
ÁLGEBRA II

Primer Cuatrimestre — 2007

Práctica 1: Grupos

1. Definiciones

1.1. Exponentes pequeños. El *exponente* de un grupo G es el menor número e tal que para todo $g \in G$ se tiene $g^e = 1$.

- [1] (a) Mostrar que un grupo G tal que $g^2 = 1$ para todo $g \in G$ es abeliano.
 [3] †(b) ¿Qué puede decir si se tiene en cambio que $g^3 = 1$?

Solución. Supongamos que G es un grupo no abeliano tal que $g^3 = 1$ para todo $g \in G$ y supongamos que no posee subgrupos propios con esta propiedad. Entonces existen elementos $x, y \in G$ tales que $xy \neq yx$ y debe ser $G = \langle x, y \rangle$.

Notemos que si $u, v \in G$, entonces $(uv)^3 = uvuvuv = 1$, de manera que

$$uvu = v^{-1}u^{-1}v^{-1}, \quad \forall u, v \in G.$$

Sea $z = y^{-1}x^{-1}yx$, de manera que $yx = xyz$. Entonces

$$\begin{aligned} yzy^{-1}z^{-1} &= y \cdot y^{-1}x^{-1}yx \cdot y^{-1} \cdot x^{-1}y^{-1}xy = x^{-1}y \underbrace{x^{-1}y^{-1}x^{-1}y^{-1}xy}_{=1} \\ &= \underbrace{x^{-1}yx^{-1}x^{-1}y^{-1}x^{-1}y^{-1}xy}_{=1} = y^{-1}xy^{-1} \underbrace{x^{-1}y^{-1}x^{-1}y^{-1}xy}_{=1} \\ &= y^{-1}xy^{-1} \underbrace{yxxy^{-1}xy}_{=1} = y^{-1}x^3y = 1 \end{aligned}$$

y

$$\begin{aligned} xzx^{-1}z^{-1} &= x \cdot y^{-1}x^{-1}yx \cdot x^{-1} \cdot x^{-1}y^{-1}xy = xy^{-1}x^{-1} \underbrace{y^{-1}x^{-1}y^{-1}xy}_{=1} \\ &= x \underbrace{y^{-1}x^{-1}y^{-1}y^{-1}x^{-1}y^{-1}xy}_{=1} = xxyx \underbrace{y^{-1}x^{-1}y^{-1}xy}_{=1} \\ &= xxyxxyxxy = (x^2y)^3 = 1 \end{aligned}$$

Vemos así que x e y conmutan con z .

Usado esto es fácil ver que todo elemento de G puede escribirse en la forma $x^i y^j z^k$ con $0 \leq i, j, k \leq 2$.

Calculando vemos que $[x^i y^j z^k, x] = z^j$ y que $[x^i z^k, y] = z^{2i}$. Entonces, si $x^i y^j z^k = x^{i'} y^{j'} z^{k'}$, tenemos que

$$z^j = [x^i y^j z^k, x] = [x^{i'} y^{j'} z^{k'}, x] = z^{j'}$$

y, como $z \neq 1$, esto implica que $j = j'$. Luego debe ser $x^i z^k = x^{i'} z^{k'}$ y

$$z^{2i} = [x^i z^k, y] = [x^{i'} z^{k'}, y] = z^{2i'}$$

y vemos que $i = i'$. Por supuesto, debe ser entonces $k = k'$. Hemos probado que la escritura de un elemento de G en la forma $x^i y^j z^k$ es *única*. En particular, G posee 27 elementos.

Calculando, vemos que

$$x^i y^j z^k \cdot x^{i'} y^{j'} z^{k'} = x^{i+i'} y^{j+j'} z^{k+k'+i'j}$$

Es fácil ver que esta fórmula define de hecho un grupo no abeliano en el que todo elemento tiene orden 3.

Notemos que podemos describir este grupo a menos de isomorfismo como $(\mathbb{Z}_3 \oplus \mathbb{Z}_3) \rtimes_{\theta} \mathbb{Z}_3$ con $\theta : \mathbb{Z}_3 \rightarrow \text{Aut}(\mathbb{Z}_3 \oplus \mathbb{Z}_3)$ determinado por la condición de que

$$\theta(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Imitando esta construcción es posible contruir ejemplos de grupos no abelianos en los que todos los elementos tienen orden p para cada número primo p . \square

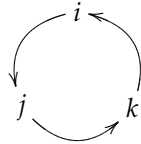
- [1] 1.2. Encontrar todos los grupos de orden a lo sumo 6.
- [2] [†]1.3. Mostrar que los tres axiomas de grupo—la asociatividad, la existencia de elemento neutro y la existencia de inversos—son independientes.

2. Ejemplos

- [1] 2.1. (a) Sea $n \in \mathbb{N}$ y sea $\mathbb{G}_n = \{z \in \mathbb{C} : z^n = 1\}$. Mostrar que \mathbb{G}_n , con respecto al producto de \mathbb{C} es un grupo abeliano cíclico.
- [1] (b) Sea $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. Mostrar que S^1 , con respecto al producto de \mathbb{C} , es un grupo abeliano. ¿Es cíclico?
- [1] 2.2. Sea \mathbb{H} el conjunto de 8 elementos $\{\pm 1, \pm i, \pm j, \pm k\}$ dotado del producto dado por la siguiente ecuaciones:

$$\begin{aligned} i \cdot j &= k, & j \cdot k &= i, & k \cdot i &= j, \\ j \cdot i &= -k, & k \cdot j &= -i, & i \cdot k &= -j, \\ i \cdot i &= j \cdot j = k \cdot k &= -1, \end{aligned}$$

y la regla usual de los signos. Mostrar que (\mathbb{H}, \cdot) es un grupo no abeliano. Llamamos a \mathbb{H} el *grupo de cuaterniones*. El siguiente diagrama permite recordar la tabla de multiplicación de \mathbb{H} .



- [1] 2.3. Sea k un cuerpo y $n \in \mathbb{N}$. Ponemos

$$\text{GL}_n(k) = \{A \in M_n(k) : \det A \neq 0\}$$

y

$$\text{SL}_n(k) = \{A \in M_n(k) : \det A = 1\}.$$

Mostrar que, dotados de la multiplicación usual de matrices, estos dos conjuntos resultan ser grupos. Descríbalos para $n = 1$. ¿Cuándo son abelianos?

- [1] 2.4. *Grupo opuesto*. Sea G un grupo. Sea (G^{op}, \cdot) tal que $G^{\text{op}} = G$ como conjunto, y el producto es

$$\cdot : (g, h) \in G^{\text{op}} \times G^{\text{op}} \mapsto hg \in G^{\text{op}}.$$

Mostrar que (G^{op}, \cdot) es un grupo.

2.5. Sea G un grupo y X un conjunto.

- [1] (a) Sea $G^X = \{f : X \rightarrow G\}$ dotado del producto $\cdot : G^X \times G^X \rightarrow G^X$ dado por

$$(f \cdot g)(x) = f(x)g(x), \quad \forall f, g \in G^X, \forall x \in X.$$

Mostrar que G^X es un grupo. ¿Cuándo es abeliano?

- [1] (b) Sea $x_0 \in X$ y sea $H_{x_0} = \{f \in G^X : f(x_0) = 1\}$. Mostrar que H_{x_0} es un subgrupo de G . ¿Es normal?

- [1] 2.6. *Producto directo*. Sean G y H dos grupos. Consideremos la operación \cdot sobre el conjunto $K = G \times H$ dada por

$$\cdot : ((g_1, h_1), (g_2, h_2)) \in K \times K \mapsto (g_1 g_2, h_1 h_2) \in K.$$

Mostrar que K es un grupo. Llamamos a K el *producto directo de G y H* y lo notamos $G \times H$.

2.7. \mathbb{F}_p -espacios vectoriales.

- [2] (a) Sea G un grupo abeliano y sea p un número primo. Supongamos que todo elemento de G tiene orden p . Mostrar que es posible definir una multiplicación $\cdot : \mathbb{F}_p \times G \rightarrow G$ por escalares de \mathbb{F}_p de manera que $(G, +, \cdot)$ resulte un \mathbb{F}_p -espacio vectorial.
- [2] (b) Supongamos además que G es finito. Mostrar que existe $n \in \mathbb{N}_0$ tal que

$$G \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ veces}}.$$

3. Subgrupos

- [1] 3.1. Sea G un grupo y $H \subset G$ un subconjunto. Mostrar que las siguientes afirmaciones son equivalentes:

- (i) H es un subgrupo de G .
 (ii) H es no vacío y cualesquiera sean $x, y \in H$, es $xy^{-1} \in H$.

Si además G es finito, estas afirmaciones son equivalentes a:

- (c) H es no vacío y cualesquiera sean $x, y \in H$, es $xy \in H$.

Dar un contraejemplo para esta última equivalencia cuando G es infinito.

3.2. Sea G un grupo y H_1 y H_2 subgrupos de G .

- [1] (a) $H_1 \cap H_2$ es un subgrupo de G .
 [1] (b) $H_1 \cup H_2$ es un subgrupo de G sii $H_1 \subset H_2$ o $H_2 \subset H_1$.

- [2] 3.3. Dado un grupo G , ¿es el subconjunto de elementos de orden finito un subgrupo de G ?

3.4. Sea G un grupo.

- [1] (a) Sea \mathcal{H} una familia de subgrupos de G . Mostrar que $\bigcap_{H \in \mathcal{H}} H$ es un subgrupo de G .

- [1+] (b) Sea ahora $X \subset G$ un subconjunto arbitrario. Mostrar que existe un menor subgrupo de G que contiene a X . Describirlo en término de los elementos de X .

El subgrupo cuya existencia se afirma en la segunda parte de este ejercicio se denomina el *subgrupo de G generado por X* y se denota $\langle X \rangle$. Si $X = \{x_1, \dots, x_r\}$, escribimos $\langle x_1, \dots, x_r \rangle$ en lugar de $\langle \{x_1, \dots, x_n\} \rangle$.

- [1] 3.5. Sea G un grupo, $X \subset G$ un subconjunto tal que $G = \langle X \rangle$ y sea N un subgrupo de G . Mostrar que N es normal en G sii $xNx^{-1} \subset N$ para todo $x \in X$.

- [1+] 3.6. Sea $n \in \mathbb{N}$ y sea $\omega \in \mathbb{G}_{2^n}$ una raíz primitiva 2^n -ésima. Consideremos las matrices

$$R = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

y sea $\mathbb{H}_n = \langle R, S \rangle$ el subgrupo generado por R y S en $\text{GL}_2(\mathbb{C})$. Llamamos a \mathbb{H}_n el *n -ésimo grupo de cuaterniones generalizados*.

Determinar el orden de \mathbb{H}_n y listar sus elementos.

- [1] 3.7. (a) Sea $G = \text{GL}_2(\mathbb{Z})$ y sean $\alpha, \beta \in G$ dados por

$$\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Muestre que $\alpha^4 = \beta^3$, pero que $\alpha\beta$ tiene orden infinito. Así, $\langle \alpha, \beta \rangle$ es infinito.

Este ejemplo muestra que finitos elementos de orden finito pueden generar un subgrupo infinito.

- (b) Determine $\langle \alpha, \beta \rangle$.

Solución. Escribamos $G = \langle \alpha, \beta \rangle$. Afiramos que $G = \text{SL}_2(\mathbb{Z})$. Es $\alpha\beta = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, así que calculando vemos inmediatamente que $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = (\alpha\beta)^x \in G$ para todo $x \in \mathbb{Z}$.

Sea $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ y mostremos que $A \in G$ haciendo inducción sobre $m = c + d$.

Como

$$A\alpha = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}, \quad A\alpha^2 = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}, \quad A\alpha^3 = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix},$$

podemos suponer que $c, d \geq 0$ sin pérdida de generalidad.

Para empezar, si $m = 1$, debe ser $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ ó $A = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}$. En el primer caso debe ser $a = 1$ y vemos que $A = (\alpha\beta)^b$. En el segundo debe ser $b = -1$, y calculando vemos que $A = (\alpha\beta)^a\alpha$.

Supongamos que $m > 1$. Notemos que debe ser $cd \neq 0$. Si $c \geq d$, entonces es

$$A\beta = \begin{pmatrix} -b & a-b \\ -d & c-d \end{pmatrix}.$$

Si $c = d$, entonces $d = 1$ y $A\beta\alpha^2 = \begin{pmatrix} b & b-a \\ 1 & 0 \end{pmatrix}$, que sabemos ya que está en G . Si, por otro lado, $c > d$, entonces $|d| + |c - d| < m$, así que $A\beta$ está en G , por nuestra hipótesis inductiva. \square

3.8. Generación de S_n .

- [1] (a) Mostrar que
(i) $S_n = \langle \{(ij) : 1 \leq i < j \leq n\} \rangle$;

- (ii) $S_n = \langle \{(1i) : 1 \leq i \leq n\} \rangle$;
 (iii) $S_n = \langle \{(i i+1) : 1 \leq i < n\} \rangle$;
 (iv) $S_n = \langle (12), (123 \dots n) \rangle$;
 [1+] †(b) Sea $\mathcal{T} = \{(ij) : 1 \leq i < j \leq n\}$ el conjunto de todas las transposiciones. Encuentre una condición necesaria y suficiente para que un subconjunto $T \subset \mathcal{T}$ para que $S_n = \langle T \rangle$.

3.9. Sea G un grupo.

- [1] (a) Sea \mathcal{H} una familia de subgrupos normales de G . Mostrar que $\bigcap_{H \in \mathcal{H}} H$ es un subgrupo normal de G .
 [1] (b) Sea $X \subset G$ un subconjunto arbitrario. Mostrar que existe un menor subgrupo normal de G que contiene a X . Describirlo en término de los elementos de X .

El subgrupo cuya existencia se afirma en la segunda parte de este ejercicio se denomina el *subgrupo normal de G generado por X* . En general, este subgrupo no coincide con el subgrupo generado por X , construido en 3.4.

- [1] (c) Supongamos que $X \subset G$ es un conjunto tal que, cualquiera sea $g \in G$, es $gXg^{-1} \subset X$. Mostrar que entonces el subgrupo normal generado por X coincide con el subgrupo generado por X .
3.10. (a) Sea G un grupo y sea $N \subset G$ un subgrupo tal que $gNg^{-1} \subset N$ para todo $g \in G$. Muestre que N es normal.

Solución. Sea $g \in G$. Entonces como $gNg^{-1} \subset N$, es $N = g^{-1}gNg^{-1}g \subset g^{-1}Ng$. Así, $gNg^{-1} \supset N$ para todo $g \in G$. Esto, junto con la hipótesis, implica que N es normal

- (b) Sea $G = \text{GL}_2(\mathbb{Q})$ y $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\} \subset G$. Entonces H es un subgrupo de G . Sea ahora $g = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} \in G$. Muestre que $gHg^{-1} \subsetneq H$.

3.11. Si G es un grupo y $A, B \subset G$ son subconjuntos, definimos

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

Consideremos un grupo G y $A, B \subset G$ dos subconjuntos arbitrarios.

- [1] (a) AB es un subgrupo de G sii $AB = BA$.
 [1] (b) $G = AB$ sii $G = \langle A, B \rangle$ y $AB = BA$.
 [1] (c) Si $AB = BA$ y $C \subset G$ es un subgrupo tal que $A \subset C$, entonces $AB \cap C = A(B \cap C)$.
 [1] (d) Si $G = AB$ y $C \subset G$ es un subgrupo tal que $A \subset C$, entonces $C = A(B \cap C)$.

3.12. Sea G un grupo. Si $a, b \in G$, escribimos $[a, b] = aba^{-1}b^{-1}$; $[a, b]$ es el *conmutador de a y b* . Claramente $[a, b] = 1$ sii a y b conmutan, así que en cierta forma $[a, b]$ mide la no-conmutatividad de a y b .

- [1] (a) Sea $X = \{[a, b] : a, b \in G\}$ y sea $G' = \langle X \rangle$ el subgrupo generado por X en G . Mostrar que G' es normal en G . Llamamos a G' es *subgrupo derivado de G* y lo escribimos $[G, G]$.
 [1] (b) G es abeliano sii $[G, G] = 1$.

- [1] (c) Determinar $[G, G]$ cuando G es \mathbb{H} o un grupo diedral D_n .
Un grupo es *perfecto* si coincide con su subgrupo derivado.
- [3] [†](d) Sea k un cuerpo finito. Mostrar que $[\mathrm{GL}_n(k), \mathrm{GL}_n(k)] = \mathrm{SL}_n(k)$ con la excepción de $\mathrm{GL}_2(\mathbb{F}_2)$. Mostrar que $\mathrm{SL}_n(k)$ es perfecto con la excepción de $\mathrm{SL}_2(\mathbb{F}_2)$ y $\mathrm{SL}_2(\mathbb{F}_3)$. ¿Qué sucede en los casos excepcionales?
- [1] **3.13.** (a) Sea G un grupo y sea $Z(G) = \{g \in G : gh = hg \text{ para todo } h \in G\}$. Mostrar que $Z(G)$ es un subgrupo normal de G . Llamamos a $Z(G)$ el *centro de G* y decimos que los elementos de $Z(G)$ son *centrales* en G .
- [1] (b) Sea G un grupo y $X \subset G$ un subconjunto tal que $G = \langle X \rangle$. Mostrar que es

$$Z(G) = \{g \in G : gx = gx \text{ para todo } x \in X\}.$$

- [1+] (c) Encontrar el centro de un grupo abeliano, de D_n para cada $n \geq 1$, de \mathbb{H} , de S_n para cada $n \geq 1$, de $\mathrm{GL}_n(R)$ para cada $n \geq 1$ y $R \in \{\mathbb{R}, \mathbb{Z}, \mathbb{C}, \mathbb{F}_p\}$.
- [1] (d) Sea G un grupo y X un conjunto. Determinar el centro de G^X .
- [1] **3.14.** Sea G un grupo y H un subgrupo abeliano de G . Mostrar que $HZ(G)$ es un subgrupo abeliano de G .
- 3.15.** Sea G un grupo.
- [1] (a) Sea $g \in G$. El *centralizador de g en G* es el subconjunto $C(g) = \{h \in G : gh = hg\}$. Mostrar que se trata de un subgrupo de G y que es, en efecto, el subgrupo más grande de G que contiene a g y en el que g es central.
- [1] (b) Sea $N \subset G$ un subconjunto. El *centralizador de N en G* es el subconjunto $C(N) = \{h \in G : nh = hn \text{ para cada } n \in N\}$. Mostrar que se trata de un subgrupo de G .
- [1] (c) Muestre que si $N \subset G$ es un subconjunto, $C(\langle N \rangle) = C(N)$.
- [1] (d) Sea $H \subset G$ un subgrupo de G . El *normalizador de H en G* es el subconjunto $N(H) = \{g \in G : gH = Hg\}$. Mostrar que se trata de un subgrupo de G . Mostrar, más aún, que H es un subgrupo normal de $N(H)$.
- [1] (e) Si $N \subset G$ es un subconjunto normal (es decir, si para cada $g \in G$, gNg^{-1}), entonces $Z(N)$ es un subgrupo normal de G .

- [1+] **3.16.** Si $g = (i_1 i_2 \cdots i_{k-1} i_k) \in S_n$ es un ciclo de orden k , determinar $C(g)$.
- 3.17.** Sea G un grupo y S y T subconjuntos de G tales que $S \subset T$. Entonces:

- [1] (a) $C(S) \supset C(T)$;

Solución. Si $g \in C(T)$, entonces para cada $t \in T$ es $gt = tg$. Como $S \subset T$, vemos que para cada $s \in S$ es $gs = sg$ y, entonces, que $C(S) \subset C(T)$. \square

- [1] (b) $C(C(S)) \supset S$; y

Solución. Sea $s \in S$. Si $c \in C(S)$, entonces $cs = sc$. Luego s conmuta con todos los elementos de $C(S)$ y esto nos dice precisamente que $s \in C(C(S))$.

[1+] (c) $C(C(C(S))) = C(S)$.

Solución. Como $S \subset C(C(S))$, usando (a) vemos que $C(S) \supset C(C(C(S)))$. Por otro lado $C(C(C(S))) \supset C(S)$ aplicando (b). \square

3.18. Sea G un grupo y $g \in G$. Entonces:

- [1] (a) $g \in C(g)$;
 [1] (b) $C(C(g)) = Z(C(g))$;
 [1+] (c) $C(g) \subset C(h)$ sii $h \in Z(C(g))$; y
 [1+] (d) $C(g) \subset C(h)$ sii $Z(C(g)) \supset Z(C(h))$.

3.19. Sean G un grupo y H y K subgrupos de G .

- [1] (a) Si alguno de H o K es normal en G entonces HK es un subgrupo.
 [1] (b) Si los dos son normales, entonces $HK = KH$ y se trata de un subgrupo normal de G .

[1] **3.20.** Sea G un grupo y N un subgrupo normal de G . Mostrar que $[N, G] \subset N$.

[†]**3.21.** El objetivo de este ejercicio es dar un ejemplo de que la normalidad de subgrupos no es transitiva.

- [1] (a) Sea G el conjunto de todas las funciones $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ que pueden escribirse en la forma

$$f \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by + e \\ cx + dy + f \end{pmatrix}$$

para ciertos $a, b, c, d, e, f \in \mathbb{R}$ con $ad - bc \neq 0$. Mostrar que G , con respecto a la composición de funciones, es un grupo.

- [1] (b) Sea T el subconjunto de G formado por las funciones $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ que pueden escribirse en la forma

$$f \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + e \\ y + f \end{pmatrix}$$

para ciertos $e, f \in \mathbb{R}$. Mostrar que T es un subgrupo *normal* en G .

- [1] (c) Sea L el subconjunto de T formado por las funciones $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ que pueden escribirse en la forma

$$f \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + e \\ y + f \end{pmatrix}$$

para ciertos $e, f \in \mathbb{Z}$. Mostrar que se trata de un subgrupo de T ; como T es abeliano, L es normal en T .

- [1] (d) Mostrar que L no es normal en G .

[1+] **3.22.** Encontrar todos los subgrupos de D_4 . Clasifíquelos bajo isomorfismo y determinar cuáles son normales.

- [2-] **3.23.** Sea \mathbb{H} el grupo de los cuaterniones. Mostrar que posee un único elemento de orden 2 y que éste es central. Deducir que $H \not\cong D_4$ y que todo subgrupo de H es normal.

Un grupo no abeliano con esta propiedad se dice *Hamiltoniano*. El siguiente teorema de Reinhold Baer (1902–1979) describe completamente esta clase de grupos:

Teorema. (R. Baer, Situation der Untergruppen und Struktur der Gruppe, S. B. Heidelberg. Akad. Wiss. 2 (1933), 12-17) *Un grupo finito es hamiltoniano sii es isomorfo a $\mathbb{H} \times A$ para algún grupo abeliano que no tiene elementos de orden 4.*

- [2-] **3.24.** Sea G un grupo y N un subgrupo normal de G de índice finito n . Mostrar que si $g \in G$, entonces $g^n \in N$. Dar un ejemplo para mostrar que esto puede ser falso si N no es normal.

- [2-] **3.25.** (a) Mostrar que un grupo no trivial sin subgrupos propios es cíclico de orden primo.

Solución. Sea G un grupo no trivial sin subgrupos propios y sea $g \in G \setminus \{1\}$. Entonces $\langle g \rangle$ es un subgrupo no trivial, así que la hipótesis implica que $G = \langle g \rangle$ y vemos que G es cíclico.

Si $|g|$ no es primo y existe $k > 1$ tal que $k \mid |g|$, entonces $\langle g^k \rangle$ es un subgrupo propio no trivial de $\langle g \rangle = G$. Esto contradice la hipótesis. Luego $|G| = |g|$ es primo. \square

- [2-] (b) Sea G un grupo cíclico y $g \in G$ un generador. Sea $n = |G|$ y sea p un número primo tal que $p \mid n$. Entonces $\langle g^p \rangle$ es un subgrupo maximal de G .

Solución. Supongamos por el contrario que $\langle g^p \rangle$ no es maximal, de manera que existe $k \in \mathbb{N}$ tal que $\langle g^p \rangle \subsetneq \langle g^k, g^p \rangle \subsetneq \langle g \rangle$. Si notamos que $\langle g^k, g^p \rangle = \langle g^{k-p}, g^p \rangle$ vemos que podemos suponer sin pérdida de generalidad que $0 < k < p$. Pero entonces existen $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha k + \beta p = 1$ y, en particular, $g = (g^k)^\alpha (g^p)^\beta \in \langle g^k, g^p \rangle$, contradiciendo nuestra hipótesis. \square

- [2] (c) Mostrar que un grupo finito que posee un solo subgrupo maximal es cíclico que tiene como orden una potencia de un número primo.

Solución. Sea G un grupo con un único subgrupo maximal M . Sea $g \in G \setminus M$. Entonces $\langle g \rangle \not\subset M$ así que debe ser $G = \langle g \rangle$. Pongamos $n = |g|$.

Sea p un divisor primo de n . Entonces el ejercicio anterior implica que $\langle g^p \rangle$ es un subgrupo maximal de G . Vemos así que $M = \langle g^p \rangle$ y, en particular, $|M| = n/p$. Si n posee otro divisor primo $q \neq p$, entonces el mismo razonamiento muestra que $|M| = n/q$. Por supuesto, esto es absurdo.

Concluimos así que n posee exactamente un divisor primo. \square

- [2] [†]**3.26.** Sea G un grupo finito y H el subgrupo de G generado por los elementos de orden impar. Entonces H es normal y tiene índice una potencia de 2.

Solución. Que H es normal es claro en vista de 3.9(c), porque el conjunto generador de H es normal. Resta ver que $[G : H]$ es una potencia de 2.

Supongamos por el contrario que existe un primo impar p que divide a $[G : H]$. Entonces existe $g \in G \setminus H$ tal que gH tiene orden p en G/H , es decir, tal que $g^p \in H$. Escribamos $|g| = p^r m$ con $(p, m) = 1$. Claramente g^m tiene orden p^r , que es impar, así que $g^m \in H$. Como existen α y $\beta \in \mathbb{Z}$ tales que $\alpha p + \beta m = 1$, concluimos que $g = (g^p)^\alpha (g^m)^\beta \in H$, contradiciendo la elección de g . \square

[†]**3.27. Subgrupo de Frattini.** Sea G un grupo. Sea \mathcal{M} el conjunto de subgrupos propios maximales de G . Si $\mathcal{M} \neq \emptyset$, ponemos $\Phi(G) = \bigcap_{M \in \mathcal{M}} M$; si, en cambio, $\mathcal{M} = \emptyset$, ponemos $\Phi(G) = G$. $\Phi(G)$ es el *subgrupo de Frattini*, en honor de Giovanni Frattini (1852–1925, Italia).

- [1] (a) Determinar el subgrupo de Frattini de \mathbb{Z}_{p^2} si p es primo.

Un elemento $g \in G$ es un *no-generador* si siempre que $X \subset G$ es un conjunto generador de G y $g \in X$, entonces $X \setminus \{g\}$ también genera a G .

- [3] (b) Mostrar que $\Phi(G)$ es el conjunto de elementos no-generadores de G .

Solución. Sea \mathcal{N} el conjunto de elementos no-generadores de G .

Supongamos primero que $\mathcal{M} \neq \emptyset$. Sea $g \in G$ tal que existe $M \in \mathcal{M}$ con $g \notin M$. Entonces $M \subsetneq \langle M \cup \{g\} \rangle$ y debe ser $\langle M \cup \{g\} \rangle = G$. Pero M no genera a G , así que vemos que $g \notin \mathcal{N}$. Esto muestra que $\mathcal{N} \subset \Phi(G)$. Por otro lado, si $g \notin \mathcal{N}$, existe $X \subset G$ tal que $\langle X \rangle = G$ pero $\langle X \setminus \{g\} \rangle \neq G$. Sea $M \in \mathcal{M}$ tal que $\langle X \setminus \{g\} \rangle \subset M$. Entonces claramente $g \notin M$ y vemos que $g \notin \Phi(M)$. Concluimos que $\mathcal{N} \supset \Phi(G)$ y que, entonces, se tiene de hecho la igualdad.

Supongamos ahora que $\mathcal{M} = \emptyset$. En este caso tenemos que mostrar que $\mathcal{N} = G$. Buscando una contradicción, supongamos que $g \in G \setminus \mathcal{N}$, de manera que existe $X \subset G$ tal que $\langle X \rangle = G$ pero $\langle X \setminus \{g\} \rangle \subsetneq G$.

Consideremos la familia $\mathcal{F} = \{H \subset G : H \text{ es subgrupo de } G, X \setminus \{g\} \subset H \text{ y } g \notin H\}$, que no es vacía porque $\langle X \setminus \{g\} \rangle \in \mathcal{F}$. El lema de Zorn nos provee inmediatamente de un elemento $M \in \mathcal{F}$ maximal en \mathcal{F} . Afirmamos que M es de hecho maximal. En efecto, si $h \in G \setminus M$, es $\langle M \cup \{h\} \rangle \supsetneq M$, así que $\langle M \cup \{h\} \rangle \notin \mathcal{F}$. Como claramente $X \setminus \{g\} \subset \langle M \cup \{h\} \rangle$, debe ser $g \in \langle M \cup \{h\} \rangle$ y entonces $\langle M \cup \{h\} \rangle = G$. Vemos que $M \in \mathcal{M} = \emptyset$, lo que es absurdo.

Tiene que ser entonces $G \setminus \mathcal{N}$, como queríamos. \square

- [1] (c) Mostrar que $\Phi(G)$ es normal.

Solución. El conjunto de no-generadores de G es claramente normal. \square

- [2] **3.28.** Sea G un grupo y H un subgrupo propio de G . Entonces $\langle G \setminus H \rangle = G$.

Solución. Supongamos que $H' = \langle G \setminus H \rangle \subsetneq G$. Como $H \cup H' = G$, debe ser $H' \subset H$ ó $H \subset H'$. En el primer caso, es $G \setminus H \subset H' \subset H$, así que $G \setminus H = \emptyset$, lo que es imposible; en el segundo, $G = H \cup (G \setminus H) \subset H'$, lo que también es imposible. Vemos así que nuestra suposición contradice las hipótesis. \square

- [2-] **3.29.** Sea $G \subset \mathbb{C}^\times$ un subgrupo finito del grupo multiplicativo \mathbb{C}^\times . Entonces existe $n \in \mathbb{N}$ tal que $G = \mathbb{G}_n$ es el grupo de las raíces n -ésimas de la unidad.

Solución. Sea $G \subset \mathbb{C}^\times$ un subgrupo finito de orden n . Entonces si $z \in G$, es $z^n = 1$ y vemos que cada elemento de G es raíz de $p(X) = X^n - 1$. Como el conjunto de raíces de p es precisamente \mathbb{G}_n , vemos que G es un subgrupo de \mathbb{G}_n . Como $|G| = n = |\mathbb{G}_n|$, debe ser, de hecho, $G = \mathbb{G}_n$. \square

4. Homomorfismos

- [1] **4.1.** Sea G un grupo y X un conjunto. Sea $x_0 \in X$ y sea

$$\text{ev}_{x_0} : f \in G^X \mapsto f(x_0) \in G.$$

Mostrar que se trata de un homomorfismo de grupos. Determinar su núcleo e imagen.

- [1+] **4.2.** Mostrar que cualquiera sea el grupo G , existe un isomorfismo $G \cong G^{\text{op}}$ entre G y su grupo opuesto.

- [1] **4.3.** Sean G y H grupos, y sea $\text{hom}_{\text{Grp}}(G, H)$ el conjunto de todos los homomorfismos $f : G \rightarrow H$. ¿Se trata en general de un subgrupo de H^G ? Encuentre condiciones sobre H que garanticen que lo sea.

- [1] **4.4.** Muestre que el grupo \mathbb{H} del ejercicio 2.2 y el grupo \mathbb{H}_1 del ejercicio 3.6 son isomorfos.

4.5. Sea G un grupo.

- [1] (a) Sea $g \in G$ e $\text{inn}_g : h \in G \mapsto ghg^{-1} \in G$. Mostrar que $\text{inn}_g \in \text{Aut}(G)$.
 [1] (b) Mostrar que la aplicación $\text{inn} : g \in G \mapsto \text{inn}_g \in \text{Aut}(G)$ es un homomorfismo de grupos.
 [1] (c) Describir el núcleo de inn . Los automorfismos que están en la imagen de G se llaman *automorfismos interiores* y la imagen misma se denota $\text{Inn}(G)$.
 [1] (d) Mostrar que $\text{Inn}(G)$ es un subgrupo normal de $\text{Aut}(G)$.

- [2] **4.6.** Sea G un grupo finito. Supongamos que existe $f \in \text{Aut}(G)$ tal que $f^2 = 1$ y f no deja fijo ningún elemento de G aparte de 1. Entonces cada $g \in G$ es $f(g) = g^{-1}$ y G es abeliano de orden impar.

Sugerencia. Muestre la aplicación $\phi : g \in G \mapsto g^{-1}f(g) \in G$ es biyectiva y muestre que $f(g) = g^{-1}$ escribiendo a g en la forma $h^{-1}f(h)$ para algún elemento h de G .

Solución. Si $\phi(g) = \phi(h)$, es $g^{-1}f(g) = h^{-1}f(h)$ y vemos que $hg^{-1} = f(h)f(g^{-1}) = f(hg^{-1})$. Luego hg^{-1} queda fijo por f y debe ser $h = g$. Hemos mostrado, así, que ϕ es inyectiva. Como G es finito, esto implica que es también sobreyectiva.

Sea ahora $g \in G$. Como ϕ es sobreyectiva, existe $h \in G$ tal que $g = h^{-1}f(h)$. Entonces

$$f(g) = f(h^{-1}f(h)) = f(h^{-1})h = (h^{-1}f(h))^{-1} = g^{-1}.$$

Luego f coincide con la inversión de G . Es fácil ver, ahora, que como f es un homomorfismo, G debe ser abeliano.

Finalmente, como $f^2 = 1$ y f deja exactamente un punto fijo, es claro que $|G|$ debe ser impar. \square

4.7. Sea G un grupo. Un subgrupo H de G se dice *característico* si cualquiera sea $f \in \text{Aut}(G)$, $f(H) \subset H$.

- [1] (a) Muestre que si $H \subset G$ es un subgrupo característico, entonces para cada $f \in \text{Aut}(G)$ es $f(H) = H$.
- [1] (b) Muestre que $Z(G)$ y $[G, G]$ son característicos.
- [1] (c) $\Phi(G)$ es un subgrupo característico de G .
- [1] (d) Si H es un subgrupo característico de G , entonces H es normal en G .
- [1] (e) Si un grupo G posee un único subgrupo H de un orden dado, éste es característico.
- [1] (f) Si H es un subgrupo característico en G y K es un subgrupo característico en H , entonces H es un subgrupo característico de G . Comparar con 3.21.
- [1] (g) Si $N \subset G$ es un subconjunto característico (es decir, si para cada $f \in \text{Aut}(G)$, $f(N) \subset N$), entonces $\langle N \rangle$ y $C(N)$ son subgrupos característicos de G .

Un subgrupo H de G se dice *totalmente característico* si $f(H) \subset H$ siempre que $f \in \text{End}(G)$.

- [1] (h) Un subgrupo totalmente característico es característico.

Solución. Sea G un grupo y H un subgrupo de G totalmente característico. Sea $\phi \in \text{Aut}(G)$ y supongamos que $\phi(H) \subsetneq H$. Entonces aplicando ϕ^{-1} a esta inclusión vemos que $H \subsetneq \phi^{-1}(H)$. Pero esto contradice la hipótesis de ser H totalmente característico. \square

- [2] (i) Dar ejemplos de un subgrupo totalmente característico y de un subgrupo característico pero no totalmente característico.

Solución. Si G es un grupo y $n \in \mathbb{Z}$, los subgrupos $\langle g^n : g \in G \rangle$ y $\langle g : |g| < \infty \rangle$ son totalmente característicos.

El centro de un grupo, en general, no es totalmente característico. Veamos un ejemplo de esto. Sea $G = \text{GL}_2(\mathbb{Q})$. Si $g \in G$, entonces existen enteros impares s y t y un entero $v(g)$ tales que $\det g = 2^{v(g)}s/t$. Es claro que s , t y $v(g)$ están claramente unívocamente determinados por g . Usando esto, es fácil ver que $v : G \rightarrow \mathbb{Z}$ es un homomorfismo de grupos.

Consideremos la aplicación $f : G \rightarrow G$ tal que si $g \in G$ es

$$f(g) = \begin{pmatrix} 1 & v(g) \\ 0 & 1 \end{pmatrix}.$$

Se trata de un homomorfismo de grupos.

Ahora bien, podemos ver que $f(Z(G)) \not\subset Z(G)$. Por ejemplo, el elemento $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ es central en G pero $f(g) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ no está en $Z(G)$. \square

- [1+] (j) Todos los subgrupos de un grupo cíclico son totalmente invariantes. ¿Vale la recíproca?

- [1+] [†]4.8. (a) Sea G un grupo y sean H y K subgrupos de G de índice finito. Entonces $L = H \cap K$ también tiene índice finito.

Sugerencia. Para verlo muestre que es posible definir una aplicación $\phi : G/L \rightarrow G/H \times G/K$ de manera que $\phi(xL) = (xH, xK)$ y muestre que ésta es inyectiva.

Solución. Hay que mostrar primero que ϕ está bien definida. Supongamos que $x, y \in G$ son tales que $xL = yL$. Entonces $x^{-1}y \in L = H \cap K$, así que $xH = xx^{-1}yH = yH$; de forma similar vemos que $xK = yK$.

Para terminar, basta mostrar que ϕ es inyectiva. Supongamos que $x, y \in G$ son tales que $\phi(xL) = \phi(yL)$, es decir, es $xH = yH$ y $xK = yK$. Entonces $x^{-1}y \in H$ y a la vez $x^{-1}y \in K$. Luego $x^{-1}y \in L$ y, por supuesto, esto implica que $xL = yL$. \square

- [1+] (b) El conjunto de elementos de un grupo que poseen un número finito de conjugados es un subgrupo característico.

Solución. Sea G un grupo. Si $g \in G$, entonces claramente $|cl\ g| = [G : C(g)]$. Luego el conjunto en cuestión es $H = \{g \in G : [G : C(g)] < \infty\}$.

Es claro que $C(g) = C(g^{-1})$ cualquiera sea $g \in G$, así que H es cerrado por la inversión de G . Por otro lado, si $g, h \in H$, entonces $C(gh) \supset C(g) \cap C(h)$. Como $g, h \in H$, $C(g) \cap C(h)$ tiene índice finito en G por el punto anterior y, claramente, esto implica que $C(gh)$ tiene índice finito. Esto muestra que H es en efecto un subgrupo de G .

Que H es característico sigue inmediatamente que para cada $f \in \text{Aut}(G)$, $[G : C(g)] = [G : C(f(g))]$. \square

4.9. Sea $f : G \rightarrow H$ un homomorfismo de grupos.

- [1] (a) Si H es abeliano, entonces $[G, G] \subset \ker f$.
 [1] (b) Mostrar que $f([G, G]) \subset [H, H]$. En particular, concluya que $[G, G]$ es un subgrupo característico de G .

4.10. Sea $f : G \rightarrow H$ un homomorfismo de grupos. ¿Es cierto en general que $f(Z(G)) \subset Z(H)$? En caso negativo, de condiciones suficientes que garanticen esta inclusión. Bajo esas condiciones, ¿es $f(Z(G)) = Z(H)$?

4.11. Sea G un grupo.

- [1] (a) Mostrar que la función $\text{ev}_1 : f \in \text{hom}_{\text{Grp}}(\mathbb{Z}, G) \mapsto f(1) \in G$ es una biyección.
 [1] (b) Describir $\text{hom}_{\text{Grp}}(\mathbb{Z}^2, G)$ y, para cada $n \in \mathbb{N}$, $\text{hom}_{\text{Grp}}(\mathbb{Z}_n, G)$.

- [1] **4.12.** (a) Determinar $\text{hom}_{\text{Grp}}(\mathbb{Q}, \mathbb{Z})$ y $\text{hom}_{\text{Grp}}(\mathbb{Q}, G)$ para un grupo finito G .
 [1] (b) Describir la imagen $D(G)$ de $\text{ev}_1 : f \in \text{hom}_{\text{Grp}}(\mathbb{Q}, G) \mapsto f(1) \in G$.
 [1] (c) Mostrar que cuando G es abeliano, $D(G)$ es un subgrupo característico de G .

4.13. Sea G un grupo.

- [1] (a) Encontrar una condición necesaria y suficiente sobre G para que la aplicación $(g, h) \in G \times G \mapsto gh \in G$ resulte un homomorfismo de grupos.
 [1] (b) Encontrar una condición necesaria y suficiente sobre G para que la aplicación $g \in G \mapsto g^{-1} \in G$ resulte un homomorfismo de grupos.
 [1] (c) Encontrar una condición necesaria y suficiente sobre G para que la aplicación $g \in G \mapsto g^2 \in G$ resulte un homomorfismo de grupos.

- [1+] **4.14.** Sean $m, n \in \mathbb{N}$. Si $(m, n) = 1$, entonces $\text{hom}_{\text{Grp}}(\mathbb{Z}_m, \mathbb{Z}_n)$ es trivial. ¿Qué sucede en general?

4.15. Sea G un grupo finito y $\phi : G \rightarrow G$ un endomorfismo de G .

- [1+] (a) Existe $n \in \mathbb{N}$ tal que si $m \geq n$, entonces $\phi^m(G) = \phi^n(G)$. Sea $\alpha = \phi^n$.

Solución. Tenemos una cadena decreciente de subgrupos de G :

$$G \supset \phi(G) \subset \phi^2(G) \supset \dots$$

Como G es finito, esta cadena tiene que estacionarse. \square

- [2] (b) Mostrar que $\text{im } \alpha$ es normal o dar un contraejemplo.

Solución. Hay un homomorfismo $\phi : S_3 \rightarrow S_3$ tal que $\phi((ij)) = (12)$ cualquiera sea la transposición $(ij) \in S_3$. Es fácil ver que $\phi^1(G) = \phi^k(G) = \langle (12) \rangle$ para todo $k \geq 1$. Luego $\alpha = \phi$ y claramente $\text{im } \alpha$ no es normal.

- [1+] **4.16.** Usando el hecho que $\text{GL}_2(\mathbb{F}_2)$ permuta los elementos no nulos de \mathbb{F}_2^2 , encuentre un isomorfismo $\text{GL}_2(\mathbb{F}_2) \cong S_3$.

Solución. Si $g \in \text{GL}_2(\mathbb{F}_2)$, podemos definir una aplicación $\phi(g) : v \in \mathbb{F}_2^2 \mapsto gv \in \mathbb{F}_2^2$ dada por el producto matricial. Como $\det g \neq 0$, $\phi(g)$ es una biyección tal que $\phi(g)(0) = 0$. Luego $\phi(g)$ preserva $\mathbb{F}_2^2 \setminus 0$ y la restricción a este conjunto es una biyección. Es claro que la aplicación $\phi' : g \in \text{GL}_2(\mathbb{F}_2) \mapsto \phi(g)|_{\mathbb{F}_2^2 \setminus 0} \in S(\mathbb{F}_2^2 \setminus 0)$ es un homomorfismo de grupos.

Casi por definición este homomorfismo es inyectivo. Contando, vemos que $\text{GL}_2(\mathbb{F}_2)$ tiene 6 elementos, así que ϕ' debe ser una isomorfismo. \square

- [1] **4.17.** (a) Sea G un grupo y sea $X \subset G$ un subconjunto tal que $\langle X \rangle = G$. Sea $f \in \text{End}(G)$ tal que $f(x) = x$ para todo elemento $x \in X$. Entonces $f = \text{id}_G$.

Solución. Basta mostrar que $f(g) = g$ cualquiera sea $g \in G$. Sea entonces $g \in G$. Como X genera a G , existen $x_1, x_2, \dots, x_n \in X$ tal que $g = x_1 x_2 \dots x_n$. Entonces $f(g) = f(x_1) f(x_2) \dots f(x_n) = x_1 x_2 \dots x_n = g$. \square

- [1+] (b) Sea X el conjunto de los elementos de orden 2 de S_3 . Muestre que cada automorfismo de S_3 induce una permutación de X y deduzca que $\text{Aut}(S_3) \cong S_3$.

Solución. Definimos $\phi : S_3 \rightarrow S(X)$ de manera que si $g \in S_3$ y $x \in X$, $\phi(g)(x) = gxg^{-1}$. Es fácil ver que se trata de un homomorfismo de grupos. Como $\langle X \rangle = G$, usando la parte anterior concluimos que ϕ es inyectivo. Como $|X| = 3$, es $|S_3| = |S(X)| = 3!$ y ϕ debe ser un isomorfismo. \square

4.18. Sea $n \geq 2$. Consideramos el polinomio *discriminante*

$$\Delta(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in \mathbb{Z}[x_1, \dots, x_n]$$

Si $\pi \in S_n$ es una permutación de $\{1, \dots, n\}$, definimos

$$\varepsilon(\pi) = \frac{\Delta(x_{\pi(1)}, \dots, x_{\pi(n)})}{\Delta(x_1, \dots, x_n)}.$$

- [1] (a) Mostrar que cualquiera sea $\pi \in S_n$, es $\varepsilon(\pi) \in \{\pm 1\}$.
- [1] (b) Mostrar que $\varepsilon : S_n \rightarrow \{\pm 1\}$ es un homomorfismo de grupo si dotamos a $\{\pm 1\}$ del producto usual.

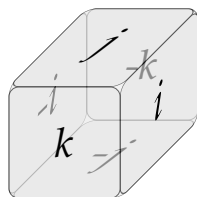
El subgrupo $A_n = \ker \varepsilon$ es el n -ésimo grupo alternante.

- [1] (c) Describir A_2 y A_3 .
- [1] (d) Sea $\tau = (ij) \in S_n$ una transposición. Determinar el valor de $\varepsilon(\tau)$.
- [2-] (e) Recordemos que todo elemento $\pi \in S_n$ puede ser escrito—de muchas maneras—como producto de transposiciones. Muestre que la paridad del número de transposiciones empleadas depende solamente de π .

Una permutación que puede escribirse de alguna forma como un producto de un número par de transposiciones se dice *par*.

4.19. Automorfismos de \mathbb{H} .

- [1] (a) Determine todos los automorfismos interiores de \mathbb{H} .
- [2] (b) De ejemplos de automorfismos de \mathbb{H} no interiores.
- [2] (c) Muestre que $\text{Aut}(\mathbb{H}) \cong S_4$.



†4.20. Automorfismos de S_n .

- (a) Sea $\phi \in \text{Aut}(S_n)$ y sea $g = (123)$. Mostrar que $\phi(g)$ es un producto de 3-ciclos disjuntos, que $\phi(\text{cl}(g)) \subset \text{cl}(\phi(g))$ y que, de hecho, la restricción $\phi : \text{cl}(g) \rightarrow \text{cl}(\phi(g))$ es una biyección.
- (b) Mostrar que

$$|\text{cl}(g)| = \frac{n!}{3(n-3)!}$$

y que si $\phi(g)$ es producto de r 3-ciclos disjuntos,

$$|\text{cl}(\phi(g))| = \frac{n!}{3^r r!(n-3r)!}$$

- (c) Mostrar que o bien $r = 1$ o bien $r = 2$ y $n = 6$.

Supongamos desde ahora que $n \neq 6$.

- (d) La imagen de todo 3-ciclo por ϕ es un 3-ciclo.
- (e) Sea $3 \leq i \leq n$ y supongamos que $\phi((123)) = (\alpha\beta\gamma)$ y $\phi((12i)) = (\alpha'\beta'\gamma')$. Muestre que $(\alpha\beta\gamma)(\alpha'\beta'\gamma')$ tiene orden dos y use esto para concluir que $|\{\alpha, \beta, \gamma, \alpha', \beta', \gamma'\}| = 4$.

- (f) Muestre que existen $\alpha, \beta, \gamma_3, \dots, \gamma_n$ distintos de manera que para cada $3 \leq i \leq n$ es $\phi((12i)) = (\alpha \beta \gamma_i)$.
- (g) Sea $\pi \in S_n$ tal que $\pi(1) = \alpha$, $\pi(2) = \beta$ y $\pi(i) = \gamma_i$ para cada $3 \leq i \leq n$. Muestre que $\phi(x) = \pi x \pi^{-1}$.
- (h) Muestre que $\text{inn} : S_n \rightarrow \text{Aut}(S_n)$ es un isomorfismo.
- (i) Determine $\text{Aut}(S_6)$.

5. Cocientes

5.1. Mostrar que

- (a) $\mathbb{C}^\times / \mathbb{R}^+ \cong S^1$;
- (b) $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$ cualquiera sea $m \in \mathbb{N}$;
- (c) $\text{GL}_n(k) / \text{SL}_n(k) \cong k^\times$ si k es un cuerpo y $n \in \mathbb{N}$;
- (d) $S^1 / \mathbb{G}_n \cong S^1$ si $n \in \mathbb{N}$;
- (e) si $m|n$, $\mathbb{G}_n / \mathbb{G}_m \cong \mathbb{G}_{n/m}$.

5.2. Si G es un grupo no abeliano, entonces $G/Z(G)$ no es cíclico.

Sugerencia. Use 3.14.

Solución. En caso contrario, existiría $g \in G$ tal que $G = \langle x, Z(G) \rangle$. Como claramente $\langle x, Z(G) \rangle = (x)Z(G)$, el ejercicio 3.14 tendríamos que G es abeliano. \square

5.3. Muestre que $G/Z(G) \cong \text{Inn}(G)$.

Solución. Es claro que la aplicación $\text{inn} : G \rightarrow \text{Aut}(G)$ considerada en 4.5 tiene a $Z(G)$ como núcleo y, por definición, $\text{Inn}(G) = \text{im inn}$. \square

5.4. Si G es un grupo y H y K son subgrupos normales de G , muestre que $G/(H \cap K)$ es isomorfo a un subgrupo de $G/H \times G/L$.

5.5. Dado un grupo G , el grupo $\text{Out}(G)$ de automorfismos exteriores de G es el cociente $\text{Aut}(G) / \text{Inn}(G)$; recordemos que en el ejercicio 4.5(d) vimos que $\text{Inn}(G)$ es normal en $\text{Aut}(G)$. Es importante observar que los elementos de $\text{Out}(G)$ no son automorfismos de G .

Determinar $\text{Out}(G)$ cuando $G \in \{S_3, S_4, \mathbb{H}\}$.

Solución. Sea $\mathcal{T} = \{(12), (13), (23)\}$ el conjunto de las 3 transposiciones de S_3 , que es precisamente el subconjunto de S_3 formado por los elementos de orden 2. Si $f \in \text{Aut}(G)$ y $t \in \mathcal{T}$, entonces $f(t)^2 = 1$ así que $f(t) \in \mathcal{T}$; vemos así que $f(\mathcal{T}) \subset \mathcal{T}$ y, como f es biyectiva, que f se restringe a \mathcal{T} y da un elemento $f|_{\mathcal{T}} \in S(\mathcal{T})$. Es claro que obtenemos de esta forma un homomorfismo $\phi : f \in \text{Aut}(S_3) \mapsto f|_{\mathcal{T}} \in S(\mathcal{T})$. Más aún, como \mathcal{T} genera a S_3 , ϕ es inyectivo y, en particular, $|\text{Aut}(S_3)| \leq 3!$.

Como $Z(S_3) = 1$, 5.3 nos dice que $|\text{Inn}(S_3)| = |S_3/Z(S_3)| = 3!$. Comparando cardinales, vemos que $\text{Inn}(S_3) = \text{Aut}(S_3)$ y, entonces, que $\text{Out}(S_3) = 1$.

5.6. Sea G un grupo y sea H un subgrupo no normal. Mostrar que el conjunto de coclases izquierdas de H en G no forma un grupo bajo la multiplicación usual.

Solución. Supongamos que G/H es un grupo. El único elemento idempotente de un grupo es el neutro, así que, como $HH = H$ porque H es un subgrupo de G , vemos que H es el elemento neutro de G/H . Entonces, cualquiera sea $g \in G$, debe ser $HgH = gH$, o, equivalentemente, $g^{-1}HgH = H$. Como por supuesto $H \supset \{1\}$, es $H = g^{-1}HgH \supset g^{-1}Hg\{1\} = g^{-1}Hg$. La arbitrariedad de g implica que H es normal. \square

6. Productos

6.1. Sean U y V dos grupos. Sean además $f : U \rightarrow W$ y $g : V \rightarrow W$ dos homomorfismos de grupos. Entonces la aplicación $h : (u, v) \in U \times V \mapsto f(u)g(v) \in K$ es un homomorfismo de grupos si todo elemento de $f(U)$ conmuta con todo elemento de $h(V)$.

6.2. Si G y H son grupos, determine $Z(G \times H)$.

6.3. *Producto directo interno.* Sea G un grupo.

(a) Sean N y M dos subgrupos normales de G y supongamos que $N \cap M = 1$ y $G = NM$. Mostrar que entonces es $G \cong N \times M$.

Solución. Mostremos primero que si $n \in N$ y $m \in M$, entonces $nm = mn$. Como M es normal, $nmn^{-1} \in M$ y entonces $nmn^{-1}m^{-1} \in M$; de forma similar, $mnm^{-1} \in N$ porque N es normal y entonces $mnm^{-1}m^{-1} \in N$. Así $nmn^{-1}m^{-1} \in N \cap M = 1$.

Consideremos ahora la aplicación $\phi : (n, m) \in N \times M \mapsto nm \in G$. Usando lo ya hecho es inmediato verificar que se trata de un homomorfismo de grupos. La hipótesis de que $G = NM$ implica que ϕ es sobreyectivo. Supongamos que $(n, m) \in \ker \phi$. Entonces $nm = 1$ en G y $N \ni n = m^{-1} \in M$, así que $n, m \in N \cap M = 1$. Luego $\ker \phi = 1$ y ϕ es inyectiva. \square

(b) Supongamos que G es grupo finito de orden mn con $(m, n) = 1$. Si G posee exactamente un subgrupo N de orden n y exactamente un subgrupo M de orden m , entonces G es isomorfo al producto directo de N y M .

Solución. Si $g \in G$, gNg^{-1} es un subgrupo de G de orden n , de manera que debe ser $gNg^{-1} = N$; vemos así que N es normal en G . De forma similar, M es un subgrupo normal de G . Si $g \in N \cap M$, entonces $|g|$ divide a n y a m , así que divide a $(n, m) = 1$ y debe ser $g = 1$; luego $N \cap M = 1$. Como en (a), usando esto podemos mostrar que todo elemento de N conmuta con todo elemento de M y, entonces, que $\phi : (n, m) \in N \times M \rightarrow nm \in G$ es un homomorfismo inyectivo de grupos. Como $|N \times M| = |G|$, ϕ es sobreyectivo y, finalmente, vemos que se trata de un isomorfismo.

†(c) Sean $k \in \mathbb{N}$ y $(N_i)_{i=1}^k$ una familia de subgrupos normales de G tales que

$G = \langle \bigcup_{i=1}^k N_i \rangle$ y para cada $j \in \{1, \dots, k\}$ se tiene que

$$N_j \cap \left\langle \bigcup_{\substack{1 \leq i \leq k \\ i \neq j}} N_i \right\rangle = 1.$$

Mostrar que entonces $G \cong N_1 \times \dots \times N_k$.

Solución. Razonando como en (a) vemos que si $1 \leq i < j \leq k$, $n_i \in N_i$ y $n_j \in N_j$,

$$[n_i, n_j] \in N_i \cap N_j \subset N_i \cap \left\langle \bigcup_{\substack{1 \leq l \leq k \\ l \neq i}} N_l \right\rangle = 1,$$

de manera que los elementos de N_i y de N_j conmutan. Luego la aplicación

$$\phi : (n_1, \dots, n_k) \in N_1 \times \dots \times N_k \mapsto n_1 \dots n_k \in G$$

es un homomorfismo de grupos, que es sobreyectivo porque $G = \langle \bigcup_{i=1}^k N_i \rangle$. Para ver que es inyectivo, sea $(n_1, \dots, n_k) \in \ker \phi$. Si $1 \leq i \leq k$,

$$n_i = n_{i-1}^{-1} n_{i-2}^{-1} \dots n_2^{-1} n_1^{-1} n_k^{-1} n_{k-1}^{-1} \dots n_{i+2}^{-1} n_{i+1}^{-1} \in N_i \cap \left\langle \bigcup_{\substack{1 \leq l \leq k \\ l \neq i}} N_l \right\rangle = 1.$$

Luego $(n_1, \dots, n_k) = 1$ y $\ker \phi$ es trivial.

†(d) Otra vez, supongamos que G es finito y sean N_1, \dots, N_k subgrupos normales de G de órdenes r_1, \dots, r_k tales que $(r_i, r_j) = 1$ si $1 \leq i, j \leq k$ y $|G| = r_1 \dots r_k$. Entonces $G \cong N_1 \times \dots \times N_k$.

Solución. Como en (b), se ve que si $1 \leq i < j \leq k$, todo elemento de N_i conmuta con todo elemento de N_j . De esto deducimos que la aplicación

$$\phi : (n_1, \dots, n_k) \in N_1 \times \dots \times N_k \mapsto n_1 \dots n_k \in G$$

es un homomorfismo de grupos. Teniendo en cuenta los órdenes de los grupos considerados, es claro que para probar el resultado deseado basta mostrar que ϕ es inyectivo. Sea $(n_1, \dots, n_k) \in \ker \phi$. Como $\phi(n_1, \dots, n_k) = n_1 \dots n_k = 1$, es

$$n_1 = n_k^{-1} \dots n_2^{-1} \in N_1 \cap \langle N_2 \cup \dots \cup N_k \rangle.$$

Pongamos $M = \langle N_2 \cup \dots \cup N_k \rangle$. La función $\psi : (g_2, \dots, g_k) \in N_2 \times \dots \times N_k \mapsto g_2 \dots g_k \in M$ es un homomorfismo de grupos y es claramente sobreyectivo. Como el orden del dominio de ψ es $r_2 \dots r_k$, concluimos que el orden de M divide a $r_2 \dots r_k$. Pero entonces el orden de n_1 divide a r_1 y a $r_2 \dots r_k$, esto es, $n_1 = 1$. De la misma forma se ve que todas las componentes de (n_1, \dots, n_k) son triviales, y esto nos dice que ϕ es inyectiva, como queríamos. \square

6.4. Producto semi-directo.

(a) Sean G y N grupos y sea $\theta : G \rightarrow \text{Aut}(N)$ un homomorfismo de grupos. Sea $K = N \rtimes G$ y consideremos el producto en K dado por

$$(n, g) \cdot (n', g') = (n\theta(g)(n'), gg'), \quad \forall (n, g), (n', g') \in K.$$

Mostrar que, con respecto a este producto, K es un grupo.

Llamamos al grupo K construido el *producto semi-directo (o cruzado) de N por G con respecto a θ* y lo notamos $N \rtimes_{\theta} G$.

- (b) Encontrar homomorfismos ‘naturales’ de grupo $\iota : N \rightarrow N \rtimes_{\theta} G$ y $\pi : N \rtimes_{\theta} G \rightarrow N$ tales que ι sea inyectivo, π sea sobreyectivo e $\text{im } \iota = \ker \pi$.
- (c) Mostrar que si $\theta = 1$ es el homomorfismo trivial, $N \rtimes_{\theta} G \cong N \times G$ es simplemente el producto directo.

6.5. Producto semi-directo interno. Sea K un grupo y sean G y N subgrupos de K con N normal en K . Las siguientes afirmaciones son equivalentes:

- (a) $K = NG$ y $N \cap G = \{1\}$;
- (b) $K = GN$ y $N \cap G = \{1\}$;
- (c) Todo elemento de K puede escribirse de forma única como un producto de un elemento de N por uno de G .
- (d) Todo elemento de K puede escribirse de forma única como un producto de un elemento de G por uno de N .
- (e) La composición de la inclusión $\text{incl} : G \hookrightarrow K$ con la proyección canónica $\text{can} : K \twoheadrightarrow K/N$ es un isomorfismo $\tau : G \cong K/N$.
- (f) Existe un homomorfismo $\sigma : K \rightarrow N$ que se restringe a la identidad de N y cuyo núcleo es N .

Además, cuando estas afirmaciones valen, existe un homomorfismo de grupos $\theta : G \rightarrow \text{Aut}(N)$ y un isomorfismo de grupos $\xi : N \rtimes_{\theta} G \rightarrow K$ tales que el siguiente diagrama conmuta:

$$\begin{array}{ccccc}
 N & \xrightarrow{\iota} & N \rtimes_{\theta} G & \xrightarrow{\pi} & G \\
 \downarrow & & \downarrow \xi & & \downarrow \tau \\
 N & \xrightarrow{\text{incl}} & K & \xrightarrow{\text{can}} & K/N
 \end{array}$$

Los homomorfismos ι y π del diagrama fueron construidos en el ejercicio 6.4.

6.6. Mostrar que $S_3 \cong \mathbb{Z}_3 \rtimes_{\theta} \mathbb{Z}_2$ para un homomorfismo $\theta : \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_3)$ apropiado.

6.7. Mostrar que S_n es el producto semi-directo de A_n y $\langle(12)\rangle$.

[†]**6.8.** Mostrar que \mathbb{H} no puede ser escrito como un producto semi-directo de forma no trivial.

[†]**6.9.** Sea G un grupo finito y $\phi : G \rightarrow G$ un endomorfismo de G y α el endomorfismo de G construido en el ejercicio 4.15. Mostrar que G es el producto semi-directo de $\ker \alpha$ e $\text{im } \alpha$.

7. Acciones

7.1. Si un grupo G actúa sobre un conjunto finito X , el *carácter* de X es la aplicación $\chi_X : G \rightarrow \mathbb{N}_0$ dada por

$$\chi_X(g) = |\{x \in X : gx = x\}|, \quad \forall g \in G.$$

Si no hay ambigüedad sobre X , escribimos simplemente χ .

(a) Si G actúa transitivamente sobre X , es muestre que

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = 1.$$

Sugerencia. Considere el conjunto $S = \{(g, x) \in G \times X : gx = x\}$ y cuente sus elementos de dos formas distintas.

Solución. Consideremos el conjunto $S = \{(g, x) \in G \times X : gx = x\}$. Contamos los elementos de S de dos formas distintas. Primero, agrupando elementos de acuerdo a su segunda coordenada, vemos que

$$|S| = \sum_{x \in X} |G_x|. \tag{1}$$

Ahora bien, como la acción es transitiva, si fijamos $x_0 \in X$, es $|G_x| = |G_{x_0}|$ para cualquier $x \in X$, y entonces

$$|S| = |X| |G_{x_0}| = |G|.$$

Por otro lado, agrupando los elementos de S de acuerdo a su primera coordenada, vemos que

$$|S| = \sum_{g \in G} \chi(g). \tag{2}$$

Comparando (1) y (2) obtenemos el resultado deseado. \square

(b) En general, si la acción no es necesariamente transitiva, es

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = |X/G|.$$

Aquí, X/G es el conjunto de órbitas de G en X .

Solución. Claramente $\chi_X = \sum_{\mathcal{O} \in X/G} \chi_{\mathcal{O}}$, así que

$$\frac{1}{|G|} \sum_{g \in G} \chi_X(g) = \sum_{\mathcal{O} \in X/G} \frac{1}{|G|} \sum_{g \in G} \chi_{\mathcal{O}}(g) = |X/G|$$

porque la acción de G sobre cada órbita es por supuesto transitiva. \square

[†](c) Si G actúa transitivamente sobre X y $x_0 \in X$, entonces, si G_{x_0} es el estabilizador de x_0 en G , es

$$\frac{1}{|G|} \sum_{g \in G} \chi(g)^2 = |X/G_{x_0}|.$$

Sugerencia. Una forma de hacer esto consiste en contar los elementos del conjunto $S = \{(g, x, y) \in G \times X \times X : gx = x, gy = y\}$ de dos formas distintas.

Solución. Por un lado, tenemos que

$$|S| = \sum_{g \in G} |\{(x, y) \in X \times X : gx = x, gy = y\}| = \sum_{g \in G} \chi(g)^2.$$

Por otro,

$$|S| = \sum_{x \in X} |\{(g, y) \in G \times X : gx = x, gy = y\}| = \sum_{x \in X} \sum_{g \in G_x} \chi(g);$$

como la acción es transitiva, esto es

$$= |X| \sum_{g \in G_{x_0}} \chi(g),$$

y, finalmente, usando la parte anterior de este ejercicio,

$$= |X||G||X/G_{x_0}|.$$

Comparando los dos resultados obtenidos, obtenemos la identidad deseada. \square

7.2. Grupos lineales finitos. Sea k un cuerpo finito de q elementos.

- (a) Sea $V = k^2$ el k -espacio vectorial de vectores columna y sea X el conjunto de vectores no nulos de V . Mostrar que la acción de $\text{GL}_2(k)$ sobre V por multiplicación a izquierda preserva a X y que la acción de $\text{GL}_2(k)$ sobre X es transitiva.
- (b) Sea $v_0 = (1, 0)^t \in X$. Determinar el estabilizador $\text{GL}_2(k)_{v_0}$ de v_0 en $\text{GL}_2(k)$.
- (c) Mostrar que $|\text{GL}_2(k)| = (q^2 - 1)(q^2 - q)$.
- \dagger (d) Más generalmente, mostrar que si $n \in \mathbb{N}$, es

$$|\text{GL}_n(k)| = \prod_{i=0}^{n-1} (q^n - q^i).$$

- \dagger (e) Sea $n \in \mathbb{N}$. Muestre que el morfismo $\det : \text{GL}_n(k) \rightarrow k^\times$ es sobreyectivo y concluya que

$$|\text{SL}_n(k)| = \frac{1}{q-1} \prod_{i=0}^{n-1} (q^n - q^i).$$

7.3. Subgrupos grandes.

- (a) Sea G un grupo finito y H un subgrupo de índice 2. Construya explícitamente un homomorfismo de grupos $f : G \rightarrow \mathbb{Z}_2$ tal que $\ker f = H$, mostrando en particular que H es normal.

El objetivo de lo que sigue es obtener una prueba de la siguiente proposición que generaliza a este resultado:

Proposición. Sea G un grupo finito, sea p el menor número primo que divide a $|G|$ y sea H un subgrupo de G de índice p . Entonces H es normal.

Notemos que, en las condiciones de este enunciado G no puede poseer subgrupos de índice menor que p .

- (b) Sea $X = G/H = \{gH : g \in G\}$ el conjunto de coclases a izquierda de H en G ; así, $|X| = p$. Consideramos sobre X la acción usual de G por multiplicación, dada por

$$(g, hH) \in G \times X \mapsto ghH \in X.$$

y sea $\theta : G \rightarrow S(X)$ el homomorfismo de grupos correspondiente. Mostrar que si $K = \ker \theta$, se tiene que $H \supset K$ y, como $\text{im } \theta$ es un subgrupo de $S(X)$, que $|G : K|$ divide a $p!$.

(c) Muestre que $|G : K| = |G : H|$, para concluir que $H = K$ y, así, que H es normal.

Sugerencia. Para hacerlo, observe primero que $p = |G : H| \leq |G : K|$, de manera que $|G : K| \neq 1$. Si q es un primo que divide a $|G : K|$, lo hecho en la parte anterior implica que $q \leq p$; esto junto con la elección de p implica que $|G : K| = p^r$ para algún $r \geq 1$. Muestre para terminar que debe ser $r = 1$.

8. Teoremas de Sylow

[1] **8.1.** Sea p un número primo. Un grupo abeliano finito de exponente p^r con $r > 0$ posee elementos de orden p .

Solución. Sea $\pi : g \in G \mapsto g^p \in G$. Como G es abeliano, π es un homomorfismo de grupos. Queremos mostrar que no es inyectivo. De serlo, sería biyectivo y tendría orden finito n en $\text{Aut}(G)$.

Pero entonces cualquiera sea $g \in G$, es $g = \text{id}_G^r(g) = \pi^{rn}(g) = g^{p^{rn}} = 1$. Esto no es posible porque G no es trivial. \square

[2] **8.2.** Sea p un número primo y G un grupo de orden $p^r > 1$. Entonces $Z(G)$ no es trivial.

Solución. Si $x \in G$ es tal que $|\text{cl } x| > 1$, entonces, como $|\text{cl } x| = [G : C(x)]$ es un divisor de $|G|$, vemos que $p \mid |\text{cl } x|$. Ahora, como

$$|G| = \sum_{\substack{c \in \text{Cl}(G) \\ |c| > 1}} |c| + |Z(G)|$$

y p divide al miembro izquierdo y al primer término del derecho, concluimos que $p \mid |Z(G)|$. \square

[2+] **8.3.** Sea G un grupo finito de orden $|G| = p^r m$ con p primo y $(p, m) = 1$. Entonces G posee subgrupos de orden p^r .

Solución. Hagamos inducción sobre $|G|$; por supuesto, si $|G| = 1$, no hay nada que probar.

Usando **8.2** vemos que $Z(G)$ es no trivial. Como se trata de un abeliano cuyo exponente divide a p^r , **8.1** nos dice que existe un subgrupo $A \subset Z(G)$ de orden p .

Como A es normal en $Z(G)$, que a su vez es característico en G , vemos que A es normal en G . Además, $p^{r-1}m = |G/A| < |G|$ así que nuestra hipótesis inductiva implica que existe un subgrupo $H' \subset G/A$ de orden p^{r-1} .

Sea $\pi : G \rightarrow G/A$ la proyección canónica y sea $H = \pi^{-1}(H')$. Entonces H es un subgrupo de G de orden p^r . \square

Definición. Sea p un número primo. Un elemento g de G es p -primario si su orden es una potencia de p . Un grupo G es un p -grupo si el orden de todo elemento de G es una potencia de p .

8.4. Sea p un número primo.

(a) Si G es un p -grupo y H es un subgrupo de G , entonces H es un p -grupo.

- (b) Si G es un p -grupo y $f : G \rightarrow H$ es un homomorfismo sobreyectivo, H es un p -grupo.
 (c) Si G es un grupo, H un subgrupo normal de G y tanto H como G/H son p -grupos, entonces G es un p -grupo.

[2] **8.5.** Un grupo finito G es un p -grupo sii $|G| = p^r$ para algún $r \geq 1$.

Solución. Si $|G|$ es divisible por un número primo q distinto de p , entonces, usando 8.3 vemos que G posee un q -subgrupo H no trivial, que entonces por 8.2 posee un centro $Z(H)$ no trivial, que a su vez, en vista de 8.1, posee elementos de orden q . Esto es imposible si G es un p -grupo. Esto prueba la necesidad de la condición.

Para ver la suficiencia, supongamos que G tiene orden p^r para algún $r \in \mathbb{N}$ y sea $g \in G$. Como $|g| \mid |G|$, es claro que $|g|$ es una potencia de p . Así, G es un p -grupo, como queríamos.

Definición. Sea p un número primo y G un grupo. Un p -subgrupo de Sylow de G es un p -subgrupo maximal de G . Escribimos $\text{Syl}_p(G)$ al conjunto de los p -subgrupos de Sylow de G .

8.6. Sea G un grupo finito y p un número primo.

[1+] (a) Si $|G| = p^r m$ con $(p, m) = 1$ y $H \subset G$ es un subgrupo tal que $|H| = p^r$, entonces $H \in \text{Syl}_p(G)$.

Solución. Sea $H \subset G$ un subgrupo de orden p^r y supongamos que no es un p -subgrupo maximal. Entonces existe otro p -subgrupo $H' \subset G$ tal que $H \subsetneq H'$. Entonces $|H'| = p^{r'}$ con $r' > r$. Pero debe ser $p^{r'} = |H'| \mid |G| = p^r m$, lo que es imposible. \square

[1] (b) Si $p \mid |G|$, entonces $\text{Syl}_p(G) \neq \emptyset$.

Solución. Sea p^r la mayor potencia de p que divide a $|G|$. Entonces (8.3) nos dice que existen subgrupos de G de orden p^r y el punto anterior nos dice que estos son maximales. \square

[1+] **8.7.** Si G es un grupo y $H \in \text{Syl}_p(G)$ y $x \in G \setminus H$ tiene orden $|x| = p^n$, entonces $x \notin N(H)$.

Sugerencia. Suponga lo contrario y considere el orden del elemento xH en $\langle H \cup \{x\} \rangle / H$.

Solución. Supongamos que $x \in N(H)$, de manera que H es normal en $H' = \langle N \cup \{x\} \rangle$. Como $H' \supsetneq H$, H' no es un p -subgrupo de G y entonces H'/H no es un p -grupo. Como H'/H esta generado por xH , es cíclico, así que $|xH|$ no es una potencia de p . Esto contradice la hipótesis de que $|x| = p^n$. \square

8.8. Sea G un grupo finito y $K \in \text{Syl}_p(G)$. Sea \mathcal{C} el conjunto de subgrupos de G conjugados de K .

[1] (a) Sea $H \in \text{Syl}_p(G)$ y sea \sim la relación en \mathcal{C} tal que

$$L \sim L' \text{ sii existe } h \in H \text{ tal que } hLh^{-1} = L.$$

Muestre que se trata de una relación de equivalencia.

- [1+] (b) Sea $L \in \mathcal{C}$ y notemos $[L]$ a la clase de equivalencia de L . Entonces $|[L]| = [H : H \cap N(L)]$. Además, si $L \neq H$ es $|[L]| > 1$ y es divisible por p . Si, por el contrario, $L = H$, entonces $|[H]| = 1$.

Solución. La acción de H sobre $[L]$ por conjugación es transitiva y el estabilizador de L en H es precisamente $H \cap N(L)$, así que $|[L]| = [H : H \cap N(L)]$.

Supongamos que $H \neq L$. Si $[H : H \cap N(L)] = 1$, entonces $H = H \cap N(L)$ y vemos que $L \subset N(L) \subset H$. Como $|L| = |H|$, esto es imposible. Luego $[H : H \cap N(L)] > 1$. Como H es un p -grupo, este índice debe ser divisible por p .

Es inmediato que $[H] = \{H\}$, así que la última afirmación es clara. \square

- (c) Muestre que

$$|\mathcal{C}| \equiv \begin{cases} 0 & (\text{mód } p), \text{ si } H \notin \mathcal{C}; \\ 1 & (\text{mód } p), \text{ si } H \in \mathcal{C}. \end{cases}$$

Solución. Supongamos que $H \notin \mathcal{C}$, entonces todas las clases de equivalencia de \mathcal{C} tienen cardinal divisible por p , así que $|\mathcal{C}| \equiv 0 \pmod{p}$.

Si en cambio $H \in \mathcal{C}$, entonces todas las clases de equivalencia de \mathcal{C} , salvo $[H]$, tienen cardinal divisible por p , así que $|\mathcal{C}| \equiv 1 \pmod{p}$.

- (d) Concluya que H es conjugado de K y que $|\mathcal{C}| \equiv 1 \pmod{p}$.

8.9. Pruebe el siguiente teorema de Peter Ludwig Mejdell Sylow (1832–1918, Noruega) que es, probablemente, el teorema más importante de la teoría de grupos finitos.

Teorema. (M. L. Sylow, *Théorèmes sur les groupes de substitutions*, Math. Ann. 5 (1872), no. 4, 584–594.) Sea p un número primo. Sea G un grupo finito de orden $p^r m$ con $(p, m) = 1$. Entonces

- Un subgrupo H de G es un p -subgrupo de Sylow sii $|H| = p^r$.
- Todos los p -subgrupos de Sylow de G son conjugados.
- Sea n_p el número de p -subgrupos de Sylow de G . Entonces $n_p \equiv 1 \pmod{p}$.
- $n_p \mid m$.

8.10. Muestre que no hay grupos simples de orden 28 ó 312.

Solución. Sea G de orden $28 = 2^2 \cdot 7$. Entonces $n_7 \mid 2^2$, así que $n_7 \in \{1, 2, 4\}$. Pero también $n_7 \equiv 1 \pmod{7}$, así que necesariamente $n_7 = 1$ y concluimos que un 7-subgrupo de Sylow es normal.

Sea ahora G de orden $312 = 2^3 \cdot 3 \cdot 7$. El único divisor positivo de $2^3 \cdot 3$ congruente con 1 módulo 7 es 1, así que $n_7 = 1$. Luego G no es simple. \square

8.11. Muestre que un grupo de orden 12 ó 56 no es simple.

Solución. Sea G un grupo de orden $12 = 2^2 \cdot 3$. Entonces $n_3 \mid 4$ y $n_3 \equiv 1 \pmod{3}$, así que si hay 3-subgrupos de Sylow no normales en G , debe ser $n_3 = 4$. Entonces hay en G exactamente $8 = 4 \cdot (3 - 1)$ elementos de orden 3. Eso deja a lo sumo 3 elementos en G que pueden ser 2-primarios. Como hay al menos un 2-subgrupo de Sylow de orden 4, vemos que tiene que haber exactamente uno, que resulta entonces normal. Así, G no es simple.

Sea ahora G un grupo de orden $56 = 2^3 \cdot 7$. Entonces $n_7 \mid 8$ y $n_7 \equiv 1 \pmod{7}$. Esto implica que $n_7 \in \{1, 8\}$. Si $n_7 = 1$, G no es simple. Supongamos entonces que $n_7 = 8$. Como cada 7-grupo de Sylow es cíclico, vemos que hay en G exactamente $48 = 8 \cdot (7 - 1)$ elementos de orden 7. Por otro lado, hay al menos un 2-subgrupo de Sylow, que tiene orden 8, así que hay al menos 7 elementos 2-primarios no triviales en G . Como $1 + 7 + 48 = |G|$, concluimos que hay en G exactamente 7 elementos no triviales 2-primarios y que entonces $n_2 = 1$. \square

8.12. Si p y q son primos distintos, un grupo de orden pq no es simple.

Solución. Si G tiene orden pq y es simple, el teorema de Sylow implica que $n_p = q$ y $n_q = p$. Contando los elementos de G agrupados de acuerdo a su orden, vemos que $pq = 1 + (p - 1)q + (q - 1)p$, es decir, que $(p - 1)(q - 1) = 0$. Esto es imposible. \square

8.13. Sea G un grupo de orden $p^r m$ con p primo, $r \geq 1$ y $p > m$. Entonces G no es simple.

Solución. n_p divide a m , así que $n_p < p$. Como $n_p \equiv 1 \pmod{p}$, debe ser $n_p = 1$. \square

8.14. Sea G un grupo de orden $p^2 q$ con p y q primos distintos. Entonces G no es simple.

Solución. Supongamos que G es simple. Si $q < p$, entonces como $n_p \mid q$ y $n_p \equiv 1 \pmod{p}$, debe ser $n_p = 1$, lo que es imposible. Luego debe ser $q > p$. Como sabemos que $n_q \equiv 1 \pmod{q}$, $n_q \mid p^2$ y $n_q > 1$, debe ser $n_q = p^2$. Como cada q -subgrupo de Sylow es cíclico, esto implica que hay exactamente $(q - 1)p^2 = p^2 q - p^2$ elementos de orden q en G . Luego hay a lo sumo p^2 elementos p -primarios, que deben formar el único p -subgrupo de Sylow. Así $n_p = 1$. (Alternativamente, vimos que en el segundo caso debe ser $p^2 \equiv 1 \pmod{q}$; usando que $X^2 - 1$ tiene a lo sumo dos raíces en \mathbb{Z}_q , vemos que $p = 1$ ó $p = q - 1$ y claramente ambas opciones son imposibles.) \square

8.15. Muestre que un grupo de orden menor que 60 no es simple.

8.16. Mostrar que si G es un grupo y P es un subgrupo de Sylow de G , entonces P es un subgrupo característico de $N(P)$.

8.17. Si todos los subgrupos de Sylow de un grupo finito G son normales, entonces $G \cong \prod_p \text{primo } P_p$. En particular, un grupo abeliano finito es producto de sus subgrupos de Sylow.

9. Varia

9.1. Grupos múltiplemente transitivos

Sea G un grupo y supongamos que G actúa fielmente sobre un conjunto X . Sea $k \geq 1$.

9.1.1. Mostrar que obtenemos una acción de G sobre X^k si definimos

$$g \cdot (x_1, \dots, x_k) = (gx_1, \dots, gx_k), \quad \text{si } g \in G \text{ y } (x_1, \dots, x_k) \in X^k.$$

Mostrar que si $|X| > 1$, la acción de G sobre X^k no es transitiva.

Definición. Pongamos $X^{(k)} = \{(x_1, \dots, x_k) \in X^k : x_i \neq x_j \text{ si } 1 \leq i < j \leq k\}$. Diremos que la acción de G sobre X es k -transitiva si G actúa transitivamente sobre $X^{(k)}$.

9.1.2. Mostrar que la acción canónica de S_n sobre $\{1, \dots, n\}$ es n -transitiva.

9.1.3. Mostrar que la acción canónica de A_n sobre $\{1, \dots, n\}$ es $(n-2)$ -transitiva pero no $(n-1)$ -transitiva.

9.1.4. Sea K un cuerpo, V un K -espacio vectorial. Mostrar que $\text{Aut}_K(V)$ actúa 1-transitivamente sobre $V \setminus \{0\}$ pero no 2-transitivamente.

9.1.5. Sea otra vez K un cuerpo, V un K -espacio vectorial con $\dim_K V \geq 2$, y sea X el conjunto de todos los subespacios de V de dimensión 1. Mostrar que la acción de $\text{Aut}_K(V)$ sobre V induce una acción natural sobre X , que es 2-transitiva pero no 3-transitiva.

9.1.6. Mostrar que la acción sobre el conjunto de vértices de un tetraedro regular del grupo de rotaciones del sólido es 2- pero no 3-transitiva.

9.1.7. Sea A un grupo finito no trivial y $A' = A \setminus \{1\}$. Claramente $\text{Aut}(A)$ actúa sobre A' .

- (a) Si $\text{Aut}(A)$ actúa 1-transitivamente en A' , entonces existe un número primo p tal que todo elemento de A' es de orden p . Esto implica que A es un p -grupo, así que su centro no es trivial. Concluir que A es abeliano y entonces, usando el ejercicio 2.7, que $G \cong \mathbb{Z}_p \times \dots \times \mathbb{Z}_p$.
- (b) Determinar todos los grupos A tales que $\text{Aut}(A)$ actúa 2-transitivamente sobre A' .

Definición. Diremos que la acción de G sobre X es finamente k -transitiva si es k -transitiva y además, para cada $\forall (x_1, \dots, x_k) \in X^{(k)}$ y cada $g_1, g_2 \in G$, es

$$\forall i \in \{1, \dots, k\}, g_1(x_i) = g_2(x_i) \implies g_1 = g_2.$$

En otras palabras, esta condición dice que dos elementos de G que actúan de la misma forma sobre k elementos de X deben coincidir.

9.1.8. Si la acción de G es finamente k -transitiva sobre X y $n = |X|$, entonces

$$|G| = \frac{n!}{(n-k)!}.$$

9.1.9. La acción de S_n sobre $\{1, \dots, n\}$ es finamente n -transitiva, finamente $(n - 1)$ -transitiva pero no finamente $(n - 2)$ -transitiva.

9.1.10. La acción de A_n sobre $\{1, \dots, n\}$ es finamente $(n - 2)$ -transitiva.

9.1.11. *Acciones finamente 1-transitivas.* Este ejercicio describe todas las acciones finamente 1-transitivas.

(a) Sea G un grupo finito. Pongamos $R = G$ y consideremos la acción regular a izquierda $G \times R \rightarrow R$; recordemos que

$$g \cdot r = gr, \quad \forall g \in G, r \in R.$$

Mostrar que la acción de G sobre R es finamente 1-transitiva.

(b) Sea G un grupo finito que actúa sobre un conjunto X no vacío de forma finamente 1-transitiva. Mostrar que existe una función biyectiva $\phi : R \rightarrow X$ tal que el diagrama

$$\begin{array}{ccc} G \times R & \longrightarrow & R \\ \text{id}_G \times \phi \downarrow & & \downarrow \phi \\ G \times X & \longrightarrow & X \end{array}$$

conmuta, si las flechas verticales están dadas por las acciones de G .

9.1.12. Sea K un cuerpo finito de q elementos.

(a) Consideremos el conjunto $\text{AGL}(1, K) = K^\times \times K$ y dotémoslo de un producto dado por

$$(a, b) \cdot (a', b') = (aa', b + ab'), \quad \forall (a, b), (a', b') \in \text{AGL}(1, K).$$

Muestre que $(\text{AGL}(1, K), \cdot)$ es un grupo.

(b) Consideremos ahora el conjunto $X = K$ y la aplicación $\text{AGL}(1, K) \times K \rightarrow K$ dada por

$$(a, b) \cdot x = ax + b, \quad \forall (a, b) \in \text{AGL}(1, K), \forall x \in X.$$

Muestre que esto da una acción de $\text{AGL}(1, K)$ sobre X .

(c) Muestre que esta acción es finamente 2-transitiva.

9.1.13. Sea G un grupo finito y sea X un conjunto no vacío sobre el que G actúa de forma finamente 2-transitiva.

(a) Sea $x_0 \in X$ y $H = G_{x_0}$. Pongamos $X' = X \setminus \{x_0\}$. Entonces H actúa de forma finamente 1-transitiva sobre X' y es un subgrupo maximal de G .

Solución. Sea $t \in G \setminus H$. Queremos ver que $\langle t, H \rangle = G$. Sea $g \in G \setminus H$. Es $gx_0 \neq x_0$ y $tx_0 \neq x_0$, así que $gx_0, tx_0 \in X'$. Como H actúa de manera transitiva sobre X' , existe $h \in H$ tal que $hgx_0 = tx_0$. Vemos entonces que $t^{-1}hgx_0 = x_0$, es decir, que $t^{-1}hg \in H$. Pero esto implica que $g \in \langle t, H \rangle$. \square

(b) $H \cap gHg^{-1} \neq 1$ sii $g \in H$. En particular, $N(H) = H$ y $C(h) \subset H$ para cada $h \in H \setminus \{1\}$.

Solución. Supongamos que $g \notin H$ y sea $h \in H \cap gHg^{-1}$. Entonces existe $h' \in H$ tal que $h = gh'g^{-1}$ y vemos que $hgx = gh'g^{-1}gx_0 = gh'x_0 = gx_0$, porque $h' \in H$. Como además $hx_0 = x_0$, h tiene dos puntos fijos y debe ser $h = 1$. \square

- (c) G posee involuciones y son todas conjugadas. Notemos I al conjunto de las involuciones de G .

Solución. Es $|G| = n(n-1)$ por 9.1.8, que es par. Luego existen elementos de orden 2 en G . Veamos que son todos conjugados.

Sean $s, t \in G$ dos involuciones y sea $y \in X$. Como G es 2-transitivo, existe $u \in G$ tal que $uy = y$ y $usy = ty$. Pongamos $v = usu^{-1}$. Entonces $vy = usu^{-1}y = usy = ty$ y $vt = usu^{-1}t = us^2 = uy = y = tty$, así que v y t coinciden en dos elementos de X . Luego $t = v = usu^{-1}$ y vemos que s y t son conjugados. \square

- (d) Sea $N' = \{g \in G : \text{para cada } x \in X, gx \neq x\}$ y $N = N' \cup \{1\}$. Entonces es $|N'| = n-1$. Además, N es un subconjunto normal de G .

Solución. Como la acción es transitiva, para cada $x \in X$ hay exactamente $|H| - 1$ elementos que dejan fijo solamente a x . Luego hay exactamente $n(|H| - 1)$ elementos en G que dejan fijo algún elemento de X y vemos que hay $n|H| - 1 - n(|H| - 1) = n - 1$ elementos en G que mueven todos los elementos de X .

La segunda afirmación del enunciado es inmediata. \square

- (e) La acción de N sobre X es simplemente transitiva.

Solución. Consideremos la aplicación $\phi : n \in N \mapsto nx_0 \in X$. Se trata de una inyección: en efecto, si $\phi(n) = \phi(n')$, vemos que $n^{-1}n$ es un elemento de N que deja fijo a x_0 , así que debe ser $n^{-1}n = 1$, esto es, $n = n'$. Como $|N| = |X|$, se sigue que ϕ es biyectiva. Es fácil deducir de esto que la acción de N es simplemente transitiva. \square

- (f) H posee a lo sumo una involución. Si H posee una involución, $|I| = n$; en caso contrario, $|I| = n - 1$.

Solución. Supongamos que H posee r involuciones y $r \geq 1$. Como ninguna de ellas puede fijar un elemento de X' , vemos que cada una de ellas tiene a x_0 como único punto fijo. Ahora, como la acción de G es transitiva, para cada $y \in X$ hay exactamente r involuciones en G que dejan fijo a y y concluimos que hay rn involuciones en total en G .

Cada involución de G es producto de $\frac{1}{2}(n-1)$ transposiciones y hay rn de ellas. Como dos involuciones de G no pueden compartir una transposición y en $S(X)$ hay exactamente $\frac{1}{2}n(n-1)$ transposiciones, vemos que la única posibilidad es que r sea 1. Esto prueba además que en este caso hay n involuciones en G .

Supongamos ahora que H no contiene involuciones. Sea $s \in I$. Para cada $y \in X'$ elijamos $h_y \in H$ de manera que $h_y s x_0 = y$; esto es posible porque $s x_0, y \in X'$ y H actúa transitivamente sobre X' . Es $h_y s h_y^{-1} x_0 = h_y s x_0 = y$. Esto nos dice que $\{h_y s h_y^{-1} : y \in X'\}$ es un conjunto de exactamente $n-1$ involuciones distintas. Como en este caso es $I \subset N'$, vemos que hay a lo sumo $n-1$ involuciones y, en definitiva, que $|I| = n-1$. \square

(g) Si $s, t \in I$ y $s \neq t$, entonces st no tiene puntos fijos en X .

Solución. Sean $s, t \in I$ y supongamos que $y \in X$ es tal que $sty = y$. Claramente también es $tsy = y$. Si $sy = y$, entonces $s, t \in G_y$ y como G_y es conjugado de H , 9.1.13(f) implica que $s = t$. Si, por el contrario $z = sy \neq y$, entonces $sz = s^2y = y$ y $tz = tsy = y$, así que s y t coinciden en dos elementos de X (a saber, y y z) así que debe ser $s = t$. En cualquier caso, vemos que debe ser $s = t$. \square

(h) Sea $j \in G \setminus H$ una involución. Si $H \cap I \neq \emptyset$, sea además i la única involución de H . Entonces

$$I = \begin{cases} j^H, & \text{si } H \cap I = \emptyset; \\ j^H \cup \{i\}, & \text{si } H \cap I \neq \emptyset. \end{cases}$$

$$\text{Aquí } j^H = \{hjh^{-1} : h \in H\}.$$

Solución. Hay que mostrar que todas las involuciones de $G \setminus H$ son conjugadas por H . Para ello basta observar que si $s, t \in G \setminus H$ son involuciones, existe un único elemento $u \in G$ tal que $ux_0 = x_0$ y $usx_0 = tx_0$ (porque $sx_0 \neq x_0 \neq tx_0$), de manera que $u \in H$ y, como en 9.1.13(c) se puede ver que $t = usu^{-1}$. \square

(i) Es $I^2 \setminus \{1\} = N'$ y N es un subgrupo normal abeliano de G . De hecho, si $H \cap I = \emptyset$, se tiene que $I = N'$. Más precisamente, existe un número primo p tal que $N \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, y $p = 2$ sii $H \cap I = \emptyset$.

Solución. Supongamos primero que $H \cap I \neq \emptyset$. Entonces hay exactamente n involuciones en G , digamos $I = \{s_1, \dots, s_n\}$ y podemos suponer sin pérdida de generalidad que $s_n \in H$. Usando 9.1.13(g), vemos que $\{s_1s_n, \dots, s_{n-1}s_n\} \subset N'$; como los $n - 1$ elementos listados son distintos entre sí, 9.1.13(d) implica que $\{s_1s_n, \dots, s_{n-1}s_n\} = N'$. Razonando análogamente, podemos ver que $\{s_ns_1, \dots, s_ns_{n-1}\} = N'$, de manera que todo elemento de N' puede escribirse como s_1s_n y como s_ns_j para apropiados $i, j \in \{1, \dots, n - 1\}$.

En particular, todo elemento de N^2 es de la forma $s_1s_n \cdot s_ns_i = s_1s_j$ con $i, j \in \{1, \dots, n\}$ y, usando 9.1.13(g), vemos que si $N^2 \subset N$. Como G es finito, 3.1c nos dice que N es un subgrupo de G , que es normal porque N' es un subconjunto normal de G .

Como N es normal, la conjugación induce un morfismo de grupos $\alpha : H \rightarrow \text{Aut}(N)$ y, si $h \in H$ y $s_1s_n \in N$, es $\alpha(h)(s_1s_n) = hs_1h^{-1}s_n$ porque $hs_nh^{-1} = s_n$. El resultado de 9.1.13(h) implica entonces que la acción de $\text{Aut}(N)$ sobre N' es transitiva y 9.1.7(a) implica que existe un primo p tal que $N \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.

Si $p = 2$, hay involuciones en N' y existen $i, j \in \{1, \dots, n - 1\}$ tales que $s_1s_n = s_j$. Esto implica que $s_n = s_1s_n \cdot s_ns_j \in N'$. Pero esto es imposible porque s_n deja fijo a x . Luego p es impar.

Supongamos ahora que $H \cap I = \emptyset$. En este caso $I = \{s_1, \dots, s_{n-1}\}$ tiene exactamente $n - 1$ elementos y cada uno de ellos está en N' . Comparando cardinales, vemos inmediatamente que $N' = I$. En vista de 9.1.13(g), es $N^2 = I^2 \subset N'$, así que $N^2 \subset N$ y otra vez vemos que N es un subgrupo normal de G .

La acción por conjugación de G sobre $N' = I$ es transitiva en vista de 9.1.13(c) así que 9.1.7(a) implica que existe un primo p tal que $N \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$. Finalmente, como hay elementos de orden 2 en N , claramente debe ser $p = 2$. \square

(j) Si T es un subgrupo normal de G con $Z(T) \neq 1$, entonces $G = Z(T) \rtimes H$.

Solución. Como T es normal en G y $Z(T)$ es característico en T , $Z(T)$ es normal en G . Entonces $Z(T)H$ es un subgrupo de G .

Supongamos que $z \in Z(T) \cap H \setminus \{1\}$. Entonces en vista de 9.1.13(b), $T \subset C(z) \subset H$. Pero, en ese caso, es $g \in G \setminus H$, $T = T \cap gTg^{-1} \subset H \cap gHg^{-1} = 1$, lo que contradice la hipótesis. Luego $Z(T) \cap H = 1$; en particular, $Z(T)H$ es estrictamente más grande que H y como H es maximal en G , concluimos que el subgrupo $Z(T)H$ coincide con G .

Considerando la acción de H sobre $Z(T)$ inducida por la conjugación en G , es fácil mostrar ahora que la aplicación $\phi : (z, h) \in Z(T) \times H \rightarrow zh \in G$ es un isomorfismo. \square

(k) $G \cong N \rtimes H$ con respecto a la acción por conjugación de H sobre N .

Solución. El resultado sigue inmediatamente de 9.1.13(i) y 9.1.13(j). \square

(l) Fijemos $x_1 \in X'$. Definimos una aplicación $\zeta : N' \rightarrow H$ de la siguiente manera: si $n \in N'$, entonces $nx_0 \in X'$ porque n no deja fijo ningún elemento de X , así que como la acción de H sobre X' es simplemente transitiva, existe exactamente un elemento $\zeta(n) \in H$ tal que $\zeta(n)x_1 = nx_0$. Mostrar que ζ es una biyección.

Solución. Si $n, n' \in N'$ son tales que $\zeta(n) = \zeta(n')$, entonces es $nx_0 = \zeta(n)x_1 = \zeta(n')x_1 = n'x_0$ y vemos que $n^{-1}n'$ tiene un punto fijo. Como se trata de un elemento de N debe ser el elemento neutro, y concluimos que $n = n'$. Esto es, ζ es inyectiva.

Sea ahora $h \in H$. Como N actúa transitivamente en X , existe $n \in N$ tal que $hx_1 = nx_0$. No puede ser que $n = 1$ porque en ese caso sería $hx_1 = x_0$, contradiciendo el hecho de que $hX' = X'$. Luego $n \in N'$ y claramente es $h = \zeta(n)$. \square

(m) Fijemos $x_1 \in X'$. Definimos en X dos operaciones \cdot y $+$ en X de la siguiente manera.

Sean $x, y \in X$. Si $x = x_0$, ponemos $x \cdot y = x_0$. Si $x \neq x_0$, existe exactamente un elemento $h \in H$ tal que $hx_1 = x$, y ponemos $x \cdot y = hy$. Por otro lado, sabemos que existe exactamente un elemento $n \in N$ tal que $nx_0 = x$; ponemos $x + y = ny$.

Mostrar que $(X, +)$ es un grupo abeliano isomorfo a N y que (X', \cdot) es un grupo isomorfo a H .

(n) Mostrar que si H es abeliano, entonces $(X, +, \cdot)$ es un cuerpo K y que $G \cong \text{AGL}(1, K)$.

9.2. Grupos nilpotentes

Sea G un grupo. Definimos una sucesión creciente

$$1 = Z_0 \subset Z_1 \subset \cdots \subset Z_n \subset \cdots$$

de subgrupos normales de G inductivamente de la siguiente manera, empezando por $Z_0 = 1$: sea $i \in \mathbb{N}_0$ y supongamos que ha hemos contruido Z_i . Como Z_i es normal, podemos considerar el homomorfismo canónico $\pi : G \rightarrow G/Z_i$. Ponemos entonces $Z_{i+1} = \pi^{-1}(Z(G/Z_i))$; se trata claramente de un subgrupo

normal de G , y es $Z_{i+1}/Z_i \cong Z(G/Z_i)$. La sucesión de subgrupos $(Z_i)_{i \geq 0}$ se llama la *cadena central superior* de G .

Definición. Si existe $n \in \mathbb{N}_0$ tal que $Z_n = G$, decimos que G es nilpotente. El menor tal n es la longitud nilpotente de G .

9.2.1. Un grupo abeliano es nilpotente. ¿Es nilpotente S_3 ? Dé un ejemplo de un grupo nilpotente y no abeliano.

Definición. Una sucesión creciente $(N_i)_{i \geq 0}$ de subgrupos normales de un grupo G tal que $N_0 = 1$ y $N_{i+1}/N_i \subset Z(G/N_i)$ para cada $i \geq 0$ es una *cadena central ascendente*. Si existe $n \in \mathbb{N}_0$ tal que $N_n = G$ entonces decimos que la *cadena termina* o que *llega a G* .

9.2.2. Si G es un grupo y $(N_i)_{i \geq 0}$ es una cadena central ascendente en G , muestre que para cada $i \geq 0$ se tiene que $[N_{i+1}, G] \subset N_i$.

Solución. Como $N_{i+1}/N_i \subset Z(G/N_i)$, si $n \in N_{i+1}$ y $g \in G$, las clases nN_i y gN_i conmutan en G/N_i , es decir, $ng \equiv gn \pmod{N_i}$ o, lo que es lo mismo, $[n, g] \in N_i$. El resultado buscado sigue inmediatamente de esto. \square

9.2.3. Si G es un grupo y $(Z_i)_{i \geq 0}$ es su cadena central superior, entonces para cada $i \geq 0$ se tiene que $Z_{i+1} = \{g \in G : [g, G] \subset Z_i\}$.

Solución. Esto es inmediato a partir de la ecuación $Z_{i+1}/Z_i = Z(G/Z_i)$. \square

9.2.4. Mostrar que si un grupo G posee una cadena central ascendente $(N_i)_{i \geq 0}$ que llega a G , entonces es nilpotente. Una forma de hacer esto es ver que $N_i \subset Z_i$ para cada $i \geq 0$.

Solución. Es claro que $N_0 \subset Z_0$. Supongamos inductivamente que $i \geq 0$ y que sabemos que $N_i \subset Z_i$. Entonces la aplicación identidad $\text{id} : G \rightarrow G$ induce un homomorfismo sobreyectivo $\pi : G/N_i \rightarrow G/Z_i$ y, entonces,

$$\pi(N_{i+1}/N_i) \subset \pi(Z(G/N_i)) \subset Z(G/Z_i) = Z_{i+1}/Z_i. \quad (3)$$

Ahora bien, $\pi(N_{i+1}/N_i) = N_{i+1}Z_i/N_iZ_i$ y, como $N_i \subset Z_i$, esto es igual a $N_{i+1}Z_i/Z_i$. Luego la inclusión (3) nos dice que $N_{i+1}Z_i/Z_i \subset Z_{i+1}/Z_i$, es decir, que $N_{i+1}Z_i \subset Z_{i+1}$. De esta inclusión se ve claramente que $N_{i+1} \subset Z_{i+1}$. \square

9.2.5. Sea G un grupo tal que $G/Z(G)$ es nilpotente. Entonces G es nilpotente.

Solución. Sea $(Z'_i)_{i \geq 0}$ la cadena central superior de $G' = G/Z(G)$ y sea, para cada $i \geq 1$, $N_i \subset G$ el único subgrupo de G tal que $N_i/Z(G) = Z'_{i-1}$. Pongamos finalmente $N_0 = 1$. Afirmamos que $(N_i)_{i \geq 0}$ es una cadena central ascendente que termina en G . En efecto, si $i \geq 1$, usando libremente los isomorfismos canónicos, tenemos que

$$Z(G/N_i) = Z\left(\frac{G/Z(G)}{N_i/Z(G)}\right) = Z(G'/Z'_{i-1}) = Z'_i/Z'_{i-1} = \frac{N_{i+1}/Z(G)}{N_i/Z(G)} = N_{i+1}/N_i.$$

Por otro lado, $Z(G/N_0) = N_1/N_0$ porque la construcción hecha implica que $N_1 = Z(G)$. \square

9.2.6. Un p -grupo finito es nilpotente.

Solución. Sea G un p -grupo finito. Sabemos que su centro $Z(G)$ es no trivial y $G/Z(G)$ es un p -grupo de cardinal menor que $|G|$, así que podemos, inductivamente, suponer que es nilpotente. El resultado sigue entonces del ejercicio 9.2.5.

9.2.7. Los subgrupos Z_i que aparecen en la serie central de G son subgrupos característicos en G .

Esto puede verse por inducción en i , siendo inmediato para $i = 0$. Para ver que Z_{i+1} es característico en G si Z_i lo es, proceda de la siguiente manera: muestre que todo $\alpha \in \text{Aut}(G)$ induce, de manera natural, un automorfismo $\bar{\alpha} \in \text{Aut}(G/Z_i)$ tal que conmuta

$$\begin{array}{ccc} G & \twoheadrightarrow & G/Z_i \\ \alpha \downarrow & & \downarrow \bar{\alpha} \\ G & \twoheadrightarrow & G/Z_i \end{array}$$

Usando que el centro de un grupo es característico, concluir que Z_{i+1} es característico.

9.2.8. Un cociente de un grupo nilpotente es nilpotente. Para mostrarlo, considere un homomorfismo $f : G \rightarrow G'$ con dominio G nilpotente y verifique que si $(Z_i)_{i \geq 0}$ es la cadena central superior de G , entonces $(f(Z_i))_{i \geq 0}$ es una cadena central ascendente de G' que termina en G' .

Solución. Sea $K = \ker f$ e identifiquemos a G' con G/K y a f con la proyección canónica $G \rightarrow G/K$; entonces para cada $i \geq 0$ es $f(Z_i) = Z_iK/K$. Tenemos que

$$f(Z_{i+1})/f(Z_i) = (Z_{i+1}K/K)/(Z_iK/K) \cong Z_{i+1}K/Z_iK$$

y

$$G'/f(Z_i) = (G/K)/(Z_iK/K) \cong G/Z_iK,$$

así que para ver que $(f(Z_i))_{i \geq 0}$ es una cadena central ascendente que termina en G' bastará mostrar que $Z_{i+1}K/Z_iK \subset Z(G/Z_iK)$. En término de elementos, esta inclusión es equivalente a que siempre que $z_{i+1} \in Z_{i+1}$, $k \in K$ y $g \in G$, existe $l \in Z_iK$ tal que $z_{i+1}kg = gz_{i+1}kl$.

Consideremos entonces $z_{i+1} \in Z_{i+1}$, $k \in K$ y $g \in G$. Como K es normal en G , existe $k' \in K$ tal que $kg = gk'$; por otro lado, como $Z_{i+1}/Z_i = Z(G/Z_i)$, existe $z_i \in Z_i$ tal que $z_{i+1}g = gz_{i+1}z_i$. Es

$$z_{i+1}kg = z_{i+1}gk' = gz_{i+1}z_ik',$$

así que podemos tomar $l = z_ik' \in Z_iK$. □

9.2.9. Todo subgrupo de un grupo nilpotente es nilpotente.

Solución. Sea G un grupo nilpotente, $G' \subset G$ un subgrupo y $(Z_i)_{i \geq 0}$ la cadena central superior de G . Es evidente que $G' \cap Z_0 = 1$. Por otro lado, si $i \geq 0$,

$$Z\left(\frac{G'}{G' \cap Z_i}\right) \supset \frac{G'}{G' \cap Z_i} \cap Z\left(\frac{G'}{Z_i}\right) = \frac{G'}{G' \cap Z_i} \cap \frac{Z_{i+1}}{Z_i} = \frac{G'Z_i}{Z_i} \cap \frac{Z_{i+1}}{Z_i}$$

y como $Z_{i+1} \supset Z_i$, esto es

$$\begin{aligned} &= \frac{G'Z_i \cap Z_{i+1}}{Z_i} = \frac{(G' \cap Z_{i+1})Z_i}{Z_i} = \frac{G' \cap Z_{i+1}}{(G' \cap Z_{i+1}) \cap Z_i} \\ &= \frac{G' \cap Z_{i+1}}{G' \cap Z_i}. \end{aligned}$$

Esto muestra que $(G' \cap Z_i)_{\geq 0}$ es una cadena central que, claramente, llega a G' . \square

9.2.10. Todo producto de grupos nilpotentes es nilpotente.

9.2.11. Si G es nilpotente y N es normal en G , entonces $N \cap Z(G) \neq 1$.

Solución. Sea $(Z_i)_{i \geq 0}$ la cadena central superior de G y sea $i_0 = \max\{i \in \mathbb{N}_0 : N \cap Z_i = 1\}$. Esto tiene sentido porque G es nilpotente. Notemos que $Z \cap Z_{i_0+1} \neq 1$.

Como N es normal, $N \cap Z_{i_0+1}$ es normal en G y $[N \cap Z_{i_0+1}, G] \subset N \cap Z_{i_0+1}$ por 3.20; por otro lado, 9.2.2 nos dice que $[Z_{i_0+1}, G] \subset Z_{i_0}$. Vemos así que

$$[N \cap Z_{i_0+1}, G] \subset N \cap Z_{i_0} = 1$$

y, en particular, que $1 \neq N \cap Z_{i_0+1} \subset Z(G)$. Es claro que esto implica que $N \cap Z(G) \neq 1$. \square

9.2.12. Todo subgrupo propio de un grupo nilpotente está estrictamente contenido en su normalizador. En particular, todo subgrupo maximal es normal.

Solución. Sea G un grupo nilpotente, $(Z_i)_{i \geq 0}$ su cadena central superior y sea $H \subsetneq G$ un subgrupo propio. Pongamos $i_0 = \max\{i \in \mathbb{N}_0 : Z_i \subset H\}$. Usando 9.2.2, vemos que $[Z_{i_0+1}, H] \subset [Z_{i_0+1}, G] \subset Z_{i_0} \subset H$. Si tomamos $z \in Z_{i_0+1} \setminus H$, es $[z, H] \subset H$ o, equivalentemente, $zHz^{-1} = H$. Esto nos dice que $z \in N(H) \setminus H$ y vemos que $H \subsetneq N(H)$. \square

9.2.13. Si G es nilpotente y $P \subset G$ es un subgrupo de Sylow de G , entonces P es normal y, en particular, único.

Solución. Supongamos que P no es normal en G , de manera que $N(P) \subsetneq G$. Entonces tanto P como $N(P)$ son subgrupos propios de G y el ejercicio 9.2.12 implica que

$$P \subsetneq N(P) \subsetneq N(N(P)). \tag{4}$$

En vista de 8.16, P es un subgrupo característico de $N(P)$, y como la conjugación por un elemento de $N(N(P))$ induce un automorfismo de $N(P)$, vemos que P es normal en $N(N(P))$. La definición de $N(P)$, entonces, implica que $N(N(P)) \subset N(P)$, contradiciendo (4). \square

9.2.14. Si G es nilpotente y finito y para cada primo p , P_p es el p -subgrupo de Sylow, entonces $G \cong \prod_p P_p$.

Solución. En vista de 9.2.13, cada subgrupo de Sylow es normal en G . Si P_1, \dots, P_k son los subgrupos no triviales de Sylow de G , entonces $|G| = |P_1| \cdots |P_k|$ y los órdenes de estos subgrupos son coprimos dos a dos. El resultado deseado sigue entonces de 6.3(d). \square

Esta serie de ejercicios prueba el siguiente teorema:

Teorema. *Un grupo finito es nilpotente sii es isomorfo al producto de sus subgrupos de Sylow.*



William Burnside
1852–1927, Inglaterra

William Burnside fue el primero en desarrollar la teoría de grupos desde el punto de vista abstracto. Publicó en 1897 *The Theory of Groups of Finite Order*, el primer libro sobre la teoría de grupos publicado en inglés. En 1904 demostró que todo grupo de orden $p^n q^m$ es soluble, uno de sus resultados más importantes, y conjeturó que todo grupo de orden impar es soluble. Este último resultado fue obtenido en 1962 por Walter Feit y John Griggs Thompson, quienes dieron una demostración de 250 páginas (Feit, W. y Thompson, J. G. Solvability of Groups of Odd Order. *Pacific J. Math.* 13, 775-1029, 1963)