Revista Colombiana de Matemáticas
Vol. XXVI (1992) pgs. 55- 68

CONVERGENCIA DÉBIL HACIA EL PRODUCTO INFINITO DE LEYES DE POISSON EN UN PROBLEMA COMBINATORIO DE LOS GRUPOS SIMÉTRICOS

por

Jaime Lobo S.

RESUMEN. Extendiendo un problema clásico de las probabilidades, definimos en el grupo simétrico de orden n un vector aleatorio que cuenta el número de puntos fijos sobre las clases laterales generadas por un grupo cíclico. Demostramos que las distribuciones generadas en $\mathbb{N}^{\infty}$ por dichos vectores convergen débilmente al producto infinito de leyes de Poisson de parámetro 1. Finalmente estudiamos el funcional del número de desarreglos en las clases laterales, para el cual deducimos un teorema límite.[1]

§1. Planteamiento del problema y algunos preliminares

Sea S_n el grupo simétrico de grado n, grupo de las permutaciones en n elementos provisto de la medida de Haar de masa 1: $p_n(\omega) = 1/n!$. Dado ω en S_n, un elemento i es un punto fijo de ω si $\omega(i) = i$, punto móvil de ω en el caso contrario. Llamamos desarreglo a una permutación sin puntos fijos.

Un problema clásico de la teoría de probabilidades ("problème des recontres"), se puede plantear en su forma más general de la

---

[1] *Palabras claves*: Puntos fijos - desarreglos - clases laterales generadas por un grupo cíclico - ley producto infinito de leyes de Poisson - convergencia débil de una sucesión de leyes - momentos - números de Stirling - polinomios factoriales - bloques S-compatibles.

manera siguiente: escogiendo al azar una permutación de S_n, ¿cuál es la probabilidad de que sea un desarreglo? El cálculo de la probabilidad del evento: ω es un desarreglo, ([3], pág. 10), puede efectuarse gracias a la fórmula de inclusión - exclusión (ver fórmula (1) más adelante), que da:

$$1 - 1/1! + \dots + (-1)^n/n!$$

cuyo límite cuando $n \to \infty$ es $1/e$. No es difícil ahora el cálculo de la probabilidad del evento: ω posee exactamente k puntos fijos ($k \leq n$), cuyo valor es

$$1/k!\,(1 - 1/1! + \dots + (-1)^{n-k}/(n-k)!)$$

Se constata que ésta tiende a $1/k!\, e^{-1}$. Resumiendo, podemos decir que la ley de la variable aleatoria: número de puntos fijos de ω, tiende a la ley de Poisson de parámetro 1 cuando $n \to \infty$.

Deseamos extender este resultado a un problema que involucra vectores aleatorios. Sea π la permutación $(1\ 2\ 3\ \dots\ n)$ y $\langle\pi\rangle$ el grupo cíclico generado por π: $\{\pi, \pi^2, \dots \pi^n = e\}$. Definimos para cada $i = 1, \dots, n$ la variable f_i en S_n:

$$f_i(\omega) = \text{número de puntos fijos de } \pi^i\,\omega.$$

Identificaremos el vector $(f_1, f_2, \dots, f_n)$ con el vector infinito-dimensional:

$$f^{(n)} = (f_1, f_2, \dots, f_n, 0, 0, \dots)$$

de $\mathbb{N}^\infty$. Las distribuciones a estudiar estarán definidas en este último espacio. Este vector aleatorio es pues a valores discretos, y mide el número de puntos fijos sobre las clases laterales generadas por $\langle\pi\rangle$.

El objeto del presente trabajo es estudiar el comportamiento límite de las distribuciones con respecto a p_n, de los vectores aleatorios$(f_1, f_2, \dots, f_n)$. Para este objeto definimos P_n como la distribución en $\mathbb{N}^\infty$ del vector aleatorio $f^{(n)}$: $P_n = p_n \circ (f^{(n)})^{-1}$, (es decir $P_n(g) = p_n(g(f^{(n)}))$ para toda función acotada medible g). Denotamos por $\mathcal{P}(1)$ la ley de Poisson de parámetro 1, $\mathcal{P}^{\otimes k}(1)$ el k-ésimo producto de estas leyes (definido en $\mathbb{N}^k$), $\mathcal{P}^{\infty}(1)$ su producto infinito (ley en $\mathbb{N}^{\infty}$). El resultado fundamental es:

TEOREMA DE CONVERGENCIA. P_n *converge a* $\mathcal{P}^{\infty}(1)$ *cuando* $n \to \infty$, *en el sentido de convergencia débil de medidas en* $\mathbb{N}^{\infty}$.

Nótese que tomando k = 1 se deduce en particular que las leyes marginales unidimensionales convergen a $\mathcal{P}(1)$, que es exactamente lo anotado anteriormente para las leyes de f_i. Aunque el resultado para estas leyes unidimensionales es inmediato, no lo es así para la sucesión P_n. En efecto para todo n las variables proyección (x_i) en $\mathbb{N}^{\infty}$ no son independientes, pues por la misma definición de P_n:

$$P_n(x_1 + ... + x_n = n) = 1$$

mientras que según el teorema éstas resultan ser independientes y equidistribuidas en el límite.

§2. Lemas auxiliares

A efecto de establecer el teorema de convergencia utilizaremos propiedades particulares de las leyes $\mathcal{P}^{\otimes k}(1)$. Las mencionamos explícitamente pues algunas de ellas no aparecen así en la literatura revisada por el autor. Denotaremos por $\mathcal{P}(1;\ x^n)$ el n-ésimo momento de la ley $\mathcal{P}(1)$:

PROPIEDADES

(a) $\mathcal{P}(1;\ x^n) = \sum_{1 \leq k \leq n} S(n, k)$, donde S(n, k) denota el número de Stirling de segunda especie.

(b) $\sum_{n \geq 0} \mathcal{P}(1;\ x^n)\, t^n/n! = \exp(e^t - 1)$, para todo t.

(c) La ley $\mathcal{P}(1)$ está caracterizada por sus momentos (cualquier ley cuyos momentos coinciden con los de $\mathcal{P}(1)$ debe coincidir con $\mathcal{P}(1)$).

(a) y (b) son resultados conocidos sobre los números de Stirling y los números de Bell ([1], pág. 45 por ejemplo). El resultado de (c) es una consecuencia inmediata de los anteriores, pues de la convergencia de la serie potencial en (b) se deduce la de la serie $\Sigma_{n \geq 0} \mathbf{P}(1;\ x^n)\ t^n/n!$, que define el laplaciano de $\mathbf{P}(1)$ y de ahí la conclusión (ver [3], cap. VII, para más detalles sobre este problema).

LEMA 1. *Sea* $(Q_n)_{n \in \mathbb{N}}$ *una sucesión de probabilidades en* $\mathbb{N}^k$ *cuyos momentos de todos los órdenes convergen a los de* $\mathbf{P}^{\otimes k}(1)$. *Entonces* $(Q_n)_{n \in \mathbb{N}}$ *converge débilmente a* $\mathbf{P}^{\otimes k}(1)$.

Demostración. Si los momentos de todos los órdenes de una sucesión de probabilidades en $\mathbb{N}^k$ convergen a los de una probabilidad Q, caracterizada por sus momentos, entonces hay convergencia débil (ver [3], pág. 269). Concluimos entonces de esto y de la propiedad (c). ∎

Utilizaremos de ahora en adelante la fórmula clásica de inclusión-exclusión: dados p subconjuntos $A_1, \ldots, A_p$ de un conjunto finito tenemos:

$$|A_1 \cup \ldots \cup A_p| = \Sigma_{1 \leq i \leq p} |A_i| - \Sigma_{1 \leq i_1 < i_2 \leq p} |A_{i_1} A_{i_2}| + \ldots + (-1)^{p-1} |A_1 \ldots A_p| \quad (1)$$

Denotemos por $[x]_p$, $p \in \mathbb{N}$, el polinomio factorial de grado p:

$$[x]_p = x\,(x-1)\ \ldots\ (x-(p-1))/p!$$

y para $n \geq p$, sea $B_p[n]$ la familia de subconjuntos de p elementos de $\{1, \ldots, n\}$. Dados enteros $\ell_1, \ldots \ell_p$, denotamos $B_{\ell_1, \ldots, \ell_p} = B_{\ell_1}[n] \otimes \ldots \otimes B_{\ell_p}[n]$, familia del p-producto cartesiano del conjunto potencia de $\{1, \ldots, n\}$. La cardinalidad de $B_{\ell_1, \ldots, \ell_p}$ es pues $[n]_{\ell_1} \ldots [n]_{\ell_p}$.

Identifiquemos ahora el conjunto $\{1, \ldots n\}$ con el grupo de congruencias Z_n: $i \to i \pmod n$. Definimos la adición de conjuntos mediante esta identificación: $A + \ell = \{a + \ell \pmod n,\ a \in A\}$. Para cada $p \leq n$, la aplicación en $B_p[n]$: $A \to A + \ell$, es claramente biyectiva.

Sea $\mathbf{S} = (s_{i,j})$, una matriz de dimensión p con valores en Z_n. Definimos la familia $C(\mathbf{S})$ de $B_{\ell_1, \dots, \ell_p}$:

$C(\mathbf{S}) = \{(A_1, \dots, A_p) \in B_{\ell_1, \dots, \ell_p} : \forall (i,j)_{i \neq j}$ $A_i, A_j + s_{ij}$ son disjuntos y A_i, A_j son disjuntos$\}$ cuyos elementos llamaremos $\mathbf{S}$-compatibles en $B_{\ell_1, \dots, \ell_p}$.

LEMA 2. $|C(\mathbf{S})| = n^{\Sigma_i \ell_i}/\ell_1! \dots \ell_p! + O(n^{\Sigma_i \ell_i - 1})$.

Demostración. Introduciendo los conjuntos (para $i \neq j$):

$C(\mathbf{S})^{(i,j)} = \{(A_1, \dots, A_p) \in B_{\ell_1, \dots, \ell_p} : : A_i, A_j + s_{i,j}$ son disjuntos y A_i, A_j son disjuntos$\}$

podemos escribir:

$$|C(\mathbf{S})| = \left|\bigcap_{1 \leq i < j \leq p} C(\mathbf{S})^{(i,j)}\right|$$

de tal manera que:

$$|C(\mathbf{S})| = |B_{\ell_1, \dots, \ell_p}| - \left|\bigcup_{1 \leq i < j \leq p} \overline{C(\mathbf{S})^{(i,j)}}\right|$$

donde el complemento se toma con respecto a $B_{\ell_1, \dots, \ell_p}$. Como

$$|B_{\ell_1, \dots, \ell_p}| = |n|_{\ell_1} \dots |n|_{\ell_p} = n^{\Sigma_i \ell_i}/\ell_1! \dots \ell_p! + O\left(n^{\Sigma_i \ell_i - 1}\right),$$

Basta mostrar que

$$\left|\bigcup_{1 \leq i < j \leq p} \overline{C(\mathbf{S})^{(i,j)}}\right| \text{ es } O\left(n^{\Sigma_i \ell_i - 1}\right).$$

Usando la fórmula (1) para

$$\left|\bigcup_{1 \leq i < j \leq p} \overline{C(\mathbf{S})^{(i,j)}}\right|$$

obtenemos una expresión cuyos términos son de la forma

$$\left|\bigcap_{(i,j) \in A} C(\mathbf{S})^{(i,j)}\right|$$

donde A recorre los subconjuntos $\{1, \dots, p\}^{\otimes 2}$. Siendo el número de términos independiente de n, basta demostrar que cada uno de ellos es de la forma $O(n^{\Sigma_i \ell_i - 1})$. Cada término está acotado por un

$\left|C(S)^{(i,j)}\right|$. Por otra parte $C(S)^{(i,j)}$ es unión de dos conjuntos de la forma $B^{i,j}$:

$$B^{i,j} = \{(A_1, \ldots, A_p) \in B_{\ell_1,\ldots,\ell_p} : A_i, A_j \text{ tienen un punto en común}\}$$

y basta entonces demostrar la relación $\left|B^{i,j}\right| = O(n^{\Sigma_i \ell_i - 1})$. Para esto denotamos:

$$B^{i,j}(k) = \{(A_1, \ldots, A_p) \in B_{\ell_1,\ldots,\ell_p} : k \in A_i, k \in A_j\}.$$

Entonces $B^{i,j} = \bigcup_{1 \leq k \leq n} B^{i,j}(k)$. Aplicamos la fórmula (1) a $\left|B^{i,j}\right|$. Los términos que aparecen son de la forma ($1 \leq s \leq n$):

$$\sum_{1 \leq k_1 < k_2 < \ldots < k_s \leq n} \left|B^{i,j}(k_1) \ldots B^{i,j}(k_s)\right| \tag{2}$$

Es claro que este término es 0 si $s > \ell_i$ o $s > \ell_j$ y por lo tanto el número de términos de la expansión no puede exceder $\min(\ell_i, \ell_j)$. En el caso contrario tendremos que $(A_1, \ldots, A_p) \in B^{i,j}(k_1) \ldots B^{i,j}(k_s)$ si y sólo si

$$\{k_1, \ldots, k_s\} \subset A_i \ \text{ y } \ \{k_1, \ldots, k_s\} \subset A_j .$$

Entonces s elementos de A_i y de A_j están fijos y el resto de los $\ell_i - s$ de A_i (resp. $\ell_j - s$ de A_j) varían en un conjunto de $n - s$ elementos. Se deduce que

$$\left|B^{i,j}(k_1) \ldots B^{i,j}(k_s)\right| = [n - s]_{\ell_i - s} [n - s]_{\ell_j - s} \prod_{t \neq i,j} [n]_{\ell_t}$$

expresión que no depende de los $k_1, \ldots, k_s$. Puesto que la suma (2) se extiende a todos los s-conjuntos de $\{1, \ldots, n\}$, su valor es :

$$[n]_s [n - s]_{\ell_i - s} [n - s]_{\ell_j - s} \prod_{t \neq i,j} [n]_{\ell_t}$$

que es el valor en n del producto de polinomios factoriales, siendo el grado:

$$s + (\ell_i - s) + (\ell_j - s) + \Sigma_{t \neq i,j} \ell_t = \Sigma_t \ell_t - s.$$

Sumando sobre s obtenemos entonces el valor en n de un polinomio de grado $\Sigma_t \ell_t - 1$. Por lo tanto $\left|B^{i,j}\right| = O(n^{\Sigma_i \ell_i - 1})$, lo que acaba la demostración. ■

Sean $i_1 < \ldots i_p$ y $\ell_1, \ldots, \ell_p$ enteros. Dados $(A_1, \ldots, A_p) \in B_{\ell_1,\ldots,\ell_p}$, definimos el conjunto de S_n:

$$M(A_1, \ldots, A_p) = \left\{\omega \in S_n : A_j \subset \{\text{puntos fijos de } \pi^{i_j}\omega\}, j = 1, \ldots, p\right\}$$

Sea $\mathbf{S}$ la matriz de entradas $s_{j,j'} = i_j - i_{j'}$.

LEMA 3. *Si* $(A_1, \ldots, A_p)$ *es* $\mathbf{S}$*-compatible en* $B_{\ell_1,\ldots,\ell_p}$ *y además* $n > \Sigma_i \ell_i$, *entonces:*

$$\left|M(A_1, \ldots, A_p)\right| = \left(n - \Sigma_i \ell_i\right)!$$

y es cero de otra manera.

Demostración. Las condiciones que definen a $M(A_1, \ldots, A_p)$:

$$A_j \subset \{\text{puntos fijos de } \pi^{i_j}\omega\}, \qquad j = 1, \ldots, p \tag{3}$$

equivalen evidentemente a fijar los valores de ω en los conjuntos $A_1, \ldots, A_p$. Por lo tanto cualquier permutación que verifique (3) se identifica con una permutación de $n - \Sigma_i \ell_i$ elementos, y recíprocamente, de donde se sigue que el valor de la cardinalidad cuando $M(A_1, \ldots, A_p)$ no es vacío y se cumple $n > \Sigma_i \ell_i$.

Para establecer la condición de compatibilidad, observamos primero que siendo los conjuntos de puntos fijos de diferentes $\pi^{i_j}\omega$ disjuntos es necesario que los A_j sean disjuntos dos a dos. Bajo esta condición es también necesario que las imágenes de los A_j sean disjuntas. Pero si k es punto fijo de $\pi^{i_j}\omega$, su imagen bajo ω debe ser $\pi^{-i_j}(k)$, y por lo tanto $\omega(A_j) = \pi^{-i_j}(A_j)$. Las dos condiciones anteriores resultan ser también suficientes para que se de (3), o sea equivalen a:

$$A_j A_{j'} = \emptyset, \; j \neq j' \;\; \text{y} \;\; \pi^{-i_j}(A_j) \cdot \pi^{-i_{j'}}(A_{j'}) = \emptyset, \; j \neq j' \tag{4}$$

Pero $\pi^{-i_j}(A_j) \cdot \pi^{-i_{j'}}(A_{j'}) = \emptyset$ equivale a $A_j \cdot \pi^{(i_j - i_{j'})}(A_{j'}) = \emptyset$. Como además $\pi^{(i_j - i_{j'})}(A_{j'}) = A_{j'} + (i_j - i_{j'})$, deducimos que las condiciones (4) equivalen a que $(A_1, \ldots, A_p)$ sea $\mathbf{S}$-compatible en $B_{\ell_1,\ldots,\ell_p}$, para $\mathbf{S}$ definida en el enunciado. ■

§3. Demostración del teorema de convergencia

Dada la caracterización de la convergencia débil de medidas en $\mathbb{N}^\infty$, el resultado del teorema puede enunciarse en términos de convergencia débil de leyes finito-dimensionales: P_n converge a $\mathbf{P}(1)^\infty$ si para todo $(t_1, t_2, \ldots, t_k)$ en $\mathbb{N}^k$, las medidas $P_n \circ \pi^{-1}_{(t_1, t_2, \ldots, t_k)}$ incluidas en $\mathbb{N}^k$ por las proyecciones canónicas convergen a $\mathbf{P}^{\otimes k}(1)$ (ver [2]). Denotando siempre por x_i las proyecciones canónicas de $\mathbb{N}^\infty$, basta demostrar, según el Lema 1 del §1, que las potencias de P_n de todos los órdenes convergen a las potencias respectivas de $\mathbf{P}^\infty(1)$. Esto significa, dados $i_1 < \ldots < i_p$ y $n_1, \ldots, n_p$ enteros, estudiar el límite de

$$E_n\left[(x_{i_1})^{n_1} \ldots (x_{i_p})^{n_p}\right]$$

cuando $n \to \infty$. Podemos suponer entonces que $n > n_1 + \ldots + n_p$.

Usando la relación $P_n = p_n \bullet (f^{(n)})^{-1}$ escribimos:

$$E_n\left[(x_{i_1})^{n_1} \ldots (x_{i_p})^{n_p}\right] = E_{p_n}\left[(f_{i_1})^{n_1} \ldots (f_{i_p})^{n_p}\right]$$

Para cada i expresamos f_i de la siguiente manera:

$$f_i(\omega) = \Sigma_{1 \le k \le n} 1_{\{k \text{ es un punto fijo de } \pi^i\omega\}}$$

Calculemos $(f_i)^m$.

$$(f_i)^m = \Sigma_{(k_1, \ldots, k_m) \in \{1, \ldots, n\}} 1_{\{k_1, \ldots, k_m \text{ son puntos fijos de } \pi^i\omega\}}$$

$$= \Sigma_{1 \le j \le m} S(m, j)\, j!\, \Sigma_{A \in \{1, \ldots, n\}, |A| = j} 1_{\{A \in \{\text{puntos fijos de } \pi^i\omega\}\}}$$

En el último paso se usó el hecho de que el número de sobreyecciones de $\{1, \ldots, m\}$ en $\{1, \ldots, j\}$ es $S(m, j)\, j!$, donde $S(m, j)$ es el número de Stirling de segunda especie ([1], pág. 39). Siendo así, podemos escribir:

$$(f_{i_1})^{n_1} \ldots (f_{i_p})^{n_p} = \Sigma_{1 \le \ell_i \le n_i} S(n_1, \ell_1) \ldots S(n_p, \ell_p)\, \ell_1! \ldots \ell_p!\, \Sigma(\ell_1, \ldots, \ell_p)$$

donde

$$\Sigma(\ell_1, \ldots, \ell_p) = \Sigma_{(A_1, \ldots, A_p),\, |A_i| = \ell_i,\, i = 1, \ldots, p}\, I(M(A_1, \ldots, A_p))$$

y donde $I(M(A_1, ..., A_p))$ = función indicadora de $M(A_1, ..., A_p)$, siendo $M(A_1, ..., A_p)$ como en el Lema 3.

Aplicando el Lema 3 y el supuesto de que $n > n_1 + ... + n_p$, calculamos la esperanza con respecto a p_n de $\Sigma(\ell_1, ..., \ell_p)$:

$$E_{p_n}\left[\Sigma(\ell_1, ..., \ell_p)\right] = \sum_{(A_1, ..., A_p),\, |A_i| = \ell_i,\, i = 1, ..., p} E_{p_n}\left[I(M(A_1, ..., A_p))\right]$$

$$= \sum_{\substack{(A_1, ..., A_p),\, |A_i| = \ell_i,\, i = 1, ..., p \\ (A_1, ..., A_p)\ \mathrm{S}\text{- compatible}}} \frac{\left(n - \Sigma_i \ell_i\right)!}{n!} \tag{3}$$

$$= \frac{\left(n - \Sigma_i \ell_i\right)!}{n!\,\left|C(\mathrm{S})\right|}$$

siendo $|C(\mathrm{S})|$ como en el Lema 2.

Finalmente tomamos la esperanza de $(f_{i_1})^{n_1} ... (f_{i_p})^{n_p}$:

$$E_{p_n}\left[\left(f_{i_1}\right)^{n_1} .. \left(f_{i_p}\right)^{n_p}\right] = \Sigma_{\substack{1 \le \ell_i \le n_i \\ 1 \le i \le p}} S(n_1, \ell_1) .. S(n_p, \ell_p)\, \ell_1! .. \ell_p!\, E_{p_n}\left[\Sigma(\ell_1, ..., \ell_p)\right]$$

$$= \Sigma_{\substack{1 \le \ell_i \le n_i \\ 1 \le i \le p}} S(n_1, \ell_1) .. S(n_p, \ell_p)\, \ell_1! .. \ell_p!\, \frac{\left(n - \Sigma_i \ell_i\right)!}{n!\,\left|C(\mathrm{S})\right|}$$

(en esta última expresión $|C(\mathrm{S})|$ depende en realidad de $\ell_1, ..., \ell_p$).

Según el Lema 2, $|C(\mathrm{S})| = n^{\Sigma_i \ell_i}/\ell_1!, ...\ \ell_p!, + O(n^{\Sigma_i \ell_i - 1})$ y como $\frac{n!}{\left(n - \Sigma_i \ell_i\right)!}$ es $[n]$, cuyo grado es $\Sigma_i \ell_i$, obtenemos:

$$E_{p_n}\left[\left(f_{i_1}\right)^{n_1} ... \left(f_{i_p}\right)^{n_p}\right] = \Sigma_{\substack{1 \le \ell_i \le n_i \\ 1 \le i \le p}} S(n_1, \ell_1)\ ...\ S(n_p, \ell_p) + O(1/n)$$

$$= \prod_{i = 1, ..., p} \left(\sum_{j = 1, ..., n_i} S(n_i, j)\right) + O(1/n)$$

y esta expresión es igual, según propiedad (a) de §1, a:

$$\pi_{i=1,\dots,p} \mathbf{P}(1; x^{n_i}) + O(1/n) = \mathbf{P}^{\otimes p}(1; x^{n_1} \dots x^{n_p}) + O(1/n)$$

lo que demuestra que:

$$E_n\left[(x_{i_1})^{n_1} \dots (x_{i_p})^{n_p}\right] \underset{n \to \infty}{\longrightarrow} \mathbf{P}^{\otimes p}(1; x^{n_1} \dots x^{n_p}) \;. \blacksquare$$

§4. Estudio de la ley del número de desarreglos en las clases de $\langle\pi\rangle$

Consideremos la variable aleatoria en S_n del número de desarreglos en una clase de $\langle\pi\rangle$:

$$D_n(\omega) = |\{i,\ 1 \leq i \leq n : f_i(\omega) = 0\}|.$$

Podemos establecer ciertas propiedades generales referentes a las leyes de los D_n.

PROPOSICIÓN 1. $p_n(D_n = 1) = 1/(n-1)!$ *para todo* n. *Las probabilidades* $p_n(D_n = q)$ *son nulas en los siguientes casos:*

(a) n *par*, $q = 0$
(b) n *impar*, $q = 1$
(c) n *primo*, $q = n - 2$

Demostración. Sea ω en S_n, tal que $D_n(\omega) = 1$. Esto se cumple si y sólo si un elemento en la clase $\langle\pi\rangle\omega$ es la permutación identidad, lo que significa que ω debe ser un elemento de $\langle\pi\rangle$. Como $|\langle\pi\rangle| = n$, se demuestra la primera aserción.

Identificamos $\{1, \dots, n\}$ con el grupo de congruencias Z_n, con lo cual los elementos del grupo cíclico $\langle\pi\rangle$ se identifican con las translaciones: $\pi^j(a) = a + j$. Sea ω una permutación. Entonces se puede decir que i es un punto fijo de $\pi^j(\omega)$ si y sólo si $j = -\pi^{-i}(\omega(i))$, lo que se deduce de las relaciones:

$$\pi^j(\omega(i)) = i \Leftrightarrow \omega(i) + j = i \Leftrightarrow \omega(i) - i = -j \Leftrightarrow j = -\pi^{-i}(\omega(i)).$$

De lo anterior se infiere que:

$$\{j : f_j \neq 0\} = \{- \pi^{-1}(\omega(i)), i \in Z_n\}. \qquad (5)$$

Por otra parte tenemos:

$$\Sigma_i -\pi^{-1}(\omega(i)) = \Sigma_i i - \Sigma_i \omega(i) = 0 \bmod(n). \qquad (6)$$

D_n es entonces la cardinalidad de $\{j : f \neq 0\}$. El resultado de la proposición se obtiene fácilmente de estas relaciones:

(a) Si para algún ω se tuviera $D_n(\omega) = 0$, entonces (5) implica que

$$\{-\pi^{-1}(\omega(i)), i \in Z_n\} = Z_n$$

por lo que:

$$\Sigma_i -\pi^{-1}(\omega(i)) = \Sigma_i i = n(n+1)/2 \ (\bmod n).$$

Pero si n es par, $n(n + 1)/2 = n/2 \neq 0 \bmod (n)$, y la última relación sería incompatible con (6).

(b) Supongamos ahora que $D_n(\omega) = 1$. Considerando un elemento en la clase $\langle\pi\rangle\omega$, podemos suponer que $\{j : f \neq 0\} = Z_n - \{0\}$. Siendo así, sea $q \neq 0$, único en Z_n tal que $|\{i : -\pi^{-1}(\omega(i)) = q\}| = 2$. Entonces de (5):

$$\Sigma_i -\pi^{-1}(\omega(i)) = \Sigma_{i=1,\dots,n-1} i + q = \Sigma_i i + q = n(n+1)/2 + q \bmod (n).$$

Si n es impar, $n(n + 1)/2 = 0 \bmod(n)$, y la relación anterior es incompatible con (6).

(c) Si $D_n(\omega) = n-2$ sean p, q en Z_n, $p \neq q$, tales que

$$\{j : f_j \neq 0\} = \{p, q\}.$$

Considerando un elemento en la clase $\langle\pi\rangle\omega$, podemos suponer $p = 0$, $q \neq 0$. Entonces existe un entero m tal que:

$$\Sigma_i -\pi^{-1}(\omega(i)) = mq \bmod(n).$$

La relación (6) implica que $mq = 0 \bmod(n)$; pero si n es primo, la relación $mq = 0 \bmod(n)$ sólo puede darse si $q = 0$, pues Z_n es un campo, y esto contradice la escogencia de q. ■

El teorema de convergencia puede ser aprovechado para estudiar la convergencia de las leyes de D_n. Esto significa estudiar en $\mathbb{N}^{\infty}$ el comportamiento asintótico de las leyes con respecto a P_n en $\mathbb{N}^{\infty}$ de las variables:

$$D_n((x_i)_{i \in \mathbb{N}}) = \left|\{i,\ 1 \leq i \leq n: x_i = 0\}\right|.$$

Pero bajo $\mathcal{P}^{\infty}(1)$, las proyecciones canónicas son independientes y equidistribuidas según $\mathcal{P}(1)$, y por lo tanto D_n sigue la ley binomial de parámetros n, e^{-1}. Podemos aplicar entonces el teorema del límite central conjuntamente con la convergencia débil de las leyes P_n hacia $\mathcal{P}^{\infty}(1)$ para deducir:

COROLARIO 1.

$$\lim_{n \to \infty} \lim_{k \to \infty} P_k\left(\frac{D_n - n\,e^{-1}}{\sqrt{e^{-1}(1-e^{-1})\,n}} \leq b\right) = \int_{-\infty}^{b} \frac{1}{\sqrt{2\pi}} \exp\left(\frac{-x^2}{2}\right) dx.$$

Pasando las medidas p_n en S_n, podemos traducir el resultado anterior diciendo: para a < b, n y k suficientemente grandes, el efectivo total de permutaciones en S_n tales que

$$a\sqrt{\frac{e^{-1}(1-e^{-1})}{n}} < \frac{D_k}{k} - e^{-1} < b\sqrt{\frac{e^{-1}(1-e^{-1})}{n}}$$

es aproximadamente n! ($\phi(b) - \phi(a)$), donde ϕ designa la distribución normal de media 0 y varianza 1.

El resultado anterior puede ser de interés para efectos de una aproximación "aleatoria" del número 1/e. En efecto, para n y k suficientemente grandes, D_k/k, el promedio ponderado parcial del número de desarreglos en una clase de $\langle\pi\rangle$ estaría próximo a 1/e con una probabilidad muy grande. Esto parece ser más ventajoso que emplear el resultado clásico: p_n (ω es desarreglo) $\approx$ 1/e, pues se requeriría con esto simular en S_n una sucesión finita de tamaño N de permutaciones independientes y calcular para ellas el promedio ponderado del número de desarreglos, con un N generalmente muy grande dado que la sucesión generada es binomial de parámetro $\approx$ 1/e.

REFERENCIAS

[1] COMTET L., *Analyse combinatoire*, Tomo II. Presses Universitaries de France, 1970

[2] BILLINGSLEY P., *Convergence of Probablility Measures*. Wiley, 1968.

[3] FELLER W., *An Introduction to Probability Theory and its Applications*, Volume II, Wiley, 2ª edición, 1968.

[4] DUBREIL P., *Teoría de Grupos*. Ed. Reverté, 1975.

Escuela de Matemáticas
Universidad de Costa Rica
San José, Costa Rica.

(Recibido en noviembre de 1990, la versión revisada en mayo de 1992).