Introducción a la teoría de grupos finitos

por Alberto García Raboso

8 de marzo de 2007

Este documento ha sido realizado en AMS-LaTeX 2_ε.

v. 1.0 (26 de agosto de 2001).

v. 1.1 (24 de febrero de 2004): Actualización de dirección de correo electrónico.

v. 1.2 (8 de marzo de 2007): Corrección de algunas erratas (gracias a Jorge Núñez Pascual). Modificada tabla al final del capítulo 10 para incluir grupos abelianos (por sugerencia de Jorge Núñez Pascual). Actualización de dirección de correo electrónico.

Se puede contactar con el autor en <agraboso@physics.rutgers.edu> y <agraboso@gmail.com>

Índice general

Capítulo 1

Grupos y subgrupos

1.1. Primeras definiciones y propiedades

Definición 1.1.1 *Un* grupo *es un conjunto G dotado de una operación binaria $*$ que satisface los siguientes axiomas:*

(G1) *Operación interna:*

$$\forall x, y \in G,\ x * y \in G$$

(G2) *Propiedad asociativa:*

$$\forall x, y, z \in G,\ (x * y) * z = x * (y * z)$$

(G3) *Existencia de elemento neutro:*

$$\exists e \in G\ :\ \forall g \in G,\ e * g = g * e = g$$

(G4) *Existencia de elemento inverso:*

$$\forall g \in G,\ \exists g^{-1} \in G\ :\ g * g^{-1} = e = g^{-1} * g$$

Definición 1.1.2 *Se dice que un grupo $(G, *)$ es* abeliano *si para todos $x, y \in G$ se cumple $x * y = y * x$.*

Definición 1.1.3 *Sea $(G, *)$ un grupo. Se llama* orden *de $(G, *)$ al cardinal $|G|$ del conjunto subyacente. Se dice que $(G, *)$ es finito si dicho cardinal lo es, e infinito en caso contrario.*

Proposición 1.1.4 (Propiedades cancelativas) *Sea $(G, *)$ un grupo. Para todos $a, b, c \in G$ se cumple*

$$a * c = b * c \Longrightarrow a = b$$
$$c * a = c * b \Longrightarrow a = b$$

DEMOSTRACIÓN. Dado $c \in G$, el axioma (G4) asegura la existencia de un elemento $c^{-1} \in G$ tal que $c * c^{-1} = e$. Entonces, componiendo $a * c = b * c$ por la derecha con c^{-1}, se tiene

$$\begin{aligned} (a * c) * c^{-1} &= (b * c) * c^{-1} && \text{utilizando (G2)} \\ a * (c * c^{-1}) &= b * (c * c^{-1}) && \text{utilizando (G4)} \\ a * e &= b * e && \text{utilizando (G3)} \\ a &= b \end{aligned}$$

Análogamente, y dado que $c^{-1} * c = e$, componiendo $c * a = c * b$ por la izquierda con c^{-1},

$$\begin{aligned} c^{-1} * (c * a) &= c^{-1} * (c * b) && \text{utilizando (G2)} \\ (c^{-1} * c) * a &= (c^{-1} * c) * b && \text{utilizando (G4)} \\ e * a &= e * b && \text{utilizando (G3)} \\ a &= b \end{aligned}$$

□ Q.E.D.

Proposición 1.1.5 *El elemento neutro e de un grupo $(G, *)$ es unico.*

DEMOSTRACIÓN. Supongamos que existiesen en $(G, *)$ dos elementos neutros distintos $e, f \in G$. Entonces, utilizando el axioma (G3), $e = e * f = f$. □ Q.E.D.

Proposición 1.1.6 *El elemento inverso de cualquier elemento g de un grupo $(G, *)$ es único.*

DEMOSTRACIÓN. Supongamos que existiesen dos elementos $g^{-1}, g^\star \in G$ tales que $g * g^{-1} = g^{-1} * g = e$ y $g * g^\star = g^\star * g = e$. Entonces, $g * g^{-1} = g * g^\star$, y, utilizando la propiedad cancelativa por la izquierda, se tiene $g^{-1} = g^\star$. □ Q.E.D.

Proposición 1.1.7 *Sea $(G, *)$ un grupo. Para todo $g \in G$ se tiene que $(g^{-1})^{-1} = g$.*

DEMOSTRACIÓN. Dada la unicidad del elemento inverso, basta observar que $g * g^{-1} = g^{-1} * g = e$. □ Q.E.D.

Proposición 1.1.8 *Sea $(G, *)$ un grupo. Para todos $x, y \in G$ se tiene que $(x * y)^{-1} = y^{-1} * x^{-1}$.*

DEMOSTRACIÓN. La unicidad del elemento inverso y las relaciones

$$(x * y) * (x * y)^{-1} = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = x * x^{-1} = e$$
$$(x * y)^{-1} * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * e * y = y^{-1} * y = e$$

demuestran el enunciado. □ Q.E.D.

Proposición 1.1.9 *Sea $(G,*)$ un grupo. Entonces,*

$$(G,*) \text{es abeliano} \iff \forall x,y \in G,\ (x*y)^{-1} = x^{-1}*y^{-1}$$

DEMOSTRACIÓN. De la definición de grupo abeliano, $(x*y)^{-1} = y^{-1}*x^{-1} = x^{-1}*y^{-1}$.

Recíprocamente, si para todos $x,y \in G$ se tiene $(x*y)^{-1} = x^{-1}*y^{-1}$, entonces, utilizando sucesivamente las proposiciones 1.1.7 y 1.1.8, la hipótesis y de nuevo la proposición 1.1.7,

$$x*y = (x^{-1})^{-1}*(y^{-1})^{-1} = (y^{-1}*x^{-1})^{-1} = (y^{-1})^{-1}*(x^{-1})^{-1} = y*x$$

□ Q.E.D.

1.2. Subgrupos

Definición 1.2.1 *Dado un grupo $(G,*)$ y un subconjunto $H \subseteq G$, se dice que $(H,*)$ es un* subgrupo *de $(G,*)$, y se denota $(H,*) \leq (G,*)$, si H es un grupo con respecto a la operación $*$ definida en G.*

Definición 1.2.2 *Sea $(G,*)$ un grupo. Los subconjuntos G y $\{e\}$ reciben el nombre de* subgrupos impropios *de G. El resto de subgrupos de G reciben el nombre de* subgrupos propios *de G.*

Proposición 1.2.3 *Sea $(G,*)$ un grupo, y sea $H \subseteq G, H \neq \emptyset$. $(H,*)$ es un subgrupo de $(G,*)$ si y sólo si para todos $x,y \in H$ se cumple $x*y^{-1} \in H$.*

DEMOSTRACIÓN. Sea H un subgrupo de G. Si $x,y \in H$ entonces, por (G4), $y^{-1} \in H$, y, por (G1), $x*y^{-1} \in H$.

Recíprocamente, sea $x \in H$. Entonces $x*x^{-1} = e \in H$ y $e*x^{-1} = x^{-1} \in H$, demostrando (G3)y (G4). Para probar (G1), basta observar que $x*y = x*(y^{-1})^{-1} \in H$. Por último, la asociatividad de la operación en H se deduce de la asociatividad de la operación en G. □ Q.E.D.

Proposición 1.2.4 *Sea I un conjunto de índices, y sean $H_i,\ i \in I$ subgrupos de un grupo $(G,*)$. Entonces, $\bigcap_{i\in I} H_i$ es un subgrupo de G.*

DEMOSTRACIÓN. Sean $x,y \in H_i$ para todo $i \in I$. Por ser H_i subgrupos, $x*y^{-1} \in H_i$ para todo $i \in I$. Entonces, $x,y,x*y^{-1} \in \bigcap_{i\in I} H_i$. □ Q.E.D.

Definición 1.2.5 *Sea X un subconjunto cualquiera de un grupo G. Se llama* subgrupo generado por X, *y se denota $\langle X\rangle$, a la intersección de todos los subgrupos de G que contienen a X.*

Proposición 1.2.6 *En las condiciones de la definición anterior,*

$$\langle X\rangle = \{x_1^{\alpha_1}*x_2^{\alpha_2}*\cdots*x_n^{\alpha_n} \ :\ x_1,x_2,\ldots,x_n \in X,\ \alpha_1,\alpha_2,\ldots,\alpha_n \in \mathbb{Z}\}$$

DEMOSTRACIÓN. Sea H_X el conjunto del miembro derecho de la igualdad. Es claro que H_X es un subgrupo de G. Como $X \subseteq H_X$ y $\langle X \rangle$ es el mínimo subgrupo que contiene a X, se tiene que $\langle X \rangle \subseteq H_X$.

Falta probar la inclusión contraria. Puesto que $\langle X \rangle$ es un subgrupo de G y $X \subseteq \langle X \rangle$, si $x_i \in X$, $x_i \in \langle X \rangle$ para todo $i = 1, 2, \ldots, n$, de donde $x_1^{\alpha_1} * x_2^{\alpha_2} * \cdots * x_n^{\alpha_n} \in \langle X \rangle$ y $H_X \subseteq \langle X \rangle$. □ Q.E.D.

Definición 1.2.7 *Se llama* retículo de los subgrupos *de un grupo* $(G, *)$ *al conjunto de todos los subgrupos de* $(G, *)$*, junto con sus relaciones de inclusión.*

1.3. Homomorfismos de grupos

Definición 1.3.1 *Sean* $(G_1, *), (G_2, \star)$ *grupos, y sea* $f : G_1 \longrightarrow G_2$ *una aplicación entre ellos. Se dice que* f *es un* homomorfismo de grupos *si*

$$f(x * y) = f(x) \star f(y)$$

Un homomorfismo inyectivo recibe el nombre de monomorfismo*; un homomorfismo suprayectivo,* epimorfismo*; un homomorfismo biyectivo,* isomorfismo*; y un isomorfismo de* G *en sí mismo,* automorfismo*.*

Si existe un isomorfismo entre $(G_1, *)$ *y* $(G_2, \star)$*, se dice que ambos grupos son isomorfos, y se denota* $(G_1, *) \cong (G_2, \star)$*.*

Proposición 1.3.2 *Sean* $(G, *), (H, \star)$ *grupos, y sea* $f : G \longrightarrow H$ *un homomorfismo entre ellos. Entonces, para todos* $x, y \in G$*,*

$$f(x * y^{-1}) = f(x) \star f(y)^{-1}$$
$$f(y^{-1} * x) = f(y)^{-1} \star f(x)$$

DEMOSTRACIÓN. Utilizando que f es un homomorfismo,

$$f(x * y^{-1}) \star f(y) = f((x * y^{-1}) * y) = f(x)$$

y basta componer con $f(y)^{-1}$ por la derecha. La demostración del segundo aserto es análoga. □ Q.E.D.

Corolario 1.3.3 *Sean* $(G, *), (H, \star)$ *grupos, y sea* $f : G \longrightarrow H$ *un homomorfismo entre ellos. Entonces,*

1. $f(e_G) = e_H$*.*
2. *Para todo* $g \in G$*,* $f(g^{-1}) = f(g)^{-1}$*.*

DEMOSTRACIÓN.

1. Basta aplicar la proposición anterior al caso $x = y$.

2. Basta aplicar la proposición anterior al caso $x = e_G, y = g$.

□ Q.E.D.

Proposición 1.3.4 *La relación de isomorfía de grupos es una relación de equivalencia.*

DEMOSTRACIÓN. Sean G, H, K grupos.

La aplicación $id_G : G \longrightarrow G$ es claramente un isomorfismo, por lo que $G \cong G$.

Si ϕ es un isomorfismo de G en H, ϕ^{-1} existe y es una biyección de H en G. Si $x_1, x_2 \in G, y_1, y_2 \in H$, entonces $\phi^{-1}(y_i) = x_i$ si y sólo si $\phi(x_i) = y_i$. Además, $\phi(x_1x_2) = y_1y_2$, de donde $\phi^{-1}(y_1y_2) = x_1x_2$. Así,

$$\phi^{-1}(y_1)\phi^{-1}(y_2) = x_1x_2 = \phi^{-1}(y_1y_2)$$

demostrando que ϕ^{-1} es un homomorfismo. Por tanto, $H \cong G$.

Finalmente, si ϕ es un isomorfismo de G en H, y ψ es un isomorfismo de H en K, $\psi \circ \phi$ es una biyección de G en K. Además,

$$\begin{aligned} \psi \circ \phi(xy) &= \psi(\phi(xy)) \\ &= \psi(\phi(x)\phi(y)) && \text{por ser } \phi \text{ homomorfismo} \\ &= \psi(\phi(x))\psi(\phi(y)) && \text{por ser } \psi \text{ homomorfismo} \\ &= (\psi \circ \phi(x))(\psi \circ \phi(y)) \end{aligned}$$

de modo que $\psi \circ \phi$ es un homomorfismo, y $G \cong K$. □ Q.E.D.

Definición 1.3.5 *Sean $(G, *), (H, \star)$ grupos, y sea $f : G \longrightarrow H$ un homomorfismo entre ellos. Se llaman* núcleo *e* imagen de *f a los conjuntos*

$$\begin{aligned} \ker f &= \{g \in G : f(g) = e\} \\ \mathrm{im} f = f(G) &= \{h \in H : \exists g \in G : f(g) = h\} \end{aligned}$$

Proposición 1.3.6 *Sean G, H grupos, y $f : G \longrightarrow H$ un homomorfismo. Si G es abeliano, $f(G)$ es abeliano.*

DEMOSTRACIÓN.

$$f(x)f(y) = f(xy) = f(yx) = f(y)f(x)$$

□ Q.E.D.

Proposición 1.3.7 *El conjunto* Aut G *de automorfismos de un grupo G es un grupo bajo la operación de composición.*

DEMOSTRACIÓN. Sean $f, g : G \longrightarrow G$ automorfismos de G. Entonces, tanto $f_1 \circ f_2$ como $f_2 \circ f_1$ son biyecciones de G en G. Para demostar que son automorfismos, basta, por tanto, comprobar que son homomorfismos.

$$\begin{aligned}(f_1 \circ f_2)(gh) &= f_1(f_2(gh)) \\ &= f_1(f_2(g)f_2(h)) && \text{por ser } f_2 \text{ homomorfismo} \\ &= f_1(f_2(g))f_1(f_2(h)) && \text{por ser } f_1 \text{ homomorfismo} \\ &= (f_1 \circ f_2)(g)(f_1 \circ f_2)(h)\end{aligned}$$

con demostración análoga para $f_2 \circ f_1$.

La asociatividad se deduce de la asociatividad de la composición de aplicaciones.

La aplicación identidad es, evidentemente, un automorfismo, y cumple $f \circ id_G = id_G \circ f = f$, demostrando la existencia de elemento neutro.

Por último, la inversa de una aplicación biyectiva es biyectiva, y, si $g' = f^{-1}(g)$ y $h' = f^{-1}(h)$,

$$\begin{aligned}f^{-1}(gh) &= f^{-1}(f(g')f(h')) \\ &= f^{-1}(f(g'h')) && \text{por ser } f \text{ homomorfismo} \\ &= g'h' = f^{-1}(g)h^{-1}(h)\end{aligned}$$

demuestra que es un homomorfismo. □ Q.E.D.

Capítulo 2

Teorema de Lagrange

2.1. Clases de un grupo módulo un subgrupo

Definición 2.1.1 *Sea H un subgrupo de un grupo G. Se llama* clase por la izquierda de G módulo H *a cada conjunto*

$$gH = \{gh : \ h \in H\}$$

con $g \in G$.

Análogamente, se llama clase por la derecha de G módulo H *a cada conjunto*

$$Hg = \{hg : \ h \in H\}$$

de nuevo con $g \in G$.

Proposición 2.1.2 *Sea H un subgrupo de un grupo G. Entonces, la relación $\sim_H$ definida en G según*

$$x \sim_H y \iff x^{-1}y \in H$$

es una relación de equivalencia, con $[g] = gH$.

Demostración. La relación $\sim_H$ es reflexiva ya que $x^{-1}x = e \in H$ por ser H subgrupo. Es simétrica, puesto que, si $x \sim_H y$, $x^{-1}y \in H$, entonces $(x^{-1}y)^{-1} = y^{-1}x \in H$ y se tiene $y \sim_H x$. Finalmente, es transitiva, porque, si $x \sim_H y$, $y \sim_H z$, $x^{-1}y, y^{-1}z \in H$, entonces $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$ y $x \sim_H z$. Por tanto, la relación $\sim_H$ es de equivalencia.

Si $x \sim_H g$, entonces $g^{-1}x = h$ para algún $h \in H$, por lo que $x = gh \in gH$. Recíprocamente, si $gh \in gH$ entonces $g^{-1}(gh) = h \in H$ y $g \sim_H gh$. □ Q.E.D.

Corolario 2.1.3 *Sea H un subgrupo de un grupo G. Las clases por la izquierda módulo H forman una partición de G.*

Proposición 2.1.4 *Sea H un subgrupo de un grupo G. Para todo $g \in G$ existe una biyección entre H y gH.*

DEMOSTRACIÓN. Sea $\alpha\colon H \longrightarrow gH$ definida según $\alpha(h) = gh$. Para comprobar que es inyectiva, basta notar que, si $\alpha(x) = \alpha(y)$, se tiene $gx = gy \Rightarrow x = y$. La sobreyectividad es evidente: todo elemento de gH es de la forma gh con $h \in H$, y, por tanto, es la imagen de h por α. □ Q.E.D.

Corolario 2.1.5 $|H| = |gH|$

Proposición 2.1.6 *Sea H un subgrupo de un grupo G. La aplicación α definida según $\alpha(gH) = Hg^{-1}$ establece una biyección entre el conjunto de clases por la izquierda de G módulo H y el conjunto de clases por la derecha de G módulo H.*

DEMOSTRACIÓN. Para probar que α es inyectiva, supongamos que $\alpha(x) = \alpha(y)$. Entonces, $Hx^{-1} = Hy^{-1}$ y existe $h \in H$ tal que $x^{-1} = hy^{-1}$. Así, $y^{-1}x = h^{-1} \in H$ y por tanto $xH = yH$. La sobreyectividad se deduce de que, para todo $x \in G$, $\alpha(x^{-1}H) = Hx$. □ Q.E.D.

2.2. Teorema de Lagrange

Definición 2.2.1 *Se llama* índice de H en G, *y se denota* $[G : H]$, *al número de clases por la izquierda de G módulo H.*

Teorema 2.2.2 (Lagrange) *Sea H un subgrupo de un grupo finito G. Entonces, $|H|$ divide a $|G|$. En particular, se tiene que*

$$|G| = [G : H]|H|$$

DEMOSTRACIÓN. Basta observar que la relación de equivalencia $\sim_H$ particiona G en $[G : H]$ clases distintas, todas ellas con el mismo cardinal $|H|$. □ Q.E.D.

Corolario 2.2.3 *Sean H y K subgrupos de un grupo G tales que $H \leq K \leq G$. Entonces,*

$$[G : H] = [G : K][K : H]$$

DEMOSTRACIÓN. Del teorema de Lagrange,

$$[G : K][K : H] = \frac{|G|}{|K|}\frac{|K|}{|H|} = \frac{|G|}{|H|} = [G : H]$$

□ Q.E.D.

2.3. Producto interno de subgrupos

Definición 2.3.1 *Dados dos subgrupos A y B de un grupo G. Se llama* producto interno de A y B *al conjunto*

$$AB = \{ab : \ a \in A, b \in B\}$$

.

Proposición 2.3.2 *Sean A y B subgrupos de un grupo G. AB es un subgrupo de G si y sólo si $AB = BA$, en cuyo caso se dice que A y B conmutan.*

Demostración. Supongamos que AB es un subgrupo. Sea $ab \in AB$. Existe entonces un elemento $a'b' \in AB$ tal que $a'b' = (ab)^{-1}$ de donde

$$ab = (a'b')^{-1} = (b')^{-1}(a')^{-1} \in BA$$

lo cual demuestra que $AB \subseteq BA$. Por otro lado, para todo $ba \in BA$ se tiene

$$ba = (a^{-1}b^{-1})^{-1} \in AB$$

por lo que $BA \subseteq AB$ y, finalmente, $AB = BA$.

Recíprocamente, sean $a_1b_1, a_2b_2 \in AB$. Como $AB = BA$, existe elementos $a' \in A, b' \in B$ tales que $b_1a_2 = a'b'$. Así,

$$(a_1b_1)(a_2b_2) = (a_1a')(b'b_2) \in AB$$

demostrando (G1). La asociatividad (G2), se deduce de la de la operación definida en G. (G3) es evidente, ya que $e \in A, e \in B \Rightarrow e \in AB$. Por último, para probar (G4) basta observar que $(ab)^{-1} = b^{-1}a^{-1} \in BA = AB$. □Q.E.D.

Proposición 2.3.3 *Sean A y B subgrupos finitos de un grupo G. Entonces,*

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

Demostración. Sea $\{x_i(A \cap B) : \ i = 1, \ldots, k\}$ el conjunto de clases por la izquierda de A módulo $A \cap B$, de modo que $x_i x_j^{-1} \notin A \cap B$. Puesto que éstas establecen una partición en A, para todo $a \in A$ podemos escribir $a = x_i g$ para algún $1 \leq i \leq k$ y algún $g \in A \cap B$.

Así, todo elemento $ab \in AB$ puede escribirse según $ab = x_i(gb) \in x_iB$. Además, $x_iB \neq x_jB$, ya que, en caso contrario, $x_ix_j^{-1} \in B$, y, como $x_ix_j^{-1} \in A$ por definición, se tendría $x_ix_j^{-1} \in A \cap B$.

Esto demuestra que $\{x_iB : \ i = 1, \ldots, k\}$ es el conjunto de clases por la izquierda de AB módulo B, de manera que

$$[A : A \cap B] = \frac{|A|}{|A \cap B|} = k = \frac{|AB|}{|B|} = [AB : B]$$

de donde se deduce la afirmación del enunciado. □ Q.E.D.

Capítulo 3

Grupos cíclicos

3.1. Definición de grupo cíclico

Definición 3.1.1 *Se dice que un grupo $(G, *)$ es* cíclico *si existe al menos un elemento $a \in G$ tal que $\langle a \rangle = G$. Entonces, se dice que a es un* generador *de G.*

Definición 3.1.2 *Sea $(G, *)$ un grupo. Se define el* orden *de $a \in G$ como* $\text{ord}(a) = |\langle a \rangle|$.

Definición 3.1.3 *Sea $(G, *)$ un grupo. Se dice que $a \in G$ es un* elemento de torsión *de G si* $\text{ord}(a)$ *es finito.*

Proposición 3.1.4 *Sea $(G, *)$ un grupo finito y $a \in G$. Si $n = \text{ord}(a)$, entonces $a^n = e$ y*

$$\langle a \rangle = \{a, a^2, \ldots, a^{n-1}, a^n = e\}$$

siendo distintos todos los elementos de este conjunto.

Demostración. Puesto que $(G, *)$ es un grupo finito, el conjunto $\{x^r : r \in \mathbb{Z}\}$ debe contener repeticiones. Existen, pues, enteros positivos $i < j$ tales que $x^i = x^j$. Entonces,

$$e = x^j * x^{-j} = x^j * x^{-i} = x^{j-i}$$

Tomando n como el menor entero positivo tal que $x^n = e$, veamos que los elementos del conjunto $\{x, x^2, \ldots, x^{n-1}, x^n = e\}$ son todos distintos.

En efecto, si existieran en él dos elementos iguales $x^r = x^s$ con $r < s < n$, se tendra que $x^{s-r} = e$ con $s - r < n$, en contradicción con la definición de n.

□ Q.E.D.

3.2. Propiedades de los elementos de torsión

Proposición 3.2.1 *Sea $(G, *)$ un grupo y $a, b \in G$ elementos de torsión. Se cumplen las siguientes propiedades:*

1. $a^k = e \iff \text{ord}(a)|k$,
2. $\text{ord}(a) = 1 \iff a = e$,
3. $\text{ord}(a^{-1}) = \text{ord}(a)$,
4. $\text{ord}(a^k) = \frac{\text{ord}(a)}{(\text{ord}(a),k)}$ *(donde* (m,n) *denota el máximo común divisor de* m *y* n*)*,
5. *si* $\text{ord}(ab)$ *es finito, entonces* $\text{ord}(ab) = \text{ord}(ba)$*, y*
6. *si* $ab = ba$*, entonces* $\text{ord}(ab)|[\text{ord}(a), \text{ord}(b)]$*; además, si* $\text{ord}(a)$ *y* $\text{ord}(b)$ *son coprimos,* $\text{ord}(ab) = \text{ord}(a)\text{ord}(b)$ *(siendo* $[m,n]$ *el mínimo común múltiple de* m *y* n*).*

Demostración.

1. Sea $k = cn + r : \ c, r \in \mathbb{N}, 0 \leq r < n$. Entonces,
$$x^k = x^{cn+r} = x^{cn}x^r = x^r$$
de donde, necesariamente, ha de ser $r = 0$ y $k = cn$. El recíproco es evidente.
2. Si $\text{ord}(a) = 1$, entonces $a^1 = a = e$. Recíprocamente, si $a = e$, $\langle a \rangle = \{e\}$ y $\text{ord}(a) = |\langle a \rangle| = 1$.
3. Basta observar que $(a^{-1})^m = e \iff (a^m)^{-1} = e \iff a^m = e$.
4. Denotando $n = \text{ord}(a), d = (n,k)$, podemos hacer $n = n'd, k = k'd$. Si $(a^k)^m = a^{km} = e$, se tiene que $n|km$, o equivalentemente, $n'|k'm$. Como $(n', k') = 1$, $n'|m$. Así, $\text{ord}(a^k) = n'$.
5. Sea $m = \text{ord}(ab)$, de modo que $(ab)^m = e$. Entonces,
$$(ab)^m = (ab)(ab)\dots(ab)(ab) = a(ba)\dots(ba)b = e$$
$$\iff (ba)^{m-1} = a^{-1}b^{-1} \iff (ba)^{m-1} = (ba)^{-1} \iff (ba)^m = e$$
6. Si a y b conmutan, se tiene $(ab)^k = a^k b^k$. Por tanto, si $M = [\text{ord}(a), \text{ord}(b)]$, el primer apartado implica que $(ab)^M = a^M b^M = e$ y $M|\text{ord}(ab)$.

   Además, si $n = \text{ord}(a), m = \text{ord}(b), (m,n) = 1$, hacemos $s = \text{ord}(ab)$, y utilizamos los resultados anteriores,
$$(ab)^s = a^s b^s = e \iff a^s = b^{-s} \iff \text{ord}(a^s) = \text{ord}(b^s) \iff$$
$$\iff \frac{n}{(n,s)} = \frac{m}{(m,s)} \Rightarrow n|s, m|s \Rightarrow M|s$$
   Como también $s|M$, se tiene $s = M$.

□ Q.E.D.

3.3. Corolarios del teorema de Lagrange

Corolario 3.3.1 *Para todo $g \in G$ con G finito,* $\mathrm{ord}(g)||G|$

Demostración. Se deduce de la definición del orden de x como $|\langle x\rangle|$. □ Q.E.D.

Corolario 3.3.2 *Sea G un grupo de orden p primo. Entonces G es cíclico.*

Demostración. Sea $g \in G, g \neq e$. Puesto que los únicos divisores de un número primo son la unidad y él mismo, y $\mathrm{ord}(g) = 1$ implicaría $g = e$, se debe tener $|\langle g\rangle| = p$. □ Q.E.D.

3.4. Teoremas de Euler y Fermat

Proposición 3.4.1 *Sea $\bar{a} \in \mathbb{Z}_n^*$. Se dice que $\bar{a}$ es una* unidad de $\mathbb{Z}_n$ *si existe $\bar{b} \in \mathbb{Z}_n^*$ tal que $\bar{a}\bar{b} = \bar{b}\bar{a} = \bar{1}$.*

El conjunto de unidades de $\mathbb{Z}_n$ se denota $U(\mathbb{Z}_n)$, y cumple

$$U(\mathbb{Z}_n) = \{p \in \mathbb{N} : \ p \leq n, \ (p, n) = 1\}$$

Demostración. De la definición, es claro que el inverso multiplicativo de una unidad de $\mathbb{Z}_n$ es también una unidad de $\mathbb{Z}_n$.

Así, sean $\bar{a}, \bar{b} \in U(\mathbb{Z}_n)$ inversos recíprocos. Entonces, $ab \equiv 1 \pmod{n}$, de donde $(ab, n) = (1, n) = 1$ y, por tanto, $(a, n) = (b, n) = 1$.

Recíprocamente, sea $\bar{a} \in \mathbb{Z}_n^*$ tal que $(a, n) = 1$. La ecuación $ax \equiv 1 \pmod{n}$ tiene entonces una solución única hasta congruencia. □ Q.E.D.

Proposición 3.4.2 *$(U(\mathbb{Z}_n), \cdot)$ es un grupo abeliano.*

Demostración. La asociatividad se deduce de la asociatividad del producto de números enteros, y el axioma (G4) es consecuencia directa de la definición de $U(\mathbb{Z}_n)$.

Sean $\bar{a}, \bar{b} \in U(\mathbb{Z}_n)$, y sean $\bar{c}, \bar{d}$ sus respectivos inversos. Entonces,

$$\overline{ab}\,\overline{dc} = \overline{a}\,\overline{bd}\,\overline{c} = \overline{a}\,\overline{1}\,\overline{c} = \overline{ac} = \overline{1}$$
$$\overline{dc}\,\overline{ab} = \overline{d}\,\overline{ca}\,\overline{b} = \overline{d}\,\overline{1}\,\overline{b} = \overline{db} = \overline{1}$$

lo que demuestra que $\overline{ab} \in U(\mathbb{Z}_n)$ y $\overline{1} \in U(\mathbb{Z}_n)$. □ Q.E.D.

Definición 3.4.3 *Se llama función φ de Euler a la aplicación $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ definida según $\varphi(n) = |U(\mathbb{Z}_n)|$*

Proposición 3.4.4 *La función φ de Euler cumple las siguientes propiedades:*

1. *Si $(m, n) = 1$, entonces $\varphi(mn) = \varphi(m)\varphi(n)$,*

2. $\varphi(p^k) = p^{k-1}(p-1)$ *si* p *es primo, y*

3. $\varphi(n) = n\prod(1-\frac{1}{p_i})$, *donde* p_i *son los divisores primos de* n.

Demostración.

1. Consideremos los números $1, 2, 3, \ldots, mn$, y formemos la tabla

$$\begin{array}{ccccccc} 0, & 1, & 2, & \ldots & k, & \ldots & n-1, \\ n, & n+1, & n+2, & \ldots & n+k, & \ldots & 2n-1, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots, \\ (m-1)n, & (m-1)n+1, & (m-1)n+2, & \ldots & (m-1)n+k, & \ldots & mn-1 \end{array}$$

   Si $(mn, 1) = 1$, entonces se debe tener $(m, 1) = (n, 1) = 1$. En cada fila hay $\varphi(n)$ números primos con n. Observando que los números de una misma columna son congruentes entre sí módulo n, deducimos que, si $(k, n) = 1$, entonces todos los números de la k-ésima columna son primos con n.

   Consideremos una de estas columnas con $(k, n) = 1$:

$$n, \quad n+k, \quad 2n+k, \quad \ldots, \quad (m-1)n+k$$

   Estos números pueen considerarse como los valores de la función lineal $nx + k : \ (n, m) = 1$, donde x recorre un sistema completo de restos módulo m,

$$x = 0, 1, 2, \ldots, m-1$$

   Entonces, cada columna de la forma anterior forma un sistema completo de restos módulo m, y, por tanto, contiene $\varphi(m)$ números que son primos con m.

2. Es claro que $\varphi(p) = p - 1$ con p primo. Sea ahora $n = p^k, k > 1$. El sistema completo de restos módulo p^k consta de p^{k-1} sistemas completos de restos módulo p, y en cada uno de ellos hay $\varphi(p)$ números primos con p.

3. Sea $n = \prod p_i^{k_i}$. Utilizando los apartados anteriores,

$$\begin{aligned} \varphi(n) &= \prod \varphi(p_i^{k_i}) = \prod p_i^{k_i-1}(p_i - 1) \\ &= \prod p_i^{k_i}(1 - \frac{1}{p_i}) = n\prod(1 - \frac{1}{p_i}) \end{aligned}$$

□ Q.E.D.

Teorema 3.4.5 (Euler) *Para todos* $a \in \mathbb{Z}, n \in \mathbb{N}$ *tales que* $(a, n) = 1$, *se tiene*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

DEMOSTRACIÓN. Por el teorema de Lagrange, $\text{ord}(a)||U(\mathbb{Z}_n)| = \varphi(n)$, de donde $a^{\varphi(n)} = 1$ en $U(\mathbb{Z}_n)$. □ Q.E.D.

Teorema 3.4.6 (Pequeño Teorema de Fermat) *Para todo $a \in \mathbb{Z}$ y todo $p \in \mathbb{N}$ primo con $p \nmid a$, se tiene*

$$a^{p-1} \equiv 1 \pmod{p}$$

DEMOSTRACIÓN. Aplicando el segundo apartado de la proposición 3.4.4 al teorema de Euler,

$$a^{\varphi(p)} \equiv 1 \pmod{p} \Longrightarrow a^{p-1} \equiv 1 \pmod{p}$$

□ Q.E.D.

3.5. Clasificación de grupos cíclicos

Proposición 3.5.1 *Todo grupo cíclico es abeliano.*

DEMOSTRACIÓN. Puesto que todo elemento de un grupo cíclico $G = \langle g \rangle$ es de la forma g^n para algún $n \in \mathbb{Z}$, se tiene

$$g^i g^j = g^{i+j} = g^{j+i} = g^j g^i$$

□ Q.E.D.

Teorema 3.5.2 (Teorema de clasificación de grupos cíclicos) *Si $(G, *)$ es un grupo cíclico infinito, entonces es isomorfo a $(\mathbb{Z}, +)$*

Si $(H, *)$ es un grupo cíclico de orden finito $|H| = n$, entonces es isomorfo a $(\mathbb{Z}_n, +)$.

DEMOSTRACIÓN. Sea $(G, *)$ un grupo cíclico infinito y $\phi\colon (\mathbb{Z}, +) \longrightarrow (G, *)$ la aplicación dada por $\phi(r) = g^r$. La aplicación ϕ es un homomorfismo, ya que $\phi(r + s) = g^{r+s} = \phi(r) + \phi(s)$, y es evidentemente biyectiva. Por tanto ϕ es un isomorfismo.

Sea $(H, *)$ un grupo cíclico de orden finito $|H| = n$ y $\psi\colon (\mathbb{Z}_n, +) \longrightarrow (H, *)$ la aplicación dada por $\psi(\bar{r}) = g^r$.

Veamos que ψ está bien definida. Sean $r, s \in \mathbb{Z}$ tales que $r \equiv s \pmod{n}$, i.e., $r = s + kn$. Entonces,

$$\psi(\bar{r}) = g^r = g^{s+kn} = g^s = \psi(\bar{s})$$

El mismo argumento prueba que esta aplicación es inyectiva. Además, es un homomorfismo, ya que

$$\psi(\bar{r} + \bar{s}) = g^{r+s} = g^r g^s = \psi(\bar{r})\psi(\bar{s})$$

Puesto que una aplicación inyectiva entre conjuntos con la misma cardinalidad es biyectiva, ψ es un isomorfismo de grupos. □ Q.E.D.

3.6. Subgrupos de grupos cíclicos

Proposición 3.6.1 *Todo subgrupo de un grupo cíclico es cíclico.*

DEMOSTRACIÓN. Sea $G = \langle g \rangle$ un grupo cíclico, y sea $H \leq G$. Es claro que si H es un subgrupo impropio de G es cíclico. Supongamos que H es un subgrupo propio. Sea $g^k \in H$ tal que $g^m \notin H$ para $m < k$, y sea g^s otro elemento de H. Utilizando el algoritmo de división de Euclides, podemos escribir $s = ck + r$ con $0 \leq r < k$. Como H es un subgrupo, $(g^k)^{-1} = g^{-k} \in H$. Por tanto,

$$g^s(g^{-k})^c = g^{s-ck} = g^r \in H$$

en contra de la definición de k, a menos que $r = 0$.

Así, cada elemento de H es de la forma $(g^k)^n$ para algún $n \in \mathbb{Z}$, y H es cíclico generado por g^k. □ Q.E.D.

Proposición 3.6.2 *Sea $G = \langle g \rangle$ un grupo cíclico de orden n. Entonces,*

1. *Para cada divisor d de n, existe un único subgrupo de G de orden d, $\langle g^{\frac{n}{d}} \rangle$.*

2. *Si d y e son divisores de n, entonces la intersección de los subgrupos de órdenes d y e es el subgrupo de orden (d, e).*

3. *Si d y e son divisores de n, entonces el producto interno de los subgrupos de órdenes d y e es el subgrupo de orden $[d, e]$.*

DEMOSTRACIÓN.

1. Es claro que el elemento $g^{\frac{n}{d}}$ tiene d potencias distintas, de donde $\langle g^{\frac{n}{d}} \rangle$ es un subgrupo de orden d. Supongamos que existiese otro subgrupo H de orden d, generado por un elemento $x = g^r$ para algún $r \in \mathbb{Z}$. Entonces, $x^{rd} = e$, por lo que $n | rd$. Así, r debe ser de la forma $k\frac{n}{d}$ para algún $k \in \mathbb{Z}$ y x es una potencia de $g^{\frac{n}{d}}$. Por lo tanto, H debe ser un subgrupo de $\langle g^{\frac{n}{d}} \rangle$, y, puesto que tiene el mismo cardinal, coinciden.

2. Sea $x = g^r \in \langle g^{\frac{n}{d}} \rangle \cap \langle g^{\frac{n}{e}} \rangle$. Como $\frac{n}{d} | r, \frac{n}{e} | r$, se tiene que $[\frac{n}{d}, \frac{n}{e}] | r$. Pero, si $d = d'(d, e), e = e'(d, e)$,

$$\left[\frac{n}{d}, \frac{n}{e}\right] = \frac{n}{(d, e)}\left[\frac{1}{d'}, \frac{1}{e'}\right] = \frac{n}{(d, e)}$$

   Por tanto, $\frac{n}{(d,e)} | r$ y $x \in \langle g^{\frac{n}{(d,e)}} \rangle$.

   Recíprocamente, sea $y = g^s \in \langle g^{\frac{n}{(d,e)}} \rangle$, de modo que $\frac{n}{(d,e)} | s$. Como $\frac{n}{d} | \frac{n}{(d,e)}$ y $\frac{n}{e} | \frac{n}{(d,e)}$, se tiene que $\frac{n}{d} | s$ y $\frac{n}{e} | s$, de donde $y \in \langle g^{\frac{n}{d}} \rangle \cap \langle g^{\frac{n}{e}} \rangle$.

3. Sea $x \in \langle g^{\frac{n}{d}} \rangle \langle g^{\frac{n}{e}} \rangle$. Entonces, existen enteros k_1, k_2 tales que

$$x = g^{k_1 \frac{n}{d} + k_2 \frac{n}{e}} = g^{\frac{n}{de}(k_1 e + k_2 d)}$$

y, evidentemente, $\frac{n}{de}(k_1 e + k_2 d) | \frac{n}{[d,e]}$, de donde $x \in \langle g^{\frac{n}{[d,e]}} \rangle$.

Recíprocamente, sea $y \in \langle g^{\frac{n}{[d,e]}} \rangle$. Entonces, existe un entero k tal que $y = g^{k \frac{n}{[d,e]}}$. Utilizando la ecuación $ab = (a,b)[a,b]$ y la propiedad lineal del máximo común divisor,

$$y = g^{k \frac{n}{[d,e]}} = g^{k \frac{n}{de}(k_1 d + k_2 e)} = g^{k k_2 \frac{n}{d}} g^{k k_1 \frac{n}{e}} \in \langle g^{\frac{n}{d}} \rangle \langle g^{\frac{n}{e}} \rangle$$

□ Q.E.D.

Proposición 3.6.3 *Sea $G = \langle g \rangle$ un grupo cíclico infinito. Entonces,*

1. *Para cada $d \in \mathbb{N}$, existe exactamente un subgrupo de G de índice d, $\langle g^d \rangle$. Además, todo subgrupo no trivial de G es de índice finito.*

2. *Sean $d, e \in \mathbb{N}$. La intersección de los subgrupos de índices d y e es el subgrupo de índice $[d, e]$.*

3. *Sean $d, e \in \mathbb{N}$. El producto interno de los subgrupos de índices d y e es el subgrupo de índice (d, e).*

Demostración.

1. Es claro que $\langle g^d \rangle$ tiene índice d. Basta observar que las clases por la izquierda de G módulo $\langle g^d \rangle$ son $g^k \langle g^d \rangle$ para cada $0 \leq k < d$.

   Supongamos que existiese otro subgrupo $H = \langle g^s \rangle$ de índice d. Entonces, $g^l \langle g^s \rangle$ con $0 \leq k < s$ son las clases por la izquierda de G módulo H, de donde, necesariamente, $s = d$.

2. Es claro que si $x = g^r \in \langle g^d \rangle \cap \langle g^e \rangle$, se debe tener $d|r, e|r$ y, por tanto, $[d, e]|r$ y $x \in \langle g^{[d,e]} \rangle$.

   Recíprocamente, si $y = g^s \in \langle g^{[d,e]} \rangle$, entonces $[d, e]|s$, y, por tanto, $d|s, e|s$, de donde $y \in \langle g^d \rangle \cap \langle g^e \rangle$.

3. Sea $x = g^r \in \langle g^d \rangle \langle g^e \rangle$. Existen, entonces, enteros k_1, k_2 tales que $r = k_1 d + k_2 e$. Es evidente que $(d, e)|s$, de donde $x \in \langle g^{(d,e)} \rangle$.

   Recíprocamente, sea $y = g^s \in \langle g^{(d,e)} \rangle$. Entonces, existe un entero k tal que $s = k(d, e)$. Así, utilizando la propiedad lineal del máximo común divisor,

$$y = g^{k(d,e)} = g^{k k_1 d + k k_2 e} = g^{k k_1 d} g^{k k_2 e} \in \langle g^d \rangle \langle g^e \rangle$$

□ Q.E.D.

3.7. Generadores de grupos cíclicos

Proposición 3.7.1 *Los enteros* 1 *y* -1 *son los únicos generadores del grupo* $(\mathbb{Z}, +)$.

Demostración. Es claro que todo entero n puede ponerse en cualquiera de las dos formas

$$n = n \cdot 1$$
$$n = -n \cdot (-1)$$

de modo que 1 y -1 generan efectivamente $(\mathbb{Z}, +)$. Sin embargo, el elemento 1 no puede ponerse en la forma $1 = m + m + \cdots + m = nm$ con $n \in \mathbb{Z}$ para ningún $m \neq 1, -1$. □ Q.E.D.

Proposición 3.7.2 *Un elemento* g^k *es un generador de un grupo cíclico* $G = \langle g \rangle$ *de orden finito* n *si y sólo si* $(k, n) = 1$.

Demostración. Basta utilizar la proposición 3.2.1, según la cual

$$\text{ord}(g^k) = \frac{\text{ord}(g)}{(k, \text{ord}(g))} = \frac{n}{(k, n)}$$

de donde $\text{ord}(g^k) = n$ si y sólo si $(k, n) = 1$. □ Q.E.D.

Corolario 3.7.3 *Todo grupo cíclico de orden finito* n *tiene* $\varphi(n)$ *generadores*

Demostración. De entre todos los elementos de $G = \langle g \rangle$, sólamente serán generadores aquéllos que sean de la forma $g^k,\ k < n,\ (k, n) = 1$. Este conjunto es $U(\mathbb{Z}_n)$, cuyo cardinal es $\varphi(n)$. □ Q.E.D.

3.8. Imagen homomórfica de grupos cíclicos

Proposición 3.8.1 *Sea* $G = \langle g \rangle$ *un grupo cíclico, y sea* $f : G \longrightarrow G'$ *un homomorfismo. Entonces,* $f(G) = \langle f(g) \rangle$.

Demostración. Basta observar que todo $x \in f(G)$ es de la forma $x = f(g^n) = f(g)^n$. □ Q.E.D.

Proposición 3.8.2 *Sea* a *un elemento de torsión de un grupo* G*, y sea* $f : G \longrightarrow G'$ *un homomorfismo. Entonces,* $\text{ord}(f(a))|\text{ord}(a)$*, con igualdad si* f *es inyectiva.*

Demostración. Sea $a \in G$ tal que $\text{ord}(a) = n,\ \text{ord}(f(a)) = m$. Entonces, $e = f(a^n) = f(a)^n$, de donde $m|n$. Además, si f es inyectiva, $f(a)^m = e$ implica $a^m = e$, y $n|m$. □ Q.E.D.

3.9. Automorfismos de grupos cíclicos

Proposición 3.9.1 *Sea $G \cong (\mathbb{Z}, +)$. Se tiene que*

$$\operatorname{Aut} G \cong \mathbb{Z}_2$$

Demostración. Sea $f : G \longrightarrow G$ un automorfismo, y sea g un generador de G. Puesto que $G = f(G) = \langle f(g) \rangle$, se tiene que $f(g)$ debe ser también un generador. Como G posee únicamente dos generadores, $\operatorname{Aut} G$ es un grupo de orden dos, y, por tanto, isomorfo a $\mathbb{Z}_2$. □ Q.E.D.

Proposición 3.9.2 *Sea $G \cong (\mathbb{Z}_n, +)$. Se tiene que*

$$\operatorname{Aut} G \cong U(\mathbb{Z}_n)$$

Demostración. Sea $f : G \longrightarrow G$ un automorfismo, y sea g un generador de G. Puesto que todo automorfismo es inyectivo, $\operatorname{ord}(f(g)) = \operatorname{ord}(g) = n$, de donde $f(g)$ debe ser también un generador de G. Así,

$$\operatorname{Aut} G = \{f_i : G \longrightarrow G,\ f_i(g) = g^i :\ (i, n) = 1\}$$

Sea $\zeta \colon \operatorname{Aut} G \longrightarrow U(\mathbb{Z}_n)$ definida según $\zeta(f_i) = i$. Utilizando el hecho de que $\operatorname{Aut} G$ es un grupo,

$$\zeta(f_i f_j) = \zeta(f_{ij}) = ij = \zeta(f_i)\zeta(f_j)$$

lo que prueba que ζ es un homomorfismo. Puesto que ζ es evidentemente biyectiva, es un isomorfismo. □ Q.E.D.

Capítulo 4

Acciones de grupos. Subgrupos normales

4.1. El teorema de órbita-estabilizador

Definición 4.1.1 *Sea G un grupo, y X un conjunto. Una* acción de G sobre X *es una familia de aplicaciones*

$$\Phi = \{\phi_g \colon\ X \longrightarrow X :\ g \in G\}$$

que cumple las siguientes propiedades:

(A1) $\phi_e(x) = x$, *y*

(A2) $\phi_a(\phi_b(x)) = \phi_{ab}(x)$.

Definición 4.1.2 *Dada una acción Φ de un grupo G sobre un conjunto X, y un elemento $x \in X$, se llama* estabilizador de x *al conjunto*

$$G_x = \{g \in G :\ \phi_g(x) = x\}$$

Proposición 4.1.3 *En las condiciones de la definición anterior, $G_x \leq G$*

Demostración. El axioma (A1) asegura que el elemento neutro de G pertenece a G_x. (A2) asegura que, si $a, b \in G_x$, entonces,

$$\phi_{ab}(x) = \phi_a(\phi_b(x)) = \phi_a(x) = x$$

por lo que $ab \in G_x$. Por último, si $a \in G_x$, se tiene que

$$\phi_{a^{-1}}(x) = \phi_{a^{-1}}(\phi_a(x)) = \phi_e(x) = x$$

demostrando que $a^{-1} \in G_x$. □ Q.E.D.

Proposición 4.1.4 *Dada una acción Φ de un grupo G sobre un conjunto X, la relación definida según*

$$x \sim_\Phi y \iff \exists g \in G : \ \phi_g(x) = y$$

es de equivalencia.

DEMOSTRACIÓN. El axioma (A1) asegura que $x \sim_\Phi x$.

Si $x \sim_\Phi y$, entonces $\phi_g(x) = y$ para algún $g \in G$. Así,

$$\phi_{g^{-1}}(y) = \phi_{g^{-1}}(\phi_g(x)) = \phi_{g^{-1}g}(x) = \phi_e(x) = x$$

demostrando que $y \sim_\Phi x$.

Por último, si $x \sim_\Phi y,\ y \sim_\Phi z$, entonces $\phi_g(x) = y,\ \phi_h(y) = z$ y

$$z = \phi_h(y) = \phi_h(\phi_g(x)) = \phi_{hg}(x)$$

de donde se deduce la transitividad de la relación. □ Q.E.D.

Definición 4.1.5 *La clase de equivalencia de un elemento $x \in X$ bajo la relación de la proposición anterior recibe el nombre de* órbita de x.

$$\mathrm{orb}(x) = \{y \in X : \ y \sim_\Phi x\}$$

Teorema 4.1.6 (Órbita-estabilizador) *Sea Φ una acción de un grupo G sobre un conjunto X. Para cada $x \in X$,*

$$|\mathrm{orb}(x)| = [G : G_x]$$

DEMOSTRACIÓN. Dado $x \in X$, definimos una aplicación θ de la órbita de x en el conjunto de clases por la izquierda de G módulo G_x según $\theta(\phi_g(x)) = gG_x$.

Comprobemos que θ está bien definida. Supongamos que $\phi_g(x) = \phi_h(x)$. Entonces, $\phi_{h^{-1}g}(x) = x$ y, por tanto, $h^{-1}g \in G_x$, de donde $gG_x = hG_x$.

Veamos que es inyectiva. Si $\theta(\phi_g(x)) = \theta(\phi_h(x))$, se tiene que $gG_x = hG_x$ y $h^{-1}g \in G_x$. Así,

$$\phi_h(x) = \phi_h(\phi_{h^{-1}g}(x)) = \phi_{hh^{-1}g}(x) = \phi_g(x)$$

Por último, θ es suprayectiva, ya que cada gG_x es $\theta(\phi_g(x))$ por definición.

Por tanto, θ es una biyección, y sus conjuntos dominio e imagen poseen el mismo cardinal. □ Q.E.D.

4.2. Elementos conjugados y clases de conjugación

Definición 4.2.1 *Sea G un grupo. Dado $H \leq G$, la acción de H sobre G definida según*

$$\mathrm{Conj}(G,H) = \{\kappa_h \colon G \longrightarrow G,\ \kappa_h(g) = hgh^{-1} :\ h \in H\}$$

recibe el nombre de conjugación de G por H.

La órbita de un elemento $g \in G$ se denomina clase de conjugación de g en H.

$$\mathrm{Cl}_H(g) = \{\kappa_h(g) :\ h \in H\}$$

El estabilizador de $g \in G$ recibe el nombre de centralizador de g en H.

$$C_H(g) = \{h \in H :\ \kappa_h(g) = g\}$$

Proposición 4.2.2 *Sea G un grupo. La familia de aplicaciones que forma la acción* $\mathrm{Conj}(G,H)$ *posee estructura de grupo bajo la operación de composición. Este grupo,* $\mathrm{Int}\, G$ *recibe el nombre* grupo de automorfismos internos de G, *y se tiene*

$$\mathrm{Int}\, G \leq \mathrm{Aut}\, G$$

Demostración. Es claro que $\mathrm{Int}\, G \subseteq \mathrm{Aut}\, G$. El axioma (A2) asegura que $\mathrm{Int}\, G$ es cerrado por la operación de composición. El axioma (A1) asegura la existencia del elemento neutro, κ_e. Por último,

$$(\kappa_{a^{-1}} \circ \kappa_a)(x) = \kappa_{a^{-1}a}(x) = \kappa_e(x)$$
$$(\kappa_a \circ \kappa_{a^{-1}})(x) = \kappa_{aa^{-1}}(x) = \kappa_e(x)$$

asegura la existencia de inversos. □ Q.E.D.

Proposición 4.2.3 *Sea G un grupo, y sean $x, y \in G$. Entonces,*

1. $y \in \mathrm{Cl}_G(x) \iff \exists a, b \in G : x = ab, y = ba$,
2. $y \in \mathrm{Cl}_G(x) \Longrightarrow \mathrm{ord}(x) = \mathrm{ord}(y)$, y
3. G*es abeliano* $\iff \mathrm{Cl}_G(x) = x\ \forall x \in G$.

Demostración. Sea $y = zxz^{-1}$.

1. Haciendo $a = z^{-1}$ y $b = zx$, se tiene $x = ab$ e $y = ba$. Recíprocamente, sea $x = ab$. Entonces, $y = ba = b(ab)b^{-1} = bxb^{-1}$, de modo que $y \in \mathrm{Cl}_G(x)$.
2. Sea $\mathrm{ord}(x) = n,\ \mathrm{ord}(y) = m$. Entonces,

$$y^m = e \iff (zxz^{-1})^m = zx^m z^{-1} = e \iff x^n = e$$

3. Sea G abeliano. Entonces, para cada $x \in G$ se tiene $gxg^{-1} = xgg^{-1} = x$ con $g \in G$. Recíprocamente, si $\mathrm{Cl}_G(x) = x$, entonces $gxg^{-1} = x$ para todos $x, g \in G$, o, equivalentemente, $gx = xg$.

□ Q.E.D.

Proposición 4.2.4

$$C_H(g) = C_G(g) \cap H$$

Demostración. Basta observar que

$$\begin{aligned} C_H(g) &= \{h \in H : \ \kappa_h(g) = g\} \\ &= \{h \in G : \ \kappa_h(g) = g\} \cap H = C_G(g) \cap H \end{aligned}$$

□ Q.E.D.

Definición 4.2.5 *Se llama* centro de G *al subgrupo*

$$Z(G) = \bigcap_{g \in G} C_G(g) = \{g \in G : \ gh = hg \ \forall h \in G\}$$

Proposición 4.2.6 *$Z(G)$ es un subgrupo abeliano de G.*

Demostración. De la propia definición de $Z(G)$ com intersección de subgrupos, se deduce que es un subgrupo, y la caracterización $Z(G) = \{g \in G : gh = hg \ \forall h \in G\}$ demuestra que éste es abeliano.

De hecho, se puede demostrar que $Z(G)$ es el mayor subgrupo abeliano contenido en G, en el sentido de que todo subgrupo abeliano de G está contenido en él, de modo que G es abeliano si y sólo si $G = Z(G)$. □ Q.E.D.

Proposición 4.2.7 (Ecuación de clases de conjugación) *Sea G un grupo finito, y sea $\mathcal{C} = \{x_1, x_2, \ldots, x_m\}$ una colección completa de representantes de clases de conjugación de G en G. Entonces,*

$$|G| = |Z(G)| + \sum_{\substack{x \in \mathcal{C} \\ x \notin Z(G)}} |\mathrm{Cl}(x)|$$

Demostración. G puede escribirse como unión disjunta de clases de conjugación según

$$\begin{aligned} G &= \bigcup_{x \in \mathcal{C}} \mathrm{Cl}(x) \\ &= \bigcup_{\substack{x \in \mathcal{C} \\ x \in Z(G)}} \mathrm{Cl}(x) \cup \bigcup_{\substack{x \in \mathcal{C} \\ x \notin Z(G)}} \mathrm{Cl}(x) \end{aligned}$$

Ahora bien, las clases de conjugación de los elementos de $Z(G)$ constan de un único elemento. Por tanto,

$$\begin{aligned} |G| &= |Z(G)| + |\bigcup_{\substack{x\in\mathcal{C}\\ x\notin Z(G)}} \mathrm{Cl}(x)| \\ &= |Z(G)| + \sum_{\substack{x\in\mathcal{C}\\ x\notin Z(G)}} |\mathrm{Cl}(x)| \end{aligned}$$

□ Q.E.D.

Definición 4.2.8 *Sea G un grupo. Dado $H \leq G$, la acción de H sobre el conjunto de subgrupos de G, denotado $\wp(G)$, definida según*

$$\mathrm{Conj}(\wp(G), H) = \{\chi_h \colon \wp(G) \longrightarrow \wp(G),\ \chi_h(K) = hKh^{-1} :\ h \in H\}$$

recibe el nombre de conjugación de subgrupos de G por H.

La órbita de un subgrupo $K \subseteq G$ se denomina clase de conjugación de K en H.

$$\mathrm{Cl}_H(K) = \{\chi_h(K) :\ h \in H\}$$

El estabilizador de $K \subseteq G$ recibe el nombre de normalizador de K en H.

$$N_H(K) = \{h \in H :\ \chi_h(K) = K\}$$

4.3. Subgrupos normales

Definición 4.3.1 *Sea G un grupo, y sea $H \leq G$. Se dice que H es* normal *en G, y se denota $H \lhd G$ si, para todo $g \in G$, se tiene $gHg^{-1} = H$.*

Proposición 4.3.2 *Son equivalentes:*

1. *H es normal en G.*
2. *Para todo $g \in G$, $gH = Hg$.*
3. *$G = N_G(H)$.*
4. *$\mathrm{Cl}_G(H) = H$.*

Demostración.

(1 ⇒ 2) Componiendo $gHg^{-1} = H$ por la derecha con g, obtenemos $gH = Hg$.

(2 ⇒ 3) El normalizador de H en G es

$$\begin{aligned} N_G(H) &= \{g \in G : \chi_g(H) = H\} \\ &= \{g \in G : gHg^{-1} = H\} \\ &= \{g \in G : Hgg^{-1} = He = H\} \qquad \text{utilizando la hipótesis} \\ &= H \end{aligned}$$

($3 \Rightarrow 4$) Si $G = N_G(H)$, entonces $gHg^{-1} = H$ para todo $g \in G$,de donde $\mathrm{Cl}_G(H) = H$.

($4 \Rightarrow 1$) Sea gHg^{-1} un conjugado de H. Entonces, $gHg^{-1} \in \mathrm{Cl}_G(H) = H$, de donde $gHg^{-1} = H$ y $H \lhd G$. □ Q.E.D.

Proposición 4.3.3 *Sea G un grupo. Entonces,*

1. *$\{e\} \lhd G, G \lhd G$.*
2. *Si $H \leq G$, entonces $H \lhd N_G(H)$.*
3. *Si $H \leq Z(G)$, entonces $H \lhd G$.*
4. *Si $H \leq G$ y G abeliano, entonces $H \lhd G$.*
5. *Si $H \leq G$ y $[G : H] = 2$, entonces $H \lhd G$.*
6. *Si H es el único subgrupo de G de orden n, entonces $H \lhd G$.*

Demostración.

1. Para todo $g \in G$, $g\{e\}g^{-1} = \{e\}$, luego $\{e\} \lhd G$. Para todo $g \in G$, $gGg^{-1} = G$, luego $G \lhd G$.
2. Basta observar el tercer apartado de la proposición 4.3.2. De hecho, $N_G(H)$ es el mayor subgrupo en el cual H es normal, en el sentido de que cualquier otro subgrupo en el que H sea normal debe estar contenido en $N_G(H)$.
3. Si $H \leq Z(G)$, todo $h \in H$ conmuta con todo $g \in G$. Por tanto, $gH = Hg$ y, por el segundo apartado de la proposición 4.3.2, $H \lhd G$.
4. Si G es abeliano, es claro que $gH = Hg$ y $H \lhd G$ por el segundo apartado de la proposición 4.3.2.
5. Si $[G : H] = 2$, las clases por la izquierda y por la derecha de G módulo H deben coincidir: G y $G\backslash H$. Aplicando ahora el segundo apartado de la proposición 4.3.2, $H \lhd G$.
6. Para todo $g \in G$, se tiene $|gHg^{-1}| = |H|$. Puesto que H es el único subgrupo de G de orden n, $gHg^{-1} = H$, demostrando la normalidad de H en G.

□ Q.E.D.

Proposición 4.3.4 *Sean H y K subgrupos de un grupo G. Si $K \lhd G$, entonces $HK \leq G$ y $H \cap K \lhd H$; si además $H \lhd G$, entonces $HK \lhd G$ y $H \cap K \lhd G$.*

DEMOSTRACIÓN. Como $K \lhd G$, se tiene que $hK = Kh$ para todo $h \in G$. En particular, $HK = KH$, y, por la proposición 2.3.2, $HK \leq G$.

Para todo $x \in H \cap K$ y todo $h \in H$, $hxh^{-1} \in H$ por ser H subgrupo de G. Además, puesto que $x \in K$ y K es normal en G, $hxh^{-1} \in K$. Por tanto, $hxh^{-1} \in H \cap K$.

Si tanto H como K son normales en G, sus clases por la izquierda y por la derecha coinciden, de donde, para todo $g \in G$

$$gHKg^{-1} = HgKg^{-1} = HKgg^{-1} = HK$$

demostrando la normalidad de HK en G.

Por último, si $x \in H \cap K$, entonces $gxg^{-1} \in H \cap K$ para todo $g \in G$. □ Q.E.D.

Definición 4.3.5 *Se dice que un grupo G es simple si sus únicos subgrupos normales son sus subgrupos impropios.*

Capítulo 5

Grupos cociente y teoremas de isomorfía

5.1. Grupo cociente y teorema de correspondencia

Proposición 5.1.1 *Sea N un subgrupo normal de un grupo G. El conjunto de clases por la izquierda de G módulo N es un grupo bajo la operación $(xN)(yN) = xyN$. Este grupo recibe el nombre de* grupo cociente de G sobre N *y se denota G/N.*

Demostración. En primer lugar, es necesario comprobar que la operación está bien definida. Si $xN = uN$ e $yN = vN$, entonces, $u^{-1}x, v^{-1}y \in N$ y se tiene

$$\begin{aligned}(uv)^{-1}(xy) &= v^{-1}u^{-1}xy \\ &= v^{-1}ny \qquad\qquad \text{donde } n = u^{-1}x \in N \\ &= v^{-1}y(y^{-1}ny)\end{aligned}$$

Dado que N es normal, $y^{-1}ny \in N$. Como $v^{-1}y \in N$, también $(uv)^{-1}(xy) \in N$ y $xyN = uvN$.

Los axiomas de grupo se cumplen, entonces, de manera evidente: el elemento neutro es $1N = N$, y el inverso de gN es $g^{-1}N$. □ Q.E.D.

Teorema 5.1.2 (Teorema de correspondencia) *Sea N un subgrupo normal de un grupo G. Existe una correspondencia biyectiva entre los subgrupos de G/N y los subgrupos de G que contienen a N. Además, $H \lhd G$ si y sólo si $H/N \lhd G/N$.*

Demostración. Sea $H^\star$ un subgrupo de G/N. Definimos la aplicación β del conjunto de las partes de G/N en el conjunto de las partes de G según

$$\beta(H^\star) = \{g \in G : \ gN \in H^\star\}$$

$\beta(H^\star)$ es un subgrupo de G, ya que es no vacío ($N \subseteq \beta(H^\star)$, pues, para todo $n \in N$ se tiene $nN \in N \in H^\star$ por ser $H^\star \leq G/N$)

$$\begin{aligned} a, b \in \beta(H^\star) &\Longrightarrow aN, b^{-1}N \in H^\star \\ &\Longrightarrow ab^{-1}N \in H^\star \\ &\Longrightarrow ab^{-1} \in \beta(H^\star) \end{aligned}$$

Recíprocamente, sea $N \leq H \leq G$. Definimos la aplicación α del conjunto de las partes de G/N en el conjunto de las partes de G según

$$\alpha(H) = \{hN \in G/N : \ h \in H\} = H/N$$

$\alpha(H)$ es un subgrupo de G/N, ya que es no vacío ($e \in \alpha(H)$) y

$$h_1N, h_2N \in \alpha(H) \Rightarrow h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H \Rightarrow h_1h_2^{-1}N \in \alpha(H)$$

Veamos ahora que tanto α como β son biyecciones, inversas la una de la otra. En efecto, sea $N \leq H \leq G$. Entonces,

$$\beta \circ \alpha(H) = \beta(H/N) = \{g \in G : \ gN \in H/N\} = H$$

Recíprocamente, si $H^\star \leq G/N$, entonces

$$\alpha \circ \beta(H^\star) = \alpha(\{g \in G : \ gN \in H^\star\}) = \{gN \in H^\star\} = H^\star$$

Si $H \lhd G$, entonces $ghg^{-1} \in H$ para todo $g \in G$, de donde

$$(gN)(hN)(gN)^{-1} = (ghg^{-1})N \in H/N \quad \forall gN \in G/N$$

demostrando la normalidad de H/N en G/N. Recíprocamente, si $H/N \lhd G/N$, entonces $(gN)(hN)(gN)^{-1} = (ghg^{-1})N \in H/N$ para todo $gN \in G/N$ implica que $ghg^1 \in H$ para todos $h \in H$ y $g \in G$, de modo que $H \lhd G$. $\square$ Q.E.D.

5.2. Homomorfismos, subgrupos y teoremas de isomorfía

Proposición 5.2.1 *Sean G_1 y G_2 grupos, y $f : G_1 \longrightarrow G_2$ un homomorfismo.*

1. $H_1 \leq G_1 \Longrightarrow f(H_1) \leq G_2$.
2. $H_2 \leq G_2 \Longrightarrow f^{-1}(H_2) \leq G_1$.
3. $H_1 \lhd G_1$ *y* f *suprayectivo* $\Longrightarrow f(H_1) \lhd G_2$.
4. $H_2 \lhd G_2 \Longrightarrow f^{-1}(H_2) \lhd G_1$.

Demostración.

1. Sean $u, v \in f(H_1)$, de modo que existen $x, y \in H_1$ tales que $u = f(x), v = f(y)$. Entonces,

$$uv^{-1} = f(x)f(y)^{-1} = f(xy^{-1}) \in f(H_1)$$

2. Sean $u, v \in H_2$, de modo que existen $x, y \in H_1$ tales que $u = f(x), v = f(y)$. Entonces,

$$uv^{-1} = f(x)f(y)^{-1} = f(xy^{-1}) \in H_2 \Rightarrow xy^{-1} \in f^{-1}(H_2)$$

3. Sea $u \in f(H_1)$, de modo que existe $x \in H_1$ tal que $f(x) = u$. Para todo $v \in G_2$, existe $g \in G_1$ tal que $f(g) = v$, por ser f suprayectiva. Así,

$$vuv^{-1} = f(g)f(x)f(g)^{-1} = f(gxg^{-1}) \in f(H_1)$$

   ya que H_1 es normal, de donde $gxg^{-1} \in H_1$.

4. Sea $x \in f^{-1}(H_2)$, de modo que existe $u \in H_2$ tal que $f(x) = u$. Para todo $g \in G_1$, existe $v \in G_2$ tal que $f(g) = v$. Como $H_2 \lhd G_2$,

$$vuv^{-1} = f(g)f(h)f(g)^{-1} = f(gxg^{-1}) \in H_2$$

   de donde $gxg^{-1} \in f^{-1}(H_2)$ para todo $g \in G_1$, luego $f^{-1}(H_2) \lhd G_1$.

□ Q.E.D.

Teorema 5.2.2 (Primer teorema de isomorfía) *Sean G y H grupos, y $f\colon G \longrightarrow H$ un homomorfismo. Entonces,*

1. $\mathrm{im}f \leq H$,
2. $\ker f \lhd G$, *y*
3. $G/\ker f \cong \mathrm{im}f$.

Demostración.

1. Basta aplicar el primer apartado de la proposición anterior al subgrupo impropio G.
2. Aplíquese el último apartado de la proposición anterior al subgrupo impropio $\{e\}$.
3. Sea $\theta\colon G/N \longrightarrow \mathrm{im}f$ la aplicación tal que $\theta(xN) = f(x)$.

   Supongamos que $xN = yN$, de modo que $x^{-1}y \in N$. Entonces,

$$\theta(xN) = f(x) = f(x)e = f(x)f(x^{-1}y) = f(y) = \theta(yN)$$

   demostrando que θ está bien definida.

El hecho de que f sea un homomorfismo implica que θ también lo es, según

$$\theta((xN)(yN)) = \theta(xyN) = f(xy) = f(x)f(y) = \theta(xN)\theta(yN)$$

Además, es suprayectiva, ya que cada $f(x) \in \mathrm{im} f$ es $\theta(xN)$ por definición, e inyectiva, ya que

$$\begin{aligned}\theta(xN) = \theta(yN) \Rightarrow f(x) = f(y) \Rightarrow f(xy^{-1}) = e \\ \Rightarrow xy^{-1} \in N \Rightarrow xN = yN\end{aligned}$$

Por tanto, θ es un isomorfismo.

□ Q.E.D.

Teorema 5.2.3 (Segundo teorema de isomorfía) *Sean $H \leq G,\ N \lhd G$. Entonces,*

$$\frac{H}{N \cap H} \cong \frac{HN}{N}$$

Demostración. Sea $\varphi\colon G \longrightarrow G/N$ el homomorfismo canónico con núcleo N definido según $\varphi(g) = gN$. Si consideramos la restricción de φ a H, tenemos $\varphi(H) = HN/N$ y $\ker\varphi|_H = H \cap N$. Basta, entonces, aplicar el primer teorema de isomofía a $\varphi|_H$. □ Q.E.D.

Teorema 5.2.4 (Tercer teorema de isomorfía) *Sean $H,\ N \lhd G,\ N \leq H$. Entonces,*

$$\frac{G/N}{H/N} \cong G/H$$

Demostración. Considérese la aplicación $\chi\colon G/N \longrightarrow G/H$ definida según $\chi(gN) = gH$. Se tiene $\mathrm{im}\,\chi = G/H$ y $\ker\chi = H/N$. Basta aplicar ahora el primer teorema de isomorfía. □ Q.E.D.

5.3. Corolarios de los teoremas de isomorfía

Proposición 5.3.1

$$G/Z(G) \cong \mathrm{Int}\, G$$

Demostración. Sea $\xi\colon G \longrightarrow \mathrm{Int}\, G$ la aplicación definida según $\xi(g) = \kappa_g$. Esta aplicación es un homomorfismo, pues

$$\xi(gh)(x) = \kappa_{gh}(x) = [\kappa_g \circ \kappa_h](x) = [\xi(g) \circ \xi(h)](x)$$

y es suprayectiva, ya que κ_g es $\xi(g)$ por definición. Basta ahora aplicar el primer teorema de isomorfía, ya que

$$\begin{aligned}\ker \xi &= \{g \in G : \ \kappa_g = \kappa_e\} \\ &= \{g \in G : \ \kappa_g(x) = \kappa_e(x) \ \forall x \in G\} \\ &= \{g \in G : \ gxg^{-1} = x \ \forall x \in G\} \\ &= Z(G)\end{aligned}$$

□ Q.E.D.

Corolario 5.3.2 *Sea G un grupo. Son equivalentes:*

1. *G es abeliano,*
2. *$\operatorname{Int} G$ es trivial, y*
3. *$\operatorname{Int} G$ es cíclico.*

Demostración.

$(1 \Rightarrow 2)$ Para todos $a, g \in G$, $\kappa_a(g) = aga^{-1} = gaa^{-1} = a$.

$(2 \Rightarrow 3)$ Evidente.

$(3 \Rightarrow 1)$ Supongamos que $\operatorname{Int} G$ es cíclico. Utilizando la proposición anterior, existe un elemento $a \in G$ tal que $G/Z(G) \cong \langle aZ(G)\rangle$. Para todos $x, y \in G$ existen enteros i, j y elementos $b, c \in Z(G)$ tales que $x = a^i b, y = a^j c$. Entonces, $xy = a^i b a^j c$, y, puesto que todos estos elementos conmutan entre sí, $xy = a^i b a^j c = a^j c a^i b = yx$. □ Q.E.D.

Capítulo 6

Grupos simétricos, alternados y diédricos

6.1. Permutaciones. Descomposición en ciclos disjuntos

Definición 6.1.1 *Se llama* grupo simétrico de orden n, S_n, *al grupo de permutaciones del conjunto* $\{1, 2, \ldots, n\}$.

Proposición 6.1.2

$$|S_n| = n!$$

Demostración. Existen $n!$ permutaciones en un conjunto de n elementos. □ Q.E.D.

Proposición 6.1.3 *Sean* $\pi \in S_n$, *e* $i \in \{1, 2, \ldots, n\}$. *Si* k *es el menor entero positivo tal que* $\pi^k(i) \in \{i, \pi(i), \ldots, \pi^{k-1}(i)\}$, *entonces* $\pi^k(i) = i$.

Demostración. Supongamos que $\pi^k(i) = \pi^r(i)$ para algún $0 < r < k$. Entonces, $\pi^{k-r}(i) = i$, en contra de la definición de k. Por tanto, $r = 0$. □ Q.E.D.

Definición 6.1.4 *Una permutación* ρ *se llama* k-ciclo *si existen* $k \in \mathbb{N}$ *e* $i \in \{1, 2, \ldots, n\}$ *tales que*

- k *es el menor entero positivo tal que* $\rho^k(i) = i$, *y*
- $\rho(j) = j$ *para todo* $j \notin \{i, \rho(i), \ldots, \rho^{k-1}(i)\}$.

Se denota entonces $\rho = (i\rho(i) \ldots \rho^{k-1}(i))$. *Un 2-ciclo recibe el nombre de* transposición.

Proposición 6.1.5 *Sea* ρ *un* k*-ciclo. Entonces,* $\mathrm{ord}(\rho) = k$.

DEMOSTRACIÓN. Basta observar que ρ un k-ciclo si k es el mínimo entero positivo tal que $\rho^k(i) = i$, por la proposición 6.1.3. □ Q.E.D.

Definición 6.1.6 *Se dice que ρ, σ son* permutaciones disjuntas *si no existe $i \in \{1, 2, \ldots, n\}$ tal que $\rho(i) \neq i$ y $\sigma(i) \neq i$.*

Proposición 6.1.7 *Toda permutación puede escribirse como producto de ciclos disjuntos.*

DEMOSTRACIÓN. Sea $\sigma \in S_n$. Definamos una relación en $\{1, 2, \ldots, n\}$ según

$$iRj \iff \exists k \in \mathbb{N} : \ \sigma^k(i) = j$$

Esta relación es de equivalencia.

iRi, i.e., existe $r \in \mathbb{N}$ tal que $\sigma^r(i) = i$, ya que, en caso contrario, el conjunto $\{\sigma^k(i) : \ k \in \mathbb{N}\}$ sería infinito. Si iRj, entonces existe $k \in \mathbb{N}$ tal que $\sigma^k(i) = j$, de donde $i = \sigma^r(i) = \sigma^{r-k}\sigma^k(i) = \sigma^{r-k}(j)$. Por último, si iRj y jRk, se tienen $k, m \in \mathbb{N}$ tales que $\sigma^k(i) = j$ y $\sigma^m(j) = k$, de donde $\sigma^{k+m}(i) = k$.

Por la proposición 6.1.3, cada una de las clases de equivalencia de esta relación es un ciclo. La disjunción de estas clases implica la disjunción de los ciclos. □ Q.E.D.

Proposición 6.1.8 *Sean ρ, σ permutaciones disjuntas. Entonces $\rho\sigma = \sigma\rho$, y, para todo $k \in \mathbb{N}$, $(\rho\sigma)^k = \rho^k\sigma^k$.*

DEMOSTRACIÓN. Sea $i \in \{1, 2, \ldots, n\}$ que queda fijo por ρ. Entonces, $\sigma^r(i)$ queda también fijo por ρ, de donde $\rho\sigma(i) = \sigma(i) = \sigma\rho(i)$.

Anlogamente, si $j \in \{1, 2, \ldots, n\}$ queda fijo por σ, $\rho^r(j)$ queda también fijo por σ y $\rho\sigma(j) = \rho(j) = \sigma\rho(j)$.

Por último, si $k \in \{1, 2, \ldots, n\}$ queda fijo por ambas, es evidente que $\rho\sigma(k) = \sigma\rho(k) = k$.

Si ρ y σ conmutan, es evidente entonces que $(\rho\sigma)^k = \rho^k\sigma^k$ para todo $k \in \mathbb{N}$. □ Q.E.D.

Corolario 6.1.9 *Sean ρ, σ permutaciones disjuntas. Entonces,*

$$\text{ord}(\rho\sigma) = [\text{ord}(\rho), \text{ord}(\sigma)]$$

DEMOSTRACIÓN. Si $(\rho\sigma)^m = \rho^m\sigma^m = e$, entonces $\rho^m = e; \sigma^m = e$, por ser permutaciones disjuntas. Así $m = \text{ord}(\rho\sigma)$ es el mínimo entero positivo tal que $\text{ord}(\rho)|m$ y $\text{ord}(\sigma)|m$, es decir, $m = [\text{ord}(\rho), \text{ord}(\sigma)]$. □ Q.E.D.

6.2. Descomposición en transposiciones. Sistemas de generadores de S_n

Proposición 6.2.1 *Todo k-ciclo en S_n puede descomponerse en un producto de $k-1$ transposiciones.*

DEMOSTRACIÓN. Basta observar que el k-ciclo $\pi = (12\dots k)$ admite la factorización $\pi = (1k)\dots(13)(12)$, de donde

$$(i_1 i_2 \dots i_k) = (i_1 i_k)\dots(i_1 i_3)(i_1 i_2)$$

□ Q.E.D.

Corolario 6.2.2 *Las transposiciones generan S_n.*

DEMOSTRACIÓN. Evidente de la proposición anterior □ Q.E.D.

Proposición 6.2.3 *Sean $\rho, \pi \in S_n$. La descomposición en ciclos disjuntos de $\pi\rho\pi^{-1}$ se obtiene de la de ρ sustituyendo cada entero i en la descomposición de ρ por el entero $\pi(i)$.*

DEMOSTRACIÓN. En efecto, $\pi\rho\pi^{-1}(\pi(i)) = \pi\rho(i)$. Por tanto, $\pi\rho\pi^{-1}$ aplica $\pi(i)$ en $\pi(\rho(i))$, mientras que ρ aplica i en $\rho(i)$. □ Q.E.D.

Corolario 6.2.4 *Para todo $n \in \mathbb{N}$, las transposiciones de la forma $(k\ k+1)$ con $1 \leq k \leq n-1$ generan S_n.*

DEMOSTRACIÓN. Veamos que toda transposición (ij) con $i < j$ puede escribirse como producto de transposiciones de la forma $(k\ k+1)$. Utilizando la proposición anterior, vemos que

$$(i\ i+2) = (i+1\ i+2)(i\ i+1)(i+1\ i+2)^{-1}$$

En general,

$$(ij) = (j-1\ j)(j-2\ j-1)\dots(i+1\ i+2)(i\ i+1)$$
$$(i+1\ i+2)^{-1}\dots(j-2\ j-1)^{-1}(j-1\ j)^{-1}$$

Basta ahora utilizar las proposiciones 6.2.1 y 6.1.7. □ Q.E.D.

6.3. Signatura de una permutación

Proposición 6.3.1 *Sea F_n el conjunto de los polinomios en n variables, y sea Ξ la familia de aplicaciones $\xi_\sigma : F_n \longrightarrow F_n$ con $\sigma \in S_n$ definidas según*

$$\xi_\sigma(f(x_1, x_2, \dots, x_n)) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$$

Ξ es una acción de S_n sobre F_n.

DEMOSTRACIÓN. En efecto, si denotamos I la permutación identidad,

$$\xi_I(f(x_1, x_2, \ldots, x_n)) = f(x_1, x_2, \ldots, x_n)$$

verificando (A1). Para comprobar (A2), basta observar que

$$\begin{aligned}\xi_\rho \circ \xi_\sigma(f(x_1, x_2, \ldots, x_n)) &= \xi_\rho(f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})) \\ &= f(x_{\rho\sigma(1)}, x_{\rho\sigma(2)}, \ldots, x_{\rho\sigma(n)}) \\ &= \xi_{\rho\sigma}(f(x_1, x_2, \ldots, x_n))\end{aligned}$$

□ Q.E.D.

Proposición 6.3.2 *Si*

$$\Delta_n = \prod_{1 \le i < j \le n} (x_i - x_j) \in F_n$$

se define la signatura de σ *como la aplicación* $\operatorname{sgn}\colon S_n \longrightarrow \{-1, 1\}$ *definida según*

$$\operatorname{sgn}(\sigma)\Delta_n = \xi_\sigma(\Delta_n)$$

Esta aplicación sgn *es un homomorfismo.*

DEMOSTRACIÓN. Es claro que, para todo $\lambda \in \mathbb{R}$, $\xi_\sigma(\lambda f) = \lambda \xi_\sigma(f)$. Por tanto, utilizando la proposición anterior,

$$\begin{aligned}\operatorname{sgn}(\rho\sigma)\Delta_n &= \xi_{\rho\sigma}\Delta_n && \text{por definición} \\ &= \xi_\rho \circ \xi_\sigma(\Delta_n) && \text{por el axioma (A2)} \\ &= \xi_\rho(\operatorname{sgn}(\sigma)\Delta_n) && \text{por definición} \\ &= \operatorname{sgn}(\sigma)\xi_\rho(\Delta_n) \\ &= \operatorname{sgn}(\sigma)\operatorname{sgn}(\rho)\Delta_n && \text{por definición}\end{aligned}$$

□ Q.E.D.

Definición 6.3.3 *Se dice que $\sigma \in S_n$ es una permutación par si* $\operatorname{sgn}(\sigma) = 1$. *Se dice que $\sigma \in S_n$ es una permutación impar si* $\operatorname{sgn}(\sigma) = -1$.

Corolario 6.3.4 *Sean $\pi, \sigma \in S_n$. Entonces,*

1. $\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$, *y*
2. $\operatorname{sgn}(\pi\sigma\pi^{-1}) = \operatorname{sgn}(\sigma)$.

DEMOSTRACIÓN. Utilizando que sgn es un homomorfismo,

$$1 = \operatorname{sgn}(I) = \operatorname{sgn}(\pi\pi^{-1}) = \operatorname{sgn}(\pi)\operatorname{sgn}(\pi^{-1})$$

de donde $\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$, y

$$\operatorname{sgn}(\pi\sigma\pi^{-1}) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)\operatorname{sgn}(\pi) = \operatorname{sgn}(\sigma)$$

□ Q.E.D.

Corolario 6.3.5 *Sea σ un k-ciclo. Entonces,* $\operatorname{sgn}(\sigma) = (-1)^{k-1}$

Demostración. Es claro que la transposición (12) es impar, puesto que produce un único cambio de signo en Δ_n, la del factor $(x_1 - x_2)$. Una transposición de la forma $(1k)$ puede escribirse como

$$(1k) = (2k)(12)(2k)^{-1}$$

luego es impar por el corolario 6.3.4. Finalmente,

$$(lk) = (1l)(1k)(1l)^{-1}$$

por lo queda demostrado que toda transposición es impar.

Por la proposición 6.2.1, todo k-ciclo puede factorizarse en un producto de $k-1$ transposiciones. Del hecho de que sgn es un homomorfismo se sigue el enunciado. □ Q.E.D.

Proposición 6.3.6 *Sea $\sigma \in S_n$ una permutación par. Entonces, toda descomposición de σ en transposiciones posee un número par de transposiciones.*

Anlogamente, si $\sigma \in S_n$ es una permutación impar, toda descomposición de σ en transposiciones posee un número impar de transposiciones.

Demostración. Supongamos que $\sigma \in S_n$ posee dos factorizaciones distintas con k y l transposiciones, respectivamente. Entonces, las signaturas de cada una de ellas debe coincidir con la signatura de σ. Así, si σ es par,

$$\operatorname{sgn}(\sigma) = 1 = (-1)^k = (-1)^l$$

de manera que tanto k como l deben ser pares. Análogamente, si σ es impar,

$$\operatorname{sgn}(\sigma) = -1 = (-1)^k = (-1)^l$$

y k y l deben ser impares. □ Q.E.D.

6.4. Grupos alternados

Definición 6.4.1 *Se llama* grupo alternado de orden n, A_n *al subgrupo de todas las permutaciones pares de S_n.*

Proposición 6.4.2 $A_n = \ker(\operatorname{sgn})$.

Demostración. En efecto,

$$\ker(\operatorname{sgn}) = \{\sigma \in S_n : \ \operatorname{sgn}(\sigma) = 1\}$$

es efectivamente el conjunto de todas las permutaciones pares de S_n. □Q.E.D.

Corolario 6.4.3

1. $A_n \lhd S_n$.
2. $|A_n| = \frac{n!}{2}$.

DEMOSTRACIÓN. Por el primer teorema de isomorf´a, aplicado al homomorfismo sgn, $A_n \lhd S_n$ y $S_n/A_n \cong \{-1, 1\}$. Aplicando ahora el teorema de Lagrange,

$$|A_n| = \frac{|S_n|}{[S_n : A_n]} = \frac{|S_n|}{|S_n/A_n|} = \frac{n!}{2}$$

□ Q.E.D.

Proposición 6.4.4

1. $A_2 = I$.
2. $A_3 \cong \mathbb{Z}_3$.

DEMOSTRACIÓN.

1. Es evidente del hecho de que $S_2 = \{I, (12)\}$.
2. Puesto que $S_3 = \{I, (12), (13), (23), (123), (132)\}$, se tiene que $A_3 = \{I, (123), (132)\}$. Pero

   $$(123)(123) = (132)(123)(123)(123) = I$$

   Así, A_3 es un grupo cíclico de orden 3, y, por tanto, isomorfo a $\mathbb{Z}_3$.

□ Q.E.D.

Proposición 6.4.5 *Para cada $n \geq 3$, los 3-ciclos generan A_n.*

DEMOSTRACIÓN. De la propia definición de grupo alternado, cada permutación de A_n puede escribirse como producto de un número par de transposiciones. Agrupando las transposiciones por pares, $(ij)(kl)$, se tienen dos casos. Si i, j, k, l son enteros distintos,

$$(ij)(kl) = (ikj)(ikl)$$

Si alguno de ellos coincide,

$$(ij)(il) = (ilj)$$

Por tanto, todo elemento de A_n con $n \geq 3$ puede escribirse como producto de 3-ciclos. □ Q.E.D.

Corolario 6.4.6 *Para cada par $r_0, s_0 \in \{1, 2, \ldots, n\}$ con $r_0 \neq s_0$, los 3-ciclos de la forma $(r_0 s_0 i)$ generan A_n.*

DEMOSTRACIÓN. El resultado se sigue de la proposición anterior, observando que

$$(ijk) = (r_0 ij)(r_0 jk)$$
$$(r_0 jk) = (r_0 s_0 j)(r_0 s_0 i)(r_0 s_0 i)$$

□ Q.E.D.

6.5. Estructura de los grupos simétricos y alternados

Proposición 6.5.1 *Sean $n, m \in \mathbb{N}$ tales que $n \leq m$. Entonces,*

1. *$S_n \leq S_m$, y*
2. *$A_n \leq A_m$.*

DEMOSTRACIÓN. Basta ver que $S_n \subseteq S_m$ y $A_n \subseteq A_m$, y que S_n y A_n poseen estructura de grupo. □ Q.E.D.

Proposición 6.5.2 *S_n es no abeliano para $n \geq 3$.*

DEMOSTRACIÓN. S_3 no es conmutativo, ya que $(12), (13) \in S_3$ y

$$(12)(13) = (132)$$
$$(13)(12) = (123)$$

Como $S_3 \leq S_n$ para $n \geq 3$, S_n es no abeliano para $n \geq 3$. □ Q.E.D.

Proposición 6.5.3 *A_n es no abeliano para $n \geq 4$.*

DEMOSTRACIÓN. A_4 no es conmutativo, ya que $(123), (134) \in A_4$ y

$$(123)(134) = (234)$$
$$(134)(123) = (124)$$

Como $A_4 \leq A_n$ para $n \geq 4$, A_n es no abeliano para $n \geq 4$. □ Q.E.D.

Proposición 6.5.4 *Para $n \geq 3$, $Z(S_n) = I$.*

DEMOSTRACIÓN. Sea $\sigma \in S_n,\ \sigma \neq I$. Entonces, existen $i, j \in 1, 2, \ldots, n$ tales que $\sigma(i) = j \neq i$. Sea $k \in 1, 2, \ldots, n$ distinto de i y de j, y sea $\tau = (jk)$. Entonces,

$$\sigma\tau(i) = \sigma(i) = j$$
$$\tau\sigma(i) = \tau(j) = k$$

Por tanto, $Z(S_n) = I$. □ Q.E.D.

Proposición 6.5.5 *Para $n \geq 4$, $Z(A_n) = I$.*

DEMOSTRACIÓN. Sea $\sigma \in A_n,\ \sigma \neq I$. Entonces, existen $i, j \in 1, 2, \ldots, n$ tales que $\sigma(i) = j \neq i$. Sea $k, l \in 1, 2, \ldots, n$ distintos de i y de j, y sea $\tau = (jkl)$. Entonces,

$$\sigma\tau(i) = \sigma(i) = j$$
$$\tau\sigma(i) = \tau(j) = k$$

Por tanto, $Z(A_n) = I$. □ Q.E.D.

Corolario 6.5.6 *S_n y A_n no tienen subgrupos normales de orden dos.*

DEMOSTRACIÓN. A_3 no puede tener subgrupos de orden dos, pues contradiría el teorema de Lagrange, ya que $|A_3| = 3$.

En el resto de casos, el centro de los grupos considerados es el subgrupo trivial. Supongamos, entonces, que existiese un subgrupo normal de orden dos, $H = \{e, a\}$. Para cualquier elemento $b \neq a$ del grupo considerado, se tendría $bab^{-1} = a$, o, equivalentemente, $ab = ba$, en contra de que el centro del grupo es trivial. □ Q.E.D.

6.6. Teorema de Abel

Proposición 6.6.1 *Sea $N \lhd A_n$ con $n \geq 3$. Si N contiene un 3-ciclo, entonces $N = A_n$.*

DEMOSTRACIÓN. Sea $(r_0 s_0 i) \in N$. Entonces todo 3-ciclo de la forma $(r_0 s_0 j)$ pertenece a N, ya que

$$((ij)(r_0 s_0))^{-1}(r_0 s_0 i)^2((ij)(r_0 s_0)) = (r_0 s_0 j)$$

y N es normal. Así,

$$\langle (r_0 s_0 i), (r_0 s_0 j), ... \rangle \subseteq N$$

Pero, por el corolario 6.4.6, el primer miembro de la última inclusión es A_n. □ Q.E.D.

Proposición 6.6.2 *A_5 es simple.*

DEMOSTRACIÓN. Sea $N \lhd A_5,\ N \neq \{I\}$, y sea $\sigma \in N,\ \sigma \neq I$. Se tienen tres casos:

1. $\sigma = (ab)(cd)$: tomando un entero e distinto de a, b, c, d, sea $\rho = (abe) \in A_n$. Entonces,
$$\sigma[\rho\sigma\rho^{-1}] = (abe) \in N$$
por ser N un subgrupo normal de A_n.

2. $\sigma = (abc)$.

3. $\sigma = (abcde)$: puesto que N es un subgrupo normal,
$$\sigma^{-1}[(abc)\sigma(abc)^{-1}] = (ace) \in N$$

Así pues, aplicando la proposición anterior, se debe tener $N = A_n$. □ Q.E.D.

Teorema 6.6.3 (Abel) *A_n es simple si $n \geq 5$.*

DEMOSTRACIÓN. Según la proposición anterior, A_5 es simple. Supongamos que A_k es simple para todo $5 \leq k \leq n-1$.

Sea $N \lhd A_n,\ N \neq \{I\}$. Veamos que existe una permutación $\sigma \in N,\ \sigma \neq I$ tal que $\sigma(i) = i$ para algún $i \in \{1, 2, \ldots, n\}$.

Supongamos que no existiese tal σ. Sea $\pi \in A_n$. Entonces existen tres enteros distintos $a, b, c \in \{2, \ldots, n\}$ tales que $\pi(1) = a,\ \pi(b) = c$. Si $\rho = (1a)(bcde)$, entonces $(\rho\pi\rho^{-1})\sigma \in N$, por ser N normal. Pero

$$(\rho\pi\rho^{-1})\pi(1) = 1$$
$$(\rho\pi\rho^{-1})\pi(c) = d$$

de manera que $(\rho\pi\rho^{-1})\pi$ fija 1 y no es la permutación identidad, en contra de la hipótesis.

Así pues, sea $G(i) = \{\sigma \in A_n :\ \sigma(i) = i\} \cong A_{n-1}$, que es simple por la hipótesis de inducción. Entonces, $N(i) = N \cap G(i)$, que es un subgrupo normal de $G(i)$, debe ser $N(i) = G(i)$.

Por tanto, todo subgrupo normal de A_n contiene a A_5, de donde debe también contener un 3-ciclo. Por el corolario 6.4.6, se tiene entonces $N = A_n$.
□ Q.E.D.

6.7. Teorema de Cayley

Teorema 6.7.1 (Cayley) *Todo grupo G es isomorfo a un subgrupo del grupo de las biyecciones de G. En particular, si G es finito, G es isomorfo a un subgrupo de un grupo de permutaciones.*

DEMOSTRACIÓN. Sea F una aplicación que asigna a cada $g \in G$ la aplicación $F_g \colon G \longrightarrow G$ definida según $F_g(x) = gx$. Cada F_g es inyectiva, pues

$$F_g(x) = F_g(y) \Longrightarrow gx = gy \Longrightarrow x = y$$

y también suprayectiva, ya que $x = F_g(g^{-1}x)$. Así, $F : G \longrightarrow B(G)$, donde $B(G)$ es el grupo de las biyecciones de G con la operación de composición.

F es un homomorfismo, puesto que

$$F_{gh}(x) = ghx = F_g(hx) = F_g \circ F_h(x)$$

Además, $\ker f = \{e\}$. Por el primer teorema de isomorfía, G es isomorfo a su imagen, que es un subgrupo de $B(G)$. □ Q.E.D.

6.8. Grupos diédricos

Definición 6.8.1 *Se llama* grupo diédrico de orden $2n$, D_{2n} *al grupo de simetrías de un polígono regular de n lados.*

Proposición 6.8.2 *Sea A la rotación de ángulo $\frac{2\pi}{n}$ alrededor del centro de un polígono regular de n lados, y sea B la simetría con respecto a la recta que pasa por el centro del mismo y por uno cualquiera de sus vértices. Entonces,*

$$A, A^2, \ldots, A^n; A \circ B, A^2 \circ B, \ldots, A^n \circ B$$

son todas las simetrías del polígono, i.e.,

$$D_{2n} = \{A, A^2, \ldots, A^n; A \circ B, A^2 \circ B, \ldots, A^n \circ B\}$$

DEMOSTRACIÓN. Los movimientos del plano que dejan invariante un polígono regular de n lados, es decir, sus simetrías, son:

- Las rotaciones de ángulo $k\frac{2\pi}{n}$ para $k \in \mathbb{Z}$:
  Como la composición de giros alrededor de un centro común es también un giro alrededor del mismo centro, estas rotaciones están generadas por el giro A. Puesto que $A^n = I$, se tiene $\text{ord}(A) = n$ y

  $$\langle A \rangle = \{A, A^2, \ldots, A^n = I\}$$

  es el conjunto de rotaciones que dejan invariante el citado polígono.

- Las simetrías con respecto a cada una de las rectas que pasan por el centro del polígono y por uno de sus vértices, o por el centro del polígono y por el punto medio de uno de sus lados:
  Numerando los vértices con los n primeros números naturales, el giro A viene determinado poer las ecuaciones

  $$\begin{aligned} &A(n) = 1 \\ &A(i) = i + 1 \qquad\qquad \text{para todo } 1 \leq i < n \end{aligned}$$

Si elegimos B como la simetría con respecto a la recta que pasa por el centro y por el vértice 1, entonces

$$\begin{aligned} B(1) &= 1 \\ B(i) &= n - i + 2 \qquad \text{para todo } 1 < i \leq n \end{aligned}$$

Veamos que $A \circ B$ es también una simetría con respecto a una recta. En efecto,

$$\begin{aligned} A \circ B(1) &= 2 \\ A \circ B(2) &= 1 \\ A \circ B(i) &= n - i + 3 \qquad \text{para todo } 3 \leq i \leq n \end{aligned}$$

son las ecuaciones de la simetría con respecto a la recta que pasa por el centro y por el punto medio del lado que determinan los vértices 1 y 2.

Análogamente, puede mostrarse que el resto de composiciones de la forma $A^k \circ B$ son simetrías con respecto a rectas. Éstas, junto con B, son las n simetrías con respecto a rectas del polígono regular de n lados.

□ Q.E.D.

Proposición 6.8.3 *En las condiciones de la proposición anterior,*

$$A \circ B = B \circ A^{-1}$$

Demostración. El movimiento A^{-1} viene dado por las ecuaciones

$$\begin{aligned} A^{-1}(1) &= n \\ A^{-1}(i) &= i - 1 \qquad \text{para todo } 1 < i \leq n \end{aligned}$$

Entonces,

$$\begin{aligned} B \circ A^{-1}(1) &= 2 \\ B \circ A^{-1}(2) &= 1 \\ B \circ A^{-1}(i) &= n - i + 3 \qquad \text{para todo } 2 < i \leq n \end{aligned}$$

ecuaciones que coinciden con las de $A \circ B$, dadas en la demostración de la proposición anterior. □ Q.E.D.

Proposición 6.8.4 *El grupo diédrico D_{2n} es isomorfo a un subgrupo de S_n.*

Demostración. En efecto, basta definir el homomorfismo inyectivo $F : D_n \longrightarrow S_n$ según

$$\begin{aligned} F(A) &= (12 \ldots n) \\ F(B) &= (2\, n)(3\, n-1) \ldots \end{aligned}$$

□ Q.E.D.

Capítulo 7

Producto directo y semidirecto

7.1. Producto directo de grupos

Proposición 7.1.1 *Sean $G_i,\ i = 1, 2, \ldots, n$ grupos. El producto cartesiano $G_1 \times G_2 \times \ldots \times G_n$ dotado de la operación*

$$(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n')$$

posee estructura de grupo, y recibe el nombre de producto directo *de los grupos $G_i,\ i = 1, 2, \ldots, n$.*

Demostración. La operación interna y la asociatividad son evidentes de la estructura de grupo de G y H. El elemento neutro de $G \times H$ es $(e_1, e_2, \ldots, e_n)$. El elemento inverso de $(g_1, g_2, \ldots, g_n)$ es $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$. □ Q.E.D.

Proposición 7.1.2 *Sean G y H grupos. Entonces,*

1. *$G \times H \cong H \times G$,*
2. *$G \cong \underline{G} = \{(g, e_H) :\ g \in G\}$, y*
3. *$\underline{G} \lhd G \times H$.*

Demostración.

1. Basta considerar la aplicación $\varphi : G \times H \longrightarrow H \times G$ definida según $\varphi(g, h) = (h, g)$, que es claramente un isomorfismo.
2. Basta considerar la aplicación $\psi_1 : G \longrightarrow \underline{G}$ definida según $\psi_1(g) = (g, e_H)$, que es de nuevo un isomorfismo.
3. Si consideramos la proyección canónica sobre la segunda componente $\pi_2 : G \times H \longrightarrow H$ definida según $\pi_2(g, h) = h$, podemos observar que $\ker \pi_2 = \underline{G}$, de modo que, por el primer teorema de isomorfía, $\underline{G} \lhd G \times H$.

□ Q.E.D.

Proposición 7.1.3 *Sea G un grupo, y sean $M, N \lhd G$. Si $M \cap N = \{e\}$, y $MN = G$, entonces $G \cong M \times N$.*

Demostración. Puesto que $G = MN$, para cada $g \in G$ existen $n \in N,\ m \in M$ tales que $g = mn$. Como $M \cap N = \{e\}$, esta representación debe ser única. En efecto, si $mn = m'n'$, entonces $(m')^{-1}m = n'n^{-1} \in M \cap N$, de donde $m = m'$ y $n = n'$. Así, la aplicación $f : G \longrightarrow M \times N$ tal que $f(g) = (m, n)$ está bien definida y es biyectiva.

Falta comprobar que f es un homomorfismo de grupos. Para ello, basta observar que si $n \in N,\ m \in M$, se cumple $nm = mn$, ya que la normalidad de M y N implican

$$n^{-1}m^{-1}nm = n^{-1}(m^{-1}nm) \in NN = N$$
$$n^{-1}m^{-1}nm = (n^{-1}m^{-1}n)m \in MM = M$$

y puesto que $M \cap N = \{e\}$, se debe tener $n^{-1}m^{-1}nm = e$. Entonces, si $g = mn,\ g' = m'n'$,

$$\begin{aligned}
f(gg') &= f((mn)(m'n')) && \text{por la definición de } f \\
&= f(m(nm')n') && \text{por la propiedad asociativa} \\
&= f(m(m'n)n') \\
&= f((mm')(nn')) && \text{por la propiedad asociativa} \\
&= (mm', nn') && \text{por la definición de } f \\
&= (m, n)(m', n') && \text{por la definición de producto directo} \\
&= f(g)f(g')
\end{aligned}$$

□ Q.E.D.

Proposición 7.1.4 *Un grupo G es isomorfo al producto directo de sus subgrupos $H_i,\ i = 1, 2, \ldots, n$ si*

1. *$H_j \lhd G$ para cada $j = 1, 2, \ldots, n$,*
2. *$H_j \cap (\prod_{i \neq j} H_i) = \{e\}$ para cada $j = 1, 2, \ldots, n$, y*
3. *$\prod_{i=1}^{n} H_i = G$.*

Demostración. Debido a la condición tercera, para cada $g \in G$ existen $h_j \in H_j,\ j = 1, 2, \ldots, n$ tales que $g = h_1 h_2 \ldots h_n$. Esta descomposición es única, ya que, si $h_1 h_2 \ldots h_n = (h'_1 h'_2 \ldots h'_n)$, entonces

$$(h'_1)^{-1} h_1 = (h'_2 \ldots h'_n)(h_1 \ldots h_n)^{-1}$$

De la normalidad de los H_j se sigue que el segundo miembro pertenece a $\prod_{i\neq 1} H_i$, y, como el primero pertenece a H_1, la segunda condición del enunciado nos lleva a que $h_1 = h_1'$. Continuando con este argumento, se llega a que $h_j = h_j'$ para todo $j \in \{1, 2, \ldots, n\}$.

Así, podemos definir la aplicación $f\colon G \longrightarrow H_1 \times \ldots \times H_n$ según

$$f(g) = (h_1, h_2, \ldots, h_n)$$

Esta aplicación es evidentemente biyectiva, y es un homomorfismo, pues, si $g = h_1 h_2 \ldots h_n$ y $g' = h_1' h_2' \ldots h_n'$,

$$\begin{aligned} f(gg') &= (h_1 h_1', h_2 h_2', \ldots, h_n h_n') \\ &= (h_1, h_2, \ldots, h_n)(h_1', h_2', \ldots, h_n') \\ &= f(g) f(g') \end{aligned}$$

□ Q.E.D.

Proposición 7.1.5 *Sea $A \lhd G$, $B \lhd H$. Entonces, $A \times B \lhd G \times H$ y*

$$\frac{G \times H}{A \times B} \cong \frac{G}{A} \times \frac{H}{B}$$

Demostración. Si $\varphi_G\colon G \longrightarrow G/A$ y $\varphi_H\colon H \longrightarrow H/B$ son los homomorfismos canónicos con núcleos A y B, respectivamente, consideremos la aplicación

$$\varphi_{G\times H} \equiv \varphi_G \times \varphi_H\colon G \times H \longrightarrow G/A \times H/B$$

Esta aplicación es un homomorfismo suprayectivo con núcleo $A \times B$. El enunciado se sigue entonces de la aplicación del primer teorema de isomorfía. □ Q.E.D.

Proposición 7.1.6 *Sean $m, n \in \mathbb{Z}$ tales que $(m, n) = 1$. Entonces,*

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$$

Demostración. Sea x un generador de $\mathbb{Z}_m$, e y un generador de $\mathbb{Z}_n$. Entonces, los elementos $(x, 0), (0, y) \in \mathbb{Z}_m \times \mathbb{Z}_n$ tiene órdenes m, n, respectivamente. Por tanto, por la proposición 3.2.1, se tiene

$$\operatorname{ord}((x, y)) = [\operatorname{ord}(x, 0), \operatorname{ord}(0, y)] = [m, n] = mn$$

□ Q.E.D.

7.2. Producto semidirecto de grupos

Proposición 7.2.1 *Sean G, H grupos, y sea $\phi : H \longrightarrow \operatorname{Aut} G$ un homomorfismo. El producto cartesiano $G \times H$ dotado de la operación*

$$(a, b) \rtimes_\phi (c, d) = (a\phi_b(c), bd)$$

posee estructura de grupo, y recibe el nombre de producto semidirecto *de G y H con respecto a ϕ, y se denota $G \rtimes_\phi H$.*

Demostración. Es claro que la operación es cerrada en el producto cartesiano $G \times H$.

La asociatividad se demuestra según

$$\begin{aligned}
[(a, b) \rtimes_\phi (c, d)] \rtimes_\phi (e, f) &= (a\phi_b(c), bd) \rtimes_\phi (e, f) \\
&= (a\phi_b(c)\phi_{bd}(e), bdf) \\
&= (a\phi_b(c)\phi_b(\phi_d(e)), bdf) \\
&= (a\phi_b(c\phi_d(e)), bdf) \\
&= (a, b) \rtimes_\phi (c\phi_d(e), df) \\
&= (a, b) \rtimes_\phi [(c, d) \rtimes_\phi (e, f)]
\end{aligned}$$

El elemento neutro es, claramente, (e_G, e_H), pues

$$(a, b) \rtimes_\phi (e_G, e_H) = (a\phi_b(e_G), be_H) = (a, b)$$

El inverso de un elemento (a, b) es $(\phi_{b^{-1}}(a^{-1}), b^{-1})$. En efecto,

$$\begin{aligned}
(a, b) \rtimes_\phi (\phi_{b^{-1}}(a^{-1}), b^{-1}) &= (a\phi_b(\phi_{b^{-1}}(a^{-1})), bb^{-1}) \\
&= (a\phi_{bb^{-1}}(a^{-1}), bb^{-1}) \\
&= (aa^{-1}, bb^{-1}) = (e_G, e_H) \\
(\phi_{b^{-1}}(a^{-1}), b^{-1}) \rtimes_\phi (a, b) &= (\phi_{b^{-1}}(a^{-1})\phi_{b^{-1}}(a), b^{-1}b) \\
&= (\phi_{b^{-1}}(a^{-1}a), b^{-1}b) = (e_G, e_H)
\end{aligned}$$

□ Q.E.D.

Proposición 7.2.2 *Sean G y H grupos. Entonces,*

1. *$G \cong \underline{G} = \{(g, e_H) : \ g \in G\}$, y $\underline{G} \lhd G \rtimes_\phi H$.*
2. *$H \cong \underline{H} = \{(e_G, h) : \ h \in H\}$*

Demostración.

1. La aplicación biyectiva $f\colon G \longrightarrow \underline{G}$ definida según $f(g) = (g, e_H)$ es un homomorfismo, pues

$$f(gg') = (gg', e_H) = (g\phi_{e_H}(g'), e_H) = (g, e_H) \rtimes_\phi (g', e_H) = f(g) \rtimes_\phi f(g')$$

Además, para todos $(g, e_H) \in \underline{G},\ (a, b) \in G \rtimes_\phi H$, se tiene

$$\begin{aligned}(a, b) \rtimes_\phi (g, e_H) \rtimes_\phi (a, b)^{-1} &= (a\phi_b(g), b) \rtimes_\phi (\phi_{b^{-1}}(a^{-1}), b^{-1}) \\ &= (a\phi_b(g)\phi_b(\phi_{b^{-1}}(a^{-1})), e_H) \\ &= (a\phi_b(g)a^{-1}, e_H) \in \underline{G}\end{aligned}$$

2. La aplicación biyectiva $f\colon H \longrightarrow \underline{H}$ definida según $f(h) = (e_G, h)$ es un homomorfismo, pues

$$f(hh') = (e_G, hh') = (e_G\phi_h(e_G), hh') = (e_G, h)\rtimes_\phi(e_G, h') = f(h)\rtimes_\phi f(h')$$

□ Q.E.D.

Proposición 7.2.3 *Sea G un grupo, y sean $M \lhd G,\ N \leq G$. Si $M \cap N = \{e\}$, y $MN = G$, entonces $G \cong M \rtimes_\kappa N$, donde $\kappa\colon N \longrightarrow \operatorname{Aut} M$ viene dada por $\kappa_n(m) = nmn^{-1}$.*

Demostración. Al igual que en la demostración de la proposición 7.1.3, cada $g \in G$ posee una factorización única $g = mn$. La aplicación $f\colon G \longrightarrow M \rtimes_\phi N$ dada por $f(g) = (m, n)$ está, por tanto, bien definida, y es biyectiva.

Sean $g_1 = m_1n_1$ y $g_2 = m_2n_2$. Entonces,

$$g_1g_2 = m_1n_1m_2n_2 = m_1n_1m_2(n_1^{-1}n_1)n_2 = m_1\kappa_{n_1}(m_2)n_1n_2$$

Por tanto,

$$f(g_1g_2) = (m_1\kappa_{n_1}(m_2), n_1n_2) = (m_1, n_1) \rtimes_\kappa (m_2, n_2) = f(g_1) \rtimes_\kappa f(g_2)$$

lo cual muestra que f es un isomorfismo. □ Q.E.D.

Capítulo 8

p-grupos y teoremas de Sylow. Grupos solubles

8.1. p-grupos y p-subgrupos de Sylow

Definición 8.1.1 *Sea G un grupo, y p un divisor primo de $|G|$. Denotamos por $|G|_p$ la máxima potencia de p que divide a $|G|$.*

- *Se dice que $g \in G$ es un p-elemento si* $\mathrm{ord}(g)$ *es una potencia de p.*
- *Se dice que G es un p-grupo si $|G|$ es una potencia de p.*
- *Se dice que $H \leq G$ es un p-subgrupo si $|H|$ es una potencia de p.*
- *Se dice que $H \leq G$ es un p-subgrupo de Sylow si $|H| = |G|_p$.*

Proposición 8.1.2 *Sea G un p-grupo finito no trivial. Entonces, $Z(G)$ es no trivial.*

Demostración. Sean $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_r$ las distintas clases de conjugación de G, de modo que

$$|G| = |\mathcal{C}_1| + |\mathcal{C}_2| + \cdots + |\mathcal{C}_r| \qquad (*)$$

Sin pérdida de generalidad, tomamos $\mathcal{C}_1 = \{e\}$. Por el teorema de órbita-estabilizador, si $x_i \in \mathcal{C}_i$ con $i \neq 1$, se tiene

$$|\mathcal{C}_i| = \frac{|G|}{|C_G(x_i)|}$$

de modo que $|\mathcal{C}_i|$ debe ser una potencia de p.

Pero entonces, se tendría que el segundo miembro de (*) es congruente con 1 módulo p, mientras que el primero es divisible por p. Así pues, debe existir un valor de i (distinto de 1) tal que $C_G(x_i) = G$, por lo que $x_i \in Z(G)$. □ Q.E.D.

Proposición 8.1.3 *Sea G un grupo de orden p^2 con p primo. Entonces, G es abeliano.*

Demostración. Por el teorema anterior, $Z(G)$ es no trivial. Por el teorema de Lagrange, se debe tener $|Z(G)| = p$ ó $|Z(G)| = p^2$. Si $|Z(G)| = p^2$, es claro que $G = Z(G)$, por lo que G es abeliano. Si $|Z(G)| = p$, entonces $G/Z(G)$ es cíclico de orden p. Por el corolario 5.3.2, G es abeliano. □ Q.E.D.

8.2. Teoremas de Sylow

Proposición 8.2.1 *Sea p número primo, y sea $m \in \mathbb{Z}$, $(m, p) = 1$. Entonces,*

$$\binom{p^n m}{p^n} \equiv m \pmod{p}$$

Demostración. El número combinatorio $\binom{p^n m}{p^n}$ es el coeficiente del término x^{p^n} en la expansión binomial de

$$(1+x)^{p^n m} = ((1+x)^{p^n})^m$$

Ahora bien,

$$(1+x)^{p^n} \equiv 1 + x^{p^n} \pmod{p}$$

ya que los coeficientes de los demás términos de la expansión son divisibles por p. Así, el coeficiente $\binom{p^n m}{p^n}$ es congruente al coeficiente de x^{p^n} de $(1+x^{p^n})^m$, y, por tanto, es congruente con m módulo p. □ Q.E.D.

Teorema 8.2.2 (Teorema de Sylow) *Sea p un número primo, y G un grupo finito de orden $p^n m$ con $(p, m) = 1$. Entonces,*

1. *G tiene, al menos, un p-subgrupo de Sylow.*
2. *El número de p-subgrupos de Sylow de G es congruente a 1 módulo p, y divide a m.*
3. *Todo p-subgrupo de G está contenido en un p-subgrupo de Sylow.*
4. *Todos los p-subgrupos de Sylow de G son conjugados.*

Demostración.

1. Sea X la colección de los subconjuntos de G con $|G|_p = p^n$ elementos, y consideremos la acción de G sobre X definida según

   $$\phi_g(S) = gS$$

   Sean $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ las órbitas de esta acción, de modo que se tiene la unión disjunta

   $$X = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_r$$

Como, por la proposición 8.2.1, $|X| = \binom{p^n m}{p^n} \equiv 1 \pmod{p}$, debe existir alguna órbita $\mathcal{O}$ tal que $p \nmid |\mathcal{O}|$. Sea $A \in \mathcal{O}$ tal que $1 \in A$. Entonces, $G_A \subseteq G_A A = A$, de donde $|G_A| \leq |A| = |G|_p$. Además, por el teorema de órbita-estabilizador, $|G| = |\mathcal{O}||G_A|$, de donde $|G|_p | |G_A|$.

Por tanto, $G_A = A$, de donde $|G_A| = |G|_p$ y G_A es un p-subgrupo de Sylow de G. Además,

$$\begin{aligned} G/G_A &= \{gG_A : \ g \in G\} \\ &= \{gA : \ g \in G\} \\ &= \mathcal{O} \end{aligned}$$

Por otro lado, sea P es un p-subgrupo de Sylow de G. Entonces, G/P es una colección de subconjuntos de G con cardinal $|G|_p$, y, por tanto, $G/P \subseteq X$. Además, $|G/P|$ es la órbita en X de P, y $(p, |G/P|) = (p, m) = 1$. Por tanto, existe una correspondencia biyectiva entre la colección de los p-subgrupos de Sylow de G y las órbitas en X cuya cardinalidad es coprima con p, siendo cada una de éstas órbitas los grupos cociente de G sobre el p-subgrupo de Sylow correspondiente.

2. Sea X' el conjunto de los elementos de X que pertenecen a una órbita cuya cardinalidad es coprima con p. Entonces, $|X'| = rm$, donde r es el número de tales órbitas. Como $|X \backslash X'|$ es divisible por p,

$$\begin{aligned} |X'| &\equiv |X| \pmod{p} \\ rm &\equiv \binom{p^n m}{p^n} \pmod{p} \\ rm &\equiv 1 \pmod{p} && \text{por la proposición 8.2.1} \\ r &\equiv 1 \pmod{p} && \text{ya que } (p, m) = 1 \end{aligned}$$

Basta ahora recordar la correspondencia biyectiva entre órbitas de cardinalidad coprima con p y p-subgrupos de Sylow, de donde r es el número de éstos últimos.

3. Sea P un p-subgrupo de Sylow de G, y Q un p-subgrupo cualquiera de G con $|Q| = p^r$. Sea

$$Y = \{gPg^{-1} : \ g \in G\}$$

Consideremos la acción de Q sobre Y dada por

$$\phi_x(gPg^{-1}) = x(gPg^{-1})x^{-1} = (xg)P(xg)^{-1}$$

Por el teorema de órbita-estabilizador, la cardinalidad de cada una de las órbitas de esta acción debe ser una potencia (quizá trivial) de p. En efecto,

$$|\text{orb}(gPg^{-1})| = [Q : Q_{gPg^{-1}}] = \frac{|Q|}{|Q_{gPg^{-1}}|} = \frac{p^r}{|Q_{gPg^{-1}}|}$$

Además,

$$|Y| = [G : N_G(P)] = \frac{[G : P]}{[N_G(P) : P]} = \frac{m}{[N_G(P) : P]}$$

por lo que $|Y||m$. Como $p \nmid m$, se tiene, entonces, $p \nmid |Y|$. Así, debe existir alguna órbita con un único elemento, pues, en caso contrario, se tendría $p||Y|$, ya que Y puede escribirse como unión disjunta de órbitas.

Sea $\{P_1 = gPg^{-1}\}$ una de tales órbitas. Entonces, para todo $x \in Q$, $xPx^{-1} = P$. Por tanto, $QP_1 = P_1Q$ y $QP_1 \leq G$ por la proposición 2.3.2. Utilizando la proposición 2.3.3, es claro que QP_1 es un p-subgrupo, de donde, necesariamente, $QP_1 = P_1$, y, por tanto, $Q \leq P_1$.

4. Si Q es también un p-subgrupo de Sylow, $Q \leq P_1$ y $|Q| = |P_1|$ implican $Q = P_1 = gPg^{-1}$.

□ Q.E.D.

8.3. Corolarios de los teoremas de Sylow

Proposición 8.3.1 *Sean G un grupo finito, P un p-subgrupo de Sylow de G, y $N \lhd G$. Entonces,*

1. *PN/N es un p-subgrupo de Sylow de G/N.*
2. *$P \cap N$ es un p-subgrupo de Sylow de N, y*

Demostración. En primer lugar, observemos que para demostrar que un subgrupo H de un grupo G es un p-subgrupo de Sylow, basta comprobar que H es un p-subgrupo y que $[G : H]$ no es divisible por p.

1. Por el teorema de correspondencia, $[G : PN] = [G/N : PN/N]$. Pero, como $[G : PN]$ divide a $[G : P]$ por factorización de índices) y $p \nmid [G : P]$, se tiene $p \nmid [G/N : PN/N]$. Puesto que $PN/N \cong P/(P \cap N)$ por el segundo teorema de isomorfía, PN/N es un p-grupo, ya que $P/(P \cap N)$ lo es. Así, PN/N es un p-subgrupo de G/N.

2. De la proposición 2.3.3, se tiene que $[N : P \cap N] = [PN : P]$. Como PN es un subgrupo de G por la proposición 4.3.4, y P es un p-subgrupo de Sylow de G, $p \nmid [PN : P]$. Por tanto, $P \cap N$ es un p-subgrupo de G cuyo índice en N es coprimo con p, i.e., $P \cap N$ es un p-subgrupo de Sylow de N.

□ Q.E.D.

Teorema 8.3.2 (Cauchy) *Sea G un grupo finito. Para todo p primo tal que $p||G|$ existe un elemento de orden p.*

DEMOSTRACIÓN. Por el teorema de Sylow, existe en G un p-subgrupo de Sylow, P. Por el teorema de Lagrange, todos los elementos de P son p-elementos, y, por tanto, alguna potencia de ellos posee orden p. □ Q.E.D.

Corolario 8.3.3 *Sea G un grupo finito. G no tiene subgrupos propios si y sólo si $|G|$ es primo.*

DEMOSTRACIÓN. Supongamos que $|G|$ no fuese primo. Entonces, por el teorema de Cauchy, debe existir un elemento g de orden p para cada primo p que divide a $|G|$, y $\langle g\rangle$ sería un subgrupo propio de G.

El recíproco es evidente del teorema de Lagrange. □ Q.E.D.

Corolario 8.3.4 *Un grupo finito G es un p-grupo si y sólo si todos sus elementos son p-elementos.*

DEMOSTRACIÓN. Por el teorema de Lagrange, si $|G| = p^n$, el orden de todo elemento de G debe ser una potencia de p.

Recíprocamente, supongamos que todos los elementos de G son p-elementos. Si existiese un número primo $q \neq p$ tal que $q||G|$, el teorema de Sylow implicaría que existe un q-subgrupo de Sylow, en contra de la hipótesis. □ Q.E.D.

Corolario 8.3.5 *Sea G un p-grupo de orden finito p^n. Para cada entero $i = 0, 1, \ldots, n$ existe un subgrupo normal en G de orden p^i.*

DEMOSTRACIÓN. Para $n = 0$ la proposición es evidente. Supongamos que el enunciado es cierto para todo $k < n$.

Sea $|G| = p^n$. Por la proposición 8.1.2, $Z(G)$ es no trivial. Por tanto, existe $0 < r \leq n$ tal que $|Z(G)| = p^r$. Por el teorema de Cauchy, $Z(G)$ posee un elemento g de orden p. Así, $H = |\langle g\rangle| = p$ y $H \lhd G$.

Por la hipótesis de inducción, G/H (que tiene orden p^{n-1}) posee subgrupos normales J_i de orden p^i para cada $i = 0, 1, \ldots, n-1$. Por el teorema de correspondencia, cada $J_i \lhd G/H$ es de la forma $J_i = H_i/H$, donde $H_i \lhd G$ y $|H_i| = p^{i+1}$. □ Q.E.D.

8.4. Grupos solubles

Definición 8.4.1 *Sea G un grupo finito. Se llama* serie de composición *a una cadena de subgrupos*

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_{k-1} \leq H_k = G$$

tal que $H_i \lhd H_{i+1}$, y H_{i+1}/H_i es un grupo simple para todo $i = 0, 1, 2, \ldots, k-1$.

Los grupos cociente H_{i+1}/H_i reciben el nombre de factores de composición.

Teorema 8.4.2 (Jordan-Hölder) *Sea G un grupo finito. Si G posee dos series de composición,*

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_{k-1} \leq H_k = G$$
$$\{e\} = J_0 \leq J_1 \leq J_2 \leq \cdots \leq J_{r-1} \leq J_r = G$$

entonces $k = r$ y existe $\sigma \in S_k$ tal que $H_{i+1}/H_i \cong J_{\sigma(i)+1}/J_{\sigma(i)}$.

Definición 8.4.3 *Un grupo G es* soluble *si existe en él una serie de composición*

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_{k-1} \leq H_k = G$$

en la cual los factores de composición H_{i+1}/H_i, $i = 0, 1, 2, \ldots, k-1$ son abelianos.

Proposición 8.4.4 *S_3, S_4, A_3 y A_4 son solubles.*

Demostración. Basta exhibir las series de composición

$$\{I\} \leq A_3 \leq S_3$$
$$\{I\} \leq \langle (12)(34), (13)(24) \rangle \leq A_4 \leq S_4$$
$$\{I\} \leq A_3$$
$$\{I\} \leq \langle (12)(34), (13)(24) \rangle \leq A_4$$

cuyos factores de composición son abelianos. □ Q.E.D.

Proposición 8.4.5 *S_n y A_n no son solubles para $n \geq 5$.*

Demostración. Para todo $n \geq 5$, el teorema de Abel asegura que A_n es simple. Por tanto,

$$\{I\} \leq A_n \leq S_n$$

es una serie de composición en S_n, pero el factor de composición $A_n/\{e\} \cong A_n$ no es abeliano. Por el teorema de Jordan-Hölder, cualquier otra serie de composición en S_n posee algún factor de composición isomorfo a A_n, y, por tanto, no puede existir en S_n una serie de composición con factores de composición abelianos.

Análogamente,

$$\{I\} \leq A_n$$

es una serie de composición en A_n con un único factor de composición no abeliano, A_n. De nuevo, el teorema de Jordan-Hölder asegura la imposibilidad de la existencia de una serie de composición con factores de composición abelianos. □ Q.E.D.

Definición 8.4.6 *Sea G un grupo, y sean $x, y \in G$*

$$[x, y] = x^{-1}y^{-1}xy$$

Se llama subgrupo conmutador de G *al subgrupo generado por todos los conmutadores de elementos de G.*

$$G' = \langle \{[x, y] : \ x, y \in G\} \rangle$$

Proposición 8.4.7 *Sea G un grupo, y G' su subgrupo conmutador. Entonces, $G' \lhd G$ y G/G' es abeliano. Además, si $N \lhd G$, G/N es abeliano si y sólo si $G' \leq N$.*

Demostración. Sean $a, b, \in G$, de modo que $[a, b] \in G'$. Para todo $g \in G$,

$$[gag^{-1}, gbg^{-1}] = (ga^{-1}g^{-1})(gb^{-1}g^{-1})(gag^{-1})(gbg^{-1}) = ga^{-1}b^{-1}abg^{-1} = g[a, b]g^{-1}$$

demostrando la normalidad de G' en G.

Sean ahora $xG', yG' \in G/G'$. Entonces,

$$(xG')(yG') = xyG' = xy[x, y]G' = yxG' = (yG')(xG')$$

Supongamos que $N \lhd G$ y que G/N es abeliano. Entonces, para todos $x, y \in G$ se tiene $(xN)(yN) = (yN)(xN)$, de donde $x^{-1}y^{-1}xyN = N$ y $[x, y] \in N$, mostrando que $G' \leq N$. Recíprocamente, si $G' \leq N$ entonces

$$(xN)(yN) = xyN = xy[x, y]N = yxN = (yN)(xN)$$

y G/N es abeliano. □ Q.E.D.

Definición 8.4.8 *Se llama* serie derivada de G *a la cadena de subgrupos*

$$G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(k)} \geq \cdots$$

donde $G^{(0)} = G$ y $G^{(k)} = (G^{(k-1)})'$.

Proposición 8.4.9 *Un grupo G es soluble si y sólo si $G^{(k)} = \{e\}$ para algún $k \geq 0$.*

Demostración. Supongamos que G es soluble, de manera que existe una serie de composición

$$\{e\} = H_n \leq H_{n-1} \leq \cdots \leq H_1 \leq H_0 = G$$

en la que cada factor H_{i-1}/H_i es abeliano. $G^{(i)}$ es un subgrupo de H_i para $i = 0$, y para $i = 1$ por la proposición 8.4.7. Si $G^{(i-1)} \leq H_{i-1}$, entonces, $G^{(i)} \leq (H_{i-1})'$. Como H_{i-1}/H_i es abeliano, la proposición 8.4.7 asegura que $(H_{i-1})' \leq H_i$, y, por tanto, $G^{(i)} \leq (H_{i-1})' \leq H_i$. Como $H_n = \{e\}$, se tiene, finalmente, $G^{(n)} = \{e\}$.

Recíprocamente, si $G^{(k)} = \{e\}$ para algún $k \geq 0$, entonces

$$\{e\} = G^{(k)} \leq G^{(k-1)} \leq \cdots \leq G^{(1)} \leq G^{(0)} = G$$

es una serie de composición con factores abelianos, según la proposición 8.4.7.
□ Q.E.D.

Capítulo 9

Grupos abelianos finitos

9.1. Factorización de elementos de grupos abelianos finitos

Proposición 9.1.1 *Sea G un grupo, y $x \in G$ un elemento de orden mn con $(m,n) = 1$. El elemento x puede escribirse de manera única como el producto de dos elementos y, z que conmutan entre sí, con órdenes n y m, respectivamente. Además, y, z son potencias de x.*

Demostración. Utilizando la propiedad lineal del máximo común divisor, existen enteros u, v tales que $1 = um + vn$. Entonces, $x = x^{um+vn} = x^{um}x^{vn}$. Tomando $y = x^{um},\ z = x^{vn}$ se tiene que y, z son potencias de x, y, por tanto, conmutan entre sí.

Sean $n' = \text{ord}(y),\ m' = \text{ord}(z)$. Dado que $y^n = x^{umn} = e,\ z^m = x^{vmn} = e$, se tiene que $n'|n,\ m'|m$. Por otro lado,

$$x^{n'm'} = (yz)^{n'm'} = y^{n'm'}z^{n'm'} = e$$

implica que $mn|m'n'$, de donde $n = n', m = m'$.

Supongamos ahora que existen dos elementos y_1, z_1 que cumplen también los requerimientos del enunciado. Entonces, es claro que y_1, z_1 conmutan con x, pues

$$xy_1 = y_1z_1y_1 = y_1x$$
$$xz_1 = z_1y_1z_1 = z_1x$$

Por tanto, y_1, z_1 conmutan con y, z, puesto que éstos últimos son potencias de x.

Por otro lado, $yz = x = y_1z_1$ implica $w = y_1^{-1}y = z_1z^{-1}$. Entonces,

$$w^n = (y_1^{-1})^n y^n = e$$
$$w^m = x_1^m(z^{-1})^m = e$$

Como $(m,n)=1$, se debe tener, necesariamente, $w=e$, de donde $y=y_1$ y $z=z_1$. □ Q.E.D.

Corolario 9.1.2 *Para cada elemento $x \in G$ de orden $p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$, donde los p_j son números primos distintos, existe una única factorización*

$$x = x_1x_2\dots x_k$$

de modo que $x_ix_j = x_jx_i$ para todos $i,j \in \{1,2,\dots,k\}$ y cada x_i es una potencia de x de orden $p_i^{n_i}$.

Demostración. Basta aplicar repetidas veces la proposición anterior. □Q.E.D.

Proposición 9.1.3 *Todo grupo abeliano finito es isomorfo al producto directo de todos sus p-subgrupos de Sylow.*

Demostración. Sea G un grupo abeliano con $|G| = n = p_1^{n_1}p_2^{n_2}\dots p_k^{n_k}$.

Puesto que G es abeliano, aplicando la proposición 4.2.3 y el teorema de Sylow, deducimos que, para cada p_i, existe un único p_i-subgrupo de Sylow, al que denotaremos S_{p_i}, que, además, es normal en G.

Además, si

$$g \in S_{p_j} \cap (\prod_{i\neq j} S_{p_i})$$

se tiene $\mathrm{ord}(g) = p_j^{m_j}$ con $0 \leq m_j \leq n_j$. Por otro lado, utilizando el corolario 9.1.2, podemos escribir $g = \prod_{i\neq j} y_i$ con $y_i \in S_{p_i}$, de modo que

$$\mathrm{ord}(g) = [\mathrm{ord}(y_i)]_{i\neq j} = \prod_{i\neq j} p_i^{m_i}$$

Se sigue entonces que $g = e$.

Del corolario 9.1.2 se deduce que $G = S_{p_1}S_{p_2}\dots S_{p_k}$. Finalmente, aplicando la proposición 7.1.4 se obtiene el enunciado. □ Q.E.D.

9.2. Clasificación de los grupos abelianos finitos

Definición 9.2.1 *Dado un grupo abeliano G, se dice que $\{a_1,a_2,\dots,a_r\}$ es un* sistema de generadores *de G si todo elemento $x \in G$ puede escribirse en la forma*

$$x = n_1a_1 + n_2a_2 + \dots + n_ra_r$$

con $n_j \in \mathbb{Z}$.

Si la expresión anterior es única, se dice que $\{a_1,a_2,\dots,a_r\}$ es una base *de G.*

Proposición 9.2.2 *Sea G un grupo abeliano, y $\{a_1,a_2,\dots,a_r\}$ un sistema de generadores de G. Son equivalentes:*

1. $\{a_1, a_2, \ldots, a_r\}$ *es una base de* G.

2. *Si existen* $n_1, n_2, \ldots, n_r \in \mathbb{Z}$ *tales que*

$$n_1a_1 + n_2a_2 + \cdots + n_ra_r = 0$$

se debe tener $n_ja_j = 0$ *para todo* $j = 1, 2, \ldots, r$.

Demostración.

$(1 \Rightarrow 2)$ Supongamos que $\{a_1, a_2, \ldots, a_r\}$ es una base de G. Entonces,

$$n_1a_1 + n_2a_2 + \cdots + n_ra_r = 0 = 0a_1 + 0a_2 + \cdots + 0a_r$$

y, de la unicidad de la representación, se deduce que $n_ja_j = 0$ para todo $j = 1, 2, \ldots, r$.

$(2 \Rightarrow 1)$ Recíprocamente, supongamos que $x \in G$ posee dos descomposiciones

$$n_1a_1 + n_2a_2 + \cdots + n_ra_r = x = n'_1a_1 + n'_2a_2 + \cdots + n'_ra_r$$

Se tiene entonces

$$(n_1 - n'_1)a_1 + (n_1 - n'_2)a_2 + \cdots + (n_1 - n'_3)a_r = 0$$

y la hipótesis asegura que $(n_j - n'_j)a_j = 0$ para todo $j = 1, 2, \ldots, r$. □ Q.E.D.

Proposición 9.2.3 *Sea* $\{a_1, a_2, \ldots, a_r\}$ *una base de un grupo abeliano finito* G. *Entonces,*

$$G \cong \bigoplus_{i=1}^{r} \langle a_i \rangle$$

Demostración. Como G es abeliano, cada $\langle a_j \rangle$ es normal en G. Puesto que $\{a_1, a_2, \ldots, a_r\}$ es un sistema de generadores de G, $G = \langle a_1 \rangle + \langle a_r \rangle + \cdots + \langle a_r \rangle$. Finalmente, si

$$x \in \langle a_j \rangle \cap (\prod_{i \neq j} \langle a_i \rangle)$$

se tiene que

$$x = n_ja_j = \sum_{i \neq j} n_ia_i$$

y, de la proposición anterior, se tiene $x = 0$. El resultado se deduce entonces de la proposición 7.1.4. □ Q.E.D.

Teorema 9.2.4 (Teorema de estructura de los grupos abelianos finitos) *Todo grupo abeliano finito es isomorfo a una suma directa de grupos cíclicos de órdenes potencias de primos.*

DEMOSTRACIÓN. Por las proposiciones 9.1.3 y 9.2.3, basta demostrar que cualquier p-subgrupo de Sylow tiene una base. Así pues, sea G un p-grupo.

Elegimos $a_1 \in G$ de orden máximo p^{m_1}. Si $G_1 = \langle a_1 \rangle = G$, entonces $\{a_1\}$ es una base de G.

Supongamos entonces que $G_1 \subsetneq G$. Supongamos que tenemos k elementos $a_1, a_2, \ldots, a_k$ de órdenes $p_{m_1}, p_{m_2}, \ldots, p_{m_k}$ tales que

1. $m_1 \geq m_2 \geq \ldots \geq m_k$ y todo elemento de G que no pertenezca a $G_k = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \cdots \oplus \langle a_k \rangle$ tiene orden p^t con $t \leq m_k$, y

2. $\{a_1, a_2, \ldots, a_k\}$ es una base de G_k.

Si $G_k \subsetneq G$, tomamos $b \in G \backslash G_k$ de orden p^t. Sea r el menor entero positivo tal que $rb \in G_k$ (existe, pues $p^t b = 0 \in G_k$). Utilizando el algoritmo de Euclides, podemos escribir

$$p^t = cr + r' \qquad \text{con } 0 \leq r' < r$$

Por tanto, $r'b = p^t b - crb \in G_k$, por lo que $r' = 0$. Por tanto, $r | p^t$. Pongamos, entonces, $r = p^{m_{k+1}}$, y puesto que $t \geq m_{k+1}$ se tiene

$$m_1 \geq m_2 \geq \ldots \geq m_k \geq m_{k+1}$$

Puesto que $rb \in G_k$, se tiene

$$rb = \sum_{i=1}^{k} n_i a_i$$

Multiplicando esta igualdad por $\frac{p^t}{r} = p^{t - m_{k+1}}$,

$$p^t b = 0 = \sum_{i=1}^{k} n_i \frac{p^t}{r} a_i$$

Utilizando (2), se sigue que $n_i \frac{p^t}{r} a_i = 0$, y, por tanto, $\frac{n_i p^t}{r}$ es un múltiplo de p^{m_i}. Así,

$$\frac{n_i p^t}{r} = n_i' p^{m_i}, \qquad n_i' \in \mathbb{N}, \qquad i = 1, 2, \ldots, k$$

Entonces, $n_i = r(n_i' p^{m_i - t}) = r n_i''$, donde $n_i'' \in \mathbb{N}$.

Definimos

$$a_{k+1} = b - \sum_{i=1}^{k} n_i'' a_i$$

Se tiene que $r a_{k+1} = rb - \sum_{i=1}^{k} r n_i'' a_i = rb - \sum_{i=1}^{k} n_i a_i = 0$, y, por tanto, $\text{ord}(a_{k+1}) | r$. Por otro lado, $s a_{k+1} = 0$ implica $sb \in G_k$, de donde $r \leq s$ por la definición de r. Así, $\text{ord}(a_{k+1}) = r = p^{m_{k+1}}$.

Si

$$0 = \sum_{i=1}^{k+1} c_i a_i$$

entonces $c_{k+1}a_{k+1} \in G_k$, de donde, por la definición de a_{k+1}, se tiene que $c_{k+1}b \in G_k$.

Dividiendo c_{k+1} entre r, se tiene $c_{k+1} = cr + r''$ con $0 \leq r'' < r$. Debe ser, entonces, $r'' = 0$, ya que $r''b = c_{k+1}b - crb \in G_k$. Por ello, c_{k+1} es un múltiplo de $r = p^{m_{k+1}}$, y, por tanto,

$$c_{k+1} = p^{m_{k+1}} c'_{k+1}$$

Por tanto, $c_{k+1}a_{k+1} = 0$, lo cual, unido a (2), implica que $\{a_1, a_2, \ldots, a_k, a_{k+1}\}$ es una base de G_{k+1}. □ Q.E.D.

Proposición 9.2.5 *Todo grupo abeliano finito G es isomorfo a una suma directa de la forma*

$$G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{n_r}}$$

Esta descomposición es única, salvo por el orden.

Demostración. La existencia es consecuencia directa del teorema de estructura, pues todo grupo cíclico finito de orden k es isomorfo a $(\mathbb{Z}_k, +)$.

Puesto que, para cada primo p que divide a G, existe un único p-subgrupo de Sylow, basta demostrar la unicidad para éstos, i.e., basta hacerlo para p-grupos.

Sea, por tanto, G un p-grupo abeliano finito, de orden p^t. Supongamos que G posee dos descomposiciones

$$G \cong A_1 \oplus A_2 \oplus \cdots \oplus A_r$$
$$G \cong B_1 \oplus B_2 \oplus \cdots \oplus B_s$$

donde $A_i = (\mathbb{Z}_{p^{e_i}}, +)$ y $B_j = (\mathbb{Z}_{p^{f_j}}, +)$, y

$$e_1 \geq e_2 \geq \ldots \geq e_r$$
$$f_1 \geq f_2 \geq \cdots \geq f_s$$

Para $t = 1$, el enunciado de la proposición se cumple trivialmente. Supongamos que también es cierto para todo p-grupo de orden p^k con $k < t$.

Sea $pG = \{py : \ y \in G\} \leq G$ (no es una clase por la izquierda). Si $pG = \{e\}$, todo elemento de G (excepto el neutro e) es de orden p, y, por tanto, $e_i = f_j = 1$ para todos $i = 1, 2, \ldots, r$ y $j = 1, 2, \ldots, s$, de donde $p^t = |G| = p^r = p^s$.

Si $pG \neq \{e\}$, veamos que podemos escribir

$$pG \cong \langle pa_1 \rangle \oplus \langle pa_2 \rangle \oplus \cdots \oplus \langle pa_r \rangle$$
$$pG \cong \langle pb_1 \rangle \oplus \langle pb_2 \rangle \oplus \cdots \oplus \langle pb_s \rangle$$

donde $\langle a_i\rangle = A_i$ y $\langle b_j\rangle = B_j$.

Si $px \in pG,\ x \in G$, y, por tanto,

$$x = \sum_{i=1}^{r} n_i a_i \quad \Longrightarrow \quad px = \sum_{i=1}^{r} n_i p a_i$$

Supongamos que $px = 0$. Entonces, $\sum_{i=1}^{r} n_i p a_i = 0$, y, puesto que $\{a_i\}_{i=1}^{r}$ es una base de G, se debe tener $n_i p a_i = 0$ para cada $i = 1, 2, \ldots, r$. Así, $\{pa_i\}_{i=1}^{r}$ es una base de pG, y, aplicando la proposición 9.2.3 se obtiene el primer isomorfismo.

El segundo se demuestra de forma análoga.

Finalmente,

$$|pG| = p^{e_1-1}p^{e_2-1}\ldots p^{e_r-1} = p^{t-r}$$
$$|pG| = p^{f_1-1}p^{f_2-1}\ldots p^{f_s-1} = p^{t-s}$$

de donde $r = s$ y $e_i = f_i$ para cada $i = 1, 2, \ldots, r$. □ Q.E.D.

Definición 9.2.6 *Sea G un grupo abeliano finito*

$$G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{n_r}}$$

Los números $(p_1^{n_1}, p_2^{n_2}, \ldots, p_r^{n_r})$ se llaman divisores elementales *del grupo G.*

Corolario 9.2.7 *Dos grupos abelianos finitos con divisores elementales distintos no son isomorfos.*

Demostración. El enunciado es una reformulación de la proposición 9.2.5 en términos de la definición anterior. □ Q.E.D.

Corolario 9.2.8 *Todo grupo abeliano finito G es isomorfo a una suma directa de la forma*

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t}$$

donde $m_1 \geq 2$ y m_i divide a cada m_j con $j \geq i$.

Demostración. Con todos los divisores elementales de G, construimos la matriz

$$\begin{pmatrix} p_1^{n_{11}} & p_2^{n_{12}} & \cdots & p_r^{n_{1r}} \\ p_1^{n_{21}} & p_2^{n_{22}} & \cdots & p_r^{n_{2r}} \\ \vdots & \vdots & \ddots & \vdots \\ p_1^{n_{t1}} & p_2^{n_{t2}} & \cdots & p_r^{n_{tr}} \end{pmatrix}$$

en la cual $n_{ij} \leq n_{i+1,j}$.

Entonces, definimos $m_i = p_1^{n_{i1}} p_2^{n_{i2}} \ldots p_r^{n_{ir}}$. Es claro que m_i divide a cada m_j con $j \geq i$. Además, por la proposición 7.1.6,

$$\mathbb{Z}_{m_i} \cong \mathbb{Z}_{p_1^{n_{i1}}} \oplus \mathbb{Z}_{p_2^{n_{i2}}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{n_{ir}}}$$

Así, el enunciado se sigue trivialmente de la proposición 9.2.5. □ Q.E.D.

Definición 9.2.9 *Sea G un grupo abeliano finito*

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t}$$

donde $m_1 \geq 2$ y m_i divide a cada m_j con $j \geq i$. Los números m_i reciben el nombre de coeficientes de torsión o invariantes *de G.*

Corolario 9.2.10 *Dos grupos abelianos finitos con coeficientes de torsión distintos no son isomorfos.*

Demostración. De nuevo, este enunciado es una reformulación del corolario 9.2.8 en términos de la definición anterior. □ Q.E.D.

Corolario 9.2.11 *Sea G un grupo abeliano finito de orden n. Para cada divisor d de n existe un elemento de orden d.*

Demostración. Por el corolario 9.1.2, si $d = \prod_{i=1}^{n} p_i^{n_i}$, el elemento x tiene una factorización única $x = \prod_{i=1}^{n} x_i$, donde cada x_i es de orden $p_i^{n_i}$- Éstos últimos existen por el corolario 8.3.5. □ Q.E.D.

9.3. Cuerpos finitos

Definición 9.3.1 *Un cuerpo $(F, +, \cdot)$ es un conjunto no vacío F, dotado con dos operaciones, suma $(+)$ y multiplicación $(\cdot)$, tales que*

- *$(F, +)$ y $(F^\times = F\backslash\{0\}, \cdot)$ son grupos abelianos, y*
- *$\forall x, y, z \in F,\ x \cdot (y + z) = x \cdot y + x \cdot z$ (propiedad distributiva).*

Los elementos neutros con respecto a la suma y a la multiplicación se denotan 0 y 1, respectivamente. El inverso aditivo de un elemento $x \in F$ se denota $-x$, y su inverso multiplicativo, x^{-1}.

Definición 9.3.2 *Se llama* característica *de un cuerpo $(F, +, \cdot)$ al orden aditivo del elemento neutro de la multiplicación.*

Proposición 9.3.3 *La característica de un cuerpo $(F, +, \cdot)$ es cero o un número primo.*

Demostración. Sea F un cuerpo de característica positiva k, y supongamos que d_1 y d_2 son divisores propios de k. Entonces

$$0 = k1 = d_1 d_2 1 = (d_1 1)(d_2 1)$$

Puesto que no existen en F divisores de cero, alguno de los dos factores debe ser cero, en contra de la definición de k. □ Q.E.D.

Proposición 9.3.4 *Sea F un cuerpo finito de característica p. Entonces, existe $n \in \mathbb{N}$ tal que*

$$(F, +) \cong \bigoplus_{i=1}^{n} \mathbb{Z}_p$$

Demostración. Para todo $x \in F$, utilizando la definición de característica,

$$px = p(1x) = (p1)x = 0$$

de donde todo elemento de F tiene orden p. Basta, entonces, aplicar la proposición 9.2.5. □ Q.E.D.

Proposición 9.3.5 *El grupo multiplicativo de todo cuerpo finito es cíclico.*

Demostración. Aplicando el corolario 9.2.8,

$$F^{\times} \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$$

donde $mi|m_j$ para todo $j \geq i$. Por tanto, para cada $x \in F$ se tiene $\text{ord}(x)|m_r$ y $x^{m_r} = 1$. Sin embargo, el polinomio $x^{m_r} - 1$ tiene, como máximo, m_r soluciones. Se sigue, entonces, que $|F^{\times}| = m_r$, luego $F^{\times}$ es cíclico. □ Q.E.D.

9.4. Grupos abelianos de orden bajo

Para elaborar la siguiente tabla se han utilizado las proposiciones 7.1.6 y 9.2.5 y los corolarios 3.3.2 y 9.2.7.

n	Grupos abelianos de orden n
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$
10	$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_4 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7$
15	$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$
16	$\mathbb{Z}_{16}$, $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Capítulo 10

Clasificación de grupos de orden menor que 16

10.1. Primeros grupos clasificados

A partir de lo demostrado en los capítulos anteriores, podemos clasificar ya los siguientes grupos.

Grupos de orden primo. Por el corolario 3.3.2, los grupos de orden primo son cíclicos simples, y, por tanto, abelianos.

Son de este tipo los grupos de orden 2, 3, 5, 7, 11 y 13.

Grupos de orden p^2. Según la proposición 8.1.3, todo grupo de orden el cuadrado de un primo p es abeliano. Así pues, el corolario 9.2.7 asegura que todo grupo de orden p^2 es isomorfo a $\mathbb{Z}_{p^2}$ ó a $\mathbb{Z}_p \times \mathbb{Z}_p$.

En esta clase se encuadran los grupos de orden 4 y 9.

10.2. Grupos de orden pq

Proposición 10.2.1 *Sean p y q primos con $p > q$, y G un grupo de orden pq. Entonces,*

- *Si $p \not\equiv 1 \pmod{q}$, entonces $G \cong \mathbb{Z}_{pq}$.*
- *Si $p \equiv 1 \pmod{q}$ y G es abeliano, entonces $G \cong \mathbb{Z}_{pq}$.*
- *Si $p \equiv 1 \pmod{q}$ y G no es abeliano, entonces $G \cong \mathbb{Z}_p \rtimes_\kappa \mathbb{Z}_q$.*

Demostración. Sean n_p, n_q el número de p-subgrupos y q-subgrupos de Sylow, respectivamente. Por el teorema de Sylow, $n_p \equiv 1 \pmod{p}$ y $n_p | q$. Como $p > q$, esto implica $n_p = 1$. Entonces, si P es el único p-subgrupo de Sylow de G, se tiene $P \lhd G$.

Sea Q un p-subgrupo de Sylow de G. Como también $n_q \equiv 1 \pmod{q}$ y $n_q | p$, el subgrupo Q puede tener o bien un único conjugado (él mismo), o bien p conjugados.

El primer caso se da si $p \not\equiv 1 \pmod{q}$, o si $p \equiv 1 \pmod{q}$ y G es abeliano. Entonces, $Q \lhd G$. Puesto que, por el teorema de Lagrange, $P \cap Q = \{e\}$, la proposición 2.3.3 asegura que $PQ = G$. Aplicando la proposición 7.1.3, $G \cong P \times Q$. Pero $P \cong \mathbb{Z}_p$ y $Q \cong \mathbb{Z}_q$, por ser P y Q grupos de orden primo. Finalmente, basta observar que $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ por la proposición 7.1.6.

Si $p \equiv 1 \pmod{q}$ y G no es abeliano, G tiene p q-subgrupos de Sylow. Como, por el teorema de Lagrange, $P \cap Q = \{e\}$, de nuevo la proposición 2.3.3 asegura que $PQ = G$. Entonces, por la proposición 7.2.3, $G \cong P \rtimes_\kappa Q$, donde $\kappa \colon N \longrightarrow \operatorname{Aut} M$ viene dada por $\kappa_n(m) = nmn^{-1}$. Finalmente, basta observar que $P \cong \mathbb{Z}_p$ y $Q \cong \mathbb{Z}_q$. □ Q.E.D.

Esta proposición nos permite clasificar los grupos de orden $6 = 3 \times 2$, $10 = 5 \times 2$, $14 = 7 \times 2$ y $15 = 5 \times 3$.

Grupos de orden $2p$. Si $q = 2$ y p es un primo impar, se tiene que $p \equiv 1 \pmod{q}$. Aplicando la proposición anterior, se tiene que todo grupo abeliano de orden $2p$ es isomorfo a $\mathbb{Z}_{2p}$.

El grupo diédrico de orden $2p$, D_{2p}, es no abeliano. Puesto que la proposición anterior asegura que existe una única clase de isomorfía de grupos no abelianos de orden $2p$, llegamos a la conclusión de que todo grupo no abeliano de orden $2p$ es isomorfo a $D_{2p} \cong \mathbb{Z}_p \rtimes_\kappa \mathbb{Z}_2$.

Quedan así clasificados los grupos de orden 6, 10 y 14.

Nótese que S_3 es un grupo no abeliano de orden 6, por lo que $S_3 \cong D_6$.

Grupos de orden 15. Si $p = 5$ y $q = 3$, se tiene que $p \not\equiv 1 \pmod{q}$, de donde todo grupo de orden 15 debe ser cíclico, y, por tanto, abeliano.

10.3. Grupos de orden 8

Según los resultados del capítulo anterior, existen tres clases de isomorfía de grupos abelianos de orden 8, a saber:

$$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Investiguemos ahora los grupos no abelianos de orden 8.

Proposición 10.3.1 *Sea G un grupo no abeliano de orden p^3 con p primo. Entonces, $|Z(G)| = p$ y $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$*

DEMOSTRACIÓN. Por la proposición 8.1.2, $Z(G)$ es no trivial. Por el teorema de Lagrange, debe ser, entonces, $|Z(G)| = p$ ó $|Z(G)| = p^2$. Pero $|Z(G)| = p^2$ implicaría que Int $G \cong G/Z(G)$ es cíclico, y, por el corolario 5.3.2, G sería abeliano. Por tanto, $|Z(G)| = p$.

Entonces, $|G/Z(G)| = p^2$. Si $G/Z(G) \cong \mathbb{Z}_{p^2}$, el corolario 5.3.2 implicaría de nuevo la conmutatividad de G, por lo que $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. □ Q.E.D.

Proposición 10.3.2 *Sea G un grupo no abeliano de orden 8. Entonces, existe en G algún elemento de orden 4.*

DEMOSTRACIÓN. En efecto, sea $H = \langle g, h\rangle$ con $g, h \in G$ elementos de orden 2. Entonces,

$$H = \{e, g, h, gh, hg\}$$

Entonces, el teorema de Lagrange implica que $gh = hg$. □ Q.E.D.

Sea G un grupo no abeliano de orden 8, de modo que $Z(G) = \{e, z\}$. Supongamos que z es el único elemento de orden 2 en G. Por el corolario 8.3.5, podemos escoger un elemento $y \in G$ de orden 4 tal que $Q = \langle y\rangle \lhd G$. Entonces, $G/Q = \langle xQ\rangle$, y como x no puede ser un elemento de orden 2, se tiene que $x^2 = z$. Además, también $y^2 = z$. Por tanto,

$$G = \{e, z, x, x^3, y, y^3\}$$

Además, $xyx^{-1} \in Q = \{e, z, y, y^3\}$. Pero

- Si $xyx^{-1} = e$ se tendría $y = e$.
- Si $xyx^{-1} = z$ se tendría $y = z$.
- Si $xyx^{-1} = y$ se tendría $xy = yx$, de donde G sería abeliano.

Por tanto, $xyx^{-1} = y^3$, de donde $xy = y^3x$. Por tanto, encontramos la presentación

$$\langle x, y :\ x^4 = e,\ x^2 = y^2,\ xy = y^3x\rangle$$

Este grupo recibe el nombre de *grupo cuaterniónico*, y se denota Q_8. Sus elementos suelen denotarse $1, -1, i, -i, j, -j, k, -k$, cumpliendo las siguientes relaciones:

$$i^2 = j^2 = k^2 = -1$$

$$\begin{array}{lll} ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j \end{array}$$

Sea, de nuevo, G un grupo no abeliano de orden 8, de modo que $Z(G) = \{e, z\}$. Supongamos ahora que existe en G un elemento x de orden 2 distinto de z. Si y es un elemento de orden 4, entonces

$$G = \{e, y, y^2, y^3, x, xy, xy^2, xy^3\}$$

Puesto que $yx \in G$, la única posibilidad que no lleva a contradicción con las hipótesis es $yx = xy^3$. Por tanto, este grupo es isomorfo a D_8.

10.4. Grupos de orden 12

Proposición 10.4.1 *Sea G un grupo de orden 12. Entonces, G tiene un subgrupo de Sylow normal.*

Demostración. Por el teorema de Sylow, el número de 3-subgrupos de Sylow de G debe ser uno o cuatro.

Supongamos que G posee cuatro 3-subgrupos de Sylow, P_1, P_2, P_3, P_4. Cada intersección $P_i \cap P_j$ con $i \neq j$ debe ser un subgrupo propio de P_i. Como $P_i \cong \mathbb{Z}_3$, es necesario que $P_i \cap P_j = \{e\}$. Por tanto, G contiene el neutro, y ocho elementos de orden 3, incluidos en sus 3-subgrupos de Sylow. Quedan, por tanto, tres elementos de orden 2, por lo cual sólo puede existir un 2-subgrupo de Sylow. □ Q.E.D.

Sea G un grupo de orden 12, V un 2-subgrupo de Sylow y T un 3-subgrupo de Sylow. Según resultados anteriores, se tiene $T \cong \mathbb{Z}_3$, y $V \cong \mathbb{Z}_4$ ó $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Además, por la proposición anterior, uno de los dos debe ser normal en G.

Analicemos los distintos casos.

1. $V \lhd G,\ T \lhd G,\ V \cong \mathbb{Z}_4$:
   Por la proposición 7.1.3, $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.

2. $V \lhd G,\ T \lhd G,\ V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$:
   Por la proposición 7.1.3, $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

3. $V \lhd G,\ T \leq G,\ V \cong \mathbb{Z}_4$:
   Por la proposición 7.2.3, $G \cong \mathbb{Z}_4 \rtimes_\kappa \mathbb{Z}_3$. Sin embargo $\kappa\colon \mathbb{Z}_3 \longrightarrow \operatorname{Aut}\mathbb{Z}_4 \cong \mathbb{Z}_2$ sólo puede ser el homomorfismo trivial, por lo cual $\mathbb{Z}_4 \rtimes_\kappa \mathbb{Z}_3 = \mathbb{Z}_4 \times \mathbb{Z}_3$. En este caso, también $T \lhd G$, repitiendo el primer caso.

4. $V \lhd G,\ T \leq G,\ V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$:
   Por la proposición 7.2.3, $G \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\kappa \mathbb{Z}_3$. Si $\kappa\colon \mathbb{Z}_3 \longrightarrow \operatorname{Aut}\mathbb{Z}_2 \times \mathbb{Z}_2$

está definida según

$$\begin{array}{lll} \kappa_{\bar{0}}(\bar{0}\bar{1}) = \bar{0}\bar{1} & \kappa_{\bar{0}}(\bar{1}\bar{0}) = \bar{1}\bar{0} & \kappa_{\bar{0}}(\bar{1}\bar{1}) = \bar{1}\bar{1} \\ \kappa_{\bar{1}}(\bar{0}\bar{1}) = \bar{1}\bar{0} & \kappa_{\bar{1}}(\bar{1}\bar{0}) = \bar{1}\bar{1} & \kappa_{\bar{1}}(\bar{1}\bar{1}) = \bar{0}\bar{1} \\ \kappa_{\bar{2}}(\bar{0}\bar{1}) = \bar{1}\bar{1} & \kappa_{\bar{2}}(\bar{1}\bar{0}) = \bar{0}\bar{1} & \kappa_{\bar{2}}(\bar{1}\bar{1}) = \bar{1}\bar{0} \end{array}$$

y denotamos $a = (\bar{0}\bar{1}, \bar{0}),\ b = (\bar{1}\bar{0}, \bar{0}),\ c = (\bar{0}\bar{0}, \bar{1})$, este grupo admite la presentación

$$\langle a, b, c :\ a^2 = b^2 = c^3 = e,\ ab = ba,\ cac^{-1} = a,\ cbc^{-1} = ab \rangle$$

El homomorfismo que aplica

$$\begin{aligned} a &\longmapsto (12)(34) \\ b &\longmapsto (14)(23) \\ c &\longmapsto (123) \end{aligned}$$

establece un isomorfismo de este grupo con el cuarto grupo alternado, A_4.

5. $V \leq G,\ T \lhd G,\ V \cong \mathbb{Z}_4$:
Por la proposición 7.2.3, $G \cong \mathbb{Z}_3 \rtimes_\kappa \mathbb{Z}_4$, donde el homomorfismo $\kappa : \mathbb{Z}_4 \longrightarrow \operatorname{Aut} \mathbb{Z}_3$ viene dado por

$$\begin{aligned} \kappa_{\bar{0}}(\bar{1}) = \kappa_{\bar{2}}(\bar{1}) &= \bar{1} \\ \kappa_{\bar{1}}(\bar{1}) = \kappa_{\bar{3}}(\bar{1}) &= \bar{2} \end{aligned}$$

Tomando $a = (\bar{1}, \bar{2}),\ b = (\bar{1}, \bar{1})$, concluimos que este grupo admite la presentación

$$\langle a, b :\ a^6 = e,\ a^3 = b^2,\ bab^{-1} = a^{-1} \rangle$$

Suele denominarse grupo cuaterniónico generalizado de orden 12, Q_{12}.

6. $V \leq G,\ T \lhd G,\ V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$:
Por la proposición 7.2.3, $G \cong \mathbb{Z}_3 \rtimes_\kappa (\mathbb{Z}_2 \times \mathbb{Z}_2)$. Si $\kappa \colon \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \operatorname{Aut} \mathbb{Z}_3$ viene dado por

$$\begin{aligned} \kappa_{\bar{0}\bar{0}}(\bar{1}) = \kappa_{\bar{1}\bar{1}}(\bar{1}) &= \bar{1} \\ \kappa_{\bar{0}\bar{1}}(\bar{1}) = \kappa_{\bar{1}\bar{0}}(\bar{1}) &= \bar{2} \end{aligned}$$

la elección $a = (\bar{1}, (\bar{1}, \bar{1})),\ b = (\bar{1}, (\bar{1}, \bar{0}))$ nos lleva a la presentación

$$\langle a, b :\ a^6 = b^2 = e,\ ab = ba^{-1} \rangle$$

es decir, al grupo D_{12} de simetrías de un hexágono regular.

10.5. Resumen

La siguiente tabla muestra las distintas clases de isomorfía de grupos de orden menor que 16, resumiendo los resultados de este capítulo, así como los del anterior.

n	Grupos abelianos de orden n	Grupos no abelianos de orden n
2	$\mathbb{Z}_2$	-
3	$\mathbb{Z}_3$	-
4	$\mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2$	-
5	$\mathbb{Z}_5$	-
6	$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$	$D_6 \cong S_3$
7	$\mathbb{Z}_7$	-
8	$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$D_8,\ Q_8$
9	$\mathbb{Z}_9, \quad \mathbb{Z}_3 \times \mathbb{Z}_3$	-
10	$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$	D_{10}
11	$\mathbb{Z}_{11}$	-
12	$\mathbb{Z}_4 \times \mathbb{Z}_3, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$	$D_{12},\ Q_{12},\ A_4$
13	$\mathbb{Z}_{13}$	-
14	$\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7$	D_{14}
15	$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$	-

Bibliografía

[1] J.L. Alperin, Rowen B. Bell. *Groups and Representations.* Graduate Texts in Mathematics 162, Springer-Verlag New York Inc., New York, 1995, ISBN 0-387-94526-1.

[2] José Dorronsoro, Eugenio Hernández. *Números, grupos y anillos.* Addison-Wesley / Universidad Autónoma de Madrid, Salamanca, 1996, ISBN 0-201-65395-8, ISBN 84-7829-009-5.

[3] John F. Humphreys. *A Course in Group Theory.* Oxford Science Publications, Oxford University Press Inc., New York, 1996, ISBN 0-19-853459-0.

[4] Serge Lang. *Algebra.* Addison-Wesley Publishing Company Inc., Reading, Massachusetts, 3rd edition, 1993, ISBN 0-201-55540-9.