ROBERTO FRUCHT

CORONA DE GRUPOS Y SUS SUBGRUPOS

CON UNA

APLICACION A LOS DETERMINANTES

UNION MATEMATICA ARGENTINA
Publicación N.º 24

BUENOS AIRES
1942

CORONA DE GRUPOS Y SUS SUBGRUPOS, CON UNA APLICACION A LOS DETERMINANTES

por ROBERTO FRUCHT

INTRODUCCION

Varios autores (véase el breve resumen histórico en el § 1) han observado que con dos grupos de permutaciones P_r y H respectivamente en r y s variables, se puede formar un nuevo grupo de permutaciones en rs variables, la «corona» $P_r[H]$. Para la definición de este grupo véase el § 2, para ejemplos de «coronas» el § 3. Después de haber indicado, en el § 4, la fórmula general para el producto de dos permutaciones de una corona, y en el § 5 unas consecuencias de dicha fórmula, paso, en el § 6, a la consideración de ciertos subgrupos de una corona, que están en analogía con los subgrupos «meromorfos» considerados en el caso de un producto directo por R. Remak en Lit. 5) (*).

Como a estos subgrupos da origen un subgrupo invariante J del grupo H, los denoto por $P_r[H;J]$ Tomando para P_r el grupo de orden 2, para H el grupo simétrico en n cifras y para el subgrupo invariante J el grupo alternado en n cifras, obtengo (en el § 7) un grupo interesantísimo del orden $(n!)^2$, que sólo para $n \leqq 3$ es isomorfo al producto de dos grupos simétricos en n cifras. En el § 8 se demuestra además que dicho grupo es isomorfo al grupo de las permutaciones de los elementos de un determinante del orden n, las que no alteran el valor del determinante.

§ 1. Breve resumen histórico.

Parece que el primero que haya considerado, en un caso particular, la ley de formación de coronas de grupos, haya sido A. Scholz en Lit. 8); él observó que con dos grupos abstractos S y T, respectivamente de los órdenes σ y τ, se puede formar un nuevo grupo abstracto del orden $\sigma\tau^\sigma$, llamado

(*) Con la palabra "Lit." me refiero siempre a la lista de "Literatura citada" al final de este artículo.

por él $S \# T$; este grupo no es nada más que el caso particular de una corona de grupos $S[T]$, cuando para S se toma la representación del respectivo grupo abstracto por permutaciones regulares. El ejemplo de grupos cíclicos había sido considerado por Scholz en una publicación precedente (Lit. 7), bajo el nombre «Metabelsche Dispositionsgruppe».

Otro caso particular, el de las coronas del tipo $S_n[H]$ (designando por S_n siempre el grupo simétrico en n variables, del orden $n!$), ha sido considerado, casi simultáneamente, por B. Neumann (Lit. 3) y W. Specht (Lit. 10). El primero concentra su interés en la generación de $S_n[H]$ — y en particular de $S_n[S_m]$ — por pocos elementos, estableciendo entre ellos relaciones que definan el grupo; en cambio Specht, siguiendo un consejo de I. Schur, ha estudiado el problema de la representación de $S_n[H]$ por matrices (sustituciones lineales homogéneas), y el mismo problema también para el caso de la corona más general $P_r[H]$, en una segunda publicación (Lit. 11) (**).

Más tarde, e independientemente de las publicaciones citadas, G. Pólya llegó al concepto de las coronas de grupos, en una publicación (Lit. 4) igualmente interesante para quien se ocupe de grupos, topología combinatoria, teoría de funciones complejas o química orgánica. Pólya da una definición muy intuitiva de la corona $P_r[H]$ y aplicaciones interesantísimas a la topología combinatoria, observando que el grupo de automorfismos de un «álbero» se puede obtener aplicando a cierto número de grupos simétricos S_{m_1}, S_{m_2}, ... S_{mk}, un número finito de veces, las dos operaciones: formación del producto directo y de la corona.

Con la traducción «corona» del término alemán «Kranz», yo quisiera seguir la terminología de Pólya, que me parece ser muy feliz. Pero observo que en lo que sigue no supongo el conocimiento del artículo de Pólya ni de las otras publicaciones citadas más arriba, sino que desarrollaré completamente el concepto de la corona, en la forma más adecuada para el estudio de las cuestiones a cuya solución quisiera contribuir con la presente publicación.

(**) Cabe observar que Neumann y Specht designan la corona por $S_n(H)$ resp. $P_r(H)$. La notación $P_r[H]$ y la misma palabra "corona" (en alemán "Kranz") se encuentran por primera vez en la publicación de Pólya (Lit. 4).

§ 2. *Definición de la corona* $P_r[H]$. *Descomposición en componentes.*

Dados dos grupos de permutaciones P_r y H, respectivamente en r y s variables, consideramos en una sala r mesas distintas; cada una sea rodeada de s sillas distintas en cierto orden bien determinado. Distribuimos ahora rs personas, numeradas desde *1* hasta rs, sobre las sillas, de modo que *cada* silla sea ocupada exactamente por *una* persona. Sometiendo las r mesas (con sus sillas, sin alterar, por ahora, el orden relativo de estas últimas alrededor de cada mesa) a las permutaciones del grupo P_r, y sometiendo sucesivamente las sillas de cada mesa a permutaciones del grupo H, las rs personas sufrirán ciertas permutaciones cuyo conjunto *forma un grupo* de permutaciones en rs variables.

Esta es una explicación intuitiva del concepto de la corona $P_r[H]$. Una definición exacta sería la siguiente:

Dados, como antes, un grupo de permutaciones en r variables P_r, del orden π, y otro en s variables, H, del orden η, consideramos r «ejemplares» de H, es decir r grupos $H^{(1)}$, $H^{(2)}$, ..., $H^{(r)}$, cada uno isomorfo (*) al grupo H, y con ellos formamos el producto directo $H^{(1)} \times H^{(2)} \times \ldots \times H^{(r)}$, es decir, el grupo del orden η^r en rs variables, por ejemplo en las variables

$$(I.) \quad \begin{cases} x_1^{(1)} & x_2^{(1)} & \ldots & x_s^{(1)} \\ x_1^{(2)} & x_2^{(2)} & \ldots & x_s^{(2)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_1^{(r)} & x_2^{(r)} & \ldots & x_s^{(r)} \end{cases}$$

que resulta cuando para cada $\rho = 1, 2, \ldots, r$, las variables $x_1^{(\rho)}$, $x_2^{(\rho)}$, ..., $x^{(\rho)}_s$ son sometidas a las permutaciones del grupo $H^{(\rho)}$.

En otras palabras, si $h_1^{(1)}$ es una permutación de $H^{(1)}$ (correspondiente, en base del isomorfismo $H^{(1)} \sim H$, a la per-

(*) Empleo las palabras "isomorfo" e "isomorfismo" siempre en el sentido de una correspondencia recíprocamente unívoca entre los elementos de dos grupos G y H, la que mantiene la ley de multiplicación, y denoto este isomorfismo abreviadamente por $G \sim H$.

mutación h_1 de H), $h_2^{(2)}$ una de $H^{(2)}$ (correspondiente a la h_2 de H), etc., el elemento $h_1^{(1)} . h_2^{(2)} \ldots h_r^{(r)}$ de $H^{(1)} \times H^{(2)} \times \ldots \times H^{(r)}$ es la permutación de las rs variables $x_\sigma^{(\rho)}$ que se compone de la permutación $h_1^{(1)}$ de las variables $x_\sigma{}^{(1)}$ que forman la primera fila del esquema (I.), de la permutación $h_2^{(2)}$ de las variables $x_\sigma{}^{(2)}$ de la segunda fila, etc.

Ahora bien, si el grupo P_r tiene el orden $\pi = 1$, definimos: $P_r[H] = H^{(1)} \times H^{(2)} \times \ldots \times H^{(r)}$; si el orden π de P_r es mayor que *1*, a cada permutación p de P_r hacemos corresponder la permutación $p^{(o)}$ de las variables $x_\sigma^{(\rho)}$ que resulta cuando las *r filas* horizontales del esquema (I.) son sometidas a la permutación p (sin alterar el orden de las variables en cada fila), y consideramos las permutaciones

$$p^{(o)} . h_1^{(1)} . h_2^{(2)} . \ldots . h_r^{(r)}$$

de las variables $x_\sigma^{(\rho)}$ del esquema (I.), es decir, aquellas, en donde primeramente las filas del esquema son sometidas a una permutación de P_r y después las variables en las filas a permutaciones que corresponden a las del grupo H. Estas $\pi\eta^r$ permutaciones del tipo $p^{(o)} . h_1^{(1)} . h_2^{(2)} . \ldots . h_r^{(r)}$ forman la *corona* $P_r[H]$.

Se ve fácilmente que la corona $P_r[H]$ es realmente un *grupo*. Sin anticipar la fórmula para el producto de dos permutaciones de $P_r[H]$, la que será indicada en el § 4 (y que sirvió a Specht como definición de la corona), se comprende «a priori» que el resultado de dos permutaciones sucesivas del tipo descrito es también una permutación del mismo tipo (lo que es suficiente para que un conjunto de permutaciones forme un grupo).

Cabe observar que es *unívoca* la representación de las permutaciones de la corona $P_r[H]$ en la forma

$$u = p^{(o)} h_1^{(1)} h_2^{(2)} . \ldots . h_r^{(r)}$$

en donde $p^{(0)}$ es una permutación de las filas (sin alterar en ellas el orden relativo de las variables) y $h_\rho^{(\rho)}$ es una permutación de las variables de la ρ-ésima fila del esquema (I.) ($\rho = 1, 2, \ldots r$). Diremos que $p^{(0)}$ es la *componente* de la permutación u respecto

de P_r y $h_\rho^{(\rho)}$ la *componente* de u respecto de $H^{(\rho)}$ ($\rho = 1, 2, \ldots r$). Está claro cómo hay que proceder para encontrar las componentes de una permutación u de las variables del esquema (I.) la que pertenece a la corona $P_r[H]$: primeramente se considera sólo la permutación p que sufren las filas horizontales del esquema (sin tomar en cuenta, por ahora, lo que pasa con las variables mismas en las filas); escribiendo dicha permutación de las filas como permutación de las variables $x_\sigma^{(\rho)}$, obtenemos la componente $p^{(0)}$ de u respecto de P_r. Las otras componentes se determinan después fácilmente como las permutaciones de las variables en cada fila que hay que agregar a $p^{(0)}$ para obtener u.

Un ejemplo de esta descomposición en componentes seguirá en el § 3.

§ 3. Ejemplos para coronas.

a) Consideremos un octaedro regular (Fig. 1) y su grupo, es decir el grupo de los movimientos (rotaciones) que lo dejan invariante. Como se sabe, este grupo es isomorfo al grupo simétrico S_4 en 4 variables, porque hay isomorfirmo entre dichos movimientos y todas las permutaciones de las 4 rectas que unen los centros de gravedad de dos triángulos opuestos del octaedro.

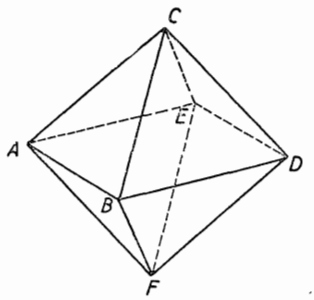

Fig. 1

Ahora pasamos a la consideración del grupo que resulta cuando a los movimientos del octaedro agregamos todavía las transformaciones compuestas de un movimiento y de la «reflexión al centro», la que reemplaza cada vértice del octaedro

por el diametralmente opuesto (por ejemplo A por D, B por E, etc.). La reflexión al centro forma, con la identidad, un grupo S_2 del orden 2, y es conmutable con cada movimiento; por consiguiente, el nuevo grupo que estamos considerando, es isomorfo al producto *directo* $S_4 \times S_2$ del orden 48.

Por otra parte, el mismo grupo se puede interpretar también como corona $S_3[S_2]$, considerando como variables de permutar los 6 vértices del octaedro; como los 6 vértices se pueden dividir en 3 pares de 2 vértices diametralmente opuestos:

$$(\text{II.}) \quad \left\{ \begin{array}{ll} A & D \\ B & E \\ C & F \end{array} \right.$$

y como el grupo considerado comprende todas las permutaciones de las filas del esquema (II.) — grupo: S_3 — con sucesivas permutaciones, según S_2, en las filas, resulta, por definición, la corona $S_3[S_2]$.

Así el «grupo amplificado del octaedro» enseña la existencia de un isomorfismo entre el producto directo $S_4 \times S_2$ y la corona $S_3[S_2]$ (*) y vemos en este caso que una corona, considerada como grupo abstracto, puede ser isomorfa a un producto directo.

Aprovechemos este primer ejemplo «concreto» de una corona para ilustrar, en un ejemplo, la descomposición en componentes de una permutación de la corona. Sea u una rotación del octaedro alrededor del eje «vertical» CF por el ángulo 90°, seguida por la sustitución de cada vértice por el diametralmente opuesto:

$$u = \begin{pmatrix} A\,B\,C\,D\,E\,F \\ E\,A\,F\,B\,D\,C \end{pmatrix}.$$

¿Cuáles son las componentes de u? Como u permuta A y D, las «variables» de la primera fila, en B y E, las de la

(*) La existencia de este isomorfismo explica porqué en una publicación mía anterior (Lit. 1), el grupo considerado ahora, aparece sólo en la forma del producto directo $S_4 \times S_2$, mientras Pólya, en la pág. 214 de la publicación ya citada (Lit. 4), da la preferencia a la interpretación como corona $S_3[S_2]$.

segunda, etc., vemos que la permutación de las tres filas es la siguiente:

$$p = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}$$

y por eso:

$$p^{(0)} = \begin{pmatrix} A\,D \\ B\,E \end{pmatrix} \cdot \begin{pmatrix} B\,E \\ A\,D \end{pmatrix} \cdot \begin{pmatrix} C\,F \\ C\,F \end{pmatrix} = \begin{pmatrix} A\,B\,C\,D\,E\,F \\ B\,A\,C\,E\,D\,F \end{pmatrix}.$$

$p^{(0)}$ no es todavía igual a u, sino que es necesario hacer seguir a $p^{(0)}$ las siguientes permutaciones *en las distintas filas* para llegar a u:

en la primera: ninguna (tenemos $B \rightarrow A$ y $E \rightarrow D$ en $p^{(0)}$ como en u)

en la segunda: permutación de B en E y viceversa

en la tercera: permutación de C en F y viceversa.

Por eso, las componentes de u respecto de $H^{(1)}$, $H^{(2)}$ y $H^{(3)}$ son, respectivamente, la identidad, $h_2^{(2)} = \begin{pmatrix} B\,E \\ E\,B \end{pmatrix}$ y $h_3^{(3)} = \begin{pmatrix} F\,C \\ C\,F \end{pmatrix}$

b) Introduciendo todavía un sistema de coordenadas cartesianas, con el centro del octaedro regular como origen O y con $\overrightarrow{OA}$, $\overrightarrow{OB}$, $\overrightarrow{OC}$, como ejes positivos de las x_1, x_2, x_3; vemos que el grupo $S_3[S_2]$ se puede representar también como grupo de transformaciones de coordenadas del tipo:

$$x_1 = \varepsilon_1 x'_\alpha \ , \quad x_2 = \varepsilon_2 x'_\beta \ , \quad x_3 = \varepsilon_3 x'_\gamma \ ,$$

en donde $\begin{pmatrix} \varepsilon\ \zeta\ \iota \\ \alpha\ \beta\ \gamma \end{pmatrix}$ es una permutación cualquiera y $\varepsilon_1^2 = \varepsilon_2^2 = \varepsilon_3^2 = 1$.

De un modo general, todas las transformaciones en m variables:

$$x_r = \varepsilon_r x'_{\alpha_r} \qquad (r = 1, 2, \ldots, m),$$

siendo $\begin{pmatrix} 1 & 2 & \ldots & m \\ \alpha_1 & \alpha_2 & \ldots & \alpha_m \end{pmatrix}$ una permutación cualquiera en m cifras y $\varepsilon_r^2 = 1$ $(r = 1, 2, \ldots, m)$, forman un grupo del orden $2^m . m!$, el grupo «hiperoctaedral», que se puede interpretar como corona $S_m[S_2]$ (véase Specht, Lit. 10). En este caso, las $2m$ variables de permutar son los puntos del espacio de m dimensiones los que tienen todas sus coordenadas iguales a cero, con excepción

de una que es igual a *1* o a *— 1*; las componentes de las permutaciones de dichos puntos respecto de S_m son las permutaciones de los *m* ejes de coordenadas sin tomar en cuenta su sentido positivo o negativo.

Las permutaciones de la corona $S_m[S_2]$ se pueden también caracterizar como las permutaciones de las variables $x_1, x_2, \ldots, x_{2m}$, que dejan invariante el polinomio:

$$(x_1 + x_2)(x_3 + x_4)(x_5 + x_6) \cdot \ldots \cdot (x_{2m-1} + x_{2m})$$

o el otro («dual» al primero) (*):

$$x_1 x_2 + x_3 x_4 + x_5 x_6 + \ldots + x_{2m-1} x_{2m}.$$

En el caso particular de $m = 2$ obtenemos un grupo $S_2[S_2]$ del orden 8, que es isomorfo al grupo diédrico del mismo orden (= grupo de movimientos de un cuadrado en el espacio).

c) Las coronas $S_m[S_2]$ que acabamos de considerar representan sólo un caso particular ($n = 2$) de las coronas $S_m[S_n]$ del orden $m!\,(n!)^m$. Evidentemente, $S_m[S_n]$ se puede obtener como grupo de las permutaciones de *mn* variables $x_1, x_2, \ldots x_{mn}$ que no alteran el valor del polinomio:

$$(x_1 + x_2 + x_3 + \ldots + x_n)(x_{n+1} + x_{n+2} + \ldots + x_{2n})$$
$$(x_{2n+1} + \ldots + x_{3n}) \cdot \ldots \cdot (x_{(m-1)n+1} + \ldots + x_{mn})$$

o del otro («dual» al primero):

$$x_1 x_2 x_3 \cdot \ldots \cdot x_n + x_{n+1}\, x_{n+2} x_{n+3} \cdot \ldots \cdot x_{2n} +$$
$$x_{2n+1} x_{2n+2} \cdot \ldots \cdot x_{3n} + \ldots + x_{(m-1)n+1} \cdot \ldots \cdot x_{mn}.$$

En otras palabras, se trata de todas las permutaciones que permutan entre sí las filas horizontales del esquema:

(*) Hay aquí un principio de dualidad análogo al que rige, en la lógica formalística, para las operaciones "$\&$" y "v".

$$(\text{III.}) \quad \begin{cases} x_1, & x_2, & \dots x_n \\ x_{n+1}, & x_{n+2}, & \dots x_{2n} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ x_{(m-1)n+1}, & x_{(m-1)n+2}, & \dots x_{mn} \end{cases}$$

de cualquier manera, permutando, además, las variables de cada fila de todos los modos posibles. Por eso, Specht llama $S_m[S_n]$ el grupo imprimitivo completo del tipo (m, n).

d) El grupo «hiperoctaedral» $S_m[S_2]$ se puede considerar también como caso particular de la corona $S_m[C_n]$ del orden $m!\,n^m$, designando por C_n el grupo cíclico del orden n. $S_m[C_n]$ se puede caracterizar, en el grupo simétrico S_{mn} (que comprende todas las permutaciones de las cifras $1, 2, 3, \dots mn-1, mn$), como el subgrupo de las permutaciones conmutables con un producto de m ciclos de a n cifras, por ejemplo con:

$$(1, 2, 3, \dots n)\ (n+1, n+2, n+3, \dots, 2n)$$
$$(2n+1, 2n+2, \dots, 3n) \dots\dots ((m-1)n+1, \dots, mn).$$

Consideremos todavía el caso particular de que $n+1=p$ sea un número primo. En este caso, $S_m[C_n]=S_m[C_{p-1}]$ se puede interpretar también como el grupo de ciertos automorfismos de un grupo abeliano del orden p^m que es el producto directo de m grupos cíclicos del orden p. Sean $a_1, a_2, \dots, a_m$ m elementos del orden p que engendran dicho grupo abeliano (o, en otras palabras, que forman una base del grupo abeliano). Entre todos los automorfismos del grupo abeliano, habrá ciertos que permutan cada elemento a_μ $(\mu=1, 2, \dots, m)$ en un elemento a_r o en una potencia a_r^ρ de un elemento a_r $(r \neq \mu$ o $r=\mu)$. Evidentemente, estos automorfismos forman una corona $S_m[C_{p-1}]$, del orden $m!(p-1)^m$, y tratándose de un subgrupo del grupo de *todos* los automorfismos del grupo abeliano considerado, resulta que $m!(p-1)^m$ debe ser un divisor del orden de este último grupo, es decir de

$$(p^m-1)(p^m-p)(p^m-p^2)\dots\dots(p^m-p^{m-1})$$
$$= p^{1+2+3\dots+m-1}.(p-1)(p^2-1)(p^3-1)\dots\dots(p^{m-1}-1)(p^m-1)$$
$$= p^{\frac{m(m-1)}{2}}.(p-1)^m.(1+p)(1+p+p^2)$$
$$(1+p+p^2+p^3)\dots\dots(1+p+p^2+\dots+p^{m-1})$$

Simplificando aún por el factor común $(p-1)^m$, obtenemos así un teorema de la teoría de los números:

Para cada número entero positivo m *y cada número primo* p *el producto*

$$p^{\frac{m(m-1)}{2}} \cdot (1+p)(1+p+p^2)$$
$$(1+p+p^2+p^3) \cdot \ldots \cdot (1+p+p^2+p^3+\ldots+p^{m-1})$$

es divisible por m!

Cabe observar que este teorema resulta también como consecuencia inmediata de la siguiente fórmula demostrada por I. Schur (Lit. 9): Con las notaciones abreviadas

$$s_\mu = 1+x+x^2+\ldots+x^\mu ,$$

$$\left[\begin{matrix} m \\ o \end{matrix}\right] = 1$$

y

$$\left[\begin{matrix} m \\ \mu \end{matrix}\right] = \frac{(x^m-1)(x^{m-1}-1)(x^{m-2}-1) \cdot \ldots \cdot (x^{m-\mu+1}-1)}{(x-1)(x^2-1)(x^3-1) \cdot \ldots \cdot (x^\mu-1)}$$

para $0 < \mu \leqq m$ es

$$x^{\frac{m(m-1)}{2}} \cdot s_1 s_2 s_3 \cdot \ldots \cdot s_{m-1} = m! \cdot \sum_{\mu=o}^{m-1} (-1)^\mu \left[\begin{matrix} m \\ \mu \end{matrix}\right] x^{\frac{\mu(\mu-1)}{2}} \binom{s_{m-\mu-1}}{m}$$

Esta fórmula enseña que para cualquier número entero x (y no sólo un número primo p) el producto

$$x^{\frac{m(m-1)}{2}} \cdot s_1 s_2 s_3 \cdot \ldots \cdot s_{m-1} = x^{\frac{m(m-1)}{2}} \cdot (1+x)(1+x+x^2)$$
$$(1+x+x^2+x^3) \cdot \ldots \cdot (1+x+x^2+\ldots+x^{m-1})$$

es divisible por $m!$

e) Un subgrupo del grupo $S_m[C_n]$ es la corona $C_m[C_n]$ del orden $m\,n^m$ (siendo, por supuesto, C_m el grupo cíclico del orden m). Para $C_m[C_n]$ se puede dar la siguiente interpretación «cinemática» (variando ligeramente un ejemplo indicado por Pólya):

Cada uno de los m vértices de un polígono regular que pueda girar en su plano alrededor de su centro, sea reemplazado por una circunferencia del pequeño radio r, situada en el mismo plano y que pueda girar alrededor de su centro. Sobre cada circunferencia márquense todavía n puntos equidistantes. (Una ilustración del caso: $m=5$, $n=4$, se encuentra en la Fig. 2). *Fijando cierta posición primitiva* del polígono y de las «ruedas», consideramos ahora todos los movimientos planos de ellos que conduzcan a una posición que difiera de la primitiva sólo por una permutación de los mn puntos marcados sobre las n circunferencias («ruedas»). Dichas permutaciones forman un grupo isomorfo a $C_m[C_n]$, considerando como variables de permutar los mn puntos marcados; más exactamente dicho: los de *una* circunferencia forman siempre las variables de una fila del esquema (III.).

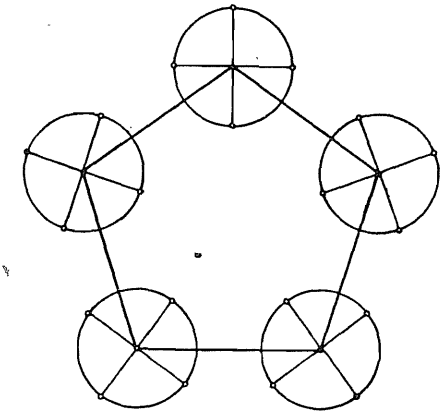

Fig. 2

En lugar de las permutaciones de las mn variables, podemos considerar también las sustituciones *monomiales* en m variables $z_1, z_2, \ldots, z_m$ que correspondan a las m ruedas, distinguiendo los n puntos de *una* rueda sólo por factores $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$, en donde ε es una primitiva raíz n-ésima de la unidad.

Así, el grupo $C_m[C_n]$ se podría engendrar por las dos sustituciones monomiales:

$$\begin{pmatrix} z_1 & z_2 & z_3 & \ldots & z_{m-1} & z_m \\ z_2 & z_3 & z_4 & \ldots & z_m & z_1 \end{pmatrix}$$

y

$$\begin{pmatrix} z_1 & z_2 & z_3 & \dots & z_{m-1} & z_m \\ \varepsilon z_1 & z_2 & z_3 & \dots & z_{m-1} & z_m \end{pmatrix}$$

f) De un modo más general, cada corona del tipo $P_r[C_n]$ se puede escribir como el grupo de sustituciones monomiales en r variables que se obtiene cuando a cada permutación de P_r, escrita en r variables $z_1, z_2, \dots, z_r$:

$$\begin{pmatrix} z_1 & z_2 & z_3 & \dots & z_r \\ z_{\alpha_1} & z_{\alpha_2} & z_{\alpha_3} & \dots & z_{\alpha r} \end{pmatrix}$$

hacemos corresponder las n^r sustituciones monomiales:

$$\begin{pmatrix} z_1 & z_2 & z_3 & \dots & z_r \\ \varepsilon_1 z_{\alpha_1} & \varepsilon_2 z_{\alpha_2} & \varepsilon_3 z_{\alpha_3} & \dots & \varepsilon_r z_{\alpha r} \end{pmatrix}$$

con $\varepsilon_\rho{}^n = 1$ $(\rho = 1, 2, \dots r)$.

Recíprocamente, cada grupo de sustituciones monomiales en r variables, cuyos «factores» ε_ρ son raíces n-ésimas de la unidad, es un subgrupo de la corona $S_r[C_n]$ del orden $r!n^r$ (*).

§ 4. *La ley de multiplicación en* $P_r[H]$.

Volvemos ahora al caso general de una corona cualquiera $P_r[H]$, formada con dos grupos de permutaciones P_r y H, respectivamente en r y s variables, y preguntamos: ¿cuál es el producto de dos permutaciones de $P_r[H]$, por ejemplo el producto

$$(p^{(0)} h_1^{(1)} h_2^{(2)} \dots h_r^{(r)}) \cdot (q^{(0)} k_1^{(1)} k_2^{(2)} \dots k_r^{(r)}),$$

siendo $h_\rho^{(\rho)}$ y $k_\rho^{(\rho)}$ dos permutaciones de $H^{(\rho)}$ (**) $(\rho = 1, 2, \dots, r)$

(*) Para los que conocen la teoría de los "graphs", añado que la corona $S_r[H]$ se puede interpretar como el grupo de automorfismos del "graph" formado por r "ejemplares" de Γ, cuando H es el grupo de automorfismos de un "graph conexo" Γ. En una publicación anterior (Lit. 2), he demostrado que para cada grupo abstracto H existe una infinidad de estos "graphs" que tengan un grupo de automorfismos isomorfos a H.

(**) Que correspondan a las permutaciones h_ρ y k_ρ de H en virtud del isomorfismo $H^{(\rho)} \sim H$.

y $p^{(0)}$ y $q^{(0)}$ las permutaciones de las variables $x_\sigma^{(\rho)}$ que resultan cuando aplicamos dos permutaciones p y q de P_r a las r filas horizontales del esquema (I.)? (En otras palabras, queremos determinar el producto de las permutaciones con las componentes $p^{(0)}, h_1^{(1)}, h_2^{(2)}, \ldots, h_r^{(r)}$ y $q^{(0)}, k_1^{(1)}, k_2^{(2)}, \ldots, k_r^{(r)}$).

Supongamos que q sea la permutación que transforma la cifra ρ en β_ρ $(\rho = 1, 2, \ldots, r)$:

$$(IV.) \qquad q = \begin{pmatrix} 1 & 2 & \ldots & r \\ \beta_1 & \beta_2 & \ldots & \beta_r \end{pmatrix}$$

En este caso, $q^{(0)}$ será la misma permutación, pero aplicada a las r *filas* del esquema (I.), y por consiguiente, transformará $x_\sigma^{(\rho)}$ en $x_\sigma^{(\beta\rho)}$ $(\rho = 1, 2, \ldots, r;\ \sigma = 1, 2, \ldots, s)$.

En primer lugar determinaciones la permutación $(q^{(0)})^{-1} h_1^{(1)} q^{(0)}$, es decir la transformada de la permutación $h_1^{(1)}$ por la permutación $q^{(0)}$. $h_1^{(1)}$ permuta sólo las variables $x_\sigma^{(1)}$ de la primera fila de (I.); pero, a raíz de la permutación precedente $(q^{(0)})^{-1}$ se encuentran allí las variables que pertenecían primitivamente a la fila β_1; y por la sucesiva aplicación de $q^{(0)}$, dichas variables vuelven a ocupar la fila β_1, después de haber sufrido la permutación $h_1^{(1)}$ en la primera fila. Entonces, el efecto de la permutación $(q^{(0)})^{-1} h_1^{(1)} q^{(0)}$ será el siguiente: las variables $x_1^{(\beta_1)}, x_2^{(\beta_1)}, \ldots, x_s^{(\beta_1)}$ de la fila β_1 son permutadas entre sí, como si hubiéramos aplicado a ellas la permutación $h_1^{(\beta_1)}$ (es decir la permutación que corresponde a la permutación h_1 de H, en virtud del isomorfismo $H^{(\beta_1)} \sim H$); las variables de todas las otras filas no sufren ninguna permutación. Así vemos que es:

$$(q^{(0)})^{-1} h_1^{(1)} q^{(0)} = h_1^{(\beta_1)}$$

De manera análoga siguen las relaciones

$$(q^{(0)})^{-1} h_\rho^{(\rho)} q^{(0)} = h_\rho^{(\beta\rho)},$$

y multiplicando todas éstas, para $\rho = 1, 2, \ldots, r$, obtenemos el resultado

$$(q^{(0)})^{-1} (h_1^{(1)} h_2^{(2)} \ldots . h_r^{(r)}) \, q^{(0)} = h_1^{(\beta_1)} h_2^{(\beta_2)} \ldots . h_r^{(\beta_r)}.$$

Introduciendo todavía la permutación q^{-1}, inversa a la (IV.):

$$(IV'.) \qquad q^{-1} = \begin{pmatrix} 1 & 2 & 3 & \dots & r \\ \gamma_1 & \gamma_2 & \gamma_3 & \dots & \gamma_r \end{pmatrix},$$

obtenemos la siguiente fórmula para la transformación de $h_1^{(1)} h_2^{(2)} \dots . h_r^{(r)}$ con $q^{(0)}$:

$$(V.) \quad (q^{(0)})^{-1} (h_1^{(1)} h_2^{(2)} \dots . h_r^{(r)}) . q^{(0)} = h_{\gamma_1}^{(1)} h_{\gamma_2}^{(2)} \dots . h_{\gamma_r}^{(r)}.$$

Esta fórmula permite ahora el cálculo del producto de dos permutaciones

$$u = p^{(0)} h_1^{(1)} h_2^{(2)} \dots . h_r^{(r)}$$

y

$$v = q^{(0)} k_1^{(1)} k_2^{(2)} \dots . k_r^{(r)}$$

de $P_r[H]$:

$$\begin{aligned} u\,v &= p^{(0)} h_1^{(1)} h_2^{(2)} \dots . h_r^{(r)} q^{(0)} k_1^{(1)} k_2^{(2)} \dots . k_r^{(r)} \\ &= p^{(0)} q^{(0)} . (q^{(0)})^{-1} . (h_1^{(1)} h_2^{(2)} \dots . h_r^{(r)}) . q^{(0)} . k_1^{(1)} k_2^{(2)} \dots . k_r^{(r)} \\ &= p^{(0)} q^{(0)} . h_{\gamma_1}^{(1)} h_{\gamma_2}^{(2)} \dots . h_{\gamma_r}^{(r)} . k_1^{(1)} k_2^{(2)} \dots . k_r^{(r)} \\ &= p^{(0)} q^{(0)} . h_{\gamma_1}^{(1)} k_1^{(1)} . h_{\gamma_2}^{(2)} k_2^{(2)} \dots . h_{\gamma_r}^{(r)} k_r^{(r)}. \end{aligned}$$

Observando que es

$$p^{(0)} q^{(0)} = (pq)^{(0)}$$

y escribiendo más brevemente $(h_{\gamma\rho} k_\rho)^{(\rho)}$ para la permutación $h_{\gamma\rho}^{(\rho)} k_\rho^{(\rho)}$ de $H^{(\rho)}$ que corresponde a la $h_{\gamma\rho} k_\rho$ de H (en virtud del isomorfismo $H^{(\rho)} \sim H$), sigue la *ley de multiplicación en* $P_r[H]$:

$$(VI.) \quad (p^{(0)} h_1^{(1)} h_2^{(2)} \dots . h_r^{(r)})(q^{(0)} k_1^{(1)} k_2^{(2)} \dots . k_r^{(r)}) = (p\,q)^{(0)} (h_{\gamma_1} k_1)^{(1)} (h_{\gamma_2} k_2)^{(2)} \dots . (h_{\gamma_r} k_r)^{(r)}.$$

Esta fórmula enseña que en la multiplicación de dos permutaciones de $P_r[H]$, *las componentes respecto de* P_r *se mul-*

tiplican, pero no las otras componentes, sino que la componente del producto respecto de $H^{(\rho)}$, es igual a $(h_{\gamma\rho}\ k_\rho\ )^{(\rho)}$, es decir a la permutación correspondiente al producto de $h_{\gamma\rho}$ (y no de h_ρ) por k_ρ , en donde γ_ρ es la cifra en que la permutación q^{-1} permuta la cifra ρ (*).

§ 5. Observaciones generales sobre coronas.

a) La fórmula (VI.) aplicada al caso

$$p = q = \begin{pmatrix} 1 & 2 & 3 & \dots & r \\ 1 & 2 & 3 & \dots & r \end{pmatrix},$$

permite comprobar la exactitud de un teorema que ha sido establecido por Specht:

Las permutaciones de $P_r[H]$ *cuya componente respecto de* P_r *es igual a la identidad (o en otras palabras, las permutaciones que permutan sólo entre sí las variables de la primera fila, las de la segunda fila, etc., sin que haya una permutación de las filas del esquema (I.) entre sí) forman un subgrupo invariante* $E_r[H]$ *de* $P_r[H]$, *del orden* η^r, *e isomorfo al producto directo* $H^{(1)} \times H^{(2)} \times \dots \times H^{(r)}$.

Además rige el isomorfismo

$$\frac{P_r[H]}{E_r[H]} \sim P_r,$$

y por eso podemos enunciar el siguiente teorema más general:

Si P_r *posee un subgrupo* P'_r, *del orden* π' *y del índice* $\frac{\pi}{\pi'}$, *también* $P_r[H]$ *posee un subgrupo* $P'_r[H]$ *del mismo índice* $\frac{\pi}{\pi'}$ *(o del orden* $\pi' . \eta^r$*). Si* P'_r *es un subgrupo invariante de* P_r, *también la corona* $P'_r[H]$ *es un subgrupo invariante de la corona* $P_r[H]$.

(*) Ahí está la diferencia entre la corona $P_r[H]$ y el producto directo

$$P_r \times H^{(1)} \times H^{(2)} \times \dots \times H^{(r)};$$

pues. en el caso de un producto directo, se multiplicarían no sólo las componentes respecto de P_r , sino también las otras.

Ejemplo: El grupo simétrico S_m posee en el grupo alternado A_m un subgrupo invariante del índice 2; por eso, también la corona $S_m[S_n]$ (considerada en § 3, c) posee un subgrupo invariante del índice 2 en $A_m[S_n]$. Este último grupo se puede caracterizar como el conjunto de las permutaciones de $x_1, x_2, \ldots, x_{mn}$, que dejan invariante el polinomio

$$(x_1 x_2 \ldots x_n - x_{n+1} x_{n+2} \cdot \ldots \cdot x_{2n})$$

$$(x_1 x_2 \cdot \ldots \cdot x_n - x_{2n+1} x_{2n+2} \cdot \ldots \cdot x_{3n}) \cdot \ldots \cdot$$

$$(x_{(m-2)n+1} x_{(m-2)n+2} \cdot \ldots \cdot x_{(m-1)n} - x_{(m-1)n+1} x_{(m-1)n+2} \cdot \ldots \cdot x_{mn}).$$

b) Hasta ahora hemos considerado las coronas $P_r[H]$ como grupos de permutaciones, por ejemplo de las variables del esquema (I.); pero, ahora la fórmula (VI.) nos da también la posibilidad de comparar diferentes coronas y, eventualmente, constatar su isomorfismo como grupos *abstractos*.

Por ejemplo, si conocemos un grupo de permutaciones H' en s' variables que sea isomorfo al grupo de permutaciones H en s variables (pero $s' \neq s$), podemos formar, con un grupo de permutaciones P_r en r variables, las coronas $P_r[H]$ y $P_r[H']$, que serán diferentes como grupos de permutaciones (lo serán ya en virtud del distinto número de variables de permutar que es respectivamente igual a rs y rs'). Pero la fórmula (VI.), en que no entra por nada la cuestión si las componentes $h_\mu^{(r)}$ y $k_\rho^{(\rho)}$ sean permutaciones en s o s' variables, enseña que hay isomorfismo entre $P_r[H]$ y $P_r[H']$, considerando las dos coronas como grupos abstractos:

$$P_r[H] \sim P_r[H'], \text{ cuando } H \sim H'.$$

Ejemplo: Designemos por $R_6^{(S_3)}$ la representación del grupo S_3 por permutaciones «regulares» en 6 variables (*); la corona $S_2[R_6^{(S_3)}]$ será un grupo de permutaciones del orden 72

(*) Quiere decir que representamos dos elementos (de órdenes 2 y 3 respectivamente) que engendran el grupo abstracto S_3, por las siguientes permutaciones en 6 cifras:

$$\begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 4\,6\,5\,1\,3\,2 \end{pmatrix} \text{ respectivamente } \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,3\,1\,5\,6\,4 \end{pmatrix}$$

en 12 variables, pero, como grupo abstracto, isomorfo a la corona $S_2[S_3]$, grupo de permutaciones en 6 variables.

c) En cambio, *si* $r \neq t$ *y* $\eta\,(= \textit{orden de } H) > 1$, *no hay nunca isomorfismo entre las coronas* $P_r[H]$ *y* $Q_t[H]$, *aunque* P_r *y* Q_t *sean dos grupos de permutaciones (respectivamente en* r *y* t *variables) isomorfos entre sí.*

Demostración: No puede haber isomorfismo, porque el orden de $Q^t[H]$, $\pi\,\eta^t$, es distinto del orden de $P_r[H]$, $\pi\,\eta^r$ (por ser $r \neq t$ y $\eta > 1$).

Ejemplo: $R_6^{(S_3)}[S_2]$ del orden $6 \cdot 2^6 = 384$ no es isomorfo a $S_3[S_2]$, grupo del orden $6 \cdot 2^3 = 48$.

d) El teorema que acabamos de demostrar enseña que el concepto de corona *no* es un concepto de la teoría *abstracta* de grupos, como lo sería, por ejemplo, el de producto directo (siendo

$$G \times H \sim G' \times H',$$

cuando

$$G \sim G' \text{ y } H \sim H').$$

Así, con dos grupos abstractos G y H se pueden formar diferentes (y no isomorfas) coronas: $G_{r_1}[H]$, $G_{r_2}[H]$, $G_{r_3}[H]$, ..., tomando varias representaciones del mismo grupo abstracto G por permutaciones (distintas por el número de las variables de permutar) (**). Si se deseara conseguir que hubiese solamente *una* corona $G[H]$ para dos grupos *abstractos* G y H, sería menester elegir una representación de G por permutaciones, entre todas posibles; tomando, por ejemplo, la representación de G por permutaciones regulares, llegaríamos (como ya observé en el § 1), al «producto» $G \# H$ de Scholz (Lit. 8). De lo contrario, el concepto de corona es sólo un concepto «semi-abstracto», perteneciendo por la mitad al campo de los grupos de permutaciones. Según mi opinión, en eso hay que ver una ventaja; pues, de esta manera dos repre-

(**) Naturalmente, se podrían formar también coronas del tipo $H_{s_1}[G]$, $H_{s_2}[G]$,... Cabe observar que para coronas no vale una "ley conmutativa" (como para productos directos: $G \times H \sim H \times G$); por lo general, las dos coronas $G_r[H_s]$ y $H_s[G_r]$ serán grupos distintos (y no isomorfos).

sentaciones G_{r_1} y G_{r_2} del mismo grupo abstracto G por permutaciones conducen, por lo general, a dos coronas $G_{r_1}[H]$ y $G_{r_2}[H]$ diferentes (es decir no isomorfas entre sí).

e) Sin embargo, se obtienen casos interesantes de coronas sólo cuando estas últimas resultan ser grupos *transitivos* de permutaciones. A este respecto, se podría fácilmente demostrar el siguiente teorema:

Para que el grupo de permutaciones $P_r[H]$ *sea transitivo en sus* rs *variables es necesario y suficiente que los dos grupos de permutaciones* P_r *y* H *sean transitivos en sus* r *(resp.* s*) variables.*

f) Está claro que el grupo de permutaciones $P_r[H]$ es siempre *imprimitivo*; los campos de imprimitividad son formados por las filas horizontales del esquema (I.).

§ 6. *Subgrupos* $P_r[H; J]$ *de una corona.*

Pasamos ahora a la consideración de ciertos subgrupos interesantes de una corona $P_r[H]$.

Ya en § 5 a) hemos conocido los subgrupos $P_r'[H]$, que corresponden unívocamente a los subgrupos P_r' de P_r.

Otros subgrupos de $P_r[H]$ se obtienen admitiendo, para las componentes respecto de $H^{(1)}, H^{(2)}, \ldots, H^{(r)}$, sólo permutaciones que (en los isomorfismos $H^{(\rho)} \sim H$) corresponden a un subgrupo H' de H (*).

Combinando los dos métodos indicados para la formación de subgrupos, obtendremos coronas del tipo $P'_r[H']$ como subgrupos de $P_r[H]$ (con P_r' subgrupo de P_r y H' subgrupo de H).

Pero, así como en el caso de un producto directo, los subgrupos más interesantes son los que no son más productos directos (**), también *las coronas poseen cierta clase más interesante de subgrupos* que (por lo general) no son más coronas (y que están en cierta analogía a los «productos subdirectos» estudiados por Remak en el caso de productos directos (**).

(*) Tomando para H' el subgrupo E del orden 1, obtendremos $P_r\ [E]$, el subgrupo (del orden π) de las permutaciones de $P_r\ [H]$ cuyas componentes — con excepción de la respecto de P_r, son todas iguales a la identidad.

(**) Véanse a este respecto las publicaciones de R. Remak sobre productos directos y sus subgrupos (Lit. 5 & 6).

Supongamos que el grupo H (del orden η) posea un subgrupo *invariante* J del orden e (y del índice $\gamma = \frac{\eta}{e}$). Dividimos los elementos de H en γ conjuntos de mód. e elementos, reuniendo en *un* conjunto los elementos que son entre sí congruentes mod. J (*). Eligiendo en cada conjunto un representante h_μ ($\mu = 1, 2, \ldots, \gamma$), obtenemos la siguiente descomposición de los elementos de H en los γ conjuntos:

$$H = Jh_1 + Jh_2 + \ldots + Jh_\gamma \tag{VII.}$$

En este desarrollo, siendo J un subgrupo *invariante* de H, se puede definir una multiplicación de los conjuntos mismos (**):

$$(Jh_\alpha)\,.\,(Jh_\beta) = Jh_{\rho(\alpha,\beta)} \tag{VIII.}$$

porque todos los productos de un elemento cualquiera de un determinado conjunto Jh_α con un elemento cualquiera de un conjunto Jh_β pertenecen a un mismo conjunto, cuyo «número» depende sólo de los números α y β.

Ahora construiremos en $P_r[H]$ un subgrupo $P_r[H;J]$ de la siguiente manera: Si $u = q^{(0)} k_1^{(1)} k_2^{(2)} \ldots k_r^{(r)}$ es una permutación de $P_r[H]$ y si a $k_1^{(1)}$ (la componente de u respecto de $H^{(1)}$) corresponde (en virtud del isomorfismo $H^{(1)} \sim H$) la permutación k_1 de H, determinamos el conjunto Jh_k en (VII.) al que pertenece dicho elemento k_1; u haga parte de $P_r[H;J]$ sólo si pertenecen al *mismo* conjunto Jh_k también todas las otras permutaciones $k_2, k_3, \ldots, k_r$ de H, que corresponden (en virtud de los isomorfismos $H^{(2)} \sim H$, $H^{(3)} \sim H$, $\ldots$, $H^{(r)} \sim H$) a las permutaciones $k_2^{(2)}, k_3^{(3)}, \ldots, k_r^{(r)}$ (que son las componentes de u respecto de $H^{(2)}, H^{(3)}, \ldots, H^{(r)}$).

En otras palabras, $P_r[H;J]$ comprende, por definición, sólo las permutaciones de $P_r[H]$ cuyas componentes respecto de $H^{(1)}, H^{(2)}, \ldots, H^{(r)}$ correspondan a elementos $k_1, k_2, \ldots, k_r$ de H que pertenezcan *todos* a un *mismo* conjunto Jh_k (o todos a Jh_1, o todos a Jh_2, etc.).

(*) Dos elementos h y k de H se llaman congruentes mód. J, cuando $h\,k^{-1}$ (el producto de h por el inverso de k) pertenece al subgrupo invariante J.

(**) Es la misma que da origen al grupo $\frac{H}{J}$.

El número de las permutaciones del tipo considerado es igual a

$$\pi\gamma e^r = \pi\eta\, e^{r-1} = \pi\frac{\eta^r}{\gamma^{r-1}};$$

hay que demostrar aún que ellas forman un grupo. Para eso, escribimos la ley de multiplicación (VI.) en $P_r[H]$ en la forma

$$\text{(VI.')}\quad (p^{(0)}\, k_1^{(1)} k_2^{(2)} \ldots . k_r^{(r)})(q^{(0)} l_1^{(1)} l_2^{(2)} \ldots . l_r^{(r)}) = (pq)^{(0)} (k_{\gamma_1} l_1)^{(1)} (k_{\gamma_2} l_2)^{(2)} \ldots . (k_{\gamma_r} l_r)^{(r)},$$

con

$$\text{(IV.')}\qquad q^{-1} = \begin{pmatrix} 1 & 2 & 3 & \ldots & r \\ \gamma_1 & \gamma_2 & \gamma_3 & \ldots & \gamma_r \end{pmatrix}$$

en donde se tratará, ahora, de dos permutaciones del tipo particular que estamos considerando: para los elementos $k_1, k_2, \ldots, k_r$ de H, que corresponden a las componentes $k_1^{(1)}, k_2^{(2)}, \ldots, k_r^{(r)}$, existe un conjunto Jh_α a que todos ellos pertenecen, y hay *un* conjunto Jh_β al que pertenecen todos los elementos $l_1, l_2, \ldots, l_r$ de H, que corresponden a las componentes $l_1^{(1)}, l_2^{(2)}, \ldots, l_r^{(r)}$. La fórmula (VI.') enseña que el producto de nuestras dos permutaciones tiene, respecto de $H^{(1)}, H^{(2)}, \ldots, H^{(r)}$, las componentes $(k_{\gamma_1} l_1)^{(1)}, (k\gamma_2 l_2)^{(2)}, \ldots, (k\gamma_r l_r)^{(r)}$. Los elementos correspondientes de H son los productos $k_{\gamma_1} l_1$, $k_{\gamma_2} l_2, \ldots, k\gamma_r l_r$, y como cada $k\gamma_\rho$ pertenece al conjunto Jh_α, y cada l_ρ al conjunto Jh_β, todos esos productos $k_{\gamma_1} l_1$, $k_{\gamma_2} l_2, \ldots, k\gamma_r l_r$ pertenecen a un *mismo* conjunto $Jh_{\rho(\alpha,\beta)}$, definido por (VIII.). Así hemos demostrado que el producto de dos permutaciones de $P_r[H;J]$ tiene la misma propiedad que caracteriza $P_r[H;J]$, o que $P_r[H;J]$ es un grupo:

Cada subgrupo invariante J *de* H, *del índice* $\gamma = \frac{\eta}{e}$, *da origen a un subgrupo* $P_r[H;J]$ *de la corona* $P_r[H]$, *que es del orden* $\pi\gamma e^r = \pi\gamma e^{r-1}$ *y comprende las permutaciones de* $P_r[H]$ *cuyas componentes respecto de* $H^{(1)}, H^{(2)}, \ldots, H^{(r)}$ *corresponden a* r *elementos de* H *que son congruentes entre sí mód.* J.

Ejemplo: Si d es un divisor de n, en la corona $C_m[C_n]$ del orden mn^m podemos formar el subgrupo $C_m[C_n; C_d]$ del orden mnd^{m-1}. Por ejemplo, el grupo $C_5[C_4]$ del orden $5 \cdot 4^5 = 5120$

(véase Fig. 2) posee el subgrupo $C_5[C_4; C_2]$ del orden $5 . 4 . 2^4 = 320$, cuyos elementos son rotaciones cualesquiera del pentágono, con sucesivas rotaciones de las 5 «ruedas» con ángulos que, simultáneamente para las 5 ruedas, son o un múltiplo *par* o un múltiplo *impar* de 90°.

Si H posee varios subgrupos invariantes $J, J', \ldots$, podemos por supuesto, formar varios subgrupos $P_r[H;J]$, $P_r[H;J']$, etc. de $P_r[H]$. Se demuestra fácilmente que $P_r[H;J']$ será un subgrupo de $P_r[H;J]$, si J' es un subgrupo de J.

Dos casos extremos se pueden presentar para $P_r[H;J]$: que J es igual al entero grupo H, y que $J = E$ (= subgrupo del orden 1) comprende sólo la identidad H. Evidentemente es $P_r[H;H] = P_r[H]$. Más interesante es el otro caso: $P_r[H;E]$ *es del orden* $\pi\eta$ *y comprende, por definición, las permutaciones de* $P_r[H]$ *que tienen la forma* $q^{(0)}\, k^{(1)}\, k^{(2)} \ldots k^{(r)}$, *en donde las componentes* $k^{(1)}, k^{(2)}, \ldots, k^{(r)}$ *respecto de* $H^{(1)}, H^{(2)}, \ldots, H^{(r)}$ *corresponden todos a un mismo elemento* k *de* H.

Formando el producto de dos permutaciones de dicho subgrupo $P_r[H;E]$, la ley de multiplicación (VI.') enseña que en este caso particular ($k_1 = k_2 = \ldots = k_r = k$; $l_1 = l_2 = \ldots = l_r = l$), se multiplican no sólo las componentes respecto de P_r, sino también las respecto de $H^{(1)}, H^{(2)}, \ldots, H^{(r)}$:

$$(p^{(0)}\, k^{(1)}\, k^{(2)} \ldots . k^{(r)}) . (q^{(0)}\, l^{(1)}\, l^{(2)} \ldots . l^{(r)}) =$$
$$(pq)^{(0)}\, (kl)^{(1)}\, (kl)^{(2)} \ldots . (kl)^{(r)}.$$

Además enseña esta fórmula (o también la fórmula (V.) del § 4) que los elementos $q^{(0)}$ del subgrupo $P_r[E]$ son conmutables con los elementos del tipo $k^{(1)}k^{(2)} \ldots . k^{(r)}$ (los que tienen la componente respecto de P_r igual a la identidad y las otras correspondientes a un mismo elemento de H). Como estos elementos forman un subgrupo del orden η, isomorfo a H, el subgrupo $P_r[H;E]$ es isomorfo al producto *directo* de $P_r[E]$ (o P_r) y H:

$$(IX.) \qquad P_r[H;E] \sim P_r \times H.$$

Ejemplo: En $S_3[S_2]$ — que es, según § 3, a), el grupo amplificado del octaedro — el subgrupo $S_3[S_2;E]$ será isomorfo al producto directo $S_3 \times S_2$. En la Fig. 1, este subgrupo es el

que deja invariante la recta que une el centro del triángulo *ABC* con el del triángulo *DEF*.

§ 7. El grupo $S_2[S_n; A_n]$ *del orden* $(n!)^2$.

Tomando $P_r = S_2$ (con $r=2$, $\pi=2$), $H = S_n$ (con $\eta = n!$) y $J = A_n$ (el grupo alternado, con $e = \frac{n!}{2}$ y $\gamma = 2$), como subgrupo $P_r[H;J]$ de la corona $P_r[H]$ obtenemos el subgrupo $S_2[S_n; A_n]$ de $S_2[S_n]$, que se puede caracterizar como el conjunto de las permutaciones en $2n$ variables $x_1, x_2, \ldots, x_{2n}$ que dejan invariante el polinomio:

$$\prod_{k<\lambda}(x_k - x_\lambda) \cdot \prod_{k<\lambda}(x_{n+k} - x_{n+\lambda}). \qquad (1 \leqq k < \lambda \leqq n)$$

Este grupo $S_2[S_n; A_n]$ ofrece un interés particular por tener el mismo orden $(n!)^2$ como un producto directo de dos grupos simétricos en n variables. Por eso se podría creer que $S_2[S_n; A_n]$ fuera isomorfo a un producto directo del tipo $T \times U$ con $T \sim U \sim S_n$. Pero, como demostraremos en este párrafo, hay isomorfismo sólo para $n=2$ y $n=3$; *ya para* $n=4$, *el grupo* $S_2[S_n; A_n]$ *no es isomorfo a* $S_n \times S_n$, sino de distinta estructura.

En el caso de $n=2$, siendo $A_2 = E$ del orden *1*, se trata del grupo $S_2[S_2; E]$ que, en virtud de la fórmula (IX.) del § 6, es isomorfo al producto directo $S_2 \times S_2$.

Para demostrar también el isomorfismo:

$$(X.) \qquad S_2[S_3; A_3] \sim S_3 \times S_3$$

conviene considerar los dos grupos como subgrupos de S_6, denotando las variables de permutar brevemente por las cifras de *1* a *6;* bastará indicar un automorfismo A del grupo S_6 que tenga la siguiente propiedad: A deja invariante la permutación

$$a = (1, 2)\,(4, 5),$$

pero transforma

$$b = (1,\ 5,\ 2,\ 6,\ 3,\ 4) = (1,4)(2,5)(3,6)\,.\,(4,5,6)$$

en

$$c = (2,3)(4,5,6)$$

y, por consiguiente, transforma el subgrupo $S_2[S_3; A_3]$, engendrado por a y b, en el subgrupo $S_3 \times S_3$, engendrado por a y c. Como dos subgrupos que son transformables por un automorfismo, son isomorfos entre sí, con la indicación del automorfismo A habremos demostrado la fórmula (X.).

Pues bien, un automorfismo A de S_6 que tiene las propiedades indicadas es el que transforma las permutaciones (*):

$$b = (1, 5, 2, 6, 3, 4)$$

y $$d = (1, 5)$$

en

$$b' = (2,3)(4,5,6) = c$$

y $$d' = (1,3)(2,6)(4,5);$$

con eso (**) queda demostrada la fórmula (X.).

Pasando al próximo caso: $n = 4$, demostraremos que $S_2[S_4; A_4]$ no es isomorfo al producto directo $S_4 \times S_4$, aunque el orden de los dos grupos sea el mismo: $(4!)^2 = 576$. Denotaremos las variables de $S_2[S_4; A_4]$ por las cifras de *1* a *8*; las permutaciones de $S_2[S_4; A_4]$ tendrán entonces la forma $p^{(0)}\, k_1^{(1)}\, k_2^{(2)}$, en donde $k_1^{(1)}$ y $k_2^{(2)}$ son, respectivamente, permutaciones de *1, 2, 3, 4* y *5, 6, 7, 8, ambas pares o ambas impares;* $p^{(0)}$ es o la identidad o la permutación $(1,5)(2,6)(3,7)(4,8)$.

¿Cuántas permutaciones de $S_2[S_4; A_4]$ tienen el orden *3*? Como las componentes de las permutaciones de $S_2[S_4]$ respecto de $P_r = S_2$ se multiplican en la multiplicación — véase la fórmula (VI.) — para un elemento de $S_2[S_4; A_4]$ que tenga el orden *3*, la componente respecto de $P_r = S_2$ no puede tener el orden 2 y por eso, debe ser la identidad. Así vemos que los elementos del orden *3* son:

(*) las que engendran ya todo el grupo simétrico S_6, de modo que A es, completamente definido por la indicación de las permutaciones b' y d' que corresponden a b y d.

(**) Siendo $c = b'$ por definición, basta demostrar que A deja invariante la permutación $a = (1, 2)(4, 5)$, lo que se puede averiguar por cálculo directo del elemento $(b'^{-1}\, d'\, b')^{-1}\, d'\, (b'^{-1}\, d'\, b')\,.\,(b'\, d'\, b'^{-1})^{-1}\, d'\, (b'\, d'\, b'^{-1})$ que corresponde (en virtud del automorfismo A) a

$$a = (b^{-1}\, d\, b)^{-1}\, d\, (b^{-1}\, d\, b)\,.\,(b\, d\, b^{-1})^{-1}\, d\, (b\, d\, b^{-1})\,.$$

los *8* ciclos del orden *3* en las primeras *4* variables: *(1, 2, 3), (1,3,2), (1,2,4), (1,4,2), (1,3,4), (1,4,3), (2,3,4), (2,4,3)*; los en las otras *4* variables: *(5,6,7), (5,7,6), (5,6,8), (5,8,6), (5,7,8), (5,8,7), (6,7,8), (6,8,7)*;
y además, los *64* productos de uno de los primeros *8* ciclos con uno de los segundos *8* ciclos; *no hay otros elementos del orden 3 en* $S_2[S_4; A_4]$.

Todos estos son también los elementos del orden *3* en el grupo $S_4 \times S_4$, formado por los productos de permutaciones cualesquiera en las cifras *1, 2, 3, 4* con permutaciones cualesquiera de *5, 6, 7, 8*.

¿Cómo se distribuyen estos *80* elementos del orden *3* en clases de elementos conjugados (*), sea en $S_2[S_4; A_4]$, sea en $S_4 \times S_4$? En $S_4 \times S_4$ tenemos *3* clases de elementos conjugados: una formada por los *8* ciclos: *(1,2,3), (1,3,2), (1,3,4)*, etc. otra formada por los *8* ciclos: *(5,6,7), (5,7,6), (5,7,8)*, etc. y una tercera formada por los 64 productos: *(1,2,3) (5,6,7), (1,2,3)(5,7,6), (1,3,2)(5,6,7)* etc.

Pero, *en* $S_2[S_4; A_4]$ *los* 16 *ciclos del orden* 3 *forman una única clase* de elementos conjugados; por ejemplo es:

$(1,2,4) = [(3,4)(5,6)]^{-1} . (1,2,3) . [(3,4)(5,6)]$ o $(5,6,7) = [(1,5)(2,6)(3,7)(4,8)]^{-1} . (1,2,3) . [(1,5)(2,6)(3,7)(4,8)]$, en donde $(3,4)(5,6)$ y $(1,5)(2,6)(3,7)(4,8)$ son permutaciones de $S_2[S_4; A_4]$.

Así vemos que en $S_2[S_4; A_4]$ existe una clase con *16* elementos conjugados del orden *3*, hecho que no se presenta en el grupo $S_4 \times S_4$, en donde las clases formadas por elementos de orden *3*, tienen o *8* o *64* elementos. Por eso, los dos grupos tienen una estructura diferente y *no puede haber isomorfismo entre ellos.*

De un modo más general, se puede demostrar que *para ningún valor de* $n \geqq 4$ *hay isomorfismo entre* $S_2[S_n; A_n]$ *y* $S_n \times S_n$; pues, en $S_2[S_n; A_n]$ todos los $4\binom{n}{3}$ ciclos del orden *3* forman una única clase de elementos conjugados, mientras en

(*) Dos elementos u y v de un grupo se llaman conjugados. si en el mismo grupo hay un elemento z tal que $z^{-1}uz = v$.

$S_n \times S_n$ no hay, entre los elementos del orden 3, ninguna clase con $4\binom{n}{3}$ elementos conjugados.

§ 8. *Las permutaciones que no alteran el valor de un determinante.*

Sea

$$D_n(a_{11},\ a_{12},\ \ldots,\ a_{nn}) = \begin{vmatrix} a_{11},\ a_{12},\ \ldots,\ a_{1n} \\ a_{21},\ a_{22},\ \ldots,\ a_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1},\ a_{n2},\ \ldots,\ a_{nn} \end{vmatrix}$$

el determinante formado con n^2 *variables independientes* a_{11}, a_{12}, ..., a_{nn}. ¿A cuáles permutaciones se pueden someter las variables $a_{k\lambda}$ sin alterar el valor del polinomio $D_n(a_{11},\ a_{12},\ \ldots,\ a_{nn})$?

Para $n=2$, por ejemplo, vemos que las 4 permutaciones:

$$\begin{pmatrix} a_{11}\,a_{12}\,a_{21}\,a_{22} \\ a_{11}\,a_{12}\,a_{21}\,a_{22} \end{pmatrix},\ \begin{pmatrix} a_{11}\,a_{12}\,a_{21}\,a_{22} \\ a_{11}\,a_{21}\,a_{12}\,a_{22} \end{pmatrix},\ \begin{pmatrix} a_{11}\,a_{12}\,a_{21}\,a_{22} \\ a_{22}\,a_{12}\,a_{21}\,a_{11} \end{pmatrix},\ \begin{pmatrix} a_{11}\,a_{12}\,a_{21}\,a_{22} \\ a_{22}\,a_{21}\,a_{12}\,a_{11} \end{pmatrix}$$

no alteran el valor del determinante $D_2(a_{11}, a_{12}, a_{21}, a_{22})$, siendo

$$\begin{vmatrix} a_{11}\,a_{12} \\ a_{21}\,a_{22} \end{vmatrix} = \begin{vmatrix} a_{11}\,a_{21} \\ a_{12}\,a_{22} \end{vmatrix} = \begin{vmatrix} a_{22}\,a_{12} \\ a_{21}\,a_{11} \end{vmatrix} = \begin{vmatrix} a_{22}\,a_{21} \\ a_{12}\,a_{11} \end{vmatrix},$$

y no hay más ques estas 4 permutaciones con la propiedad buscada; ellas forman un grupo abeliano, producto directo de dos grupos cíclicos del orden 2.

También para $n>2$, las permutaciones de las n^2 variables $a_{k\lambda}$ que dejan invariante el determinante $D_n(a_{11}, a_{12}, \ldots, a_{nn})$, evidentemente forman un grupo; demostraremos que este grupo es del orden $(n!)^2$ e isomorfo al grupo $S_2[S_n; A_n]$ considerado en el § 7.

Demostración: Cuando dos variables $a_{\alpha\beta}$ y $a_{\gamma\delta}$ no pertenecen a una misma fila (siendo $\alpha \neq \gamma$) ni a una misma columna (siendo, además, $\beta \neq \delta$) del determinante, en el desarrollo

$$D_n(a_{11}, a_{12}, \ldots, a_{nn}) = \Sigma \pm a_{1\alpha_1}\, a_{2\alpha_2}\, a_{3\alpha_3},\ \ldots\ .\ a_{n\alpha_n}$$

del determinante en una suma (y resta) de *n!* productos, existe por lo menos *un* producto que comprenda los dos factores $a_{\alpha\beta}$ y $a_{\gamma\delta}$; en cambio, cuando es $\alpha = \gamma$ o $\beta = \delta$, *ninguno* de dichos *n!* productos es divisible por el producto $a_{\alpha\beta}\, a_{\gamma\delta}$. Una permutación *p* de las variables $a_{k\lambda}$ que no altera el valor de su determinante, puede permutar esos *n!* productos sólo entre sí, y por consiguiente, la propiedad de dos variables de pertenecer a una misma línea (*) er invariante frente a la permutación *p*, o en otras palabras, cuando dos variables pertenecen a una misma fila o columna, también después de haber sometido a la permutación *p*, se encontrarán en una misma fila o columna.

Este razonamiento se puede fácilmente extender a *3, 4, ..., n* variables de una línea (fila o columna), demostrando que variables de una misma línea quedan variables de una línea (de la misma u otra). En otras palabras, una permutación *p* de las variables $a_{k\lambda}$ que no altera su determinante $D_n(a_{11}, a_{12}, \ldots, a_{nn})$, *produce una permutación de las* 2n *líneas del determinante entre sí, y más exactamente, una permutación («imprimitiva») o de las filas entre sí y de las columnas entre sí, o bien cambiándose las filas por columnas y éstas por aquéllas.*

Aun más, como cada elemento de un determinante está caracterizado unívocamente por el número de su fila y el de su columna, bastará indicar la descrita permutación de las líneas (filas y columnas) producida por *p*, para caracterizar completamente la permutación *p* misma. Así vemos que el grupo de las permutaciones de las variables $a_{k\lambda}$ que deja invariante su determinante, es isomorfo a un subgrupo del grupo de todas las permutaciones de las filas entre sí y de las columnas entre sí o de los cambios de filas por columnas y recíprocamente. Este grupo es una corona $S_2[S_n]$, considerando las filas y las columnas del determinante como las *2n* variables de permutar.

Nuestro grupo es un *subgrupo* de este grupo $S_2[S_n]$ (y no ya el grupo entero); pues, no todas las permutaciones descritas de filas y columnas dejan invariante el determinante, sino que hay unas que cambian el signo del determinante, dejando invariante sólo el cuadrado de $D_n(a_{11}, a_{12}, \ldots, a_{nn})$. Como cada permutación *impar* de las filas o columnas cambia

(*) La palabra "línea" designa indistintamente una fila o una columna.

el signo del determinante, para evitar un cambio del signo de $D_n(a_{11}, a_{12}, \ldots, a_{nn})$, o hay que limitarse a permutaciones *pares* de filas y columnas, o hay que combinar una permutación *impar* de las filas con una permutación *impar* de las columnas, y en ambos casos se puede hacer preceder un cambio de las filas por las columnas y de éstas por aquéllas (sin alterar su orden relativo). Pero, el conjunto de estas permutaciones forma justamente el subgrupo $S_2[S_n; A_n]$ de $S_2[S_n]$.

En resumen: *Las permutaciones de las* n^2 *variables* $a_{k\lambda}$ *que no alteran su determinante*

$$D_n(a_{11}, a_{12}, \ldots, a_{nn}) = \begin{vmatrix} a_{11} \ldots a_{1n} \\ \ldots\ldots\ldots \\ a_{n1} \ldots a_{nn} \end{vmatrix}$$

forman un grupo del orden $(n!)^2$, *isomorfo a* $S_2[S_n; A_n]$ *(pero, para* $n \geqq 4$, *no isomorfo a* $S_n \times S_n$). *Las permutaciones que dejan invariante el cuadrado* $\{D_n(a_{11}, a_{12}, \ldots, a_{nn})\}^2$, *forman un grupo del orden* $2(n!)^2$, *isomorfo a la corona* $S_2[S_n]$. *El isomorfismo resulta considerando las permutaciones de las filas y columnas de* $D_n(a_{11}, a_{12}, \ldots, a_{nn})$.

Por fin, se puede observar que las permutaciones de las n^2 variables $a_{k\lambda}$ que dejan invariante no sólo su determinante, sino también el producto $a_{11}\, a_{22}\, a_{33} \ldots\ldots a_{nn}$ de los elementos de la diagonal principal, forman el subgrupo $S_2[S_n; E]$ que es (en virtud de la fórmula (IX.) del § 6) isomorfo al producto directo $S_2 \times S_n$.

LITERATURA CITADA

1) R. FRUCHT: *Die Gruppe des Petersenschen Graphen und der Kantensysteme der regulären Polyeder.* Commentarii Mathematici Helvetici, vol. 9, fasc. 3 (1936/37).

2) R. FRUCHT: *Herstellung von Graphen mit vorgegebener abstrakter Gruppe.* Compositio Mathematica, vol. 6, fasc. 2 (1938).

3) B. NEUMANN: *Die Automorphismengruppe der freien Gruppen.* Math. Annalen, Bd. 107, Heft 3 (1932).

4) G. PÓLYA: *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen.* Acta mathematica, Bd. 68 (1937).

5) R. REMAK: *Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte.* Journal für die reine und angewandte Mathematik, Bd. 163, Heft 1 (1930).

6) R. REMAK: *Über die erzeugenden invarianten Untergruppen der subdirekten Darstellungen endlicher Gruppen.* Journal für die reine und angewandte Mathematik. Bd. 164, Heft 4 (1931).

7) A. SCHOLZ: *Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoisscher Gruppe.* Math. Zeitschrift, Bd. 30, Heft 3 (1929).

8) A. SCHOLZ: *Ein Beitrag zur Theorie der Zusammensetzung endlicher Gruppen.* Math. Zeitschrift, Bd. 32, Heft 2 (1930).

9) I. SCHUR: *Ein Beitrag zur elementaren Zahlentheorie.* Sitzungsberichte der Preussischen Akademie der Wissenschaften. Phys. - Math. Klasse. 1933. III.

10) W. SPECHT: *Eine Verallgemeinerung der symmetrischen Gruppe.* Schriften des mathematischen Seminars und des Instituts für angewandte Mathematik der Universität Berlin. Bd. I (1932).

11) W. SPECHT: *Eine Verallgemeinerung der Permutationsgruppen.* Math. Zeitschrift, Bd. 37, Heft 3 (1933).