ESTRUCTURAS ALGEBRAICAS III (GRUPOS FINITOS)

ESTRUCTURAS ALGEBRAICAS III
(GRUPOS FINITOS)

por
Horacio Hernán O'Brien
Facultad de Ciencias Exactas y
Naturales
Universidad de Buenos Aires
Buenos Aires, Argentina

Programa Regional de Desarrollo Científico y Tecnológico
Departamento de Asuntos Científicos
Secretaría General de la
Organización de los Estados Americanos
Washington, D.C. - 1973

Esta monografía ha sido preparada para su publicación en el Departamento de Asuntos Científicos de la Secretaría General de la Organización de los Estados Americanos.

Editora: Eva V. Chesneau

Asesor Técnico: Dr. Samuel Gitler
Centro de Investigación del IPN
México 14, D.F., México

A los lectores

El programa de monografías científicas es una faceta de la vasta labor de la Organización de los Estados Americanos, a cargo del Departamento de Asuntos Científicos de la Secretaría General de dicha Organización, a cuyo financiamiento contribuye en forma importante el Programa Regional de Desarrollo Científico y Tecnológico.

Concebido por los Jefes de Estado Americanos en su Reunión celebrada en Punta del Este, Uruguay, en 1967, y cristalizado en las deliberaciones y mandatos de la Quinta Reunión del Consejo Interamericano Cultural, llevada a cabo en Maracay, Venezuela, en 1968, el Programa Regional de Desarrollo Científico y Tecnológico es la expresión de las aspiraciones preconizadas por los Jefes de Estado Americanos en el sentido de poner la ciencia y la tecnología al servicio de los pueblos latinoamericanos.

Demostrando gran visión, tal altas autoridades reconocieron que la ciencia y la tecnología están transformando la estructura económica y social de muchas naciones y que, en esta hora, por ser instrumento indispensable de progreso en América Latina, necesitan un impulso sin precedentes.

El Programa Regional de Desarrollo Científico y Tecnológico es un complemento de los esfuerzos nacionales de los países latinoamericanos y se orienta hacia la adopción de medidas que permitan el fomento de la investigación, la enseñanza y la difusión de la ciencia y la tecnología; la formación y perfeccionamiento de personal científico; el intercambio de información, y la transferencia y adaptación a los países latinoamericanos del conocimiento y las tecnologías generadas en otras regiones.

En el cumplimiento de estas premisas fundamentales, el programa de monografías representa una contribución directa a la enseñanza de las ciencias en niveles educativos que abarcan importantísimos sectores de la población y, al mismo tiempo, propugna la difusión del saber científico.

La colección de monografías científicas consta de cuatro series, en español y portugués, sobre temas de física, química, biología y matemática. Desde sus comienzos, estas obras se destinaron a profesores y alumnos de ciencias de enseñanza secundaria y de los primeros años de la universitaria; de estos se tiene ya testimonio de su buena acogida.

Este prefacio brinda al Programa Regional de Desarrollo Científico y Tecnológico y a la Secretaría General de la Organización de los Estados Americanos la ocasión de agradecer al doctor Horacio Hernán O'Brien, autor de esta monografía, y a quienes tengan el interés y buena voluntad de contribuir a su divulgación.

enero de 1973

INDICE

1

PROPIEDADES ELEMENTALES

La primera parte de este capítulo se dedica a enumerar resultados elementales sobre la teoría de grupos, los cuales se suponen conocidos por el lector, y a establecer la notación y terminología que se utilizará en la monografía.

En particular, se asume que el lector está familiarizado con las nociones de "grupo", "subgrupo", "subgrupo invariante" y "grupo cociente" (Véanse las monografías Estructuras Algebraicas I y II publicadas en esta misma serie).

§1.1. GENERALIDADES

En todo lo que sigue, sea G un grupo, H un subgrupo y S un subconjunto de G. Denotaremos por $|S|$ el cardinal del conjunto S; en particular, $|H|$ = orden del subgrupo H; y por $|G:H|$, el cardinal del conjunto cociente G/H, que llamaremos *índice de* H *en* G.

Se tiene, por el teorema de Lagrange:

$$|G| = |H| \cdot |G:H|.$$

Con $\langle S \rangle$ indicaremos el subgrupo de G generado por S, el cual coincide con la intersección de la familia de todos los subgrupos de G que contienen el subconjunto S. Otra expresión posible es:

$$\langle S \rangle = \{s_1 s_2 \ldots s_n / n \geq 0, \quad s_i \in S \ \text{ó} \ s_i^{-1} \in S\}.$$

En particular, para cada $x \in G$, indicaremos con $\langle x \rangle$ el subgrupo $\langle \{x\} \rangle$, es decir, el subgrupo cíclico generado por el elemento x.

Para cada par de elementos $x, y \in G$, escribiremos $[x, y]$, y llamaremos *conmutador de* x *con* y al elemento de G: $xyx^{-1}y^{-1}$. Si $S' = \{[x, y]/x, y \in G\}$, entonces escribiremos $[G, G]$ para indicar el subgrupo $\langle S' \rangle$, y lo llamaremos *subgrupo conmutador*.

Dos elementos $x, y \in G$ conmutan si, y sólo si, $[x, y] = 1$; por lo tanto, G es abeliano si, y sólo si, $[G, G] = \{1\}$.

Si $G = \langle S \rangle$, entonces se dirá que S es un *sistema de generadores de* G; G es cíclico si, y sólo si, $G = \langle x \rangle$ para algún $x \in G$.

Vamos a designar con el símbolo 1 tanto el elemento neutro, como el subgrupo $\{1\}$ de G.

Si S_1 es también subconjunto de G, escribiremos SS_1 para indicar el subconjunto $\{ss_1/s \in S, s_1 \in S_1\}$. Para cada $x \in G$, indicaremos con

xS (Sx) el subconjunto $\{x\}S$ ($S\{x\}$). Para $x \in G$, el subconjunto xSx^{-1} lo llamaremos *conjugado de* S.

Denotaremos por $\langle \bar{S} \rangle$ el *subgrupo invariante generado por* S (mínimo subgrupo invariante de G que contiene a S). Si escribimos:

$$S' = \bigcup_{x \in G} xSx^{-1}$$

se tiene $\langle \bar{S} \rangle = \langle S' \rangle$.

Llamaremos *centralizador de* S *en* H al subgrupo de G:

$$C(S, H) = \{y \in H / yx = xy \quad (\forall\, x \in S)\}$$

y *centro de* H:

$$z(H) = C(H, H).$$

Se verifica que H es abeliano si, y sólo si, $z(H) = H$.

Llamaremos *normalizador de* S *en* H al sugrupo:

$$N(S, H) = \{y \in H / ySy^{-1} = S\}.$$

Se verifica siempre que $C(S, H) \subsetneq N(S, H)$.

2

El subconjunto S se dirá *invariante* en G si, y sólo si, coincide con todos sus conjugados (si, y sólo si, $G = N(S, G)$). Son ejemplos de subgrupos invariantes $[G, G]$, así como cualquier subgrupo $H_1 \subseteq z(G)$.

Un grupo $G \neq 1$ se dirá simple si, y sólo si, G no posee subgrupos invariantes no triviales ($\neq 1, \neq G$). Si H es un subgrupo invariante, designaremos también por G/H el grupo cociente.

Sea F otro grupo, un *morfismo* (u homomorfismo) es una aplicación $f: G \to F$ que satisface $f(xy) = f(x)\, f(y)$, para todo par de elementos $x, y \in G$. El *núcleo de f* es $\mathrm{Nuf} = \{x \in G / f(x) = 1\}$, que es siempre subgrupo invariante de G; en tanto que la *imagen* $\mathrm{Imf} = \{y \in F / \exists x \in G\ f(x) = y\}$ es, en general, sólo subgrupo de F.

Un *isomorfismo* es un morfismo f que satisface $\mathrm{Nuf} = 1$, $\mathrm{Imf} = F$. Este caso lo indicaremos con $G \simeq F$. Un isomorfismo de un grupo en sí mismo se llama *automorfismo* y el conjunto de todos los automorfismos de un grupo G se denota por Aut(G). Éste tiene, a su vez, una estructura natural de grupo respecto a la composición de aplicaciones.

Un subconjunto S, tal que $f(S) = S$ para todo $f \in \mathrm{Aut}(G)$, se denomina subconjunto característico de G.

Para cada $x \in G$, la aplicación $I_x: G \to G$, definida por $I_x(y) = xyx^{-1}$, es un automorfismo de G llamado *interior;* y la aplicación $I: G \to \mathrm{Aut}(G)$, dada por $I(x) = I_x$, es un morfismo cuyo núcleo es el centro de G e imagen Int(G) el *grupo de automorfismos interiores de* G. Todo subconjunto característico es invariante.

Un grupo G se dice *completo* si, y sólo si, I es un isomorfismo, es decir, $z(G) = 1$, $\mathrm{Int}(G) = \mathrm{Aut}(G)$. Se tienen los siguientes *teoremas de isomorfismo:*

i) si $f: G \to G'$ es un epimorfismo (morfismo sobre), entonces

$$G/_{\mathrm{Ker}\, f} \simeq G';$$

ii) si N es un subgrupo invariante de un grupo G, H es un subgrupo tal que $N \subseteq H$, entonces en el grupo cociente $G/_N$, el subgrupo $H/_N$ es invariante si, y sólo si, H es invariante en G, y en este caso:

$$G/_N \simeq \frac{G/_H}{H/_N};$$

iii) si H y N son subgrupos de G, N invariante, entonces $H \cap N$ es un subgrupo invariante en H, HN es un subgrupo de G, y además

$$HN/_N \simeq H/_{H \cap N}.$$

Si G y G' son grupos, el conjunto de todos los pares ordenados (x, x'), $x \in G$, $x' \in G'$ tiene estructura de grupo definiendo:

$$(x, x')(y, y') = (xx', yy') \qquad (x, y \in G;\ x', y' \in G').$$

Este grupo se denomina *producto directo (externo)* de G con G', y se denota por $G \times G'$ (en el caso de que G y G' sean grupos abelianos, escribiremos $G \oplus G'$). 3

Si H y N son subgrupos invariantes de un grupo G, tales que $H \cap N = 1$ y $G = HN$, entonces G es *producto directo (interno)* de H con N. Cuando esto ocurre, la aplicación $\varphi: H \times N \to G$, definida por $\varphi(h, n) = hn$, es un isomorfismo y recíprocamente. Vamos a utilizar la misma notación $G = H \times N$.

En lo que resta del capítulo daremos ejemplos de grupos con el objeto de facilitar la exposición posterior. Asimismo, plantearemos las nociones básicas de la teoría de grupos libres, lo que nos permitirá construir grupos a partir de sistemas de generadores y relaciones.

§1.2. EJEMPLOS

Ejemplo 1. El grupo aditivo de números enteros $\mathbf{Z}$, así como el grupo de raíces n-ésimas de la unidad en el cuerpo de los números complejos $\mathbf{C}_n$ (n natural) son ejemplos de grupos ya conocidos por el lector. Estos grupos poseen la propiedad adicional de ser *cíclicos:* en efecto, 1 es generador de $\mathbf{Z}$ (también lo es -1); los generadores en $\mathbf{C}_n$ son las llamadas raíces n-ésimas primitivas (véase Estructuras Algebraicas II).

El grupo $\mathbf{C}_n$ es isomorfo al grupo cociente $\mathbf{Z}_n = \mathbf{Z}/_{\langle n \rangle}$, llamado grupo de enteros módulo $n (n \in \mathbf{N})$.

Si $w \in \mathbf{C}_n$ es una raíz primitiva, la aplicación $\varphi: \mathbf{Z} \to \mathbf{C}_n$, definida por $\varphi(r) = w^r$, es un epimorfismo con núcleo $\mathrm{Nu}\,\varphi = \langle n \rangle$. Por el primer teorema de isomorfismo tenemos:

$$\mathbf{Z}_n = \mathbf{Z}/_{\mathrm{Nu}\,\xi} \simeq \mathbf{G}_n.$$

Los grupos mencionados "agotan" los grupos cíclicos en el siguiente sentido: si G es un grupo cíclico, entonces o bien $G \simeq \mathbf{Z}$, o bien $G \simeq \mathbf{Z}_n$ para algún $n \in \mathbf{N}$.

En efecto, si G es cíclico, existe $x \in G$ tal que $G = \langle x \rangle$; por lo tanto, la aplicación $\xi: \mathbf{Z} \to G$, definida por $\xi(r) = x^r$, es un epimorfismo. Si $\mathrm{Nu}\,\xi = \{0\}$, entonces ξ es un isomorfismo, por tanto $\mathbf{Z} \simeq G$; en caso contrario, $\mathrm{Nu}\,\xi = \langle m \rangle$ para algún $m \in \mathbf{N}$, y otra vez por el teorema de isomorfismo

$$\mathbf{Z}_n = \mathbf{Z}/_{\langle n \rangle} \simeq G.$$

Ejemplo 2. Grupos abelianos finitos. El teorema de estructura de grupos abelianos finitos[12] establece que: Si G es abeliano finito, existen enteros positivos únicos $n_1, \ldots, n_r$, tales que $n_{i+1} | n_i$, y además:

$$G \simeq \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus \ldots \oplus \mathbf{Z}_{n_r}.$$

Ejemplo 3. Grupo simétrico. Si X es un conjunto no vacío, el conjunto de la totalidad de aplicaciones biyectivas $\sigma: X \to X$ tiene estructura de grupo respecto a la composición de aplicaciones. Este grupo se denomina *grupo de transformaciones de* X (o *grupo simétrico de* X) y se denota por Trans(X) (o también S(X)) (cf. Estructuras Algebraicas I). Si $|X| > 2$, entonces el grupo es no abeliano. En efecto, sean $x, y, z \in X$, las aplicaciones definidas por:

4

$\sigma(x) = y$

$\sigma(y) = z$

$\sigma(z) = x$

$\sigma(w) = w$ (para $w \in X$ distinto de x, y, z)

$\sigma'(x) = y$

$\sigma'(y) = x$

$\sigma'(w) = w$ (para $w \in X$ distinto de x, y)

son biyecciones de X en X, y por lo tanto, elementos de Trans(X). Se verifica que

$$(\sigma \circ \sigma')(x) = \sigma(y) = z$$

$$(\sigma' \circ \sigma)(x) = \sigma'(y) = x$$

por lo tanto, $\sigma \circ \sigma' \neq \sigma' \circ \sigma$.

Si X e Y son dos conjuntos no vacíos coordinables, es decir, si existe $\sigma: X \to Y$ aplicación biyectiva, entonces $S(X) \simeq S(Y)$. En efecto, la aplicación $\tau: S(X) \to S(Y)$, definida por $\tau(\varepsilon) = \sigma \circ \varepsilon \circ \sigma^{-1}$, es un isomorfismo. (Dejamos al lector la verificación correspondiente.) Cuando X es el conjunto $\{1, 2, \ldots n\}$, escribimos $\mathbf{S}_n$ en vez de S(X). Este es un grupo de orden $n!$

Para cada elemento $\sigma \in \mathbf{S}_n$, ponemos $\sigma_i = \sigma(i)$, y utilizamos la notación $\begin{pmatrix} i \\ \sigma_i \end{pmatrix}$ para indicar el elemento σ. Por ejemplo, los $6 = 3!$ elementos de $\mathbf{S}_3$ son:

$$I = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right.$$
$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

A los elementos de $\mathbf{S}_n$ los denominaremos *permutaciones*.

Ejemplo 4. Grupos de congruencia de figuras geométricas. Por congruencia de una figura geométrica F se entiende todo movimiento rígido (que preserva distancias), que aplica F en sí mismo. Se define el producto $t_1 \circ t_2$ de dos congruencias t_1, t_2, como el movimiento resultante de la aplicación sucesiva de t_1 y t_2 (en este orden).

El movimiento $t_1 \circ t_2$ será una congruencia de la figura F, si t_1 y t_2 lo son. El conjunto de todas las congruencias de la figura F es un grupo respecto del producto antes definido, pues se satisface la propiedad asociativa, existe un movimiento nulo (elemento neutro), donde todos los puntos quedan fijos, y para cada congruencia, el movimiento inverso también es congruencia.

Congruencias de polígonos regulares

Consideremos un polígono regular de n lados, cuyos vértices designamos $A_1, A_2, \ldots, A_n$. Nos interesan aquellos movimientos del plano que llevan al polígono a coincidir consigo mismo. Estos aplican cada vértice en otro vértice, cada lado pasa a ocupar el lugar de otro, y el centro 0 del polígono queda fijo. 5

a) Son ejemplos de tales movimientos las rotaciones $r_k (0 \leq k < n)$ en un ángulo $\frac{2k\pi}{n}$ con centro en 0. La rotación r_k aplica el vértice A_1 en el A_{k+1}, el vértice A_2 en el A_{k+2} y así sucesivamente.

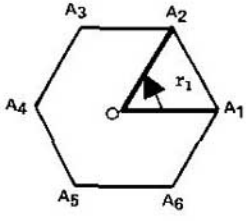


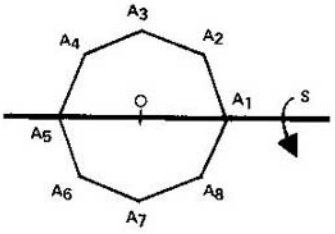
Fig. 1.

Ahora, el grupo de rotaciones $\{r_k / 0 \leq k < n\}$ es un grupo cíclico (pues $r_k = r_1^k$) de n elementos, y en consecuencia es isomorfo a $\mathbf{Z}_n$.

b) Sea G el grupo de congruencias del polígono regular de n lados. Las rotaciones $r_k (0 \leq k < n)$, consideradas en el caso anterior, son

elementos del grupo G, pero no son todos, puesto que, por ejemplo, la "simetría" s definida por

$$s: \begin{cases} A_1 \to A_1 \\ A_2 \to A_n \\ A_3 \to A_{n-1} \\ \cdots\cdots \\ \cdots\cdots \\ A_{n-1} \to A_3 \\ A_n \to A_2 \end{cases}$$



no es ninguna de las rotaciones r_k. Fig. 2.

Consideremos el subconjunto H_1 de G, que consiste en las congruencias en G que dejan fijo el vértice A_1. Si $t \in H_1$, entonces t deja fijo A_1. Como t es un movimiento que aplica vértice en vértice y conserva distancias, entonces el vértice A_2 debe aplicarse en A_n, o bien debe quedar fijo. En el primer caso, t aplica A_3 en A_{n-1}, y en el segundo, queda fijo. Prosiguiendo en esta forma con todos los vértices obtenemos:

$$t = \mathrm{Id}, \text{ o bien } t = s.$$

6 Por lo tanto se tiene $H_1 = \{\mathrm{Id}, s\}$.

Ahora estamos en condiciones de calcular todos los elementos de G. Sea $t \in G$ y supóngase que t aplica el vértice A_1 en el vértice $A_k (1 \le k \le n)$, por lo tanto $r_{k-1}^{-1} \circ t$ deja fijo A_1, y entonces $r_{k-1}^{-1} \circ t \in H_1$, y en consecuencia

$$t = r_{k-1}, \text{ o bien } t = r_{k-1} \circ s$$

lo cual prueba que todos los elementos del grupo G son de la forma r_k o bien $r_k \circ s$ para $1 \le k < n$. Todos estos elementos son distintos de acuerdo con el siguiente razonamiento:

Ya sabemos que si $k \neq k'$, $0 \le k, k' < n$, entonces $r_k \neq r_{k'}$. Análogamente, si $k \neq k'$, $0 \le k, k' < n$, debe tenerse $r_{k'} \circ s \neq r_k \circ s$, pues, en caso contrario, se tendría $r_k = r_{k'}$, lo que contradice lo anterior.

Por último, si $r_k = r_{k'} \circ s$, resultaría $s = r_{k-k'}$, es decir s sería una de las rotaciones r_t, que ya sabemos es imposible.

Como consecuencia de lo anterior, el grupo G consta de los $2n$ elementos r_k, $r_k \circ s (0 \le k < n)$ y puede generarse con los elementos r_1, s, es decir $G = \langle \{r_1, s\} \rangle$. Es inmediato que $r_1^n = s^2 = \mathrm{Id}$. Por otra parte, el elemento $r_1 \circ s$ es la aplicación

$$r_1 \circ s: \begin{cases} A_1 \to A_2 \\ A_2 \to A_1 \\ A_3 \to A_n \\ \cdots\cdots \\ \cdots\cdots \\ A_n \to A_3 \end{cases}$$

En consecuencia $(r_1 \circ s)^2 = \mathrm{Id}$. Por tanto, el grupo G de congruencias de un polígono regular es un grupo no abeliano de orden $2n$, generado por los elementos r_1 y s, que satisfacen

$$r_1^n = s^2 = (r_1 \circ s)^2 = \mathrm{Id}.$$

G se denomina *grupo diédrico* (o dihedral) y se denota por $\mathbf{D}_n$.

Ejemplo 5. Grupos de rotaciones de poliedros regulares. Los movimientos rígidos en el espacio que dejan fijo un punto dado constituyen un grupo: el grupo de rotaciones respecto de ese punto. Dado un poliedro regular de centro 0, la totalidad de rotaciones respecto de 0 que aplican al poliedro en sí mismo también forman un grupo: *el grupo de rotaciones del poliedro*, el cual es subgrupo del anterior.

a) Rotaciones del tetraedro regular

Consideremos un tetraedro regular con vértices A_1, A_2, A_3, A_4 Sean:

B_1 el baricentro de la cara $A_2\,A_3\,A_4$

B_2 el baricentro de la cara $A_1\,A_3\,A_4$

B_3 el baricentro de la cara $A_1\,A_2\,A_4$

B_4 el baricentro de la cara $A_1\,A_2\,A_3$

Sea G el grupo de rotaciones del tetraedro. Todo elemento de G induce una permutación de los vértices $A_1, \ldots, A_4$. Sea H el subgrupo de rotaciones que dejan fijo el vértice A_1; los elementos de H permutan entre sí los vértices A_2, A_3, A_4. Por lo tanto, si $s \in H$, entonces s debe ser una rotación respecto del eje $\overline{A_1 B_1}$ de ángulo:

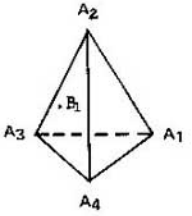


Fig. 3.

$$0, \frac{2\pi}{3}, \text{ o bien } \frac{4\pi}{3}.$$

Sean s_0, s_1, s_2 los elementos de H. Sean t_0, t_1, t_2, t_3 rotaciones fijas del tetraedro que aplican el vértice A_1 en A_1, A_2, A_3, A_4, respectivamente. Por ejemplo, $t_0 = I$; t_1, t_2 pueden tomarse como rotaciones respecto del eje $\overline{A_4 B_4}$ en un ángulo $\frac{2\pi}{3}$ y $\frac{4\pi}{3}$, y t_3 puede elegirse como una rotación respecto de $\overline{A_3 B_3}$ en un ángulo $\frac{2\pi}{3}$.

Vamos a demostrar que todo elemento de G se escribe unívocamente en la forma $t_i \circ s_j \; (0 \le i \le 3,\ 0 \le j \le 2)$. Sea $t \in G$, y supóngase que t aplique A_1 en $A_i \; (1 \le i \le 4)$, en este caso el elemento $t_{i-1}^{-1} \circ t$ deja fijo A_1, y en consecuencia es un elemento de H; sea s_j, entonces $t = t_{i-1} \circ s_j$ en forma única, como se quería verificar. Esto prueba que los elementos $t_i \circ s_j$ son *todos los elementos de* G; veamos que son distintos.

En efecto, si $t_i \circ s_j = t_{i_1} \circ s_{j_1}$, y dado que s_j y s_{j_1} dejan fijo A_1, y como t_i aplica A_1 en A_{i+1}, se tiene

$t_i \circ s_j$ aplica A_1 en A_{i+1}

$t_{i_1} \circ s_{j_1}$ aplica A_1 en $A_{i_1 j_1}$.

Por lo tanto, $i = i_1$, es decir $i_1 = i_{i_1}$, de donde resulta $s_j = s_{j_1}$.

En definitiva, el grupo G de rotaciones del tetraedro tiene por elementos a los $t_i \circ s_j$ y de ahí se deduce que G tiene orden 12.

b) Rotaciones del cubo.

Sea G el grupo de rotaciones del cubo. Numeremos sus vértices:

Sea A el baricentro de la cara 1485

A' el baricentro de la cara 2376

B el baricentro de la cara 1265

B' el baricentro de la cara 4378

C el baricentro de la cara 1432

C' el baricentro de la cara 5876

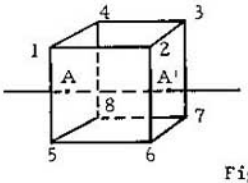


Fig. 4.

con rotaciones en ángulo 0, $\pi/2$, π, $3\pi/2$ respecto de los ejes AA', BB' y $\overline{CC'}$ se puede aplicar el vértice 1 en cualquier otro vértice, excepto en el vértice 7.

8

Si D es el punto medio de la arista $\overline{48}$, y si D' es el correspondiente de $\overline{26}$, la rotación en un ángulo π respecto del eje $\overline{DD'}$ lleva el vértice 1 al 7. Tenemos de tal modo que, para cada vértice i ($1 \le i \le 8$), existe un elemento $t_i \in G$ que aplica el vértice 1 en el i.

Si, como antes, H designa el subgrupo de G de los elementos que dejan fijo el vértice 1 (también entonces el 7), los elementos de H son rotaciones (con ángulo 0, $\frac{2}{3}\pi$ ó $\frac{4}{3}\pi$) respecto del eje $\overline{17}$. Por lo tanto, H tiene tres elementos s_0, s_1, s_2. Como en el caso del tetraedro, se verifica que los elementos $t_i \circ s_j$ ($1 \le i \le 8$, $0 \le j \le 2$) son distintos y que todo elemento de G tiene dicha forma. Se concluye, entonces, que G tiene exactamente $8 \cdot 3 = 24$ elementos.

Nota. Puede probarse que hay únicamente 5 poliedros regulares, a saber: tetraedro, hexaedro (cubo), octaedro, dodecaedro, icosaedro. Imaginemos que los centros de las caras del octaedro son los vértices de un cubo inscrito en él, y recíprocamente, en todo cubo se puede inscribir un octaedro cuyos vértices coincidan con los centros de las caras del cubo. Esto se expresa diciendo que los poliedros en cuestión *son duales*. También son duales el dodecaedro y el icosaedro (el tetraedro es dual de sí mismo). Es claro que poliedros duales tienen el mismo grupo de rotaciones, y por tanto, el grupo del octaedro también tiene 24 elementos. El grupo de rotaciones del dodecaedro (y por lo tanto del icosaedro) es un grupo de orden 60 y se obtiene en forma análoga a los grupos de rotaciones del cubo y del tetraedro.

Ejemplo 6. Si K es un cuerpo, el grupo general lineal, $GL(n,K)$, que consiste en la totalidad de matrices inversibles de grado n sobre el cuerpo K, constituye un ejemplo importante de grupo.

Sea $K = \mathbf{C}$ cuerpo de números complejos, $n = 2$. Consideremos $w \in \mathbf{G}_{2^n}$ $(n \geq 2)$ una raíz primitiva.

Al subgrupo $\mathbf{H}_n$ en $GL(2, \mathbf{C})$ generado por las matrices:

$$A = \begin{Vmatrix} w & 0 \\ 0 & w^{-1} \end{Vmatrix}; \qquad B = \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}$$

lo llamamos *grupo cuaterniónico generalizado.*

Vamos a calcular el orden de $\mathbf{H}_n$. Se verifica

$$A^i = \begin{Vmatrix} w^i & 0 \\ 0 & w^{-i} \end{Vmatrix} \qquad (i \geq 0)$$

y como w es una raíz primitiva de orden 2^n (es decir, $w^{2^n} = 1, w^{2^{n-1}} \neq 1$), se deduce que A tiene orden 2^n. Además, por la condición impuesta a w, $w^{2^{n-1}} = -1$, y entonces

$$A^{2^{n-1}} = \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix}$$

Por otra parte

$$B^2 = \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix} \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix} = A^{2^{n-1}}$$

$$B^4 = \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix} \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix} = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} = I$$

$$A^{-1}B = \begin{Vmatrix} w^{-1} & 0 \\ 0 & w \end{Vmatrix} \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & -w^{-1} \\ w & 0 \end{Vmatrix}$$

$$BA = \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix} \begin{Vmatrix} w & 0 \\ 0 & w^{-1} \end{Vmatrix} = \begin{Vmatrix} 0 & -w^{-1} \\ w & 0 \end{Vmatrix}$$

es decir, $A^{-1}B = BA$.

Esta última relación indica que todo elemento de $\mathbf{H}_n$ puede escribirse en la forma A^iB^j, pues aplicándola reiteradamente es posible lograr que en cada elemento de $\mathbf{H}_n$ toda potencia de A aparezca siempre a la izquierda de cada potencia de B. Como el orden de A es 2^n y el de B es 4, bastará considerar el caso $0 \leq i < 2^n$, $0 \leq j < 4$. Por último, como $B^2 = A^{2^{n-1}}$, reemplazando, será suficiente considerar $0 \leq j < 2$.

Deducimos de ello que $\mathbf{H}_n$ posee *a lo sumo* $2^n \cdot 2 = 2^{n+1}$ elementos. Pero los elementos de $\mathbf{H}_n$:

$$A^i = \begin{Vmatrix} w^i & 0 \\ 0 & w^{-i} \end{Vmatrix} \qquad (0 \leq i < 2^n)$$

$$A^iB = \begin{Vmatrix} w^i & 0 \\ 0 & w^{-i} \end{Vmatrix} \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & -w^i \\ w^{-i} & 0 \end{Vmatrix} \quad (0 \leq i < 2^n)$$

son distintos, y en consecuencia, el orden de H_s es exactamente 2^{m+1}.

Nota. Por último, como caso particular, cuando $m = 2$, se obtiene el llamado *grupo cuaterniónico*. Este grupo de orden 8 tiene la propiedad de que todos sus subgrupos son invariantes (es no abeliano!). Un grupo G con la propiedad de que todos sus subgrupos son invariantes se denomina *hamiltoniano*.

Un resultado clásico establece que todo grupo finito, no abeliano, hamiltoniano, es necesariamente isomorfo a alguno de los grupos del tipo

$$H_2$$
$$H_2 \times A$$
$$H_2 \times B$$
$$H_2 \times A \times B$$

donde A es grupo abeliano de orden impar y B es grupo abeliano en el cual todo elemento tiene orden 2.[3]

§1.3. GRUPOS LIBRES

10

Recuérdese que un grupo abeliano libre en el conjunto X es un grupo F con la siguiente propiedad (véase Estructuras Algebraicas II): Si G es un grupo abeliano y $f : X \to G$ una aplicación, entonces f se puede extender a un único homomorfismo de F en G. Como consecuencia de esto es inmediato que todo grupo abeliano G es cociente de un grupo abeliano libre. Es natural entonces pretender generalizar la idea de grupos abelianos libres a grupos arbitrarios: éstos serán los llamados *grupos libres*.

Sea X un conjunto no vacío (finito o infinito), cuyos elementos vamos a denotar por $x_\alpha^{+1}, x_\beta^{+1}, x_\gamma^{+1} \ldots$. Construimos un nuevo conjunto X^{-1} (disconjunto de X) en correspondencia biyectiva con X, a cuyos elementos llamaremos $x_\alpha^{-1}, x_\beta^{-1}, x_\gamma^{-1} \ldots$.

Una expresión

$$w = x_{a_1}^{\varepsilon_1} x_{a_2}^{\varepsilon_2} \ldots x_{a_n}^{\varepsilon_n} \quad (\varepsilon_i = \pm 1, i = 1 \ldots n) \qquad (*)$$

esto es, un sistema ordenado de un número finito de símbolos x_α^{+1} ó x_α^{-1} (donde cada símbolo que interviene en la expresión puede estar repetido) es llamado *una palabra*.

Si en la expresión (*) ningún símbolo x_α^{+1} está próximo a su símbolo *asociado*, x_α^{-1}, diremos entonces que w es una *palabra reducida*.

Son ejemplos de palabras:

$$x_\alpha^{+1} x_\beta^{-1} x_\alpha^{+1} x_\alpha^{+1} x_\gamma^{-1} x_\alpha^{-1}$$
$$x_\beta^{+1} x_\beta^{+1} x_\alpha^{-1} x_\gamma^{+1} x_\gamma^{+1} x_\beta^{-1}$$
$$x_\alpha^{+1} x_\beta^{-1} x_\beta^{+1} x_\alpha^{-1} x_\alpha^{+1} .$$

Las dos primeras son palabras reducidas en tanto que la tercera no. El número n en (*) se llama la *longitud de la palabra reducida* w, y se denota por $l(w)$.

Para cada conjunto X no vacío se pueden construir palabras reducidas de longitud arbitraria. Palabras reducidas de longitud 1, son exactamente los símbolos x_α^{+1} y x_α^{-1}.

Consideraremos también como palabra la expresión vacía, w_0, la cual no contiene símbolos, y escribiremos $l(w_0) = 0$.

El conjunto de todas las palabras reducidas que pueden ser escritas con la aludida colección de símbolos es un grupo con la siguiente definición de producto: Supongamos dadas dos palabras reducidas:

$$w_1 = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n} \qquad (\varepsilon_i = \pm 1,\ i = 1 \dots n)$$
$$w_2 = x_{\beta_1}^{\delta_1} x_{\beta_2}^{\delta_2} \dots x_{\beta_m}^{\delta_m} \qquad (\delta_j = \pm 1;\ j = 1 \dots m)$$

Para definir el producto $w_1 \cdot w_2$, escribimos w_2 inmediatamente después de w_1. Si la expresión resultante

$$x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n} \cdot x_{\beta_1}^{\delta_1} x_{\beta_2}^{\delta_2} \dots x_{\beta_m}^{\delta_m} \qquad (**)$$

es una palabra reducida (esto es, si los símbolos $x_{\alpha_n}, x_{\beta_1}$ son distintos, o bien son iguales, pero tienen el mismo exponente), (**) es, por definición, el producto $w_1 \cdot w_2$. En caso contrario, es necesario primero efectuar *cancelaciones*, es decir, eliminar sucesivamente en (**) pares de símbolos próximos con exponentes opuestos hasta obtener una palabra reducida. Por cierto que puede ocurrir que al efectuar estas cancelaciones se eliminen todos los símbolos de uno de los factores w_1, w_2, o bien de ambos (resultando la palabra w_0).

Veamos algunos ejemplos. Sean las palabras:

$$w_1 = x_\alpha^{+1} x_\beta^{-1} x_\alpha^{+1} x_\alpha^{+1} x_\beta^{+1}$$
$$w_2 = x_\beta^{-1} x_\alpha^{-1} x_\beta^{-1} x_\beta^{-1} x_\alpha^{+1}$$
$$w_3 = x_\alpha^{-1} x_\beta^{+1} x_\beta^{+1} x_\alpha^{+1} x_\beta^{+1}$$

por lo tanto

$$w_2 \cdot w_1 = x_\beta^{-1} x_\alpha^{-1} x_\beta^{-1} x_\beta^{-1} x_\alpha^{+1} x_\alpha^{+1} x_\beta^{-1} x_\alpha^{+1} x_\alpha^{+1} x_\beta^{+1}$$
$$w_1 \cdot w_2 = x_\alpha^{+1} x_\beta^{-1} x_\alpha^{+1} x_\beta^{-1} x_\beta^{-1} x_\alpha^{+1}$$
$$w_2 \cdot w_3 = w_0$$

El elemento neutro para este producto es claramente la palabra vacía, w_0; y el inverso de la palabra reducida

$$w = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n} \qquad (\varepsilon_i = \pm 1,\ i = 1 \dots n)$$

es la palabra

$$w^{-1} = x_{\alpha_n}^{-\varepsilon_n} \dots x_{\alpha_2}^{-\varepsilon_2} x_{\alpha_1}^{-\varepsilon_1}.$$

En particular, la inversa de x_α^{+1} es x_α^{-1}.

La demostración de la ley asociativa para el producto de palabras definidas arriba es un poco compleja debido a las cancelaciones que tal vez sería necesario efectuar. Vamos a probar la igualdad

$$w_1(w_2 \cdot w_3) = (w_1 \cdot w_2)w_3 \qquad (*)$$

por inducción en la longitud de w_2.

Observe primero el lector que la igualdad anterior se satisface trivialmente si alguna de las palabras es la vacía, w_0; basta suponerlas no vacías.

1. Consideremos primero el caso $l(w_2) = 1$, es decir $w_2 = x_a^{\varepsilon}$ ($\varepsilon = \pm 1$).

i) Si el último símbolo de w_1 y el primero de w_3 son ambos distintos de $x_a^{-\varepsilon}$, entonces en el cálculo de (*) no hay necesidad de efectuar cancelaciones y la fórmula se verifica de inmediato.

ii) También (*) se verifica trivialmente cuando sólo uno de los dos símbolos citados es igual a $x_a^{-\varepsilon}$, porque en este caso, en alguno de los productos $w_1 \cdot w_2$, $w_2 \cdot w_3$ no es necesario efectuar cancelaciones.

iii) Finalmente, cuando ambos son iguales a $x_a^{-\varepsilon}$ se presenta la situación

$$w_1 = x_{\beta_1}^{\delta_1} \ldots x_{\beta_s}^{\delta_s} x_a^{-\varepsilon}$$
$$w_3 = x_a^{-\varepsilon} x_{\gamma_1}^{\eta_1} \ldots x_{\gamma_t}^{\eta_t}.$$

12

En este caso, la expresión

$$x_{\beta_1}^{\delta_1} \ldots x_{\beta_s}^{\delta_s} x_a^{-\varepsilon} x_{\gamma_1}^{\eta_1} \ldots x_{\gamma_t}^{\eta_t}$$

es una palabra reducida (puesto que w_1 y w_3 lo son), y ésta es igual a ambos miembros de (*).

2. Supongamos (*) válida respecto a palabras reducidas w_2 de longitud menor que n, y sea $n = l(w_2) \geq 2$. Si

$$w_2 = x_{a_1}^{\delta_1} x_{a_2}^{\delta_2} \ldots x_{a_{n-1}}^{\delta_{n-1}} x_{a_n}^{\delta_n}$$

ponemos

$$w_2' = x_{a_1}^{\delta_1} x_{a_2}^{\delta_2} \ldots x_{a_{n-1}}^{\delta_{n-1}}.$$

Entonces w_2' es palabra reducida (puesto que w_2 lo es), $l(w_2') < l(w_2)$, y además

$$w_2 = w_2' \cdot x_{a_n}^{\delta_n}.$$

En consecuencia, por la hipótesis inductiva

$$w_1(w_2 \cdot w_3) = w_1([w_2' \cdot x_{a_n}^{\delta_n}]w_3) = w_1(w_2'[x_{a_n}^{\delta_n} \cdot w_3]) = (w_1 \cdot w_2')[x_{a_n}^{\delta_n} \cdot w_3] =$$

$$= [(w_1 \cdot w_2')x_{a_n}^{\delta_n}] \cdot w_3 = [w_1(w_2' \cdot x_{a_n}^{\delta_n})] \cdot w_3 = (w_1 \cdot w_2)w_3$$

Estamos en condiciones de hablar ahora del grupo de palabras reducidas asociado al conjunto X, que denotamos por L(X) y llamamos *grupo libre*.

Claramente, L(X) está completamente determinado cuando se da el conjunto X; *y no depende de las propiedades particulares de los elementos de este conjunto.*

Definimos el *rango* de L(X), y denotamos por $r(L(X))$ el cardinal del conjunto X, es decir

$$r(L(X)) = |X|.$$

Es posible probar, por consideraciones elementales de la teoría de conjuntos, que un grupo libre de rango finito es numerable y el cardinal de un grupo libre de rango infinito es igual a su rango. Un grupo libre de rango 1 es a las claras un grupo cíclico infinito, y por lo tanto isomorfo al grupo aditivo de los números enteros, **Z**. Por otra parte, un grupo libre de rango mayor que 1 es no abeliano, pues si $\alpha \neq \beta$, los elementos $x_\alpha^{+1} \cdot x_\beta^{+1}$ y $x_\beta^{+1} \cdot x_\alpha^{+1}$ son distintos en el grupo. Toda palabra en L(X) es el producto de los símbolos que la constituyen. El conjunto X es, entonces, un sistema de generadores de L(X); y un tal sistema de generadores se denomina *sistema de generadores libre.*

En todo lo que sigue se reemplazará el término "palabra" por el de "elemento de un grupo libre" y éstos se escribirán como producto de potencias de los generadores; por ejemplo, pondremos $x_\alpha^3 \cdot x_\beta^{-1} \cdot x_\alpha \cdot x_\beta^2$ en vez de $x_\alpha^{+1} x_\alpha^{+1} x_\alpha^{+1} x_\beta^{-1} x_\alpha^{+1} x_\beta^{+1} \cdot x_\beta^{+1}$.

La propiedad clave de L(X) es la siguiente: 13

1.3.1. Si G es grupo y $f: X \to G$ es una aplicación, existe un único homomorfismo $F: L(X) \to G$ que extiende a f. En efecto, para que F extienda a f estamos obligados a definir:

$$F(x_\alpha) = f(x_\alpha)$$

y en consecuencia

$$F(x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n}) = f(x_{\alpha_1})^{\varepsilon_1} f(x_{\alpha_2})^{\varepsilon_2} \dots f(x_{\alpha_n})^{\varepsilon_n}.$$

Es inmediato que F es un homomorfismo. De aquí se deduce el siguiente resultado fundamental:

1.3.2. Todo grupo es isomorfo al cociente de un grupo libre. En efecto, sea G un grupo arbitrario y sea X un conjunto de generadores de G (el conjunto X puede consistir en la totalidad de los elementos de G).

Sea $L = L(X)$ el grupo libre generado por el conjunto X. La aplicación inclusión

$$i_X: X \to G, \quad i_X(x) = x$$

se extiende unívocamente a un homomorfismo $F: L(X) \to G$. Como X es un sistema de generadores de G, F es un epimorfismo, y por el primer teorema de isomorfismo, se tiene

$$L(X)/_H \simeq G$$

donde $H = \mathrm{Nu}F$, como se quería probar.

Obsérvese que los elementos de H son las expresiones formales $x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n}$ en L(X), tales que el producto en G: $x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n} = 1$.

De la demostración resulta también que todo grupo finitamente generado es cociente de un grupo libre de rango finito, o más exactamente, todo grupo que admite un sistema de generadores de n elementos es cociente de un grupo libre de rango n.

Sea G un grupo que suponemos representado como cociente de un grupo libre L por un subgrupo invariante H. Como antes, designamos con $x_\alpha, x_\beta, \ldots$ el conjunto de generadores libres de L; sus imágenes en G por el homomorfismo natural, con $a_\alpha, a_\beta, \ldots$, y el conjunto de todos estos elementos de G (los cuales no son necesariamente distintos), con M, que llamaremos sistema de generadores.

Supongamos que

$$x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \ldots x_{\alpha_n}^{\varepsilon_n} \qquad (\varepsilon_i \text{ son enteros})$$

sea un elemento de H.

A esto le corresponde en G la ecuación

$$a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \ldots a_{\alpha_n}^{\varepsilon_n} = 1$$

llamada *una relación entre los elementos* de M en G.

Elegimos en H un subconjunto R, tal que H sea el subgrupo invariante en L generado por R. El conjunto de relaciones correspondiente a los elementos de R se denomina *sistema de relaciones* del grupo G.

Todas las relaciones entre los elementos de M se pueden considerar como "consecuencia" del sistema de relaciones, puesto que todo elemento de H puede ser expresado como producto de potencias de elementos de R y sus conjugados.

El grupo G queda completamente determinado por un sistema de generadores y por un sistema de relaciones, ya que M determina el grupo libre L y R determina el subgrupo invariante H, y por lo tanto, el cociente L/H. Por lo demostrado en 2, se tiene:

1.3.3. Todo grupo G puede definirse por un sistema de generadores y relaciones. Por otra parte, dado un conjunto de símbolos M y cualquier conjunto C de palabras en L(M), grupo libre generado por M, existe un grupo G con un sistema de generadores M y un sistema de relaciones, los elementos de C igualados al elemento unidad. En efecto, basta tomar $G = L(M)/H$ donde H es el subgrupo invariante de L(M) generado por C.

1.3.4. **Teorema** (von Dyck). Si un grupo G está definido por un sistema de generadores y relaciones y otro grupo G' está dado por el mismo sistema de generadores y su sistema de relaciones contiene el sistema de relaciones de G, entonces G' es isomorfo a un grupo cociente de G. En efecto, si se representa a G y G' como cocientes del mismo grupo libre L, se tiene

$$G = L/H, \qquad G' = L/H'$$

y, entonces, $H \subseteq H'$. El resultado sigue del segundo teorema de isomorfismo. Veamos algunos ejemplos.

Ejemplo 1. Un grupo cíclico infinito se puede definir como el grupo generado por un elemento x, sin relaciones.

Nota. Obsérvese que no es aceptable como relación la trivial: $xx^{-1} = 1$, ¿por qué?

Ejemplo 2. Un grupo cíclico de orden n se puede definir como el grupo generado por un elemento x y una sola relación: $x^n = 1$.

Ejemplo 3. El grupo cíclico $\mathbf{Z}_6 = \mathbf{Z}_2 \oplus \mathbf{Z}_3$ se puede definir como el grupo generado por los elementos x e y, que satisfacen las relaciones:

$$x^2 = 1$$
$$y^3 = 1$$
$$xyx^{-1}y^{-1} = 1.$$

Ejemplo 4. El grupo diédrico $\mathbf{D}_n$ se puede presentar como el grupo generado por elementos x e y, que satisfacen las relaciones

$$x^n = 1$$
$$y^2 = 1$$
$(xy)^2 = 1$. En efecto, sea G dicho grupo.

Hemos visto en b) del Ejemplo 4 (pág. 7) que $\mathbf{D}_n$ es un grupo de orden $2n$ y que puede generarse por dos elementos que satisfacen las relaciones anteriores y, posiblemente, otras. Por el teorema de von Dyck se tiene: 15

$$\mathbf{D}_n \simeq G/H.$$

Para que $G \simeq \mathbf{D}_n$ basta con demostrar que $|G| \leq 2n = |\mathbf{D}_n|$. Para ello, adviértase que es posible escribir todo elemento de G en la forma

$$x^i y^j (0 \leq i < n, \quad 0 \leq j < 2) \qquad (*)$$

Como los elementos de G son palabras con los símbolos x e y, será suficiente verificar que todo producto del tipo yx^r se puede llevar a la for- (*). En efecto, de la última relación: $xyx = y^{-1} = y(y^2 = 1) \therefore yx = x^{-1}y = x^{n-1}y$, luego, inductivamente, $yx^r = x^{r(n-1)}y = x^{n-r}y$.

Por último, nótese que en virtud de las relaciones

$$x^n = 1$$
$$y^2 = 1$$

todo producto del tipo $x^s y^t$ se puede llevar a la forma (*).

Ejemplo 5. Hallar el orden del grupo G generado por los elementos a y b que satisfacen las relaciones:

$$a^7 = 1$$
$$b^3 = 1$$
$$a^{-1}b^{-1}a^r b = 1 \qquad (1 \leq r \leq 6).$$

Como en el caso del grupo diédrico, obsérvese que por la relación $ba = a^r b$, todo elemento de G puede escribirse en la forma:

$$a^i b^j (0 \le i \le 6, \quad 0 \le j \le 2).$$

De esto se deduce que el orden de G es a lo sumo 21, si bien depende del valor de r en la relación $a^r b = ba$.

Vemos que

$$ba^2 = a^r ba = a^{2r} b, \text{ y análogamente,}$$

$$ba^i = a^{ir} b.$$

También

$$b^2 a = b\, ba = ba^r b = a^{r^2} b^2$$

entonces

$$b^2 a^i = a^{ir^2} b^2.$$

Luego

$$b^3 a = ba^{r^2} b^2 = a^{r^3} b^3$$

como $b^3 = 1$, se tiene $a^{r^3} = a$.

Como también $a^7 = 1$, para $r = 3, 5, 6$ se obtiene $a = 1$, y el grupo G es simplemente el grupo cíclico $\mathbf{Z}_3$ generado por b. Si $r = 1$, el elemento $ba = ab$ tiene orden 21 y así $G = \mathbf{Z}_{21}$. En los casos $r = 2, 4$, se obtienen grupos no abelianos de orden 21.

Ejemplo 6. El grupo cuaterniónico generalizado H_n se puede presentar como el grupo G generado por los elementos a y b, que satisfacen las relaciones

$$a^{2^n} = 1$$

$$aba b^{-1} = 1$$

$$a^{2^{n-1}} \cdot b^{-2} = 1.$$

En efecto, de la segunda relación se deduce que $ba = a^{-1}b$, y de la tercera que $b^2 = a^{2^{n-1}}$, por lo tanto $b^4 = 1$.

En el Ejemplo 6 (pág. 9) vimos que $|H_n| = 2^{n+1}$, y por el teorema de von Dyck debe tenerse

$$2^{n+1} = |H_n| \le |G|.$$

Para demostrar que son isomorfos, basta con comprobar que $|G| \le 2^{n+1}$. Esta demostración es la misma que la efectuada en el aludido Ejemplo 6 para probar que $|H_n| \le 2^{n+1}$.

§1.4. PRODUCTO SEMIDIRECTO

Sabemos que un grupo G es producto directo interno de dos subgrupos invariantes H_1, H_2 si, y sólo si,

i) $H_1 \cap H_2 = 1$

ii) $H_1 . H_2 = G$.

Una generalización natural de esta situación es suponer que sólo uno de los subgrupos es invariante. Diremos, entonces, que un grupo G es *producto semidirecto del subgrupo* H_1 *por el subgrupo* H_2 si, y sólo si,

i) H_1 es invariante en G

ii) $H_1 \cap H_2 = 1$

iii) $H_1 \cdot H_2 = G$

en este caso escribimos $G = H_1 \underset{s.d.}{\times} H_2$.

Es claro que todo producto directo es producto semidirecto, pero la recíproca no es necesariamente válida. Veamos un ejemplo

Sea $G = \mathbf{S}_3$ el grupo simétrico de orden $3! = 6$. Consideramos los elementos:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Se verifica de inmediato que

$$f^3 = 1, \quad g^2 = 1$$

y así:

$$H_1 = \langle f \rangle = \{1, f, f^2\}$$

$$H_2 = \langle g \rangle = \{1, g\}.$$

Además, por cálculo directo, resulta

$$gfg^{-1} = gfg = f^2$$

en tanto que

$$fgf^{-1} = fgf^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \notin H_2$$

por tanto, H_1 es invariante en $\mathbf{S}_3$, pero H_2 no lo es. Por razones de orden, $H_1 \cdot H_2 = \mathbf{S}_3$, $H_1 \cap H_2 = 1$ y así $\mathbf{S}_3 = H_1 \underset{s.d.}{\times} H_2$, pero $\mathbf{S}_3 \neq H_2 \underset{s.d.}{\times} H_1$.

Vamos a explicar ahora un método de construcción de productos semidirectos. Sean K y Q grupos y sea $\Phi: Q \to \mathrm{Aut}(K)$ un morfismo. Sobre el conjunto $G = K \times Q$ de la totalidad de pares ordenados (k, q) $(k \in K,\ q \in Q)$ definimos una ley de composición en la siguiente forma:

$$(k, q)(k', q') = (k\Phi(q)(k'), qq').$$

Para dicha ley de composición se afirma que G es un grupo.

i) Asociatividad:

$$\begin{aligned}
&[(k, q)(k', q')](k'', q'') = (k\Phi(q)(k'), qq')(k'', q'') = \\
&= (k\Phi(q)(k')\Phi(qq')(k''), qq'q'') = (k\Phi(q)(k')\Phi(q)\Phi(q')(k'')), qq'q'') = \\
&= (k\Phi(q)(k'\Phi(q')(k'')), qq'q'') = (k, q)(k'\Phi(q')(k''), q'q'') = \\
&= (k, q)[(k', q')(k'', q'')].
\end{aligned}$$

ii) Existencia de un elemento neutro. El elemento $(1,1)$, donde la primera componente es el elemento neutro de K y la segunda el de Q, satisface

$$(1,1)(k,q) = (1\,\varphi(1)(k), 1q) = (\mathrm{Id}(k), q) = (k,q)$$

y, análogamente, $(k,q)(1,1) = (k,q)$.

iii) Existencia de un inverso. Dado $(k,q) \in G$, el elemento $(\varphi(q^{-1})(k^{-1}), q^{-1})$ satisface

$$(k,q)(\varphi(q^{-1})(k^{-1}), q^{-1}) = (k\varphi(q)(\varphi(q^{-1})(k^{-1})), qq^{-1}) = (k\varphi(qq^{-1})(k^{-1}), 1) = (1,1)$$

y también

$$(\varphi(q^{-1})(k^{-1}), q^{-1})(k,q) = (1,1)$$

En virtud de i), ii), iii), G, con la ley de composición que se acaba de definir, es un grupo.

Ahora, los subconjuntos de G

$$K_1 = \{(k,1);\ k \in K\}$$

$$Q_1 = \{(1,q);\ q \in Q\}$$

son subgrupos isomorfos a K y Q, respectivamente, pues

$$(k,1)(k',1) = (k\varphi(1)(k'),1) = (kk',1);\ (k,1)^{-1} = (k^{-1},1)$$

$$(1,q)(1,q') = (1\,\varphi(q)(1), qq') = (1,qq');\ (1,q)^{-1} = (1,q^{-1}).$$

Esto permite identificar K con K_1 y Q con Q_1.

Afirmamos que $G = K \underset{\varphi}{\times} Q$.

i) K es invariante en G. En efecto,

$$(k',q')(k,1)(k',q')^{-1} = (k'\varphi(q')(k),q')(k',q')^{-1} =$$

$$= (k'\varphi(q')(k),q')(\varphi(q'^{-1})(k'^{-1}), q'^{-1}) =$$

$$= (k'\varphi(q')(k)\varphi(q')(\varphi(q'^{-1})(k'^{-1})),\ q'q'^{-1}) = (k'\varphi(q')(k)k'^{-1},1) \in K.$$

ii) Evidentemente, $K \cap Q = \{(1,1)\}$.

iii) Por último, $G = K \cdot Q$, ya que $(k,q) = (k,1)(1,q) \in K \cdot Q$.

Nota. Al grupo G construido anteriormente lo denotaremos por $K \times_\varphi Q$ a fin de poner en relieve el morfismo $\varphi: Q \to \mathrm{Aut}(K)$ que lo define.

Vamos a verificar ahora que todo producto semidirecto es del tipo anterior, o más precisamente, si $G = K \underset{id}{\times} Q$ para subgrupos K, Q de G, entonces existe un morfismo $\varphi: Q \to \mathrm{Aut}(K)$, tal que G es "naturalmente isomorfo" con $K \times_\varphi Q$.

Sea G en las condiciones anteriores, y definamos $\varphi: Q \to \mathrm{Aut}(K)$ en la forma $\varphi(q) = i_q|_K$ = automorfismo interior inducido por q restringido á l

subgrupo K. Observemos que por ser K un subgrupo invariante de G, Φ está bien definida. Aseguremos que la aplicación:

$$\alpha : K \times_{\Phi} Q \to G \text{ dada por } \alpha(k, q) = kq, \text{ es un isomorfismo:}$$

i) α es morfismo:

$$\alpha((k, q)(k', q')) = \alpha(k\Phi(q)(k'), qq') = \alpha(kqk'q^{-1}, qq') = kqk'q^{-1}qq' =$$
$$= (kq)(k'q') = \alpha(k, q) \cdot \alpha(k', q').$$

ii) α es inyectiva, puesto que si:

$$\alpha(k, q) = kq = 1, \text{ entonces}$$
$$k = q^{-1} \in K \cap Q = 1, \text{ por lo tanto } k = q = 1.$$

iii) Por último α es suryectiva, pues dado $x \in G = KQ$, existen $k \in K$ y $q \in Q$ con $x = kq = \alpha(k, q)$. En consecuencia, $G \simeq K \times_{\Phi} Q$, con lo que la afirmación está probada.

1.4.1. **Grupo diédrico generalizado.** Como ejemplo vamos a construir grupos que generalizan la idea de los grupos diédricos $\mathbf{D}_n$.

Sea A un grupo abeliano cualquiera (finito o infinito), y sea B un grupo cíclico de orden 2: $B = \{1, b\} \cdot (b^2 = 1)$. Consideremos: $\Phi : B \to$ $\to$ Aut(A), definida en la siguiente forma:

$$\Phi(1)(a) = a \qquad (\forall\ a \in A)$$
$$\Phi(b)(a) = a^{-1} \qquad (\forall\ a \in A).$$

Por ser A un grupo abeliano y tener el elemento $b \in B$ orden 2, se verifica de inmediato que Φ es un morfismo.

Sea D(A) el producto semidirecto $A \times_{\Phi} B$, llamado *grupo diédrico asociado al grupo* A. Observemos que la ley de composición en D(A) está dado por

$$(a, \alpha)(a', \alpha') = (a\Phi(\alpha)(a'), \alpha\alpha') =$$
$$= \begin{cases} (aa', \alpha\alpha') & (\text{si } \alpha = 1) \\ (aa'^{-1}, \alpha\alpha') & (\text{si } \alpha = b). \end{cases}$$

En el caso particular $A = \mathbf{Z}_n$, el grupo resultante es isomorfo a $\mathbf{D}_n$. Efectivamente, si $\mathbf{D}_n = \langle x, y / x^n = y^2 = (xy)^2 = 1 \rangle$, entonces la aplicación

$$\theta : \mathbf{Z}_n \times_{\Phi} B = D(\mathbf{Z}_n) \to \mathbf{D}_n$$

definida por

$$\theta(i, b) = x^i y$$
$$\theta(i, 1) = x^i, \qquad (0 \leq i < n) \quad \text{es un isomorfismo.}$$

Nota. En la definición del grupo D(A) interviene el grupo cíclico (de orden 2) B y, por lo tanto, parecería que el grupo diédrico asociado a

A depende de la elección de B. Esto no afecta dicha definición, pues las posibles elecciones de B dan grupos D(A) isomorfos, como se verá ahora. Más generalmente, vamos a probar que si A, B_1 y B_2 son grupos,

$$\Phi_1 : B_1 \to \mathrm{Aut}(A)$$

$$\Phi_2 : B_2 \to \mathrm{Aut}(A)$$

son morfismos, y si $\sigma : B_1 \to B_2$ es un isomorfismo que verifica $\Phi_2 \cdot \sigma = \Phi_1$, entonces $A \times_{\Phi_1} B_1 \simeq A \times_{\Phi_2} B_2$.

Para la demostración, definamos $\tau : A \times_{\Phi_1} B_1 \to A \times_{\Phi_2} B_2$ en la siguiente forma:

$$\tau(a, b) = (a, \sigma(b))$$

y verifiquemos que τ es un morfismo:

$$\tau((a, b)(a', b')) = \tau(a\,\Phi_1(b)(a'), bb') = (a\,\Phi_1(b)(a'), \sigma(bb'))$$

$$\tau(a, b) \cdot \tau(a', b') = (a, \sigma(b))(a', \sigma(b')) = (a\,\Phi_2(\sigma(b))(a'), \sigma(b)\sigma(b'))$$

como $\Phi_1 = \Phi_2 \circ \sigma$, y σ es morfismo, ambas expresiones coinciden. Además, τ es un monomorfismo, pues si $(1, 1) = \tau(a, b) = (a, \sigma(b))$, entonces $a = \sigma(b) = 1$, luego $a = b = 1$. Por ser σ un epimorfismo, así lo es τ. En nuestro caso particular, si B y B' son dos grupos cíclicos de orden 2 (suponemos que $B = \langle b \rangle$, $B' = \langle b' \rangle$) la aplicación $\sigma : B \to B'$, $\sigma(1) = 1$, $\sigma(b) = b'$ es un isomorfismo que satisface $\Phi = \Phi' \circ \sigma$, y por lo tanto, los grupos diédricos asociados son isomorfos.

Los métodos de construcción de productos semidirectos se utilizan con frecuencia para demostrar que existen grupos de una forma particular. Veamos otros ejemplos

1.4.2. Sean H y K grupos cíclicos de órdenes n y m, respectivamente; $H = \langle h \rangle$ y $K = \langle k \rangle$.

Sea r un entero, tal que

$$r^m \equiv 1 \,(n). \qquad (*)$$

Para cada elemento $k^i \in K (0 \leq i < m)$, se tiene la aplicación $\Phi(k^i) : H \to H$, dada por $\Phi(k^i)(x) = x^{r^i}$. $(x \in H)$.

Es claro que $\Phi(k^i)$ es un morfismo, pues

$$\Phi(k^i)(xy) = (xy)^{r^i} = x^{r^i} y^{r^i} = \Phi(k^i)(x)\,\Phi(k^i)(y)$$

Además, $\Phi(k^i)$ es un monomorfismo: si $x \in H$ es tal que $\Phi(k^i)(x) = x^{r^i} = 1$, entonces $|x| / r^i$, y por lo tanto existe un entero s tal que $r^i = |x| \cdot s$. Multiplicando ahora por r^{m-i}, se obtiene $r^m = |x| s r^{m-i}$, siendo $|x|$ un factor común de r^m y n. Por lo supuesto en $(*)$, $(r^m, n) = 1$, y entonces se debe tener $|x| = 1$, es decir $x = 1$. Pero como $\Phi(k^i)$ es un monomorfismo del grupo finito H, entonces es un automorfismo.

En consecuencia, queda definida una aplicación $\Phi : K \to \mathrm{Aut}(H)$. Veamos que Φ es un morfismo:

$$\Phi(k^i k^j)(x) = \Phi(k^{i+j})(x) = x^{r^{i+j}}, \text{ y también } \Phi(k^i) \circ \Phi(k^j)(x) =$$

$$= \Phi_i(k^j)(x^{r^i}) = (x^{r^i})^{r^j} = x^{r^{i+j}}$$

Existe entonces el producto semidirecto $G = H \times_\Phi K$. Ahora, en virtud de las identificaciones $h \to (h, 1)$, $k \to (1, k)$, el grupo G está generado por h, k, que satisfacen:

$$h^n = 1, \quad k^c = 1, \quad khk^{-1}h^{-r} = 1, \text{ para } r^a \equiv 1 (n). \qquad (**)$$

Como, por ser $khk^{-1} = h^r$, se deduce que todo elemento de G se escribe unívocamente en la forma $h^i k^j$ $0 \le i < n$, $0 \le j < m$, entonces G puede caracterizarse como el grupo generado por elementos h, k, que satisfacen las relaciones (**). Obsérvese, por último, que el grupo diétrico $\mathbf{D}_n$ es un caso particular de lo anterior ($m = 2$, $r = -1$).

1.4.3. Vamos a probar ahora que para todo primo impar p y para todo $n \ge 3$, existe un grupo no abeliano de orden p^n, tal que todos sus elementos tienen orden p. En principio, nótese que basta con resolver el problema para $n = 3$, y luego considerar el producto directo:

$$G \times \mathbf{Z}_p \times \ldots \times \mathbf{Z}_p \qquad (n - 3 \text{ copias de } \mathbf{Z}_p).$$

Sea el grupo $H = \mathbf{Z}_p \oplus \mathbf{Z}_p$. Es inmediato que la aplicación $\Phi : H \to H$ $\Phi(x) = (x, x + y)$ es un automorfismo.

Afirmamos que el orden de Φ es p:

$$\Phi^2(x, y) = \Phi(x, x + y) = (x, 2x + y)$$

y supuesto

$$\Phi^i(x, y) = (x, ix + y), \text{ se tiene}$$

$$\Phi^{i+1}(x, y) = \Phi(x, ix + y) = (x, x + ix + y) = (x, (i + 1)x + y).$$

Por lo tanto

$$\Phi^r(x, y) = (x, rx + y) \qquad (\forall\, r \ge 0).$$

Ahora, $\Phi^r = \mathrm{Id}_H$ si, y sólo si, $(x, y) = (x, rx + y)$ $\forall\, x, y \in \mathbf{Z}_p$) si, y sólo si, $rx = 0$ $(\forall\, x \in \mathbf{Z}_p)$. En consecuencia, el mínimo entero positivo r que satisface lo anterior es p, y éste es el orden de Φ. Por lo tanto, la aplicación $\Phi : \mathbf{Z}_p \to \mathrm{Aut}(H)$ $\Phi(r) = \Phi^r$ es un homomorfismo. Sea G el producto semidirecto asociado. Veamos que todo elemento en G tiene orden p. Se afirma que para $m \ge 1$, se tiene

$$[(x, y), z]^m = \left[(mx, \frac{m(m-1)}{2}xz + my), mz\right]$$

Si $m = 1$, no hay nada que demostrar; en el supuesto de que sea válida para el entero m:

$$[(x, y), z]^{m+1} = [(x, y), z][(x, y), z]^m = [(x, y), z]\left[(mx, \frac{m(m-1)}{2}xz + my), mz\right] =$$

$$= \left[(x, y) + \Phi^z(mx, \frac{m(m-1)}{2}xz + my), (m+1)z\right] = \left[(x, y) + (mx, zmx + \frac{m(m-1)}{2}xz + my), (m+1)z\right] =$$

$$= \left[((m+1)x, \frac{(m+1)m}{2}xz + (m+1)y), (m+1)z\right].$$

La fórmula está probada. Poniendo en ella $n = p$, resulta:

$$[(x, y), z]^p = [(px, \frac{p(p-1)}{2}xz + pyz), pz] = [(0, 0), 0]$$

pues $px = py = pz = 0$, y $\frac{p(p-1)}{2}xz = 0$, dado que p es impar. Por último, notamos que G es no abeliano, ya que

$$((1, 0), 0)((0, 0), 1) = ((1, 0), 1)$$

$$((0, 0), 1)((1, 0), 0) = ((1, 1), 1).$$

Nota. El resultado no es válido para $n = 1, 2$. En efecto, veremos en el próximo capítulo que grupos de orden p, p^2 son siempre abelianos. Tampoco es posible generalizar lo anterior al caso del primo $p = 2$, puesto que grupos en los que todo elemento tiene orden 2 son necesariamente abelianos:

$$x, y \in G \Rightarrow xxyy = x^2y^2 = 1 \cdot 1 = 1 = (xy)^2 = xyxy, \quad \therefore xy = yx.$$

1.4.4. Veamos que el grupo cuaterniónico generalizado, $\mathbf{H}_n$, no es producto semidirecto de subgrupos propios. Para establecer esto basta verificar que $\mathbf{H}_n$ posee un único elemento de orden 2, y que todo subgrupo propio de $\mathbf{H}_n$ tiene elementos de ese orden. En este caso, la intersección de subgrupos propios de $\mathbf{H}_n$ no estará nunca reducida al elemento unidad.

Por lo dicho en la § 4, podemos considerar $\mathbf{H}_n = \{A^i, A^iB / 0 \leq i < 2^n\}$ para

$$A^1 = \begin{Vmatrix} w^1 & 0 \\ 0 & w^{-1} \end{Vmatrix}; \quad A^1B = \begin{Vmatrix} 0 & -w^{-1} \\ w^{-1} & 0 \end{Vmatrix}$$

($w \in \mathbf{G}_{2^n}$ raíz primitiva). Se tiene ($0 \leq i < 2^n$)

$$(A^i)^2 = A^{2i} = \begin{Vmatrix} w^{2i} & 0 \\ 0 & w^{-2i} \end{Vmatrix} = I \text{ si, y sólo si, } i = 2^{n-1}$$

$$(A^1B)^2 = \begin{Vmatrix} 0 & -w^1 \\ w^{-1} & 0 \end{Vmatrix} \begin{Vmatrix} 0 & -w^1 \\ w^{-1} & 0 \end{Vmatrix} \neq I$$

por lo tanto, el único elemento de orden 2 del grupo H_n es $A^{2^{n-1}} = B^2$

La otra afirmación resulta de lo siguiente: Si H es un subgrupo propio de $\mathbf{H}_n$, como $H \neq 1$, existe $x \in H$, $x \neq 1$. Por el teorema de Lagrange resulta $1 \neq |x| / |\mathbf{H}_n| = 2^{n+1}$; por lo tanto $|x| = 2^i (0 < i \leq n+1)$, de donde $y = x^{2^{i-1}}$ es un elemento de H de orden 2.

Nota. Si A es anillo con unidad, el conjunto de unidades U(A), es un grupo. En el Apéndice I se ha calculado el grupo de unidades del anillo $\mathbf{Z}_n$. Consúltese otros ejemplos de grupos de unidades en Estructuras Algebraicas I y II.

2

G-ESPACIOS

Este capítulo se dedica al desarrollo de un tipo de técnica muy utilizada en el estudio de grupos, a saber la acción de grupos que operan sobre conjuntos. Por este método se obtiene la ecuación de clases (paso previo a los teoremas de Sylow) y algunas consecuencias (teorema de Cauchy, etc.), así como teoremas de caracterización de grupos de orden p^2, pq y p^3.

§ 2.1. G-ESPACIOS

Definición 2.1.1. Sea G un grupo y X un conjunto no vacío. Se dice que G *opera sobre* X si está dado un homomorfismo $\Phi: G \to S(X)$. En este caso se dice también que G *es un grupo de transformaciones de* X y que X *es un* G*-espacio*.

Para cada elemento $g \in G$ y cada $x \in X$ vamos a denotar por $g \cdot x$ el elemento $\Phi(g)(x)$. Como Φ es un morfismo, se satisface $\Phi(gg') = \Phi(g) \circ \Phi(g')$, por lo tanto

i) $g \cdot (g' \cdot x) = (gg') \cdot x \quad (g, g' \in G)(x \in X)$

ii) $1 \cdot x = x \quad$ (pues $\Phi(1) = Id_X$).

Concluimos que si G opera sobre X cabe definir una aplicación de $G \times X \to X$, $(g, x) \to g \cdot x$, que satisface i) y ii).

Recíprocamente, supóngase definida una aplicación $G \times X \to X$ denotada por $(g, x) \to g \cdot x$ de modo que se satisfagan i) y ii); veamos que G opera sobre X. Para cada $g \in G$ definimos $\Phi(g): X \to X$ en la forma natural: $\Phi(g)(x) = g \cdot x$. Veamos que si $g \in G$, $\Phi(g)$ es inyectiva. Si $x, y \in X$ son tales que $\Phi(g)(x) = \Phi(g)(y)$, es decir: $g \cdot x = g \cdot y$, entonces por la propiedad i) resulta:

$1 \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) = (g^{-1}g) \cdot y = 1 \cdot y$, y por la propiedad ii), $x = y$.

Veamos que $\Phi(g)$ es suryectiva. En efecto, dado $x \in X$, basta considerar el elemento de X: $y = g^{-1} \cdot x$, con lo cual, por i) y ii)

$$\Phi(g)(y) = g \cdot y = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = 1 \cdot x = x.$$

Por último, adviértase que Φ es un morfismo, pues por i)

$$\Phi(gg')(x) = (gg') \cdot x = g \cdot (g' \cdot x) = \Phi(g)(g' \cdot x) = \Phi(g)(\Phi(g')(x)) = (\Phi(g) \circ \Phi(g'))(x)$$

válido para todo $x \in X$, y en consecuencia

$$\Phi(gg') = \Phi(g) \circ \Phi(g').$$

Ejemplo 1. Si G es grupo y X conjunto no vacío, se define

$$g \cdot x = x \quad (g \in G)(x \in X).$$

En este caso, diremos que G opera *trivialmente* sobre X, puesto que corresponde a tomar $\Phi(g) = Id_X$, cualquiera que sea $g \in G$.

Ejemplo 2. Cualquiera que sea el conjunto no vacío X, el grupo S(X) opera naturalmente sobre X en la forma

$$g \cdot x = g(x) \quad (g \in S(X), x \in X).$$

Análogamente, cualquier subgrupo de S(X) opera sobre X de la misma forma. En particular, si H es un grupo, G = Aut(H) es un subgrupo de S(H), y tenemos una acción de G sobre H, como se ha indicado.

Ejemplo 3. Son de gran importancia las estructuras de G-espacio en las cuales X también es un grupo.

i) Si A es un grupo y G es un subgrupo de A, entonces definiendo

$$g \cdot a = ga \quad \text{(producto en el grupo A)}.$$

Se verifica inmediatamente que A es G-espacio. Diremos que G opera sobre A por *traslaciones a la izquierda*. En particular, G siempre opera sobre G por traslaciones a la izquierda.

ii) Sea, como en el caso anterior, A un grupo y G un subgrupo de A. Definimos, para $g \in G$, $a \in A$:

$$g \cdot a = ag \quad \text{(producto en el grupo A)}.$$

Se intenta averiguar bajo qué condiciones A es un G-espacio con dicha acción. Se sabe que para que esto ocurra es necesario y suficiente que se satisfagan

$$1 \cdot a = a$$
$$g \cdot (g' \cdot a) = (gg') \cdot a \qquad (g, g' \in G, a \in A)$$

condiciones que, por nuestra definición, se traducen en

$$a1 = a$$
$$ag'g = agg' \qquad (g, g' \in G, a \in A).$$

La primera de éstas se satisface siempre, pues $1 \in G \subset A$ es un elemento neutro en A. En cuanto a la segunda, puesto que debe ser válida para todo $a \in A$; en particular con $a = 1$

$$g'g = gg' \qquad (g, g' \in G)$$

esto es, el grupo G debe ser *abeliano*. Recíprocamente, supuesto G abeliano, las condiciones i) y ii) se satisfacen y por lo tanto las traslaciones a la derecha de un subgrupo G sobre un grupo A definen una estructura de G-especio, si y sólo si, G es abeliano.

iii) En cambio, A es siempre G-espacio con la acción

$$g \cdot a = ag^{-1} \qquad (g \in G,\ a \in A).$$

Esto es claro, la condición que es necesario que se cumpla, se traduce en

$$(g')^{-1}g^{-1} = (gg')^{-1} \qquad (g, g' \in G)$$

lo cual es inmediato, ya que G es un grupo.

iv) Si G es un grupo y H es un subgrupo invariante de G, entonces G opera sobre H en la forma

$$g \cdot h = ghg^{-1} \qquad (g \in G,\ h \in H).$$

En este caso, diremos que G opera sobre H *por conjugación*. Más generalmente, si H y K son subgrupos de un grupo G y si se verifica que $K \subseteq N(H, G)$ = normalizador de H en G, entonces K opera sobre H por conjugación. En particular, G opera siempre sobre sí mismo por conjugación, cualquiera que sea el grupo G.

Ejemplo 4. Sea G un grupo y H un subgrupo de G.

i) Sea X el *conjunto cociente*, $G/_H$, es decir $U \in X$ si, y sólo si, existe $x \in G$, tal que $U = \{xh; h \in H\} = xH$. Entonces G opera sobre X en la forma

$$g \cdot (xH) = gxH \qquad (g \in G,\ xH \in X).$$

Se dice en este caso que G *opera sobre* $G/_H$ *por traslación a la izquierda*. Análogamente, cualquiera que sea el subgrupo K de G, K también opera sobre $G/_H$ por traslación a la izquierda.

ii) Sea X la totalidad de subgrupos conjugados de H, es decir los elementos de X son todos los subgrupos de G de la forma xHx^{-1}, para algún $x \in G$. Entonces G (o cualquier subgrupo K de G) opera sobre X, poniendo

$$g \cdot (xHx^{-1}) = gxH(gx)^{-1} \qquad (g \in G,\ xHx^{-1} \in X).$$

En este caso se dice que G *opera sobre el conjunto de subgrupos conjugados de* H *por conjugación.*

Ejemplo 5. Si V es un espacio vectorial sobre un cuerpo K, consideramos

$X = V - \{0\}$ = totalidad de vectores no nulos en V

$G = K^*$ = grupo multiplicativo $K - \{0\}$

Entonces G opera sobre X mediante la ley de composición externa de V, es decir

$$k \cdot v = kv \qquad (k \in K^*,\ v \in X).$$

En este caso, decimos que K^* opera sobre $V - \{0\}$ por *homotecias*.

Sea G un grupo que opera sobre un conjunto X. Se define la siguiente relación en X:

$$x \sim y \text{ si, y sólo si, } \exists g \in G, \text{ con } g \cdot x = y.$$

Afirmamos que dicha relación es de equivalencia:

i) Como $1 \cdot x = x$, cualquiera que sea $x \in X$, se deduce que $x \sim x$ $(\forall x \in X)$.

ii) Sean $x, y \in X$ con $x \sim y$, por tanto $\exists g \in G$, con $g \cdot x = y$. Tenemos, entonces, $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1} \cdot g) \cdot x = 1 \cdot x = x$, es decir $y \sim x$.

iii) Sean $x, y, z \in G$ con $x \sim y$ e $y \sim z$, por tanto $g, g' \in G$, con $g \cdot x = y$, $g' \cdot y = z$. El elemento $g'g \in G$ satisface $(g'g) \cdot x = g' \cdot (g \cdot x) = g' \cdot y = z$, esto es, $x \sim z$.

Queda probado entonces que $\sim$ es relación de equivalencia y por tanto da lugar a una partición del conjunto X.

Definición 2.1.2. El conjunto cociente $X/_{\sim}$ (también denotado por X/G) se llama *espacio de órbitas de* G *en* X y sus elementos son las *órbitas de la representación* G. Si $x \in X$, designamos por 0_x la órbita correspondiente de elemento x, es decir $0_x = \{y \in X; x \sim y\}$.

Ejemplo 1. Si un grupo G opera trivialmente sobre un conjunto no vacío X, entonces todas las órbitas son puntuales, es decir cualquiera que sea $x \in X$, se tiene $0_x = \{x\}$.

Ejemplo 2. Si consideramos S_x que opera naturalmente sobre X, entonces existe una sola órbita, a saber: $0_x = X$, cualquiera que sea $x \in X$. En efecto, si X posee por lo menos dos elementos, entonces cualesquiera que sean $x, y \in X$ es posible definir una biyección $f \in S_x$ en la siguiente forma:

$$f(x) = y \qquad f(y) = x \qquad f(z) = z \quad (\text{si } z \in X,\ z \neq x,\ z \neq y)$$

lo cual muestra que $x \sim y$ cualesquiera que sean $x, y \in X$, y de ahí nuestra afirmación.

Ejemplo 3. Si un subgrupo G de un grupo A opera sobre éste por traslación a la izquierda, dado un elemento $a \in A$, se tiene que

$$0_a = \{b \in A / a \sim b\} = \{b \in A / g \in G \text{ con } g \cdot a = b\} =$$
$$= \{ga; g \in G\} = Ga.$$

En otras palabras, las órbitas en este caso son las coclases a la derecha del subgrupo G en el grupo A.

Ejemplo 4. Si V es K-espacio vectorial y consideramos $G = K^*$ que opera sobre $X = V - \{0\}$ por homotecias, la órbita 0_v de un vector $v \in X$, está dada por

$$0_v = \{kv; k \in K^*\}$$

lo cual no es otra cosa que la recta, en el espacio vectorial V, determinada por el vector v, privada del origen.

Al conjunto cociente $X/_G$ se le denomina *espacio proyectivo* deducido de V, y se le designa por $P(K, V)$.

Ejemplo 5. Sea $X = \{1, 2, 3, 4, 5, 6, 7\}$, y sea $f \in \mathbf{S}_7$ el elemento que satisface

$$f(1) = 5;\ f(2) = 7;\ f(3) = 4;\ f(4) = 1;\ f(5) = 3;\ f(6) = 6;\ f(7) = 2,$$

consideramos el grupo $G = (f) =$ un subgrupo generado por f en $\mathbf{S}_7$. Entonces G opera sobre X en forma natural, y las órbitas en este caso son

$$O_1 = O_5 = O_3 = O_4 = \{1, 3, 4, 5\}$$
$$O_2 = O_7 = \{2, 7\}$$
$$O_6 = \{6\}.$$

Definición 2.1.3. Sea G un grupo que opera sobre un conjunto X, y sea $x \in X$. Se denomina *estabilizador o grupo de isotropía de* $x \in X$ al subconjunto de G

$$G_x = \{g \in G / g \cdot x = x\}.$$

Proposición 2.1.1. Si G opera sobre X, $x \in X$, entonces G_x es un subgrupo de G.

Demostración. i) Como $1 \cdot x = x$, se tiene que $1 \in G_x$, y así $G_x \neq \emptyset$.

ii) Sean $g, h \in G_x$, por tanto $g \cdot x = x$, y también $h \cdot x = x$.

De esto último se deduce que

$$x = 1 \cdot x = (h^{-1}h) \cdot x = h^{-1} \cdot (h \cdot x) = h^{-1} \cdot x$$

y, consecuentemente

$$(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot x = x, \text{ por tanto } gh^{-1} \in G. \quad \blacktriangle$$

Proposición 2.1.2. Si G opera sobre X, y $\Phi : G \to S(X)$ es el morfismo inducido por dicha acción. Entonces, $\mathrm{Nu}\,\Phi = \bigcap_{x \in X} G_x$.

Demostración. Sea $g \in G$ se tiene que $g \in \mathrm{Nu}\,\Phi$ si, y sólo si, $\Phi(g) = \mathrm{Id}_X$ si, y sólo si, $\Phi(g)(x) = x$ cualquiera que sea $x \in X$ si, y sólo si, $g \cdot x = x$, para todo $x \in X$ si, y sólo si, $g \in G_x$, para todo $x \in X$ si, y sólo si, $g \in \bigcap_{x \in X} G_x$. $\blacktriangle$

Definición 2.1.4. Sea G un grupo que opera sobre un conjunto X, y sea $\Phi : G \to S(X)$ el morfismo inducido. Diremos que G opera *fielmente* si, y sólo si, $\mathrm{Nu}\,\Phi = \{1\}$. Esto equivale a decir que Φ es un monomorfismo, y por lo tanto, que G se identifica a un subgrupo de $S(X)$.

Proposición 2.1.3. (Teorema Cayley) Todo grupo G admite una representación fiel; es decir, para cada grupo G existe un conjunto X y una acción fiel de G sobre X.

Demostración. Tomemos $X = G$ y hagamos operar G sobre X por traslación a la izquierda. Veamos que la acción es fiel. Sea $x \in X$ y supongamos $g \in G_x$. Por lo tanto, $g \cdot x = x$, lo que equivale a decir que $gx = x$ (producto en el grupo G), de donde se deduce que $g = 1$, y de ello que $G_x = \{1\}$ cualquiera que sea $x \in X$.

Por la proposición 2.1.2 se tiene $\mathrm{Nu}\Phi = \cap G_x = \cap\{1\} = \{1\}$, como se quería probar. ▲

Ejemplo 1. Si X es un conjunto y se considera la acción obvia de $G = S(X)$ sobre X, entonces para cada elemento $x \in X$, el subgrupo $G_x =$ $=$ {totalidad de biyecciones que deja el elemento x fijo} se identifica naturalmente con el grupo simétrico $S(X - \{x\})$. La acción es claramente fiel.

Ejemplo 2. Si G es un grupo que opera por conjugación sobre un subgrupo invariante H, para $h \in H$, se tiene

$$G_h = \{g \in G / g \cdot h = h\} = \{g \in G / ghg^{-1} = h\} = C(h, G)$$

el centralizador del elemento h en el grupo G. En este caso, $\mathrm{Nu}\Phi = \bigcap_{h \in H} C(h, G) = C(H, G)$.

Ejemplo 3. Si G es un grupo, H un subgrupo y G opera sobre G/H por traslación a la izquierda, G_{xH} será la totalidad de elementos $g \in G$ que satisfacen:

$$g \cdot xH = xH$$

lo que equivale a decir que $g \in xHx^{-1}$; por lo tanto

$$G_{xH} = xHx^{-1} \cdot (\mathrm{Nu}\Phi = \bigcap_{x \in G/H} xHx^{-1}).$$

Ejemplo 4. Si G es un grupo que opera por conjugación sobre la totalidad de subgrupos conjugados de un subgrupo H, se tiene

$G_{xHx^{-1}} = N(xHx^{-1}, G)$, el normalizador de G del subgrupo xHx^{-1}.

Ejemplo 5. Si consideramos el conjunto $X = \{1, 2, 3, 4, 5, 6, 7\}$ y tomamos el elemento $f \in \mathbf{S}_7$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 4 & 1 & 3 & 6 & 2 \end{pmatrix}$$

y, como antes, hacemos operar $G = (f)$ sobre X en la forma obvia, tenemos $f^4 = \mathrm{Id}_X$, entonces $G \simeq \mathbf{Z}_4$, y así los estabilizadores de los elementos de X serán subgrupos cíclicos de 1, 2 ó 4 elementos.

El lector puede verificar fácilmente que

$$G_1 = G_3 = G_4 = G_5 = \{\mathrm{Id}\}$$
$$G_2 = G_7 = \{f^2, \mathrm{Id}\}$$
$$G_6 = G.$$

Además, es inmediato que dicha representación es fiel, pues basta comprobar (Prop. 2.1.2) que $\bigcap_{1 \le i \le 7} G_i = \{1\}$.

Ejemplo 6. Sea G un grupo que opera sobre X y $\Phi: G \to S(X)$ el morfismo inducido. Si $N = \mathrm{Nu}\Phi$, entonces existe un único homomorfismo $\Phi': G/N \to S(X)$, tal que si $\pi: G \to G/N$ es el epimorfismo canónico, se tiene $\Phi' \circ \pi = \Phi$.

Se afirma que $\mathrm{Nu}\phi' = 1$. En efecto, si $\phi'(x) = 1$, como π es suryectiva, existe $y \in G$ con $x = \pi(y) \therefore \phi(y) = (\phi' \circ \pi)(y) = \phi'(x) = 1$, es decir $y \in N \therefore x = \pi(y) = 1$.

En consecuencia, si G opera sobre X, $N = \mathrm{Nu}\phi$, entonces G/N opera fielmente sobre X.

Ejemplo 7. Sea A un grupo abeliano. Entonces $\mathbf{Z}_2 = G$ opera sobre A en la forma

$$\begin{aligned} \mathbf{Z}_2 &\xrightarrow{\phi} \mathrm{Aut}(A) \\ \phi(0)(a) &= a \quad (\forall a) \\ \phi(1)(a) &= -a \quad (\forall a), \text{ entonces} \end{aligned}$$

$G_a = G$ si, y sólo si, $a = -a$ si, y sólo si, $2a = 0$. En caso contrario, $G_a = 0$.

Consecuentemente $N = \bigcap_{a \in A} G_a \neq 0$ si, y sólo si, todos los elementos no triviales de A son de orden 2 si, y sólo si

A es $\mathbf{Z}_2$-espacio vectorial.

Ejemplo 8. Sea K un cuerpo, y $K[X_1, \ldots, X_n]$ el anillo de polinomios en n indeterminadas $X_1, \ldots, X_n$ con coeficientes en K. Entonces, $G = \mathbf{S}_n$ opera sobre $X = K[X_1, \ldots, X_n]$ en la forma:

$$t \cdot P(X_1, \ldots, X_n) = P(X_{t(1)}, \ldots, X_{t(n)})$$

i) Obsérvese que la acción de $\mathbf{S}_n$ sobre $K[X_1, \ldots, X_n]$ definida es fiel. En efecto, si $P_i = X_i (1 \leq i \leq n)$, se tiene $s \in G_{P_i}$ si, y sólo si, $s(i) = i$, por lo tanto, $\bigcap_{1 \leq i \leq n} G_{P_i} = 1$, y en consecuencia, $\mathrm{Nu}\phi = \bigcap G_P \subseteq \subseteq \bigcap_{1 \leq i \leq n} G_{P_i} = 1$. Veamos otros ejemplos:

ii) $P(X_1, \ldots, X_n) = X_1 + X_2 + \ldots + X_n$. Entonces

$$\begin{aligned} t \cdot P(X_1, \ldots, X_n) &= t \cdot (X_1 + \ldots X_n) = X_{t(1)} + X_{t(2)} + \ldots + X_{t(n)} = \\ &= X_1 + X_2 + \ldots + X_n = P(X_1, \ldots, X_n). \end{aligned}$$

Es decir, en este caso, $t \cdot P = P(\forall\, t \in \mathbf{S}_n)$, por lo tanto

$$\begin{aligned} G_P &= \mathbf{S}_n \\ 0_P &= \{P\}. \end{aligned}$$

iii) Sea $n = 4$, $P(X_1, X_2, X_3, X_4) = X_1X_2 + X_3X_4$. Entonces, tomando

$$t_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$t_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

resulta

$$t_1 \cdot P = X_1X_3 + X_2X_4$$

$$t_2 \cdot P = X_1X_4 + X_2X_3$$

y de ello resulta que

$$0_P = \{X_1X_2 + X_3X_4,\ X_1X_3 + X_2X_4,\ X_1X_4 + X_2X_3\}.$$

Para calcular el estabilizador G_P, se razona de la siguiente manera: Sea H el siguiente subgrupo de G_P

$$H = \{t \in G_P / t(1) = 1\}.$$

Para $t \in H$, se deduce que $t(2) = 2$. Entonces, t debe permutar a 3 y 4, o bien dejarlos fijos. Entonces

$$H = \{Id, f\} \qquad f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

Sean los elementos de G_P:

$$\varrho_1 = Id$$

$$\varrho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$\varrho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\varrho_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Se verifica de inmediato que

$$\varrho_1^2 = Id,\ \varrho_1(1) = i,\ \varrho_1(i) = 1$$

Sea, entonces, $\varrho \in G_P$; $\varrho(1) = i$ si, y sólo si, $(\varrho_1 \circ \varrho)(1) = 1$ si, y sólo si, $\varrho_1 \circ \varrho \in H$ si, y sólo si, $\varrho \in \varrho_1^{-1}H = \varrho_1 H$. En consecuencia

$$G_P = \bigcup_{1 \le i \le 4} \varrho_i H.$$

§ 2.2. TEOREMA IMPORTANTE

Teorema 2.2.1. Sea G un grupo que opera sobre un conjunto X. Entonces, si dos elementos de X pertenecen a la misma órbita, sus estabilizadores son subgrupos conjugados.

Demostración. Supongamos que $x, y \in X$ pertenecen a la misma órbita, y por tanto, $\varrho \cdot x = y$ para algún $\varrho \in G$. Adviértase entonces que $h \in G_y$ si, y sólo si, $h \cdot (\varrho \cdot x) = \varrho \cdot x$ si, y sólo si, $(\varrho^{-1}h\varrho) \cdot x = x$ si, y sólo si, $\varrho^{-1}h\varrho \in G_x$ si, y sólo si, $h \in \varrho G_x \varrho^{-1}$; por lo tanto, se tiene $G_y = \varrho G_x \varrho^{-1}$. ▲

Corolario 1. Los estabilizadores correspondientes a elementos de la misma órbita son siempre isomorfos.

Demostración. Por el teorema, son conjugados, y entonces isomorfos. ▲

Corolario 2. Si para algún $x \in X$ se tiene G_x invariante en G, entonces para cualquiera $y \in 0_x$ se tiene $G_y = G_x$.

Demostración. Por el teorema, G_y es conjugado de G_x, y como éste es invariante, deben coincidir. ▲

Corolario 3. Si G es grupo finito, entonces para cualquier $x \in X$ se tiene

$$|G| = |G_x| \cdot |0_x|$$

Demostración. Sean $g, h \in G$. Entonces, $g \cdot x = h \cdot x$ si, y sólo si, $(h^{-1}g) \cdot x = x$ si, y sólo si, $h^{-1}g \in G_x$ si, y sólo si, $hG_x = gG_x$. Por consiguiente, el número de elementos en la órbita 0_x es exactamente el número de coclases a la izquierda de G_x en G, y por el teorema de Lagrange, este último es $|G|/|G_x|$.

Aplicaciones

1. **Coclases dobles.** Sean H y K subgrupos de un grupo G. Sea X = = totalidad de coclases a la izquierda de H en G. K opera sobre X por traslaciones a la izquierda:

$$k \cdot xH = (kx) \cdot H.$$

La órbita de un elemento xH de X está dado por

$$0_{xH} = \{z \cdot xH; k \in K\} = \{kxH; k \in K\} = KxH$$

en tanto que el estabilizador de xH será

$$K_{xH} = \{k \in K / k \cdot xH = xH\} = \{k \in K / kxH = xH\} = \{k \in K / x^{-1}kx \in H\} =$$
$$= \{k \in K / k \in xHx^{-1}\} = K \cap xHx^{-1}.$$

Como X es una unión disjunta de órbitas, entonces G es una unión disjunta de *coclases dobles*, esto es, de conjuntos del tipo $KxH (x \in G)$. Supongamos ahora que H y K sean finitos. Se tiene entonces

$$|K| = |0_{xH}| \cdot |K_{xH}| = |0_{xH}| \cdot |K \cap xHx^{-1}| \qquad (*)$$

Ahora, como la órbita $0_{xH} = KxH$ posee $|0_{xH}|$ coclases distintas, se deduce que el subconjunto KxH posee $|H| \cdot |0_{xH}|$ elementos de G; en consecuencia, en (*):

$$|K| = \frac{|KxH|}{|H|} \cdot |K \cap xHx^{-1}|, \quad \text{es decir}$$

$$|KxH| = \frac{|K|}{|K \cap xHx^{-1}|} |H| = |H| |K : K \cap xHx^{-1}|.$$

Observe el lector que, a diferencia de lo que ocurre con coclases a la izquierda (o a la derecha) de un subgrupo H en G, las coclases dobles no son necesariamente coordinables entre sí, ni, en general, su cardinal divide el orden de G. Veamos un ejemplo:

Sea $G = S_3$, sus elementos son

$$\text{Id} = f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Entonces, considerando los subgrupos

$$H = \langle f_2 \rangle = \{\mathrm{Id}, f_2\}$$
$$K = \langle f_3 \rangle = \{\mathrm{Id}, f_3\}$$

se verifica inmediatamente que las coclases dobles son

$$H f_1 K = \{\mathrm{Id}, f_2, f_3, f_6\}$$
$$H f_4 K = \{f_4, f_5\}.$$

2. Orden $GL(n, K)$ (K cuerpo finito). Sea K un cuerpo (finito), $|K| = q$. Sea $GL(n, K)$ = grupo general lineal que consiste de la totalidad de matrices inversibles $n \times n$ sobre el cuerpo K. Se afirma que $|GL(n, K)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$. Inducción en n:

Si $n = 1$, $GL(1, K) = K - \{0\}$; luego, se tiene

$$|GL(n, K)| = |K - \{0\}| = q - 1.$$

Sea válido para n; sea V un K-espacio vectorial de dimensión $n + 1$; $\{v_1, \dots, v_{n+1}\}$ base de V.

32

Sabemos ya que $\mathrm{Aut}(V) \simeq GL(n + 1, K)$; isomorfismo que asocia a cada automorfismo f, su matriz en la base $\{v_1, \dots, v_{n+1}\}$. Ahora, $\mathrm{Aut}(V)$ opera sobre V en la forma natural

$$f \cdot v = f(v) \qquad (f \in \mathrm{Aut}(V),\ v \in V).$$

Dados dos vectores no nulos de V, siempre existe un automorfismo que aplica uno en el otro, y en consecuencia

$$0_v = V - \{0\} \qquad (v \in V - \{0\})$$
$$0_o = \{0\}.$$

En particular, $0_{v_1} = V - \{0\}$, por tanto $|0_{v_1}| = |V - \{0\}| = q^{n+1} - 1$. En cuanto al estabilizador de v_1

$$\mathrm{Aut}(V)_{v_1} = \{f \in \mathrm{Aut}(V) / f(v_1) = v_1\}$$

o equivalentemente (por medio de la identificación anterior) consta de las matrices de $GL(n + 1, K)$ de la forma

$$\begin{pmatrix} 1 & k_{12} & \dots & k_{1\,n+1} \\ 0 & K_{22} & \dots & k_{2\,n+1} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & k_{n+1\,2} & & k_{n+1\,n+1} \end{pmatrix}$$

Aquí, la submatriz inferior derecha de $n \times n$ debe pertenecer a $GL(n, K)$ y los elementos $k_{12}, \ldots, k_{1\,n+1}$ pueden variar libremente en K. Por lo tanto

$$|\mathrm{Aut}(V)_{v_1}| = |GL(n, K)| \cdot q^n$$

de donde

$$|GL(n+1, K)| = |0_{v_1}| \cdot |\mathrm{Aut}(V)_{v_1}| = (q^{n+1} - 1)((q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}))q^n =$$

$$= (q^{n+1} - 1)(q^{n+1} - q)(q^{n+1} - q^2) \ldots (q^{n+1} - q^n)$$

como se quería demostrar.

§ 2.3. ACCIÓN TRANSITIVA

Definición 2.3.5. Sea G un grupo que opera sobre un conjunto X, y sea k un número natural. Diremos que G *opera k-transitivamente*, $(k \leq |X|)$ si, y sólo si, para cualquier par de subconjuntos de k elementos $\{x_1, x_2, \ldots, x_k\} \subseteq X$; $\{y_1, y_2, \ldots, y_k\} \subseteq X$, existe $g \in G$, tal que $g \cdot x_i = y_i$ para $1 \leq i \leq k$.

Por supuesto que si G opera k-transitivamente $(k \in \mathbb{N})$, entonces opera k'-transitivamente cualquiera que sea $k' \leq k$; en particular, G opera transitivamente (es decir, 1-transitivamente), lo que equivale a decir que dos elementos de X siempre están en la misma órbita, esto es, sólo hay una órbita, a saber: X. Por lo tanto, si G es finito, el corolario 3 se traduce en

$$|G| = |G_x| \cdot |X|.$$

Corolario 4. Supongamos que G opera k-transitivamente sobre $X (k \geq 1)$, entonces:

i) Para $x, y \in G$, G_x y G_y son conjugados.

ii) Si, además, G es finito, entonces $|X|$ es finito y divide el orden de G.

iii) Si la acción de G es fiel, entonces el único subgrupo invariante de G contenido en algún estabilizador es el trivial.

Demostración. Las afirmaciones i) y ii) ya han sido demostradas antes. En cuanto a iii), si L es un subgrupo invariante de G y además $L \subseteq G_x$ para algún $x \in X$, entonces $L \subseteq G_y$ cualquiera que sea $y \in X$ (L es invariante y por i) todos los estabilizadores son conjugados), por lo tanto $L \subseteq \bigcap_{x \in X} G_x = \mathrm{Nu}\,\phi = \{1\}$ por ser la acción fiel. ▲

Ejemplo 1. S_n opera n-transitivamente sobre $X = \{1, 2, \ldots, n\}$, pues si $a_1, \ldots, a_n$ son todos distintos en X y también lo son $b_1, \ldots, b_n$, entonces $\{a_i\} = \{b_i\} = X$. Luego la aplicación $s : X \to X$, $s(a_i) = b_i$ es biyectiva, es decir $s \in S_n$.

Ejemplo 2. Sea V un K-espacio vectorial de dimensión mayor o igual a 2. Sea $P(K, V) = \frac{V - \{0\}}{K^*}$ el espacio proyectivo deducido de V. Entonces, Aut(V) opera 2-transitivamente sobre P(K, V). En efecto, probar esto equivale a verificar que dados dos pares de vectores lineal-

mente independientes en V: $\{v_1, v_2\}$, $\{w_1, w_2\}$, existe un automorfismo f de V, tal que $f(v_i) = w_i (i = 1, 2)$, y esto es inmediato. En cambio, Aut(V) no opera 3-transitivamente sobre P(K, V). Basta considerar $\{v_1, v_2, v_3\}$ linealmente independiente de a pares, pero que generen un subespacio de dimensión 2 y tomar $\{w_1, w_2, w_3\}$ linealmente independiente.

Ejemplo 3. El subgrupo de S_4, que consiste de los elementos: Id, $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$, $\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$ y $\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$ opera 1-transitivamente pero no 2-transitivamente sobre $X = \{1, 2, 3, 4\}$.

Ejemplo 4. Sea G el grupo de rotaciones del tetraedro regular, y A_1, A_2, A_3, A_4 los vértices del poliedro. Cada elemento $t \in G$ induce una permutación de los vértices

$$t = \begin{pmatrix} A_i \\ A_{t(i)} \end{pmatrix}.$$

En el ejemplo 5 del capítulo 1 se comprobó que G_1, el estabilizador del vértice A_1, consiste de los elementos

$$\text{Id};\ \begin{pmatrix}A_1&A_2&A_3&A_4\\A_1&A_3&A_4&A_2\end{pmatrix};\quad \begin{pmatrix}A_1&A_2&A_3&A_4\\A_1&A_4&A_2&A_3\end{pmatrix}$$

Así vemos que G_1 opera 1-transitivamente sobre los vértices A_2, A_3, A_4.

Análogamente, se verifica que cada estabilizador $G_i (1 \le i \le 4)$ opera 1-transitivamente sobre los vértices restantes. Teniendo en cuenta este hecho es fácil verificar que G opera 2-transitivamente sobre $\{A_i\}_{1 \le i \le 4}$. En efecto, dados $[A_i, A_j]$, $[A_k, A_r]$ con $i \neq j$, $k \neq r$, $1 \le i, j, k, r, \le 4$; se pueden presentar los siguientes casos:

i) Los índices i, j, k, r son todos distintos. En este caso, tomamos $s_1 \in G_i$ tal que $s_1(A_i) = A_r$, y también $s_2 \in G_r$ tal que $s_2(A_j) = A_k$. Luego el elemento de G, $t = s_2 \circ s_1$ satisface

$$t(A_i) = s_2 \circ s_1(A_i) = s_2(A_r) = A_k$$

$$t(A_j) = s_2 \circ s_1(A_j) = s_2(A_r) = A_r.$$

ii) $i = k$, $j \neq r$. Sea l el índice que falta. Consideramos $s_1 \in H_j$ tal que $s_1(A_i) = A_l$. Ahora bien siendo l, j, k, r distintos, por el caso i), podemos hallar $t \in G$ tal que

$$t(A_l) = A_k \quad \text{y} \quad t(A_j) = A_r.$$

En consecuencia, $t_1 = t \circ s_1$ verifica $t_1(A_i) = A_k$ $t_1(A_j) = A_r$. Los casos restantes son:

iii) $i = r$, $j \neq k$.

iv) $i = k$, $j = r$.

v) $i = r$, $j = k$.

verifique el lector que estos casos también se reducen al caso i).

En cambio, G no es 3-transitivo. En efecto, si existiera $t \in G$ tal que $t(A_1) = A_2$, $t(A_2) = A_1$ y $t(A_3) = A_3$, tendríamos $t(A_4) = A_4$.

Luego $t \in G_3 \cap G_4$; pero es inmediato que dicha intersección consiste sólo de la identidad, lo cual no satisface lo anterior. El grupo G de rotaciones del tetraedro, así como los grupos de rotaciones de los demás poliedros regulares (cubo e icosaedro) tienen propiedades muy interesantes, a saber: Si G opera sobre un conjunto X, se dice que X es un G-espacio de tipo k (k entero positivo) si, y sólo si, escribiendo $X_g = \{x \in X / g \cdot x = x\}$, $g \in G$, se tiene

i) $|X_g| = k$ para todo $g \in G$, $g \neq 1$.

ii) $\bigcap_{g \in G} X_g = \phi$.

Dado un grupo finito G, el mínimo entero positivo k, tal que G posee espacios X de tipo k, se denomina el tipo de G y se denota por $t(G)$. Cuando G no posea tales espacios, se define $t(G) = 0$.

Es válido el siguiente resultado: G es grupo finito; entonces $t(G) = 2$ si, y sólo si, G es isomorfo a alguno de los siguientes grupos:

i) grupo de rotaciones del tetraedro.

ii) grupo de rotaciones del cubo.

iii) grupo de rotaciones del icosaedro.

iv) grupo diédrico generalizado D(A), donde A es abeliano finito y su componente 2-primaria es cíclica.

Para demostrar este resultado, así como para caracterizar grupos finitos de tipo positivo, refiérase el lector a la obra citada en [33].

Ejemplo 5. Lo hecho antes para verificar que el grupo de rotaciones del tetraedro es 2-transitivo, es de aplicación general. En efecto, el lector puede probar con las mismas ideas expuestas el siguiente resultado: G es k-transitivo sobre $X (k \leq |X|)$ si, y sólo si

i) G es 1-transitivo, y además

ii) cada estabilizador G_x es $(k-1)$-transitivo sobre $X - \{x\}$.

Ejemplo 6. Si G opera sobre X, y si 0_x es una órbita, entonces G opera 1-transitivamente sobre 0_x.

Aplicaciones

1. Sea G un grupo finito, S un subconjunto no vacío de G, y $X = \{xSx^{-1} / x \in G\}$ = la totalidad de conjugados del subconjunto S en G.

G opera por conjugación en X, es decir

$$g \cdot (xSx^{-1}) = gxS(gx)^{-1} \qquad (g \in G,\ xSx^{-1} \in X).$$

Esta acción es claramente 1-transitiva. El estabilizador de S es $G_S = \{g \in G / gSg^{-1} = S\} = N(S, G)$. Entonces, tenemos

$$|G| = |G_S| \cdot |X| = |N(S, G)| \cdot |X|$$

de donde se deduce que

$$|X| = \text{número total de conjugados de S en G} = |G : N(S, G)|.$$

2. Sea G un grupo finito, y H, K subgrupos de G. Veamos que $|HK|\,|H \cap K| = |H| \cdot |K|$.

En efecto, consideremos el *conjunto* $X = HK$, y el grupo $G' = H \times K$. G' opera transitivamente sobre X definiendo

$$(h, k) \cdot x = hxk^{-1} \qquad (h \in H,\ k \in K,\ x \in HK).$$

Luego: $|H \times K| = |HK| \cdot |G_1|$, donde G_1 es el estabilizador en G del elemento $1 \in X$: $G_1 = \{(h, k)/h \cdot 1 \cdot k^{-1} = 1\} = \{(h, k)/h = k\}$, en consecuencia, $|G_1| = |H \cap K|$, y como $|H \times K| = |H| \cdot |K|$, reemplazando arriba resulta

$$|H|\,|K| = |HK|\,|H \cap K|.$$

Las dos propiedades siguientes resultan de lo demostrado:

i) $|H : H \cap K| \leq |G : K|$, y vale la igualdad si, y sólo si, $G = HK$.

ii) $|G : H \cap K| \leq |G : H| \cdot |G : K|$, y vale la igualdad si, y sólo si, $G = HK$.

En efecto, como

$$|HK| = \frac{|H|}{|H \cap K|}|K| = |H : H \cap K| \cdot |K| \qquad |G| = |G : K| \cdot |K|$$

y dado que $|HK| \leq |G|$ y vale la igualdad si, y sólo si, $G = HK$, de donde resulta i). De esto se deduce también ii) multiplicando por $|G : H|$.

Por lo general, el recíproco del teorema 2.2.1 es falso. Por ejemplo, supóngase un grupo G que opera trivialmente sobre un conjunto no vacío X. Entonces cualquiera que sea $x \in X$, se tiene que $0_x = \{x\}$ y $G_x = G$. Si ahora suponemos que X posee por lo menos dos elementos, digamos $x, y \in X$, entonces $G_x = G_y = G$, luego los estabilizadores son conjugados; en cambio $0_x = \{x\} \neq \{y\} = 0_y$.

El siguiente es un recíproco parcial:

Proposición 2.3.4. Sea G que opera sobre X, y sean $x \in X$ y L un subgrupo de G conjugado a G_x. Entonces existe un elemento $y \in X$ que tiene a L por estabilizador y está en la misma órbita que x.

Demostración. Por ser L conjugado a G_x, existe $g \in G$ con $L = gG_xg^{-1}$ y consideremos $y = g \cdot x \in X$. Es claro que x e y pertenecen a la misma órbita, veamos que $G_y = L$:

$h \in L$ si, y sólo si, $h \in gG_xg^{-1}$ si, y sólo si, $\exists h' \in G_x$ con $h = gh'g^{-1}$ si, y sólo si

$h \cdot y = (gh'g^{-1}) \cdot y = (gh'g^{-1}) \cdot g \cdot x = (gh') \cdot x = g \cdot (h' \cdot x) = g \cdot x = y$ si, y

sólo si, $h \in G_y$. ▲

§2.4. APLICACIONES

Proposición 2.4.5. Sea G un grupo, y H un subgrupo de índice n en G. Entonces existe un subgrupo invariante K de G que está contenido en H y el índice $|G : K|$ es finito y divide a $n!$

Demostración. Como $|G:H| = n$, sea $X = \{x_1H, x_2H, \ldots, x_nH\}$ un sistema completo de coclases a la izquierda de H. Hagamos operar G sobre X por traslación a la izquierda, es decir:

$$x \cdot x_iH = xx_iH.$$

Sea $\Phi: G \to S(X)$ el morfismo inducido por dicha acción. Sea $K = \mathrm{Nu}\Phi = \bigcap_{x_iH \in X} G_{x_iH} = \bigcap_{1 \le i \le n} x_iHx_i^{-1} \subseteq H$. En cuanto al índice, ya que $G/\mathrm{Nu}\Phi \simeq \mathrm{Im}\Phi$:

$$|G:K| = |G:\mathrm{Nu}\Phi| = |\mathrm{Im}\Phi|$$

como $\mathrm{Im}\Phi$ es subgrupo de S(X), cuyo orden es $n!$, todo está claro ▲

Proposición 2.4.6. Sea G un grupo de orden m, y sea p el menor primo que divide a m. Todo subgrupo de índice p en G, es invariante.

Demostración. Sea H un subgrupo de G tal que $|G:H| = p$. Por la proposición anterior existe un subgrupo K de G con las propiedades: K es invariante en G, $K \subseteq H$ y, además, $|G:K|$ divide a $p!$ Vamos a probar que $K = H$, para lo cual basta con probar que tienen el mismo orden (pues $K \subseteq H$); o equivalentemente, que tienen el mismo índice (pues G es finito). Veamos esto último: como $K \subseteq H$, entonces $|G:H| = p \le |G:K|$, luego $|G:K| \neq 1$. Sea q un primo que divide a $|G:K|$, por tanto $q/p!$, luego $q \le p$ y se deduce que $q = p$ por ser p el menor primo que divide a n. Consecuentemente, $|G:K| = p^r$ que divide a $p!$, y esto es sólo posible si $r = 1$, esto es $|G:K| = p$, como se quería probar. ▲

Ejemplo 1. El grupo cuaterniónico generalizado $\mathbf{H}_n = \langle A, B/A^{2^{n-1}} = 1, A^{2^{n-2}} = B^2, BAB^{-1} = A^{-1} \rangle$ no es simple. En este caso $H = \langle A \rangle$ tiene índice 2 en $\mathbf{H}_n$, luego es invariante.

Ejemplo 2. Sea D_n el grupo diédrico de orden $2n (n \ge 3)$ y sabemos que podemos considerar $\mathbf{D}_n = \langle a, b \rangle$, tal que $a^n = b^2 = (ab)^2 = 1$.

De la relación $(ab)^2 = 1$ se deduce que

$$ab = b^{-1}a^{-1} = ba^{-1} \text{ y, en general,}$$
$$a^ib = ba^{-i}.$$

Afirmamos que cualquiera que sea r tal que r/n, el subgrupo

$$H_r = \langle a^r \rangle \text{ es invariante en } \mathbf{D}_n.$$

Como a, b generan $\mathbf{D}_n$, basta con observar que si $x \in H_r$, entonces $bxb^{-1} \in H_r$. En efecto, si $x \in H_r$, existe j tal que $x = (a^r)^j = a^{rj}$, entonces

$$bxb^{-1} = ba^{rj}b^{-1} = bba^{-rj} = a^{-rj} = (a^r)^{-j} \in H_r.$$

Obsérvese también que H_r es un subgrupo invariante de orden n/r. Afirmamos además que $\mathbf{D}_n/H_r \simeq \mathbf{D}_r$.

Por el teorema de Lagrange, $\mathbf{D}_n/H_r$ es un grupo de orden $\frac{2n}{n/r} = 2r$. Como $\mathbf{D}_n$ está generado por a, b, el cociente estará generado por las imágenes de a y b, que las designamos con x e y, respectivamente. Se satisface

$$x^r = 1 \text{ (pues } a^r \in H_r)$$

$$y^2 = 1 \text{ (pues } b^2 = 1)$$

$$(xy)^2 = 1 \text{ (pues } (ab)^2 = 1)$$

Entonces, $\mathbf{D}_n/\mathbf{H}_n = \langle x, y \rangle \simeq \mathbf{D}_2$.

Proposición 2.4.7. Sea G un grupo finito de orden mp con p primo, $p \geq m$. Todo subgrupo H de orden p es invariante en G.

Demostración. Sea H de orden p en G, por tanto $|G:H| = m$. Entonces existe un subgrupo K de G tal que $K \subseteq H$, K invariante en G, y además $|G:K|$ divide a $m!$ Vamos a probar que $K = H$. Supongamos lo contrario, si $K \neq H$, como el orden de H es p primo, necesariamente deberá tenerse $K = \{1\}$, esto es $|K| = 1$. Por Lagrange

$$|G| = |G:K| \cdot |K|$$

es decir $mp = |G:K| \cdot 1$, luego $|G:K| = mp$, pero como $|G:K|$ divide a $m!$ resulta $mp/m!$ de aquí que $p \mid (m-1)!$, lo cual es absurdo pues p es primo y $p \geq m$. Entonces necesariamente debe tenerse $K = H$, invariante en G. ▲

§2.5. TEOREMA DE ECUACIÓN DE CLASES

Teorema 2.5.2. Sea G un grupo finito y $z(G)$ su centro. Existe una familia de subgrupos de G $\{H_i\}_{1 \leq i \leq m}$, tales que

i) $h_i = |G:H_i| > 1 \quad (1 \leq i \leq m)$

ii) $|G| = |z(G)| + \sum_{1 \leq i \leq m} h_i$.

Demostración. Se hace operar a G sobre sí mismo por conjugación, es decir

$$g \cdot x = gxg^{-1}.$$

Si $\{0_{x_i}\}_{1 \leq i \leq m}$ son las distintas órbitas, entonces el conjunto G se puede presentar como unión *disjunta* de sus órbitas; es decir $G = \bigcup_{1 \leq i \leq m} 0_{x_i}$, por tanto

$$|G| = \sum_{1 \leq i \leq m} |0_{x_i}|.$$

Ahora bien

$0_{x_i} = \{x_i\}$ si, y sólo si, $gx_ig^{-1} = x_i$, para todo $g \in G$ si, y sólo si, $x_i \in z(G)$.

En otras palabras, las órbitas puntuales son las que corresponden a elementos en el centro de G. Entonces, separando las órbitas puntuales de las que no lo son

$$|G| = \sum_{|0_{x_i}|=1} |0_{x_i}| - \sum_{|0_{x_j}|>1} |0_{x_j}| = |z(G)| + \sum_{|0_{x_j}|>1} |0_{x_j}| =$$

$$= |z(G)| + \sum_{G_{x_j} \neq 2} |G:G_{x_j}| = |z(G)| + \sum h_j$$

donde se tomó

$$H_j = G_{x_j},\ |G:G_{x_j}| = h_j \neq 1, \text{ pues } G \neq G_{x_j}. \quad \blacktriangle$$

Aplicaciones

Consideremos algunas aplicaciones de este importante resultado.

Proposición 2.5.8. (Teorema Cauchy) Sea G un grupo de orden m, y sea p primo tal que p/m. Entonces existe en G algún elemento de orden p.

Demostración. i) Si G es abeliano, el resultado es inmediato: G es suma directa de grupos cíclicos.

ii) Sea G no necesariamente abeliano. Hagamos inducción en m: Si $m = 1$, no hay primos p que lo dividan, de manera que en este caso no hay nada que demostrar. Supongamos el resultado válido para todo grupo de orden menor que m.

Si p divide el orden de algún subgrupo propio H de G, entonces, por hipótesis inductiva, H posee elementos de orden p, y por lo tanto G los posee. De manera que podemos suponer que cualquiera que sea el subgrupo propio H de G, $p \nmid |H|$. Esto último equivale a suponer que cualquiera que sea el subgrupo propio H de G, siempre se tiene $p/|G:H|$ (Lagrange). Ahora, aplicando la ecuación de clases, se tiene

$$|G| = |z(G)| + \sum_{1 \leq i \leq n}' h_i, \text{ donde } h_i = |G:H_i| > 1$$

por lo ya dicho p/h_i entonces $p/\sum_{1 \leq i \leq n}' h_i$, y como también $p/|G| = m$, resulta $p/|z(G)|$. Teniendo en cuenta que $|z(G)| \neq 0$ pues $1 \in z(G)$, y que $z(G)$ es abeliano, el resultado se sigue de la primera parte. $\blacktriangle$

Nótese que el resultado no se generaliza para p^i, $i > 1$. En efecto, aun en el caso abeliano, existen grupos tales que $p^i/|G|$, si bien G no tienen elementos de orden p^2, por ejemplo $G = \mathbf{Z}_p \oplus \ldots \oplus \mathbf{Z}_p$.

§ 2.6. p-GRUPOS

Definición 2.6.6. Sea G un grupo finito y p un número primo. Diremos que G *es un p-grupo* si, y sólo si, existe $r \in \mathbf{N}$ tal que $|G| = p^r$.

Corolario. Sea G un grupo finito y p un primo. Entonces G es un p-grupo si, y sólo si, todo elemento de G tiene por orden una potencia del primo p.

Demostración. Es claro que si G es un p-grupo todo elemento tiene por orden una potencia del primo p. (Lagrange). Recíprocamente, supongamos que cualquiera que sea $x \in G$, $x \neq 1$, existe $r \in \mathbf{N}$ con orden de $x = p^r$. Si G no fuese un p-grupo, existiría algún primo $q \neq p$ tal que $q/|G|$. Ahora bien, por la proposición 2.5.8, existiría en G algún elemento de orden q (que no es potencia del primo p) contrario a lo supuesto, y por tanto G debe ser un p-grupo. $\blacktriangle$

Proposición 2.6.9. Sea G un p-grupo finito, entonces $z(G) \neq 1$.

Demostración. Por la ecuación de clases

$$|G| = |z(G)| + \sum_{1 \leq i \leq n} h_i, \text{donde } h_i = |G : H_i| > 1$$

como G es un p-grupo (supóngase $|G| = p^r$), se tiene que p/h_i para todo i (Lagrange), luego $p/|z(G)|$, y ya que $|z(G)| \neq 0$, resulta $p \leq |z(G)|$; y por ser p un número primo, $z(G) \neq 1$.

Corolario. Si G es un p-grupo no cíclico, entonces no es simple.

Ejemplo 1. Sea $n \geq 2$. Vamos a calcular el centro del grupo cuaterniónico generalizado H_n. Sabemos, por la proposición anterior, que $z(H_n) \neq 1$. Sea

$$H_n = \langle A, B / A^{2^n} = 1,\ A^{2^{n-1}} = B^2,\ BAB^{-1} = A^{-1} \rangle$$

una presentación, y sabemos que H_n consiste de los elementos

$$A^i, A^iB (0 \leq i \leq 2^n).$$

Afirmamos que $z(H_n) = \{1, B^2\}$. En efecto, $B^2 \in z(H_n)$, ya que sabemos que es el único elemento de orden 2 de H_n (cualquiera que sea $x \in H_n$, el orden de xB^2x^{-1} es también 2).

Recíprocamente, si $x = A^i \in z(H_n)$, entonces $A^i = BA^iB^{-1} = A^{-i}BB^{-1} = A^{-i}$, y entonces $i = 2^{n-1}$, es decir $x = A^{2^{n-1}} = B^2$. Por último, si $x = A^iB \in z(H_n)$ debiera ser $A^iB = AA^iBA^{-1} = AA^iAB = A^{i+2}B \therefore A^2 = 1$, luego $n = 1$, contrario a lo que habíamos supuesto: $n \geq 2$.

Ejemplo 2. Sea A un grupo finito ($A \neq 1$). Sea $G = \text{Aut}(A)$ que opera sobre A en la forma natural

$$f \cdot a = f(a) \qquad (f \in \text{Aut}(A),\ a \in A).$$

Es claro que el elemento neutro $1 \in A$ tiene una órbita puntual: $0_1 = \{1\}$. Entonces G opera también sobre el conjunto $A' = A - \{1\}$. *Supongamos que esta acción sea transitiva.*

Luego, cualquiera que sean $x, y \in A'$, existe $f \in \text{Aut}(A)$ con $f(x) = y$. De aquí se deduce que todos los elementos de A' tienen el mismo orden, sea n dicho orden. Como en un grupo finito siempre hay elementos de orden primo, necesariamente $n = p$ es número primo. Por la proposición 2.5.8, A es un p-grupo, y por la 2.6.9, $z(A) \neq 1$. Si $1 \neq x \in z(A)$, entonces $f(x) \in z(A)$ para todo $f \in \text{Aut}(A)$ y en consecuencia $z(A) = A$, es decir, A es abeliano. Por el teorema de la estructura de grupos abelianos finitos (todo elemento de A tiene orden p) se tiene:

$$A \simeq \mathbf{Z}_p \oplus \mathbf{Z}_p \ldots \oplus \mathbf{Z}_p. \qquad (*)$$

Queda a cargo del lector verificar que los grupos del tipo (*) tienen la propiedad que Aut(A) opera transitivamente sobre A'.

Supongamos ahora que la acción de Aut(A) *sobre* A' *sea 2-transitiva.* Si opera 2-transitivamente, entonces lo hará también 1-transitivamente, y en consecuencia

$$A \simeq \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \ldots \oplus \mathbf{Z}_p \qquad (n \text{ copias}).$$

i) Sea primero $n = 1$, es decir $A \simeq \mathbf{Z}_p$. Si $p \geq 5$, tomando $x \in A'$, no existe automorfismo que satisfaga

$$f(x) = x; \qquad f(2x) = 3x$$

se concluye que si $n = 1$, debe ser $p = 2, 3$.

ii) Sea $n > 1$, $p > 2$. Supóngase, sin pérdida de generalidad, que

$$A = \mathbf{Z}_p \oplus \ldots \oplus \mathbf{Z}_p.$$

Es claro que no existe automorfismo f de A que satisfaga

$$f(1, 0, \ldots 0) = (1, 0, \ldots 0); \qquad f(2, 0, \ldots 0) = (0, 0, \ldots 1)$$

En consecuencia, si $n > 1$, debe ser $p = 2$. Por lo tanto, si Aut(A) opera 2-transitivamente, A debe ser de alguno de los tipos siguientes

$$\mathbf{Z}_3, \mathbf{Z}_2 \oplus \ldots \oplus \mathbf{Z}_2 \qquad (n \text{ copias}).$$

Las verificaciones correspondientes se dejan a cargo del lector. ¿Cuáles son los grupos finitos A, tales que Aut(A) opera n-transitivamente sobre A' ($n \geq 3$)?

Proposición 2. 6. 10. Si G es grupo de orden p^2 (p primo), entonces G es abeliano.

Demostración. Por la proposición 2. 6. 9, $z(G) \neq 1$, entonces $|z(G)| = p$ ó p^2. Si $|z(G)| = p^2$, $G = z(G)$ es abeliano.

En caso contrario, $|G : z(G)| = p$. Si tomamos $x \in z(G)$, $y \in G$, $y \notin \langle x \rangle$, entonces $G = \langle x, y \rangle$, y además, $xy = yx$, por tanto también en este caso G es abeliano. ▲

Se deduce de lo anterior que todo grupo de orden p^2 es isomorfo, o bien a $\mathbf{Z}_{p^2}$, o bien a $\mathbf{Z}_p \oplus \mathbf{Z}_p$. Obsérvese que el resultado anterior no se puede generalizar a grupos de orden $p^n (n > 2)$, puesto que se sabe ya que existen grupos no abelianos de orden p^3 (véase I. 4. 3).

Proposición 2. 6. 11. Sea G un grupo de orden p^m (p primo, $m \in \mathbf{N}$).

i) Cualquiera que sea $n \in \mathbf{N}$ tal que $0 \leq n \leq m$, G posee subgrupos invariantes de orden p^n.

ii) Todo subgrupo de orden p^{m-1} es invariante.

Demostración. i) Inducción en m. Si $m = 1$; $n = 0, 1$, entonces el resultado es obvio. Supóngase válido para grupos de orden menor o igual que p^{m-1}. Sabemos que el centro de un p-grupo es no trivial, y supongamos $|z(G)| = p^t$ con $1 \leq t \leq m$. Sea n tal que $0 \leq n \leq m$.

a) Si $n \leq t$, como $z(G)$ es un grupo abeliano, entonces posee subgrupos de orden p^n, que por estar contenidos en $z(G)$, serán invariantes en G.

b) Si $t < n$, consideremos el p-grupo cociente $G' = G/z(G)$, cuyo orden es $p^{m-t} \leq p^{m-1}$. La hipótesis inductiva se aplica a G'. Sea $\pi : G \to G'$

el epimorfismo canónico. Sea H un subgrupo invariante de G' de orden p^{n-1}, entonces se verifica inmediatamente que $\pi^{-1}(H)$ tiene las propiedades requeridas.

ii) Es consecuencia de la proposición 2.4.6.

Ejemplo 1. Sea H_n el grupo cuaterniónico generalizado de orden 2^{n+1} $H_n = \langle A, B \rangle$. Sabemos que $z(H_n) = \{1, B^2\}$. El cociente $H_n/z(H_n)$ es un grupo de orden 2^n generado por las imágenes de A y B que denotamos por a y b, respectivamente.

Se satisface

$$a^{2^{n-1}} = 1 \quad (\text{pues } A^{2^{n-1}} = B^2 \in z(H_n))$$

$$b^2 = 1 \quad (\text{pues } B^2 \in z(H_n))$$

$$(ab)^2 = abab = aba b^{-1} = 1 \quad (\text{pues } BAB^{-1} = A^{-1}).$$

En consecuencia, $H_n/z(H_n) \simeq D_{2^{n-1}}$.

La búsqueda de subgrupos invariantes en H_n se reduce a la del grupo diédrico $D_{2^{n-1}}$. Sabemos que los subgrupos $K_{2^i} = \langle a^{2^i} \rangle$ en el grupo diédrico son invariantes, y por lo tanto sus imágenes inversas $L_i = \langle A^{2^i}, B^2 \rangle$ son subgrupos invariantes en H_n.

En el caso del grupo cuaterniónico H_2 de orden 8, todo subgrupo es
42 invariante. En efecto, H_2 posee un único elemento de orden 2, y por lo tanto un único subgrupo de ese orden, $z(H_2)$, que es invariante. Los restantes subgrupos propios son todos de orden 4 e invariantes por la proposición anterior.

Proposición 2.6.12. Sea G un grupo de orden p^3 (p primo). Si G posee más de un subgrupo invariante de orden p, entonces G es abeliano y no cíclico.

Demostración. Sean H y K subgrupos invariantes de orden p. Los grupos cocientes G/H y G/K tienen orden p^2, y por la proposición 2.6.10 son abelianos, de donde se tiene que $[G, G] \subseteq H$ y $[G, G] \subseteq K$, y por consiguiente $[G, G] \subseteq H \cap K = 1$, esto es $[G, G] = 1$, luego G es abeliano. Por otra parte, G no puede ser cíclico, pues sino $G \simeq \mathbf{Z}_{p^3}$, y este último grupo no posee más de un subgrupo de orden p. ▲

Proposición 2.6.13. Sea G un grupo de orden p^3, p primo. Supongamos que G no es abeliano. Entonces $[G, G] = z(G)$ de orden p.

Demostración. Como G es un p-grupo, su centro no es trivial, de donde $|z(G)| = p, p^2$ ó p^3. El caso $|z(G)| = p^3$ es imposible, pues $G = z(G)$ sería abeliano. Tampoco puede ser $|z(G)| = p^2$, pues en este caso $|G/z(G)| = p$, y entonces G sería abeliano. Por necesidad $|z(G)| = p$. Ahora, $|G/z(G)| = p^2$, por tanto es abeliano, es decir $[G, G] \subset z(G)$. Si fueran distintos, sería $[G, G] = 1$ y en dicho caso G sería abeliano, lo que es un absurdo. ▲

El siguiente teorema completa el panorama.

§2.7. TEOREMA DE CARACTERIZACIÓN DE GRUPOS DE ORDEN p^3

Teorema 2.7.3. Sea G un grupo de orden p^3, p primo. Entonces G es isomorfo a uno, y sólo uno, de los siguientes grupos:

1) Si G es abeliano

$$\mathbf{Z}_{p^3};\ \ \mathbf{Z}_{p^2} \oplus \mathbf{Z}_p;\ \ \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p.$$

2) Si G no es abeliano

a) $p = 2$

$\mathbf{H}_2$ (grupo cuaterniónico), $\mathbf{D}_4$ (grupo diédrico)

b) $p \neq 2$

$$G_1 = \langle a, b / a^{p^2} = b^p = 1,\ bab^{-1} = a^{1+p} \rangle$$

$$G_2 = \langle a, b, c / a^p = b^p = c^p = 1,\ ab = bac,\ ac = ca,\ bc = cb \rangle.$$

Demostración. En el caso 1), G es abeliano, y se conoce el resultado (véase[12]).

Consideremos 2) a). El grupo G no posee elementos de orden 8, pues en este caso sería cíclico, y por consiguiente abeliano.

Tampoco G puede tener *todos* sus elementos ($\neq 1$) de orden 2, porque también en este caso G sería abeliano. Por el teorema de Lagrange debe existir $a \in G$, tal que su orden sea 4; consideramos $A = \langle a \rangle$. Como el índice $|G:A| = 2$, A es invariante en G (véase la proposición 2.4.6). 43

Sea $b \in G$, $b \notin A$; por cierto que $A \neq bA$, y así $G = A \cup bA$ con $A \cap bA = \emptyset$. Como $b^2 \in G$, luego $b^2 \in A \cup bA$, es decir $b^2 \in A$, o bien $b^2 \in bA$. Lo último es imposible, pues sería $b \in A$. De manera entonces que $b^2 \in A$. Como $A = \{1, a, a^2, a^3\}$, si fuera $b^2 = a$, o bien $b^2 = a^3$, se tendría $b^4 = a^2 = 1$, de donde el elemento b no tendría orden 4, ni 2; luego tendría orden 8, y por esto G es abeliano. En consecuencia, quedan las posibilidades

$$b^2 = a^2, \quad \text{o bien} \quad b^2 = 1. \tag{*}$$

Por otra parte, como A es invariante en G, el elemento $bab^{-1} \in A$, y como el orden de bab^{-1} tiene que ser el mismo de a (por ser conjugados), resulta que las posibilidades son

$$bab^{-1} = a, \quad \text{o bien} \quad bab^{-1} = a^3$$

(ya que a y a^3 son los únicos elementos de orden 4 en A). Pero, si fuese $bab^{-1} = a$, se tendría $G = \langle a, b \rangle$, donde $ab = ba$, es decir, G sería abeliano, y esto no es posible. Por consiguiente, sólo hay dos grupos no abelianos de orden 8, que son los determinados por las relaciones

$$\langle a, b / a^4 = 1,\ b^2 = a^2,\ bab^{-1} = a^3 \rangle$$

$$\langle a, b / a^4 = 1,\ b^2 = 1,\ bab^{-1} = a^3 \rangle$$

los cuales son obviamente isomorfos a $\mathbf{H}_2$ y $\mathbf{D}_4$, respectivamente.

Consideremos 2) b). Supongamos primero que G posea elementos de orden p^2. Sea $a \in G$ un tal elemento, $A = \langle a \rangle$. Como $|G:A| = p$, se tiene que A es invariante en G (proposición 2.4.6). Sea $b \in G$, tal que

$b \notin A$; por cierto que $b^p \in A$. Como A es invariante, existe r con $0 \leq r < p^2$ con

$$bab^{-1} = a^r \qquad (r \neq 0, 1).$$

Como ya se hizo anteriormente, se prueba inductivamente que cualquiera que sea $j \geq 1$:

$$b^j a b^{-j} = a^{r^j}.$$

En particular, poniendo $j = p$, teniendo en cuenta que $b^p \in A$ y el hecho que A es abeliano, resulta

$$a = b^p a b^{-p} = a^{r^p}$$

Por lo tanto, $r^p \equiv 1 (p^2)$.

Es inmediato que $(1 + p)^p = 1 + \theta p^2$ y, por lo tanto, $(1 + p)^p \equiv 1 (p^2)$; como r es raíz primitiva de la congruencia ($\mathbf{Z}_{p^2}$ es cíclico) pues $r \neq 1$, entonces existe α, $0 < \alpha < p$ tal que:

$$r^\alpha \equiv 1 + p (p^2)$$

cambiando los generadores

$$x = a \qquad y = b^\alpha$$

resulta

$$x^{p^2} = a^{p^2} = 1, \qquad y^p = b^{\alpha p} = (b^p)^\alpha \in A$$

$$yxy^{-1} = b^\alpha a b^{-\alpha} = a^{r^\alpha} = x^{r^\alpha} = x^{1+p}.$$

Ahora bien, $y^p \in A$; por lo tanto, existe $0 \leq j < p^2$ con $y^p = x^j$. Dado que G no posee elementos de orden p^3:

$$1 = y^{p^2} = x^{jp}.$$

Por tanto p/j, es decir $j = tp$ $(0 \leq t < p)$. Volvemos a cambiar de generadores

$$z = x \qquad w = yx^{-t}.$$

entonces

$$z^{p^2} = x^{p^2} = 1, \quad wzw^{-1} = yx^{-t} xx^t y^{-1} = x^{1+p} = z^{1+p}.$$

Queda como ejercicio para el lector verificar que

$$w^p = 1, \text{ y entonces } G \simeq G_1.$$

Supongamos por último que G no posea elementos de orden p^2. Por la proposición 2.6.13, $z(G) = [G, G]$ de orden p. Aquí $G/z(G)$ tiene orden p^2, luego es abeliano y no cíclico (sino sería G abeliano), por lo tanto es isomorfo a $\mathbf{Z}_p \oplus \mathbf{Z}_p$, es decir:

$$G/z(G) = \langle x, y / x^p = y^p = 1, \; xy = yx \rangle.$$

Sean $a, b \in G$ tales que en el morfismo canónico $\pi : G \to G/z(G)$ se tenga $\pi(a) = x$ y $\pi(b) = y$, como G no tiene elementos de orden p^2, los órdenes de los elementos a, b deben ser p.

El elemento $aba^{-1}b^{-1} \in [G, G] = z(G)$, sea $c = aba^{-1}b^{-1}$. Resta sólo por demostrar que el orden de c es p, o equivalentemente (G no posee elementos de orden p^2), $c \neq 1$. Pero esto es inmediato, pues si $c = 1$, entonces $ab = ba$, pero $G = \langle a, b, z(G) \rangle$ resultaría abeliano lo cual no es posible. Luego $G \simeq G_2$. ▲

Ejemplo. Respecto al teorema, queda por resolver el problema de la existencia de tales grupos. Está claro que los casos 1) y 2) a) no ofrecen dificultad alguna, pues el lector ya conoce la existencia de tales grupos. También conoce la existencia de grupos no abelianos de orden p^3, tal que todo elemento tiene orden p (véase el capítulo 1), con lo que queda también resuelto el caso 2) b) correspondiente de grupo G_2. Veamos pues la existencia de grupos isomorfos a G_1.

Todo nuestro problema es fabricar un grupo no abeliano de orden p^3 que posea elementos de orden p^2. Para ello utilizaremos los métodos de producto semidirecto.

El elemento $1 + p \in \mathbf{Z}_{p^2}$ satisface

i) $1 + p \neq 1 (p^2)$

ii) $(1 + p)^p \equiv 1 (p^2)$.

Por lo tanto, la aplicación

$f: \mathbf{Z}_{p^2} \to \mathbf{Z}_{p^2}, \quad f(x) = x(1 + p)$ es un automorfismo de orden p.

Siendo así, se define $\phi: \mathbf{Z}_p \to \mathrm{Aut}(\mathbf{Z}_{p^2})$ por $\phi(t) = f^t$ $(0 \leq t < p)$. El producto semidirecto asociado $\mathbf{Z}_{p^2} \times_\phi \mathbf{Z}_p$ es un grupo no abeliano de orden p^3 y posee elementos de orden p^2, en consecuencia $G_1 \simeq \mathbf{Z}_{p^2} \times_\phi \mathbf{Z}_p$.

Proposición 2.7.14. Sea G un grupo de orden pq; p, q primos; $p \not\equiv 1 (q)$, $q < p$. En tal caso G es cíclico.

Demostración. Por la proposición 2.5.8, G posee elementos de orden p, por lo tanto posee algún subgrupo H de orden p. Luego $|G:H| = q$, y por la proposición 2.4.6, H es invariante en G. Hagamos ahora operar G sobre el subgrupo invariante H, por conjugación. Sea $h \in H$, se tiene

$0_h = \{h\}$ si, y sólo si, $ghg^{-1} = h$ para todo $g \in G$ si, y sólo si, $h \in H \cap z(G)$.

Afirmamos que deben haber órbitas puntuales no triviales. En caso contrario, sería $H \cap z(G) = \{1\}$. Entonces, en el supuesto de que $h \in H$, $h \neq 1$, ya que debe verificarse

$$|0_h| \Big| |G| \quad \text{y} \quad |0_h| < |H| = p$$

se debiera tener $|0_h| = q$, para todo $h \neq 1$. Luego

$$p = |H| = \sum |0_h| = 1 + \sum |0_h| = 1 + rq$$

y por tanto, $p \equiv 1 (q)$, lo cual es absurdo. Entonces debe ser $H \cap z(G) \neq \{1\}$, y por ser el orden de H primo, resulta $H \cap z(G) = H$.

De esto último se concluye que $p / |z(G)|$; luego, necesariamente $|z(G)| = p$ o bien pq, es decir $|G : z(G)| = q$, o bien 1, $\therefore$ $G/_{z(G)}$ es cíclico, y entonces, G es abeliano, y así cíclico. ▲

Todo grupo abeliano cuyo orden es producto de primos distintos es cíclico. Adviértase que las condiciones: $p > q$, $p \not\equiv 1 (q)$ son equivalentes a la afirmación de que el máximo común divisor entre pq y $\phi(pq)$ es 1 (ϕ denota la función de Euler). La proposición anterior se puede generalizar como sigue: Si G es un grupo de orden n, y si $(n, \phi(n)) = 1$, entonces G es cíclico.

§ 2.8. TEOREMA DE CARACTERIZACIÓN DE GRUPOS DE ORDEN pq

Teorema 2.8.4. Sea G un grupo de orden pq; p, q primos; $p > q$. Entonces

i) Si G es abeliano, $G = \mathbf{Z}_{pq}$ (esto es, G es cíclico).

ii) Si G no es abeliano, entonces $q/p - 1$, y además, $G = \langle a, b/a^q = b^p = 1, aba^{-1} = b^{r_0}$, donde r_0 es cualquier entero que satisface: $1 < r_0 < p$, $r_0^q \equiv 1(p)\rangle$.

Demostración. Si G es abeliano, el caso i) es inmediato, pues como su orden es el producto de primos distintos, debe ser cíclico. Supongamos que G no es abeliano. Por la proposición 2.7.14, se tiene $q/p - 1$.

Por la proposición 2.5.8, G posee elementos x e y de órdenes p y q respectivamente. Sea $H = \langle x\rangle$, $K = \langle y\rangle$. El subgrupo de G generado por x e y posee elementos de orden p y de orden q y debe entonces coincidir con G; esto es $G = \langle x, y\rangle$. Por la proposición 2.4.6, H es invariante en G, luego debe existir r tal que

$$0 \leq r < p, \quad yxy^{-1} = x^r. \tag{*}$$

Si fuera $r = 0$, se tendría $x = 1$, lo que es contrario al supuesto de que el orden de x es p. Si fuera $r = 1$, entonces $yx = xy$, y por tanto $G = \langle x, y\rangle$ sería abeliano, que no es nuestro caso. Por lo tanto, $1 < r < p$.

Afirmamos que cualquiera que sea $j \geq 0$, se tiene

$$y^j x y^{-j} = x^{r^j} \tag{*}$$

Inducción en j: Si $j = 0, 1$, el resultado es bien claro. Supongamos que valga (*) para $j = n$. Resulta

$$y^{n+1}xy^{-(n+1)} = yy^nxy^{-n}y^{-1} = yx^{r^n}y^{-1} = (yxy^{-1})^{r^n} = (x^r)^{r^n} = x^{r^n \cdot r^n} = x^{r^{n+1}}.$$

Por el principio de inducción, la afirmación (*) queda probada. En particular, tomando $j = q$, y teniendo en cuenta que $y^q = 1$

$$x = y^q x y^{-q} = x^{r^q}$$

de donde se concluye que $r^q \equiv 1(p)$.

Nuestro grupo queda entonces descrito por

$$G = \langle x, y/ \quad x^p = y^q = 1 \quad yxy^{-1} = x^r \quad 1 < r < p \quad r^q \equiv 1(p)\rangle.$$

Para mostrar el isomorfismo propuesto sólo tenemos que cambiar los generadores de G. Como r es raíz primitiva de la ecuación de congruencia $r^q \equiv 1(p)$ (pues Z_p^* es cíclico), entonces existe α con $0 < \alpha < q$ tal que $r^\alpha = r_0$.

Consideremos:

$$a = y^\alpha \qquad b = x$$

por cierto que también $G = \langle a, b\rangle$ y que $a^q = (y^\alpha)^q = 1$. Por otra parte, vale

$$aba^{-1} = y^\alpha x y^{-\alpha} = x^{r^\alpha} = x^{r_0} = b^{r_0}$$

de donde se sigue el teorema.

Corolario. Ningún grupo de orden pq es simple.

Ejemplo 1. Cualquiera que sea el primo impar p, existe un único grupo (salvo isomorfismo) no abeliano de orden $2p$, a saber: $\mathbf{D}_p$ – grupo diédrico.

Ejemplo 2. Todo grupo de orden 15 es cíclico. Análogamente, grupos de órdenes 35 y 77 son necesariamente cíclicos.

Ejemplo 3. En cambio, existen grupos no abelianos de órdenes 21 y 55.

3

GRUPO SIMÉTRICO, REPRESENTACIONES

Una ténica muy utilizada en el estudio de grupos es representarlos en términos de grupos familiares. En particular, si se representa a los elementos de un grupo como permutaciones o matrices, es posible obtener información adicional a partir de la estructura cíclica y las trazas.

El teorema de Cayley (proposición 2.1.3) y otros resultados obtenidos en el capítulo anterior darán idea al lector de la importancia de establecer las propiedades del grupo simétrico y las de sus subgrupos.

En la primera parte de este capítulo se tratan algunas de estas propiedades, dejando para el final la definición de algunos conceptos acerca de la representación en grupos de matrices y teoría de caracteres.

A continuación se desarrolla el concepto de la estructura cíclica de los elementos de $\mathbf{S}_n$, que es de fundamental importancia en las explicaciones posteriores.

§3.1. ESTRUCTURA CÍCLICA

Sea $n \in \mathbf{N}$. En todo lo que sigue se considerará el conjunto $X = [1, 2, \ldots, n]$ y su grupo simétrico $S(X) = \mathbf{S}_n$ que opera naturalmente sobre X. Es claro que cualquiera que sea $t \in \mathbf{S}_n$, el subgrupo $H = (t)$ también opera sobre X. Las órbitas de esta acción se llaman *órbitas de* t. Sean $X_1, X_2, \ldots, X_r$ las órbitas de $t \in \mathbf{S}_n$. Por lo tanto, X es unión disjunta de los X_i. Para cada $i (1 \leq i \leq r)$, se define $t_i \in \mathbf{S}_n$ en la forma

$$t_i(x) = t(x) \quad (\text{si } x \in X_i) \qquad t_i(x) = x \quad (\text{si } x \notin X_i)$$

Los t_i se denominan *ciclos asociados* a t.

Por ejemplo, si t es el elemento de $\mathbf{S}_7$

$$t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 4 & 3 & 5 & 7 & 2 \end{pmatrix}$$

sus órbitas son

$$X_1 = [1] \quad X_2 = [2, 6, 7] \quad X_3 = [3, 4] \quad X_4 = [5]$$

y los ciclos asociados

$$t_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}; \qquad t_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 3 & 4 & 5 & 7 & 2 \end{pmatrix}$$

$$t_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 3 & 5 & 6 & 7 \end{pmatrix}; \qquad t_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

Los ciclos t_i asociados a la permutación t tienen propiedades interesantes. La primera es la siguiente

Si $s = |t_i|$, $x \in X_i$, entonces

$$\{x, \tau_1(x), \tau_1^2(x), \ldots, \tau_1^{s-1}(x)\} = X_1. \tag{1}$$

En efecto,

$$\tau_1^j(x) = \tau^j(x) \in X_1, \text{ pues } X_1 \text{ es órbita de } \tau.$$

Recíprocamente, si $y \in X_1$, como también $x \in X_1$, y además X_1 es órbita, entonces existe j tal que $y = \tau^j(x) = \tau_1^j(x)$. Ahora, por ser s el orden de τ_1, es claro que puede tomarse j tal que $0 \leq j < s$ con la misma propiedad. Queda así demostrado (1).

También, con las mismas notaciones, se tiene

$$|X_1| = s. \tag{2}$$

De acuerdo con (1), basta con verificar que $\{\tau_1^j(x)\}_{0 \leq j < s}$ tiene s elementos, o equivalentemente, que todos sus elementos son distintos.

En efecto, supóngase, por el contrario, que $0 \leq j < k < s$ con $\tau_1^j(x) = \tau_1^k(x)$. En consecuencia, $\tau_1^{k-j}(x) = x$. Cualquiera que sea $y \in X_1$, por (1) es $y = \tau_1^j(x)$ y entonces también $\tau_1^{k-j}(y) = \tau_1^{k-j}(\tau_1^j(x)) = \tau_1^k(x) = y$. Por último, si $z \notin X_1$, entonces $\tau_1(z) = z$, y en consecuencia, también $\tau_1^{k-j}(z) = z$. En definitiva, $\tau_1^{k-j} = \mathrm{Id}$, siendo $0 < k - j < s$, esto contradice el hecho de ser $s = |\tau_1|$. Queda entonces probado (2).

Otro hecho que podemos observar de (1) es que si denotamos por $y_1, y_2, \ldots, y_r$ los elementos de X que no pertenecen a la órbita X_1, entonces se tiene

$$\tau_1 = \begin{pmatrix} x & \tau_1(x), \ldots, \tau_1^{s-1}(x) & y_1, y_2, \ldots, y_r \\ \tau_1(x) & \tau_1^2(x), \ldots, x & y_1, y_2, \ldots, y_r \end{pmatrix} \tag{*}$$

Adviértase que $\tau_1 = (x)$ si, y sólo si, $|X_1| = 1$ si, y sólo si, $\tau_1 = \mathrm{Id}$. Al elemento (*) lo vamos a designar con

$$\tau_1 = (x\, \tau_1(x)\, \tau_1^2(x), \ldots, \tau_1^{s-1}(x)). \tag{3}$$

Obsérvese que

$$\tau_1 = (x, \tau_1(x), \tau_1^2(x), \ldots, \tau_1^{s-1}(x)) = (\tau_1(x), \tau_1^2(x), \ldots, \tau_1^{s-1}(x), x) =$$
$$= (\tau_1^2(x), \ldots, \tau_1^{s-1}(x), x, \tau_1(x)) = \ldots$$

En estas condiciones llamaremos al entero $s = |\tau_1|$ longitud del ciclo τ_1, y también diremos que τ_1 es un s-ciclo. Los 2-ciclos se llaman transposiciones.

Volviendo al ejemplo anterior, se tiene

$$\tau_1 = (1) = \mathrm{Id}, \quad \tau_2 = (2\ 6\ 7) = (6\ 7\ 2) = (7\ 2\ 6), \quad \tau_3 = (3\ 4) = (4\ 3)$$
$$\tau_4 = (5) = \mathrm{Id}.$$

Una propiedad también importante es:

Si τ_1 y τ_2 son ciclos asociados a la permutación $\tau \in \mathbf{S}_n$, entonces

$$\tau_1 \tau_2 = \tau_2 \tau_1 \tag{4}$$

Sea $x \in X$; se pueden presentar los siguientes casos (X es unión disjunta de los X_i):

1) $x \notin X_1$, $x \notin X_2$. En este caso, por definición, $\tau_1(x) = \tau_2(x) = x$, luego $\tau_1\tau_2(x) = \tau_1\tau_2(x) = x$.

iii) $x \in X_i$, $x \in X_j$. Como las órbitas son disjuntas, esto sólo es posible si $X_i = X_j$, es decir si $t = s$, en cuyo caso

$$t_i t_j(x) = t_i t_i(x) = t_j t_i(x).$$

iii) $x \in X_i$, $x \notin X_j$. Entonces se deduce que $t_i(x) \in X_i$, $t_i(x) \notin X_j$, y en consecuencia, se tiene $t_j(x) = x$, y también $t_j t_i(x) = t_i(x)$. Entonces

$$t_i t_j(x) = t_i(t_j(x)) = t_i(x) = t_j(t_i(x)) = t_j t_i(x).$$

iv) $x \notin X_i$, $x \in X_j$. Este caso es análogo al iii).

Demostremos ahora que si $\{t_i\}_{1 \le i \le r}$ son *todos* los ciclos asociados a la permutación t, entonces:

$$t = t_1 t_2 \dots t_r. \tag{5}$$

Es inmediato que, dado $x \in X$, existe un único X_i tal que $x \in X_i$, y en consecuencia

$$t_i(x) = t(x) \qquad t_j(x) = x \text{ si } j \neq i.$$

Luego, teniendo en cuanta (4), se tiene

$$t_1 t_2 \dots t_r(x) = t_1 t_2 \dots t_{r-1} t_r(x) = t_1 t_2 \dots t_{r-1}(x) = \dots = t_1 t_2(x) = t_1(x) = t(x).$$

Observemos además, que por (4) y (5), se tiene

$$t = t_1 t_2 \dots t_r = t_2 t_3 \dots t_r = \dots$$

Cabe notar que en (5) se ha probado que toda permutación $t \in \mathbf{S}_n$ se escribe como producto de ciclos disjuntos $t_i (1 \le i \le r)$; es decir, ciclos que satisfacen

$$i \neq j,\ x \in X,\ t_i(x) \neq x \Rightarrow t_j(x) = x.$$

Basándonos en el ejemplo anterior, tenemos

$$t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 4 & 3 & 5 & 7 & 2 \end{pmatrix} = (1)\ (2\ 6\ 7)\ (3\ 4)\ (5)$$

y con las mismas notaciones de antes, se verifica

$$|t| = \text{m.c.m.}\ \{|t_i| / 1 \le i \le r\} \tag{6}$$

(m.c.m. denota el mínimo común múltiplo).

Sea $s = |t|$, $s_i = |t_i|$, $m = \text{m.c.m.}\ \{s_i\}$. Por (4) y (5) se tiene

$$\text{Id} = t^s = (t_1 \dots t_r)^s = t_1^s \dots t_r^s.$$

Ahora bien, cualquiera que sea $x \in X_i$, se tiene $x = t^s(x) = t_i^s(x)$, y en consecuencia resulta $t_i^s = \text{Id}$, esto es $s_i / s\ (1 \le i \le r)$.

Por las propiedades de m resulta que m / s. Por otra parte, como s_i / m, resulta para todo $i\ (1 \le i \le r)$ $t_i^m = \text{Id}$, y en consecuencia

$$t^m = (t_1 \dots t_r)^m = t_1^m \dots t_r^m = \text{Id} \dots \text{Id} = \text{Id}.$$

De este modo, también s / m. Siendo m y s enteros positivos, se deduce que $m = s$; luego (6) está probado.

En el ejemplo considerado antes

$$|t_1| = 1;\ |t_2| = 3;\ |t_3| = 2;\ |t_4| = 1$$

por lo tanto

$$|t| = \text{m.c.m.}\,[1, 3, 2, 1] = 6.$$

Volviendo a la representación de una permutación $t \in \mathbf{S}_n$ como producto de ciclos disjuntos (5), es posible verificar la unicidad de tal descomposición (salvo el orden en que los factores están escritos).

En efecto, supóngase que

$$t = t_1 \dots t_r = t'_1 \dots t'_s$$

son dos de tales descomposiciones.

Sea $x \in X$, y siendo los factores disjuntos, existe i tal que si $j \neq i$, entonces $t_j(x) = x$, y también existe i' tal que para $j \neq i'$, $t'_j(x) = x$. Sin pérdida de generalidad, cabe suponer $i = i' = 1$, y así

$$t(x) = t_1(x) = t'_1(x)$$

en consecuencia $t_1^k(x) = t_1'^k(x)$ $(\forall\, k)$, luego se tiene $t_1 = t'_1$ en virtud de (3), y por lo tanto

$$t_1^{-1} \cdot t = t_2 \dots t_r = t'_2 \dots t'_s.$$

Ahora, por un argumento inductivo respecto del número de factores, se tiene que $r = s$ y los factores t_i son los t'_j en algún orden. Los resultados se resumen en la proposición siguiente.

Proposición 3.1.15. Todo elemento $t \in \mathbf{S}_n$ se escribe como producto de ciclos disjuntos. Esta descomposición es única, excepto el orden en que están escritos los factores. Vamos a adoptar la forma convencional de escribir $t = t_1\, t_2 \dots t_r$, siempre que

$$|t_1| \leq |t_2| \leq \dots \leq |t_r|.$$

Además, como los 1-ciclos representan el elemento $\mathrm{Id} \in \mathbf{S}_n$, optaremos por no escribirlos, y supondremos convenientemente que $1 < |t_1|$.

En nuestro ejemplo, admitidas estas convenciones, escribiremos

$$t = (3\ 4)(2\ 6\ 7).$$

Ejemplo. Veamos que $\mathbf{S}_4$ no posee elementos de orden 6. La descomposición de un elemento como producto de ciclos disjuntos ($\neq 1$) de $\mathbf{S}_4$ tiene que ser la correspondiente a alguno de los siguientes tipos:

i) $(\ .\ .)$ ii) $(\ .\ .)(\ .\ .)$ iii) $(\ .\ .\ .)$ iv) $(\ .\ .\ .\ .)$.

Teniendo en cuenta (3) y (6), vemos que las descomposiciones de tipo i) y ii) corresponden a elementos de orden 2 en $\mathbf{S}_4$, las del tipo iii) a elementos de orden 3, y las de tipo iv) a elementos de orden 4.

Proposición 3.1.16. Sea $t \in \mathbf{S}_n$, $s = (x_1\ x_2 \dots x_m) \in \mathrm{S}_n$ un m-ciclo. Entonces tst^{-1} también es un m-ciclo, y se tiene

$$tst^{-1} = (t(x_1)t(x_2) \dots t(x_m)).$$

Demostración. Para demostrar esto basta con probar:

i) Si $i < m$, entonces $tst^{-1}(t(x_i)) = t(x_{i+1})$.

ii) $tst^{-1}(t(x_m)) = t(x_1)$.

iii) Si x no es ninguno de los $t(x_i)$, entonces $tst^{-1}(x) = x$.

En efecto, si $i < m$, entonces $tst^{-1}(t(x_i)) = ts(t^{-1}t)(x_i) = ts(x_i) = t(x_{i+1})$. Además, $tst^{-1}(t(x_m)) = tst^{-1}t(x_m) = ts(x_m) = t(x_1)$. Por último, si x no es ninguno de los $t(x_i)$, $t^{-1}(x)$ no es ninguno de los x_i, por lo tanto $st^{-1}(x) = t^{-1}(x)$, y así $tst^{-1}(x) = tt^{-1}(x) = x$. ▲

Corolario. Sean $t, s \in \mathbf{S}_n$, y supongamos que

$$s = (x_1\ x_2\ \dots\ x_m)(y_1\ y_2\ \dots\ y_r) \dots (z_1\ z_2\ \dots\ z_p)$$

es una descomposición de s como producto de ciclos disjuntos. Entonces

$$tst^{-1} = (t(x_1)t(x_2) \dots t(x_m))(t(y_1)t(y_2) \dots t(y_r)) \dots (tz_1)t(z_2) \dots t(z_p)).$$

Demostración. En efecto, si ponemos

$$s_1 = (x_1\ x_2\ \dots\ x_m)$$
$$s_2 = (y_1\ y_2\ \dots\ y_r)$$
$$\dots\dots\dots\dots\dots$$
$$s_k = (z_1\ z_2\ \dots\ z_p)$$

tendremos

$$tst^{-1} = ts_1s_2 \dots s_kt^{-1} = (tst^{-1})(ts_2t^{-1}) \dots (ts_kt^{-1}).$$

El resultado se obtiene a partir de la proposición 3.1.16, pues todos los factores s_i son ciclos. ▲

Nota. El corolario de la proposición anterior nos dice que dos permutaciones conjugadas s y tst^{-1} tienen la misma estructura cíclica: es decir, en las descomposiciones como producto de ciclos disjuntos de s y tst^{-1} aparece el mismo número de factores y los órdenes de los factores son los mismos. La recíproca también es válida, es decir

Proposición 3.1.17. Dos elementos s y $s' \in \mathbf{S}_n$ tienen la misma estructura cíclica si, y sólo si, son conjugados.

Demostración. Supongamos s y s' con la misma estructura cíclica, y digamos

$$s = (x_1\ \dots\ x_m)(y_1\ \dots\ y_r) \dots (z_1\ \dots\ z_1)$$
$$s' = (x_1'\ \dots\ x_m')(y_1'\ \dots\ y_r') \dots (z_1'\ \dots\ z_1')$$

Para probar que s y s' son conjugados basta encontrar $t \in \mathbf{S}_n$, tal que $tst^{-1} = s'$, o equivalentemente (véase el corolario)

$$(t(x_1) \dots (t(x_m))(t(y_1) \dots t(y_r)) \dots (t(z_1) \dots t(z_1)) =$$
$$= (x_1'\ \dots\ x_m')(y_1'\ \dots\ y_r') \dots (z_1'\ \dots\ z_1')$$

Para lo cual será suficiente con demostrar que existe $t \in \mathbf{S}_n$, que satisface

$$\tau(x_1) = x_1' \quad \tau(y_1) = y_1' \quad \ldots \quad \tau(z_1) = z_1'$$

lo cual es inmediato, si se observa que los ciclos son disjuntos y S_n opera r-transitivamente sobre X. ▲

Ejemplo 1. Sean $\sigma = (2\ 6\ 7)(3\ 4)$, $\tau = (1\ 3\ 4\ 5\ 7)$. Entonces

$$\sigma\tau\sigma^{-1} = (\sigma(1)\sigma(3)\sigma(4)\sigma(5)\sigma(7)) = (1\ 4\ 3\ 5\ 2)$$

$$\tau\sigma\tau^{-1} = \tau(2\ 6\ 7)(3\ 4)\tau^{-1} = \tau(2\ 6\ 7)\tau^{-1}\tau(3\ 4)\tau^{-1} = (2\ 6\ 1)(4\ 5).$$

Ejemplo 2. Los elementos de S_8 siguientes:

$$\sigma = (1\ 6)(4\ 8)(2\ 5\ 3) \text{ y } \sigma' = (1\ 8)(2\ 6)(3\ 4\ 5)$$

poseen la misma estructura cíclica.

Para probar que son conjugados, basta con hallar $\tau \in S_8$ que satisfaga: $\tau(1) = 1$; $\tau(6) = 8$; $\tau(4) = 2$; $\tau(8) = 6$; $\tau(2) = 3$; $\tau(5) = 4$ y $\tau(3) = 5$. Basta tomar $\tau = (6\ 8)(4\ 2\ 3\ 5)$ para tener $\tau\sigma\tau^{-1} = \sigma'$.

§ 3.2. CLASES CONJUGADAS EN S_n

La relación en S_n: $\sigma \sim \sigma'$ si, y sólo si, σ y σ' son conjugados (si, y sólo si, poseen la misma estructura cíclica) es una relación de equivalencia en S_n. Por tanto queda inducida una partición de S_n (consúltese la referencia (11)). El número total de clases corresponde al número total de descomposiciones posibles de elementos de S_n.

Sean $C_1, \ldots, C_s$ la totalidad de clases de equivalencia.

Sea $\sigma \in C_1$, y supongamos que σ se descompone como producto de ciclos disjuntos en la siguiente forma

$$\alpha_1 : 1\text{-ciclos}$$
$$\alpha_2 : 2\text{-ciclos}$$
$$\ldots\ldots\ldots$$
$$\alpha_n : n\text{-ciclos}$$

en consecuencia $\sum_{i=1}^{n} i\alpha_i = n$ con $\alpha_i \geq 0$. Resulta así que los elementos de C_1 son exactamente aquellos que tienen una descomposición en ciclos disjuntos del tipo

$$\underbrace{(\cdot)(\cdot)\ldots(\cdot)}_{\alpha_1}\underbrace{(\cdot\,\cdot)(\cdot\,\cdot)\ldots(\cdot\,\cdot)}_{\alpha_2}\ldots$$

Luego el número de clases conjugadas distintas C_i está en correspondencia biunívoca con las sucesiones $\{(\alpha_1, \ldots, \alpha_n) \mid \alpha_i \geq 0, \sum_{i=1}^{n} i\alpha_i = n\}$. Pongamos $\mu_i = \alpha_i + \alpha_{i+1} + \ldots + \alpha_n$ entonces $\mu_1 \geq \mu_2 \geq \ldots \geq \mu_n \geq 0$ y $\sum_{i=1}^{n} \mu_i = n$. Recíprocamente dada una partición $(\mu_1, \ldots, \mu_n)$ de n con $\mu_1 \geq \ldots \geq \mu_n$,

definimos $\alpha_i = \mu_i - \mu_{i+1}$. Es fácil ver que $\sum i\alpha_i = n$. Luego el número de clases conjugadas distintas es el número de particiones de n.

Como ejemplo, consideremos $n = 5$. En este caso, las particiones de n son las siguientes:

i) 1, 1, 1, 1, 1 ii) 1, 1, 1, 2 iii) 1, 1, 3 iv) 1, 2, 2 v) 1, 4 vi) 2, 3 vii) 5.

Por lo tanto, S_5 posee 7 clases de equivalencia.

Nos proponemos hallar el número de elementos en cada clase de equivalencia. Sea C_i la clase correspondiente a descomposiciones del tipo

$$\underbrace{(.)(.)\ldots(.)}_{\alpha_1}\underbrace{(..)(..)\ldots(..)}_{\alpha_2}\ldots \qquad (*)$$

(es decir $\alpha_i : i$-ciclos).

Los n elementos de X se pueden disponer de $n!$ formas del tipo (*); pero hay que tener en cuenta que los elementos así obtenidos *no son todos distintos como permutaciones de* S_n.

i) En efecto, si permutamos entre sí los α_k ciclos de longitud k, obtenemos la misma permutación de S_n. Luego, la misma permutación se obtiene de

$$\alpha_1!\ \alpha_2!\ \ldots\ \alpha_n! \qquad (**)$$

formas distintas. Por ejemplo, $(1\ 2)(3\ 4)\ldots = (3\ 4)(1\ 2)\ldots$

ii) Además es posible obtener cada ciclo de longitud k de k formas distintas. Por ejemplo, $(1\ 2\ 3\ \ldots\ n) = (2\ 3\ \ldots\ n\ 1) = (3\ \ldots\ 1\ n\ 2) = \ldots$ Por lo tanto, la misma permutación del tipo (*) es considerada

$$1^{\alpha_1}\ 2^{\alpha_2}\ \ldots\ n^{\alpha_n} \qquad (***)$$

veces.

A fin de obtener el número exacto de elementos de C_i hay que dividir $n!$ por (*) y (**), o sea que se obtiene así la *fórmula de Cauchy:*

$$|C_i| = \frac{n!}{1^{\alpha_1}\alpha_1!\ 2^{\alpha_2}\alpha_2!\ldots n^{\alpha_n}\alpha_n!}$$

Ejemplo 1. Sea $n = 4$, y consideremos la clase correspondiente a la partición 1, 1, 3, o sea, la totalidad de elementos con descomposición del tipo

$$(.)(.)(..)$$

En este caso, $\alpha_1 = 2$ $\alpha_2 = 1$ $\alpha_3 = \alpha_4 = 0$.

Aquí, la fórmula de Cauchy nos indica que hay $\frac{4!}{1^2 2!\ 2!1!} = \frac{2\ 3\ 4}{2 \cdot 2} = 6$ elementos; y estos son:

$$(1\ 2) = (2\ 1),\quad (1\ 3) = (3\ 1),\quad (1\ 4) = (4\ 1),\quad (2\ 3) = (3\ 2)$$
$$(2\ 4) = (4\ 2),\quad (3\ 4) = (4\ 3),$$

Ejemplo 2. Si se considera la clase correspondiente a la partición 2, 2 en S_4, la fórmula de Cauchy nos indica que hay exactamente 3 elementos del tipo

$$(\ .\ )(\ .\ )$$

distintos. Estos son

$$(1\ 2)(3\ 4) = (3\ 4)(1\ 2) = (4\ 3)(1\ 2) = \ldots$$
$$(1\ 3)(2\ 4) = \ldots$$
$$(1\ 4)(2\ 3) = \ldots$$

§ 3.3. GENERACIÓN DE S_n

El siguiente resultado se refiere a la generación de S_n.

Teorema 3.3.5. Si $n \geq 2$, las $(n-1)$ transposiciones $\{(1\,i)/2 \leq i \leq n\}$ generan S_n.

Demostración. Inducción en n.

Si $n = 2$, el resultado es inmediato. Supongamos que el teorema es válido para $n-1 \geq 2$, y sea $t \in S_n$. Supongamos $t(n) = m$, para $1 \leq m \leq n$. Entonces el elemento

$$s = (1\ n)(1\ m)t$$

verifica $s(n) = n$, por lo tanto $s \in S_{n-1}$, y así la hipótesis inductiva es aplicable a s; entonces, s se escribe como producto de elementos $(1\ i)$ con $2 \leq i \leq n-1$, y en consecuencia

$$t = (1\ m)(1\ n)s$$

se escribe como producto de las transposiciones citadas. ▲

Corolario 1. Los elementos

$$s = (1\ 2\ \ldots\ n) \qquad t = (1\ 2)$$

generan S_n.

Demostración. En efecto, demostraremos que toda transposición del tipo $(1\ x)$, con $2 \leq x \leq n$, puede obtenerse a partir de s, t. Si $x = 2$, entonces $(1\ x) = t$ y no hay nada que demostrar.

Ahora bien, supongamos obtenidas ya las transposiciones $(1\ 2)$, $(1\ 3)\ \ldots\ (1\ x)$ a partir de s, t, y veamos cómo hacer lo propio con $(1\ x+1)(x < n)$. Consideremos el elemento

$$w = (1\ x)(1\ x-1)\ \ldots\ (1\ 2)\ (1\ 2\ 3\ \ldots\ n)^{x-1}$$

que, por hipótesis inductiva, puede obtenerse a partir de s, t. Dicho elemento satisface

$$x = (1\ x)(1\ x-1)\ldots(1\ 3)(1\ 2)\ (1\ 2\ 3\ldots n)^{x-1} = (2\ 3\ldots x)(1\ 2\ 3\ldots n)^{x-1} =$$

$$= (1)(2\ x+1\ \ldots$$

y por lo tanto

$$y(1\ 2)y^{-1} = (1\ x+1)$$

puede obtenerse también a partir de s, t. El corolario queda probado ▲

Corolario 2. Todo grupo finito G es isomorfo a un subgrupo de un grupo con dos generadores.

Demostración. Sea $|G| = n$. Por el teorema de Cayley existe un monomorfismo

$$G \to S(G) \simeq S_n.$$

Por lo tanto, G se identifica con un subgrupo de S_n. Por el corolario 1, el grupo S_n puede generarse con sólo dos elementos. ▲

Hay un resultado más general que el corolario 1 y que es válido en este caso, a saber

"Sea $n \neq 4$. Si $s \in S_n$, $s \neq Id$, entonces existe $t \in S_n$ tal que s, t generan S_n".

Para la demostración, refiérase el lector a la cita (36).

Corolario 3. Si $n \geq 2$, las $(n-1)$ transposiciones $\{(i\ i+1)\}_{1 \leq i \leq n-1}$ generan S_n.

Demostración. En efecto, se tiene

$$(2\ 3)(1\ 2)(2\ 3)^{-1} = (1\ 3)$$
$$(3\ 4)(1\ 3)(3\ 4)^{-1} = (1\ 4)$$
$$\ldots\ \ldots\ \ldots\ \ldots$$
$$(n-1\ n)(1\ n-1)(n-1\ n)^{-1} = (1\ n)$$

y entonces el resultado propuesto sigue del teorema 3.3.5. ▲

Ejemplo 1. Por el teorema anterior se sabe que todo elemento $s \in S_n (n \geq 2)$ puede escribirse como producto de las transposiciones $(1\ t)$ $(2 \leq t \leq n)$. La descomposición mencionada no es única, pues, por ejemplo

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(1\ 3)(1\ 2)(1\ 3).$$

Más adelante, veremos que la paridad del número de factores que intervienen en las posibles descomposiciones es un invariante.

Ejemplo 2. Sean los elementos de S_4

$$s = (1\ 3\ 2\ 4) \qquad t = (1\ 2)$$

entonces

$$st = (1\ 3\ 2\ 4)(1\ 2) = (1\ 4)(2\ 3)$$

en consecuencia

$$\varepsilon^4 = \tau^2 = (\varepsilon\tau)^2 = 1.$$

Luego, $H = \langle \varepsilon, \tau \rangle \simeq \mathbf{D}_4$.

§3.4. PARIDAD DE UNA PERMUTACIÓN: SUBGRUPO ALTERNADO

Consideremos ahora el siguiente polinomio:

$$P = P(X_1, X_2, \ldots, X_n) = \prod_{1 \le i < j \le n} (X_i - X_j) = (X_1 - X_2)(X_1 - X_3) \ldots$$

$$\ldots (X_1 - X_n)(X_2 - X_3) \ldots (X_{n-1} - X_n).$$

Sea, para cada $t \in \mathbf{S}_n$, el polinomio

$$t(P) = P(X_{t(1)}, X_{t(2)}, \ldots, X_{t(n)}) = \prod_{1 \le i < j \le n} (X_{t(i)} - X_{t(j)}).$$

Es claro que como $t \in \mathbf{S}_n$, para cada par i, j con $1 \le i < j \le n$, uno (y sólo uno) de los polinomios

$$X_i - X_j; \quad X_j - X_i$$

aparece como factor de $t(P)$. Entonces los factores de P y los de $t(P)$ son los mismos (salvo signo), y en consecuencia, para cada $t \in \mathbf{S}_n$, se tiene

$$t(P) = P, \quad \text{o bien} \quad t(P) = -P.$$

58

Definimos $\theta : S_n \to \{1, -1\}$ por la condición de ser:

$$t(P) = \theta(t)P$$

es decir, $\theta(t) = 1$, si $t(P) = P$, en caso contrario $\theta(t) = -1$.

Definición 3.4.7. Se dice que un elemento $t \in \mathbf{S}_n$ es *permutación par (respectivamente impar)* si, y sólo si, $\theta(t) = 1$ (respectivamente $\theta(t) = -1$).

Se tiene las siguientes propiedades:

i) Si $t, u \in \mathbf{S}_n$, entonces $\theta(tu) = \theta(t)\theta(u)$ (equivalentemente, $\theta : \mathbf{S}_n \to \{1, -1\}$ es un homomorfismo).

En efecto, por definición de θ, se tiene

$$\theta(tu)P = (tu)(P) = t(u(P)) = t(\theta(u)P) = \theta(u)t(P) = \theta(u)\theta(t)P =$$

$$= \theta(t)\theta(u)P, \text{ luego } \theta(tu) = \theta(t)\theta(u).$$

ii) Si $t, u \in \mathbf{S}_n$, entonces $\theta(t) = \theta(utu^{-1})$ (equivalentemente, $\theta(t)$ sólo depende de la estructura cíclica de t). Por lo demostrado en i), se tiene

$$\theta(utu^{-1}) = \theta(u)\theta(t)\theta(u^{-1}) = \theta(u)\theta(u)^{-1}\theta(t) = \theta(t).$$

iii) Las transposiciones son permutaciones impares. Como todas las transposiciones son conjugadas, en virtud de ii), basta con verificar que $\theta(1\ 2) = -1$. Si $t = (1\ 2)$, tenemos

$$t(P) = (X_2 - X_1)(X_2 - X_3) \ldots (X_2 - X_n)(X_1 - X_3)(X_1 - X_4) \ldots (X_1 - X_n)(X_3 - X_4) \ldots$$
$$\ldots (X_{n-1} - X_n) = (X_2 - X_1)(X_1 - X_3) \ldots (X_1 - X_4)(X_2 - X_3) \ldots (X_2 - X_n) \ldots$$

$\ldots (X_{n-1} - X_n) = -(X_1 - X_2)(X_1 - X_3) \ldots (X_1 - X_4)(X_2 - X_3) \ldots (X_2 - X_n) \ldots$

$\ldots (X_{n-1} - X_n) = -P$, luego $\theta(1\ 2) = -1$.

Por la propiedad iii), el homomorfismo

$$\theta : \mathbf{S}_n \to [1, -1]$$

es *sobre* (θ es un epimorfismo).

Definición 3.4.8. Se llama *grupo alternado de grado* r al subgrupo invariante $\mathrm{Nu}\,\theta$. Al grupo alternado lo designaremos con $\mathbf{A}_n$. Éste está caracterizado como el subgrupo de $\mathbf{S}_n$ que consiste de las permutaciones pares, así como también como el subconjunto de $\mathbf{S}_n$ de elementos que pueden representarse como el producto de un número par de transposiciones.

Por teoremas de isomorfismo, se tiene

$$\mathbf{S}_n/\mathbf{A}_n \simeq [1, -1]$$

y en consecuencia

$$|\mathbf{A}_n| = \tfrac{1}{2}|\mathbf{S}_n| = \tfrac{1}{2}n!.$$

Ejemplo 1. El elemento $(5\ 2\ 3\ 4) \in \mathbf{S}_5$ no pertenece a $\mathbf{A}_5$. En efecto, se tiene la descomposición

$$(5\ 2\ 3\ 4) = (5\ 4)(5\ 3)(5\ 2)$$

como producto de tres transposiciones, luego $(5\ 2\ 3\ 4)$ es una permutación impar y por tanto no es un elemento de $\mathbf{A}_5$.

Ejemplo 2. Sea el elemento de $\mathbf{S}_8$

$$s = (6\ 7\ 8)(2\ 3\ 5)(1\ 7\ 3)$$

Se tiene la descomposición

$$s = (6\ 8)(6\ 7)(2\ 5)(2\ 3)(1\ 3)(1\ 7)$$

como s se puede escribir como producto de seis transposiciones, entonces es una permutación par y así $s \in \mathbf{A}_8$.

Ejemplo 3. Cualquiera que sea $s \in \mathbf{S}_n$, se tiene $s^2 \in \mathbf{A}_n$: En efecto, si s se puede descomponer como producto de t transposiciones, entonces s^2 podrá descomponerse como producto de $2t$, y por lo tanto $s^2 \in \mathbf{A}_n$. Como consecuencia de esto se tiene

$$\langle s^2 / s \in \mathbf{S}_n \rangle \subseteq \mathbf{A}_n.$$

La recíproca también es válida, y para verificarlo hay que probar que todo elemento de $\mathbf{A}_n$ es producto de cuadrados de $\mathbf{S}_n$. Como los elementos de $\mathbf{A}_n$ son los que se pueden escribir como producto de un número par de transposiciones, basta con verificar que el producto de dos transposiciones es el cuadrado de un elemento en $\mathbf{S}_n$. En efecto, se pueden presentar los siguientes casos:

1) $(a\ b)(c\ d)$, donde a, b, c, d son todos distintos. Entonces

$$(a\ b)(c\ d) = (a\ c\ b\ d)^2.$$

ii) $(a\ b)(a\ c)$, donde a, b, c son distintos; luego

$$(a\ b)(a\ c) = (a\ b\ c)^2$$

iii) $(a\ b)(a\ b)$; a, b distintos. Por lo tanto

$$(a\ b)(a\ b) = (a\ b)^2 = 1.$$

Luego se tiene

$$\mathbf{A}_n = \langle s^2 / s \in \mathbf{S}_n \rangle.$$

Ejemplo 4. Recordemos que para grupo G, el subgrupo conmutador [G, G] es el subgrupo generado por los elementos

$$[x, y] = xyx^{-1}y^{-1} \qquad (x, y \in G)$$

como $\mathbf{A}_n \subseteq \mathbf{S}_n$, se tiene $[\mathbf{A}_n, \mathbf{A}_n] \subseteq [\mathbf{S}_n, \mathbf{S}_n]$. Además, si $x, y \in \mathbf{S}_n$, entonces x, x^{-1} tienen la misma paridad; luego también $x, yx^{-1}y^{-1}$ tienen la misma paridad, lo cual implica $[x, y] \in \mathbf{A}_n$, es decir: $[\mathbf{A}_n, \mathbf{A}_n] \subseteq [\mathbf{S}_n, \mathbf{S}_n] \subseteq \mathbf{A}_n$.

Ejemplo 5. Si $n \geq 3$, $\mathbf{A}_n$ es $(n-2)$-transitivo. En efecto, sean $n \geq 3$, $\{x_1 \ldots x_{n-2}\}$, $\{y_1 \ldots y_{n-2}\}$ dos subconjuntos de X de $(n-2)$ elementos. Luego, existen $z_1, z_2 \in X$ tales que $z_1 \neq y_j$ para $1 \leq i \leq 2$, $1 \leq j \leq n-2$. Por ser $\mathbf{S}_n$ n-transitivo existe $s \in \mathbf{S}_n$ que satisface

$$s(x_i) = y_i$$

Si la permutación s es par, nada queda por demostrar. Si s es impar, la permutación

$$t = (z_1 z_2)s$$

es par y también satisface $t(x_i) = y_i$.

El siguiente ejemplo muestra que $\mathbf{A}_n$ no es $(n-1)$-transitivo. Sea $n = 3$; es imposible hallar $s \in \mathbf{A}_3$ que verifique las dos condiciones

$$s(1) = 2 \text{ y } s(2) = 1$$

En efecto, el único tal $s \in S_3$ que las verifica es $s = (1\ 2)$, que no es elemento de $\mathbf{A}_3$.

Ejemplo 6. Sea $n \geq 2$, entonces $\mathbf{S}_n$ es el producto semidirecto de $\mathbf{A}_n$ y el subgrupo $H = \langle (1\ 2) \rangle$. Sabemos ya que $\mathbf{A}_n$ es invariante en $\mathbf{S}_n$, por lo que sólo queda por verificar

i) $\mathbf{A}_n \cap H = 1$

ii) $\mathbf{S}_n = \mathbf{A}_n H$.

En principio, observemos que $(1\ 2)^2 = (1\ 2)(1\ 2) = 1$, es decir $H = \{1, (1\ 2)\}$. Como $(1\ 2)$ es permutación impar, entonces $(1\ 2) \notin \mathbf{A}_n$, luego resulta i). Sea $s \in \mathbf{S}_n$; si s es permutación par ($s \in \mathbf{A}_n$), entonces $s = s \cdot 1 \in \mathbf{A}_n H$. En caso contrario, $s(1\ 2)$ es par, luego $s(1\ 2) \in \mathbf{A}_n$ y se tiene

$$s = s \cdot 1 = s(1\ 2)(1\ 2) = (s(1\ 2))(1\ 2) \in \mathbf{A}_n H.$$

El siguiente resultado más general es válido:

Proposición 3.4.18. Sea G un subgrupo de $\mathbf{S}_n (n \geq 2)$. Entonces, $G \subseteq \mathbf{A}_n$ o bien el subgrupo de permutaciones pares de G es un subgrupo invariante de índice 2 en G.

Demostración. Si G no posee permutaciones impares, entonces $G \subseteq \mathbf{A}_n$. En caso contrario, sea $t \in G$ una permutación impar. Cuando s recorre todo el grupo G, también lo hace $t \cdot s$, y en consecuencia

$$\sum_{s \in G}' \theta(s) = \sum_{s \in G}' \theta(ts).$$

Pero, como también

$$\sum_{s \in G}' \theta(ts) = \sum_{s \in G}' \theta(t)\theta(s) = \sum_{s \in G}' -\theta(s) = -\sum_{s \in G}' \theta(s).$$

De las dos condiciones se deduce que $\sum_{s \in G}' \theta(s) = 0$.

Como $\theta(s) = \pm 1$, lo anterior significa que en la sumatoria hay tantos sumandos positivos como negativos, o en otras palabras, que G posee el mismo número de permutaciones pares que impares. Como las permutaciones pares de G son los elementos de $G \cap \mathbf{A}_n$, y puesto que éste es invariante en G (pues $\mathbf{A}_n$ es invariante en $\mathbf{S}_n$), el resultado sigue. ▲

El siguiente es un ejemplo típico de cómo se pueden obtener propiedades de grupos abstractos a partir de grupos simétricos.

Corolario. Si G es un grupo de orden $2^k m$ con m impar, y si G posee subgrupos cíclicos de orden 2^k, entonces G posee subgrupos invariantes de índice 2.

Demostración. Sea $n = 2^k m$. Consideremos la representación (Teorema de Cayley)

$$\Phi : G \to S(G) \simeq \mathbf{S}_n, \text{ dada por } \Phi(x)(y) = xy \text{ (para } x, y \in G)$$

sea $x \in G$ un elemento de orden 2^k. Por la misma definición de Φ, el elemento $\sigma' = \Phi(\sigma)$ se descompone como producto de m ciclos disjuntos de longitud 2^k. Los ciclos de longitud 2^k son permutaciones impares; entonces σ' es producto de un número impar $(= m)$ de permutaciones impares y en consecuencia $\sigma' \notin \mathbf{A}_n$. Por la proposición, Im Φ (y entonces G) posee subgrupos invariantes de índice 2. ▲

Proposición 3.4.19. Sea $n > 2$

i) Un ciclo $s = (x_1\, x_2\, \ldots\, x_r) \in \mathbf{S}_n$ es una permutación par si, y sólo si, r es impar.

ii) Si $n \geq 3$, $\mathbf{A}_n$ está generado por la totalidad de 3-ciclos.

Demostración. i) En efecto, $s = (x_1\, x_2\, \ldots\, x_r) = (x_1\, x_r)(x_1\, x_{r-1}) \ldots (x_1\, x_2)$ es una expresión de s como producto de $r - 1$ transposiciones.

ii) Por i), todo 3-ciclo es una permutación par, y por lo tanto, pertenece a $\mathbf{A}_n$. Recíprocamente, veamos que toda permutación par se puede escribir como producto de 3-ciclos. Para ello será suficiente probar que todo producto de dos transposiciones se escribe como producto de 3-ciclos. Tres casos debemos considerar:

1. $(a\ b)(c\ d)$ con a, b, c y d distintas: Entonces $(a\ b)(c\ d) = (a\ b\ c)(b\ c\ d)$.
2. $(a\ b)(c\ a)$ con a, b y c distintas: $(a\ b)(c\ a) = (a\ b)(a\ c) = (a\ c\ b)$.
3. $(a\ b)(a\ b)$ con a y b distintas: $(a\ b)(a\ b) = 1 = (a\ b\ c)(a\ b\ c)(a\ b\ c)$ ▲

Corolario 1. Si $n \geq 3$, $\mathbf{A}_n$ está generado por los 3-ciclos de la forma

$$(1\ 2\ 3),\ (1\ 2\ 4), \ldots, (1\ 2\ n).$$

Demostración. Por la proposición 3.4.19, parte ii), basta con probar todo 3-ciclo $(a\ b\ c)$ puede obtenerse a partir de 3 ciclos de la forma $(1\ 2\ t)$ $(3 \leq t \leq n)$. Cualquiera que sean a, b y c distintos, se tiene

$$(a\ b\ c) = (1\ c\ b)(1\ a\ b)(1\ 2\ c).$$

Por lo tanto, será suficiente mostrar que todo 3-ciclo de la forma $(1\ a\ b)$ se puede descomponer como producto de 3-ciclos de la forma $(1\ 2\ t)(3 \leq t \leq n)$. Sea entonces $(1\ a\ b)$ con 1, a y b distintos. Se presentan tres casos posibles:

i) $(1\ a\ b)$ con $a = 2$, en cuyo caso $(1\ 2\ b)$ ya tiene la forma requerida y nada hay que demostrar.

ii) $(1\ a\ b)$ con $b = 2$, en este caso vale que $(1\ a\ b) = (1\ a\ 2) = (1\ 2\ a)^2$, y por lo tanto, también está resuelto.

iii) $(1\ a\ b)$ con $a \neq 2$, $b \neq 2$. En este caso, se tiene la descomposición $(1\ a\ b) = (1\ 2\ b)(1\ 2\ a)(1\ 2\ b)$, que completa la demostración. ▲

Corolario 2. Si $n \geq 3$, la totalidad de permutaciones del tipo $(i\ i+1)(j\ j+1)$ (para $1 \leq i, j \leq n$, $i \neq j \neq i+1$) generan $\mathbf{A}_n$.

Demostración. Sea H el subgrupo generado por las permutaciones del tipo anterior. Como H consiste de permutaciones pares, entonces se tiene $H \subseteq \mathbf{A}_n$. Para demostrar la otra inclusión sera suficiente verificar que $(1\ 2\ t) \in H$, siempre que $(1 \leq t \leq n)$, en virtud del corolario 1.

Inducción en n. Si $n = 3$, entonces $((2\ 3)(1\ 2))^2 = (1\ 3\ 2)^2 = (1\ 2\ 3) \in H$, luego $H = \mathbf{A}_3$. Supongamos válido el resultado para $n \geq 3$, y en consecuencia las permutaciones $(1\ 2\ t) \in H$ con $1 \leq t < n$.

Como $(1\ 2)(n\ n+1) \in H$, $x = (1\ 2)(n\ n+1)(1\ 2\ n)(1\ 2)(n\ n+1) = (2\ n+1) \in H$, entonces también $x^2 = (1\ 2\ n+1) \in H$, así $(1\ 2\ t) \in H (1 \leq t \leq n+1)$, con lo que $\mathbf{A}_n \subseteq H$. ▲

Ejemplo 1. Veamos que $\mathbf{A}_4$ no posee subgrupos de orden 6. En efecto, sea H un tal subgrupo. Entonces H posee elementos de orden 2 y de orden 3 (por el teorema de Cauchy).

Sea $x \in H$ de orden 2. La estructura cíclica de elementos de orden 2 en $\mathbf{S}_4$ es una de las siguientes:

i) $(\ .\ )(\ .\ )$ ii) $(\ .\ .\ )$.

La segunda corresponde a elementos que no pertenecen a $\mathbf{A}_4$, pues son permutaciones impares. Se tiene entonces $x = (a\ b)(c\ d)$. Sea $y \in H$ de

orden 3, y entonces y es un 3-ciclo. Sin pérdida de generalidad supongamos $y = (a\ b\ c) \in H$. Luego $xyx^{-1} = (b\ a\ d) \in H$.

Por consiguiente, los siguientes cuatro elementos de orden 3 son distintos y pertenecen al subgrupo H

$$y,\ y^2,\ xyx^{-1},\ xy^2x^{-1}.$$

Pero, como H es de orden 6, por el teorema de estructura de grupos de orden pq (teorema 2.8.4) H no puede tener más de 2 elementos de orden 3. Esto es un absurdo que proviene de haber supuesto que $\mathbf{A}_4$ tiene subgrupos de orden 6.

Respecto a los subgrupos abelianos de $\mathbf{S}_n$, se puede probar el siguiente resultado: Si G es un subgrupo abeliano de $\mathbf{S}_n$, entonces $|G| \leq 3^{[n/3]}$

$([n/3]$ = parte entera de $n/3)$.

La cota es óptima, pues si $n = 3k + t$ $(0 \leq t < 3)$, entonces el grupo generado por los k elementos de orden 3

$$\begin{aligned} x_1 &= (1\ 2\ 3) \\ x_2 &= (4\ 5\ 6) \\ &\cdots\cdots\cdots \\ &\cdots\cdots\cdots \\ x_k &= (3k-2\ 3k-1\ 3k) \end{aligned}$$

es abeliano (los generadores conmutan) y tiene orden $3^{[n/3]} = 3^k$.

Ejemplo 2. El único subgrupo de orden 12 de $\mathbf{S}_4$ es $\mathbf{A}_4$. Sea H un subgrupo de orden 12. Se tiene

$$k = |\mathbf{S}_4 : H \cap \mathbf{A}_4| \leq |\mathbf{S}_4 : H| \cdot |\mathbf{S}_4 : \mathbf{A}_4| = 2 \cdot 2 = 4.$$

Por lo tanto, dicho índice puede ser 1, 2, 3 ó 4.

i) El caso $k = 1$ está descartado, pues implica $\mathbf{S}_4 = H \cap \mathbf{A}_4 \subseteq \mathbf{A}_4$, luego sería $\mathbf{S}_4 = \mathbf{A}_4$, lo que es absurdo.

ii) Si $k = 2$, entonces $|H \cap \mathbf{A}_4| = 12$, y como $H \cap \mathbf{A}_4 \subseteq \mathbf{A}_4$, por razones de orden debe ser $H = \mathbf{A}_4$.

iii) Si fuera $k = 3$, sería $|H \cap \mathbf{A}_4| = 8$. Pero, entonces, $H \cap \mathbf{A}_4$, sería un subgrupo de orden 8 del grupo $\mathbf{A}_4$ (de orden 12); esto es imposible según el Teorema de Lagrange.

iv) Si fuera $k = 4$, se tendría $|H \cap \mathbf{A}_4| = 6$. Pero ya sabemos que $\mathbf{A}_4$ no posee subgrupos de orden 6. Luego este caso tampoco es posible.

En el capítulo 5 se probará que para $n \neq 4$, los únicos subgrupos invariantes de $\mathbf{S}_n$ son 1, $\mathbf{A}_n$ y $\mathbf{S}_n$. A partir de este hecho y de que todo subgrupo de índice 2 es invariante, demostraremos que el único subgrupo de orden $\frac{1}{2}n!$ en $\mathbf{S}_n$ es $\mathbf{A}_n$.

Ejemplo 3. El grupo G de rotaciones del tetraedro es isomorfo a $\mathbf{A}_4$. En efecto, a cada rotación r del tetraedro se le puede asociar la permutación de los cuatro vértices inducida por r. Esto da un homomorfismo

$$f : G \to S_4.$$

Pero f es un monomorfismo, pues si r es una rotación que deja los cuatro vértices fijos ($f(r) = \mathrm{Id}$), entonces r debe ser la rotación nula ($r = \mathrm{Id}$). Entonces $G \simeq \mathrm{Im} f$, que es un subgrupo de orden 12 en S_4. Como hemos visto que el único subgrupo con esa propiedad es A_4, se tiene $\mathrm{Im} f = A_4$, con lo cual $G \simeq A_4$.

Ejemplo 4. El grupo de rotaciones del cubo es isomorfo a S_4.

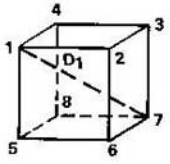


Fig. 5.

Sea G dicho grupo. Sabemos que $|G| = 24$. El cubo, cuyos vértices se han numerado 1, 2 ... 8 posee 4 diagonales principales, a saber

$$D_1 : \overline{1\,7} \qquad D_2 : \overline{2\,8} \qquad D_3 : \overline{3\,5} \qquad D_4 : \overline{4\,6}$$

Todo elemento $r \in G$ permuta entre sí las diagonales D_i, y entonces tenemos definido un morfismo

$$f : G \to S_4$$

que hace corresponder a cada rotación $r \in G$, la permutación inducida entre las diagonales. Si, para una rotación dada, una diagonal (digamos D_1) queda fija, entonces, o bien D_1 es el eje de la rotación, o bien la rotación cambia entre sí los puntos extremos 1 y 7. En este último caso, si 0 es el punto medio del lado $\overline{2\,6}$ y $0'$ es el del $\overline{4\,8}$, la rotación debe corresponder al eje $\overline{00'}$ en un ángulo π. Análogamente, si una rotación deja fija la diagonal D_3, debe ser de eje D_3, o de eje $\overline{00'}$.

En consecuencia, si una rotación $r \in G$ deja fijas las cuatro diagonales, entonces por dejar fijas las diagonales D_1 y D_3 debe ser una rotación de eje $\overline{00'}$; pero las rotaciones ($\neq 1$) de este tipo permutan entre sí las diagonales D_2 y D_4, y por lo tanto, necesariamente, $r = 1$. Esto prueba que el morfismo

$$f : G \to S_4$$

es inyectivo, y como los grupos en cuestión tienen el mismo orden, debe ser isomorfo.

Al probarse que el único subgrupo de índice 2 de S_5 es A_5 se puede demostrar que el grupo de rotaciones del icosaedro es isomorfo a A_5.

Ejemplo 5. Sabemos que cualquiera que sea $n \in \mathbf{N}$, se tiene

$$[A_n, A_n] \subseteq [S_n, S_n] \subseteq A_n$$

Afirmamos:

i) Si $n \geq 3$, entonces $[S_n, S_n] = A_n$.

ii) Si $n \geq 5$, entonces $[A_n, A_n] = A_n$.

i) En efecto, para probar que $A_n \subseteq [S_n, S_n]$, como A_n está generado por 3-ciclos, bastará con probar que todo 3-ciclo $(a\ b\ c) \in [S_n, S_n]$. Así es, pues

$$(a\ b\ c) = (a\ b)(a\ c)(a\ b)(a\ c) = (a\ b)(a\ c)(a\ b)^{-1}(a\ c)^{-1} \in [S_n, S_n].$$

ii) Debemos probar que todo 3-ciclo pertenece a $[A_n, A_n]$, por las mismas razones que antes.

Sea $t = (a\ b\ c)$ un 3-ciclo; como $n \geq 5$ se puede hallar d y e tal que a, b, c, d y e sean todos distintas, entonces

$$(a\ b\ c) = [(d\ c\ a)(a\ e\ d)][(a\ e\ d)(d\ b\ a)]$$

es producto de dos elementos de $[A_n, A_n]$, y en consecuencia $A_n \subseteq [A_n, A_n]$.

Consideremos $n = 4$, y calculemos $[A_4, A_4]$: Sean los elementos de A_4:

$$a = (1\ 2)(3\ 4) \qquad b = (1\ 3)(2\ 4) \qquad c = (1\ 4)(2\ 3)$$

y consideremos el subgrupo $H = \{1, a, b, c\}$.

El subgrupo H es invariante en A_4 (también en S_4), pues si $t \in A_4$: $t(xy)(zw)t^{-1} = t(xy)t^{-1}t(zw)t^{-1} = (t(x)t(y))(t(z)t(w))$ es necesariamente uno de los elementos de H (que son los únicos con estructura cíclica 2,2). Ahora bien, el cociente A_4/H tiene orden 3, luego es *abeliano* (isomorfo a Z_3), y de aquí se deduce que $[A_4, A_4] \subseteq H$.

Para la otra inclusión, obsérvese que

$$a = [(1\ 2\ 3)(3\ 4\ 1)], \qquad b = [(1\ 3\ 2)(2\ 4\ 1)], \qquad c = [(1\ 4\ 2)(2\ 3\ 1)^2].$$

Luego $[A_4, A_4] = H \neq A_4$.

§ 3.5. CENTRO DE S_n Y A_n

Proposición 3.5.20. Para S_n y A_n tenemos: i) Si $n \geq 3$, $z(S_n) = I$.

ii) Si $n \geq 4$, $z(A_n) = I$.

Demostración. i) Sea $x \in z(S_n)$, y supóngase x descompuesto como producto de ciclos disjuntos. Sea $x \neq I$.

a) Si x posee por lo menos 2 ciclos no triviales, digamos

$$x = (x_1 x_2 \ldots)(y_1 y_2 \ldots) \ldots$$

consideremos $t = (x_1 y_1 y_2) \in S_n$ y se verifica

$$txt^{-1} = (y_1 x_2 \ldots)(y_2 x_1 \ldots) \neq x.$$

b) Si x posee sólo un ciclo de longitud ≥ 3, digamos

$$x = (x_1 x_2 x_3 \ldots)$$

consideremos $h = (x_1 x_2) \in S_n$, y se tiene

$$hxh^{-1} = (x_2 x_1 x_3 \ldots) \neq x.$$

c) Si x posee sólo un ciclo de longitud < 3, entonces

$$x = (x_1 x_2).$$

Ahora, como $n \geq 3$, existe $y \in X$ tal que $y \neq x_1$ e $y \neq x_2$. Consideremos $v = (x_1 y) \in S_n$

$$vxv^{-1} = (y x_2) \neq x$$

con lo cual quedan agotadas todas las posibilidades.

ii) Sea, como antes, $x \in z(\mathbf{A}_n)$, $x \neq 1$, descompuesto como producto de ciclos disjuntos, $n \geq 4$.

a) Si x posee por lo menos dos ciclos no triviales, repetimos el razonamiento hecho en el caso i)a), pues adviértase que $t \in \mathbf{A}_n$.

b) Si x posee un solo ciclo y éste es de longitud ≥ 4. Por lo tanto

$$x = (x_1 x_2 x_3 x_4 \ldots)$$

consideremos en este caso $w = (x_1 x_2)(x_3 x_4) \in \mathbf{A}_n$, por lo tanto

$$wxw^{-1} = (x_2 x_1 x_4 x_3 \ldots) \neq x.$$

c) Si x posee un solo ciclo y éste es de longitud < 4, por ser $x \in \mathbf{A}_n$, debe tener longitud 3

$$x = (x_1 x_2 x_3).$$

Teniendo en cuenta que $n \geq 4$, existe $y \in X$ tal que $y \neq x_i$ $(i = 1, 2, 3)$. Consideremos entonces $y = (x_1 x_2)(x_3 y) \in \mathbf{A}_n$

$$yxy^{-1} = (x_2 x_1 y) \neq x.$$

La proposición nos dice que $I: G \to \mathrm{Aut}(G)$, definida por $I(x)(y) = xyx^{-1}$, es un monomorfismo en los casos

$$G = \mathbf{S}_n (n \geq 3) \qquad G = \mathbf{A}_n (n \geq 4).$$

Puede verse que en el primer caso I es un isomorfismo, excepto si $n = 6$ (es decir, $\mathbf{S}_n$ es completo), en tanto que en el segundo no lo es. Como $\mathbf{A}_n$ es invariante en $\mathbf{S}_n$, cabe considerar también $\Phi: \mathbf{S}_n \to \mathrm{Aut}(\mathbf{A}_n)$ en la forma $\Phi(s)(t) = sts^{-1}$, y en dicho caso Φ sí es un isomorfismo.

Es válido el siguiente resultado general:

Teorema 3.5.6. Si $n \geq 3$ y $n \neq 6$ $\mathrm{Aut}(\mathbf{S}_n) = \mathbf{S}_n$ e $I: \mathbf{S}_n \to \mathrm{Aut}(\mathbf{S}_n)$ es isomorfismo. Por otra parte el homomorfismo $\Phi: \mathbf{S}_n \to \mathrm{Aut}(\mathbf{A}_n)$ dado por $\Phi(x)(y) = xyx^{-1}$ es también isomorfismo. Estos resultados se demuestran en el Apéndice II.

§3.6. TEOREMAS DE CARACTERIZACIÓN

Los siguientes teoremas caracterizan a los grupos $\mathbf{S}_n$ y $\mathbf{A}_n$ como grupos definidos por generadores y relaciones (véase el capítulo 1). Las demostraciones se deben a E.H. Moore (1897).[36]

Teorema 3.6.7. Sea $k \geq 2$. Sea G un grupo con generadores $x_1, \ldots, x_{k-1}$, que satisfacen las relaciones

1) $x_i^2 = 1 \qquad (1 \leq i \leq k-1)$

2) $x_i x_j = x_j x_i \quad (1 \leq i, j \leq k-1, \; j \neq i \pm 1)$

3) $x_j x_{j+1} x_j = x_{j+1} x_j x_{j+1} \quad (1 \leq j \leq k-2)$.

Entonces, $G \simeq \mathbf{S}_k$.

Demostración. Si $k = 2$, el resultado es inmediato. Sabemos (véase el teorema 3.3.5, corolario 3) que $\mathbf{S}_k$ está generado por elementos

$$y_i = (i\ i+1)$$

que satisfacen las relaciones 1), 2) y 3) (y, eventualmente, otras); por lo tanto, de acuerdo con lo visto en el capítulo I debe haber un subgrupo invariante H de G tal que

$$G/H \simeq S_k$$

y, consecuentemente, $|G| \geq k!$.

Consideremos el subgrupo G' de G donde

$$G' = (x_1, x_2, \ldots, x_{k-2}).$$

Cabe suponer, por hipótesis inductiva, que

$$G' \simeq S_{k-1}$$

y, consecuentemente, $|G'| = (k-1)!$

ya que G' admite generadores $x_i (1 \leq i \leq k-2)$ que satisfacen las relaciones 1), 2) y 3). Consideremos ahora los siguientes subconjuntos de G

$$\begin{aligned} C_1 &= G' x_{k-1} \cdot x_{k-2} \ldots x_2 \cdot x_1 \\ C_2 &= G' x_{k-1} \cdot x_{k-2} \ldots x_2 \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ C_{k-1} &= G' x_{k-1} \\ C_k &= G'. \end{aligned}$$

Es claro que $|C_i| = |C_k| = (k-1)!$ Ahora bien, sea r tal que $1 \leq r \leq k-1$, entonces

$$C_{r+1} x_r = G' x_{k-1} \ldots x_{r+1} x_r = C_r$$

$$C_r x_r = G' x_{k-1} \ldots x_{r+1} x_r x_r = C_{r+1}$$

(ya que $x_r^2 = 1$).

Si $i > r+1$, se tiene

$$C_i x_r = G' x_{k-1} \ldots x_i x_r = G' x_r x_{k-1} \ldots x_i = G' x_{k-1} \ldots x_i = C_i$$

(pues $x_i x_r = x_r x_i$, $x_{i+1} x_r = x_r x_{i+1} \ldots x_{k-1} x_r = x_r x_{k-1}$, y además $G' x_r = G'$, dado que $x_r \in G'$).

Por último, si $i \leq r$, resulta

$$\begin{aligned} C_i x_r &= G' x_{k-1} \ldots x_{r+1} x_r x_{r-1} \ldots x_i x_r = G' x_{k-1} \ldots x_{r+1} (x_r x_{r-1} x_r) x_{r-2} \ldots x_i = \\ &= G' x_{k-1} \ldots x_{r+1} x_{r-1} x_r x_{r-1} x_{r-2} \ldots x_i = \\ &= G' x_{r-1} x_{k-1} \ldots x_{r+1} x_r x_{r-1} x_{r-2} \ldots x_i = G' x_{k-1} \ldots x_i = C_i \end{aligned}$$

(utilizando las relaciones 2), 3) y el hecho de que $x_{r-1} \in G'$).

Se ha probado entonces que cualesquiera que sean i, r con $1 \leq i \leq k-1$, $r \leq k-1$), existe j con $1 \leq j \leq k-1$ tal que

$$C_i x_r = C_j.$$

En consecuencia, cualquiera que sea $x \in G$ se tendrá que, para cada $i (1 \leq i \leq k-1)$, existe j con $1 \leq j \leq k-1$ tal que

$C_i x = C_j$ (por ser x producto de los generadores x_r $(1 \leq r \leq k-1)$).

Es así que el producto arbitrario de un elemento de alguno de los conjuntos C_i por un elemento arbitrario x de G siempre pertenece a alguno de los conjuntos mencionados.

En particular, si se toma siempre $1 \in C_k$, se concluye que todo elemento de G pertenece a algún C_i; entonces

$$G \subseteq \bigcup_{1 \le i \le k} C_i$$

y por lo tanto

$$|G| \le \sum_{1 \le i \le k} |C_i| = k|C_k| = k(k-1)! = k!$$

Se deduce entonces que $|G| = k!$, entonces $H = 1$, y así $G \simeq \mathbf{S}_k$. ▲

Nota. Obsérvese que las relaciones 1), 2) y 3) del teorema anterior se pueden combinar en la fórmula

$$1 = x_i^2 = (x_i x_{i+1})^3 = (x_i x_j)^2 \text{ para } (1 \le i, j \le k-1,\ j > i+1) \quad (*)$$

Teorema 3.6.8. Sea $k \ge 3$ y sea G un grupo generado por los elementos $y_1, y_2, \ldots, y_{k-2}$, los cuales satisfacen las relaciones

$$1 = y_i^3 = y_{i+1}^2 = (y_i y_{i+1})^3 = (y_i y_j)^2 \quad (**)$$

(para $1 \le i, j \le k-2$, $j > i+1$). Entonces, $G \simeq \mathbf{A}_k$.

Demostración. Sea G un tal grupo, Consideremos un nuevo grupo G' generado por los y_i y un nuevo elemento x_1 tal que, además de (**), se satisfaga

$$x_1^2 = 1,\ y_i x_1 = x_1 y_i^{-1} \quad (1 \le i \le k-2) \quad (***)$$

Si escribimos

$$x_{i+1} = y_i x_1 \quad (1 \le i \le k-2)$$

Entonces

$$G' = \langle x_1, y_1, \ldots, y_{k-2} \rangle = \langle x_1, x_2, \ldots, x_{k-1} \rangle.$$

Ahora bien las relaciones (**) y (***) equivalen a las relaciones (*), y por el teorema anterior, $G' \simeq \mathbf{S}_k$, luego $|G'| = k!$. Habiendo ampliado el grupo G al grupo G' mediante la introducción de un nuevo generador x_1, de forma que se satisfaga (***), es claro que

$$G' = G \cup G_{x_1}$$

y por lo tanto $|G| = k!/2$.

Queda sólo por probar que, en el isomorfismo $G' \simeq \mathbf{S}_k$, el grupo G se aplica en $\mathbf{A}_k$ o, por razones de orden, que la imagen de G en dicho isomorfismo consiste en permutaciones pares. Para ello sera suficiente probar que los generadores y_i de G se aplican en permutaciones pares; y con este fin, teniendo en cuenta que $y_i = x_{i+1} x_1$, bastará con probar a su vez que todos los $x_i (1 \le i \le k-1)$ tienen la misma paridad.

En efecto, de la relación $(x_i x_{i+1})^3 = 1$, se deduce que la paridad de x_i es la misma que la del elemento $x_{i+1} x_i x_{i+1}^{-1} = x_i x_{i+1} x_i^{-1}$ (por ser conjugados), la cual es a la vez la paridad de x_{i+1} (por la misma razón); repitiendo el proceso resulta que los $x_i (1 \le i \le k-1)$ tienen todos la misma paridad. La demostración está completa. ▲

§3.7. REPRESENTACIONES

En lo que resta de este capítulo se estudiarán las representaciones lineales de un grupo finito G, es decir, morfismo $f: G \to GL(n, K)$ para K cuerpo. De aquí en adelante, G designa un grupo finito y supondremos que el cuerpo K es **C**: el cuerpo de los números complejos, aunque se previene al lector que muchos de los resultados continúan siendo válidos sobre cuerpos K algebraicamente cerrados de característica 0, o característica p, tal que $p \nmid |G|$.

Definición 3.7.9. Sea V un espacio vectorial de dimensión finita sobre el cuerpo **C** de números complejos y G un grupo finito. Una *representación de* G *en* V es un homomorfismo

$$\rho : G \to \mathrm{Aut}(V)$$

donde Aut(V) denota el grupo de automorfismos del **C**-espacio vectorial V. En estas condiciones, se dice que V es el *espacio de la representación* ρ. Si el espacio vectorial V tiene dimensión n, se dice que n *es el grado de la representación* ρ.

Sea $[v_i] = \{v_1 \dots v_n\}$ una **C**-base de V; en estas condiciones, la aplicación $f \to \|f\|$ define un isomorfismo entre Aut(V) y el grupo $GL(n, \mathbf{C})$ de matrices inversibles de $n \times n$ con coeficientes en el cuerpo **C**. En consecuencia, se tiene un homomorfismo

$$R : G \to GL(n, \mathbf{C}) \text{ definido por } R(x) = \|\rho(x)\|_{[v_i]}$$

Recíprocamente, todo homomorfismo de G en $GL(n, \mathbf{C})$ induce una representación de G en V. Por lo tanto, una forma equivalente de definir la representación de un grupo finito G es llamar así a todo homomorfismo $R : G \to GL(n, \mathbf{C})$. Es importante observar que la correspondencia biunívoca $\rho \leftrightarrow R$ depende de la elección de una base en el espacio vectorial V.

Definición 3.7.10. Sean ρ y ρ' dos representaciones del grupo G en espacios vectoriales V y V'. Se dice que las representaciones son equivalentes ($\rho \sim \rho'$) sí, y sólo si, existe un isomorfismo $\sigma : V \to V$ tal que

$$\sigma \circ \rho(x) = \rho'(x) \circ \sigma \qquad (x \in G).$$

Es inmediato que la relación anterior es de equivalencia en la clase de todas las representaciones del grupo G. Análogamente, dados los morfismos $R, R' : G \to GL(n, \mathbf{C})$, diremos que son equivalentes si, y sólo si, existe $T \in GL(n, \mathbf{C})$ tal que

$$TR(x) = R'(x)T \qquad (x \in G).$$

Ahora es claro que en la correspondencia $\rho \leftrightarrow R$, $\rho' \leftrightarrow R'$, se tiene $\rho \sim \rho'$ si, y sólo si, $R \sim R'$. En efecto, si R es la matriz de ρ en la base $[v_i]$ de V y R' lo es de ρ' en la base $[v_i']$ de V', la matriz T es la matriz de σ en las bases $[v_i]$ y $[v_i']$.

Ejemplo 1. Una representación de grado 1 de un grupo finito G no es otra cosa que un homomorfismo de G en C* (grupo multiplicativo de complejos no nulos). Si $\rho : G \to C^*$ es una tal representación, como G es finito ($n = |G|$), entonces $x^n = 1$ para todo $x \in G$ y, en consecuencia, $\rho(x)^n = \rho(x^n) = \rho(1) = 1$. Se deduce entonces que $\rho(x)$ es raíz n-ésima de

la unidad. En particular, si se define $\rho(x) = 1$ para todo $x \in G$, se obtiene una representación de grado 1, la cual se denomina *representación unitaria de* G.

Si consideramos $G = \mathbf{Z}_n$, las representaciones de grado 1 son los posibles morfismos de $\mathbf{Z}_n$ en el grupo $\mathbf{G}_n$ de las n-raíces de la unidad. Como $\mathbf{Z}_n$ es cíclico, cada morfismo queda determinado por la imagen de un generador. Sea $1 \in \mathbf{Z}_n$ el generador canónico de $\mathbf{Z}_n$, entonces para $w \in \mathbf{G}_n$ existe una presentación

$$\rho_w : \mathbf{Z}_n \to \mathbf{C}^* \qquad \rho_w(1) = w, \text{ es decir } \rho_w(t) = w^t \qquad (0 \leq t < n).$$

Ejemplo 2. Sea G un grupo de orden n, y sea V un **C**-espacio vectorial de dimensión n con base $[v_t]_{t \in G}$. Sea, para cada $x \in G$, el endomorfismo $\rho(x)$ que satisface

$$\rho(x)(v_t) = v_{xt}.$$

Como, para cada $x \in G$, $\rho(x)$ permuta una base de V, entonces $\rho(x) \in \in \mathrm{Aut}(V)$. Además, si $x, y, t \in G$, se tiene

$$\rho(xy)(v_t) = v_{xyt} = \rho(x)(v_{yt}) = \rho(x)(\rho(y)(v_t)) = (\rho(x) \circ \rho(y))(v_t)$$

$$\therefore \rho(xy) = \rho(x) \circ \rho(y)$$

y en consecuencia, $\rho : G \to \mathrm{Aut}(V)$ es una representación llamada *representación regular*. El grado de la representación regular coincide con el orden de G. Por ejemplo, si se considera el grupo simétrico $\mathbf{S}_3 = \{1, (12), (13), (23), (123), (132)\}$ es claro que ρ queda determinada al conocer su acción sobre el sistema de generadores $\{(12), (123)\}$ de $\mathbf{S}_3$. El lector puede verificar que

$$R(12) = \begin{Vmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{Vmatrix} \qquad R(123) = \begin{Vmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{Vmatrix}$$

Sea, como siempre, G un grupo finito. La totalidad de sumas formales

$$\sum_{t \in G} \alpha_t \cdot t \qquad (\alpha_t \in \mathbf{C})$$

tiene una estructura natural algebraica sobre **C**, definiendo

$$\sum_{t \in G} \alpha_t \cdot t + \sum_{t \in G} \beta_t \cdot t = \sum_{t \in G} (\alpha_t + \beta_t) t$$

$$\left(\sum_{r \in G} \alpha_r \cdot r \right) \cdot \left(\sum_{s \in G} \beta_s \cdot s \right) = \sum_{r,s \in G} (\alpha_r \beta_s) rs = \sum_{t \in G} \gamma_t \cdot t$$

(donde $\gamma_t = \sum_{\substack{r,s \in G \\ rs = t}} \alpha_r \beta_s$. Se denomina *álgebra del grupo de* G *sobre* **C** y se denota por $\mathbf{C}(G)$.

Para cada $t \in G$, podemos considerar la suma formal $1 \cdot t (1 \in \mathbf{C})$, es decir

$$1 \cdot t + \sum_{s \neq t} 0 \cdot s$$

y la aplicación $G \to \mathbf{C}(G)$ inducida es un monomorfismo que identifica a G con un subgrupo del grupo de unidades $U(\mathbf{C}(G))$ de $\mathbf{C}(G)$. Es evidente, además, que $\{1 \cdot t / t \in G\}$ es una $\mathbf{C}$-base de $\mathbf{C}(G)$. Ahora bien, si $\rho : G \to \mathrm{Aut}(V)$ es una representación de G, entonces V puede convertirse en $\mathbf{C}(G)$ módulo unitario definiendo la acción de $t \in G$ por

$$t \cdot v = \rho(t)(v) \qquad (t \in G)(v \in V) \tag{$*$}$$

y luego extender por linealidad, es decir

$$\left(\sum_{t \in G} \alpha_t \cdot t\right) \cdot v = \sum_{t \in G} \alpha_t \rho(t)(v).$$

Recíprocamente, si V es $\mathbf{C}(G)$ módulo *unitario*, la relación $(*)$ permite definir una representación ρ de G en V. (Los detalles se dejan a cargo del lector.) Por otra parte, según nuestra definición, dos representaciones ρ_1 y ρ_2 con espacios V_1 y V_2 son equivalentes si, y sólo si, existe un isomorfismo de $\mathbf{C}$-espacios vectoriales $\sigma : V_1 \to V_2$ tal que $\sigma \circ \rho_1(x) = \rho_2(x) \circ \sigma$, o sea

$$\sigma(xv) = x\sigma(v) \qquad (x \in G)(v \in V)$$

esto es, σ es isomorfismo de $\mathbf{C}(G)$-módulos.

En consecuencia, representaciones equivalentes corresponden a $\mathbf{C}(G)$-módulos isomorfos. Luego el estudio de representaciones de un grupo G equivale al de $\mathbf{C}(G)$-módulos unitarios. 71

Ejemplo. La representación regular corresponde al anillo $\mathbf{C}(G)$ considerado como un módulo sobre sí mismo. En efecto, sobre la $\mathbf{C}$-base $\{1 \cdot t / t \in G\}$ de $\mathbf{C}(G)$, la acción del anillo $\mathbf{C}(G)$ es

$$\rho \cdot (1 \cdot t) = 1 \cdot \rho t \qquad (\rho, t \in G)$$

la cual coincide con la correspondiente a la representación regular.

Definición 3.7.11. Sea $\rho : G \to \mathrm{Aut}(V)$ una representación, y sea W un subespacio de V. Se dice que W *es estable bajo* G, o también G-invariante, si, y sólo si,

$$x \in G,\ w \in W \to \rho(x)(w) \in W$$

(según la interpretación anterior, los subespacios estables no son otra cosa que los $\mathbf{C}(G)$-submódulos de V). En este caso, para cada $x \in G$, la restricción a W del automorfismo $\rho(x)$ es un automorfismo de W. En esta situación se tiene definido un morfismo

$$\rho^* : G \to \mathrm{Aut}(W) \qquad \rho^*(x) = \rho(x)|_W$$

el cual es una representación de G en W. En este caso, diremos que ρ^* es una *subrepresentación de* ρ.

Ejemplo. Sea ρ la representación regular de un grupo G, y sea V el espacio de la representación con base $[v_t]_{t \in G}$. Consideremos el

vector $v = \sum_{t \in G} v_t$, y el subespacio generado por él $W = \langle v \rangle$. Por la independencia lineal, $v \neq 0$; luego, W tiene dimensión 1. Además

$$\rho(x)(v) = \rho(x)\Big(\sum_{t \in G} v_t\Big) = \sum_{t \in G} \rho(x)(v_t) = \sum_{t \in G} v_{xt} = v$$

y de ahí se concluye que W es G-invariante, y que ρ^W equivale a la representación unitaria de G.

Por otra parte, el subespacio $W' = \langle v_t / t \in G,\ t \neq 1 \rangle$ no es G-estable, pues para $t \neq 1$, $v_t \in W'$, y en cambio

$$\rho(t^{-1})(v_t) = v_{t^{-1}t} = v_1 \notin W'$$

obsérvese que $W + W' = V$, y que $W \cap W' = 0$ esto es, W' es complementario de W. Sin embargo, siempre es posible hallar un complementario G-invariante.

Teorema 3.7.9. Sea $\rho : G \to \mathrm{Aut}(V)$ una representación de G en V, y sea W un subespacio G-invariante de V. En tal caso existe un complementario W° de W en V que también es G-invariante.

72 **Demostración.** Sea W' un complementario cualquiera de W en V, y sea $p : V \to V$ el proyector asociado ($\mathrm{Nu}p = W'$, $\mathrm{Im}p = W$). Consideremos la transformación lineal

$$p^\circ = \frac{1}{n} \sum_{t \in G} \rho(t) \circ p \circ \rho(t^{-1})$$

(donde n = orden de G).

Como p aplica V en W y W es G-invariante, entonces $p^\circ : V \to W$. Por otra parte, si $w \in W$, entonces $\rho(t^{-1})(w) \in W$, luego $p(\rho(t^{-1})(w)) = \rho(t^{-1})(w)$, y en consecuencia $\rho(t)(\rho(t^{-1})(w))) = \rho(t) \circ \rho(t^{-1})(w) = w$. Por lo tanto, para $w \in W$ se tiene $p^\circ(w) = w$. Se deduce que p° es un proyector de V sobre W correspondiente a un cierto complementario $W^\circ = \mathrm{Nu}p^\circ$ de W.

Además, se tiene para cualquier $x \in G$

$$\rho(x)p^\circ\rho(x^{-1}) = \frac{1}{n} \sum_{t \in G} \rho(x)\rho(t) \circ p \circ \rho(t^{-1})\rho(x^{-1}) =$$

$$= \frac{1}{n} \sum_{t \in G} \rho(xt) \circ p \circ \rho((xt)^{-1}) = \frac{1}{n} \sum_{t \in G} \rho(t)\rho(t^{-1}) = p^\circ,$$

es decir $\rho(x) \circ p^\circ = p^\circ \circ \rho(x)$ para todo $x \in G$. Si suponemos $w \in W^\circ = \mathrm{Nu}p^\circ$, $x \in G$ entonces $0 = \rho(x) \circ p^\circ(w) = p^\circ(\rho(x)(w))$, es decir $\rho(x)(w) \in \mathrm{Nu}p^\circ = W^\circ$.

Por consiguiente, W° es G-invariante y el teorema está probado. ▲

Ejemplo. Volvamos al ejemplo anterior. El proyector p que corresponde al complemento W' está determinado por

$$p(v_1) = \sum_{t\in G} v_t, \quad p(v_t) = 0 \quad (\text{si } t \neq 1).$$

En consecuencia, si $x \in G$, se tiene

$$p^\circ(v_x) = \frac{1}{n}\sum_{t\in G} \rho(t)p\rho(t^{-1})(v_x) = \frac{1}{n}\sum_{t\in G}\rho(t)p(v_{t\cdot 1_x}) = \frac{1}{n}\rho(x)p(v_{x\cdot 1_x}) =$$

$$= \frac{1}{n}\rho(x)\sum_{t\in G} v_t = \frac{1}{n}\sum_{t\in G} v_{xt} = \frac{1}{n}\sum_{t\in G} v_t = \frac{1}{n}v.$$

Entonces

$$p^\circ \sum_{x\in G}\lambda_x v_x = \sum_{x\in G}\lambda_x \frac{1}{n}v .$$

Por lo tanto

$$W^\circ = \{\sum_{x\in G}\lambda_x v_x / \sum_{x\in G}\lambda_x = 0\}$$

es el complemento G-invariante de W que muestra el teorema.

Vamos a mantener las notaciones e hipótesis del teorema. Sea $v \in V$; $w \in W$, $w^\circ \in W^\circ$ con $v = w + w^\circ$. Entonces cualquiera que sea $x \in G$, se tiene

$$\rho(x)(v) = \rho(x)(w) + \rho(x)(w^\circ)$$

y puesto que W y W° son G estables $\rho(x)(w) \in W$, $\rho(x)(w^\circ) \in W^\circ$. Entonces las subrepresentaciones ρ^w y ρ^{w° determinan la representación ρ, ya que se tiene

$$\rho(x)(v) = \rho^w(x)(w) + \rho^{w^\circ}(x)(w^\circ) \quad (\text{para } v = w + w^\circ).$$

Definición 3.7.12. En las condiciones anteriores diremos que la representación ρ es una *suma directa* de las subrepresentaciones ρ^w y ρ^{w°. También escribiremos $V = W \oplus W^\circ$. Si R^w es una forma matricial de ρ^w y si R^{w° es una de ρ^{w°, entonces una forma matricial R de ρ se representa como sigue

$$R(x) = \begin{Vmatrix} R^w(x) & 0 \\ 0 & R^{w^\circ}(x) \end{Vmatrix}$$

para cada $x \in G$.

En forma análoga, se puede definir la suma directa de un número finito de representaciones.

Definición 3.7.13. Sea ρ una representación de G en un espacio V. Se dice que ρ es *irreducible* si, y sólo si, $V \neq 0$, y además, ningún subespacio propio de V es G-invariante. Por lo expuesto en el teorema anterior, esto equivale a decir que V no se puede descomponer en una suma directa de subrepresentaciones no triviales y también que el $\mathbf{C}(G)$-módulo V, es simple.

Toda representación de grado 1 es claramente irreducible. Todo grupo *no abeliano* posee, por lo menos, una representación irreducible de grado ≥ 2.

Ejemplo 1. Sea $\mathbf{D}_n$ el grupo diédrico de orden $2n$, y supongamos $\mathbf{D}_n = \langle a, b / a^n = b^2 = (ab)^2 = 1 \rangle$. Para cada raíz n-ésima de la unidad $w \in \mathbf{G}_n$ definimos $R_w : \mathbf{D}_n \to GL(2, \mathbf{C})$ en la forma

$$R_w(a^r) = \begin{Vmatrix} w^r & 0 \\ 0 & w^{-r} \end{Vmatrix} \qquad R_w(a^r b) = \begin{Vmatrix} 0 & w^{-r} \\ w^r & 0 \end{Vmatrix}$$

Es inmediato verificar que R_w es un morfismo. Sea, para cada $w \in \mathbf{G}_n$, ρ_w la representación inducida.

Nos preguntamos, ¿cúando una representación ρ_w es reducible? Para que ρ_w sea reducible debe existir un subespacio de dimensión 1 que sea $\mathbf{D}_n$-invariante. Sea $(x_1, x_2) \neq 0$, $W = \langle (x_1, x_2) \rangle$ un subespacio $\mathbf{D}_n$-invariante. En consecuencia, para cada $x \in \mathbf{D}_n$ debe existir $\lambda \in \mathbf{C}^*$, tal que

$$\rho_w(x)(x_1, x_2) = \lambda(x_1, x_2).$$

Como $\mathbf{D}_n$ está generado por a, b, bastará por considerar sólo los casos $x = a$ y $x = b$. Se obtiene

$$(wx_1, w^{-1}x_2) = \lambda(x_1, x_2)$$
$$(w^{-1}x_2, wx_1) = \lambda'(x_1, x_2)$$

lo cual se traduce en las condiciones

$$wx_1 = \lambda x_1 \quad \text{y} \quad w^{-1}x_2 = \lambda x_2$$
$$w^{-1}x_2 = \lambda' x_1 \quad \text{y} \quad wx_1 = \lambda' x_2$$

como $\lambda' \neq 0$, $w \neq 0$, se deduce de la segunda condición que o bien $x_1 = x_2 = 0$ o bien $x_1 \neq 0 \neq x_2$. Como hemos supuesto $(x_1, x_2) \neq 0$, lo primero no es posible, y por tanto, $x_1 \neq 0$, $x_2 \neq 0$. Luego, por la primera condición

$$w = \lambda = w^{-1}, \quad \text{es decir } w^2 = 1, \quad \text{esto es } w \in \mathbf{G}_2.$$

En consecuencia

$$\rho_w \text{ es reducible si, y sólo si, } w \in \mathbf{G}_2.$$

En efecto, si $w \in \mathbf{G}_2$, los subespacios complementarios

$$W_1 = \langle (1, 1) \rangle \qquad v_1 = (1, 1)$$

$$W_2 = \langle (1, -1) \rangle \qquad v_2 = (1, -1)$$

son $\mathbf{D}_n$-invariantes.

i) Sea $w = 1$; calculando R_1 en la base $[v_1, v_2]$ se obtiene

$$R_1(a) = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} \qquad R_1(b) = \begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix}$$

que da lugar a las subrepresentaciones de grado 1

$$T_1(a) = 1 \qquad T_2(a) = 1$$

$$T_1(b) = 1 \qquad T_2(b) = -1$$

ii) En el caso n par, es decir, $-1 \in \mathbf{G}_n$, tenemos para R_{-1} en la misma base

$$R_{-1}(a) = \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix} \qquad R_{-1}(b) = \begin{Vmatrix} -1 & 0 \\ 0 & 1 \end{Vmatrix}$$

que da lugar a las subrepresentaciones de grado 1

$$T_3(a) = -1 \qquad T_4(a) = -1$$

$$T_3(b) = -1 \qquad T_4(b) = 1$$

Entonces se satisface

i) $T_1 \oplus T_2 = R_1$ ii) $T_3 \odot T_4 = R_{-1}$.

iii) $T_t (1 \leq t \leq 4)$ son irreducibles (pues tienen grado 1) y no equivalentes entre sí (¡para que representaciones de grado 1 sean equivalentes entre sí deben coincidir!).

Ejemplo 2. Sea G un grupo abeliano finito. Por el teorema de estructura, G es una suma directa de cíclicos, o sea

$$G \simeq \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus \ldots \oplus \mathbf{Z}_{n_r}$$

(con n_{i+1}/n_i). Ahora bien, una representación de grado 1 de G, $\sigma : G \to \mathbf{C}^*$, queda completamente determinada por

$$\sigma(1, 0, \ldots, 0) \in \mathbf{G}_{n_1}$$

$$\sigma(0, 1, \ldots, 0) \in \mathbf{G}_{n_2}$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$\sigma(0, \ldots, 1) \in \mathbf{G}_{n_r}$$

y para cada elección $w_i \in \mathbf{G}_{n_i}$, se tiene una representación σ definida como sigue

$$\sigma(\lambda_1, \lambda_2, \ldots, \lambda_r) = \prod_{1 \leq i \leq r} w_i^{\lambda_i} = w_1^{\lambda_1} w_2^{\lambda_2} \ldots w_r^{\lambda_r}.$$

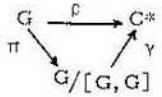
Las $|G|$ representaciones así obtenidas son distintas (luego no equivalentes), pues si

$$\sigma'(\lambda_1, \lambda_2, \ldots, \lambda_r) = \prod w_i'^{\lambda_i} \qquad (w_i' \in \mathbf{G}_{n_i})$$

entonces $\rho = \rho'$ si, y sólo si, $\rho(1,0,\ldots,0) = \rho'(1,0,\ldots,0)$, $\rho(0,1,\ldots,0) = \rho'(0,1,\ldots,0) \ldots \rho(0,0,\ldots,1) = \rho'(0,0,\ldots,1)$ si, y sólo si, $w_1 = w_1' w_2 = w_1' w_2^2 \ldots w_r = w_1' w_r^r$. En consecuencia: *Si G es un grupo abeliano finito, entonces G posee* $|G|$ *representaciones de grado 1 (no equivalentes).*

Ejemplo 3. Afirmamos que cualquiera que sea el grupo finito G, entonces G posee exactamente $|G/[G,G]|$ representaciones de grado 1. Nótese en principio que el grupo cociente $G/[G,G]$ es abeliano, en consecuencia, por lo visto anteriormente, el grupo cociente $G/[G,G]$ posee exactamente $|G/[G,G]|$ representaciones de grado 1. Todo lo que hay que mostrar es que hay una correspondencia biyectiva entre las representaciones de grado 1 de G y las de $G/[G,G]$.

Sea $\pi : G \to G/[G,G]$ la proyección al cociente. Si $\rho : G \to C^*$ es una representación de G, como C^* es abeliano, se tiene $\rho(xyx^{-1}y^{-1}) = \rho(x)\rho(y)\rho(x)^{-1}\rho(y)^{-1} = 1$, por tanto $[G,G] \subseteq \mathrm{Nu}\,\rho$, y por teoremas de isomorfismo se induce un morfismo $\gamma : G/[G,G] \to C^*$ tal que $\gamma \circ \pi = \rho$



Recíprocamente, dada una representación de grado 1, $\delta : G/[G,G] \to C^*$, la composición $\delta \circ \pi$ es una representación de G. La correspondencia es biyectiva, por lo tanto el resultado sigue.

Ejemplo 4. Si, por ejemplo, $n \geq 2$, se sabe que $[S_n, S_n] = A_n$, y por tanto, $S_n/[S_n, S_n] \simeq Z_2$; en efecto, hay sólo dos representaciones de grado 1; a saber

$$\rho_1 = \text{representación unitaria}$$

$$\rho_2(s) = \begin{cases} 1 \text{ si } s \text{ es permutación par} \\ -1 \text{ si } s \text{ es permutación impar.} \end{cases}$$

La importancia de las representaciones irreducibles se debe a que éstas sirven para obtener las demás representaciones por suma directa:

§ 3.8. TEOREMA DE MASCHKE

Teorema 3.8.10. (Maschke) Toda representación es suma directa de representaciones irreducibles.

Demostración. Sea V el espacio de una representación ρ del grupo G. Razonamos por inducción sobre $\dim V$.

Si $\dim V = 1$, el teorema es válido, pues ρ es irreducible. Supongamos entonces $\dim V \geq 2$. Si ρ es irreducible, nada hay que probar. En caso contrario, existe un subespacio propio y G-invariante W, y por el teorema 3.7.9 existe un complemento G-invariante W° de W. Entonces $V = W \oplus W^\circ$ y $\rho = \rho^W + \rho^{W^\circ}$, y puesto que $\dim W < \dim V$, $\dim W^\circ < \dim V$, el resultado sigue de la hipótesis inductiva aplicada a ρ^W y ρ^{W°. ▲

Esta condición se expresa diciendo que todo C(G)-módulo es una suma directa de C(G)-módulos simples, o también que el anillo C(G) es artiniano semisimple. En particular, tiene gran importancia la descomposición de la representación regular ya que ella suministra información sobre la descomposición del anillo C(G). Cabe preguntarse si la descomposición de una representación V como suma de irreducibles $V = V_1 \oplus V_2 \oplus \ldots \oplus V_r$ es única. La contestación es negativa; basta tomar la representación

$$\rho : G \to GL(n, C) \text{ dada por } \rho(x) = I$$

(para todo $x \in G$) y observar que cualquier subespacio es G invariante, y si tiene dimensión 1, es irreducible. Por lo tanto, todo subespacio de dimensión 1 puede formar parte de una descomposición en irreducibles.

Ejemplo. Consideremos la representación regular del grupo cíclico $\mathbf{Z}_n$ cuyos elementos designamos $0, 1, 2, \ldots, n-1$. Sea V un C-espacio vectorial de dimensión n con base $\{v_0, v_1, \ldots, v_{n-1}\}$. Entonces, si ρ es la representación regular, se tiene

$$\rho^{(1)}(v_j) = v_k, \text{ donde } k \equiv i + j \ (n) \quad (0 \leq k < n);$$

vamos a hallar los subespacios $\mathbf{Z}_n$-invariantes de dimensión 1 de V. Si $W = \langle w \rangle$ es el subespacio generado por un vector no nulo w, la condición necesaria y suficiente para que sea $\mathbf{Z}_n$-invariante es que $\rho(1)(w) = \lambda w$ para algún $\lambda \in C^*$. La condición es claramente necesaria, y en cuanto a ser suficiente, vemos que por ser ρ un homomorfismo, entonces $\rho(i)(w) = \lambda^i w$, y por lo tanto

$$\rho(i)(\mu w) = \mu \lambda^i w = \lambda^i(\mu w), \text{ es decir W es } \mathbf{Z}_n\text{-invariante.}$$

En la representación matricial de ρ en la base dada se tiene

$$R(1) = \begin{Vmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ . & . & \ldots & . & . \\ 0 & 0 & \ldots & 1 & 0 \end{Vmatrix}$$

y se debe verificar para cuáles valores $\lambda \in C^*$ existen vectores $w \in V$ con $R(1)w = \lambda w$, es decir $(\lambda I - R(1))(w) = 0 \ (w \neq 0)$. Los valores λ (vectores w) que verifican lo anterior se denominan *autovalores (autovectores)* de la matriz $R(1)$. Por lo tanto, $R(1) - \lambda I$ debe ser una matriz singular, esto es, de determinante nulo:

$$\text{Det}\left(\begin{Vmatrix} \lambda & 0 & \ldots & 0 & -1 \\ -1 & \lambda & \ldots & 0 & 0 \\ . & . & \ldots & . & . \\ 0 & 0 & \ldots & \lambda & 0 \\ 0 & 0 & \ldots & -1 & \lambda \end{Vmatrix} \right) = 0.$$

El lector puede comprobar inductivamente que la condición anterior es equivalente a

$$\lambda^n - 1 = 0$$

es decir, que λ es una raíz n-ésima de la unidad. Sea, entonces, $\lambda \in \mathbf{G}_n$ y sea $w = x_0 v_0 + x_1 v_1 + \ldots + x_{n-1} v_{n-1}$. La condición $(R(1) - \lambda I)w = 0$ es equivalente a

$$\begin{cases} \lambda x_0 = x_{n-1} \\ \lambda x_{i+1} = x_i \end{cases} \qquad (0 \leq i < n-1).$$

La primera condición se obtiene aplicando reiteradamente la segunda:

$$\lambda x_0 = \lambda^2 x_1 = \ldots = \lambda^{n-1} x_{n-2} = \lambda^n x_{n-1} = x_{n-1} \qquad (\lambda \in \mathbf{G}_n)$$

Por lo tanto, tomando, por ejemplo, $x_{n-1} = 1$, se tiene

$$x_{n-i} = \lambda x_{n-i+1} = \lambda^{i-1} \qquad (2 \leq i \leq n)$$

De este modo, el vector

$$w_\lambda = \sum_{0 \leq i < n} x_i v_i = \sum_{0 \leq i < n} \lambda^{n-1-i} v_i$$

satisface

$$\rho(1)(w_\lambda) = \lambda \cdot w_\lambda$$

y por lo ya visto, los subespacios $W_\lambda = \langle w_\lambda \rangle$ son $\mathbf{Z}_n$-invariantes. Sea,
78 para cada $\lambda \in \mathbf{G}_n$, ρ_λ la subrepresentación inducida por ρ en W_λ, es decir

$$\rho(i)(\mu w_\lambda) = \lambda^i (\mu w_\lambda)$$

Para comprobar que ρ es la suma directa de las subrepresentaciones ρ_λ basta con verificar que V es la suma directa de los subespacios W_λ, para lo cual será suficiente probar que $\{w_\lambda\}_{\lambda \in \mathbf{G}_n}$ es una base de V. Es un hecho conocido (y el lector puede comprobarlo fácilmente) que autovectores correspondientes a autovalores *distintos* son necesariamente linealmente independientes. El conjunto $\{w_\lambda\}_{\lambda \in \mathbf{G}_n}$ está en estas condiciones, y por razones de dimensión debe ser una base. En consecuencia, $\rho = \bigoplus_{\lambda \in \mathbf{G}_n} \rho_\lambda$.

Ejemplo. Sea la representación $R : \mathbf{S}_3 \to GL(3, C)$ que sobre los generadores (12) y (132) de $\mathbf{S}_3$ se comporta en la forma

$$R(12) = \begin{Vmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{Vmatrix} \qquad R(132) = \begin{Vmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{Vmatrix}$$

Si R es reducible, entonces será la suma directa de subrepresentaciones R_1 y R_2 con grado $R_1 = 1$, grado $R_2 = 2$. Para hallar R_1 hay que encontrar un subespacio W_1 de dimensión 1, $\mathbf{S}_3$-invariante. La condición para que $W_1 = \langle v_1 \rangle$ sea $\mathbf{S}_3$-invariante es ahora que v_1 sea autovector *de las dos matrices* R(12) y R(132). Comencemos, como en el ejemplo anterior, por hallar los autovalores de las matrices en cuestión.

$$\mathrm{Det}(XI - R(12)) = \mathrm{Det} \begin{Vmatrix} x & -1 & 0 \\ -1 & x & 0 \\ 0 & 0 & x-1 \end{Vmatrix} = (x-1)^2(x+1)$$

y los autovalores asociados son

$$\lambda_1 = \lambda_2 = 1 \qquad \lambda_3 = -1$$

$$\mathrm{Det}(x\mathrm{I}-\mathrm{R}(132)) = \mathrm{Det}\begin{vmatrix} x & -1 & 0 \\ 0 & x & -1 \\ -1 & 0 & x \end{vmatrix} = x^3-1$$

y sus autovalores las raíces cúbicas de la unidad

$$\mu_1 = 1 \qquad \mu_2 = w \qquad \mu_3 = w^2.$$

Los subespacios asociados son

$$\lambda_1 = \lambda_2 = 1 : \{(x, y, z)/x = y\}$$
$$\lambda_3 = -1 : \{(x, y, z)/x = -y, z = 0\}$$
$$\mu_1 = 1 : \{(x, y, z)/x = y = z\}$$
$$\mu_2 = w : \{(x, y, z)/y = wx\ z = w^2x\}$$
$$\mu_3 = w^2 : \{(x, y, z)/y = w^2x\ z = wx\}$$

Entonces, tomando $v_1 = (1, 1, 1)$, se tiene

$\mathrm{R}(12)(1, 1, 1) = \mathrm{R}(132)(1, 1, 1) = (1, 1, 1) \therefore W_1 = \langle v_1 \rangle$ es $\mathbf{S}_3$-invariante.

Además, si $v_2 = (1, w, w^2)$, $v_3 = (1, w^2, w)$, resulta

$$\mathrm{R}(12)(v_2) = wv_3 \qquad \mathrm{R}(12)(v_3) = w^2v_2$$

y es claro que

$$\mathrm{R}(132)(v_2) = wv_2 \qquad \mathrm{R}(132)(v_3) = w^2v_3.$$

En consecuencia

$$W_2 = \langle v_2, v_3 \rangle \text{ es } \mathbf{S}_3\text{-invariante.}$$

Luego, la representación R es la suma directa de las subrepresentaciones R_1 y R_2, donde: R_1 = representación unitaria, y

$$\mathrm{R}_2(12) = \begin{Vmatrix} 0 & w^2 \\ w & 0 \end{Vmatrix} \qquad \mathrm{R}_2(132) = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}.$$

Ahora bien, R_2 es irreducible puesto que los subespacios $R_2(132)$-invariantes son $\langle v_2 \rangle$ y $\langle v_3 \rangle$, los cuales no son $R_2(12)$-invariantes. La descomposición de R en suma directa de irreducibles es pues $R = R_1 \oplus R_2$.

§ 3.9. CARACTERES

El estudio de grupos y sus representaciones se facilita enormemente con la introducción de funciones numéricas en el grupo. De estas funciones, llamadas caracteres, nos hemos limitado a señalar algunos hechos básicos, recomendando al lector interesado la consulta de la bibliografía citada al final.

Si a es una matriz, $a = (a_{ij}) \in K^{n\times n}$, se llama *traza* de la matriz al escalar

$$\mathrm{Tr}(a) = \sum_{1\le i\le n} a_{ii}.$$

Es fácil verificar la propiedad siguiente

$$\mathrm{Tr}(ab) = \mathrm{Tr}(ba) \qquad (a, b \in K^{n\times n})$$

y, su consecuencia

$$\mathrm{Tr}(bab^{-1}) = \mathrm{Tr}(a) \qquad (a, b \in K^{n\times n},\ b \text{ inversible}).$$

Sea $\rho : G \to \mathrm{Aut}(V)$ una representación de un grupo finito G, y llamemos *carácter de* ρ a la función χ definida en G que toma valores en C

$$\chi(x) = \mathrm{Tr}(R(x))$$

donde R denota una expresión matricial de la representación ρ. Adviértase que por las propiedades de la traza antes mencionadas el carácter χ_ρ no depende de la representación matricial R de ρ considerada. Por esta misma razón, las representaciones equivalentes tienen el mismo carácter. Es claro que

$$\chi_\rho(1) = \mathrm{Tr}(R(1)) = \mathrm{Tr}(I) = \text{grado } \rho, \text{ y también que}$$

$$\chi_\rho(yxy^{-1}) = \mathrm{Tr}(R(yxy^{-1})) = \mathrm{Tr}(R(y)R(x)R(y)^{-1}) = \mathrm{Tr}(R(x)) = \chi_\rho(x)$$

o sea, todo carácter es constante sobre cada clase de conjugación de G. En virtud de que $\chi_\rho(x)$ es la suma de las raíces características de $R(x)$ (las cuales son raíces de la unidad, pues $R(x)$ tiene orden finito) es posible verificar que

$$\chi_\rho(x^{-1}) = \overline{\chi_\rho(x)} \qquad (\text{cf } [12]).$$

Si $\rho_t : G \to \mathrm{Aut}(V_t)$ $(t = 1, 2)$ son dos representaciones, $R_t(x)$ son formas matriciales y χ_t los caracteres, entonces una forma matricial de $\rho_1 \oplus \rho_2$ es

$$R(x) = \begin{Vmatrix} R_1(x) & 0 \\ 0 & R_2(x) \end{Vmatrix}$$

y su carácter χ satisface

$$\chi(x) = \mathrm{Tr}(R(x)) = \mathrm{Tr}(R_1(x)) + \mathrm{Tr}(R_2(x)) = \chi_1(x) + \chi_2(x)$$

o sea $\chi = \chi_1 + \chi_2$.

Ejemplo 1. Si ρ es la representación unitaria de un grupo finito G, entonces se tiene

$$\chi(x) = 1 \qquad (\forall\, x \in G).$$

Ejemplo 2. Si ρ es la representación regular de un grupo G de orden n, χ su carácter, y si el espacio vectorial asociado V tiene base $[v_t]_{t\in G}$, resulta por definición de ρ

$$\rho(x)(v_t) = v_{xt}.$$

Entonces, $\rho(x)(v_t) = v_t$ si, y sólo si, $xt = t$ si, y sólo si, $x = 1$. Si R es la forma matricial de ρ, entonces la diagonal de $R(x)$ consiste de ceros si $x \neq 1$, y en 1 si $x = 1$, y en consecuencia

$$\chi(x) = \begin{cases} n \text{ si } x = 1 \\ 0 \text{ si } x \neq 1. \end{cases}$$

Ejemplo 3. En particular, si $G = \mathbf{Z}_n$, habíamos visto ya que la representación regular ρ era la suma directa de las representaciones de grado 1, $\rho_\lambda (\lambda \in \mathbf{G}_n)$ definidas por

$$\rho_\lambda(t)(w_\lambda) = \lambda^t w_\lambda .$$

Es decir, si χ_λ representa el carácter de ρ_λ, se obtiene

$$\chi_\lambda(t) = \lambda^t .$$

En consecuencia

$$\chi_\rho(t) = \sum_{\lambda \in \mathbf{G}_n} \chi_\lambda(t) = \sum_{\lambda \in \mathbf{G}_n} \lambda^t .$$

Si comparamos con lo obtenido en el ejemplo anterior, resulta

$$\sum_{\lambda \in \mathbf{G}_n} \lambda^t = 0 \quad (\text{para } 0 < t < n).$$

Si Φ, $\Psi : G \to \mathbf{C}$ son dos funciones, se define

$$\langle \Phi, \Psi \rangle = \frac{1}{n} \sum_{t \in G} \overline{\Phi(t)} \Psi(t) \qquad (n = |G|).$$

Es muy fácil verificar que $\langle , \rangle$ es un producto interno, es decir: es semilineal en la primera variable, lineal en la segunda y además $\langle \Phi, \Phi \rangle > 0$ para $\Phi \neq 0$.

Una propiedad muy importante, que enunciamos sin demostración, es la siguiente: Sean $\rho_i (i = 1, 2)$ dos representaciones irreducibles de un grupo finito G, con caracteres χ_i. Entonces

i) Si ρ_1 y ρ_2 son equivalentes, $\langle \chi_1, \chi_2 \rangle = 1$.

ii) Si ρ_1 y ρ_2 no son equivalentes $\langle \chi_1, \chi_2 \rangle = 0$.

Esto nos dice que los caracteres correspondientes a representaciones irreducibles son ortogonales. En particular, i) da la condición necesaria para que una representación ρ sea irreducible: $\langle \chi_0, \chi_\rho \rangle = 1$. Más adelante, veremos que es suficiente.

Ejemplo. Sea $G \neq 1$ es un grupo finito, $n = |G|$. Si ρ es la representación regular, y χ_ρ su carácter, de acuerdo con lo ya visto

$$\langle \chi_\rho, \chi_\rho \rangle = \frac{1}{n} \sum_{t \in G} \chi_\rho(t) \chi_0(t) = \frac{1}{n} \chi_\rho(1) \cdot \chi_\rho(1) = n \neq 1.$$

Por tanto, la representación regular nunca es irreducible ($G \neq 1$), lo que confirma un resultado ya conocido.

Dada una representación $V = \sum_{1 \leq i \leq k} W_i$, donde los W_i son irreducibles. Si Φ es el carácter de V y Φ_i el de W_i, cualquiera que sea la representación irreducible W con carácter χ, se tiene: El número de W_i isomorfos a W es igual a $\langle \Phi, \chi \rangle$. En efecto, se sabe que $\Phi = \sum_{1 \leq i \leq k} \Phi_i$, luego $\langle \Phi, \chi \rangle = \langle \sum \Phi_i, \chi \rangle = \sum \langle \Phi_i, \chi \rangle$. Pero, de acuerdo con lo anterior, el pro-

ducto interno $\langle \psi_i, \chi \rangle$ es igual a 1 (respectivamente 0) si, y sólo si, W_i es isomorfo (respectivamente no isomorfo) a W.

De aquí se deducen algunas consecuencias interesantes:

1. El número de W_i isomorfo a W no depende de la descomposición de V en suma directa de irreducibles. En efecto, $\langle \psi, \chi \rangle$ no depende.

2. Dos representaciones son isomorfas si, y sólo si, tienen el mismo carácter. En efecto, si dichas representaciones tienen el mismo carácter, ambas contendrán el mismo número de veces cada representación irreducible.

Ejemplo. Sobre el grupo diédrico $\mathbf{D}_n = \langle a, b / a^n = b^2 = (ab)^2 = 1 \rangle$ se habían definido representaciones dadas por:

$$R_w(a^r) = \begin{Vmatrix} w^r & 0 \\ 0 & w^{-r} \end{Vmatrix} \qquad R_w(a^r b) = \begin{Vmatrix} 0 & w^{-r} \\ w^r & 0 \end{Vmatrix}$$

donde $w \in \mathbf{G}_n$.

El carácter χ_w asociado a R_w es

$$\begin{cases} \chi_w(a^r) = w^r + w^{-r} = 2 \text{ Real } (w^r) \\ \chi_w(a^r b) = 0. \end{cases}$$

¿Cuándo será R_w equivalente a $R_{w'}$ respecto a dos raíces w y w' en $\mathbf{G}_n$?
La condición necesaria y suficiente para que esto ocurra es que $\chi_w = \chi_{w'}$,
82 o sea $2\,\text{Real}(w^r) = 2\,\text{Real}(w'^r)$ $(0 \le r < n)$. En particular

$$\text{Real}\, w = \text{Real}\, w'$$

en consecuencia (siendo $w, w' \in \mathbf{G}_n$) es necesario que $w = \overline{w'}$. También la condición es suficiente y en consecuencia las representaciones R_w son no isomorfas cuando $w \in \mathbf{G}_n$ tienen como argumento:

$$\frac{2k\pi}{n};\ 0 \le k \le n/2 \ \text{(si } n \text{ es par)} \qquad \frac{2k\pi}{n};\ 0 \le k \le n - 1/2 \ \text{(si } n \text{ es impar).}$$

Una función $f : G \to C$ se dice *central* si $f(yxy^{-1}) = f(x)$ cualesquiera que sean $x, y \in G$. En otras palabras, f es constante sobre cada clase de conjugación de G. Son ejemplos de funciones centrales los caracteres de G.

Sean $C_1 \ldots C_k$ la totalidad de clases conjugadas de G. Si H designa el conjunto de funciones centrales, es claro que H es un espacio vectorial sobre C de dimensión k.

Si $\chi_1, \chi_2, \ldots, \chi_r$ son caracteres correspondientes a representaciones irreducibles no isomorfas, entonces $\{\chi_i\}_{1 \le i \le r}$ es un conjunto linealmente independiente en H; pues, si $0 = \sum \alpha_i \chi_i$, por las relaciones de ortogonalidad se tiene $0 = \langle \chi_j, 0 \rangle = \langle \chi_j, \sum \alpha_i \chi_i \rangle = \sum \alpha_i \langle \chi_j, \chi_i \rangle = \alpha_j$. En consecuencia, $r \le k$. Aun puede probarse más, si $\chi_1, \ldots, \chi_r$ son *todos* los caracteres de representaciones irreducibles no isomorfas, entonces $r = k$; es decir, $\chi_1 \ldots \chi_r$ es base de H.

Sean, en lo que sigue, $\chi_1 \ldots \chi_k$ los distintos caracteres de representaciones irreducibles $V_1 \ldots V_k$ de G. Si V es una representación cualquiera de G, entonces existirán enteros no negativos m_i tales que

$$V = m_1V_1 \oplus m_2V_2 \oplus \dots \oplus m_kV_k$$

y el carácter ξ de V estará dado por

$$\xi = \sum_{1 \le i \le k} m_i\chi_i$$

donde $m_i = \langle \chi_i, \Phi \rangle$. Por las relaciones de ortogonalidad se deduce que

$$\langle \xi, \xi \rangle = \sum_{1 \le i \le k} m_i^2$$

En consecuencia

i. Si Φ es el carácter de una representación V, entonces $\langle \xi, \xi \rangle$ es entero, no negativo.

ii. $\langle \Phi, \Phi \rangle = 1$ si, y sólo si, V es irreducible.

En efecto, $\langle \Phi, \Phi \rangle = 1$ si, y sólo si, algún $m_i = 1$, y los demás son nulos si, y sólo si, $V = V_i$.

Descomposición de la Representación Regular

Sea n_i = grado de $\chi_i (n_i = \chi_i(1))$, $n = |G|$. Si R es la representación regular de G y χ su carácter, sabemos que

$$\chi(x) = 0 \text{ si } x \neq 1 \qquad \chi(1) = n.$$

Entonces

$$\langle \chi, \chi_i \rangle = \frac{1}{n} \sum_{t \in G} \overline{\chi(t)}\chi_i(t) = \frac{1}{n} n\chi_i(1) = \chi_i(1) = n_i.$$

Por tanto, $\chi = \sum_{1 \le i \le k} n_i\chi_i$, o sea cada representación irreducible es sumando directo de la representación regular un número de veces igual a su grado. Calculando $\chi = \sum_{1 \le i \le k} n_i\chi_i$ en $1 \in G$, se obtiene

$$n = \sum_{1 \le i \le k} n_i^2 \qquad (*)$$

lo cual da un criterio en la búsqueda de los caracteres irreducibles de un grupo G. Además, se deduce también de (*) que un grupo G es abeliano si, y sólo si, posee $|G|$ clases conjugadas si, y sólo si, $k = |G|$ si, y sólo si, $n_i = 1 \ (\forall\, i)$ si, y sólo si, todos sus caracteres irreducibles son de grado 1.

Ejemplo 1. Grupo cíclico $\mathbf{Z}_n$: Se tenía n representaciones irreducibles de grado 1, $\{\rho_\lambda\}_{\lambda \in G_n}$, con caracteres $\{\chi_\lambda\}_{\lambda \in G_n}$ dados por

$$\chi_\lambda(t) = \lambda^t.$$

La fórmula (*) se verifica en este caso, y por lo tanto los $\chi_\lambda (\lambda \in G_n)$ son *todos* los caracteres irreducibles de $\mathbf{Z}_n$.

Ejemplo 2. Grupo abeliano finito. Análogamente al caso anterior, las representaciones definidas en pág. 75 son todas irreducibles de grado 1, y como también se verifica (*), son *todas* las representaciones irreducibles.

Ejemplo 3. Grupo diédrico $\mathbf{D}_n$: Con las notaciones de la pág. 74 y la pág. 82.

i) Si n es par: Tenemos cuatro representaciones irreducibles de grado 1 no isomorfas: T_1, T_2, T_3 y T_4. También hay $(n/2) - 1$ representaciones irreducibles de grado 2 no isomorfas entre sí: R_w para w con argumento $\frac{2k\pi}{n}(1 \leq k \leq (n/2) - 1)$. Se tiene entonces

$$4 + (n/2) - 1)2^2 = n/2 \cdot 4 = 2n = |\mathbf{D}_n|$$

y también se verifica (*); las anteriores son todas las representaciones irreducibles de $\mathbf{D}_n$.

ii) n impar: Hay dos representaciones irreducibles de grado 1 no isomorfas: T_1 y T_2. Tenemos $n - 1/2$ representaciones irreducibles de grado 2 no isomorfas entre sí: R_w con argumento $w = \frac{2k\pi}{n}(1 \leq k < \frac{n-1}{2})$. Luego

$$2 + n - 1/2 \cdot 4 = 2 + 2(n - 1) = 2n = |\mathbf{D}_n|$$

como antes, las propuestas son todas las representaciones irreducibles de $\mathbf{D}_n$.

Ejemplo 4. Consideremos el grupo alternado $\mathbf{A}_4$. Las clases conjugadas de $\mathbf{A}_4$ son:

$$C_1 = \{1\}, \quad C_2 = \{(12)(34), (13)(24), (14)(23)\}$$
$$C_3 = \{(123), (214), (341), (432)\} \quad C_4 = \{(132), (241), (314), (423)\}$$

Sabemos que $\mathbf{A}_4/[\mathbf{A}_4, \mathbf{A}_4] \simeq Z_3$. Luego, tenemos tres caracteres irreducibles de grado 1, que son

$$\chi_1 = \text{carácter unitario.}$$

$$\chi_2(x) = \begin{cases} 1 & (x \in C_1 \cup C_2) \\ w & (x \in C_3) \\ w^2 & (x \in C_4) \end{cases} \qquad \chi_3(x) = \begin{cases} 1 & (x \in C_1 \cup C_2) \\ w^2 & (x \in C_3) \\ w & (x \in C_4) \end{cases}$$

Donde $w \neq 1$ es la raíz cúbica de la unidad.

Sabiendo que $\mathbf{A}_4$ posee cuatro clases conjugadas, debe tener cuatro caracteres irreducibles, tres de ellos son los ya mostrados. Aplicando la fórmula (*), se obtiene $12 = 1 + 1 + 1 + n_4^2$. Luego, el carácter que falta χ_4 tiene grado 3. En consecuencia, $\chi_4(1) = 3$. Sólo queda por hallar $\chi_4(x)$ cuando $x \in C_i (i = 2, 3, 4)$ para tener completamente determinado χ_4. Utilizamos las relaciones de ortogonalidad

$$(\chi_i, \chi_4) = 0 \qquad (i = 1, 2, 3)$$

Sean $\chi_4(x) = \alpha$ (si $x \in C_2$); $\chi_4(x) = \beta$ (si $x \in C_3$); $\chi_4(x) = \gamma$ (si $x \in C_4$)

$$0 = (\chi_1, \chi_4) = \frac{1}{12}(1 \cdot 3 + 3 \cdot 1 \cdot \alpha + 4 \cdot 1 \cdot \beta + 4 \cdot 1 \cdot \gamma) = \frac{1}{12}(3 + 3\alpha + 4\beta + 4\gamma)$$

$$0 = \langle \chi_2, \chi_4 \rangle = \frac{1}{12}(3 + 3\alpha + 4w^2\beta + 4w\gamma)$$

$$0 = \langle \chi_3, \chi_4 \rangle = \frac{1}{12}(3 + 3\alpha + 4w\beta + 4w^2\gamma).$$

Resolviendo este sistema de ecuaciones en α, β y γ se obtiene inmediatamente $\alpha = -1$, $\beta = \gamma = 0$. Es decir

$$\chi_4(1) = 3$$

$$\chi_4(x) = -1 \quad \text{si } x \in C_2$$

$$\chi_4(x) = 0 \quad \text{si } x \in C_3 \cup C_4 .$$

A partir de la teoría de caracteres es posible obtener resultados importantes acerca de la estructura del grupo. A modo de ejemplo, citamos el célebre teorema de Burnside: Sean p y q números primos,

Si $|G| = p^r q^s$ con $r + s > 1$, entonces G no es simple.

La demostración de este resultado requiere un desarrollo mucho más elaborado que escapa los límites de esta monografía.

4

TEOREMAS DE SYLOW

Sabemos ya que si G es un grupo de orden n, el orden de cada subgrupo H de G divide al entero n. También se ha visto con ejemplos que la recíproca no es necesariamente válida (si m/n puede no haber subgrupos de orden m en G): $\mathbf{A}_4$ no posee subgrupos de orden 3.

En este capítulo probaremos que si m/n, y si m es potencia de un primo ($m = p^r$), entonces todo grupo de orden n posee subgrupos de orden m. Además, fijaremos las condiciones respecto al número de tales subgrupos. En particular, verificaremos la existencia de p-subgrupos de orden máximo y demostraremos que todos ellos son conjugados. Estos resultados se conocen como teoremas de Sylow y se cuentan entre los más importantes de la teoría de grupos finitos.

§ 4.1. TEOREMAS DE SYLOW

Lema. Sea A un conjunto de $p^r m$ elementos, p primo. Sea X la familia de los subconjuntos de A que poseen exactamente p^r elementos. Entonces

$$|X| = m\,(p^r m).$$

Demostración. Es claro que

$$|X| = \binom{p^r m}{p^r} = m\binom{p^r m - 1}{p^r - 1} =$$

$$= m\,\frac{(p^r m - (p^r - 1))(p^r m - (p^r m - 2)) \ldots (p^r m - 1)}{(p^r - 1)(p^r - 2) \ldots 1} = m \prod_{1 \le t \le p^r - 1} \left(\frac{p^r m}{t} - 1\right) \qquad (*)$$

como $p^r \nmid t$ para $1 \le t \le p^r - 1$, entonces cabe escribir

$$\frac{p^r m}{t} = \frac{p m_1}{s_1} \text{ donde } m_1 \text{ y } s_1 \text{ son enteros coprimos y } p \nmid s_1.$$

Luego

$$\binom{p^r m - 1}{p^r - 1} = \prod_{1 \le t \le p^r - 1} \left(\frac{p m_1}{s_1} - 1\right) = (-1)^{p^r - 1} + p\frac{n}{s} \qquad (**)$$

donde n y s son enteros coprimos y $p \nmid s$. Como el coeficiente binomial de (**) es siempre un número entero, $s = 1$; y así

$$|X| = m\binom{p^r m - 1}{p^r - 1} = m(-1)^{p^r - 1} + prm. \qquad (***)$$

Ahora, si p es impar, $p^r - 1$ es par, por lo tanto $m(-1)^{p^r - 1} = m$, y el resultado sigue de (***).

Si $p = 2$, $p^r - 1$ es impar, por lo tanto $m(-1)^{p^r - 1} = -m \equiv m \pmod{2m}$ y el resultado propuesto es válido también. ▲

Teorema 4.1.11. (Sylow) Sea G un grupo de $p^r m$ elementos, p primo. Sea n_r el número de subgrupos de G de orden p^r. Entonces $n_r \equiv 1(p)$. En particular $n_r \geq 1$.

Demostración. Sea, en el lema anterior, $\Lambda = G$ y X = la familia de subconjuntos de G de p^r elementos. G opera sobre X por traslación a la izquierda, es decir

Si $A \in X$, $A = \{a_1, a_2 \ldots a_{p^r}\} \subseteq G$, $g \in G$, entonces

$$g \cdot A = \{ga_1, ga_2 \ldots ga_{p^r}\} \in X.$$

Se afirma que si $A \in X$, $a \in A$, entonces la coclase $G_A \cdot a$ está contenida en A. En efecto, $ga \in gA = A$ para $g \in G_A$. Luego, $G_A a \subseteq A$.

De esto se deduce que $A \in X$ es un conjunto de p^r elementos que satisface: Existen $a_1, \ldots, a_s \in A$ con

$$A = \bigcup_{1 \leq i \leq s} G_A a_i \qquad \text{(unión disjunta).}$$

Como todas las coclases a la derecha, $G_A a_i$ tienen el mismo número de elementos: $|G_A|$; se concluye que $|G_A| / |A|$, o sea $|G_A| / p^r$. Se deduce que la órbita O_A tiene cardinal $p^s m$ para algún $s \geq 0$. Además, $s = 0$ si, y sólo si, $|G_A| = p^r$ si, y sólo si, A es una coclase, digamos $A = G_A a$ de G_A en G. Recíprocamente, si $A \in X$ es una coclase a la derecha de algún subgrupo H de G, digamos $A = Ha$, entonces $H = G_A$, pues

$$g \cdot Ha = Ha \text{ si, y sólo si, } g \in H.$$

En el supuesto de que sea n_r el número de subgrupos de orden p^r en G, hay mn_r coclases a la derecha de subgrupos de orden p^r en G, y todos estos son elementos de X. Para aquellos $A' \in X$ que no son coclase a la derecha de ningún subgrupo de orden p^r en G, se tiene

$$|G : G_{A'}| = |O_{A'}| \equiv 0(pm)$$

y así, el número de elementos $A \in X$ que no son coclase a la derecha de algún subgrupo de orden p^r en G es congruente a 0 módulo (pm). Se sigue que

$$|X| \equiv mn_r(pm).$$

Por el lema anterior, se tiene

$$m \equiv mn_r(pm), \text{ es decir } n_r \equiv 1(p). \qquad \blacktriangle$$

Ejemplo 1. Consideremos el grupo simétrico S_3, cuyo orden es $3! = 2 \cdot 3$. Si consideramos $p = 2$, se tiene que cada uno de los elementos

$$(12);\ (13);\ (23)$$

generan un subgrupo de orden 2 en S_3. En este caso $(r = 1)$, se tiene $n_1 = 3 \equiv 1(2)$. Para $p = 3$, el elemento (123) genera el único subgrupo de orden 3 de S_3: $\{1, (123), (132)\}$. En consecuencia, $(r = 1)$, resulta $n_r = 1$ y también $n_r = 1 \equiv 1(3)$. Como un caso particular del teorema se tiene

Corolario. Sea G un grupo finito de orden $p^r m$ con p primo, $(p, m) = 1$. Entonces G posee subgrupos de orden p^r, y el número de tales subgrupos es congruente a 1 módulo p.

Definición 4.1.14. Sea G un grupo finito de orden $p^r m$ con p primo, $(p, m) = 1$. Se denomina *p-subgrupo de Sylow de* G a todo subgrupo de G de orden p^r. La existencia de tales subgrupos está asegurada por el corolario anterior.

Teorema 4.1.12. (Sylow) Sea G un grupo finito y P un p-subgrupo de Sylow de G. Si H es un p-subgrupo de G, entonces H es conjugado a algún subgrupo de P.

Demostración. Como sabemos que G es unión disjunta de coclases dobles $PxH (x \in G)$, existirán $x_1, \ldots, x_t \in G$ con

$$G = \bigcup_{1 \le i \le t} Px_iH.$$

Luego, por ser dicha unión disjunta

$$|G| = \sum_{1 \le i \le t} |Px_iH|.$$

Sea $|P| = p^r (r \ge 0)$, por lo tanto $p^{r+1} \nmid |G|$, y así p^{r+1} no divide al cardinal de alguna coclase doble, digamos $p^{r+1} \nmid |Px_iH|$. Ahora, recordando que

$$|Px_1H| = |P| \cdot |H : H \cap x_1Px_1^{-1}|,$$

se tiene $p \nmid |H : H \cap x_1Px_1^{-1}|$, y siendo H un p-grupo se deduce que $|H : H \cap x_1Px_1^{-1}| = 1$, esto es $H = H \cap x_1Px_1^{-1}$, o sea $H \subseteq x_1Px_1^{-1}$, lo cual equivale a decir $x_1^{-1}Hx_1 \subseteq P$, esto es, H es conjugado al subgrupo de $P: x_1^{-1}Hx_1$ ▲

Obsérvese que lo demostrado en el teorema no implica que dados dos p-subgrupos H_1 y H_2 del mismo orden éstos sean necesariamente conjugados. Por ejemplo, en S_4 los elementos (12) y (12)(34) tienen orden 2, luego $H = \langle (12) \rangle$ y $K = \langle (12)(34) \rangle$ son 2-subgrupos isomorfos de S_4. Sin embargo, H y K no son conjugados pues los elementos que los generan no tienen la misma estructura cíclica. En el caso de p-subgrupos de Sylow se tiene:

Corolario 1. Todos los p-subgrupos de Sylow de un grupo finito G son conjugados. Todo p-subgrupo de G está contenido en un p-subgrupo de Sylow de G. Si G posee un único p-subgrupo de Sylow para algún p primo, éste es invariante.

Ejemplo. Consideremos el grupo simétrico S_4 y calculemos los p-subgrupos de Sylow de S_4. Las clases conjugadas de S_4 son las siguientes

$$C_1 = \{1\}; \ |C_1| = 1 \qquad C_2 = \{(..)\}; \ |C_2| = 6$$
$$C_3 = \{(...)\}; \ |C_3| = 8 \qquad C_4 = \{(....)\}; \ |C_4| = 6$$
$$C_5 = \{(..)(..)\}; \ |C_5| = 3.$$

Como $|S_4| = 24 = 2^3 \cdot 3$, se consideran los 3-subgrupos de Sylow (estos son cíclicos de orden 3) y los 2-subgrupos de Sylow (los cuales tienen orden $2^3 = 8$). Los 3-subgrupos de Sylow no presentan dificultad, pues como cada uno de ellos es cíclico, estará generado por un elemento de la clase C_3, y entonces su cuadrado también tendrá orden 3 (luego

pertenece a C_3). En consecuencia, cada 3-subgrupo de Sylow consiste en dos elementos de la clase C_3 y la identidad. Hay por tanto exactamente $8/2 = 4$, 3-subgrupos de Sylow, y estos son

$$H_1 = \langle (123) \rangle, \quad H_2 = \langle (124) \rangle, \quad H_3 = \langle (134) \rangle, \quad H_4 = \langle (234) \rangle.$$

Consideremos ahora los 2-subgrupos de Sylow. En principio nótese que el subgrupo

$$K = \{1, (12)(34), (13)(24), (14)(23)\}$$

es invariante. En efecto, esta condición es consecuencia de que los elementos de K son los únicos que poseen esa estructura cíclica (o equivalentemente, K es unión de clases conjugadas: $K = C_1 \cup C_5$). Como K es 2-grupo, está contenido en algún 2-subgrupo de Sylow de S_4; y como todos los 2-subgrupos de Sylow son conjugados y K es invariante, entonces K está contenido *en todo* 2-subgrupo de Sylow de S_4.

Para cada $x \in C_4$, el subgrupo $\langle x \rangle$ tiene orden 4, luego está contenido en algún 2-subgrupo de Sylow: P_x. Como $x \notin K$, entonces por razones de orden

$$P_x = \langle x, K \rangle$$

y como los 2-subgrupos de Sylow son conjugados, por razones de estructura cíclica: todos los 2-subgrupos de Sylow de S_4 son del tipo anterior. Pero, adviértase que $\langle x \rangle = \langle x^3 \rangle$, para $x \in C_4$, luego

$$P_x = P_{x^3}.$$

Por tener la clase C_4 exactamente 6 elementos, deducimos que S_4 posee *a lo sumo* $6/2 = 3$, 2-subgrupos de Sylow, y estos son

$$P_1 = \langle (1234), K \rangle \quad P_2 = \langle (1243), K \rangle \quad P_3 = \langle (1423), K \rangle.$$

Es inmediato verificar que dichos subgrupos son distintos y que $P_i = D_4$ $(1 \leq i \leq 3)$.

Corolario 2. Sea G un grupo finito de orden $p^r m$, p-primo, $(p, m) = 1$. Sea n_p = número de p-subgrupos de Sylow de G. Sea H_p un tal p-subgrupo de Sylow. Entonces $n_p = |G : N(H_p, G)|$.

Demostración. En efecto, n_p = número de subgrupos conjugados de $H_p = |G : N(H_p G)|$, como ya se demostró en el capítulo 2. ▲

Corolario 3. Sea G un grupo de orden $p^r m$, p primo, $(p, m) = 1$. Sea n_p = número de p-subgrupos de Sylow de G. Entonces: i) $n_p \equiv 1 (p)$ y ii) n_p / m.

Demostración. En efecto, i) es consecuencia del teorema 4.1.11 y ii) resulta de ser

$$n_p = |G : N(H_p, G)| \, | \, |G : H_p| = m$$

cualquiera que sea el p-subgrupo de Sylow H_p. ▲

§ 4.2. EJEMPLOS

Ejemplo 1. Sea A un grupo abeliano finito de orden $p^r m$, p primo, $(p, m) = 1$. Se afirma que A posee un único p-subgrupo de Sylow: A_p = componente p-primaria de A. En efecto, A_p es un p-subgrupo de Sylow, pues es un subgrupo de A de orden p^r. Además, es el único, pues

los otros p-subgrupos de Sylow son conjugados en A_p, pero como A es abeliano, coinciden con A_p.

Ejemplo 2. Cálculo de los p-subgrupos de Sylow del grupo multiplicativo

$$G = \left\{ \begin{Vmatrix} a & 0 \\ 0 & b \end{Vmatrix}, \begin{Vmatrix} 0 & a \\ b & 0 \end{Vmatrix};\ a, b \in G_3 \right\}$$

por cierto que el orden de G es $18 = 3^2 \cdot 2$.

Un 3-subgrupo de Sylow tendrá orden 9, y por tanto índice 2, luego será invariante en G. Es así que G posee un único 3-subgrupo de Sylow. En efecto, el subgrupo

$$H_3 = \left\{ \begin{Vmatrix} a & 0 \\ 0 & b \end{Vmatrix};\ a, b \in G_3 \right\}$$

tiene las propiedades requeridas.

Un 2-subgrupo de Sylow debe tener orden 2; esto es, será cíclico, generado por un elemento de orden 2. Calculemos los elementos de orden 2 en el grupo G. Ningún elemento de la forma $\begin{Vmatrix} a & 0 \\ 0 & b \end{Vmatrix}$ puede tener orden 2, pues dichos elementos pertenecen a H_3 de orden 9. En cuanto a los del tipo $\begin{Vmatrix} 0 & a \\ b & 0 \end{Vmatrix}$, se tiene

$$\begin{Vmatrix} 0 & a \\ b & 0 \end{Vmatrix}^2 = \begin{Vmatrix} ab & 0 \\ 0 & ab \end{Vmatrix} = I \text{ si, y sólo si, } ab = 1$$

y supuesto $w \in G_3$, $w \neq 1$, resultan las posibilidades

$$a = b = 1, \quad a = w;\ b = w^2, \quad a = w^2;\ b = w.$$

Luego los elementos de orden 2 en G son

$$x = \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}; \quad y = \begin{Vmatrix} 0 & w \\ w^2 & 0 \end{Vmatrix}; \quad z = \begin{Vmatrix} 0 & w^2 \\ w & 0 \end{Vmatrix}$$

y los 2-subgrupos de Sylow de G

$$H_2 = \langle x \rangle; \quad H_2' = \langle y \rangle; \quad H_2'' = \langle z \rangle.$$

Ejemplo 3. Sea $G = \mathbf{D}_n$ un grupo diédrico de orden $2n$. Recordemos que $\mathbf{D}_n = \langle a, b / a^n = b^2 = (ab)^2 = 1 \rangle$, y que todo elemento de dicho grupo se escribe unívocamente en la forma

$$a^i b, \text{ o bien } a^i \qquad (0 \leq i < n)$$

y que todo subgrupo $H \subset \langle a \rangle$ es invariante. Supongamos $n = 2^s t$, $(t, 2) = 1$. Luego, $|\mathbf{D}_n| = 2^{s+1} t$, y se afirma que

i) $\mathbf{D}_n$ posee exactamente t, 2-subgrupos de Sylow, de orden 2^{s+1} e isomorfos a $\mathbf{D}_{2^s}$.

ii) Si p es impar, $\mathbf{D}_n$ posee un único p-subgrupo de Sylow, el cual es cíclico y tiene por orden la mayor potencia del primo p que divida al entero t.

Consideremos el subgrupo invariante cíclico de orden 2^s

$$H = \langle a^t \rangle.$$

En virtud de que H es un 2-subgrupo de $\mathbf{D}_n$, está contenido en un 2-subgrupo de Sylow. Ahora bien, como los 2-subgrupos de Sylow son conjugados y H es invariante, entonces H está contenido en todo 2-subgrupo de Sylow de $\mathbf{D}_n$. En consecuencia, para encontrar los 2-subgrupos de Sylow habrá que considerar subgrupos del tipo $\langle x, H\rangle$ con $x \notin H$. Los elementos $x \in \langle a\rangle - H$ no nos sirven, pues su orden es coprimo a 2. Cualquiera que sea $t (0 \leq t < n)$, se tiene

$$K_t = \langle a^t b, H\rangle = \langle a^t b\rangle \cdot H$$

que es un subgrupo, pues H es invariante, y tiene por orden

$$|\langle a^t b, H\rangle| = |\langle a^t b\rangle H| = \frac{|\langle a^t b\rangle| \cdot |H|}{|\langle a^t b\rangle \cap H|} = \frac{2 \cdot 2^n}{1} = 2^{n+1}$$

luego los K_t son 2-subgrupos de Sylow de $\mathbf{D}_n$. Ahora

$$K_t = \langle a^t b, H\rangle = \langle a^t b, a^t\rangle = \{a^{tj+t} b, a^{tj}/0 \leq j < 2^n\}$$

y de aquí se deduce que K_t posee 2^n elementos de la forma $a^k b$, y como hay exactamente $n = 2^n t$ de ellos, sólo los subgrupos

$$K_0\ K_1 \ldots K_{t-1} \text{ son distintos.}$$

Por último, es claro que los K_t son diédricos, puesto que $\{a^t b, a^t\}$ es un conjunto de generadores y satisface

92 $$(a^t)^{2^n} = a^n = 1 \qquad (a^t b)^2 = (a^t a^t b)^2 = (a^{t+t} b)^2 = 1.$$

Para probar iii), nótese que si p es primo impar $p/2n = 2^{n+1} t$, entonces p/t, y suponiendo que $t = p^r k$ con $(p, k) = 1$, el subgrupo invariante

$$L = \langle a^{2^n k}\rangle$$

es el único p-subgrupo de Sylow de $\mathbf{D}_n$.

Ejemplo 4. Cálculo de p-subgrupos de Sylow en $\mathbf{S}_p$. Como $p! = p(p-1)!$ con $(p, (p-1)!) = 1$, todo p-subgrupo de Sylow en $\mathbf{S}_p$ tendrá p elementos, y por consiguiente será cíclico generado por un elemento de orden p. Dichos elementos en $\mathbf{S}_p$ son necesariamente p-ciclos. Sabemos que en $\mathbf{S}_p$ hay exactamente

$$\frac{p!}{p(p-p)!} = (p-1)! \quad p\text{-ciclos.}$$

Sea n_p = número de p-subgrupos de Sylow. Entonces, teniendo en cuenta que en cada tal subgrupo hay exactamente $p-1$, p-ciclos, se tiene que $n_p(p-1) = (p-1)!$, de donde $n_p = (p-2)!$, y por los teoremas anteriores obtenemos

$$(p-2)! \equiv 1 (p)$$

el llamado *teorema de Wilson.*

Para el cálculo de los subgrupos de Sylow de $\mathbf{S}_n$ consúltese la obra citada en (15).

§4. 3. APLICACIONES

1. No existe un grupo simple de orden 56. En efecto, $56 = 7 \cdot 2^3$. Sea n_7 el número de subgrupos de orden 7 de G. Sabemos, por los teoremas de Sylow, que n_7 verifica

i) $n_7 \equiv 1(7)$ ii) $n_7/8$.

De la segunda condición resulta

$$n_7 = 1, 2, 4, 8.$$

De estos, 2 y 4 no verifican la primera condición, y en consecuencia quedan descartados. Si $n_7 = 1$, existe un único 7-subgrupo de Sylow, que es por tanto invariante, y así el grupo no puede ser simple. Si $n_7 = 8$ entonces el grupo posee exactamente $8(7-1) = 8 \cdot 6 = 48$ elementos de orden 7. Los elementos restantes $56 - 48 = 8$ sólo pueden formar 1,2-subgrupo de Sylow, es decir $n_2 = 1$ y así el (único) 2-subgrupo de Sylow es invariante, luego el grupo no es simple.

2. No existe un grupo simple de orden 30. La descomposición en factores primos es: $30 = 2 \cdot 3 \cdot 5$, y como el número de 5-subgrupos de Sylow, n_5, debe satisfacer

i) $n_5 \equiv 1(5)$ ii) $n_5/6$

resulta $n_5 = 1, 6$. Si $n_5 = 1$, G no es simple. Luego $n_5 = 6$. Análogamente, se obtiene $n_3 = 10$. En consecuencia, el grupo posee *por lo menos* $6(5-1) + 10(3-1) + 1 = 24 + 20 + 1 = 45$ elementos, lo cual es absurdo.

3. No existe un grupo simple de orden 80. En efecto, por los teoremas de Sylow debe tenerse $n_5 = 16$. Luego el grupo posee $16(5-1) = 64$ elementos de orden 5, y los 16 elementos restantes sólo pueden formar un 2-subgrupo de Sylow, por lo tanto invariante.

4. No hay un grupo simple de orden 84. Si n_7 debe satisfacer

i) $n_7/12$ ii) $n_7 \equiv 1(7)$

la única posibilidad es $n_7 = 1$.

5. No hay grupos simples de orden 12. Se tiene $12 = 3 \cdot 2^2$. Sea n_3 el número de 3-subrgrupos de Sylow, entonces $n_3/4$, $n_3 \equiv 1(2)$. De la primera condición se deduce que

$$n_3 = 1, 2, 4.$$

El caso $n_3 = 2$ queda descartado por no cumplir la segunda condición. Si fuese $n_3 = 1$, dicho subgrupo sería invariante y el grupo no sería simple. En el caso $n_3 = 4$, el grupo posee $4(3-1) = 8$ elementos de orden 3, por lo tanto los $12 - 8 = 4$ elementos restantes sólo pueden constituir un 2-subgrupo de Sylow, el cual sería invariante, y entonces el grupo no es simple. Más generalmente:

Proposición 4.3.21. No hay grupo simple de orden p^2q, con p, q primos.

Demostración. Si el grupo es abeliano, la proposición es evidente. Si $p = q$, entonces el grupo en cuestión es un p-grupo, luego su centro es $\neq 1$, y así, es un subgrupo invariante no trivial. Supongamos $p \neq q$. Si $q < p$, por los teoremas de Sylow ($q \not\equiv 1(p)$), el grupo posee un único p-subgrupo de Sylow, que, por lo tanto, será invariante. Sea $p < q$. Como $p \not\equiv 1(q)$, existen 1 ó p^2-subgrupos de orden q. Si $n_q = 1$, dicho q-subgrupo de Sylow es invariante. Si $n_q = p^2$, los restantes $p^2q - p^2(q-1) = p^2$ elementos pueden formar un solo p-subgrupo de Sylow. Luego será invariante. ▲

Mediante el grupo simétrico es posible resolver casos particulares del teorema de Burnside citado en el capítulo anterior.

Proposición 4.3.22. Sea p primo impar y sea $m = 1, 2$ ó 3, $n \geq 0$. Si G es un grupo no cíclico de orden $2^m p^n$, entonces G no es simple.

Demostración. Si $n = 0$, el resultado es trivial. Sea n_p = número de p-subgrupos de Sylow. Se debe verificar $n_p / 2^m$, por lo tanto $n_p = 1, 2, 4$ y 8. Además, debe ser $n_p \equiv 1 (p)$.

i) Si $n_p = 1$, el grupo no es simple.

ii) El caso $n_p = 2$ no es posible, pues no se verifica que $n_p \equiv 1 (p)$.

iii) El caso $n_p = 4$ sólo verifica $n_p \equiv 1 (p)$, si $p = 3$.

iv) El caso $n_p = 8$ ídem, con $p = 7$.

Supongamos $n_p = 4$, $p = 3$.

Sea P un 3-subgrupo de Sylow, $N = N(P, G)$. Por lo tanto, $4 = |G : N|$. Aplicando la proposición 2.4.5 al subgrupo N de G, se concluye (si G es simple) que éste es isomorfo a un subgrupo de $\mathfrak{S}_4$, por lo tanto $n = 1$, y el grupo G es de orden $2^2 \cdot 3$. Sea Q un 2-subgrupo de Sylow, luego $|G : Q| = 3$, y por lo tanto, aplicando otra vez la proposición 2.4.5, G es isomorfo a un subgrupo de $\mathfrak{S}_3$, o sea $n = 1$. De ello se deduce que $|G| = 6$. Pero, sabemos ya que grupos de orden pq no son simples.

Supongamos $n_p = 8$, $p = 7$. Sea, como antes, P un p-subgrupo de Sylow, $N = N(P, G)$. Aplicando la proposición 2.4.5, se obtiene $|G|/8!$, y así $n = 1$, y dado que $n_p = 8$, entonces $m = 3$. Luego, $|G| = 8 \cdot 7 = 56$; y ya sabemos que los grupos de este orden no son simples. ▲

Proposición 4.3.23. Sea G un grupo no cíclico de orden n. Sea H un subgrupo de G, $N = N(H, G)$, $|G : N| = m$. Si $m! < n$, entonces G no es simple.

Demostración. Supongamos que G sea simple. Aplicando la proposición 2.4.5, y teniendo en cuenta que G no posee subgrupos invariantes propios, resulta $n / m!$, lo cual es imposible si $m! < n$. ▲

Corolario. Si G es un grupo no cíclico de orden n, y si para algún primo p, p / n, se verifica $n_p! < n$, entonces G no es simple.

Demostración. Tómese como H un p-subgrupo de Sylow. ▲

Ejemplo 1. No hay grupo simple de orden 48. Se tiene $48 = 2^4 \cdot 3$. Por lo tanto, $n_2 = 1, 3$. Si $n_2 = 3$, aplicando el corolario de la proposición 4.3.23, se deduce que G no es simple.

Ejemplo 2. No hay grupo simple de orden $96 = 2^5 \cdot 3$. En efecto, $n_2 = 1, 3$. Si $n_2 = 3$, por la proposición 4.3.23, G no es simple.

Ejemplo 3. Sea G un grupo de orden 12 sin elementos de orden 2 en el centro, entonces $G \simeq A_4$. Sea n_3 el número de 3-subgrupos de Sylow de G. Por los teoremas de Sylow, se tiene $n_3 = 1$ ó 4. Si $n_3 = 1$, $P = \{1, x, x^2\}$ es el único 3-subgrupo de Sylow. Luego x y x^2 son los únicos elementos de orden 3 en G. Ahora bien, G opera por conjugación sobre $X = \{x, x^2\}$, luego $|0_x| = 1$ ó 2. En consecuencia, $|H_x| = 12$ ó 6, o sea

siempre hay elementos de orden 2 en G que conmutan con x. Sea $z \in G$ un elemento tal y P' un 2-subgrupo de Sylow de G tal que $z \in P'$. Como P' es abeliano y conmuta con todo elemento de P', entonces conmuta también con todo elemento de $\langle P, P' \rangle = G$; en consecuencia, z es un elemento de orden 2 en el centro de G, lo cual es absurdo. Por lo tanto debe tenerse $n_3 = 4$. Aplicando la proposición 2.4.5 al subgrupo de Sylow P de índice 4, y teniendo en cuenta que, por lo anterior, P no es invariante, resulta un monomorfismo $\phi : G \to \mathbf{S}_4$. Como $\phi(G)$ es un subgrupo de orden 12 de $\mathbf{S}_4$ y el único subgrupo tal es $\mathbf{A}_4$, tenemos $G \simeq \mathbf{A}_4$.

Proposición 4.3.24. Sea G un grupo finito, H un subgrupo invariante y P un p-subgrupo de Sylow de G. Entonces

i) $P \cap H$ es un p-subgrupo de Sylow de H.

ii) $\frac{P \cdot H}{H}$ es un p-subgrupo de Sylow de G/H.

Demostración. Sea $|H| = p^k \cdot r_1$ con $(p, r_1) = 1$, $|G/H| = p^t \cdot r_2 (p, r_2) = 1$. Por lo tanto $|G| = p^{k+t} r_1 r_2$ con $(p, r_1 r_2) = 1$, $|P| = p^{k+t}$. Para probar i) será suficiente demostrar que $|P \cap H| = p^k$. Es claro que $|P \cap H| = p^e$ $0 \leq e \leq k$. Sea S un p-subgrupo de Sylow de H; $|S| = p^k$, y además, S es un p-subgrupo de G. Por el teorema de Sylow existe un p-subgrupo de Sylow de G, digamos P_1, tal que $S \subseteq P_1$. También, por los teoremas de Sylow, P y P_1 son conjugados en G, luego existe $x \in G$ tal que

$$x^{-1} P_1 x = P, \text{ y así, } x^{-1} S x \subseteq x^{-1} P_1 x \subseteq P.$$

Pero, por ser H invariante, se tiene $x^{-1} S x \subseteq x^{-1} H x = H$. Por lo tanto, $x^{-1} S x \subseteq H \cap P$, de donde $p^k = |x^{-1} S x| = |S| \leq |P \cap H|$, y consecuentemente, $|P \cap H| = p^k$, de donde resulta i). Para probar ii), vemos que, por los teoremas de isomorfismo, se tiene $\frac{P \cdot H}{H} \simeq \frac{P}{P \cap H}$ y además, por lo ya indicado

$$\left| \frac{PH}{H} \right| = \left| \frac{P}{P \cap H} \right| = \frac{|P|}{|P \cap H|} = \frac{p^{k+t}}{p^k} = p^t;$$

siendo $\frac{PH}{H}$ un p-grupo de G/H de orden p^t, resulta que es un p-subgrupo de Sylow.

Ejemplo 1. La condición H *invariante en* G es evidentemente necesaria. Por ejemplo, si $G = \mathbf{S}_3$, $H = \langle (12) \rangle = \{1, (12)\}$. Entonces H posee un 2-subgrupo de Sylow: H mismo. Ahora bien, $P = \langle (13) \rangle = \{1, (13)\}$ es un 2-subgrupo de $\mathbf{S}_3$, pero $P \cap H = 1$ no lo es de H.

Ejemplo 2. Grupo de Sylow en el caso infinito. Si G es un grupo infinito, se denomina p-subgrupo de Sylow de G a todo subgrupo maximal en el conjunto de todos los p-subgrupos de G. Esta definición, en virtud de los teoremas de Sylow, es a las claras una extensión de la del caso finito. Lamentablemente, las analogías con los teoremas de Sylow, en el caso infinito, no se conservan. Por ejemplo, consideremos el producto semidirecto: $G = (Z \oplus Z) \times_{\phi} Z_4$ donde

$$\phi : Z_4 \to \mathrm{Aut}(Z \oplus Z)$$

está definida por

$$\phi(1)(r, s) = (-s, r).$$

Es fácil verificar que cualquiera que sea $(r,s) \in Z \oplus Z$, los subgrupos $H_{r,s} = \langle (1,(r,s)) \rangle$ definen una clase de 2-subgrupos de Sylow conjugados de orden 4. El subgrupo $H = \langle (2,(1,0)) \rangle$ es un 2-subgrupo de Sylow de orden 2, y por razones de orden, no es conjugado a ningún $H_{r,s}$.

§ 4.4. GRUPOS RESOLUBLES

Es frecuente en matemática encarar el estudio de entes complejos reduciéndolos a componentes más simples que puedan considerarse irreducibles en algún sentido. Por ejemplo, los números enteros se descomponen en primos, los polinomios en factores irreducibles, los grupos abelianos finitos en p-grupos cíclicos. Tales descomposiciones no son de gran valor si no llevan aparejada la noción de *unicidad*, en algún sentido. Veamos aquí una tal descomposición en grupos finitos.

Definición 4.4.15. Un subgrupo invariante H de un grupo G se dirá *invariante maximal* si, y sólo si, no existe un subgrupo invariante K de G tal que

$$G \supsetneq K \supsetneq H;$$

obsérvese que lo anterior equivale a afirmar que el grupo cociente G/H no posee subgrupos invariantes, es decir, es simple. Por cierto que cada vez que H sea invariante en G y el cociente G/H tenga orden primo, H será invariante maximal. Si G es un grupo finito no simple, entonces

posee subgrupos invariantes propios, y en este caso también subgrupos invariantes maximales: sea H_2 un tal subgrupo. Si H_2 no es simple, existirá un subgrupo invariante maximal H_3 de H_2, ... Continuando en esta forma, comprobamos que todo grupo finito G posee una *serie de composición*, es decir, una sucesión de subgrupos propios

$$G = H_1 \supsetneq H_2 \supsetneq H_3 \supsetneq \cdots \supsetneq H_r = 1 \qquad (*)$$

donde H_{i+1} es invariante maximal en H_i $(1 \leq i < r)$. Los grupos cocientes H_i/H_{i+1} se denominan *grupos cocientes de la serie* (*). Note el lector que H_{i+1} es invariante (maximal) en H_1, pero no necesariamente en los grupos $G, H_2 \ldots H_{i-1}$.

$$\text{Si } G = K_1 \supsetneq K_2 \supsetneq K_3 \supsetneq \cdots \supsetneq K_s = 1 \qquad (**)$$

es otra serie de composición de G, diremos que (*) y (**) *son equivalentes* si existe una biyección entre los grupos cocientes tal que grupos cocientes correspondientes sean isomorfos.

Ejemplo. Las series de composición de $\mathbf{Z}_{30}$: $\mathbf{Z}_{30} \supsetneq \mathbf{Z}_6 \supsetneq \mathbf{Z}_3 \supsetneq 1$; $\mathbf{Z}_{30} \supsetneq \mathbf{Z}_{10} \supsetneq \mathbf{Z}_2 \supsetneq 1$ tienen por grupos cocientes $\mathbf{Z}_5$, $\mathbf{Z}_2$, $\mathbf{Z}_3$ y $\mathbf{Z}_3$, $\mathbf{Z}_5$, $\mathbf{Z}_2$ y por lo tanto son equivalentes.

§ 4.5. TEOREMAS DE JORDAN-HÖLDER

Teorema 4.5.13. Dos series de composición (*) y (**) de un grupo G son siempre equivalentes.

Demostración. Inducción en el orden de G. Si $|G| = 2$, la única serie de composición de G es $G \supsetneq 1$, y por tanto nada hay que demostrar.

Supongamos el teorema válido para grupos cuyo orden sea menor que el orden de G. Si G es un grupo simple, la única serie es $G \supsetneq 1$, luego el teorema es válido en este caso. Si G no es simple, cabe distinguir dos casos:

i) $H_2 = K_2$. En este primer caso, por hipótesis inductiva, las dos series de composición de H_2, deducidas de (*) y (**) al eliminar el grupo de la izquierda, son equivalentes; luego las series originales también lo son.

ii) Si $H_2 \neq K_2$. Como ambos son invariantes en G, así lo es $H_2 \cdot K_2$. Como $H_2 \neq K_2$, luego $H_2 \subsetneq H_2K_2$; y por la maximalidad de H_2, debe ser $G = H_2 \cdot K_2$. Poniendo $L_1 = H_2 \cap K_2$, se tiene por el teorema de isomorfirmo:

$$\left.\begin{aligned} G/H_2 &= H_2K_2/H_2 \simeq K_2/L_1 \\ G/K_2 &= H_2K_2/K_2 \simeq H_2/L_1 \end{aligned}\right\} \quad (1)$$

Por consiguiente, K_2/L_1 y H_2/L_1 son simples, pues G/H_2 y G/K_2 lo son. Sea $L_1 \supsetneq L_2 \supsetneq \cdots \supsetneq L_t = 1$ una serie de composición de L_1. En tal caso las siguientes son series de composición de G: (por 2)

$$G \supsetneq H_2 \supsetneq L_1 \supsetneq L_2 \supsetneq \cdots \supsetneq L_t = 1 \quad (3)$$

$$G \supsetneq K_2 \supsetneq L_1 \supsetneq L_2 \supsetneq \cdots \supsetneq L_t = 1 \quad (4)$$

Los grupos cocientes son

$$G/H_2, H_2/L_1, L_1/L_2, \ldots, L_t$$

$$G/K_2, K_2/L_1, L_1/L_2, \ldots, L_t$$

Entonces, por (1), las series (3) y (4) son equivalentes ya que, salvo la permutación de los dos grupos de la izquierda, los demás son los mismos. También son equivalentes las series de H_2, deducidas en (*) y (3) al eliminar el grupo de la izquierda, entonces (*) y (3) son equivalentes. Análogamente con (**) y (4). Luego, (*) y (**) son equivalentes. ▲

Ejemplo 1. El grupo S_3 tiene por única serie de composición

$$S_3 \supsetneq A_3 \supsetneq 1$$

con grupos cocientes; Z_2, Z_3.

Ejemplo 2. El grupo S_4 tiene por serie de composición

$$S_4 \supsetneq A_4 \supsetneq H \supsetneq L \supsetneq 1$$

donde $H = \{1, (12)(34), (13)(24), (14)(23)\}$ y $L = \{1, (12)(34)\}$. Los grupos cocientes son: Z_2, Z_3, Z_2, Z_2.

Ejemplo 3. El grupo cíclico Z_6 tiene dos series de composición

$$Z_6 \supsetneq Z_3 \supsetneq 1 \quad \text{y} \quad Z_6 \supsetneq Z_2 \supsetneq 1$$

con cocientes: Z_2, Z_3 y Z_3, Z_2.

Ejemplo 4. En el próximo capítulo demostraremos que si $n \geq 5$, A_n es simple (y no cíclico), y por lo tanto

$$S_n \supsetneq A_n \supsetneq 1$$

será serie de composición de $S_n (n \geq 5)$.

Definición 4.5.16. Un grupo G se dice resoluble si, y sólo si, para alguna serie de composición (y en tal caso, para todas):

$$G = H_1 \supsetneq H_2 \supsetneq \cdots \supsetneq H_r = 1$$

los grupos cocientes tienen orden primo. Para otras definiciones equivalentes de grupo resoluble consulte el lector la cita (15). Un resultado muy útil lo da la siguiente proposición.

Proposición 4.5.25. Sea H un subgrupo invariante de G. Si H y G/H son resolubles, entonces G también lo es.

Demostración. Sean

$$H = H_1 \supsetneq H_2 \supsetneq \cdots \supsetneq H_r = 1$$

$$G/H = G_1/H \supsetneq G_2/H \supsetneq \cdots \supsetneq G_s/H = H$$

series de composición. Como, por los teoremas de isomorfismo

$$\frac{G_i/H}{G_{i+1}/H} \simeq G_i/G_{i+1}$$

se infiere que

$$G = G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_{s-1} \supsetneq H \supsetneq H_2 \supsetneq \cdots \supsetneq H_r = 1$$

es una serie de composición de G, donde todos los cocientes tienen orden primo. Luego G es resoluble. ▲

Ejemplo. i) Los ejemplos 1, 2 y 3 corresponden a grupos resolubles en tanto que $S_n (n \geq 5)$ no, pues $|A_n|$ no es primo.

ii) Los p-grupos son resolubles. Sea G de orden p^r y supongamos (hipótesis inductiva) que todo p-grupo de orden menor que p^r es resoluble. Sabemos que todo p-grupo posee un subgrupo invariante H de orden p^{r-1}, el cual por tener orden p es resoluble. La proposición anterior nos dice ahora que G es resoluble.

iii) Un enunciado equivalente al teorema de Burnside es el siguiente: Todo grupo de orden $p^r \cdot q^s$ (p, q primos) es resoluble.

iv) Si G es simple y resoluble, entonces $G \simeq Z_p$ para algún primo p. Un resultado muy importante debido a W. Feit y J. Thompson[32] establece que: Todo grupo finito de orden impar es resoluble.

Respecto a los grupos resolubles, es posible demostrar una generalización de los teoremas de Sylow, a saber: Sea G un grupo resoluble de orden m, n con $(m, n) = 1$. Entonces

i) G posee subgrupos de orden m.

ii) Los subgrupos de orden m son conjugados.

iii) Todo subgrupo de orden m', tal que m'/m, está contenido en un subgrupo de orden m.

iv) El número h_m de subgrupos de orden m se puede expresar como producto de factores, cada uno de los cuales:

- es congruente a 1 tomando como módulo algún factor primo de m, y
- es potencia de un número primo.

Una demostración de este resultado figura en la cita (15) de la bibliografía.

5

GRUPOS SIMPLES, EXTENSIONES

En la teoría de grupos finitos, los grupos simples desempeñan un papel muy importante ya que se les puede considerar como el punto de partida del estudio de la teoría. Se conocen varias familias de grupos simples, y en este capítulo nos ocuparemos de una tal familia: $\mathbf{A}_n (n \in \mathbf{N})$. Por resultados obtenidos en capítulos anteriores, mostraremos que el único grupo simple no cíclico de orden no superior a 100 es $\mathbf{A}_5$. La parte final del capítulo la destinaremos al problema de extensiones y veremos en qué forma los grupos simples se pueden utilizar para construir los demás grupos finitos.

§ 5.1. SIMPLICIDAD DE A_n

Teorema 5.1.14. Si $n \in \mathbf{N}$, $n \neq 4$, el grupo $\mathbf{A}_n$ es simple.

Demostración. Si $n \in \mathbf{N}$ y $n \leq 3$, el resultado es trivial. Supongamos entonces $n \geq 5$. Sea H un subgrupo invariante de $\mathbf{A}_n$, $H \neq 1$, y supongamos $1 \neq s \in H$. Ahora, como $z(\mathbf{A}_n) = 1$ y $\mathbf{A}_n$ está generado por 3-ciclos, es posible hallar un 3-ciclo t tal que $st \neq ts$. Por lo tanto, $1 \neq \varrho = tst^{-1}s^{-1} \in H$ es un elemento que puede escribirse como producto de dos 3-ciclos, a saber: t, sts^{-1}. Por lo dicho, ϱ es una permutación en $\mathbf{A}_n$ que "mueve" un número $r \leq 6$ de elementos. Descomponemos ϱ como producto de ciclos disjuntos y las posibilidades para r y la longitud de dichos ciclos se indican abajo

	$r = 6$		$r = 4$
i)	$6 = 6$	vii)	$4 = 4$
ii)	$6 = 2 + 4$	viii)	$4 = 2 + 2$
iii)	$6 = 3 + 3$		$r = 3$
iv)	$6 = 2 + 2 + 2$	ix)	$3 = 3$
	$r = 5$		$r = 2$
v)	$5 = 5$	x)	$2 = 2$
vi)	$5 = 2 + 3$		

(donde, por ejemplo el caso iv), debe entenderse: ϱ es una permutación que "mueve" 6 letras y se descompone como producto de 3, 2-ciclos disjuntos). Analicemos cada uno de estos casos. Los casos i), iv), vi), vii) y x) no pueden ocurrir, pues ϱ sería permutación impar y así $\varrho \in \mathbf{A}_n$.

Caso ii): Aquí $\varrho = (x_1x_2)(x_3x_4x_5x_6)$. Luego $\varrho^2 = (x_3x_5)(x_4x_6) \in H$, y entonces se reduce al caso viii).

Caso iii): Ahora $\varrho = (x_1\, x_2 x_3)(x_4\, x_5\, x_6)$. Sea $t = (x_2x_3\, x_4) \in \mathbf{A}_n$. Por lo tanto

$$t\varrho t^{-1} = (x_1 x_3 x_4)(x_2 x_5 x_6)$$

y así

$$t\varrho t^{-1} = (x_1 x_5 x_2 x_4 x_6) \in H \text{ y se reduce al caso v).}$$

Caso v): Se tiene $\varrho = (x_1 x_2 x_3 x_4 x_5)$. Sea $t = (x_2 x_3 x_4) \in \mathbf{A}_n$. Se tiene $t\varrho^{-1}t^{-1}\varrho = (x_1 x_4 x_2) \in H$, y entonces se reduce al caso ix).

Caso viii): En este caso, $\varrho = (x_1 x_2)(x_3 x_4)$. Como $n \geq 5$ existe y, con $y \neq x_i (i = 1, 2, 3, 4)$. Consideremos $u = (x_2, y, x_3) \in \mathbf{A}_n$ y se tiene $u\varrho u^{-1} = (x_1 y)(x_2 x_4)$ y por lo tanto $u\varrho u^{-1}\varrho = (x_1 x_4 x_3 x_2 y) \in H$ se reduce al caso v).

Caso ix): Se tiene, entonces, $\varrho = (x_1 x_2 x_3) \in H$. Como $n \geq 5$, $n - 2 \geq 3$, y dado que $\mathbf{A}_n$ es $(n-2)$-transitivo, cualquiera que sea $t = (n_1 n_2 n_3) \in \mathbf{A}_n$ es posible hallar $h \in A_n$, con $h(x_i) = n_i (i = (1, 2, 3)$. Por lo tanto

$$t = h\varrho h^{-1} \in H$$

lo cual dice que todo 3-ciclo es elemento de H, y como $\mathbf{A}_n$ está generado por 3-ciclos, debe ser $\mathbf{A}_n \subseteq H$, de donde $\mathbf{A}_n = H$. ▲

Corolario 1. Si $n \geq 3$, $n \neq 4$, entonces el único subgrupo invariante propio de $\mathbf{S}_n$ es A_n.

Demostración. Sea H invariante en $\mathbf{S}_n$; $1 \neq H \neq \mathbf{S}_n$. Por lo tanto, $H \cap \mathbf{A}_n$ es invariante en $\mathbf{A}_n$, y siendo $\mathbf{A}_n$ simple, se tiene

$$H \cap \mathbf{A}_n = 1, \text{ o bien } H \cap \mathbf{A}_n = \mathbf{A}_n.$$

En el último caso, $\mathbf{A}_n \subseteq H$, siendo $H \neq \mathbf{S}_n$, se deduce que $A_n = H$. En el primer caso se deduce que todo elemento no trivial de H es una permutación impar. En particular, $1 \neq \gamma \in H$ implica $\gamma^2 = 1$ (pues γ^2 es par). Afirmamos que el orden de H es 2. En efecto, si $1 \neq \gamma \neq \delta$, $1 \neq \delta$; $\gamma, \delta \in H$ sería $\gamma\delta \in H$ y $\gamma\delta \neq 1$ es una permutación par. Entonces $H = \{1, \gamma\}$, donde $\gamma^2 = 1$. Si se descompone γ como producto de ciclos disjuntos será

$$\gamma = (x_1 x_2) \ldots (x_{2t+1} x_{2t+2}) \qquad t \geq 0.$$

Ahora, tomando $\delta = (x_1 x_3) \in \mathbf{S}_n$, resulta $\gamma \neq \delta\gamma\delta^{-1} \neq 1$ con $\delta\gamma\delta^{-1} \in H$, lo cual es contrario a lo ya visto. ▲

Corolario 2. Todo grupo finito se puede sumergir en un grupo finito simple.

Demostración. Sea G un grupo de orden $m = 2^r \cdot k$ con $r \geq 0$, $k \geq 1$, $(2, k) = 1$.

a) Supongamos que G no posee elementos de orden 2^r. Por lo tanto, cualquiera que sea $x \in G$, orden de $x = 2^t s$ con $0 \leq t < r$, s/k. Sea $\Phi: G \to \mathbf{S}_n$ la representación de Cayley, es decir

$$\Phi(x)(y) = xy.$$

Sabemos que Φ es un monomorfismo y si $x \in G$, $x \neq 1$, entonces $\Phi(x)$ "mueve" todo elemento de G. Además, por las hipótesis formuladas en a), si se descompone $\Phi(x)$ como producto de ciclos disjuntos, habrá exactamente $2^r k/2^t s = 2^{r-t} k s^{-1}$ ciclos de longitud $2^t s$. Como $t < r$, el

número de ciclos es par, y así $\varphi(x) \in A_m$, para todo $x \in G$; por lo tanto, $\mathrm{Im}\varphi \subset A_m$. Si $m \neq 4$, A_m es simple y nuestro problema está resuelto. Si $m = 4$, consideramos la inclusión natural $A_4 \subset A_5$ y en tal caso $G \subseteq A_5$ es la inyección buscada.

b) Si G posee elementos de orden 2^r, consideramos el grupo $H = G \times Z_2$ de orden $2^{r+1} \cdot k$, sin elementos de orden 2^{r+1} y la inclusión natural $G \subseteq H$. Ahora H está en las condiciones de a). ▲

Nota. De estos resultados se deduce lo anticipado en el capítulo anterior: S_n es resoluble si, y sólo si, $n \leq 4$. El concepto de grupo resoluble tiene aplicación fundamental en la teoría de ecuaciones algebraicas, según la cual la *ecuación general* de grado n

$$a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \qquad (*)$$

es resoluble por radicales si, y sólo si, el grupo S_n es resoluble. Esta condición se satisface para $n \leq 4$, lo cual explica porqué hay fórmulas algebraicas que permiten obtener las raíces de (*) en función de los coeficientes. Por otra parte, llegamos a la conclusión de que no es posible hallar tales fórmulas para ecuaciones de grado 5 o mayor.

Proposición 5.1.26. Si G es un grupo simple de orden 60, entonces $G \simeq A_5$.

Demostración. Por los teoremas de Sylow, y teniendo en cuenta que G es simple, $n_p \neq 1$, se tienen las posibilidades

$$n_2 = 3, 5 \text{ ó } 15; \quad n_3 = 4 \text{ ó } 10; \quad n_5 = 6.$$

Por la proposición 4.3.23 los casos $n_2 = 3$ y $n_3 = 4$ están descartados. Luego, G posee 20 elementos de orden 3 y 24 de orden 5. (*)

i) Supongamos $n_2 = 15$. Si cada par de 2-subgrupos de Sylow de G tuvieran siempre intersección trivial, habrían entonces $15(4 - 1) + 1 = 46$ elementos en todos los 2-subgrupos de Sylow, que sumados a los 44 de (*) harían que el grupo G tuviera por lo menos $46 + 44 = 90$ elementos, lo que es absurdo. Luego, existen 2-subgrupos de Sylow, P_1 y P_2, tales que $P_1 \cap P_2 = L \neq 1$. Sea $P = \langle P_1, P_2 \rangle$. Como $P_i (i = 1, 2)$ son abelianos, L es invariante en P. Como $P_i \subseteq P (i = 1, 2) P_1 \neq P_2$, entonces $|P| > 4$. Luego $|P| = 12$, 20 ó 60. Si $N = N(P, G)$, como $P \subseteq N$, se tiene $|G : N| = 1, 3$ ó 5. Los dos primeros casos quedan descartados por la proposición 4.3.23, luego $|G : N| = 5$. (**)

ii) Si $n_2 = 5$, sea P un 2-subgrupo de Sylow de G, $N = N(P, G)$, luego $|G : N| = 5$ (***). En los dos casos posibles ($n_2 = 5$, 15) existe un subgrupo P, tal que $|G : N| = 5$. $(N = N(P, G))$.

Si X designa la totalidad de conjugados de P, entonces $|X| = 5$. Hacemos operar G sobre X por conjugación. Luego se tiene definido un morfismo $\varphi : G \to S(X) \simeq S_5$. Como G es simple, $\mathrm{Nu}\varphi = 1$; G se identifica a un subgrupo de orden 60 de S_5, que por tener índice 2 es invariante. Por el corolario 1, del teorema 5.1.14, se tiene $\varphi(G) = A_5$, luego $G \simeq A_5$. ▲

Teorema 5.1.15. Si G es grupo simple no cíclico de orden menor a 100, entonces $G \simeq A_5$.

Demostración. El caso $n = 60$ fue considerado en la proposición anterior. La tabla que sigue muestra la descomposición en factores primos de los números menores que 100 y las referencias indican el resultado que se aplica en cada caso para deducir que un grupo de ese orden no satisface las hipótesis.

Tabla

$1 = 1$		$34 = 2 \cdot 17$	D	$67 = 67$	A
$2 = 2$	A	$35 = 5 \cdot 7$	D	$68 = 2^2 \cdot 17$	E
$3 = 3$	A	$36 = 2^2 \cdot 3^2$	F	$69 = 3 \cdot 23$	D
$4 = 2^2$	B	$37 = 37$	A	$70 = 2 \cdot 5 \cdot 7$	H
$5 = 5$	A	$38 = 2 \cdot 19$	D	$71 = 71$	A
$6 = 2 \cdot 3$	D	$39 = 3 \cdot 13$	D	$72 = 2^3 \cdot 3^2$	F
$7 = 7$	A	$40 = 2^3 \cdot 5$	F	$73 = 73$	A
$8 = 2^3$	C	$41 = 41$	A	$74 = 2 \cdot 37$	D
$9 = 3^2$	B	$42 = 2 \cdot 3 \cdot 7$	G	$75 = 3 \cdot 5^2$	E
$10 = 2 \cdot 5$	D	$43 = 43$	A	$76 = 2^2 \cdot 19$	E
$11 = 11$	A	$44 = 2^2 \cdot 11$	E	$77 = 7 \cdot 11$	D
$12 = 2^2 \cdot 3$	E	$45 = 3^2 \cdot 5$	E	$78 = 2 \cdot 3 \cdot 13$	G
$13 = 13$	A	$46 = 2 \cdot 23$	D	$79 = 79$	A
$14 = 2 \cdot 7$	D	$47 = 47$	A	$80 = 2^4 \cdot 5$	J
$15 = 3 \cdot 5$	D	$48 = 2^4 \cdot 3$	I	$81 = 3^4$	C
$16 = 2^4$	C	$49 = 7^2$	B	$82 = 2 \cdot 41$	D
$17 = 17$	A	$50 = 2 \cdot 5^2$	E	$83 = 83$	A
$18 = 2 \cdot 3^2$	E	$51 = 3 \cdot 17$	D	$84 = 2^2 \cdot 3 \cdot 7$	J
$19 = 19$	A	$52 = 2^2 \cdot 13$	E	$85 = 5 \cdot 17$	D
$20 = 2^2 \cdot 5$	E	$53 = 53$	A	$86 = 2 \cdot 43$	D
$21 = 3 \cdot 7$	D	$54 = 2 \cdot 3^3$	F	$87 = 3 \cdot 29$	D
$22 = 2 \cdot 11$	D	$55 = 5 \cdot 11$	D	$88 = 2^3 \cdot 11$	F
$23 = 23$	A	$56 = 2^3 \cdot 7$	F	$89 = 89$	A
$24 = 2^3 \cdot 3$	F	$57 = 3 \cdot 19$	D	$90 = 2 \cdot 3^2 \cdot 5$	H
$25 = 5^2$	B	$58 = 2 \cdot 29$	D	$91 = 7 \cdot 13$	D
$26 = 2 \cdot 13$	D	$59 = 59$	A	$92 = 2^2 \cdot 23$	E
$27 = 3^3$	C	$60 = 2^2 \cdot 3 \cdot 5$		$93 = 3 \cdot 31$	D
$28 = 2^2 \cdot 7$	E	$61 = 61$	A	$94 = 2 \cdot 47$	D
$29 = 29$	A	$62 = 2 \cdot 31$	D	$95 = 5 \cdot 19$	D
$30 = 2 \cdot 3 \cdot 5$	J	$63 = 3^2 \cdot 7$	E	$96 = 2^5 \cdot 3$	I
$31 = 31$	A	$64 = 2^6$	C	$97 = 97$	A
$32 = 2^5$	C	$65 = 5 \cdot 13$	D	$98 = 2 \cdot 7^2$	E
$33 = 3 \cdot 11$	D	$66 = 2 \cdot 3 \cdot 11$	G	$99 = 3^2 \cdot 11$	E
				$100 = 2^2 \cdot 5^2$	F

Referencias:

A el orden es número primo.

B el orden es p^2 $\therefore$ el grupo es abeliano. Proposición 2.6.10.

C el orden es p^r $\therefore$ es p-grupo y su centro $\neq 1$. Proposición 2.6.9.

D el orden es $p \cdot q$ con $p \neq q$. Corolario, teorema 2.8.4.

E el orden es p^2q con $p \neq q$. Proposición 4.3.21.

F el orden es $2^n p^m$; $m = 1, 2, 3$, $n \geq 0$, $(p, 2) = 1$. Proposición 4.3.22.

G el orden es mp con $m \leq p$, p primo. Proposición 2.4.7.

H el orden es $2^k m$ y $k > 0$, $m > 0$, $(2, m) = 1$ y posee un subgrupo cíclico de orden 2^k. Corolario, proposición 3.4.18.

I el orden es proposición 4.3.23.

J dicho orden fue considerado anteriormente como ejemplo. ▲

Nota. Se conocen varias otras familias de grupos simples; por ejemplo, una de las más sencillas es la de los grupos *especiales proyectivos:*

$$\mathrm{PSL}(n, k) = \mathrm{SL}(n, k)/z(\mathrm{SL}(n, \mathrm{K})).$$

Estos grupos son simples para $n \geq 3$ y K cuerpo cualquiera, o bien $n = 2$, K cuerpo de más de 3 elementos. Para una demostración de este hecho, véase (22). Así también, respecto a otras de tales familias, consúltense las citas (6), (13) y (7). En la (13), se da una lista de los grupos simples conocidos y en la (7), se muestran los 53 grupos simples conocidos cuyo orden no supera a 1.000.000. De ellos, todos, excepto tres, pertenecen a familias infinitas de grupos simples. También allí se muestran grupos simples no isomorfos del mismo orden: estos son A_8 y $\mathrm{PSL}(3, k)$ (k cuerpo de 4 elementos), cuyo orden es 20.160. En el otro extremo están los resultados que aseguran la no simplicidad de grupos de un orden dado: los teoremas de Burnside y de Feit y Thompson citados en el capítulo anterior son ejemplo de ello.

Brauer y Tuan[30] prueban que el orden de un grupo simple no cíclico de orden pqr^n (p, q, r son primos distintos) debe ser necesariamente 60 ó 168. Brauer[28] prueba que el único grupo simple de orden $4p^rq^s$ (p, q primos $r \leq 2$) es el grupo A_5. Los únicos grupos simples de órdenes $3p^rq^s$ ($r \leq 2$) son A_8 y $\mathrm{PSL}(2, Z_7)$. Feit[31] prueba que si G es un grupo 2-transitivo de S_{s+1} tal que ningún elemento $s \in G$ deja fijo tres letras y si $|G| = qm(m+1)$, entonces, o bien G posee un subgrupo invariante de orden $m+1$, o bien $m = p^r$ para algún primo. Se han hallado muchos otros resultados de este tipo. Se recomienda al lector interesado en estas cuestiones consultar la cita (5), así como la bibliografía citada allí.

§ 5.2. EXTENSIONES

Dado un grupo G y un subgrupo invariante K, se puede "descomponer" el grupo G en los grupos K y G/K. El estudio de extensiones de grupos consiste en resolver el problema inverso: Dados K y G/K, ¿es posible reconstruir el grupo G? Si G, K y Q son grupos, y K es isomorfo a un subgrupo K_1 de G tal que el cociente G/K_1 es isomorfo a Q, diremos que G *es una extensión de* K *por* Q. Cada vez que esto ocurra, *identificaremos* K con K_1 y G/K_1 con Q e indicaremos con $\pi : G \to Q = G/K$ la proyección al cociente.

Ejemplo 1. Si G es un grupo y $K \subseteq G$ es un subgrupo invariante, entonces G es extensión en K por G/K.

Ejemplo 2. Si K y Q son grupos y $\theta : Q \to \mathrm{Aut}(K)$ es un morfismo, el producto semidirecto $G = K \times_\theta Q$ es una extensión de K por Q. En particular, el producto directo $G = K \times Q$ es una extensión de K por Q (así como también una extensión de Q por K).

Ejemplo 3. El grupo $G = S_3$ es una extensión de Z_3 por Z_2, vía la identificación: $Z_3 = \langle (123) \rangle$; pero no es una extensión de Z_2 por Z_3, pues S_3 no posee subgrupo invariante alguno isomorfo a Z_2.

El problema a resolver consiste en determinar la estructura (ley de composición) de cada extensión G de K por Q. Nótese que la resolución de este problema permite conocer la ley de composición de los grupos resolubles. Además, si se conocen los grupos simples (finitos), es posible determinar inductivamente la estructura de todos los grupos finitos (véase el capítulo 4). Vamos a encarar el problema en un caso particular: K *es abeliano* (para el desarrollo general se recomienda la lectura de las obras citadas en (20) y (15). Lo que sigue es enumerativo y con ello sólo se pretende dar al lector información sobre algunos hechos básicos de la teoría.

Notación. En el grupo G se utilizará la notación *aditiva* (sin suponer por eso que G es abeliano) y en el cociente Q la *multiplicativa*. En todo lo que sigue G es una extensión de K por Q.

Cada aplicación (no necesariamente morfismo) $\sigma : Q \to G$ que verifique

i) $\sigma(1) = 0$ y ii) $\pi \circ \sigma = \mathrm{Id}_Q$

se llamará *sección* de la extensión G.

1) La aplicación $\theta : Q \to \mathrm{Aut}(K)$, definida por $\theta(q)(k) = \sigma(q) + k - \sigma(q)$, es un homomorfismo que no depende de la sección σ de G:

i) θ está bien definida, pues como K es invariante, para cada sección σ, el automorfismo interior de G inducido por $\sigma(q)$ determina, por restricción al subgrupo K, un automorfismo (no necesariamente interior) de éste.

ii) La independencia de σ es consecuencia de que si τ es también sección de G, entonces

$$\pi(\sigma(q) - \tau(q)) = \pi(\sigma(q))\pi(\tau(q))^{-1} = qq^{-1} = 1$$

y entonces $\sigma(q) - \tau(q) \in K \subseteq C(K, G)$ (por ser K abeliano), y así

$$\sigma(q) + k - \sigma(q) = \tau(q) + k - \tau(q).$$

iii) Por último, θ es morfismo ya que como $\pi(\sigma(q) + \sigma(q_1) - \sigma(qq_1)) = 1$, entonces $\sigma(q) + \sigma(q_1) - \sigma(qq_1) \in K$ el cual es abeliano.

Veremos pues que cada extensión G de K por Q determina un morfismo $\theta : G \to \mathrm{Aut}(K)$ el cual satisface 1); en consecuencia, Q *opera sobre* K en la forma

$$q \cdot k = \theta(q)(k) = \sigma(q) + k - \sigma(q).$$

2) En particular, se satisfacen las relaciones

i) $q \cdot (k + k_1) = q \cdot k + q \cdot k_1$, ii) $(qq_1) \cdot k = q \cdot (q_1 \cdot k)$ y iii) $1 \cdot k = k$ cualesquiera que sean $q, q_1 \in Q$, $k, k_1 \in K$.

Ejemplo 1. Sea G una extensión de K por Q. Entonces la Q-acción definida sobre K es trivial ($q \cdot k = k, q \in Q, k \in K$) si, y sólo si, $K \subseteq z(G)$. En efecto, si $K \subseteq z(G)$, entonces todo automofismo interior de G deja fijo los elementos de K, y por consiguiente $q \cdot k = \sigma(q) + k - \sigma(q) = k$. Recíprocamente, si la acción es trivial, dados $x \in G$ y $k \in K$, siempre es posible hallar una sección σ y un elemento $q \in Q$ tal que $\sigma(q) = x$, por lo tanto $x + k - x = \sigma(q) + k - \sigma(q) = q \cdot k$, lo cual prueba que $K \subseteq z(G)$.

Ejemplo 2. Sea $\mathbf{H_2} = \langle A, B/A^4 = 1,\ A^2 = B^2,\ BAB^{-1} = A^{-1} \rangle$ el grupo cuaterniónico. Si consideramos el subgrupo invariante $\langle A \rangle \simeq \mathbf{Z_4}$, y el cociente $\mathbf{H_2}/\langle A \rangle = \{1, b\} \simeq \mathbf{Z_2}$, entonces $\mathbf{H_2}$ es extensión de $\mathbf{Z_4}$ por $\mathbf{Z_2}$. ¿Cuál es el morfismo $\theta : \{1, b\} \to \mathrm{Aut}(\langle A \rangle)$ inducido en este caso? Adviértase que como $\mathrm{Aut}(\langle A \rangle) \simeq \mathrm{Aut}(\mathbf{Z_4}) \simeq \mathbf{Z_2}$, el grupo $\langle A \rangle$ posee sólo dos automorfismos:

$$\mathrm{Id}, f \text{ (donde, } f(A) = A^3).$$

En consecuencia, sólo hay dos morfismos posibles, a saber

$$\theta_1(1) = \theta_1(b) = \mathrm{Id} \quad \text{y} \quad \theta_2(1) = \mathrm{Id},\ \theta_2(b) = f.$$

Si el morfismo buscado fuese θ_1, la acción de $\{1, b\}$ sobre $\langle A \rangle$ sería trivial, y en tal caso, por el ejemplo 1, se tendría $\langle A \rangle \subseteq z(\mathbf{H_2})$, lo cual es falso. En consecuencia, $\mathbf{H_2}$ induce θ_2. Para comprobarlo notemos que una posible sección $\sigma : \{1, b\} \to \mathbf{H_2}$ puede tomarse en la forma: $\sigma(1) = 0$, $\sigma(b) = B$, luego: $\sigma(b) + A - \sigma(b) = BAB^{-1} = A^{-1} = A^3 = \theta_2(b)(A)$, lo cual confirma lo dicho antes.

Dado un morfismo $\Phi : Q \to \mathrm{Aut}(K)$, y si G es una extensión de K por Q, diremos que G *realiza* Φ si, y sólo si, se verifica 2) con Φ en vez de θ. En virtud de 1), cabe replantear el problema de extensión de grupos así: Dados grupos K (abeliano), Q y $\Phi : Q \to \mathrm{Aut}(K)$ un morfismo, hallar todas las extensiones G de K por Q que realizan Φ (si las hay).

Ejemplo 1. Sean K y Q grupos, K abeliano, $\Phi : Q \to \mathrm{Aut}(K)$ un morfismo; entonces, el producto semidirecto $G = K \times_\Phi Q$ es una extensión de K por Q que realiza Φ. En efecto, por las identificaciones naturales (K con el subgrupo $K \times 1$ y Q con $0 \times Q$), se tiene la sección $\sigma : Q \to G$, definida por $\sigma(q) = (0, q)$. Se verifica

$$\sigma(q) + k - \sigma(q) = (0, q) + (k, 1) - (0, q) = (\Phi(q)(k), 1) = \Phi(q)(k).$$

Hemos visto que existen siempre extensiones que realizan un morfismo dado $\Phi : Q \to \mathrm{Aut}(K)$: el producto semidirecto $K \times_\Phi Q$. Sin embargo, obsérvese que las extensiones que realizan un morfismo Φ no son únicas. En efecto, hay extensiones que no son producto semidirecto.

Ejemplo 2. Sea $G = \mathbf{Z}_n$, p primo, $n \geq 2$. Sea K el único subgrupo de G isomorfo a $\mathbf{Z}_p$ y Q el cociente. En consecuencia, $Q \simeq \mathbf{Z}_{p^{n-1}}$. Entonces, G es una extensión de $\mathbf{Z}_p$ por $\mathbf{Z}_{p^{n-1}}$ mas no el producto semidirecto de

subgrupos propios, ya que todo subgrupo no trivial de G contiene a K.

Sea G una extensión que realiza $\theta : Q \to \mathrm{Aut}(K)$ y σ una sección de G. Entonces, de acuerdo con 1, iii), para $q, q_1 \in Q$ se tiene $\sigma(q) + \sigma(q_1) - \sigma(qq_1) \in K$. Luego tenemos definida una aplicación

$$f_\sigma : Q \times Q \to K, \text{ poniendo } f_\sigma(q, q_1) = \sigma(q) + \sigma(q_1) - \sigma(qq_1).$$

3) Esta función f_σ se denomina *sistema de factores* (o también cociclo, o 2-cociclo). En principio, nótese que la definicion del cociclo f_σ depende de la sección σ elegida, es decir, distintas secciones de una misma extensión G dan lugar (en general) a distintos cociclos. Por otra parte, es interesante observar que $f_\sigma(q, q_1) = 0$ $(\forall\, q, q_1 \in Q)$ si, y sólo si, σ es un morfismo.

Esta última condición equivale a afirmar que G es un producto semidirecto. Es claro que, si G es un producto semidirecto, $\sigma(q) = (0, q)$ es un morfismo, y por tanto, $f_\sigma = 0$. Análogamente, si σ puede tomarse como morfismo, entonces G es un producto semidirecto de los subgrupos K, $\sigma(Q)$ (verifique el lector). En este sentido, f_σ puede interpretarse como una medida respecto a cuán lejos está σ de ser morfismo (o G de ser un producto semidirecto).

Ejemplo. Volvamos a un ejemplo anterior: $G = \mathbf{Z}_{p^n}$, $K = \mathbf{Z}_p$, $Q = \mathbf{Z}_{p^{n-1}}$ $(n \geq 2,\ p$ primo). Utilizaremos la notación

$$G = \{0, 1, 2, \ldots, p^n - 1\} \qquad K = \{0, p^{n-1}, 2p^{n-1}, \ldots, (p-1)p^{n-1}\}$$
$$Q = \{0, 1, 2, \ldots, p^{n-1} - 1\}$$

como todos los grupos son abelianos, la notación será aditiva en todos los casos. El epimorfismo $\pi : G \to Q$ verifica $\pi(t) = t$ $(0 \leq t < p^{n-1})$, entonces una sección σ puede tomarse en la forma $\sigma(t) = t (0 \leq t < p^{n-1})$. Calculemos el cociclo f_σ: Sean $0 \leq t,\ j < p^{n-1}$,

$$f_\sigma(t, j) = \sigma(t) + \sigma(j) - \sigma(t + j) = t + j - \sigma(t + j). \text{ Si } t + j = k + rp^{n-1},$$

$(0 \leq k < p^{n-1})$, entonces en K, $t + j = k$, luego $\sigma(t + j) = \sigma(k) = k$, de donde $f_\sigma(t, j) = t + j - k = rp^{n-1}$. Teniendo en cuenta que $t, j < p^{n-1}$, entonces $r = 0, 1$ y en consecuencia

$$f_\sigma(t, j) = \begin{cases} 0 & \text{si } t + j < p^{n-1} \\ p^{n-1} & \text{si } t + j \geq p^{n-1}. \end{cases}$$

Sea $\theta : Q \to \mathrm{Aut}(K)$ un morfismo. Nuestro propósito es hallar todas las extensiones G que lo realizan e intentar caracterizarlas (en alguna medida) en término de los cociclos f_σ. La pregunta natural es: ¿qué es un cociclo? Nótese que la definición 3 no es satisfactoria, pues lo que se pretende es desligarnos de G. El siguiente resultado responde a la cuestión.

§ 5. 3. COCICLOS

4) Si $\theta : Q \to \mathrm{Aut}(K)$ es un morfismo y $f : Q \times Q \to K$ una aplicación, entonces f es un cociclo si, y sólo si, se satisfacen

i) $f(1,q) = f(q_1, 1) = 0 \qquad (\forall q \in Q)$

ii) $q \cdot f(q_1,q_2) - f(qq_1,q_2) + f(q,q_1q_2) - f(q,q_1) = 0$ cualesquiera que sean $q, q_1, q_2 \in Q$.

Necesario: Si f es un cociclo, existen una extensión G y una sección σ tales que se satisface 1; entonces i) es consecuencia de $\sigma(1) = 0$, en tanto que ii) resulta de la propiedad asociativa

$$[\sigma(q) + \sigma(q_1)] + \sigma(q_2) = \sigma(q) + [\sigma(q_1) + \sigma(q_2)].$$

Suficiente: Si f satisface i) y ii), se define sobre el conjunto $K \times Q$ la siguiente ley de composición:

$$(k,q) + (k_1,q_1) = (k + q \cdot k_1 + f(q,q_1), qq_1).$$

La demostración de que $K \times Q$ con dicha ley de composición es un grupo es análoga a la efectuada en el capítulo I respecto al producto semidirecto. El elemento neutro es $(0,1)$ y el inverso de (k,q) es $(-q^{-1} \cdot k - q^{-1} \cdot f(q,q^{-1}), q^{-1})$. A dicho grupo lo designamos con G_f. La demostración que G_f realiza θ también es similar a la de un ejemplo anterior respecto al producto semidirecto. Si, como antes, $\sigma : Q \to G_f$ está dada por $\sigma(q) = (0,q)$, un cálculo sencillo muestra que $\sigma(q) + \sigma(q_1) - \sigma(qq_1) = f(q,q_1)$. Los detalles quedan a cargo del lector.

Vamos a denotar con $Z^2_\theta(Q,K)$ la totalidad de cociclos $f : Q \times Q \to K$ para una *acción fija* $\theta : Q \to \mathrm{Aut}(K)$. En virtud de 4), es inmediato que $Z^2_\theta(Q,K)$ es un grupo abeliano, definiendo

$$(f + f')(q,q_1) = f(q,q_1) + f'(q,q_1).$$

Ejemplo. Sean $K = Q = \mathbf{Z}_3$. Como $\mathrm{Aut}(\mathbf{Z}_3) \simeq \mathbf{Z}_2$, el único morfismo $\theta : \mathbf{Z}_3 \to \mathrm{Aut}(\mathbf{Z}_3)$ es el trivial: $\theta(x) = \mathrm{Id} \ (\forall x \in \mathbf{Z}_3)$. Vamos a calcular $Z^2_\theta(\mathbf{Z}_3, \mathbf{Z}_3)$. Ponemos $\mathbf{Z}_3 = \{0,1,2\}$, todas las notaciones son aditivas. Por 4), un cociclo es una aplicación $f : \mathbf{Z}_3 \times \mathbf{Z}_3 \to \mathbf{Z}_3$ que satisface

i) $f(0,x) = f(y,0) = 0$, y ii) $f(y,z) - f(x+y,z) + f(x,y+z) - f(x,y) = 0$.

(Recuérdese que la acción determinada por θ es trivial).

La primera observación es que si alguno de los elementos x, y, z es 0, la condición ii) se deduce de la i). Por ejemplo, sea $y = 0$, observemos que

$$f(0,z) - f(x,z) + f(x,z) - f(x,0) = f(0,z) - f(x,0) = 0;$$

ésta es consecuencia de i). Por lo tanto, basta con asegurarnos que se cumple ii) cuando los elementos $x, y, z \in \mathbf{Z}_3$ son los tres no nulos. Se pueden presentar ocho posibilidades, y a continuación se analizan algunas de ellas.

i) Si $x = y = z = 1$, se debe cumplir

$$f(1,1) - f(2,1) + f(1,2) - f(1,1) = 0, \text{ o sea: } f(1,2) = f(2,1) \quad \text{(iii)}$$

ii) Si $x = y = 1$, $z = 2$, se debe verificar

$$f(1,2) - f(2,2) + f(1,0) - f(1,1) = 0;$$

por lo tanto, teniendo en cuenta i): $f(1,1) + f(2,2) = f(1,2)$ (iv)

Las 6 condiciones restantes son consecuencia de i), iii) y iv). Verifiquemos una de ellas, y las restantes se dejan a cargo del lector.

iii) Si $x = 2$, $y = z = 1$, debemos tener

$f(1,1) - f(0,1) + f(2,2) - f(2,1) = 0$; por i) se reduce a

$f(1,1) + f(2,2) = f(2,1)$, y por iii):

$f(1,1) + f(2,2) = f(1,2)$, la cual se verifica en virtud de iv).

En definitiva, la condición para que f sea un cociclo es que se satisfagan

i) $f(0,x) = f(y,0) = 0$ iii) $f(1,2) = f(2,1)$

iv) $f(1,1) + f(2,2) = f(1,2)$.

Entonces hay tantos cociclos f como posibles elecciones de pares de elementos $\alpha = f(1,1)$, $\beta = f(2,2)$ en $\mathbf{Z}_3$, pues, por las condiciones anteriores, los demás valores $f(x,y)$ quedan determinados a partir de estos. En consecuencia $Z^2_\theta(\mathbf{Z}_3, \mathbf{Z}_3)$ es un grupo abeliano de 9 elementos. Como, para cualquier $f \in Z^2_\theta(\mathbf{Z}_3, \mathbf{Z}_3)$, es $3f = 0$, se deduce que $Z^2_\theta(\mathbf{Z}_3, \mathbf{Z}_3) \simeq \mathbf{Z}_3 \oplus \oplus \mathbf{Z}_3$.

En todo lo que sigue queda *fijo* un morfismo $\theta : Q \to \mathrm{Aut}(K)$. Sabemos que la aplicación $G \to f_\sigma$, que asigna a cada extensión que realiza θ el
110 cociclo correspondiente a alguna sección σ, no está bien definida (distintas secciones dan lugar a distintos cociclos); la clave la da el siguiente resultado:

5) Si σ y τ son secciones de G, entonces existe una función $\varphi : Q \to K$ que verifica

i) $\varphi(1) = 0$, y ii) $(f_\sigma - f_\tau)(q_1, q_2) = q \cdot \varphi(q_2) - \varphi(q_1 q_2) + \varphi(q_1)$.

En efecto, por lo observado en 1)ii) basta tomar $\varphi(q) = \sigma(q) - \tau(q) : \varphi(q) \in K$. La condición i) resulta de $\sigma(1) = \tau(1) = 0$. La condición ii), por cálculo directo.

6) De acuerdo con esto, llamaremos *coborde* (o también 2-coborde) a toda función $\alpha : Q \times Q \to K$ para la cual existe $\varphi : Q \to K$ que satisfaga

i) $\varphi(1) = 0$, y ii) $\alpha(q_1, q_2) = q_1 \cdot \varphi(q_2) - \varphi(q_1 \cdot q_2) + \varphi(q_1)$.

Designaremos con $B^2_\theta(Q, K)$ la totalidad de coborde para la acción fija $\theta : Q \to \mathrm{Aut}(K)$. Por lo visto en 4) es fácil verificar que $B^2_\theta(Q, K) \subseteq \subset Z^2_\theta(Q, K)$ y es un subgrupo. Llamaremos *segundo grupo de cohomología* al grupo cociente

$$H^2_\theta(Q, K) = Z^2_\theta(Q, K) \Big/ B^2_\theta(Q, K).$$

Para cada cociclo $f \in Z^2_\theta(Q, K)$, designaremos con $[f]$ la clase de f en el cociente $H^2_\theta(Q, K)$. Ahora la aplicación $G \to [f_\sigma]$ está bien definida (pues, si σ y τ son secciones de G, entonces, por 5), $f_\sigma - f_\tau \in B^2_\theta(Q,K)$, es decir $[f_\sigma] = [f_\tau]$). Obsérvese además que la aplicación es suryectiva.

Ejemplo. Calculemos $B^2_\theta(\mathbf{Z}_3, \mathbf{Z}_3)$ correspondiente al ejemplo anterior. Sea $f \in Z^2_\theta(\mathbf{Z}_3, \mathbf{Z}_3)$. Entonces, $f \in B^2_\theta(\mathbf{Z}_3, \mathbf{Z}_3)$ si, y sólo si, existe $\varrho : \mathbf{Z}_3 \to \mathbf{Z}_3$ tal que

i) $\varrho(1) = 0$, y ii) $f(q_1, q_2) = \varrho(q_2) - \varrho(q_1 + q_2) + \varrho(q_1)$.

Como se sabe que f queda determinado por los valores $\alpha = f(1,1)$ y $\beta = f(2,2)$, cabe preguntar ¿qué condición deben cumplir α y β para que $f \in B^2_\theta(\mathbf{Z}_3, \mathbf{Z}_3)$?

$$f(1,1) = \varrho(1) - \varrho(2) + \varrho(1) = 2\varrho(1) - \varrho(2) \quad f(2,2) = \varrho(2) - \varrho(1) + \varrho(2) =$$
$$= 2\varrho(2) - \varrho(1) = -\varrho(2) + 2\varrho(1) = f(1,1).$$

Luego, una condición necesaria es que $f(1,1) = f(2,2)$. La condición también es suficiente: si $f \in Z^2_\theta(Q, K)$, $f(1,1) = f(2,2)$, y definimos ϱ en la forma: $\varrho(0) = 0$, $\varrho(1) = -f(1,1)$, $\varrho(2) = 0$. Es inmediato verificar ii). Resumiendo, $B^2_\theta(\mathbf{Z}_3, \mathbf{Z}_3) \simeq \mathbf{Z}_3$. En consecuencia, $H^2_\theta(\mathbf{Z}_3, \mathbf{Z}_3) \simeq \mathbf{Z}_3 \oplus \mathbf{Z}_3/\mathbf{Z}_3 \simeq$ $\simeq \mathbf{Z}_3$.

El siguiente resultado aclara la situación respecto a la aplicación $G \to [f_\sigma]$.

7) Sean G y G' extensiones de K por Q que realizan θ. Si f_σ y f'_τ son cociclos asociados a G y G', se tiene $[f_\sigma] = [f'_\tau]$ si, y sólo si, existe un isomorfismo $\beta : G \to G'$ que verifica

i) $\beta(k) = k$ para todo $k \in K$. 111

ii) $\pi'\beta = \pi$.

Necesario: Si $[f_\sigma] = [f'_\tau]$, entonces $f_\sigma - f'_\tau \in B^2_\theta(Q, K)$, y en consecuencia existe ϱ que satisface 5). Nótese que por ser $G/_K \simeq Q$, σ sección, todo elemento $x \in G$ se escribe unívocamente en la forma $x = k + \sigma(q)$ ($k \in K$, $q \in Q$). Entonces, se define $\beta : G \to G'$ así $\beta(x) = \beta(k + \sigma(q)) = k + \varrho(q) + \tau(q)$. Es fácil verificar que β es un isomorfismo y que se satisfacen i) y ii).

Suficiente: Si β es un tal isomorfismo, es inmediato que también $\beta \cdot \sigma$ es una sección de G', luego $[f'_\tau] = [f_{\beta\cdot\sigma}]$, por tanto basta con verificar que $[f_\sigma] = [f_{\beta\cdot\sigma}]$. El resultado sigue por definición de cociclo en 3).

En vista del resultado anterior definimos: Dadas dos extensiones G y G' de K por Q que realizan θ, se dice que son *equivalentes* (y escribiremos $G \sim G'$) si, y sólo si, existe un isomorfismo $\beta : G \to G'$ que satisface

i) $\beta(k) = k$ para todo $k \in K$ y ii) $\pi' \cdot \beta = \pi$.

Por 7) es claro que $\sim$ es una relación de equivalencia en el conjunto de todas las extensiones que realizan θ. Al conjunto cociente lo denotaremos por $\mathcal{E}(\theta, Q, K)$. Resumiendo estos resultados:

§5.4. EQUIVALENCIA DE EXTENSIONES

Teorema 5.4.16. Sea K un grupo abeliano, Q un grupo y $\theta : Q \to \mathrm{Aut}(K)$ un morfismo.

i) La aplicación $\mathcal{E}(\theta, Q, K) \to H^2_\theta(Q, K)$, definida por $G \to [f_\sigma]$, es una biyección.

ii) Si G es una extensión, se verifica: $G \to 0$ si, y sólo si, G es un producto semidirecto de K por Q.

iii) Toda extensión de K por Q que realiza θ es un producto semidirecto si, y sólo si, $H^2_\theta(Q, K) = 0$.

En i): Obsérvese que la buena definición y la inyectividad de la aplicación son consecuencia de 7); la suryectividad, es inmedianta. En ii): Si G es un producto semidirecto, es claro que $G \to 0$. Recíprocamente, si $G \to [f_\sigma] = 0$, como también $G' = K \times Q \to 0$, entonces $G \sim G'$; luego, por 7), G es un producto semidirecto. Por último, iii) es consecuencia de ii).

Resulta del teorema que $\mathcal{E}(\theta, Q, K)$ tiene una estructura de grupo abeliano tal que $G \to [f_\sigma]$ es un isomorfismo con $H^2_\theta(Q, K)$, y cuyo elemento neutro es la clase del producto semidirecto. Para una construcción explícita de la suma de clases, se recomienda al lector la consulta de (22). También se deduce que las extensiones equivalentes son isomorfas; lamentablemente, la recíproca no es válida.

Ejemplo. Sigamos considerando el caso $Q = K = \mathbf{Z}_3$, θ trivial. Habíamos visto que $H^2_\theta(\mathbf{Z}_3, \mathbf{Z}_3) \simeq \mathbf{Z}_3$, y en tal caso hay *tres* clases de equivalencia de extensiones. Ahora bien, las extensiones de $\mathbf{Z}_3$ por $\mathbf{Z}_3$ son

grupos de orden 9 y por tanto abelianos. Hay sólo *dos* grupos no isomorfos de orden 9: $\mathbf{Z}_9$ y $\mathbf{Z}_3 \oplus \mathbf{Z}_3$. En consecuencia, existen extensiones isomorfas y no equivalentes.

8) Sea K un grupo abeliano de orden m y Q un grupo de orden n. Si $(m, n) = 1$, entonces $H^2_\theta(Q, K) = 0$ (cualquiera que sea θ). Será suficiente verificar que $Z^2_\theta(Q, K) \subseteq B^2_\theta(Q, K)$. Sea $f \in Z^2_\theta(Q, K)$, y sea $\sigma(q) = \sum_{q_1 \in Q} f(q, q_1)$. La buena definición de $\sigma : Q \to K$ resulta de ser Q finito y K abeliano. Si se suma sobre q_2 la fórmula $q \cdot f(q_1, q_2) - f(qq_1, q_2) + f(q, q_1 q_2) = f(q, q_1)$ se obtiene $q \cdot \sigma(q_1) - \sigma(qq_1) + \sigma(q) = nf(q, q_1)$. Si $a, b \in Z$ son tales que $am + bn = 1$, entonces definimos $\varphi : Q \to K$ por $\varphi(q) = b\sigma(q)$. Luego $\varphi(1) = 0$ y $q \cdot \varphi(q_1) - \varphi(qq_1) + \varphi(q) = f(q, q_1) \therefore f \in B^2_\theta(Q, K)$.

Nota. Es posible probar un resultado más general, a saber: Si K y Q son grupos de órdenes m y n respectivamente, y si $(m, n) = 1$, entonces toda extensión G de K por Q es un producto semidirecto. Este resultado se conoce como el lema de Schur-Zassenhauss.

§ 5.5. GRUPOS DE ORDEN 12

Ejemplo. Veamos cómo puede probarse que hay exactamente 5 grupos no isomorfos de orden 12. En principio, observemos que todo grupo de orden 12 posee algún subgrupo de Sylow invariante, pues si $n_3 \neq 1$, entonces $n_3 = 4$ y los $12 - 2 \cdot 4 = 4$ elementos restantes sólo pueden formar un 2-subgrupo de Sylow ($\therefore$ invariante). En consecuencia, todo grupo de orden 12 es una extensión de un grupo de orden 3 y otro de orden 4, o viceversa. Como $(3, 4) = 1$, toda tal extensión es un producto semidirecto, y se tienen las posibilidades:

i) $K = Z_3$, $Q = Z_4$, por tanto $\mathrm{Aut}(K) \simeq Z_2$.

ii) $K = Z_3$, $Q = Z_2 \oplus Z_2$, luego $\mathrm{Aut}(K) \simeq Z_2$.

iii) $K = Z_4$, $Q = Z_3$, entonces $\mathrm{Aut}(K) \simeq Z_2$.

iv) $K = Z_2 \oplus Z_2$, $Q = Z_4$, en consecuencia $\mathrm{Aut}(K) \simeq S_3$.

Caso i): Como $\mathrm{Aut}(Z_3) \simeq Z_2$, sólo hay dos morfismos posibles $\theta_1 : Z_4 \to \mathrm{Aut}(Z_3)$, determinados por $\theta_1(1) = \mathrm{Id}$ y $\theta_2(1) = f$ (con $f(x) = 2x$). Los grupos de orden 12 asociados:

$$G_1 = Z_3 \oplus Z_4 = Z_3 x_{\theta_1} Z_4; \qquad G_2 = Z_3 x_{\theta_2} Z_4$$

no son isomorfos, pues el primero es abeliano y el segundo no.

Caso ii): Hay exactamente cuatro morfismos distintos $\gamma_i : Z_2 \oplus Z_2 \to \mathrm{Aut}(Z_3)$, estos son:

	(0 0)	(0, 1)	(1 0)	(1, 1)
γ_1	Id	Id	Id	Id
γ_2	Id	Id	f	f
γ_3	Id	f	Id	f
γ_4	Id	f	f	Id

El primo de ellos es trivial y corresponde al grupo $G_3 = Z_3 \oplus (Z_2 \oplus Z_2)$. Los tres restantes son isomorfos entre sí: obsérvese que cualesquiera que sean i, j $2 \le i$, $j \le 4$ siempre existe un isomorfismo

$$\gamma_{ij} : Z_2 \oplus Z_2 \to Z_2 \oplus Z_2$$

tal que $\gamma_i \cdot \gamma_{ij} = \gamma_j$, y de acuerdo con lo visto en el capítulo I se concluye que los productos semidirectos asociados son grupos isomorfos. En consecuencia

$$G_4 = Z_3 x_{\gamma_1} (Z_2 \oplus Z_2).$$

Los grupos G_3 y G_4 no son isomorfos entre sí (pues G_3 es abeliano) ni tampoco lo son a G_1 ó G_2 por la estructura de los 2-subgrupos de Sylow.

Caso iii): El único morfismo $\theta : Z_3 \to \mathrm{Aut}(Z_4)$ es el trivial, el grupo asociado es $Z_4 \oplus Z_3$, y por tanto, isomorfo a G_1.

Caso iv): En este caso, los posibles morfismos $\delta_i : Z_3 \to \mathrm{Aut}(Z_2 \oplus Z_2) \simeq S_3$ son tres

$$\delta_1(1) = \mathrm{Id}, \qquad \delta_2(1) = (123), \qquad \delta_3(1) = (132).$$

El grupo asociado a δ_1 es $(Z_2 \oplus Z_2) \oplus Z_3$ isomorfo a G_3, los otros dos son isomorfos entre sí (razonamiento análogo al del caso ii)) y dan lugar al grupo

$$G_5 = (Z_2 \oplus Z_2) x_{\delta_2} Z_3.$$

Este grupo no es isomorfo a G_3, pues éste es abeliano; ni a G_1 ó G_2, por la estructura de los 2-subgrupos de Sylow; ni a G_4, pues éste posee 3-subgrupos de Sylow invariantes y resultaría G_5 abeliano. En consecuencia,

todo grupo de orden 12 es isomorfo a uno, y sólo uno, de los grupos $G_i (1 \leq i \leq 5)$.

1. Por ejemplo, $A_4 \simeq G_5$. En efecto, el subgrupo $[A_4, A_4]$ es invariante e isomorfo a $\mathbf{Z}_2 \oplus \mathbf{Z}_2$, entonces A_4 corresponde al caso iv), y como A_4 no es abeliano, $A_4 \not\simeq G_3$, entonces $A_4 \simeq G_5$.

2. El grupo diédrico D_6 es isomorfo a G_4. Si $D_6 = \langle a, b / a^6 = b^2 = (ab)^2 = 1 \rangle$, el subgrupo $K = \langle a^3 \rangle \simeq \mathbf{Z}_2$, y el cociente $D_6 / \langle a^3 \rangle \simeq \mathbf{Z}_2 \oplus \mathbf{Z}_2$, entonces D_6 corresponde al caso ii). No puede ser $D_6 \simeq G_3$ pues no es abeliano, entonces $D_6 \simeq G_4$.

Un resultado clásico caracteriza los grupos de orden p^2q (p, q primos distintos) en términos de generadores y relaciones. Para más información, consúltese la cita (1).

APÉNDICE 1. UNIDADES DE Z_n

Vamos a calcular el grupo de unidades del anillo $\mathbf{Z}_n$, que denotaremos por $\mathbf{U}(n)$. Observemos primeramente que si $\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$, entonces para $0 \leq i < n$: $i \in \mathbf{U}(n)$ si, y sólo si, $(\exists j)$, tal que $ji \equiv 1(n)$ si, y sólo si, $(\exists j)$, $(\exists k)$, tal que $ji - 1 = nk$ si, y sólo si, $(\exists j)(\exists k)$, tal que $1 = ji + (-k)n$ si, y sólo si, $(i, n) = 1$. Si $\phi : \mathbf{N} \to \mathbf{N}$ denota la función de Euler, es decir, $\phi(n) =$ número de enteros i, tales que $1 \leq i < n$, $(i, n) = 1$, entonces por lo anterior resulta que

$$|\mathbf{U}(n)| = \phi(n).$$

Recordemos, además, que ϕ es multiplicativa, es decir

$$(n, m) = 1 \Rightarrow \phi(nm) = \phi(n)\phi(m)$$

y que si p es primo, $n \geq 1$, entonces

$$\phi(p^n) = p^{n-1}(p-1) \qquad \text{(cf (12))}.$$

Demostraremos los siguientes resultados básicos:

1) si p es primo impar, $\mathbf{U}(p^n)$ es cíclico.

2) $\mathbf{U}(2)$ y $\mathbf{U}(4)$ son cíclicos y si $n \geq 3$, entonces $\mathbf{U}(2^n)$ es producto directo de un cíclico de orden 2 y otro de orden 2^{n-2}.

Consideremos 1). Sabemos que $\mathbf{U}(p^n)$ es un grupo abeliano de orden $p^{n-1}(p-1)$, luego será producto directo de los subgrupos de órdenes coprimos

$$\mathbf{H} = \{x \in \mathbf{U}(p^n) / x^{p^{n-1}} = 1\}$$

$$\mathbf{K} = \{x \in \mathbf{U}(p^n) / x^{p-1} = 1\}$$

$$(|\mathbf{H}| = p^{n-1},\ |\mathbf{K}| = p-1).$$

Para demostrar 1), basta con verificar que tanto H como K son cíclicos. Ante todo adviértase que todo elemento $x \in \mathbf{Z}_{p^n}$ $(0 \leq x < p^n)$ se escribe unívocamente en la forma $x = pk + r$ $(0 \leq r < p)$ $(0 \leq k < p^{n-1})$, y en consecuencia

$$x \in \mathbf{U}(p^n) \text{ si, y sólo si, } x = pk + r\ (0 < r < p)\ (0 \leq k < p^{n-1}) \qquad (*)$$

1) Demostraremos que H es cíclico. Como H es un grupo abeliano de orden p^{n-1}, entonces (cf. (12)) es la suma directa de grupos cíclicos de órdenes p^{n_i} $(1 \leq n_i < n)$. En tal caso, basta con demostrar que H posee exactamente $p-1$ elementos de orden p (en $\mathbf{Z}_{p^{n_1}} \oplus \mathbf{Z}_{p^{n_2}} \oplus \ldots \mathbf{Z}_{p^{n_r}}$ hay $p^r - 1$ tales elementos). Sea $x = pk + r$ $(0 < r < p)$ $(0 \leq k < p^{n-1})$ un elemento de orden p, por lo tanto

$$x^p = (pk + r)^p \equiv 1(p^n) \quad \text{es decir}$$

$$\sum_{0\le i\le p} \binom{p}{i}(pk)^i r^{p-i} \equiv 1(p^n) \quad \text{esto es}$$

$$r^p + \sum_{0\le i\le p} \binom{p}{i}(pk)^i r^{p-i} \equiv 1(p^2) \qquad (**)$$

como $n \ge 1$, la misma congruencia es válida con respecto al módulo p, es decir

$$r^p \equiv r^p + p \sum_{0\le i\le p} \binom{p}{i} p^{i-1} k^i r^{p-i} \equiv 1(p)$$

Pero, por el teorema de Fermat, (cf. (12)) se tiene $r^p \equiv r(p)$, y consecuentemente, $r \equiv 1(p)$; es decir $r = 1$.

Reemplazando en (**)

$$\sum_{0\le i\le p} \binom{p}{i}(pk)^i \equiv 0(p^n).$$

Pero, se tiene

$$\sum_{0\le i\le p} \binom{p}{i}(pk)^i = \binom{p}{1}pk + \binom{p}{2}(pk)^2 + \binom{p}{3}(pk)^3 + \ldots + \binom{p}{p}(pk)^p =$$

$$= p^2k + p^3k^2\frac{p-1}{2!} + p^4k^3\frac{(p-2)(p-1)}{3!} + \ldots + p^pk^p = p^2k + p^3ks \quad (s \in Z).$$

Entonces

$$p^2k + p^3ks \equiv 0(p^n).$$

Los casos $n = 1$, 2 no tienen interés, pues corresponden a la situación $H = 1$, $H \simeq Z_p$. Para $n = 3$, la ecuación implica p/k. Supongamos, por hipótesis inductiva, que cada vez que $2 \le t \le n$ y sea

$$p^2k + p^3ks \equiv 0(p^t)$$

se tenga p^{t-2}/k. Entonces, si $p^2k + p^3ks \equiv 0(p^n)$, se tiene $p^2k + p^3ks \equiv 0\ (p^{n-1})$, por lo tanto $p^{n-1-2} = p^{n-3}/k$, $k = p^{n-3}t$, y volviendo a la ecuación original $p^2p^{n-3}t + p^3p^{n-3}ts = p^{n-1}t + p^nts \equiv 0(p^n) \therefore p/t$, es decir p^{n-2}/k. En efecto, se probó que los elementos de orden p (y el elemento trivial) son los de la forma (*) con $r = 1$ y p^{n-2}/k, es decir

$$x = p^{n-1}t + 1 \quad 0 \le t < p.$$

Para $t = 0$ es $x = 1$, entonces los $p - 1$ elementos restantes son los únicos de orden p en H (y por tanto en $U(p^n)$).

ii) Veamos ahora que K es cíclico. El resultado es claro si $n = 1$, pues en este caso $K = U(p) = \mathbf{Z}_p^*$ el grupo multiplicativo de un cuerpo finito, y en consecuencia, es cíclico (cf. (12)). En el caso general ($n \ge 1$), observe el lector que la aplicación $\phi : \mathbf{Z}_{p^n} \to \mathbf{Z}_p$ dada por $\phi(x) = x^{p^{n-1}}$, es un epimorfismo de anillos: en consecuencia, $\phi(U(p^n)) = U(p)$, y por lo tanto, si $a \in U(p)$ es un generador y si $b \in U(p^n)$ es tal que $\phi(b) = a$, entonces $p - 1 = |a|$ divide $|b|$, es decir $|b| = t(p - 1)$, y así el elemento b^t tiene orden $p - 1$: es un generador de K. Por lo tanto, queda demostrado 1).

Consideremos 2). Lo afirmado sobre $U(2)$ y $U(4)$ es inmediato: $U(2) = 1$, $U(4) \simeq Z_2$. Sea, entonces, $n \geq 3$. Para probar 2) basta con establecer los siguientes hechos:

i) $U(2^n)$ posee exactamente 3 elementos de orden 2; con lo cual quedará probado que $U(2^n)$ es producto directo de 2 grupos cíclicos.

ii) $U(2^n)$ siempre tiene elementos de orden 2^{n-2}; esto asegurará que uno de los factores es isomorfo a $Z_{2^{n-2}}$ y el otro a Z_2.

Demostremos i). Como antes, los elementos $x \in U(2^n)$ son los de la forma

$$x = 2k + 1 \qquad 0 \leq k < 2^{n-1} \tag{*}$$

Entonces, $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv 1(2^n)$ si, y sólo si

$$4k(k+1) \equiv 0(2^n) \text{ si, y sólo si,}$$

$$k(k+1) \equiv 0(2^{n-2})$$

por tanto $2^{n-2}/k(k+1)$ y tenemos dos posibilidades: o bien $2^{n-2}/k$, lo cual por (*) implica $k = 0$ ó $k = 2^{n-2}$ o bien $2^{n-2}/k+1$, y por la misma razón que antes es $k = -1$, $2^{n-2} - 1$ y $2^n - 1$. Es decir, los únicos elementos de orden 2 son $2^{n-1} + 1$, $2^n - 1$ y $2^{n-1} - 1$, los cuales son distintos si $n \geq 3$.

ii) Su demostración implica que siempre

$$5^{2^{n-3}} \not\equiv 1(2^n)$$

lo cual probará que 5 tiene orden mayor o igual a 2^{n-2}, y de ahí seguirá lo propuesto. Si $n = 3$, entonces se tiene $5^{2^0} = 5 \not\equiv 1(2^3)$ pero, en cambio, $5 \equiv 1(2^{3-1})$. Sea, para cada $m \geq 3$, $k(m)$ el mayor entero que verifica

$$5^{2^{m-3}} \equiv 1(2^{k(m)}).$$

Acabamos de probar que $k(3) = 2$. Si $n \geq 3$, existe $r > 0$, tal que $5^{2^{n-3}} \equiv 1 + r2^{k(n)}$ (donde, por maximalidad de $k(m)$, debe ser r impar). Elevando al cuadrado, obtenemos

$$1 + r2^{k(n)+1} + r^2 2^{2k(n)} = (1 + r2^{k(n)})^2 = (5^{2^{n-3}})^2 = 5^{2^{(n+1-3)}}$$

(lo cual prueba que $k(n+1) \geq k(n) \geq 2$). Entonces $1 + t\,2^{k(n)+1} = 5^{2^{(n+1-3)}}$ ($t = r + r^2 2^{k(n)-1}$ es impar, pues r lo es). Pero de ello es claro que $k(n+1) = k(n) + 1$, que sumado al hecho de ser $k(3) = 2$, nos indica $k(n) = n - 1 (n \geq 3)$, y por definición de $k(n)$ se tiene

$$5^{2^{n-3}} \not\equiv 1(2^n) \qquad (n \geq 3).$$

Esto completa la demostración de 2). En general, si $n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}$, se tiene que la aplicación

$$\phi : Z_n \to Z_{p_1^{i_1}} \oplus Z_{p_2^{i_2}} \oplus \ldots \oplus Z_{p_k^{i_k}}$$

$\phi(1) = (1, 1, \ldots, 1)$ es un isomorfismo de anillos (donde 1 indica, en cada caso, el generador canónico). Por lo tanto $U(n) \simeq U(p_{i1}^{i1}) \oplus \ldots \oplus U(p_k^{i_k})$; luego lo demostrado en 1) y 2) resuelve la situación general.

Por ejemplo, $U(2^5 3^3 7^2) \simeq U(2^5) \oplus U(3^3) \oplus U(7^2) \simeq Z_2 \oplus Z_{2^3} \oplus Z_{3^2(3-1)} \oplus Z_{7(7-1)} \simeq Z_2 \oplus Z_{2^3} \oplus Z_{3^2} \oplus Z_2 \oplus Z_7 \oplus Z_6 \simeq (Z_{2^3} \oplus Z_{3^2} \oplus Z_7) \oplus (Z_2 \oplus Z_3) \oplus Z_2 \oplus$

$\oplus \mathbf{Z}_2 \simeq \mathbf{Z}_{504} \oplus \mathbf{Z}_6 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$. Por último, hacemos notar que $\mathrm{Aut}(\mathbf{Z}_n) \simeq U(n)$. Se deja como ejercicio para el lector verificar que $\phi: \mathrm{Aut}(\mathbf{Z}_n) \to \mathbf{Z}_n$. $\phi(f) = f(1)$ es un monomorfismo cuya imagen es $U(n)$.

APÉNDICE II. GRUPO DE AUTOMORFISMOS DE S_n

Teorema. Si $n \geq 3$, $n \neq 6$, entonces $\mathrm{Aut}(\mathbf{S}_n) \simeq \mathbf{S}_n$.

Demostración. Sea σ un automorfismo de $\mathbf{S}_n$.

1. Sea $x \in \mathbf{S}_n$ cualquier 3-ciclo y se afirma que $y = \sigma(x)$ debe ser el producto de 3-ciclos disjuntos. En efecto, si se considera a $\sigma(x) = y$ descompuesto como producto de ciclos disjuntos y puesto que debe ser orden x = orden $\sigma(x) = 3$, todos los ciclos no triviales deben ser necesariamente 3-ciclos. Supongamos, entonces, que $\sigma(x) = y$ es el producto de $r (r \geq 1)$ 3-ciclos disjuntos, no triviales.

2. Si designamos con $\bar{x}$ la totalidad de conjugados de x, es decir, la totalidad de 3-ciclos en $\mathbf{S}_n$, y con $\bar{y}$ la totalidad de conjugados de y, o sea la totalidad de productos de r, 3-ciclos disjuntos; entonces, el automorfismo σ aplica $\bar{x}$ en $\bar{y}$ biyectivamente. En efecto

i) Si $z \in \bar{x}$, entonces $z = txt^{-1}$, por tanto

$$\sigma(z) = \sigma(t)\sigma(x)\sigma(t^{-1}) = \sigma(t)\sigma(x)\sigma(t)^{-1} = \sigma(t)y\,\sigma(t)^{-1} \in \bar{y}.$$

Por lo tanto, σ aplica $\bar{x}$ en $\bar{y}$.

ii) σ aplica inyectivamente $\bar{x}$ en $\bar{y}$, pues σ es un automorfismo y, por tanto, es una aplicación inyectiva.

iii) Si $w \in \bar{y}$, existe v con v y $v^{-1} = w$, y por tanto $\sigma^{-1}(w) = \sigma^{-1}(v)\sigma^{-1}(y)\sigma^{-1}(v)^{-1} = (\sigma^{-1}(v))x(\sigma^{-1}(v))^{-1} \in \bar{x}$.

Luego, σ aplica $\bar{x}$ biyectivamente en $\bar{y}$, como se quería probar. En consecuencia, $|\bar{x}| = |\bar{y}|$, pero sabemos que

$$|\bar{x}| = \frac{n!}{3(n-3)!} = 2\binom{n}{3}$$

$$|\bar{y}| = \frac{n!}{3^r r!(n-3r)!}$$

de donde

$$2\frac{n!}{3!(n-3)!} = \frac{n!}{r!(n-3r)!3^r}$$

o equivalentemente

$$\frac{1}{(n-3)!} = \frac{1}{(n-3r)!\,r!\,3^{r-1}}$$

o sea

$$r!\,3^{r-1} = \frac{(n-3)!}{(n-3r)!}. \qquad (*)$$

Calculemos las soluciones, o sea los posibles valores r, n, que satisfacen (*):

i) Si $r = 1$, se reduce a

$$1 \cdot 1 = \frac{(n-3)!}{(n-3)!}$$

identidad válida cualquiera que sea n.

ii) Si $r = 2$, tenemos

$$2 \cdot 3 = \frac{(n-3)!}{(n-6)!} = (n-5)(n-4)(n-3) \qquad (**)$$

y puesto que *en este caso* $n \geq 6$, y dado que el miembro derecho de (**) es el producto de tres factores consecutivos, se deduce que $n = 6$, caso que hemos excluido de la hipótesis.

iii) Sea, por último, $r \geq 3$. Se afirma que en este caso (*) no posee solución. En efecto, (*) equivale a decir

$$\frac{r!\,3^{r-1}}{(3(r-1))!} = \frac{(n-3)!}{(n-3r)!\,(3(r-1))!} = \binom{n-3}{3(r-1)}. \qquad (***)$$

Ahora bien, el miembro derecho de (***) es siempre un número entero; veamos que el miembro izquierdo no lo es. Como $r \geq 3$, entonces $3(r-1)-r = 2r-3 \geq 3 > 2$, por tanto

$$\frac{r!\,3^{r-1}}{(3(r-1))!} = \frac{3^{r-1}}{A[3(r-1)-1][3(r-1)]}$$

donde eventualmente $A = 1$. Si ahora observamos que alguno de los números $3(r-1)-1$, $3(r-1)$ debe ser par, ese factor nunca podrá cancelarse con alguno del numerador.

3. Resumiendo, la única solución posible en (*) es, en nuestro caso, $r = 1$, n cualquiera.

4. En consecuencia, se ha probado que si σ es un automorfismo y x es un 3-ciclo, entonces $\sigma(x) = y$ también es un 3-ciclo.

5. Afirmamos que existen $\alpha, \beta, \gamma_3 \ldots \gamma_n \in X$ todos distintos, tales que

$$\sigma(1\ 2\ t) = (\alpha\ \beta\ \gamma_t) \qquad (3 \leq t \leq n).$$

En efecto, sea $\sigma(1\ 2\ 3) = (\alpha\ \beta\ \gamma)$

$$\sigma(1\ 2\ t) = (\alpha'\ \beta'\ \gamma') \qquad (t > 3)$$

se tiene

$$(1\ 2\ 3)(1\ 2\ t) = (1\ 3)(2\ t)$$

por tanto, $(1\ 2\ 3)(1\ 2\ t)$ tiene orden 2. Consecuentemente $\sigma((1\ 2\ 3)(1\ 2\ t)) = \sigma(1\ 2\ 3)\sigma(1\ 2\ t) = (\alpha\ \beta\ \gamma)(\alpha'\ \beta'\ \gamma')$ tiene que tener también orden 2. Se pueden presentar los siguientes casos:

a) Si $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ son todos distintos, el orden del elemento en cuestión es 3 y no 2. Esto no es posible.

b) Entre $\{\alpha, \beta, \gamma\}$ y $\{\alpha', \beta', \gamma'\}$ hay un sólo elemento en común. Cabe suponer, sin pérdida de generalidad, que $\alpha = \alpha'$; luego $(\alpha\ \beta\ \gamma)(\alpha\ \beta'\ \gamma') =$

$= (\alpha\ \beta'\ \gamma'\ \beta\ \gamma)$ no tiene orden 2. También este caso es imposible.

c) Entre $\{\alpha, \beta, \gamma\}$ y $\{\alpha', \beta', \gamma'\}$ hay dos elementos comunes. Como antes, no hay pérdida de generalidad en suponer que $\alpha = \alpha'$ es uno de ellos, combinado con alguna de las posibilidades: $\beta = \gamma'$, o bien $\beta = \beta'$. En el caso $\beta = \gamma'$, se tiene $(\alpha\beta\gamma)(\alpha\beta'\gamma) = (\alpha\beta'\gamma)$ que tiene orden 3 y que, por tanto, tampoco es posible. En el caso $\beta = \beta'$ $(\alpha\beta\gamma)(\alpha'\beta\gamma') = (\alpha\gamma)(\beta\gamma')$ que tiene orden 2, y *por tanto, sí es posible.*

d) Por último, quedaría sólo por considerar el caso $[\alpha\beta\gamma] = [\alpha'\beta'\gamma']$. Todo se reduce, como siempre, a considerar los casos $(\alpha\beta\gamma) = (\alpha'\beta'\gamma')$, o bien $(\alpha\beta\gamma)^2 = (\alpha'\beta'\gamma')$. En el primero $(\alpha\beta\gamma)(\alpha\beta\gamma) = (\alpha\gamma\beta)$ que tiene orden 3, y no es posible. En el segundo $(\alpha\beta\gamma)(\alpha\beta\gamma)^2 = 1$ no tiene orden 2, y tampoco es posible.

Resumiendo, el único caso admisible es

$$\alpha = \alpha' \qquad \beta = \beta'$$

de donde $\sigma(1\ 2\ t) = (\alpha\beta\gamma_t)$, con $\gamma_t \in X$ $(3 \leq t \leq n)$; α y β *fijos e independientes de* t.

Sea t el elemento de $\mathfrak{S}_n$, que satisface

$$\begin{cases} t(1) = \alpha \\ t(2) = \beta \\ t(i) = \gamma_i \quad (3 \leq i < n) \end{cases} \qquad (****)$$

ya estamos en condiciones de probar que

$$\sigma(1\ 2\ i) = t(1\ 2\ i)t^{-1}.$$

En efecto

$$\sigma(1\ 2\ i) = (\alpha\beta\gamma_i) = (t(1)t(2)t(i)) = t(1\ 2\ i)t^{-1}.$$

Sea $x \in \mathbf{A}_n$ cualquiera. Por el corolario a la proposición 3.4.19, x se escribe como producto de 3-ciclos de la forma $(1\ 2\ i)$. Supongamos que $x = s_1 s_2 \dots s_r$, con los s_i de la forma indicada, por lo tanto

$$\sigma(x) = \sigma(s_1 s_2 \dots s_r) = \sigma(s_1)\sigma(s_2) \dots \sigma(s_r) = ts_1t^{-1}ts_2t^{-1} \dots$$
$$\dots ts_rt^{-1} = ts_1s_2 \dots s_rt^{-1} = txt^{-1}.$$

6. Entonces, hemos probado que cualquiera que sea $x \in \mathbf{A}_n$, se tiene

$$\sigma(x) = txt^{-1}$$

donde $t \in \mathfrak{S}_n$ está definido en (****).

7. Afirmamos que si probamos que $\sigma(12) = t(12)t^{-1}$, luego cualquiera que sea $x \in \mathfrak{S}_n$, se tiene $\sigma(x) = txt^{-1}$. En efecto, el índice de $\mathbf{A}_n$ en $\mathfrak{S}_n$ es 2, $(1\ 2) \notin \mathbf{A}_n$, por lo tanto $\mathfrak{S}_n = \mathbf{A}_n \cup (1\ 2)\mathbf{A}_n$. Ahora, si $x \in \mathbf{A}_n$, ya sabemos que el resultado es válido, sino $x \in (1\ 2)\mathbf{A}_n$, y por lo tanto $x = (1\ 2)y$, con $y \in \mathbf{A}_n$. Así

$$\sigma(x) = \sigma(12)\sigma(y) = t(12)t^{-1}tyt^{-1} = t(12)yt^{-1} = txt^{-1};$$

tal como se propuso.

8. Probemos, entonces, que $\sigma(1\,2) = t(1\,2)t^{-1}$. Sea P el elemento de $\mathbf{S}_n$.

$P = t^{-1}\sigma(1\,2)t$, se tiene (*****)

$$P^2 = t^{-1}\sigma(1\,2)tt^{-1}\sigma(1\,2)t = t^{-1}\sigma(1\,2)\sigma(1\,2)t =$$
$$= t^{-1}\sigma[(1\,2)(1\,2)]t = t^{-1}\sigma(1)t = t^{-1}t = 1.$$

De ello se deduce que $P = P^{-1}$.

Sea Z cualquier permutación par, es decir $Z \in \mathbf{A}_n$, es válido que

$$PZP^{-1} = PZP = t^{-1}\sigma(1\,2)tZt^{-1}\sigma(1\,2)t = t^{-1}\sigma(1\,2)\sigma(Z)\sigma(1\,2)\cdot t =$$
$$= t^{-1}\sigma((1\,2)z(1\,2))t = (1\,2)Z(1\,2), \text{ por ser}$$

$(1\,2)Z(1\,2) \in \mathbf{A}_n$. Ahora bien, suponiendo que $P(j) = P_j$, se deduce de lo anterior, tomando $Z = (1\,2\,t)$, que $P(1\,2\,t)P^{-1} = (1\,2)(1\,2\,t)(1\,2)$, o sea $(P_1\,P_2\,P_t) = (2\,1\,t)$, es decir

$$P_1 = 2 \qquad P_2 = 1 \qquad P_t = t \qquad (\text{Si } t \geq 3)$$

o, equivalentemente, $P = (1\,2)$. Volviendo a la definición de P en (*****), resulta $(1\,2) = t^{-1}\sigma(1\,2)t$, o equivalentemente $\sigma(1\,2) = t(1\,2)t^{-1}$, lo cual prueba lo propuesto y así el teorema. ▲

Corolario. Si $n \geq 4$, $n \neq 6$, entonces $\mathrm{Aut}(\mathbf{A}_n) \simeq \mathbf{S}_n$.

Demostración. La aplicación $\mathbf{S}_n \xrightarrow{\Phi} \mathrm{Aut}(\mathbf{A}_n)$, $\Phi(t)(s) = tst^{-1}$ es un homomorfismo. Demostremos que es un monomorfismo. Si $x \in \mathrm{Nu}\,\Phi$, entonces $xsx^{-1} = s$, es decir $xs = sx$ para todo $s \in \mathbf{A}_n$. Si el lector se remite a lo demostrado en la proposición 3.5.20, observará que lo anterior es sólo posible en el caso

$$x = (x_1\,x_2)$$

(todo lo dicho en esa proposición, parte ii), continúa siendo válido, si bien en c) queda por considerar el caso de longitud 2). Pero, si $x_3 \neq x_1$, $x_3 \neq x_2$, entonces

$$(x_1\,x_2)(x_1\,x_2\,x_3) = (x_2\,x_3) \neq (x_1\,x_3) = (x_1\,x_2\,x_3)(x_1\,x_2).$$

En consecuencia, Φ es un monomorfismo. Por último, Φ es un epimorfirmos, ya que todo lo expuesto en el teorema hasta el punto 6 continúa siendo válido. ▲

Nota. 1. Cuando $n = 6$, se tiene $\mathrm{Aut}(\mathbf{S}_6)/\mathrm{Int}(\mathbf{S}_6) \simeq \mathbf{Z}_2$; es decir, existen automorfismos que no son interiores. La demostración del teorema da una idea de cómo tienen que ser los automorfismos no interiores de $\mathbf{S}_6$. Para una construcción explícita de un automorfismo no interior, refiérase el lector a (1).

EJERCICIOS

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 1.

Ejercicio 1. Probar que las siguientes matrices forman grupo con el producto usual de matrices.

$$\begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \quad \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix}, \quad \begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix}, \quad \begin{Vmatrix} -1 & 0 \\ 0 & 1 \end{Vmatrix}$$

¿Es dicho grupo cíclico?

Ejercicio 2. Probar que todo subgrupo propio del grupo cuaterniónico H_2 es cíclico e invariante. ¿Cuántos elementos de orden 2 posee H_2?; ¿y de orden 4? Verificar que H_2 es isomorfo al grupo $G = \{1, -1, i, -i, j, -j, k, -k\}$, cuya ley de composición está dada por:

$$\begin{aligned} 1x &= x = x1 \qquad (\forall x) \\ (-1)x &= -x = x(-1) \qquad (\forall x) \\ x^2 &= -1,\ x(-x) = 1 \qquad (\forall x \neq \pm 1) \\ ij &= k,\ jk = i,\ ki = j \\ xy &= (-y)x = y(-x) = -yx \qquad (\forall x \neq \pm 1)\ (\forall y \neq \pm 1). \end{aligned}$$

Probar que H_2 no es isomorfo a D_4. ¿Es invariante todo subgrupo de D_4? Hallar $z(D_4)$. ¿Puede describir $z(D_n)$?

Ejercicio 3. Si H_1 y H_2 son subgrupos *propios* de G, entonces $H_1 \cup H_2 \neq G$. ¿Es válido lo mismo para tres subgrupos propios?

Ejercicio 4. Dar contraejemplos a la siguiente afirmación: "Si H y K son subgrupos de G, entonces HK es un subgrupo de G". Probar que HK es un subgrupo si, y sólo si, HK = KH.

Ejercicio 5. Si A, B y C son subgrupos de un grupo G, $A \subseteq B$

a) Probar que $AC \cap B = A(C \cap B)$.

b) Si, además, $A \cap C = B \cap C$ y $AC = BC$, entonces $A = B$.

Ejercicio 6. Definir epimorfismos:

$$f: D_{2n} \to D_n \qquad g: D_{2n} \to Z_2.$$

Ejercicio 7. Si H_1 y H_2 son subgrupos invariantes de G, existe un monomorfismo natural:

$$f: G/_{H_1 \cap H_2} \to G/_{H_1} \times G/_{H_2}.$$

Ejercicio 8. Sean $G_i (i = 1, 2)$ grupos y $H_1 \subseteq G_i$ subgrupos invariantes, tales que

$$\text{i) } H_1 \simeq H_2 \qquad \text{ii) } G_1/_{H_1} \simeq G_2/_{H_2}$$

¿Es necesariamente válido que en esta situación sea $G_1 \simeq G_2$?

Ejercicio 9. Sea H un subgrupo de G tal que $G = H \cdot z(G)$. Probar que H es invariante.

Ejercicio 10. Si $G/_{z(G)}$ es cíclico, entonces G es abeliano.

Ejercicio 11. Sea G un grupo, $n \geq 2$, $x \in G$, tal que es el único elemento de orden n en G.

Probar que $n = 2$ y que $x \in z(G)$.

Ejercicio 12. Sea S y T subconjuntos de un grupo G:

a) C(S, G) es un subgrupo.

b) $S \subseteq T$, entonces $C(T, G) \subseteq C(S, G)$.

c) $S \subseteq C(C(S, G), G)$.

d) Hallar $C(x, D_4)$ para todo $x \in D_4$.

Ejercicio 13. Sea G un grupo y S un subconjunto de G.

a) N(S, G) es un subgrupo.

b) $N(x, G) = C(x, G)$.

c) Si H es un subgrupo, $H \subseteq N(H, G)$ y, además, es invariante.

Ejercicio 14. Determinar, en cada caso, el orden del grupo generado por los elementos a y b que satisfacen:

i) $a^n = b^n = (ab)^2 = 1$

ii) $a^3 = b^2 = (ab)^3 = 1$

iii) $a^2 = b^2 = 1$, $(bab^{-1})^3 = 1$.

Ejercicio 15. Construir grupos *no abelianos* de órdenes:

a) p^3 (p primo impar), con elementos de orden p^2.

b) 44 con elementos de orden 4.

c) 20.

Ejercicio 16. Si G es un grupo, $G_{/[G, G]}$ es abeliano. Si N es invariante en G y si $G/_N$ es abeliano $[GG] \subseteq N$.

Ejercicio 17. Sea G el grupo generado por los elementos x e y que satisfacen:

$$x^2 = 1 \qquad xyx^{-1}y = 1.$$

Probar que G es el producto semidirecto de subgrupos *propios*.

Ejercicio 18. Calcular [G, G] para los grupos hallados en el ejercicio 15. Probar que si N es un subgrupo invariante de G, tal que $[G, G] \cap N = 1$, entonces $N \subseteq z(G)$.

Ejercicio 19. Sea G un grupo abeliano finito, tal que la aplicación $x \to x^2$ es un automorfismo de G. Probar que el orden de G es impar.

Ejercicio 20. En un grupo G se define la siguiente relación: $x \sim y$ si, y sólo si, existe $f \in \mathrm{Aut}(G)$ tal que $f(x) = y$.

a) Probar que $\sim$ es una relación de equivalencia.

b) Si $x \sim y$, entonces $|x| = |y|$. ¿Vale la recíproca?

Ejercicio 21. Hallar Aut(G) para cada uno de los grupos.

a) Z_{37}

b) $Z_{11} \oplus Z_2 \oplus Z_3$

c) $Z_3 \oplus Z_4$.

Ejercicio 22. Verificar que la aplicación $Z_{p^n} \to Z_p$ dada por $x \to x^{p^{n-1}}$ es un epimorfismo de anillos.

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 2

Ejercicio 23. Sea, en cada uno de los siguientes casos, Aut(G) que opera sobre G en la forma usual. Hallar la órbita y estabilizadores para los grupos:

i) Z_9 iii) $Z_4 \oplus Z_2$

ii) Z_{21} iv) $Z_2 \oplus Z_2 \oplus Z_2$

Ejercicio 24. Sea G el grupo de rotaciones (en el espacio) del rectángulo. Probar que G opera 1-transitivamente.

Ejercicio 25. Sea G un grupo que opera sobre un conjunto X, $|X| = n$.

a) G es transitivo si, y sólo si, $|G : G_x| = n \qquad (\forall x \in X)$.

b) Sea $2 \leq k \leq n$; entonces G es k-transitivo si, y sólo si

i) G es transitivo

ii) G_x opera $(k-1)$-transitivamente sobre el conjunto $X - \{x\}$.

Ejercicio 26. Sea G un grupo finito que opera sobre X. Sea, para cada $g \in G$, $\hat{g}$ = número de elementos de X fijos por g. Si G opera transitivamente, entonces

$$\sum_{g \in G} \hat{g} = |G|.$$

Ejercicio 27. Sea f un automorfismo de un grupo finito G, tal que si $x \neq 1$, entonces $f(x) \neq x$.

a) Probar que $G = \{x^{-1}f(x);\ x \in G\}$.

b) Si $f^2 = Id$, entonces G es abeliano de orden impar.

Ejercicio 28. a) Probar que un grupo no abeliano G es hamiltoniano si, y sólo si, todo subgrupo cíclico es invariante, si, y sólo si, para todo par de elementos $x, y \in G$, existe $n \in \mathbf{N}$ con $yx = x^n y$.

b) ¿Es $H_2 \times \mathbf{Z}_4$ un grupo hamiltoniano?

Ejercicio 29. Si C es una clase conjugada de un grupo G, entonces para cada automorfismo f de G, $f(C)$ también es una clase conjugada. La totalidad de automorfismos f, tales que $f(C) = C$ para toda clase conjugada de G, es un subgrupo invariante de Aut(G).

Ejercicio 30. a) Sea $x \in G$, tal que para todo $y \in G$, $y \neq 1$, existe $n \in \mathbf{N}$ con $x = y^n$. Probar que $x \in z(G)$.

b) En Int(G) no existen elementos $\alpha \neq 1$, tal que: si $\theta \in \text{Int}(G)$, $\beta \neq 1$, existe $n \in \mathbf{N}$ con $\beta^n = \alpha$.

c) No existe un grupo G tal que $\text{Int}(G) \simeq H_2$.

Ejercicio 31. Sea G la totalidad de matrices de la forma

$$\begin{Vmatrix} 1 & b \\ 0 & a \end{Vmatrix} \qquad (a, b \in \mathbf{Z}_n,\ (a, n) = 1).$$

a) Verificar que G es un grupo (con el producto usual de matrices) de orden $n \cdot \phi(n)$.

b) Para $n = 4$ ¿es $G \simeq H_2$? ¿Es $G \simeq D_4$?

Ejercicio 32. a) Sea G un grupo finito de orden n. Probar que G es cíclico si, y sólo si, para cada divisor m de n, G posee un único subgrupo de orden m.

b) Si G tiene orden $p^r (r \geq 1)$ y posee un único subgrupo de orden p, ¿es G necesariamente cíclico?

Ejercicio 33. a). Si G es un grupo de orden p^n, $n \geq 2$, entonces $|[G, G]| \leq p^{n-2}$, y además

b) $|z(G)| \neq p^{n-1}$.

c) Hallar $[G, G]$ y $z(G)$ en los cinco grupos no isomorfos de orden p^3 (teorema 2. 7. 3).

Ejercicio 34. Sea S_n que opera sobre $K[X_1, X_2, \ldots, X_n]$ en la forma

$$t \cdot P(X_1, X_2, \ldots, X_n) = P(X_{t(1)}, X_{t(2)}, \ldots, X_{t(n)})$$

un polinomio P se dice simétrico si, y sólo si, $t \cdot P = P(\forall t \in S_n)$.

a) Verificar que los polinomios siguientes son simétricos:

$$P_1 = X_1 + X_2 + \ldots + X_n$$

$$P_2 = X_1X_2 + X_1X_3 + \ldots + X_{n-1}X_n$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$P_n = X_1X_2X_3 \ldots X_n.$$

Nota. Un resultado clásico de la teoría de ecuaciones establece que todo polinomio simétrico P se puede escribir unívocamente a partir de sumas y productos de los polinomios elementales P_i.

b) Mostrar que los siguientes polinomios son simétricos y escribirlos en función de los P_i.

i) $X_1^2 + X_2^2 + X_3^2 \qquad (n = 3)$

ii) $(X_1 - X_2)^2 (X_1 - X_3)^2 (X_2 - X_3)^2 \qquad (n = 3)$

iii) $(X_1 - X_2)^2 \qquad (n = 2)$

c) ¿Es simétrico el polinomio $p = \prod_{1 \le i < j \le n} (X_i - X_j)$?

En caso contrario, hallar la órbita de P.

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 3.

Ejercicio 35. Calcular y descomponer como producto de ciclos disjuntos

a) (1 2 3) (1 2 4) (5 6 1 2).

b) (2 3 7 8) (8 7 3 1) (4 2).

c) xy, yx, $[x, y]$ para x = (1 3) (2 4) (5 7 6) y = (1 2) (4 5 6 7).

d) $[x, y]$ para $x = (\alpha_1\alpha_2 \ldots \alpha_r)$, $y = (\alpha_r\alpha_{r+1} \ldots \alpha_n)$.

e) $[(1\ 2\ 3), (1\ 2\ 4)]^2$.

Ejercicio 36. Calcular los órdenes de

(1 2 3) (2 3 4), (1 2 3) (4 5)

(1 2 3) (1 2 4) (1 2 5), (1 2 3 4 5) (5 4 3)

(1 2 3) (1 2 4) (1 2 3), (1 2) (3 4) (1 2) (1 2 3 4).

Ejercicio 37. Si H es un grupo abeliano de S_n que opera transitivamente sobre $\{1, 2, \ldots n\}$, entonces $|H| = n$.

Ejercicio 38. a) Probar que los únicos subgrupos transitivos de S_3 son S_3 y A_3.

b) Hallar todos los subgrupos transitivos de S_4.

En cada uno de ellos analizar k-transitividad ($k > 1$).

Ejercicio 39. Determinar el número de clases conjugadas de S_6 y A_6, y respecto a cada una hallar el número de elementos que la integran.

Ejercicio 40. Hallar $C(x, S_n)$ en cada uno de los siguientes casos:

i) $x = (1\ 2\ 3\ 4)$ $(n = 6)$

ii) $x = (1\ 2\ 3)(4\ 5\ 6)$ $(n = 8)$

iii) $x = (1\ 2\ 3)(5\ 6)$ $(n = 6)$

iv) $x = (1\ 2\ 3\ 4\ 5)$ $(n = 5)$.

Ejercicio 41. Los elementos

$$s = (x_1 x_2 \dots x_n) \quad y \quad t = (x_1 x_2) \text{ generan } S_n.$$

b) Si $n \geq 3$, los 3-ciclos $(x_1 x_2 x_3)$, $(x_1 x_2 x_4) \dots (x_1 x_2 x_n)$ generan A_n.

c) Si $n = 2k + 1 (k \geq 1)$, los 3-ciclos $(x_1 x_2 x_3)$, $(x_1 x_4 x_5)$, $\dots$ $(x_1 x_{2k} x_{2k+1})$ generan A_n.

d) Sean los elementos

$$x = (x_1 x_2 \dots x_{n-2} x_{n-1}), \quad y = (x_1 x_2 \dots x_{n-2} x_n).$$

Entonces, si n es par, $\langle x, y \rangle = S_n$, y si n es impar, $\langle x, y \rangle = A_n$.

Ejercicio 42. Probar que $H = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ es un subgrupo invariante de S_4. ¿Es $S_4/H \simeq S_3$?

Ejercicio 43. Probar que el grupo S_3 posee exactamente tres caracteres irreducibles (dos de grado 1 y uno de grado 2), y hallarlos.

Ejercicio 44. Probar que el grupo cuaterniónico H_2 posee exactamente cinco caracteres irreducibles (cuatro de grado 1 y uno de grado 2), y hallarlos.

Ejercicio 45. a) Cuántas representaciones irreducibles de grado 1 posee S_4? Hallar los caracteres.

b) Verificar que σ y τ inducen representaciones irreducibles de grado 3 de S_4:

$$\sigma(1\ 2) = \begin{Vmatrix} -1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{Vmatrix} \qquad \sigma(2\ 3\ 4) \begin{Vmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{Vmatrix} = \tau(2\ 3\ 4)$$

$$\tau(1\ 2) = \begin{Vmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{Vmatrix}$$

¿Son σ y τ isomorfos? Hallar los caracteres.

c) Probar que S_4 posee exactamente dos representaciones irreducibles de grado 1, dos de grado 3 y una de grado 2. Hallar esta última.

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 4

Ejercicio 46. Hallar los subgrupos de Sylow en los siguientes casos:

a) Z_n b) $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} ; a, b \in Z_7, a \neq 0 \right\}$

c) $SL(2, Z_5)$ d) S_5.

Ejercicio 47. Sean G_1 y G_2 grupos finitos, $G = G_1 \times G_2$. Probar que los p-subgrupos de Sylow de G son de la forma $H_1 \times H_2$ con H_i p-subgrupo de Sylow de $G_i (i = 1, 2)$.

Ejercicio 48. Calcular los subgrupos de Sylow de

a) $S_3 \times A_4$ b) $S_3 \times Z_{20}$.

Ejercicio 49. Probar que no hay un grupo simple de cualquiera de los siguientes órdenes:

12, 28, 312, 56, 36.

Ejercicio 50. Todo grupo de orden 5. 7. 13 es cíclico.

Ejercicio 51. ¿Cuántos subgrupos de Sylow poseen los grupos no abelianos de órdenes 21, 39, 34?

Ejercicio 52. Sea G un grupo finito, P un p-subgrupo de Sylow de G y H un subgrupo tal que $N(P, G) \subseteq H$. Probar que $N(H, G) = H$.

Ejercicio 53. ¿Es cierto que si G es un grupo finito de orden n y si p^i / n, entonces todos los subgrupos de G de orden p^i son conjugados?

Ejercicio 54. Probar que A_5 no posee subgrupos de orden 15. ¿Posee S_5 tales subgrupos?

Ejercicio 55. Si G es un grupo de orden 12, tal que $G \neq A_4$, entonces G posee elementos de orden 6.

Ejercicio 56. a) Si P es un p-subgrupo de Sylow de G, entonces $N(P, G)/P$ no posee elementos $(\neq 1)$ cuyo orden sea potencia de p.

b) Si, además, x tiene por orden una potencia de p y es tal que $xPx^{-1} = P$, entonces $x \in P$.

Ejercicio 57. Un grupo finito G de orden n, con la propiedad de que para todo divisor m de n existe un subgrupo invariante de orden m, se denomina *nilpotente*.

a) G es nilpotente si, y sólo si, para cada primo p que divida el orden de G, existe un único p-subgrupo de Sylow de G (si, y sólo si, G es producto directo de sus subgrupos de Sylow).

b) Los grupos abelianos son nilpotentes.

c) Los p-grupos son nilpotentes.

d) Todo grupo nilpotente es resoluble.

e) Analizar la nilpotencia de S_n y A_n para todo $n \in \mathbf{N}$.

f) Si G posee un subgrupo invariante H tal que H y $G/_H$ son nilpotentes, ¿es necesariamente válido que G sea nilpotente?

Ejercicio 58. Si G es un grupo, se define la *serie de derivados.*

$$D^1(G) = [G, G]$$

$$D^i(G) = D^1(D^i(G)) \quad (i > 1).$$

a) Probar que $D^{i+1}(G)$ es invariante en $D^i(G)$, y que el cociente $D^i(G)/D^{i+1}(G)$ es abeliano.

b) G es resoluble si, y sólo si, para algún $n \in \mathbf{N}$ es $D^n(G) = 1$.

c) Si G es resoluble, todo subgrupo y todo cociente de G son resolubles.

Ejercicio 59. Probar que todo grupo de orden p^2q es resoluble.

Ejercicio 60. Analizar la resolubilidad de los grupos

a) $GL(2, \mathbf{Z}_3)$

b) $SL(2, \mathbf{Z}_5)$

c) $G = \left\{ \begin{pmatrix} 2^n & p(x) \\ 0 & 1 \end{pmatrix}; n \in \mathbf{Z},\ p(x) \in \mathbf{Q}[X] \right\}$

EJERCICIOS CORRESPONDIENTES AL CAPÍTULO 5

Ejercicio 61. Verificar que no hay grupos simples de orden 200, 204, 260, 520, 2540, 9075.

Ejercicio 62. ¿Cuántos elementos de orden 7 posee un grupo *simple* de orden 168? (se puede demostrar que efectivamente hay grupos simples de ese orden).

Ejercicio 63. Calcular el centro de $GL(n, K)$ (K cuerpo). ¿Es $GL(n, K)$ un grupo simple?

Ejercicio 64. Verificar que

$$G = \left\{ \begin{pmatrix} 1 & b \\ 0 & a \end{pmatrix}; a, b \in \mathbf{Z}_5,\ a \neq 0 \right\}$$

no es simple.

Ejercicio 65. ¿Existen grupos simples y resolubles?

Ejercicio 66. Sea H_n el grupo cuaterniónico generalizado de orden 2^{n+1}:

$$H_n = \langle A, B / A^{2n} = B^4 = 1,\ B^2 = A^{2n-1},\ BAB^{-1} = A^{-1} \rangle.$$

a) El subgrupo $K = \langle A \rangle$ es invariante en H_n; el cociente H_n/K es isomorfo a Z_2.

Hallar una sección σ, la Z_2- acción inducida θ y el cociclo asociado a H_n considerado como extensión de K por Z_2.

b) Ídem con el subgrupo $\langle A^2, B \rangle \simeq H_{n-1}$.

Ejercicio 67. Todo grupo de orden p^2q es producto directo de sus subgrupos de Sylow.

Hallar tantos grupos no isomorfos de orden 18 como se pueda (hay exactamente cinco de estos grupos).

Ejercicio 68. Ídem de orden 20 (también hay cinco grupos).

Ejercicio 69. Sea $n > 2$, p primo impar.

Hallar un grupo no abeliano de orden p^n generado por los elementos a, b, que satisfagan

$$a^{p^{n-1}} = b^p = 1,\ bab^{-1} = a^{1+p^{n-2}}.$$

¿Es el grupo hallado el producto semidirecto de los subgrupos $\langle a \rangle$ y $\langle b \rangle$? Se puede demostrar que el grupo construido es el único no abeliano de orden p^n que posee elementos de orden p^{n-1} (cf. (3)).

Ejercicio 70. Sea $n > 3$; construir grupos no abelianos de orden 2^n generados por los elementos a, b, que satisfagan

i) $a^{2^{n-1}} = b^2 = 1,\ bab^{-1} = a^{1+2^{n-2}}$

ii) $a^{2^{n-1}} = b^2 = 1,\ (ab)^2 = a^{2^{n-2}}$

¿Son dichos grupos producto semidirecto de los subgrupos $\langle a \rangle$ y $\langle b \rangle$? Se puede demostrar que los grupos construidos, a más de H_{n-1} y $D_{2^{n-1}}$, son los únicos no abelianos de orden 2^n que poseen elementos de orden 2^{n-1} (cf. (3)).

BIBLIOGRAFÍA

Libros

(1) BURNSIDE, W. Theory of Groups of Finite Order, Dover, Nueva York, N. Y., 512 págs. (1955).

(2) BURROWS, M. Representation Theory of Finite Groups, Academic, Nueva York, N. Y., 185 págs. (1965).

(3) CARMICHAEL, R. Introduction to Theory of Finite Groups, Dover, Nueva York, N. Y., 447 págs. (1956).

(4) CARTAN, H. y EILEMBERG, S. Homological Algebra, Princeton, Univ. Press, Princeton, N. J., 390 págs. (1956).

(5) CURTIS, C. y REINER, I. Representation Theory of Finite Groups and Associative Algebras, Wiley, Nueva York, N. Y., 685 págs. (1962).

(6) DIEUDONNE, J. La Géométrie des Groupes Classiques, Springer, Berlín, 125 págs. (1963).

(7) DICKSON, L. E. Linear Groups, Dover, Nueva York, N. Y., 312 págs. (1958).

(8) DIXON, J. D. Problems in Group Theory, Blaisdell, Waltham, Mass., 176 págs. (1967).

(9) FEIT, W. Characters of Finite Groups, Benjamin, Nueva York, N. Y., 186 págs. (1966).

(10) FUCHS, L. Abelian Groups, Pergamon, Londres, 367 págs. (1960).

(11) GENTILE, E. R. Estructuras Algebraicas, monografía N° 3, serie de matemática, O. E. A., Washington, D. C., 117 págs. (1967).

(12) GENTILE, E. R. Estructuras Algebraicas, II, monografía N° 12, serie de matemática, O. E. A., Washington, D. C., 158 págs. (1971).

(13) GORENSTEIN, D. Finite Groups, Harper & Row, Nueva York, N. Y., 527 págs. (1958).

(14) GRUEMBERG, K. W. Cohomological Topics in Group Theory, Lecture Notes in Mathematics N° 143, Springer, Berlín, 275 págs. (1970).

(15) HALL, M. The Theory of Groups, Macmillan, Nueva York, N. Y., 431 págs. (1959).

(16) JACOBSON, N. Lectures on Abstract Algebra, Vols. I y II, Van Nostrand, Nueva York, N. Y. (1951).

(17) KAPLANSKY, I. "Infinite Abelian Groups, Michigan Univ., East Lansing, Michigan, 91 págs. (1954).

(18) KUROSH, A.G. Theory of Groups, Vols. I y II, Chelsea, Bronx, N.Y. (1955).

(19) LEDERMAN, W. Introduction to the Theory of Finite Groups, Oliver & Boyd, Edimburgo, 170 págs. (1957).

(20) MAC LANE, S. Homology, Springer, Berlín, 422 págs. (1963).

(21) MILLER, G.A., BLICHFELDT, H. y DICKSON, L.E. Theory and Applications of Finite Groups, Dover, Nueva York, N.Y. (1961).

(22) ROTMAN, J.J. The Theory of Groups, Allyn & Bacon, Boston, Mass., 305 págs. (1965).

(23) SCHENKMAN, E. Group Theory, Van Nostrand, Nueva York, N.Y., 289 págs. (1965).

(24) SCOTT, W.W. Group Theory, Prentice Hall, Englewood Cliffs, N.J. (1964).

(25) SERRE, J.P. Representations Lineaire des Groupes Finis, Hermann, París, 128 págs. (1967).

(26) WEIL, H. The Classical Groups, Princeton Univ. Press, Princeton, N.J., 302 págs. (1964).

(27) WIELANDT, H. Finite Permutations Groups, Academic, Nueva York, N.Y., 114 págs. (1964).

(28) ZASSENHAUS, H. The Theory of Groups, Chelsea, Bronx, N.Y., 265 págs. (1958).

Artículos

(29) BRAUER, R. "Investigations on Group Characters", *Ann. Math.*, **42**, 936-958 (1941).

(30) BRAUER, R. y TUAN, H.F. "Simple Groups of Finite Order", *Bull. Am. Math. Soc.*, **51**, 756-766 (1945).

(31) FEIT, W. "Groups which Contain Frobenius Groups as Subgroups", Vol. I, *Proc. Sym. Pure Math.* (1959).

(32) FEIT, W. y THOMPSON, J.G. "Solvability of Groups of Odd Order", *Pacific J. Math.*, **13**, 775-1029 (1963).

(33) IWAHORI, N. "On a Property of a Finite Group", Journal of the Faculty of Science, University of Tokyo, XI, Part. 1, 47-46 (1964).

(34) KOVACS, L.G., NEUMANN, B.H. y DE VRIES, H. "Some Sylow Subgrups", *Proc. Royal Soc. (London)*, Series A260, 304-316 (1961)

(35) MOORE, E.H. "Concerning the Abstract Groups of Order k! and ½ k! *Proc. Lond. Math. Soc.*, **28**, 357-366 (1897).

(36) PICARD, S. "Sur les Bases du Groupe Symmétrique et du Groupe Alternant", *Ann. Math.*, **116**, 752-767 (1939).

COLECCIÓN DE MONOGRAFÍAS CIENTÍFICAS

Publicadas

Serie de matemática

N° 1. La Revolución en las Matemáticas Escolares, por el Consejo Nacional de Maestros de Matemáticas de los Estados Unidos de América.
N° 2. Espacios Vectoriales y Geometría Analítica, por Luis A. Santaló.
N° 3. Estructuras Algebraicas, por Enzo R. Gentile.
N° 4. Historia de las Ideas Modernas en la Matemática, por José Babini.
N° 5. Álgebra Lineal, por Orlando Villamayor.
N° 6. Algebra Linear e Geometria Euclidiana, por Alexandre Augusto Martins Rodrigues.
N° 7. El Concepto de Número, por César A. Trejo.
N° 8. Funciones de Variable Compleja, por José I. Nieto.
N° 9. Introducción a la Topología General, por Juan Horváth.
N° 10. Funções Reais, por Djairo G. de Figueiredo.
N° 11. Probabilidad e Inferencia Estadística, por Luis A. Santaló.
N° 12. Estructuras Algebraicas, II, (Álgebra Lineal), por Enzo R. Gentile.
N° 13. La Revolución en las Matemáticas Escolares (Segunda Fase), por Howard F. Fehr, John Camp y Howard Kellogg.
N° 14. Estructuras Algebraicas, III, (Grupos Finitos), por Horacio Hernán O'Brien.

Serie de física

N° 1. Concepto Moderno del Núcleo, por D. Allan Bromley.
N° 2. Panorama de la Astronomía Moderna, por Félix Cernuschi y Sayd Codina.
N° 3. La Estructura Electrónica de los Sólidos, por Leopoldo M. Falicov.
N° 4. Física de Partículas, por Igor Saavedra.
N° 5. Experimento, Razonamiento y Creación en Física, por Félix Cernuschi.
N° 6. Semiconductores, por George Bemski.
N° 7. Aceleradores de Partículas, por Fernando Alba Andrade.
N° 8. Física Cuántica, por Onofre Rojo y H. McIntosh.

Serie de química

N° 1. Cinética Química Elemental, por Harold Behrens Le Bas.
N° 2. Bioenergética, por Isaias Raw y Walter Colli.
N° 3. Macromoléculas, por Alejandro Paladini y M. Burachik.
N° 4. Mecanismo de las Reacciones Orgánicas, por Jorge A. Brieux.
N° 5. Elementos Encadenados, por Jacobo Gómez Lara.
N° 6. Enseñanza de la Química Experimental, por Francisco Giral.
N° 7. Fotoquímica de Gases, por Ralf-Dieter Penzhorn.
N° 8. Introducción a la Geoquímica, por Félix González-Bonorino.

Serie de biología

N° 1. La Genética y la Revolución en las Ciencias Biológicas, por José Luis Reissig.

N° 2. Bases Ecológicas de la Explotación Agropecuaria en la América Latina, por Guillermo Mann F.
N° 3. La Taxonomía y la Revolución en las Ciencias Biológicas, por Elías R. de la Sota.
N° 4. Principios Básicos para la Enseñanza de la Biología, por Oswaldo Frota-Pessoa.
N° 5. A Vida da Célula, por Renato Basile.
N° 6. Microorganismos, por J. M. Gutiérrez-Vázquez.
N° 7. Principios Generales de Microbiología, por Norberto J. Palleroni.
N° 8. Los Virus, por Enriqueta Pizarro-Suárez y Gamba.
N° 9. Introducción a la Ecología del Bentos Marino, por Manuel Vegas Vélez.
N° 10. Biosíntesis de Proteínas y el Código Genético, por Jorge E. Allende.

En preparación

Serie de matemática

Estructuras Algebraicas, IV, (Teoría de Cuerpos), por Darío J. Picco.
Estructuras Algebraicas, V, (Estructura de Álgebras), por Artibano Micali.

Serie de física

Introdução à Cristalografia, por Ivonne Mascarenhas.
La Radiación Cósmica, por Gastón R. Mejía y Carlos Aguirre.
Astrofísica, por Carlos Jaschek y Mercedes C. Jaschek.
Ondas, por Enrique Gaviola y Oscar Bressan.
El Láser, por Mario Garavaglia.
Cálculo de Errores, Aplicación y Teoría, por Wolfgang Meckbach.

Serie de química

Productos Vegetales de Bajo Peso Molecular, por Venancio Deulofeu y colaboradores.
Estereoquímica Orgánica, por Juan A. Garbarino.
Cromatografía en Papel y en Capa Delgada, por Jorge A. Domínguez.
Momento Polar, por Pedro Lehman.
Polarografía, por Alejandro J. Arvía.
Resonancia Magnética Nuclear de Hidrógeno, por Pedro Joseph-Nathan.
Espectroscopía Infrarroja, por Jesús Morcillo.
Fotometría de Llama y Absorción Atómica, por Juan Ramírez Muñoz.
Cromatografía Líquida de Alta Presión, por Harold M. McNair y Benjamín Esquivel.
Cromatografía de Gases, por Harold M. McNair y Benjamín Esquivel.
Introdução à Espectrometria de Massa das Substâncias Orgânicas, por Otto R. Gottlieb.
Rotación Optica, por Pierre Crabbé.
Aspectos Modernos de la Corrosión, por T. Markovic.
Química de los Esteroides, por Josef E. Herz.

Serie de biología

Elementos de Inmunología e Inmunoquímica, por Félix Córdoba y Sergio Estrada-Parra.
Inventario de Vegetación de Biomas, por Jorge Morello.
Los Sistemas Ecológicos y el Hombre, por Francesco di Castri.
Biogeografía de América Latina, por Angel L. Cabrera y Abraham Willink.
Fermentaciones, por Carlos del Río E.
Procesos Microbianos Aerobios de Importancia Industrial, por Carlos Casas-Campillo.
Transferencia de Material Genético, por Manuel Rieber.
Bacteriófagos, por Romilio Espejo T.
Microbiología de Suelos, por Johanna Döbereiner.
Micología, por Margarita Silva-Hutner y William G. Merz.
Relación Huésped-Parásito, por Manuel Rodríguez Leiva.

Nota. Las personas interesadas en adquirir estas obras deben dirigirse a la División de Ventas y Promoción, Organización de los Estados Americanos, Washington, D. C., 20006 o a las Oficinas Nacionales de la OEA en el país respectivo.