Lección nº 1 Junio, 2021

Capítulo 1

Grupos, subgrupos y homomorfismos

1.1. Grupos

Antes de pasar a la definición de grupo recordemos que, dado un conjunto no vacío G, una *ley de composición interna en* G es una función $G \times G \to G$. Notaremos por $x \cdot y$, o simplemente xy, a la imagen de un par ordenado $(x, y) \in G \times G$ a través de una ley de composición, y nos referiremos a este elemento como *la multiplicación de* x *e* y (en algunas ocasiones también es conveniente usar una notación aditiva para la ley de composición interna, de la forma $x + y$; y en este caso llamaremos a este elemento *la suma de* x *y* y).

Con esto en mente podemos pasar a la definición de grupo.

Definición (Grupo)**.** Un conjunto no vacío G junto con una ley de composición interna es un *grupo* si:

(1) La ley de composición es *asociativa*, es decir, para todos $x, y, z \in G$ se verifica

$$(xy)z = x(yz).$$

(2) Existe un elemento $1 \in G$ tal que para todo $x \in G$ se satisface

$$x1 = x = 1x.$$

A un tal elemento se lo denomina el *elemento neutro*.

(3) Para cada $x \in G$ existe un elemento $y \in G$ tal que

$$xy = 1 = yx.$$

A un tal elemento se lo denomina el *inverso* de x.

Suele denotarse un grupo como el par ordenado $(G, \cdot)$, especificando en este caso la ley de composición interna. Y, cuando no existe posibilidad a confusión, se escribe únicamente como G.

Si G es un grupo donde para todo $x, y \in G$ se satisface $xy = yx$, entonces diremos que G es un grupo *abeliano* o *conmutativo*.

Además, si G es un grupo y $|G| < +\infty$, diremos que G es un *grupo finito* y que $|G|$ es el *orden de* G.

Observaciones.

(1) El elemento neutro de un grupo es único. En efecto, si e, e' son elementos neutros de un grupo G, entonces
$$e = ee' = e'.$$

(2) De igual manera, dado un elemento x de un grupo G, su inverso es único. Para probarlo notemos que si y, y' son inversos de x entonces
$$y = ye = y(xy') = (yx)y' = ey' = y'.$$
Gracias a esto, adoptamos la notación de x^{-1} para el inverso de x.

Ejercicio 1.1. Sea G es un conjunto no vacío con una ley de composición interna definida. Probar que G es un grupo si y solo si se cumplen las dos condiciones siguientes:

(1) Existe un elemento $1 \in G$ tal que para todo $x \in G$ se verifica $1a = a$.

(2) Para cada $x \in G$ existe $y \in G$ tal que $yx = 1$.

Ahora notemos algo importante, la propiedad asociativa nos asegura que, dado cualquier tripla de elementos de x, y, z en un grupo G, la forma en que se coloquen los paréntesis para operarlos es irrelevante. Gracias a esto, podemos escribir simplemente xyz para referirnos al elemento que resulta de colocar los paréntesis de cualquier manera. Sin embargo, no es trivial que ocurre con un producto de más de 3 elementos. Por ejemplo, si tomamos $x_1, x_2, x_3, x_4 \in G$, podemos formar los productos
$$x_1(x_2(x_3x_4)), \quad x_1((x_2x_3)x_4), \quad (x_1x_2)(x_3x_4), \quad ((x_1x_2)x_3)x_4, \quad (x_1(x_2x_3))x_4;$$
y no resulta evidente que todas las expresiones anteriores sean iguales.

Ejercicio 1.2. Sea G un grupo. Demostrar que para todo n entero positivo y $x_1, x_2, \ldots, x_n$ elementos de G, la expresión $x_1x_2\cdots x_n$ es independiente del orden de los paréntesis. (*Sugerencia: use inducción sobre n.*)

Adoptemos una nueva notación para el producto de n elementos de un grupo. Dado un entero positivo n y $x_1, x_2, \ldots, x_n$ elementos de G, definimos
$$\prod_{i=1}^{n} x_i = x_1x_2\cdots x_n.$$

Definición. Sea G un grupo y $x \in G$. Definimos $x^0 = 1$ y, dado un entero $n \geq 0$, inductivamente $x^{n+1} = xx^n$ (cuando se trabaja con la notación aditiva se escribe nx en lugar de x^n). Además, también definimos $x^{-n} = (x^{-1})^n$.

Ejercicio 1.3. Sean G un grupo, $n, m \in \mathbb{Z}$ y $x, y \in G$. Probar que

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

(2) $(xy)^{-1} = y^{-1}x^{-1}$.

(3) $x^nx^m = x^{n+m}$.

(4) $(x^n)^m = x^{nm}$.

Demos ahora algunos ejemplos de grupos.

Ejemplos 1.4. En todos los ejemplos siguientes, n representa un entero positivo.

(1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ y $(\mathbb{C}, +)$ son grupos (abelianos).

(2) Dado $a \in \mathbb{Z}$, denotamos por $[a]$, o por $\overline{a}$, a la clase de equivalencia del entero a módulo n; es decir

$$[a] = \overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \text{ mód } n\} = \{a + kn \mid k \in \mathbb{Z}\}.$$

Luego, al conjunto de todas las clases de equivalencia mód n, $\mathbb{Z}/n\mathbb{Z}$, lo llamaremos el conjunto de los *enteros módulo* n, y gracias al algoritmo euclidiano sabemos que

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$

Sobre este conjunto se define la operación $[a] + [b] = [a + b]$, y con esto es posible probar que $\mathbb{Z}/n\mathbb{Z}$ es un grupo abeliano (para una descripción más detallada de este grupo y sus propiedades ver el Apéndice A).

(3) Sea E un conjunto no vacío. Definimos G como el conjunto de todas las funciones biyectivas de E sobre E. Si consideramos la composición de funciones como una ley de composición interna en G, entonces G es un grupo. En efecto, la función $\mathrm{id}_E : E \to E$ definida por $\mathrm{id}_E(x) = x$ es el elemento neutro; mientras que dada una función $f \in G$, existe su función inversa f^{-1} pues f es biyectiva, y f^{-1} es también biyectiva; la asociatividad de la operación es evidente.

A este grupo se lo denomina el *grupo simétrico sobre* E, y a sus elementos *permutaciones de* E. Además, notaremos a este grupo como $\mathrm{Sym}(E)$ o, en el caso particular que E sea un conjunto finito, como S_n, donde $n = |E|$.

Es importante mencionar que S_2 es un grupo abeliano; mientras que si $|E| \geq 3$, esto no es verdad (¿por qué?).

(4) Definimos $\mathrm{GL}(n, \mathbb{R}) = \{A \in \mathbb{M}_{n\times n}(\mathbb{R}) \mid \det(A) \neq 0\}$. Así, $\mathrm{GL}(n, \mathbb{R})$ es un grupo con la operación de multiplicación de matrices. Para probar esto notemos que, dadas dos matrices $A, B \in \mathrm{GL}(n, \mathbb{R})$, se tiene que

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

por lo que $AB \in \mathrm{GL}(n, \mathbb{R})$; además, la matriz I es el elemento neutro de este grupo; adicional a esto, si $A \in \mathrm{GL}(n, \mathbb{R})$, A es invertible y por tanto existe $A^{-1} \in \mathrm{GL}(n, \mathbb{R})$; la asociatividad de la ley de composición interna es evidente.

A este grupo se lo denomina *grupo lineal general de grado* n *sobre* $\mathbb{R}$. De manera análoga se define el grupo lineal general de grado n sobre $\mathbb{C}$, $\mathrm{GL}(n, \mathbb{C})$.

(5) El conjunto $\mathrm{SL}(n, \mathbb{R}) = \{A \in \mathbb{M}_{n\times n}(\mathbb{R}) \mid \det(A) = 1\}$ es un grupo equipado con la operación de multiplicación de matrices. La demostración de este hecho es exactamente igual que en el ejemplo anterior, por lo que la omitimos. Este grupo recibe el nombre de *grupo lineal especial de grado* n *sobre* $\mathbb{R}$, y de manera similar se define el grupo lineal especial de grado n sobre $\mathbb{C}$, $\mathrm{SL}(n, \mathbb{C})$.

(6) El conjunto $O(n) = \{A \in \mathbb{M}_{n\times n}(\mathbb{R}) \,|\, A \text{ es ortogonal}\}$ es un grupo con la multiplicación de matrices. Recordemos que una matriz cuadrada A se dice ortogonal si satisface ${}^\top AA = A^\top A = I$, en particular debe ser invertible. Para probar que este conjunto es un grupo, basta seguir los mismos argumentos que en el caso del grupo lineal general, teniendo en mente que para todo par de matrices A, B se cumple

$$ {}^\top(AB) = {}^\top B^\top A, \quad {}^\top({}^\top A) = A. $$

A este grupo se lo llama *grupo ortogonal de grado n*.

(7) Definimos $\mathrm{U}(n) = \{U \in \mathbb{M}_{n\times n}(\mathbb{C}) \,|\, U \text{ es unitaria}\}$ es un grupo equipado con la operación usual de multiplicación de matrices. Una matriz cuadrada con entradas complejas U se dice unitaria si $UU^* = U^*U = I$, donde U^* representa la matriz transpuesta conjugada de U. La demostración de que este conjunto es un grupo es igual a la del ejemplo anterior, pero ahora teniendo en cuenta que para todo par de matrices A, B

$$ (AB)^* = B^*A^*, \quad (A^*)^* = A. $$

Definición. Sea G un grupo y $x \in G$. Diremos que x tiene orden finito en G si existe un entero positivo n tal que

$$ x^n = 1. $$

Al menor entero positivo m tal que $x^m = 1$ lo llamaremos *el orden de x*.

Ejemplo 1.5. Sean p un número primo y $x \in \mathbb{Z}/p\mathbb{Z}$ con $x \notin \{0, 1\}$. Consideremos el conjunto de todos los elementos de la forma $x, x^2, \ldots, x^t, \ldots$; sabemos que estos pertenecen a $\mathbb{Z}/p\mathbb{Z}$, pero dado que este último conjunto es finito deben existir dos enteros positivos distintos r, s, tales que $x^r = x^s$. Podemos asumir que $r > s$, y entonces tenemos que $x^{r-s} = 1$ con $r - s \geq 1$. Por tanto, x tiene orden finito.

Ejercicio 1.6. Si G es un grupo finito, probar que todo elemento de G tiene orden finito.

1.1.1. Grupos Simétricos

Consideremos n un entero positivo. Dado $\sigma \in S_n$, lo representaremos matricialmente de la siguiente forma

$$ \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}. $$

Esto se conoce como *notación a dos filas* que, aunque es útil, tiene sus inconvenientes, por lo que se introduce el siguiente tipo especial de permutaciones.

Definición (k-ciclo)**.** Sean $i_1, i_2, \ldots, i_k$ enteros positivos distintos entre 1 y n, con $k \leq n$, y $\sigma \in S_n$. Si σ es tal que

$$ i_1 \longmapsto i_2 \longmapsto i_3 \longmapsto \cdots \longmapsto i_{k-1} \longmapsto i_k \longmapsto i_1, $$

y $\sigma(i) = i$ para todo $i \notin \{i_1, i_2, \ldots, i_k\}$, entonces σ se llama un *k-ciclo* y se denota como

$$ \sigma = (i_1\ i_2\ \cdots\ i_k). $$

A los 2-ciclos se los denomina comúnmente *transposiciones*.

Ejemplo 1.7. Si $p \in S_8$ y

$$p = \begin{pmatrix} 1 & 2 & 3 & \cdots & 7 & 8 \\ 2 & 3 & 4 & \cdots & 8 & 1 \end{pmatrix},$$

entonces se escribe $p = (1\ 2\ 3\ \cdots\ 7\ 8)$.

Ejercicio 1.8. Dada una permutación $\sigma \in S_n$, encuentre una forma de determinar σ^{-1} usando la notación a 2 filas.

Definición. Dos ciclos $(i_1\ \cdots\ i_r)$ y $(j_1\ \cdots\ j_s)$ se llaman *disjuntos* si $\{i_1, \ldots, i_r\} \cap \{j_1, \ldots, j_s\} = \emptyset$.

Ejercicio 1.9. Si $(i_1\ \cdots\ i_r), (j_1\ \cdots\ j_s)$ son ciclos disjuntos, probar que ambos conmutan. Es decir, que se verifica

$$(i_1\ \cdots\ i_r)(j_1\ \cdots\ j_s) = (j_1\ \cdots\ j_s)(i_1\ \cdots\ i_r).$$

Teorema 1.10. *Toda permutación $\sigma \in S_n$ es producto de ciclos disjuntos.*

En el apéndice B se presenta una demostración alternativa de este resultado, usando la teoría de acciones de grupos.

Antes de dar la demostración de este teorema, demos un ejemplo de como se puede factorizar una permutación en el producto de ciclos disjuntos.

Ejemplo 1.11. Sea $\sigma \in S_8$ definida como

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 5 & 1 & 3 & 8 & 6 & 7 \end{pmatrix}.$$

Notemos que tomando $\sigma_1 = (1\ 2\ 4), \sigma_2 = (3\ 5)$ y $\sigma_3 = (6\ 8\ 7)$ se tiene que

$$\sigma = \sigma_3\sigma_2\sigma_1 = (6\ 8\ 7)(3\ 5)(1\ 2\ 4).$$

Demostración. Sea $\sigma \in S_n$, tenemos

$$1 \longmapsto \sigma(1) \longmapsto \sigma^2(1) \longmapsto \cdots \longmapsto \sigma^{r_1-1}(1) \longmapsto \sigma^{r_1}(1) = 1,$$

y hacemos $\sigma_1 = (1\ \sigma(1)\ \cdots\ \sigma^{r_1-1}(1))$. Notemos que siempre es posible encontrar un entero positivo r_1 que cumple con la propiedad anterior descrita. En efecto, si $\sigma(1) = 1$ entonces $r_1 = 1$; mientras que si $\sigma(1) \neq 1$, entonces el conjunto $\{1, \sigma(1), \sigma^2(1), \ldots\}$ es finito pues el conjunto imagen de σ es finito. Así, tomando r_1 como el mínimo número natural tal que $\sigma^{r_1}(1) \in \{1, \ldots, \sigma^{r_1-1}(1)\}$, entonces se deduce que $\sigma^{r_1}(1) = 1$, ya que de no ser así se contradice la inyectividad de σ.

Ahora, si $r_1 - 1 = n$ tenemos que σ es un n-ciclo. De no ser así, tomamos i_2 como el menor entero positivo tal que

$$i_2 \in \{1, \ldots, n\} \setminus \{1, \sigma(1), \ldots, \sigma^{r_1-1}(1)\},$$

hacemos

$$i_2 \longmapsto \sigma(i_2) \longmapsto \sigma^2(i_2) \longmapsto \cdots \longmapsto \sigma^{r_2-1}(i_2) \longmapsto \sigma^{r_2}(i_2) = i_2,$$

y fijamos $\sigma_2 = (i_2\ \sigma(i_2)\ \cdots\ \sigma^{r_2-1}(i_2))$. Procediendo de esta manera tenemos $\sigma_k = (i_k\ \cdots\ \sigma^{r_k-1}(i_k))$, con lo cual

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_k,$$

con $\sigma_1, \ldots, \sigma_k$ ciclos disjuntos. □

Ejercicio 1.12. Sea $(i_1\ i_2\ \cdots\ i_r)$ un r-ciclo. Probar que

$$(i_1\ i_2\ \cdots\ i_r) = (i_1\ i_r)(i_1\ i_{r-1}) \cdots (i_1\ i_3)(i_1\ i_2).$$

Corolario 1.13.

(1) Toda permutación $\sigma \in S_n$ es un producto de transposiciones.

(2) Si $\sigma = \sigma_1 \cdots \sigma_r = \tau_1 \cdots \tau_s$, donde las σ_i y las τ_i son transposiciones, entonces r y s tienen la misma paridad.

Notemos que el corolario anterior nos permite dar paso a la siguiente definición.

Definición. Sea $\sigma \in S_n$. Si $\sigma = \tau_1 \cdots, \tau_r$, τ_i transposiciones, y r es par (impar), entonces σ se dice *par* (*impar*).

Notación. Dados $A \in \mathrm{GL}(n, \mathbb{R})$ y $\sigma \in S_n$, A_σ es la matriz que resulta de permutar las filas de A según la permutación σ; es decir, si $A = (a_{ij})$, entonces $A_\sigma = (a_{\sigma^{-1}(i)j})$.

Ejercicio 1.14. Sean $A \in \mathrm{GL}(n, \mathbb{R})$ y $\sigma \in S_n$. Demostrar que $A_\sigma = I_\sigma A$.

Observación. A las matrices del conjunto $\{I_\sigma \mid \sigma \in S_n\}$ se las llama *matrices de permutación*. Además, se tiene que $\det(I_\sigma) \in \{1, -1\}$ y $\det(A_\sigma) = \det(I_\sigma)\det(A)$. En particular, si τ es una transposición se cumple $\det(I_\tau) = -1$ y por tanto $\det(A_\sigma) = -\det(A)$.

Ejercicio 1.15. Demostrar que, dadas $\sigma, \tau \in S_n$, entonces $I_{\sigma\tau} = I_\sigma I_\tau$.

Demostración del Corolario 1.13. El primer punto se deduce directamente del Ejercicio 1.12. Para el segundo punto notemos que, gracias al ejercicio anterior tenemos

$$I_\sigma = I_{\sigma_1} \cdots I_{\sigma_r} = I_{\tau_1} \cdots I_{\tau_s},$$

de donde

$$\det(I_{\sigma_1}) \cdots \det(I_{\sigma_r}) = \det(I_{\tau_1}) \cdots \det(I_{\tau_s}).$$

Así, obtenemos $(-1)^r = (-1)^s$ lo que nos permite concluir que r y s tienen la misma paridad. □

Definición. El signo de $\sigma \in S_n$ es

$$\mathrm{sign}(\sigma) = \det(I_\sigma) = (-1)^r,$$

donde $\sigma = \tau_1 \cdots \tau_r$, con τ_i transposiciones.

Por la definición anterior tenemos que

$$\begin{array}{rccc} \mathrm{sign} : S_n & \longrightarrow & \{-1, 1\} \\ \sigma & \longmapsto & \det(I_\sigma) \end{array},$$

y la proposición siguiente nos brinda información con respecto a la aplicación sig.

Proposición 1.16. *Para todo $\sigma, \tau \in S_n$ se satisface*

$$\mathrm{sign}(\sigma\tau) = \mathrm{sign}(\sigma)\mathrm{sign}(\tau).$$

La Proposición 1.16 nos dice que sign es un homomorfismo de S_n en $\{1, -1\}$. Pero, dado que $\mathrm{sign}(i\ j) = -1$, entonces este es un homomorfismo sobreyectivo (i.e un epimorfismo).

Además, podemos determinar la paridad de una permutación $\sigma \in S_n$ de la siguiente manera: $\sigma \in S_n$ es par (impar) si y solo si $\operatorname{sig} \sigma = 1$ ($\operatorname{sig} \sigma = -1$).

Definición. Sean G y G' dos grupos. Una función $f : G \to G'$ se llama *homomorfismo* de grupos si

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

para todo $x, y \in G$. Además:

(1) Si f es inyectiva, será llamada *monomorfismo*. Notaremos

$$f\colon G \hookrightarrow G'.$$

(2) Si f es sobreyectiva, será llamada *epimorfismo*. Notaremos

$$f\colon G \twoheadrightarrow G', \quad G \xrightarrow{f} \!\!\!\!\rightarrow G'.$$

(3) f se dice *isomorfismo* si existe un homomorfismo $h\colon G' \to G$ tal que

$$f \circ h = \mathrm{id}_{G'}, \quad h \circ f = \mathrm{id}_G.$$

En este caso, notamos

$$f\colon G \xrightarrow{\sim} G', \quad G \cong G'.$$

Si $G = G'$, a f lo llamaremos automorfismo de G. Al conjunto de los automorfismos de G lo notaremos por $\operatorname{Aut}(G)$, el cual forma un grupo con la operación de composición de funciones.

Ejercicio 1.17. Dado $f : G \to G'$. Probar que f es un isomorfismo si y sólo si f es un homomorfismo biyectivo.

Ejercicio 1.18. Dado $f\colon G \to G'$ un homomorfismo de grupos, demostrar que

(1) $f(1) = 1'$, donde 1 y $1'$ son los elementos de neutros de G y G', respectivamente.

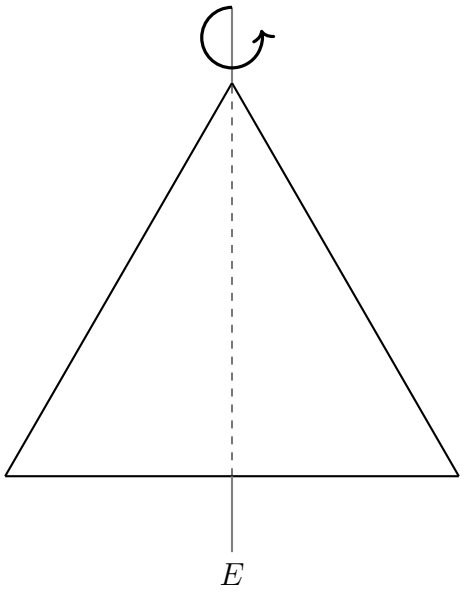
(2) Para todo $x \in G$ se verifica que $f(x^{-1}) = f(x)^{-1}$.

Ejemplo 1.19 (Grupos diedros)**.** Dado $n \in \mathbb{Z}^+$, $n \geq 3$, consideremos a P_n, el $n-$ágono regular con centro en el origen al plano $\mathbb{R}^2$. Una *simetría* de P_n es una transformación ortogonal $\rho : \mathbb{R}^2 \to \mathbb{R}^2$ tal que $\rho(P_n) = P_n$. D_{2n} denota el conjunto de todas las simetría de P_n, y si $\rho : \mathbb{R}^2 \to \mathbb{R}^2$ es una simetría de P_n, entonces el *eje de simetría* de ρ es $\ker(\rho - \mathrm{id})$.

Por ejemplo, con $n = 3$, tenemos en rectángulo equilátero P_3. Para tener una noción geométrica de un eje de simetría, consideremos a la simetría $\rho : \mathbb{R}^2 \to \mathbb{R}^2$ de P_3 dada por

$$\rho \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -x \\ y \end{pmatrix}.$$

Es fácil de ver que el eje de simetría de ρ es el conjunto $\ker(\rho - \mathrm{id}) = \{(x, y) \in \mathbb{R}^2 \,|\, x = 0\}$.

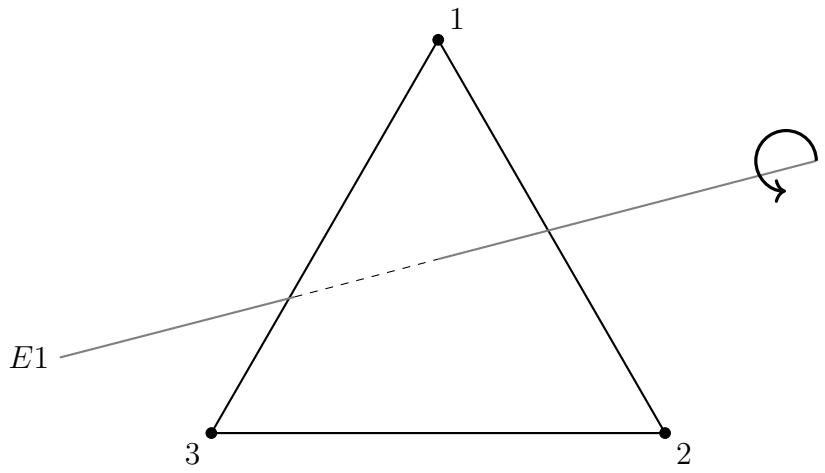


E: Eje de simetría de ρ.

Observación. Si el eje de simetría es un punto, pensaremos en este como una recta perpendicular al plano que pasa por dicho punto.

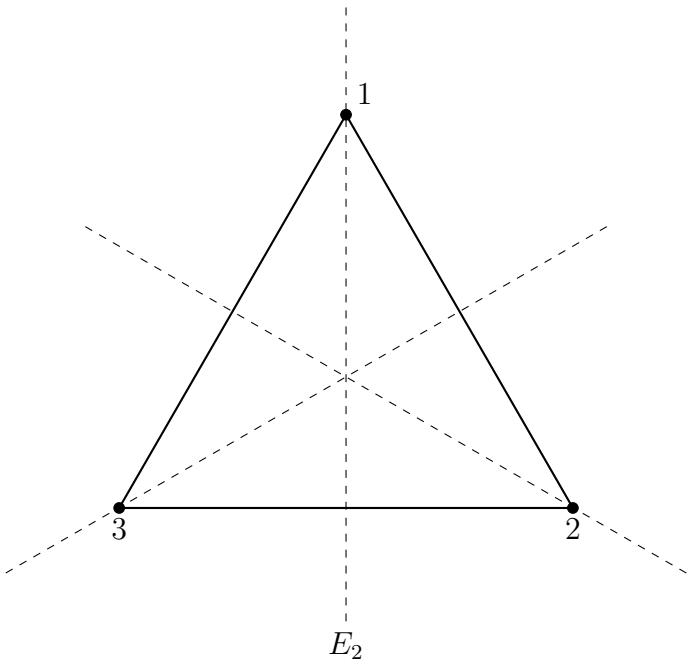
D_{2n} forma un grupo si definimos st, con $s, t \in D_{2n}$, a la simetría obtenida al aplicar primero t y luego s.

- Podemos determinar el conjunto simetrías D_6 a partir de los ejes de simetría del triángulo.



E_1: Eje de simetría que pasa por el centro del triángulo y es perpendicular al plano.

$$r^k = \begin{pmatrix} \cos(2k\pi/3) & \sin(2k\pi/3) \\ -\sin(2k\pi/3) & \cos(2k\pi/3) \end{pmatrix}, \quad k = 1, 2; \quad r^0 = r^3 = 1$$



E_2: Eje de simetría que une el vértice 1 con el punto medio del lado opuesto.

$$s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; \quad s^2 = 1;$$

Simetrías restantes : $rs, r^2s = sr$;

$$D_6 = \{1, r, r^2, s, rs, r^2s \mid r^2s = sr, r^3 = 1, s^2 = 1\}.$$

Cualquier producto de r y s se reduce a un elemento de D_6.

Ejemplo 1.20.

$$sr^2 = s(rr) = (sr)r = (r^2s)r = r^2(r^2s) = r^4s = r^3rs = rs.$$

Ejercicio 1.21. Reducir la simetría rsr^2srsr^2s.

Observaciones. 1. $|D_6| = 6$.

2. r y s son un "sistema de generadores" de D_6.
3. A toda simetría $E \in D_6$ le corresponde una única permutación de los vértices $\{1, 2, 3\}$ del triángulo $\sigma_E \in S_3$. Esto define una aplicación $\phi : D_6 \to S_3$ definida por

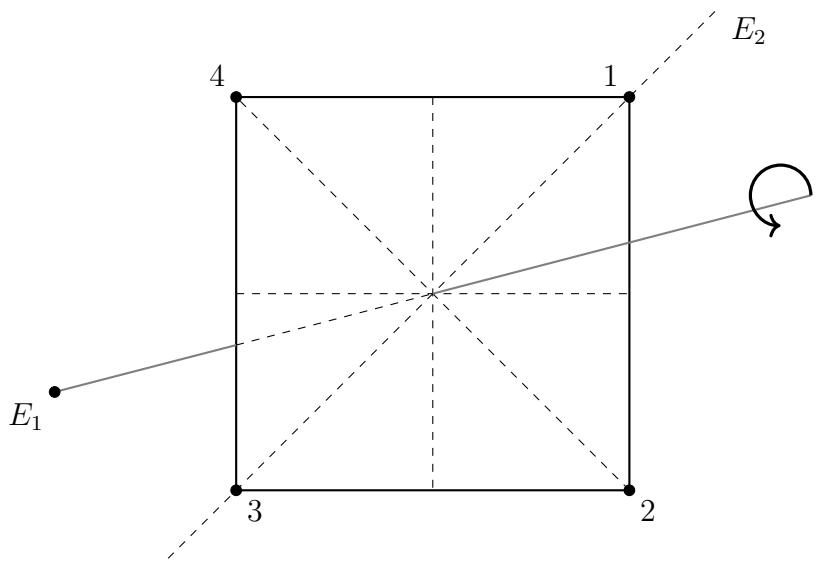
$$\begin{array}{lll} \phi(1) = \mathrm{id}, & \phi(r) = (1\ 2\ 3), & \phi(r^2) = (1\ 3\ 2) \\ \phi(s) = (2\ 3) & \phi(rs) = (1\ 2) & \phi(r^2s) = (1\ 3) \end{array}$$

ϕ es un homomorfismo y más aún, es inyectiva, por tanto es un isomorfismo de grupos.

$$\phi : D_6 \xrightarrow{\sim} S_3.$$

Notación. $D_6 = \langle r, s \mid r^3 = s^2 = e, r^2s = sr \rangle$.

- Cuando $n = 4$ buscamos el conjunto de simetrías del cuadrado.



E_1: Eje de simetría que pasa por el centro del cuadrado y es perpendicular al plano.

E_2: Eje de simetría que une el vértice 1 con el vértice 3.

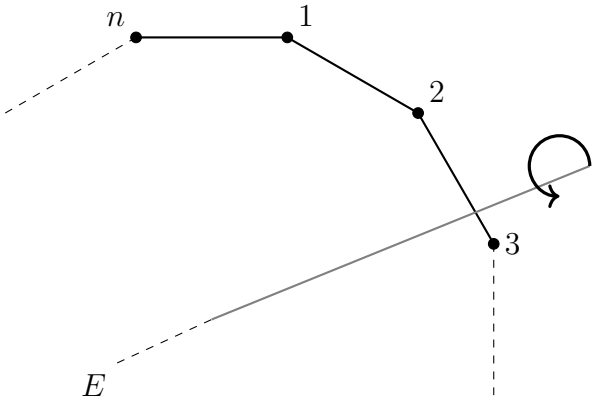
$$r^k = \begin{pmatrix} \cos(k\pi/2) & \sin(k\pi/2) \\ -\sin(k\pi/2) & \cos(k\pi/2) \end{pmatrix}, k = 1, 2, 3; \quad r^0 = r^4 = 1;$$

$$s = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \quad s^2 = 1;$$

Simetrías restantes : $rs = sr^3, r^2s, r^3s$.

$$D_8 = \langle r, s |\ r^4 = s^2 = 1, rs = sr^3 \rangle.$$

- El caso general se presenta de forma análoga.



E : Eje de simetría que pasa por el centro del $n-$ágono y es perpendicular al plano.

$$r^k = \begin{pmatrix} \cos(2k\pi/3) & \sin(2k\pi/3) \\ -\sin(2k\pi/3) & \cos(2k\pi/3) \end{pmatrix}, k = 1, \ldots, n; \quad r^0 = r^n = 1.$$

Simetrías restantes : $s, rs = sr^{n-1}, r^k s,\ k = 2, \ldots, n-1$.

Entonces

$$D_{2n} = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\} = \langle r, s \mid rs = sr^{n-1}, r^n = s^2 = 1\rangle.$$

Además, $|D_{2n}| = 2n$ y a toda simetría $E \in D_{2n}$ le corresponde una única permutación de $\{1,\ldots,n\}$-vértices del $n-$ágono $\sigma_E \in S_n$. Esto define el monomorfismo

$$\begin{aligned} \phi : D_{2n} &\to S_n \\ E &\mapsto \phi(E) = \sigma_E. \end{aligned}$$

Ejercicio 1.22. Definir el monomorfismo $\phi : D_8 \to S_4$

Ejemplo 1.23 (Grupo Cuaterniónico)**.** Consideremos las matrices

$$1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

El conjunto $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ es un grupo bajo la operación de multiplicación de matrices, conocido como *grupo de cuaterniones* o *grupo cuaterniónico*. Las relaciones que se tienen son:

$$i^2 = j^2 = k^2 = -I, ij = k;$$

$$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = -1, ij = k\rangle.$$

Ejemplo 1.24 (Vierergruppe - Grupo de 4 de Klein)**.** Consideremos las matrices

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}.$$

El conjunto $V_4 = \{1, a, b, c\}$ es un grupo bajo la operación de multiplicación de matrices, en donde se cumplen las siguientes relaciones

$$a^2 = b^2 = c^2 = 1, \quad ab = c.$$

Ejemplo 1.25 (Cuerpos)**.** Sea F un conjunto con dos leyes de composición interna $+$ y $\cdot$. Asumamos que $(F, +)$ es un grupo abeliano y denotemos por 0 a su neutro aditivo. Escribimos $F^* = F \setminus \{0\}$. Decimos que F es un *cuerpo* (algunas personas también lo llaman *campo*) si $(F^*, \cdot)$ es un grupo abeliano y si además la operación $\cdot$ se distribuye sobre $+$, es decir, para todo $x, y, z \in F$,

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z).$$

Usualmente escribimos xy en lugar de $x \cdot y$ y denotamos por 1 al elemento identidad del grupo F^*. Llamamos a $(F, +)$ el *grupo aditivo* y a $(F^*, \cdot)$ el *grupo multiplicativo* del cuerpo F.

Si omitimos la condición de conmutatividad en el grupo multiplicativo F^*, obtenemos lo que se denomina un *anillo de división* (que algunos autores denominan *cuerpo no conmutativo*).

El lector debe estar familiarizado con varios ejemplos de cuerpos, como $\mathbb{R}$, $\mathbb{C}$, $\mathbb{C}$.

1.2. Subgrupos

Definición (Subgrupo)**.** Sea G un grupo. Un conjunto $H \subseteq G$, $H \neq \emptyset$ se llama un *subgrupo* de G si:

(1) H es cerrado con respecto a la ley de composición interna de G; es decir, si para todo par de elementos $x, y \in H$ se cumple $xy \in H$.

(2) Para todo $x \in H$ se tiene que $x^{-1} \in H$.

De esta manera, H es un grupo equipado con la misma composición interna de G. Además, notamos $H \leq G$.

Observación. Las dos condiciones de la definición de subgrupo pueden resumirse como para todo par de elementos $x, y \in H$ se cumple $xy^{-1} \in H$.

Ejercicio 1.26. Sea G un grupo finito y $H \subseteq G$ no vacío. Probar que

$$H \leq G \iff \forall\, x, y \in H, \quad xy \in H.$$

Veamos algunos ejemplos de subgrupos

Ejemplos 1.27.

(1) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

(2) Dado $\phi : D_{2n} \to S_n$ un monomorfismo, entonces $\mathrm{Img}(\phi) \leq S_n$. Además, $\phi : D_{2n} \xrightarrow{\sim} \mathrm{Img}(\phi) = \phi(D_{2n})$.

(3) Sea $\phi : G \to G'$ un homomorfismo de grupos. Definimos el *núcleo de* ϕ como

$$\ker(\phi) = \{x \in G \,|\, \phi(x) = 1'\},$$

donde $1'$ es el elemento neutro de G'.
Notemos que, si $x, y \in \ker(\phi)$, entonces

$$\phi(xy) = \phi(x)\phi(y) = 1' \cdot 1' = 1',$$
$$\phi(x^{-1}) = \phi(x)^{-1} = 1'^{-1} = 1';$$

es decir $xy \in \ker(\phi)$ y $x^{-1} \in \ker(\phi)$. Por tanto, concluimos que $\ker(\phi) \leq G$.

Ejercicio 1.28. Si $\phi : G \to G'$ es un homomorfismo de grupos. Probar que

(1) ϕ es inyectivo si y solo si $\ker(\phi) = \{1\}$.

(2) $\mathrm{Img}(G) \leq G'$.

Proposición 1.29. *Sean G un grupo y $\{H_i\}_{i \in I}$ una familia de subgrupos de G. Entonces*

$$\bigcap_{i \in I} H_i \leq G.$$

Demostración. Sean $x, y \in \bigcap_{i \in I} H_i$. Así, por definición de intersección, $x, y \in H_i$ para todo $i \in I$ y, dado que todos los H_i son subgrupos de G, deducimos $xy^{-1} \in H_i$ para todo $i \in I$. Por tanto, $xy^{-1} \in \bigcap_{i \in I} H_i$ y concluimos el resultado. □

Definición (Subgrupo generado)**.** Sean G un grupo y $S \subseteq G$ un subconjunto. Definimos el *subgrupo de G generado por S*, y lo notamos $\langle S \rangle$, como

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H \leq G.$$

Formemos el subconjunto de G

$$\{s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} \mid s_i \in S, \varepsilon_i \in \{1, -1\}, n \geq 1\} \subseteq \langle S \rangle.$$

Este es un subgrupo de G que contiene a S y por ende contiene a $\langle X \rangle$. Además, como $\langle S \rangle$ es un grupo que contiene a S, es claro que debe contener a todos los elementos de la forma $s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}$, con $s_i \in S$ y $\varepsilon_i \in \{1, -1\}$. De esta manera, se tiene que $\langle S \rangle = \{s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} \mid s_i \in S, \varepsilon_i \in \{1, -1\}, n \geq 1\}$. En particular, si $G = \langle S \rangle$ diremos que G está *generado* por S y llamaremos a S un *sistema de generadores de G*. Un caso particular es cuando $S = \{g\} \subseteq G$ y así $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$, a este tipo de grupos los llamamos *grupos cíclicos* y tienen la buena propiedad de ser abelianos.

Definición (Producto Directo de Grupos)**.** Consideremos G_1 y G_2 dos grupos. Recordemos que $G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$ y definamos una ley de composición interna en $G_1 \times G_2$ como

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2),$$

donde $(x_1, y_1), (x_2, y_2) \in G_1 \times G_2$. De este modo $G_1 \times G_2$ es un grupo y lo llamamos *el producto directo de G_1 y G_2*.

Sobre el producto directo de dos grupos definimos las *proyecciones canónicas* π_1 y π_2 como

$$\begin{array}{rcl} \pi_1 : G_1 \times G_2 & \longrightarrow & G_1 \\ (x, y) & \longmapsto & x, \end{array} \qquad \begin{array}{rcl} \pi_2 : G_1 \times G_2 & \longrightarrow & G_2 \\ (x, y) & \longmapsto & y. \end{array}$$

Así se tiene que $\ker(\pi_1) = \{(e_1, y) \mid y \in G_2\} \leq G_1 \times G_2$ y $\ker(\pi_2) = \{(x, e_2) \mid x \in G_1\} \leq G_1 \times G_2$, donde e_1, e_2 son los elementos neutros de G_1 y G_2 respectivamente.

Es posible generalizar lo anterior para un número finito de grupos $G_1, \ldots, G_n$. Tomando

$$G_1 \times \cdots \times G_n = \{(x_1, \ldots, x_n) \mid x_i \in G_i,\ i \in \{1, \ldots, n\}\}$$

con el producto definido componente a componente; entonces tenemos que $G_1 \times \cdots \times G_n$ es un grupo.

Ejemplo 1.30 (Sistema de generadores de $GL(2, F)$)**.** Sean F un cuerpo arbitrario y $\mathrm{GL}(2, F)$ el grupo lineal general de matrices de orden 2×2 con elementos en F. Sea además $\alpha \in \mathrm{GL}(2, F)$, digamos $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, con $ad - bc \neq 0$; entonces necesariamente se tiene que $(a, c) \neq (0, 0)$. Multiplicando α por la izquierda (respectivamente por la derecha) por la matriz $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (si $a = 0$), entonces

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix},$$

con $a' \neq 0$. Así, reemplazando α por $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \alpha$, si es necesario, podemos suponer que $a \neq 0$.

Multiplicando la primera fila por números adecuados y agregándosela a la segunda fila podemos eliminar c. Esta operación se obtiene multiplicando por la izquierda la matriz $\begin{pmatrix} 1 & 0 \\ x & 0 \end{pmatrix}$ a la matriz α, con x conveniente.

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & b \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix},$$

con $a'd' \neq 0$.

Eliminamos b' multiplicando la primera columna por un factor adecuado $(-a'^{-1}b')$ y sumamos a la segunda columna. Esto se obtiene multiplicando a la derecha por $\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$.

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a'' & 0 \\ 0 & d'' \end{pmatrix}, \quad a''d'' \neq 0.$$

Donde podemos reescribir

$$\begin{pmatrix} a'' & 0 \\ 0 & d'' \end{pmatrix} = \begin{pmatrix} a'' & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & d'' \end{pmatrix}.$$

Así, α es el producto de matrices del conjunto

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \;\middle|\; a, b, c, d \in F,\ a \neq 0,\ d \neq 0 \right\},$$

por lo que este conjunto genera a $\mathrm{GL}(2, F)$.

Observemos que

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

por lo que

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \;\middle|\; a, b \in F,\ a \neq 0 \right\}$$

es un sistema generador de $\mathrm{GL}(2, F)$.

Si volvemos al caso de un grupo cíclico $G = \langle \{g\} \rangle$, entonces g y g^{-1} son generadores de G.

Ejemplos 1.31.

(1) $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$, por lo que 1 y -1 son generadores de $(\mathbb{Z}, +)$.

(2) Sea $n > 1$ un entero positivo dado. Entonces se tiene que $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$ y $|\mathbb{Z}/n\mathbb{Z}| = n$.

Ejercicio 1.32. Probar que un elemento $[h] \in \mathbb{Z}/n\mathbb{Z}$ es un generador de $\mathbb{Z}/n\mathbb{Z}$ si y solo si $1 \leq k < n$ y $(k, n) = 1$.

Del ejercicio anterior, $\mathbb{Z}/n\mathbb{Z}$ tiene precisamente $\varphi(n) = |\{1 \leq k < n | (k, n) = 1\}|$ generadores. A φ se la conoce como *función de Euler*. Para más detalles, consulte el Apéndice A.

Ejercicio 1.33. $n = \sum_{d|n} \varphi(d)$.

Ejemplo 1.34. Sea $n \in \mathbb{N}$, $\rho \in e^{2\pi i/n}$. Definimos

$$C_n = \{\rho^k \,|\, k = 1, \ldots, n\}, \quad \rho^n = 1.$$

Tenemos que $C_n = \langle s \rangle$ tiene n elementos, lo que es más, $C_n \cong \mathbb{Z}/n\mathbb{Z}$.

Teorema 1.35. *Sea G un grupo cíclico.*

i. Si G es infinito, entonces $G \cong \mathbb{Z}$.

ii. Si G es finito y $|G| = n$, entonces $G \cong \mathbb{Z}/n\mathbb{Z}$.

Demostración. i. Definamos la aplicación

$$\begin{aligned} \phi : G &\to \mathbb{Z} \\ g^k &\mapsto \phi(g^k) = k. \end{aligned}$$

Para mostrar que ϕ es un isomorfismo, probaremos que es un homomorfismo biyectivo.

a) Homomorfismo: Sean $g^k, g^s \in G$, se tiene

$$\phi(g^k g^s) = \phi(g^{k+s}) = k + s.$$

b) Biyectivo: La inyectividad se sigue fácilmente pues dados $g^k, g^s \in G$ tales que $\phi(g^k) = \phi(g^s)$, se tiene

$$k = \phi(g^k) = \phi(g^s) = s.$$

Para la sobreyectividad, tomamos $n \in \mathbb{Z}$ y $x = g^n \in G$, de modo que $\phi(x) = n$.

ii. Sea G un grupo cíclico de orden n, así, existe $g \in G$ tal que

$$G = \langle g \rangle = \langle 1, g, \ldots, g^{n-1} \rangle, \quad g^n = 1.$$

Definamos la aplicación

$$\begin{aligned} \phi : G &\to \mathbb{Z}/n\mathbb{Z} \\ g^k &\mapsto [k]. \end{aligned}$$

Para mostrar que ϕ es un isomorfismo, veamos que es un homomorfismo biyectivo.

a) ϕ es homomorfismo. Sean $k, h \in \{1, \ldots, n\}$,

$$\phi(g^k g^h) = \phi(g^{k+h}) = [k + h] = [k] + [h] = \varphi(g^k) + \varphi(g^h).$$

b) Es fácil de ver que ϕ es inyectivo. Luego, dado que G y $\mathbb{Z}/n\mathbb{Z}$ son finitos y $|G| = |\mathbb{Z}/n\mathbb{Z}| = n$, ϕ también es sobreyectivo.

□

Proposición 1.36. *Sea G un grupo cíclico, $G = \langle g \rangle$ y $H \leq G$. Supongamos que H no es trivial ($H \neq \{1\}$). Sea $n \geq 1$ positivo más pequeño tal que $g^n \in H$. Entonces*

i. Dado $m \in \mathbb{Z}$, $g^m \in H$ si y sólo si $n \mid m$.

ii. $H = \langle g^n \rangle$.

Demostración. i. Sea $m \in \mathbb{Z}$. Si $n \mid m$, entonces existe $q \in \mathbb{Z}$ tal que $m = qn$, y por tanto $g^m = (g^n)^q \in K$. Recíprocamente, supongamos que $g^m \in H$, esto implica que $n \leq m$ y que existan $q \in \mathbb{Z}$ y $0 \leq r < n$ tales que $m = nq + r$. Luego

$$g^m = g^r g^{nq},$$

de donde

$$g^r = g^m g^{-nq} = g^m \left(g^n\right)^{-q} \in H.$$

Pero como n es el entero positivo más pequeño tal que $g^n \in H$, esto implica que $r = 0$ y que $n|m$.

ii. Como $g^n \in H$, entonces $\langle g^n \rangle \leq H$. Por otro lado, si tomamos $h \in H$, entonces existen $m \geq 1$ y $q \in \mathbb{Z}$ tales que $h = g^m$ y $m = nq$ (pues $n \mid m$). Finalmente

$$h = (g^n)^q \in \langle g^n \rangle.$$

□

Corolario 1.37. *Un grupo es cíclico si y sólo si todos sus subgrupos son cíclicos.*

Ejercicio 1.38. Demuestre que todos los subgrupos propios de V_4 (Ejemplo 1.24) son cíclicos, pero sin embargo, todos V_4 no es cíclico.

Lema 1.39. *Sean G un grupo, $g \in G$ tal que $|g| = n < +\infty$. Entonces*

i. Dado $m \in \mathbb{Z}$, $g^m = 1$ si y sólo si $|g| \mid m$;

ii. Sean $m, l \in \mathbb{Z}$, $g^m = g^l$ si y solo si $m \equiv l \pmod{n}$;

iii. $|\langle g \rangle| = |g| = n$.

Demostración. i. Por un lado, si suponemos que $|g| \mid m$, entonces existe $k \in \mathbb{Z}$ tal que $m = |g|\, k$. Luego

$$g^m = g^{|g|k} = \left(g^{|g|}\right)^k = 1.$$

Recíprocamente, si $g^m = 1$, por definición de $|g| = n$, $m \geq n$. Así, existen $k \in \mathbb{Z}$ y $0 \leq r < |g|$ tales que $m = kn + r$. Luego

$$g^m = g^{kn+r} = g^{kn} g^r = 1,$$

lo que implica que

$$g^r = \left(g^{kn}\right)^{-1} = \left((g^n)^k\right)^{-1} = 1.$$

Pero dado que $0 \leq r < n$, entonces necesariamente r debe ser 0, y el resultado se tiene.

ii. Suponemos primero $m \equiv l \pmod{n}$, luego existe $k \in \mathbb{N}$ tal que $g - l = nk$. Es decir, $g - l \mid n$ y gracias a (i), tenemos que $g^{m-l} = 1$ y $g^m = g^l$.

De manera similar si $g^m = g^l$, entonces $g^{m-l} = 1$, y nuevamente por (i) se sigue que $m - l \mid n$. Es decir, $m \equiv l \pmod{n}$.

(1) Se puede ver fácilmente pues $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$.

□

Teorema 1.40. *Sean G un grupo cíclico y $g \in G$ tales que $G = \langle g \rangle$.*

i. Si $|G| = +\infty$, entonces todos los subgrupos de G son de la forma $\langle g^n \rangle$, $n \geq 0$.

ii. Si $|G| < +\infty$ y $|G| = |g| = n$, entonces para todo entero $d \geq 1$ tal que $d \mid n$, existe un

único subgrupo cíclico de orden d, y estos son todos los subgrupos de G.

Demostración. i. Si $|G| = +\infty$, entonces $G = \{g^m \,|\, m \in \mathbb{Z}\}$. Sea $H \leq G$ un subgrupo no trivial de G, entonces

$$H = \langle g^n \rangle,$$

con $n \geq 1$ el entero más pequeño tal que $g^n \in H$. Para ver que $\langle g^k \rangle \neq \langle g^l \rangle$ para cada par de enteros distintos k, h, basta probar que $g^k \neq g^k$. En efecto, sin pérdida de generalidad suponemos $k > h$ y $g^k = g^h$, entonces $g^{k-h} = 1$ y esto implica que $|G| < +\infty$, lo cual es absurdo.

ii. Supongo que $|G| < +\infty$ y $|G| = |g| = n$. Sea $d \geq 1$ tal que $d \,|\, n$. Definimos $f = \frac{n}{d}$ y $H_d = \langle g^f \rangle$.

Ejercicio 1.41. Probar que

$$\left|\langle g^f \rangle\right| = |H_d| = d.$$

Probaremos que $H_d \leq G$ es el único subgrupo de orden $d \mid n$ de G. Sea $H \leq G$ algún otro subgrupo de orden d. Queremos verificar que $H = H_d$. Gracias la proposición 1.36 sabemos que $H = \langle g^l \rangle$, con $l \geq 1$ entero, con la propiedad de que dado $m \in \mathbb{Z}$ tal que $g^m \in H$, entonces $l \mid m$. Pero como $g^n = 1 \in H$, esto implica que $l|n$. Finalmente, puesto que $|H| = d$,

$$g^{ld} = \left(g^l\right)^d = 1 = g^n.$$

Es decir que $n = ld$ y por tanto $l = \frac{n}{d} = f$.

□

Observación. Para todo grupo G de orden $n \geq 1$ y $d \geq 1$ tal que $d|n$, existe un único subgrupo cíclico de orden d, y por tanto hay exactamente $\varphi(d)$ generadores de este subgrupo. Considerando todos los subgrupos de orden $d|n$, para cada uno de ellos tendremos $\varphi(d)$ generadores, y así

$$\sum_{d|n} \varphi(d) = n.$$

Del resultado anterior sabemos que si G es un grupo cíclico finito y H es un subgrupo de G, entonces $|H| \,|\, |G|$, este hecho sirve de motivación para el siguiente teorema:

Teorema 1.42 (Lagrange)**.** *Sea G un grupo finito (arbitrario) y sea $H \leq G$. Entonces*

$$|H| \,|\, |G|\,.$$

Pospondremos la demostración de este teorema.

Corolario 1.43. *Sean G un grupo finito y $g \in G$, entonces $|g| \,|\, |G|$ y, en particular, $g^{|G|} = 1$.*

Definición. Sean G un grupo, $H \leq G$ y $x \in G$. Los subconjuntos $xH = \{xy \,|\, y \in H\}$ se llaman *clases laterales por la izquierda de H.*

Propiedades: Sean $x, y \in G$, entonces:

(1) Si $xH \cap yH \neq \emptyset$, entonces $xH = yH$;

(2) $xH \cap yH = \emptyset$ si y sólo si $xH \neq yH$.

Definición. Sean G un grupo y $H \leq G$. Para todo $x, y \in G$, diremos que x es *congruente a y módulo* H si y sólo si $y^{-1}x \in H$. Escribiremos

$$x \equiv y \ (H) \iff x \in yH \iff x^{-1}y \in H.$$

Ejercicio 1.44. Probar que la congruencia módulo H es una relación de equivalencia en G.

Las clases de equivalencia de esta relación de equivalencia son las clases xH, $x \in G$. De esta manera,

$$G = \bigsqcup_{i \in I} x_i H,$$

donde $\{x_i H\}$ recorre todas las clases laterales por izquierda de H distintas. El conjunto $\{x_i\}_{i \in I}$ se llama un *sistema de representantes de G módulo H*.

Observación. Sea G un grupo finito y $H \leq G$. Para todo $x, y \in G$ se tiene que

$$|xH| = |yH| = |H|.$$

Para verificarlo basta considerar la biyección:

$$\begin{aligned} f : xH &\to yH \\ xh &\mapsto f(xh) = yx^{-1}(xh) = yh. \end{aligned}$$

Definición. La cantidad de clases laterales por la izquierda distintas se llama el *índice de H en G* y lo denotaremos por $[G : H]$.

De esta manera

$$G = \bigsqcup_{i=1}^{[G:H]} x_i H,$$

y además

$$|G| = |H| \, [G : H].$$

Observación. Esto demuestra el teorema de Lagrange.

Notación. Si $x \in G$, denotamos a su clase lateral izquierda por $xH = \overline{x} = [x]$.

Ejemplo 1.45. Dado $n \in \mathbb{N}$. Tomamos $G = \mathbb{Z}$ y $H = n\mathbb{Z} = \langle n \rangle$. Las clases laterales de H son: $n\mathbb{Z}$, $1 + n\mathbb{Z}$, $2 + n\mathbb{Z}$,. . . ,$(n-1) + n\mathbb{Z}$. Luego

$$\mathbb{Z} = \bigsqcup_{i=0}^{n-1} (i + n\mathbb{Z}) = \overline{0} \cup \overline{1} \cup \cdots \cup \overline{n-1}.$$

Definición. Sean G un grupo, $H \leq G$. Consideraremos a las clases laterales por izquierda de H como elementos del conjunto

$$G/H = \{xH \mid x \in G\}.$$

G/H se llama el *conjunto cociente (por izquierda) de G módulo H*.

Si G es un grupo finito, entonces

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

Observaciones. (1) Dados G un grupo y $H \leq G$, podemos introducir a su vez *clases laterales por la derecha*, considerando la relación de equivalencia

$$xy^{-1} \in H \iff x \in Hy \iff y \in Hx.$$

Las clases laterales por la derecha de H son los subconjuntos Hx, con $x \in G$. Denotaremos por $H\backslash G$ al conjunto de las clases laterales por la derecha de H.

(2) Si G es un grupo abeliano, entonces

$$xH = Hx, \quad \forall x \in G.$$

Es decir que $G\backslash H = H/G$.

1.2.1. Subgrupos normales

Sea G un grupo, un tipo de subgrupo $H \leq G$ de interés es aquel que satisface

$$xH = Hx, \quad \forall x \in G,$$

lo cual se tiene si y sólo si

$$xHx^{-1} = H, \quad \forall x \in G.$$

Definición. Sean G un grupo y $H \leq G$. El subgrupo H se llama *subgrupo normal* si se tiene que

$$xHx^{-1} = H, \quad \forall x \in G.$$

Para este caso particular utilizaremos la siguiente notación: $H \trianglelefteq G$.

Un grupo G se dice *simple* si sus únicos subgrupos normales son G y $\{1\}$.

Ejemplo 1.46. Sean G y G' dos grupos y sea $f\colon G \longrightarrow G'$ un homomorfismo. Entonces

$$\ker(f) = \{g \in G \,|\, f(g) = 1_{G'}\} \trianglelefteq G.$$

En efecto, sean $h \in \ker(f)$ y $x \in G$:

$$f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x)1_{G'}f(x)^{-1} = 1_{G'},$$

y así $xhx^{-1} \in G$, y puesto que h es arbitrario, $x\ker(f)x^{-1} = \ker(f)$.

Recíprocamente, veremos que si H es un subgrupo normal de G, entonces H es el núcleo de algún homomorfismo de grupos $G \to G'$.

Observaciones. (1) Sean G un grupo y $H \trianglelefteq G$, entonces, dados $x, y \in G$ se tiene que

$$xH \cdot yH = xHy \cdot H = xyHH = xyH.$$

(2) $x \in G$ es un representante de la clase xH, pero también lo es xh, con $h \in H$, es decir

$$xhH = xH, \quad \forall h \in H.$$

Luego, dados $x, y \in G$ y $h, h' \in H$,

$$xhH \cdot yh'H = xH \cdot yH = xyH.$$

Lo cual nos permite definir en G/H la operación binaria

$$\begin{aligned} \cdot \colon G/H \times G/H &\to G/H \\ (\overline{x}, \overline{y}) &\mapsto \overline{xy}. \end{aligned}$$

Teorema 1.47. *Sean G un grupo y $H \trianglelefteq G$. Entonces $(G/H, \cdot)$ es un grupo.*

Demostración. Primero veamos que la identidad en este grupo está dada por $\overline{1} = 1H = H \in G/H$, pues

$$(xH) \cdot H = xH, \quad \forall x \in H.$$

Dado $xH \in x \in G$, su inverso está dado por $x^{-1}H$ pues

$$(xH)(x^{-1}H) = xx^{-1}H = H.$$

Finalmente para la asociatividad, tomamos $xH, yH, zH \in G/H$,

$$(xH \cdot yH) \cdot zH = (xyH) \cdot zH = (xy)zH = x(yz)H = (xH) \cdot (yzH) = xH \cdot (yH \cdot zH).$$

□

La relación entre G y G/H viene dada por el epimorfismo

$$\begin{aligned} \varphi : G &\to G/H \\ x &\mapsto \varphi(x) = xH, \end{aligned} \tag{1.1}$$

de la siguiente forma:

$$\ker(\varphi) = \{x \in G \,|\, xH = H\} = \{x \in G \,|\, x \in H\} = H.$$

Ejemplo 1.48. Sea $n \geq 1$ entero y consideremos S_n y C_n, el grupo simétrico y el grupo cíclico a n elementos, respectivamente. La función

$$\operatorname{sgn} : S_n \to C_2$$

es un homomorfismo, por tanto, obtenemos un sugrupo normal

$$\ker(\operatorname{sgn}) := A_n \trianglelefteq S_n$$

conocido como el *subgrupo alternante* de S_n. El subgrupo A_n está generado por las permutaciones pares ($A_n = \langle (i\ j)(k\ l) \,|\, i, j, k, l \in \mathbb{N} \setminus 0 \rangle$) y

$$S_n/A_n = \{A_n, (1\ 2)A_n\}.$$

Así $|S_n/A_n| = 2$ y $S_n/A_n \cong C_2$.

Ejemplo 1.49. Sean G un grupo y $g \in G$. Definimos la aplicación

$$\begin{aligned} I_g : G &\to G \\ x &\mapsto gxg^{-1}. \end{aligned}$$

Ejercicio 1.50. Probar que I_g es un automorfismo.

I_g se denomina el *automorfismo interior de G determinado por g*. Definamos ahora el homomorfismo

$$\begin{aligned} I : G &\to \mathrm{Aut}(G) \\ g &\mapsto I_g. \end{aligned}$$

Luego,

$$\begin{aligned} \ker(I) &= \{g \in G \,|\, I_g = \mathrm{id}_G\} \\ &= \{g \in G \,|\, gxg^{-1} = x,\ \forall x \in G\} \\ &= \{g \in G \,|\, xg = gx,\ \forall x \in G\}. \end{aligned}$$

Definición (El centro de G)**.** Sea G un grupo, el centro de G es el conjunto definido por

$$Z(G) = \{g \in G \,|\, gx = xg\ \forall x \in G\}.$$

Por lo anterior, se sigue que $\ker(I) = Z(G) \trianglelefteq G$.

Observaciones. (1) Si G es un grupo abeliano con la operación $+$, las clases laterales de un subgrupo H de G son de la forma

$$x + H,\ x \in G.$$

Dados $x + H, y + H \in G/H$, se tiene que

$$(x + H) + (y + H) = (x + y) + H, \quad -(x + H) = -x + H, \quad 0 = H.$$

(2) El epimorfismo natural $\varphi : G \twoheadrightarrow G/H$ dado por (1.1) produce la siguiente sucesión de grupos y homomorfismos

$$\{1\} \hookrightarrow H \hookrightarrow G \xrightarrow{\varphi} G/H \to \{H\},$$

denominada *sucesión exacta determinada por el epimorfismo φ.*

Teorema 1.51 (E. Noether)**.** *Sean G, G' dos grupos, $H \subset G$, φ dado por (1.1) y $\psi\colon G \to G'$ un homomorfismo tal que $H \leq \ker(\psi)$. Entonces existe un único homomorfismo $\overline{\psi}\colon G/H \to G'$ tal que el diagrama*

$$\begin{array}{ccc} G & \xrightarrow{\ \psi\ } & G' \\ \downarrow{\scriptstyle \varphi} & \nearrow{\scriptstyle \overline{\psi}} & \\ G/H & & \end{array}$$

conmuta, es decir que $\overline{\psi} \circ \varphi = \psi$ (y por tanto ψ se determina por $\overline{\psi}$ y φ). Además

$$\begin{aligned} \mathrm{Img}(\overline{\psi}) &= \mathrm{Img}(\psi) \\ \ker(\overline{\psi}) &= \{xH \,|\, x \in \ker(\psi)\} = \ker(\psi)/H \leq G/H. \end{aligned}$$

Demostración. Por hipótesis, $H \leq \ker(\psi)$. Si tomamos $x, y \in G$ tales que $xH = yH$, entonces dado $xh \in xH$, existe $h' \in H$ tal que $xh = yh'$. Así, $y^{-1}x = h^{-1}h' \in H \leq \ker(\psi)$ y

$$\psi(y^{-1}x) = \psi(y)^{-1}\psi(x) = 1_{G'}.$$

Es decir que $\psi(x) = \psi(y)$. Esto nos asegura que la función

$$\begin{aligned} \overline{\psi}\colon G/H &\to G' \\ xH &\mapsto \overline{\psi}(xH) = \psi(x) \end{aligned}$$

está bien definida.

Ejercicio 1.52. Comprobar que $\overline{\psi}$ es un homomorfismo.

Ejercicio 1.53. Probar la unicidad.

Por otro lado,

$$\mathrm{Img}(\overline{\psi}) = \{\overline{\psi}(xH) : x \in G\} = \{\psi(x) : x \in G\} = \mathrm{Img}(\psi).$$

$$\ker(\overline{\psi}) = \{xH : \overline{\psi}(xH) = 1\} = \{xH : \psi(x) = 1\} = \ker(\psi)/H.$$

□

Observación. Sean G un grupo, $H \trianglelefteq G$ y $K \leq G$ tal que $H \leq K$, entonces tenemos que H también es un subgrupo normal de G, pues como

$$xHx^{-1} = H, \quad \forall x \in G,$$

entonces en particular para todos los $x \in K$

$$xHx^{-1} = H, \quad \forall x \in K.$$

Por tanto el grupo cociente K/H está bien definido.

Teorema 1.54 (Teorema de correspondencia de subgrupos)**.** *Sean G un grupo, $H \trianglelefteq G$ y G/H el grupo cociente. Los subgrupos de G/H son todos los grupos cociente*

$$K/H,$$

con $K \leq G$ tal que $H \leq K$. Además

$$K/H \trianglelefteq G/H \iff K \trianglelefteq G.$$

Demostración. Sea $K \leq G$ tal que $H \leq K$, entonces $K/H = \{xH \,|\, x \in K\} \subseteq G/H$ es un subgrupo de G/H. En efecto, si tomamos $x, y \in K$, dado que K es un subgrupo de G, entonces $xy^{-1} \in K$, lo que implica que

$$xy^{-1}H = (xH)(yH)^{-1} \in K/H.$$

Ahora tomamos un $\overline{K}$ un subgrupo de G/H cualquiera. Definamos

$$K = \{x \in G \,|\, xH \in \overline{K}\},$$

el cual es un subgrupo de G. Es claro que $H \leq K$.

Ejercicio 1.55. Mostrar que $\overline{K} = K/H$.

Para probar que $K/H \trianglelefteq G/H$, basta ver que para todo $x \in H$ y todo $y \in K$ se tiene que

$$xHyHx^{-1}H = xyx^{-1}H.$$

□

Teorema 1.56. *Sean G, G' dos grupos, $H \leq G$ y sea $f : G \twoheadrightarrow G'$ un epimorfismo, con $H = \ker(f) \trianglelefteq G$. Entonces existe una biyección entre el conjunto de los subgrupos $L \leq G'$, y el conjunto de los subgrupos $K \leq G$ tales que $H \leq K$.*

Demostración. Consideremos la función

$$\begin{aligned} F\colon \{L \leq G'\} &\to \{K \leq G \mid H \leq K\} \\ L &\mapsto F(L) = f^{-1}(L) = \{x \in G \mid f(x) \in L\}. \end{aligned}$$

Primero probamos que F está bien definido. Sea $L \leq G'$ y $x, y \in f^{-1}(L)$. Tenemos que $f(xy^{-1}) = f(x)f(y)^{-1} \in L$, es decir que $xy^{-1} \in f^{-1}(L)$, y por tanto $f^{-1}(L)$ es un subgrupo de G. Además $H = \ker(f) = f^{-1}(\{1\}) \subseteq f^{-1}(L)$. La inyectividad se tiene gracias a que f es sobreyectiva, pues así

$$L = f\left(f^{-1}(L)\right) = f\left(f^{-1}(M)\right) = M,$$

para L, M, cualquier par de subgrupos de G.

Para la sobreyectividad, tomamos $K \leq G$ tal que $H \leq K$ y consideramos el subgrupo $L = f(K) \leq G'$. Debemos probar que $f^{-1}(f(K)) = K$. La contenencia $K \subseteq f^{-1}(f(K))$ siempre se tiene. Para la otra, sea $x \in f^{-1}(f(K))$. Luego, $f(x) \in f(K)$ y existe $y \in K$ tal que $f(x) = f(y)$. Así $f(xy^{-1}) = 1$, lo cual significa que xy^{-1} esté en H. Pero $H \subseteq K$, entonces tenemos finalmente

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

□

1.3. Teoremas de Isomorfía

Teorema 1.57 (Primer Teorema de Isomorfía)**.** *Sea $f\colon G \to G'$ un homomorfismo de grupos. Entonces se tiene un único isomorfimo*

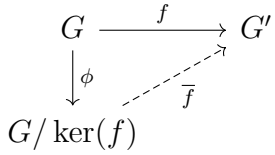
$$\bar{f}\colon G/\ker(f) \xrightarrow{\sim} \mathrm{Img}(f),$$

tal que el diagrama

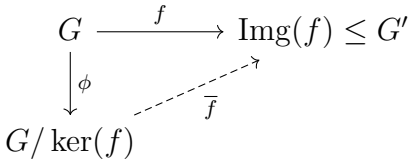
$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & \mathrm{Img}(f) \leq G' \\ \downarrow{\scriptstyle \phi} & \nearrow_{\bar{f}} & \\ G/\ker(f) & & \end{array}$$

conmuta

Demostración. Gracias al Teorema de Noether sabemos que existe un único homomorfismo $\bar{f}\colon G/\ker(f) \to G'$ tal que el diagrama



conmuta. Es decir, $f = \bar{f} \circ \phi$, por lo que podemos decir que el diagrama



conmuta.

Por tanto, basta probar que $\bar{f}$ es tanto un monomorfimo como un epimorfismo. Para la inyectividad probemos que $\ker(\bar{f}) = \{\ker(f)\}$. Así, sea $x\ker(f) \in \ker(\bar{f})$ y mostremos que $x \in \ker(f)$. Como $f = \bar{f} \circ \phi$ tenemos que

$$f(x) = \bar{f}(\phi(x)) = \bar{f}(x\ker(f)) = 1'.$$

De esta manera, $x \in \ker(f)$ y por tanto $x\ker(f) = \ker(f)$, con lo que concluimos que $\bar{f}$ es un monomorfismo.

Para la sobreyectividad, tomemos $y \in \mathrm{Img}(f)$. Entonces, existe $x \in G$ tal que $f(x) = y$. Como el diagrama conmuta sabemos que

$$\bar{f}(x\ker(f)) = \bar{f}(\phi(x)) = f(x) = y,$$

y como $x\ker(f) \in G/\ker(f)$, deducimos que $\bar{f}$ es un epimorfismo. Por tanto $\bar{f}$ es un isomorfismo y se sigue el resultado. □

Ejemplo 1.58. Consideremos $\mathbb{Z} \subseteq (\mathbb{R}, +)$, consideremos

$$\begin{array}{rcl} \exp\colon \mathbb{R} & \longrightarrow & S^1 = \{z \in \mathbb{C} \,|\, |z| = 1\} \\ x & \longmapsto & \exp(x) = e^{2\pi i x} = \cos(2\pi x) + i\sin(2\pi x). \end{array}$$

Se tiene que exp es un epimorfismo pues

$$\exp(x+y) = e^{2\pi i(x+y)} = e^{2\pi i x}e^{2\pi i y} = \exp(x)\exp(y).$$

Además

$$\ker(\exp) = \{x \in \mathbb{R} \,|\, \cos(2\pi x) + i\sin(2\pi x) = 1\} = \mathbb{Z}.$$

Y así, por el Primer Teorema de Isomorfía deducimos que

$$\mathbb{R}/\mathbb{Z} \xrightarrow{\sim} S^1,$$

y $\exp(x + \mathbb{Z}) = e^{2\pi i x}$

Ejemplo 1.59. Sabemos que $S_n \xrightarrow{\text{sign}} \{1, -1\}$. Además

$$A_n = \ker(\text{sign}) = \{\sigma \in S_n \,|\, \text{sign}(\sigma) = 1\} \trianglelefteq S_n,$$

y así $\text{sign}\colon S_n/A_n \xrightarrow{\sim} \{1, -1\}$.

Lema 1.60. *Sean $S, T \leq G$ y supongamos que al menos uno de estsos subgrupos es normal. entonces*

$$ST = TS = \langle S, T \rangle.$$

En particular, $ST \leq G$. Si $S \trianglelefteq G$ y $T \trianglelefteq G$, entonces

$$ST \trianglelefteq G.$$

Demostración. Supongamos sin pérdida de generalidad que $T \trianglelefteq G$, entonces

$$ST = \bigcup_{s \in S} sT = \bigcup_{s \in S} Ts = TS.$$

Además, como T es normal se tiene que

$$ST \cdot ST = STST = SSTT = ST \quad \text{y} \quad (ST)^{-1} = ST.$$

Por lo que concluimos que $ST \leq G$.

Ahora, si $S, T \trianglelefteq G$ tomemos $s \in S$, $t \in T$ y $g \in ST$. Así, tenemos que

$$gstg^{-1} = gsg^{-1}gtg^{-1} = s't',$$

donde $s' \in S$ y $t' \in T$. Por tanto $gSTg^{-1} = ST$, lo que nos permite concluir que $ST \trianglelefteq G$. □

Ejercicio 1.61. Si G es un grupo y $H \subseteq G$, probar que

$$H \leq G \iff \left\{ \begin{array}{l} HH \subseteq H \\ H^{-1} \subseteq H \end{array} \right\}.$$

Observaciones.

(1) En el mismo pensamiento que el lema anterior, notemos que si $S, T \leq G$ y $T \trianglelefteq S$, entonces $S \cap T \trianglelefteq S$. En efecto, sean $x \in S$ y $y \in S \cap T$, debemos probar que $xyx^{-1} \in S \cap T$. Para ello, como $y \in S$ se sigue que $xyx^{-1} \in S$, y como T es normal también tenemos que $xyx^{-1} \in T$. Por tanto, $xyx^{-1} \in S \cap T$ y concluimos que $S \cap T \trianglelefteq S$.

(2) Usando un razonamiento análogo es posible probar que si $S \leq G$ y $T \trianglelefteq G$, entonces $T \trianglelefteq ST$.

Teorema 1.62 (Segundo Teorema de Isomorfía)**.** *Sean $S, T \leq G$ y $T \trianglelefteq G$. Entonces se tiene un isomorfismo*

$$\begin{array}{rcl} S/S \cap T & \xrightarrow{\simeq} & ST/T \\ x \cdot S \cap T & \longmapsto & xT \end{array}$$

Demostración. Por el Lema 1.60 sabemos que $ST = TS \leq G$, $S \cap T \trianglelefteq S$ y $T \trianglelefteq ST$. Sea

$$\begin{array}{rcl} \phi \colon G & \twoheadrightarrow & G/T \\ g & \longmapsto & gT. \end{array}$$

Restringiendo ϕ al subgrupo S obtenemos

$$\begin{array}{rcl} \phi_{|S} \colon S & \twoheadrightarrow & ST/T \\ x & \longmapsto & xT. \end{array}$$

En efecto, dado $yT \in ST/T$, sabemos que existe $st \in ST$ tal que $y = st$ y así $yT = stT = sT$. Por tanto, es claro que $\phi_{|S}(s) = sT = yT$, con lo que concluimos que $\mathrm{Img}(\phi_{|S}) = ST/T$

Ahora, observemos que

$$\ker(\phi_{|S}) = \{s \in S \mid sT = T\} = \{s \in S \mid s \in T\} = S \cap T.$$

Luego, por el Primer Teorema de Isomorfía, $\phi_{|S}$ induce un isomorfimos $\bar{\phi_{|S}} \colon S/\ker(\phi_{|S}) \xrightarrow{\sim} ST/T$, con

$$\begin{array}{rccc} \bar{\phi_{|S}} \colon & S/S\cap T & \xrightarrow{\sim} & ST/T \\ & s \cdot S \cap T & \longmapsto & sT \end{array}$$

□

Ejercicio 1.63. Demostrar que la aplicación

$$\begin{array}{ccc} S/S\cap T & \xrightarrow{\sim} & ST/T \\ s \cdot S \cap T & \longmapsto & sT \end{array}$$

está bien definida y es un isomorfismo, sin usar el Primer Teorema de Isomorfía.

Corolario 1.64. *Si G es un grupo finito, $S, T \leq G$ y al menos uno es normal, entonces*

$$|S||T| = |S \cap T||\langle S, T\rangle|,$$
$$|S||T| = |S \cap T||ST|.$$

Demostración. Sin pérdida de generalidad supongamos que $T \trianglelefteq G$. Por el Segundo Teorema de Isomorfía $S/S \cap T \cong ST/T$, de donde, como $S \cap T \trianglelefteq S$ y $T \trianglelefteq ST$

$$\begin{aligned} |S/S \cap T| = |ST/T| \Rightarrow \frac{|S|}{|S \cap T|} &= \frac{|ST|}{|T|} \\ \Rightarrow |S||T| = |S \cap T||ST| &= |S \cap T||\langle S, T\rangle|, \end{aligned}$$

lo que termina la demostración. □

Ejercicio 1.65. Si $S, T \leq G$, probar que

(1) $|S||T| = |S \cap T||ST|$.

(2) $|ST| \leq |S \cap T||\langle S, T\rangle|$.

(3) Dar un ejemplo que muestre que la desigualdad en (2) puede ser estricta.

Teorema 1.66 (Tercer Teorema de Isomorfía)**.** *Sean $H \leq K \leq G$ subgrupos de G tales que $H, K \trianglelefteq G$. Entonces $K/H \trianglelefteq G/H$ y además*

$$(G/H)/(K/H) \cong G/K.$$

Demostración. Como $H \leq K$ se tiene un homomorfismo

$$\begin{array}{rccc} \psi \colon & G/H & \twoheadrightarrow & G/K \\ & xH & \longmapsto & xK. \end{array}$$

Observemos que

$$\ker(\psi) = \{xH \,|\, xK = K\} = \{xH \,|\, x \in K\} = K/H.$$

Y así, aplicando el Primer Teorema de Isomorfía se concluye que

$$\begin{array}{rcl} (G/H)(K/H) & \xrightarrow{\sim} & G/K \\ (xH)K/H & \longmapsto & xK. \end{array}$$

□

Ejemplos 1.67.

(1) Sea $n \geq 1$, $\mathbb{R}^n$ el grupo aditivo y $\mathbb{Z}^n \trianglelefteq \mathbb{R}^n$. Definamos $T^n = S^1 \times \cdots, \times S^1$ y

$$\begin{array}{rccl} \phi\colon & \mathbb{R}^n & \longrightarrow & T^n \\ & (x_1, \ldots, x_n) & \longmapsto & (e^{2\pi i x_1}, \ldots, e^{e\pi i x_n}). \end{array}$$

Así, ϕ es un homorfismo de grupos epiyectivo y $\ker(\phi) = \mathbb{Z}^n$. Por tanto, por el Primer Teorema de Isomorfía se tiene que

$$\mathbb{R}^n/\mathbb{Z}^n \xrightarrow{\sim} T^n.$$

Además, este isomorfismo es topológico, es decir, es un isomorfismo de grupos y a la vez un homeomorfismo de espacios topológicos, cuando equipamos a $\mathbb{R}^n/\mathbb{Z}^n$ con la topología cociente.

(2) Sean $n \geq 2$ y $O(n) \leq \mathrm{GL}(n, \mathbb{R})$ el grupo ortogonal de grado n. Sabemos que

$$\begin{aligned} O(n) &= \{A \in \mathrm{GL}(n\mathbb{R}) \,|\, A^\top A = I\} \\ &= \{A \,|\, Ax \cdot Ay = x \cdot y, \, \forall\, x, y \in \mathbb{R}^n\} \\ &= \{A \in \mathrm{GL}(n, \mathbb{R}) \,|\, \|Ax\| \leq \|x\|, \, \forall\, x \in \mathbb{R}^N\}. \end{aligned}$$

Además, para todo $A \in O(n)$ se tiene que $\det(A) \in \{1, -1\}$; es decir, $\det\colon O(n) \twoheadrightarrow \{1, -1\}$, pues las reflexiones tienen determinante -1. Por ejemplo, si S es la reflexión con respecto a $e \in \mathbb{R}^n \setminus \{0\}$, entonces

$$S(x) = x - 2\frac{x \cdot e}{e \cdot e}e.$$

Así, $\ker(\det) = SO(n)$ (este es el *grupo ortogonal especial de grado* n), lo que nos permite concluir que

$$O(n)/SO(n) \xrightarrow{\sim} \{1, -1\}.$$

Ejercicio 1.68. Sea G un grupo y S un sistema de generadores de G. Entonces, dado $H \leq G$, demostrar que

$$H \trianglelefteq G \iff \sigma H \sigma^{-1} = H \quad \forall\, \sigma \in S.$$

Ejercicio 1.69. Demostrar que $S_n = \langle (1\ 2), (1\ 2\ \cdots\ n) \rangle$.

Ejemplo 1.70. Consideremos S_3, $S_3 \leq S_4$. Definimos

$$V_4 = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Así, $V_4 \trianglelefteq S_4$. Más aún $V_4 \trianglelefteq A_4$ ($\trianglelefteq S_4$) y así

$$|A_4/V_4| = \frac{12}{4} = 3.$$

Por lo tanto $A_4/V_4 \cong C_3$

Ejercicio 1.71. Sea p un número primo. Demostrar que todo grupo G, tal que $|G| = p$, es cíclico.