ÍNDICE

Capítulo 1

GENERALIDADES. TEOREMA DE LAGRANGE

I. GRUPOS

Definición 1.1. Un *grupo* es un conjunto no vacío G en el que está definida una operacion binaria

$$G \times G \to G$$

que escribiremos

$$(a,b) \mapsto ab$$

tal que:

(i) $(ab)c = a(bc)$ para cada terna de elementos a, b y c de G. Se dice que la operacion es *asociativa*.

(ii) Existe un elemento $u \in G$ tal que

$$ua = a = au$$

para todos los elementos a de G.

(iii) Para cada elemento $a \in G$ existe $x \in G$ tal que

$$ax = u = xa.$$

Diremos que ab es el *producto* de a por b.

1.1.1. *Observaciones.* El elemento u de (ii) en la definición anterior es único pues si u' también verificara (ii) tendríamos:

$$\begin{aligned} uu' = u' = u'u \quad & (a = u' \textit{ en } (ii)) \\ u'u = u = uu' & \end{aligned}$$

de donde

$$u' = u'u = u.$$

Se dice que u es el *elemento neutro* de G. Usualmente denotaremos $1_G = u$ y si no hay posible confusión con el grupo en el que estemos trabajando, simplemente $1 = u$. Si la operación en G la notamos por $(a, b) \mapsto a + b$, la llamaremos *suma* y al elemento neutro 0_G o simplemente 0.

Asimismo, para cada $a \in G$, el elemento x de (iii) en 1.1 es único pues si $y \in G$ cumpliese (iii) tendríamos:

$$ax = u = xa$$
$$ay = u = ya$$

En particular $ax = ay$, luego $x(ax) = x(ay)$, y por la propiedad asociativa,

$$(xa)x = (xa)y,$$

esto es, $ux = uy$, de donde $x = y$.

Al único elemento x de G que cumple

$$ax = u = xa$$

le llamamos *inverso* de a y lo notamos por a^{-1}. Nótese que si $a \in G$, como $aa^{-1} = 1_G = a^{-1}a$, a es el inverso de a^{-1}, esto es,

$$(a^{-1})^{-1} = a.$$

Cuando la operación en G sea la suma, escribiremos $-a$ en vez de a^{-1}.

1.1.2. Simplificación. Sean a, b y c tres elementos de un grupo G.

(1) Si $ab = ac$, entonces $b = c$.

(2) Si $ba = ca$, entonces $b = c$.

En efecto, si $ab = ac$, se tiene $a^{-1}(ab) = a^{-1}(ac)$, luego

$$(a^{-1}a)b = (a^{-1}a)c$$

esto es, $b = 1b = 1c = c$, lo que prueba (1). Análogamente se deduce (2).

1.1.3. Asociatividad generalizada. Los productos que se obtienen al variar las formas de asociar n elementos

$$a_1, \ldots, a_n$$

de un grupo G, *conservando el orden*, son iguales. Notaremos cualquiera de esos productos por $a_1 \ldots a_n$.

Probaremos esto por inducción sobre n. Los casos $n = 1$, 2 son obvios. Supongamos $n > 2$. Debemos demostrar que si $1 < k < l < n$,

(1) $(a_1 \ldots a_k)(a_{k+1} \ldots a_n) = (a_1 \ldots a_l)(a_{l+1} \ldots a_n)$

Sean $a = a_1 \dots a_k$, $b = a_{k+1} \dots a_l$, $c = a_{l+1} \dots a_n$. Por la hipótesis de inducción,

$$a_1 \dots a_l = (a_1 \dots a_k)(a_{k+1} \dots a_l) = ab \text{ y}$$
$$a_{k+1} \dots a_n = (a_{k+1} \dots a_l)(a_{l+1} \dots a_n) = bc.$$

Por ello, probar (1) equivale a probar que

$$a(bc) = (ab)c,$$

lo cual es cierto por la propiedad asociativa.

En particular, esto permite definir, dados un elemento $a \in G$ y un natural $n \in \mathbb{N}$,

$$a^n = \underbrace{a \dots a}_{n}$$

Poniendo $a^0 = 1$, $a^{-n} = (a^{-1})^n$, tenemos definido a^k para cada entero k. La ley de asociatividad generalizada nos permite asimismo deducir que

1.1.3.1.
$$a^m a^n = a^{m+n}$$
$$(a^m)^n = a^{mn}$$

para cualesquiera números enteros m y n y cualquier $a \in G$.

1.1.4. Inverso de un producto. Dados elementos $a_1, \dots, a_n$ en un grupo G se tiene

$$(a_1 \dots a_n)^{-1} = a_n^{-1} \dots a_1^{-1}.$$

Lo probaremos por inducción, Si $n = 1$, es obvio. Si $n > 1$, usando 1.1.3,

$$(a_1 \dots a_n)\left(a_n^{-1} \dots a_1^{-1}\right) = (a_1 \dots a_{n-1})\left(a_n a_n^{-1}\right)\left(a_{n-1}^{-1} \dots a_1^{-1}\right) =$$
$$= (a_1 \dots a_{n-1})\left(a_{n-1}^{-1} \dots a_1^{-1}\right) = 1$$

por la hipótesis de inducción, mientras que

$$\left(a_n^{-1} \dots a_1^{-1}\right)(a_1 \dots a_n) = \left(a_n^{-1} \dots a_2^{-1}\right)\left(a_1^{-1} a_1\right)(a_2 \dots a_n) =$$
$$= \left(a_n^{-1} \dots a_2^{-1}\right)(a_2 \dots a_n) = 1.$$

1.2. Ejemplos

(1) Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ con la suma usual son grupos cuyo neutro es el número cero.

(2) Los conjuntos $\mathbb{Q}^*$, $\mathbb{R}^*$ y $\mathbb{C}^*$ obtenidos a partir de $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ quitando el número cero, son grupos para el producto. No ocurre así con $\mathbb{Z}^*$: el número dos no tiene inverso en $\mathbb{Z}^*$.

(3) Si X es un conjunto no vacío, el conjunto $Biy(X)$ formado por las aplicaciones $X \to X$ que son biyectivas, es un grupo con la operación composición de aplicaciones, cuyo elemento neutro es la *aplicación identidad*

$$1_X : X \to X : x \mapsto x.$$

En efecto, si f y g son biyecciones,

$$(f \circ g)\,(X) = f(g(X)) = f(X) = X,$$

lo que prueba la sobreyectividad de $f \circ g$.

Por otro lado, si x e y son elementos distintos en x, la inyectividad de g nos dice que $g(x) \neq g(y)$, y la de f permite concluir que

$$f(g(x)) \neq f(g(y))$$

y así $f \circ g$ es también inyectiva.

De este modo queda probado que la composición es una operación binaria en $Biy(X)$. El lector puede comprobar que se cumplen las condiciones (i), (ii) y (iii) de 1.1., donde ahora debe leerse $f \circ g$ en vez de fg.

El grupo simétrico S_n

Cuando el conjunto X es finito con n elementos, escribiremos S_n en vez de $Biy(X)$. Este grupo tiene $n!$ elementos pues si $X = \{a_1, ..., a_n\}$, para definir un elemento en S_n tenemos n posibles valores como imagen de a_1, $n-1$ valores como imagen de a_2 (pues al ser biyecciones las imágenes de a_1 y a_2 deben ser distintas), y en general, $n-i$ valores como imagen de a_{i+1}, $i = 0, ..., n-1$, por lo que el número de elementos de S_n es

$$n(n-1) \ldots 3 \cdot 2 \cdot 1 = n!.$$

Nótese que si dos conjuntos X e Y tienen n elementos,

$$Biy(X) = Biy(Y).$$

Más adelante (en Cap. 5) haremos un estudio detallado de los grupos S_n.

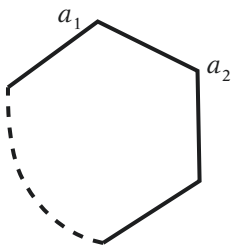
(4) El conjunto $GL_n(\mathbb{R})$ formado por las matrices de orden n con coeficientes en $\mathbb{R}$ cuyo determinante no es nulo, es un grupo con la operación producto de matrices, con elemento neutro la matriz identidad de orden n, I_n, cuyos únicos coeficientes no nulos son los de la diagonal principal, que valen uno.

De hecho, de la fórmula

$$det\,(A \cdot B) = det\,(A) \cdot det\,(B)$$

se deduce en particular que el producto es una operación binaria en $GL_n(\mathbb{R})$ y por otro lado, es sabido que las matrices con determinante no nulo tienen inversa.

(5) Sea $n \geqslant 3$ un número natural y X el polígono regular de n lados, con vértices $a_1, \ldots, a_n$



Decimos que una biyección $f : X \to X$ *conserva la distancia* si

$$\text{dist}(a, b) = \text{dist}(f(a), f(b)) \qquad \text{para cada } a, b \in X.$$

Se llama *n-ésimo grupo diedral* al conjunto

$$D_n = \{f \in Biy(X) : f \text{ conserva la distancia}\}.$$

Es inmediato comprobar que, con la operación composición de aplicaciones, D_n es un grupo. En efecto, la asociatividad para ternas de elementos de D_n es consecuencia de la asociatividad para ternas de elementos en $Biy(X)$.

Evidentemente la aplicación identidad $1_X \in D_n$ pues conserva la distancia. Así 1_X es el elemento neutro en D_n.

Por último, sea $h \in D_n$ y $h^{-1} \in Biy(X)$ la aplicación inversa. Para ver que h posee inversa en D_n basta comprobar que $h^{-1} \in D_n$, es decir, que h^{-1} conserva la distancia.

Sean pues, $a, b \in X$, $p = h^{-1}(a)$, $q = h^{-1}(b)$. Así $h(p) = a$, $h(q) = b$, y como h conserva la distancia,

$$\text{dist}(h(p), h(q)) = \text{dist}(p, q),$$

es decir

$$\text{dist}(a, b) = \text{dist}(h^{-1}(a), h^{-1}(b)).$$

Si $f \in D_n$ y p es un punto situado en el segmento que une a_i con a_{i+1}, se cumple

$$\text{dist}(a_i, a_{i+1}) = \text{dist}(a_i, p) + \text{dist}(p, a_{i+1}),$$

luego

$$\text{dist}(f(a_i), f(a_{i+1})) = \text{dist}(f(a_i), f(p)) + \text{dist}(f(p), f(a_{i+1})).$$

De aquí se sigue que $f(p)$ pertenece al segmento que une $f(a_i)$ con $f(a_{i+1})$. Como f transforma X en X se deduce de lo anterior que envía lados en lados, y por ello, como cada vértice es el punto común a dos lados, la imagen mediante f de un vértice de X es otro vértice de X.

Así pues, si $V = \{a_1, ..., a_n\}$, $f|_V \in Biy(V)$.

Por otro lado, cada $f \in D_n$ queda determinada por las imágenes $f(a_1), ..., f(a_n)$ de los vértices pues dado $p \in X$ estará entre dos vértices consecutivos a_i, a_{i+1}, luego $f(p)$ es el único punto del segmento que une $f(a_i)$ con $f(a_{i+1})$ que dista de éstos lo mismo que p dista de a_i y a_{i+1}.

En consecuencia,

1.2.1. La aplicación $f \to f|_V$ entre D_n y $S_n = Biy(V)$ es inyectiva, lo que nos permite identificar D_n como subconjunto de S_n.

Veamos cuántos elementos tiene D_n. Si $f \in D_n$ y $f(a_1) = a_i$, necesariamente será $f(a_2) = a_{i-1}$ ó a_{i+1}, $f(a_3) = a_{i-2}$, ó a_{i+2}, etc., pues f conserva la distancia. En consecuencia, por cada elección de imagen de a_1 (y hay sólo n posibles imágenes) tenemos dos modos, a lo sumo, de elegir imagen para el resto de los vértices. Por ello,

$$\text{número de elementos de } D_n \leqslant 2n.$$

Veamos que se da la igualdad, y cuáles son los elementos de D_n.

Si 0 es el centro del polígono X, el giro f de centro 0 y ángulo $2\pi/n$ pertenece evidentemente a D_n y f^n es la identidad. Así

$$\{1_X = f^n, f, f^2, ..., f^{n-1}\} \subset D_n$$

y estos elementos son distintos, pues $f^i = f^j$ para ciertos $1 \leqslant i < j \leqslant n$ implica

$$1_X = f^{-j} \circ f^i = f^{-i} \circ f^j = f^{j-i} \qquad \text{por 1.1.3.1}$$

de donde

$$a_1 = 1_X(a_1) = f^{j-i}(a_1) = a_{j-i+1},$$

lo cual es falso.

Por otro lado, la simetría g respecto de la recta que une 0 con a_1, es también elemento de D_n, pues obviamente conserva la distancia y

$$g(a_1) = a_1, g(a_i) = a_{n-i+2}, \quad 2 \leqslant i \leqslant n.$$

Componiendo con las potencias de f, tenemos

$$\{g, g \circ f, ..., g \circ f^{n-1}\} \subset D_n,$$

y así

$$\{1_X, f, f^2, ..., f^{n-1}, g, g \circ f, ..., g \circ f^{n-1}\} \subset D_n.$$

Basta ahora probar que los $2n$ elementos del conjunto de la izquierda son todos distintos, para obtener la igualdad

1.2.2. $D_n = \{1 = 1_X, f, f^2, ..., f^{n-1}, g, g \circ f, ..., g \circ f^{n-1}\}$.

Pero $g \circ f^i = g \circ f^j$ para $1 \leqslant i < j \leqslant n$ implica por 1.1.2

$$f^i = f^j, \text{ que es falso.}$$

Por último, $g \circ f^i = f^j$ para $1 \leqslant i \leqslant j \leqslant n$ implica

$$g = f^{j-i},$$

y en particular

$$a_1 = g(a_1) = f^{j-i}(a_1) = a_{j-i+1},$$

luego $j - i + 1 = 1$, esto es $j - i = 0$, $g = f^0 = 1_X$.

Entonces $a_n = g(a_2) = 1_X(a_2) = a_2$, o sea, $n = 2$, lo cual es imposible.

Definición 1.3. Diremos que el grupo G es **abeliano** si $ab = ba$ para cada par de elementos $a, b \in G$.

1.3.1. Evidentemente los grupos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ con la operación suma y los grupos $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ con la operación producto son abelianos.

1.3.2. Todo grupo con dos elementos es abeliano, pues si u es el elemento neutro y $a \neq u$ es el elemento restante,

$$uu = uu$$
$$aa = aa$$
$$au = a = ua.$$

En particular, S_2 es abeliano.

1.3.3. Para $n \geqslant 3$, S_n no es abeliano. En efecto, sea $X = \{1, 2, ..., n\}$ y $S_n = Biy(X)$. Sean f y g los elementos de S_n definidos por:

$$\begin{array}{ll} f(1) = 2 & g(1) = 2 \\ f(2) = 3 & g(2) = 1 \\ f(3) = 1 & g(k) = k,\ k \geqslant 3 \\ f(k) = k,\ k \geqslant 4 & \end{array}$$

Como $g \circ f(3) = g(1) = 2$, y $f \circ g(3) = f(3) = 1$, resulta

$$g \circ f \neq f \circ g$$

y S_n no es abeliano.

1.3.4. Para $n \geqslant 2$, $GL_n(\mathbb{R})$ no es abeliano. En efecto, la matriz $A = (a_{ij})$ dada por

$$a_{ij} = \begin{cases} 1 \text{ si } i \leq j \\ 0 \text{ si } i > j \end{cases}$$

pertenece a $GL_n(\mathbb{R})$ pues $det\,(A) = 1 \neq 0$. En consecuencia, como $det\,A^t = det\,A$, $A^t \in GL_n(\mathbb{R})$.

Ahora,

$$AA^t = \left(\begin{array}{c|c} n & * \\ \hline * & * \end{array}\right), \quad A^tA = \left(\begin{array}{c|c} 1 & * \\ \hline * & * \end{array}\right),$$

con lo que $AA^t \neq A^tA$.

1.3.5. Para $n \geqslant 3$, D_n no es abeliano.

Utilizando las notaciones de 1.2, consideramos el giro f y la simetría g en D_n. Tenemos

$$g \circ f(a_1) = g(a_2) = a_n, f \circ g(a_1) = f(a_1) = a_2,$$

luego $g \circ f \neq f \circ g$.

Veamos otras caracterizaciones de los grupos abelianos.

Proposición 1.4. Sea G un grupo.

(1) Si $x^2 = 1$ para cada $x \in G$, G es abeliano.

(2) Si $(ab)^2 = a^2b^2$ para cada $a, b \in G$, G es abeliano.

Demostración. (1) Para cada $x \in G$, $x \cdot x = 1 = x \cdot x^{-1}$, luego

$$x = x^{-1} \qquad \text{por} \quad 1.1.2.$$

Ahora, dados a y b en G, tendremos $a = a^{-1}$, $b = b^{-1}$ y si $c = ab$, será

$$ab = c = c^{-1} = (ab)^{-1} = b^{-1}a^{-1} = ba,$$

la penúltima igualdad por 1.1.4. Así G es abeliano.

(2) Dados a y b en G, se cumple

$$a(ba)b = (ab)^2 = a^2b^2 = a(ab)b.$$

Simplificando, mediante 1.1.2, obtenemos $ab = ba$.

Definición 1.5.

Sean G y G' dos grupos, cuyas operaciones notaremos por

$$G \times G \to G : (a, b) \mapsto ab$$
$$G' \times G' \to G' : (a', b') \mapsto a'b'.$$

El producto cartesiano $G'' = G \times G'$ es un grupo con la operación

$$G'' \times G'' \to G'' : ((a, a'), (b, b')) \mapsto (ab, a'b').$$

En efecto, la asociatividad en G'' es consecuencia inmediata de la asociatividad en G y G' y de que la operación en G'' se ha definido coordenada a coordenada. Evidentemente, el elemento $1_{G''} = (1_G, 1_{G'})$ es el neutro en G''. Por último, como

$$(a, b)\,(a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (1_G, 1_{G'}) = 1_{G''}$$

y

$$(a^{-1}, b^{-1})\,(a, b) = (a^{-1}a, b^{-1}b) = (1_G, 1_{G'}) = 1_{G''},$$

el elemento (a^{-1}, b^{-1}) es el opuesto, en G'', de (a, b).

Nótese además que si G y G' son abelianos, también lo es G''. Recíprocamente, si G'' es abeliano, dados $a, b \in G$ se tiene

$$(a, 1_{G'})\,(b, 1_{G'}) = (b, 1_{G'})\,(a, 1_{G'}),$$

es decir,

$$(ab, 1_{G'}) = (ba, 1_{G'}),$$

luego $ab = ba$ y G es abeliano. Análogamente se prueba que G' es abeliano. En general, dados grupos $G_1, \ldots, G_r$, se define por recurrencia

$$G_1 \times \ldots \times G_r = (G_1 \times \ldots \times G_{r-1}) \times G_r.$$

Se dice que $G_1 \times \ldots \times G_r$ es el **producto directo** de los grupos $G_1, \ldots, G_r$.

II. SUBGRUPOS

Definición 1.6. Un subconjunto no vacío H de un grupo G es un *subgrupo* de G si, con la misma operación de G, H es un grupo.

1.6.1. Observaciones. Sea H un subgrupo de un grupo G.

1.6.1.1. 1_G pertenece a H y es su elemento neutro.

1.6.1.2. Si $x \in H$, también $x^{-1} \in H$.

Demostración. Por definición H tiene un elemento neutro al que llamamos u. Desde luego, $uu = u$. Sea $u^{-1} \in G$ el inverso de u en G. Operando en G,

$$u^{-1}(uu) = u^{-1}u = 1_G,$$

luego

$$(u^{-1}u)\, u = 1_G,$$

esto es,

$$1_G u = 1_G,$$

o sea, $u = 1_G$. Esto prueba (1.6.1.1).

Si $x \in H$ existe $y \in H$ tal que $xy = 1_G = yx$, pues ya hemos visto que 1_G es el elemento neutro de H. Así,

$$xx^{-1} = xy,$$

y aplicando la propiedad cancelativa,

$$x^{-1} = y \in H.$$

La siguiente proposición caracteriza de modo sencillo la condición de ser subgrupo.

Proposición 1.7. Sea H un subconjunto no vacío de un grupo G. Las siguientes condiciones son equivalentes:

(1) H es un subgrupo de G.

(2) Para cada par de elementos $x, y \in H$, $xy^{-1} \in H$.

Demostración. (1) $\Rightarrow$ (2). En virtud de 1.6.1.2, $y^{-1} \in H$. El producto es operación binaria en H, porque H es subgrupo. Así, como $x, y^{-1} \in H$, se concluye que $xy^{-1} \in H$.

(2) $\Rightarrow$ (1). Sea $x \in H$ (existe, pues H no es vacío). Ahora la hipótesis usada con $y = x$ nos dice que

$$xx^{-1} \in H,$$

esto es $1_G \in H$, luego H posee elemento neutro.

Además, si $y \in H$, como $x = 1_G \in H$, tenemos

$$y^{-1} = 1_G y^{-1} = xy^{-1} \in H,$$

y así cada elemento de H tiene inverso en H.

Finalmente, dados $x, y \in H$, ya sabemos que $z = y^{-1} \in H$, luego

$$xy = x(y^{-1})^{-1} = xz^{-1} \in H,$$

lo que prueba que la operación de G es una operación binaria de H.

Sólo queda probar que la operación, cuando involucra elementos de H, es asociativa, pero esto es obvio, pues lo es para cualquier terna de elementos de G.

1.7.1. Observación. Evidentemente $\{1_G\}$ y G son subgrupos de cualquier grupo G. Llamaremos *subgrupos propios* de G a aquellos subgrupos *distintos* de $\{1_G\}$ y G.

1.8. Ejemplos

1.8.1. Los subgrupos de $\mathbb{Z}$ son los conjuntos de la forma

$$m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$$

para cada entero no negativo m.

Desde luego $m\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$, pues no es vacío, ya que $m = m1 \in m\mathbb{Z}$, y si $a = mx$, $b = my$ pertenecen a $m\mathbb{Z}$, $a-b = m(x-y) \in m\mathbb{Z}$. En virtud de 1.7 (aquí la notación es aditiva), $m\mathbb{Z}$ es subgrupo de $\mathbb{Z}$.

Recíprocamente sea H un subgrupo de $\mathbb{Z}$. Si H consta sólo del número cero, $H = 0\mathbb{Z}$ tiene la forma requerida. Si H tiene algún elemento no nulo, tiene alguno positivo en virtud de 1.6.1.2. Si m es el menor entero positivo en H, cualquier otro $n \in H$ positivo será

$$n = qm + r, \qquad 0 \leqslant r < m.$$

Como $qm = \underbrace{m + \ldots + m}_{q} \in H$, $r = n-qm \in H$ y es menor que m, luego,

por la elección de m, no es positivo. Así $r = 0$, y por lo tanto,

1.8.1.1. $$n = qm = mq \in m\mathbb{Z}.$$

Si $n \in H$ es negativo, $-n \in H$ y es positivo, luego

$$-n = mx \in m\mathbb{Z}$$

para algún entero x. Así

1.8.1.2. $$n = m(-x) \in m\mathbb{Z}.$$

Como también $0 = m0 \in m\mathbb{Z}$, de 1.8.1.1 y 1.8.1.2 deducimos que $H \subset m\mathbb{Z}$.

Pero como $m \in H$ también $-m \in H$, y así para cada $x \in \mathbb{Z}$,

$$mx = \begin{cases} \underbrace{m + \ldots + m}_{x} \in H & \text{si } x > 0 \\ 0 \in H & \text{si } x = 0 \\ \underbrace{(-m) + \ldots + (-m)}_{-x} & \text{si } x < 0 \end{cases}$$

con lo que $H = m\mathbb{Z}$.

1.8.2. Para cada $n \geqslant 3$, D_n es subgrupo de S_n.

De hecho, en 1.2 vimos que $D_n \subset S_n$ y que D_n es grupo con la misma operación (composición de aplicaciones) que S_n.

Uno de los modos habituales de construir grupos es:

Definición 1.8.3. Si S es un subconjunto no vacío de un grupo G, el conjunto

$$\langle S \rangle = \left\{ s_1^{h_1} \ldots s_n^{h_n} : n \in \mathbb{N},\ s_i \in S,\ h_i \in \mathbb{Z},\ 1 \leq i \leq n \right\}$$

es un subgrupo de G que contiene a S, llamado *subgrupo generado por* S.

Observaciones

1.8.3.1. $\langle S \rangle = \{x_1 \ldots x_m : m \in \mathbb{N},\ x_i \in S,\ \text{ó } x_i^{-1} \in S,\ 1 \leqslant i \leqslant m\}$.

Si $\mathcal{F}_S$ es la familia de todos los subgrupos de G que contienen a S,

1.8.3.2. $$\langle S \rangle = \bigcap_{H \in \mathcal{F}_S} H$$

y en particular, $\langle S \rangle \subset H$ para cada $H \in \mathcal{F}_S$.

Demostración. Cada $s \in S$ se escribe $s = s^1 \in \langle S \rangle$. Esto prueba que $S \subset \langle S \rangle$. En particular $\langle S \rangle$ no es vacío, por no serlo S.

Dados $x = s_1^{h_1} \ldots s_n^{h_n}$; $y = t_1^{\ell_1} \ldots t_m^{\ell_m}$, $x, y \in \langle S \rangle$ con

$$n, m \in \mathbb{N},\ s_1, \ldots, s_n, t_1, \ldots, t_m \in S,\ h_1, \ldots, h_n, \ell_1, \ldots, \ell_m \in \mathbb{Z},$$

como

$$y^{-1} = t_m^{-\ell_m} \ldots t_1^{-\ell_1}$$