

donde $\lambda_1, \lambda_2, \dots, \lambda_n$ son elementos distintos de A_n . define una permutación en A_n .

Pero, cuántas permutaciones se pueden definir sobre A_n ? , es decir, cuántos elementos tiene S_n ?

PROPOSICION 1. Existen $n! = 1 \cdot 2 \cdot 3 \dots (n-1)n$ permutaciones sobre A_n ; esto es S_n tiene $n!$ elementos.

Demost.- Hay n posibilidades para escoger $\lambda(1) = \lambda_1$; una vez escogido λ_1 , hay $(n-1)$ posibilidades para escoger $\lambda(2) = \lambda_2$; escogidos λ_1 y λ_2 quedan $(n-2)$ posibilidades para escoger $\lambda(3) = \lambda_3$; procediendo así, una vez que se han escogido $\lambda_1, \lambda_2, \dots, \lambda_{n-1}$, queda una sola posibilidad para escoger λ_n . Luego hay $n(n-1) \dots 2 \cdot 1 = n!$ formas de escoger $\lambda_1, \lambda_2, \dots, \lambda_n$ (sin repetición), así que $\#S_n = n!$

MULTIPLICACION O COMPOSICION DE PERMUTACIONES

En S_n consideremos la operación "composición de funciones" definida así: si $\sigma, \tau \in S_n$, entonces para $x \in A_n$, $x(\sigma \circ \tau) = (x\sigma)\tau$, donde $x\sigma$ se entiende como la imagen de x por σ y $(x\sigma)\tau$ es la imagen de $x\sigma$ por τ . Observe que esto es la composición de funciones solo que se hace en orden contrario al que estamos acostumbrados, en esta definición cuando calculamos $\sigma \circ \tau$ primero actúa σ y luego τ .

Por ejemplo, si $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ y $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, entonces:

$$\sigma \circ \tau = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 1 & 3 & 2 \end{array} \right) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Luego $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$; en adelante escribiremos $\sigma \circ \tau$ ó $\sigma \tau$.

Este producto puede ser leído de las permutaciones σ y τ , así: σ cambia 1 por 2 y τ cambia 2 por 3, por lo tanto $\sigma \tau$ cambia 1 por 3; σ cambia 2 por 3 y τ cambia 3 por 2, por consiguiente 2 "no se mueve" por $\sigma \tau$; σ cambia 3 por 1 y τ no mueve el 1, por esto $\sigma \tau$ cambia 3 por 1.

Aplicando primero la permutación τ y entonces la permutación σ , obtenemos el producto $\tau \sigma$, el cual nos da:

$$\tau \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

que no es el mismo producto que $\sigma \tau$.

Por lo tanto, vemos que en general el producto de permutaciones no es conmutativo. Sin embargo, puede suceder que las permutaciones conmuten, por ejemplo, las permutaciones:

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \text{y} \quad t = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

dan,

$$st = ts = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Si tenemos las permutaciones:

$$u = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \quad \text{y} \quad v = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix},$$

entonces:

$$uv = vu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}.$$

Observe que u es una permutación que no mueve 4 ni 5, y que v es una permutación que no mueve ni 1, ni 2, ni 3; en general cuando dos permutaciones mueven elementos distintos el producto es conmutativo.

Recordando las propiedades de la composición de funciones, tenemos:

G1.- Si $\sigma, \tau \in S_n$, entonces $\sigma \circ \tau \in S_n$.

G2.- Si $\sigma, \tau, \gamma \in S_n$, entonces $(\sigma \circ \tau) \circ \gamma = \sigma \circ (\tau \circ \gamma)$.

G3.- Si I es la permutación idéntica sobre A_n , es decir $xI = x$ para todo $x \in A_n$, entonces $I \circ \sigma = \sigma \circ I = \sigma$ para toda permutación $\sigma \in S_n$.

Consideremos la permutación:

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Viendo a la permutación β como un reordenamiento de los números 1, 2, 3, podemos decir que β cambia el arreglo 1 2 3 por el arreglo 2 3 1, es decir, la permutación β cambia 1 por 2, 2 por 3 y 3 por 1; esto es, cambia los números en un ciclo. De esta manera encontramos una notación más conveniente y frecuente para la permutación β :

$$\beta = (123) : \text{notación circular o cíclica de } \beta.$$

Significando que cada número en el ciclo es remplazado por el siguiente y el último número por el primero. Tenemos la siguiente definición:

DEFINICIÓN. Una permutación $t \in S_n$ es llamada un ciclo si aquellos enteros $x \in A_n$ tales que $xt \neq x$ pueden ser arreglados en un orden x_1, x_2, \dots, x_k de modo que $x_1t = x_2, x_2t = x_3, \dots, x_{k-1}t = x_k$ y $x_kt = x_1$. Un entero x tal que $xt \neq x$ se dice que es movido por t , y un entero x tal que $xt = x$ se dice que es dejado fijo por t .

La permutación,

$$t = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

es un ciclo, los elementos en A_3 movidos por t son 1 y 3, aquí

$1t=3$ y $3t=1$. Esta permutación la podemos representar en la siguiente forma llamado notación circular o cíclica: $t = (23)$. En esta notación los elementos dejados fijos por la permutación no aparecen. Hay que tener cuidado al usar esta notación, porque (23) podría también representar la permutación: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$; así que para establecer diferencias debemos hacer referencia al conjunto A_n .

La permutación

$$w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

no es un ciclo, porque no podemos arreglar los elementos movidos por w , en la forma que dice la definición; sin embargo, w es el producto de dos ciclos:

$$u = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (123) \quad \leftarrow \text{notación circular para } u.$$

$$v = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = (45) \quad \leftarrow \text{notación circular para } v.$$

Usando la notación circular, podemos escribir:

$$uv = (123)(45) = w.$$

Como obtenemos el producto de dos permutaciones escritas en forma circular?

Si $\beta = (123)$ y $t = (23)$ son permutaciones sobre A_3 , entonces:

$$\beta t = (123)(23) = (13),$$

donde βt puede ser leído de β y t así: β cambia 1 por 2 y t cambia 2 por 3, entonces βt cambia 1 por 3; β cambia 3 por 1 y t no altera el 1, por esto βt cambia 3 por 1 y 3 cierra el ciclo; β reemplaza 2 por 3 y t reemplaza 3 por 2, por consiguiente 2 no es desplazado por βt , por eso no aparece en el ciclo (13) .

De acuerdo a la definición de ciclo, la permutación idéntica es también un ciclo.

DEFINICIÓN. Sea t un ciclo en S_n . Entonces:

a) Si t no es la permutación idéntica, entonces t se dice un ciclo de longitud r si t mueve precisamente r elementos de A_n .

b) Si t es la permutación idéntica, entonces t se dice un ciclo de longitud 1.

De acuerdo a esta definición, el ciclo $\rho = (123)$ en A_3 tiene longitud 3, y el ciclo $t = (23)$ es de longitud 2.

Un ciclo de longitud 2 es llamado una transposición.

ORDEN DE UNA PERMUTACION.

Si $\sigma \in S_n$, entonces por G_2 , $(\sigma \circ \sigma) \circ \sigma = \sigma \circ (\sigma \circ \sigma)$, así que podemos eliminar los paréntesis y escribir $\sigma \circ \sigma \circ \sigma$ para representar $(\sigma \circ \sigma) \circ \sigma$ o $\sigma \circ (\sigma \circ \sigma)$ adoptando una notación del álgebra elemental, llamaremos potencias de σ a los productos: $\sigma \circ \sigma = \sigma^2$, $\sigma^2 \circ \sigma = \sigma^3$, ...

Si $\sigma = (123)$, entonces $\sigma^2 = (132)$, así mismo $\sigma^3 = I$. Continuando con estos cálculos sobre σ , obtenemos:

$$I = \sigma^3 = \sigma^6 = \dots$$

$$\sigma = \sigma^4 = \sigma^7 = \dots$$

$$\sigma^2 = \sigma^5 = \sigma^8 = \dots$$

y encontramos que no podemos obtener otras permutaciones distintas de I , σ y σ^2 , y que las permutaciones $\sigma^3, \sigma^6, \dots$ son iguales a la identidad.

DEFINICIÓN. La menor potencia de una permutación que es igual a la identidad

es el orden o período de la permutación.

Las potencias de $\tau = (1234)$ dan:

$$\tau^2 = (13)(24)$$

$$\tau^3 = (1432)$$

$$\tau^4 = I$$

Pues la permutación $\sigma = (123)$ es de orden tres, y la permutación $\tau = (1234)$ es de orden cuatro.

Si $\sigma \in S_n$ es un ciclo de longitud n , decimos que σ es una permutación circular. Una permutación circular sobre A_n intercambia cíclicamente los números $1, 2, \dots, n$.

Para formar el cuadrado de una permutación circular reemplazamos cada número por el segundo a su derecha (observa en los dos ejemplos anteriores), para formar el cubo por el tercero. En general, si tenemos una permutación circular $\sigma \in S_n$, la n -ésima potencia de σ reemplaza cada número por el n -ésimo a su derecha, es decir, reemplaza cada número por sí mismo, lo que nos da la permutación idéntica.

Cualquier potencia de tal permutación σ mayor que n es igual a alguna potencia menor que n , y todas las permutaciones distintas que podemos obtener como potencias de σ están contenidas en el conjunto:

$$\{I, \sigma, \sigma^2, \dots, \sigma^{n-1}\} \text{ o } \{\sigma, \sigma^2, \dots, \sigma^n = I\}.$$

Por lo tanto, tenemos:

PROPOSICIÓN 2. El orden de una permutación circular $\sigma \in S_n$ es n .

Para encontrar el orden de una permutación no-circular la descomponemos en sus ciclos y para los ciclos aplicamos la proposición 2 viendo cada

ciclo como una permutación circular. Por ejemplo, la permutación:

$$u = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

no es una permutación circular, pero su descomposición en ciclos es:

$$u = (123)(45)$$

entonces: $u^2 = (132)$, $u^3 = (45)$

$$u^4 = (123)$$
, $u^5 = (132)$

$$u^6 = I,$$

así que $u = (123)(45)$ es de orden seis; vemos que 6 es el mínimo común múltiplo de 3 y 2 que son los órdenes de los ciclos (123) y (45) respectivamente. El orden de una permutación no-circular es el mínimo común múltiplo de los órdenes de sus ciclos, pues justamente tal potencia de una permutación no-circular descompuesta en ciclos vuelve cada ciclo a la identidad.

64: INVERSO DE UNA PERMUTACION.

Existe siempre una permutación que deshace o reversa el intercambio de números efectuados por otra permutación, y es llamada la inversa de la permutación. El producto de una permutación y su inversa da la permutación idéntica (recuerde que si $f: A \rightarrow A$ es una función biyectiva, entonces $f^{-1}: A \rightarrow A$ es también función biyectiva y $f \circ f^{-1} = I_A = f^{-1} \circ f$)

Por ejemplo, si $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$, y $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132) = (321)$

$$\text{entonces } \sigma\tau = I = \tau\sigma.$$

De aquí se ve que obtenemos la inversa de una permutación circular tomando el orden contrario de los números en la permutación.

Siguiendo el uso del álgebra, denotaremos el inverso de una permutación σ

por σ^{-1} , así que $\sigma\sigma^{-1} = I$ y $\tau = \sigma^{-1}$ si $\sigma\tau = I = \tau\sigma$.

Para la permutación $u = (123)(45)$, $u^{-1} = (321)(54)$, así que se ve que obtenemos la inversa de una permutación tomando el orden contrario de los números en sus ciclos (cuando la permutación está descompuesta en sus ciclos).

Si el orden de una permutación σ es tres, entonces σ^2 y σ son inversas una de la otra; si el orden es dos, σ es su propia inversa.

Las permutaciones constituyen el primer ejemplo de grupo que se trató.

Entonces se hablaba de Grupos de permutaciones, y se decía que un conjunto G de permutaciones era un grupo, si:

- i) el producto de dos elementos de G estaba en G ,
- ii) la permutación idéntica estaba en G , y
- iii) cada permutación en G tenía una inversa en G .

Estas propiedades señalan las utilizadas, agregando la asociatividad, para la definición general de grupo.

CONEXION ENTRE ECUACIONES Y PERMUTACIONES.

EL DESCUBRIMIENTO DE LAGRANGE. -- Observando el siguiente trabajo podemos ver cómo están conectadas las ecuaciones con las permutaciones.

Dada la ecuación cúbica general:

$$x^3 - bx^2 + cx - d = 0 \quad (1)$$

haciendo $x = y + \frac{b}{3}$ la reducimos a la ecuación cúbica:

$$y^3 + py - q = 0 \quad (2)$$

donde $p = c - \frac{b^2}{3}$ y $q = d - \frac{bc}{3} + \frac{2b^3}{27}$.

Si hacemos ahora $y = u+v$ en (2), se obtiene la ecuación con dos incógnitas:

$$(u^3 + 3u^2v + 3uv^2 + v^3) + p(u+v) - q = 0 \quad (3)$$

que escribimos en la forma:

$$u^3 + v^3 + (3uv + p)(u+v) - q = 0 \quad (4)$$

Cualquiera sea la suma $u+v$, siempre es posible exigir que el producto uv tenga un valor fijado de antemano. Imponemos en este caso, la condición $3uv + p = 0$, es decir $uv = -\frac{p}{3}$. Utilizamos esto para eliminar v en (4) y obtener, después de simplificar, la ecuación:

$$u^6 - qu^3 - \frac{p^3}{27} = 0 \quad (5)$$

$$\left((u^3)^2 - qu^3 - \frac{p^3}{27} = 0 \right)$$

la cual es una ecuación cuadrática en u^3 , que resolvemos y obtenemos:

$$u^3 = \frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \quad (6)$$

$$= \frac{q}{2} \pm \sqrt{R} \quad \text{donde} \quad R = \frac{q^2}{4} + \frac{p^3}{27}$$

Una solución completa de las dos ecuaciones implícitas en (6) da 6 valores para u , los cuales son las 6 raíces de (5).

Se observa que si u es una raíz cúbica de $\frac{q}{2} + \sqrt{R}$, entonces $v = -\frac{p}{3u}$ es una raíz cúbica de $\frac{q}{2} - \sqrt{R}$.

Por tanto, las 6 raíces de (5) pueden expresarse en la forma:

$u, \omega u, \omega^2 u, v, \omega v, \omega^2 v$ donde $u^3 = \frac{q}{2} + \sqrt{R}$, $uv = -\frac{p}{3}$, y ω es una raíz primitiva de la unidad, es decir $\omega^3 = 1$ y $\omega^2 + \omega + 1 = 0$.

Con esto las raíces de la cúbica (2) serán:

$$y_1 = u+v = \sqrt[3]{\frac{q}{2} + \sqrt{R}} + \sqrt[3]{\frac{q}{2} - \sqrt{R}}$$