Apuntes de clase

José Antonio de la Rosa Cubero

Un r -ciclo puede escribirse como $\alpha = (x_1, x_2, \dots, x_r)$.

Un r -ciclo tiene r expresiones equivalentes:

$$(1, 4, 6) = (6, 1, 4)$$

Proposición 1. Sean $\alpha = (x_1, \dots, x_r)$ y $\beta = (y_1, \dots, y_s)$ dos ciclos en S_n . Entonces α y β son disjuntos si y solo si su intersección es vacía.

Teorema 1. Toda permutación de S_n , distinta de la identidad, se expresa de forma única como producto de ciclos disjuntos.

Es decir, dado $\alpha \in S_n \setminus id$, existen únicos ciclos $\alpha_1, \dots, \alpha_m$ disjuntos dos a dos tal que:

$$\alpha = \prod_{i=1}^m \alpha_i$$

donde la expresión es única salvo el orden del producto (los ciclos son disjuntos, luego conmutan).

Demostración. Veamos la existencia. Sea $\alpha \in S$ con $\alpha \neq id$. Sea

$$s = |\{x \in X : \alpha(x) \neq x\}|$$

Veamos que $s \geq 2$. Como $\alpha \neq id$, entonces tenemos que hay al menos dos elementos que no se mantienen fijos x e $y = \alpha(x)$.

Hacemos inducción. En el caso en el que $s \geq 2$. Entonces $\alpha = (x, y)$, puesto que la imagen de y por α no puede ser otro elemento que x , ya que el resto de elementos están fijos.

Supongamos $s > 2$ y supongamos el resultado cierto para toda permutación que mueva menos de s elementos.

Elegimos un elemento $x \in X$ tal que $\alpha(x) \neq x$. Consideramos la sucesión $x, \alpha(x), \alpha^2(x), \dots$, pero como X es finito, $\exists k > k'$ tales que $\alpha^k(x) = \alpha^{k'}(x)$, es decir $\alpha^{k-k'}(x) = x$. Tomamos el menor $r \geq 2$ tal que $\alpha^r(x) = x$.

Consideramos el siguiente ciclo:

$$\alpha_1 = (x, \alpha(x), \dots, \alpha^{r-1}(x)) \in S_n$$

Definimos la siguiente permutación:

$$\alpha'(y) = \begin{cases} y & \text{si } y \in \{x, \alpha(x), \dots, \alpha^{r-1}(x)\} \\ \alpha(y) & \text{en otro caso} \end{cases}$$

Se comprueba que $\alpha = \alpha_1 \alpha'$.

Como α' mueve $s - r$ elementos, por hipótesis de inducción tenemos que $\alpha = \alpha_1 \cdots \alpha_n$.

Probemos la unicidad. Sea $\alpha = \alpha_1 \cdots \alpha_m = \beta_1 \cdots \beta_m$.

Tenemos que

$$\alpha_1 = (x, \alpha_1(x), \alpha_1^2(x), \dots) = (x, \alpha(x), \alpha_1^2(x), \dots)$$

Pero del mismo modo tiene que existir un único β_j tal que $\beta_j(x) \neq x$ y el resto de los betas lo dejan fijos (son ciclos disjuntos).

Como el producto de ciclos disjuntos conmuta, suponemos $j = 1$ y: $\beta_1 = (x, \beta(x), \beta^2(x), \dots) = (x, \alpha(x), \alpha^2(x), \dots)$.

Por tanto $\alpha_1 = \beta_1$. Hagamos inducción en m . Si $m = 1$, $m' = 1$ porque si no tendríamos que los β_2 en adelante serían la identidad y eso no es posible, y ya lo tenemos. Si fuera cierto para cualquier natural menor que m , aplicando la hipótesis de inducción $\alpha_2 \cdots \alpha_m = \beta_2 \cdots \beta_{m'}$ y aplicando lo que hemos demostrado, tenemos que $\alpha_1 \cdots \alpha_m = \beta_1 \cdots \alpha_m$

□