# Lectura 8: Definición y ejemplos de grupos

## 8.1. Definiciones

Hasta ahora, hemos explorado la estructura de grupo en varias ocasiones pero sólo de manera incidental, sin embargo nos vemos en la necesidad de presentarla de manera explícita. En esta sección desarrollaremos los conceptos necesarios para clasificar como grupos algunas estructuras que hemos estado desarrollando a lo largo del curso.

**Definición 8.1.** Sea $G$ un conjunto cualquiera y sea $*$ una operación binaria sobre $G$. La pareja $(G, *)$ se dice *un grupo* si satisface:

1. Para cualesquiera $x$, $y$ y $z$ en el conjunto $G$, se cumple
$$(x * y) * z = x * (y * z).$$
2. Existe un único elemento $e$ de $g$, denominado *la identidad de* $G$, tal que para todo $x$ en $G$,
$$e * x = x * e = x.$$
3. Para cada elemento $x$ de $G$, existe un único elemento $x^{-1}$ en $G$, denominado *inverso de* $x$, de forma que
$$x * x^{-1} = x^{-1} * x = e.$$

Si además, un grupo satisface para todo $x$ y $y$ en $G$

$$x * y = y * x$$

decimos que el grupo es *abeliano*, una denominación alternativa, y más natural, es *conmutativo*. Por último, si el conjunto $G$ tiene $n$ elementos, diremos que *el grupo* $G$ *tiene orden* $n$.

Usando esta definición, amalgamamos los ejemplos que hemos discutido hasta ahora:

- El conjunto de los enteros $\mathbb{Z}$ con la suma entre enteros como la operación, forma un grupo tomando 0 como la identidad del grupo y $-m$ como el inverso de un entero $m$. De la misma forma lo hacen $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.
- El conjunto $\mathbb{Q}^\times$ de los todos los racionales distintos de cero, junto al producto racional como operación, forma un grupo tomando 1 como la identidad y $1/r$ como el inverso de un racional $r$. De manera similar lo hacen $\mathbb{R}^\times$ y $\mathbb{C}^\times$.
- El conjunto $\mathbb{Z}^\times$, sin embargo, no forma un grupo, pues ninguno de sus elementos, salvo 1 y -1, tiene inverso multiplicativo.

- Para un anillo $R$, el conjunto base junto a la operación $+$ del anillo, forman un grupo tomando $0_R$ como identidad y los inversos de la suma en el anillo como los inversos; a este grupo se le denomina *el grupo aditivo de* $R$. Sin embargo, $R$ junto al producto no necesariamente forma un grupo, pero si forma un grupo abeliano, entonces $R$ resulta un campo.
- El conjunto $S^1 \subset \mathbb{C}$ definido
$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$
junto al producto complejo como operación, forma un grupo tomando 1 como la identidad y notando que los conjugados funcionan como los inversos.
- Dado un anillo conmutativo $R$, el conjunto de unidades, $R^*$, junto al producto del anillo como su operación, forman un grupo con $1_R$ como su identidad. En particular, el conjunto de las unidades de $\mathbb{Z}_m^*$ forma un grupo bajo la multiplicación.
- Para cualquier entero positivo $m$, el conjunto $\Gamma_m$ de las raíces $m$-ésimas de la unidad junto al producto complejo, forman un grupo.
- Dado un conjunto $E$, el conjunto potencia $\mathcal{P}(E)$ junto a la diferencia simétrica, definida como
$$A + B = (A \backslash B) \cup (A \backslash B),$$
forma un grupo abeliano tomando $\varnothing$ como la identidad y el mismo conjunto $A$ como su inverso.

En el caso del grupo $(\mathbb{Z}, +)$ es interesante observar que la notación derivada de la definición como grupo, vuelve la representación de los inversos un tanto extraña al resultar $m^{-1} = -m$. Esto por supuesto es indeseable por lo que se realizará la siguiente convención: Un grupo $G$ en el cual su operación asociada está representada por el símbolo $+$ se dirá en *notación aditiva*, su elemento neutro se escribirá $0_G$ mientras que sus inversos se escribirán $-g$. En otras palabras, los axiomas de grupo para la identidad e inversos toman la siguiente forma.

1. Para todo $x$ en el grupo $G$,
$$x + 0_G = 0_G + x = x.$$
2. Para todo $x$ en el grupo $G$, existe $-x$ en el grupo de forma que
$$x + (-x) = (-x) + x = 0_G.$$

Además, se conviene que un grupo en notación aditiva es siempre abeliano. Esto a razón, que nuestra idea más natural de suma es siempre conmutativa. Esta convención no obliga a que todo grupo abeliano sea escrito en notación aditiva; de hecho, en todos los ejemplos anteriores las operaciones asociadas son todas conmutativas y no todos están escritos en notación aditiva. Es importante señalar sin embargo y a pesar de los ejemplos, hay grupos que no son conmutativos.

Una de las ventajas de trabajar en abstracto, es dar respuesta a preguntas en un complejo bloque de estructuras. Como ejemplo de esto, se pueden probar las leyes de cancelación en la operación de grupo, por lo que se puede asumir el resultado en todos los ejemplos anteriores y posteriores. Lo anterior sucede sin necesidad de tomar en cuenta las particularidades de cada caso. Veamos algunos ejemplos más de estos resultados.

**Proposición 8.1.** *En grupo un G cualquiera, son válidas las leyes de cancelación, i.e., para cualesquiera a, b y c elementos del grupo, si se tiene $a * b = a * c$ o en su defecto $b * a = c * a$, entonces $b = c$.*

*Demostración.* En sencillo que por los axiomas de grupo, existe el elemento $a^{-1}$ en el grupo. Por esto, si $a * b = a * c$, entonces

$$\begin{aligned} b &= e * b \\ &= (a^{-1} * a) * b \\ &= a^{-1} * (a * b) \\ &= a^{-1} * (a * c) \\ &= (a^{-1} * a) * c \\ &= e * c \\ &= c. \end{aligned}$$

Bajo la otra hipótesis, el resultado se demuestra por analogía. ■

La proposición anterior tiene el propósito de ilustrar lo explícito que puede resultar el usar los axiomas de grupo, aunque en general no es necesaria tanta precisión, ante cualquier duda lo mejor será proveer un argumento tan explícito como el anterior.

**Proposición 8.2.** *Para cualesquiera elementos a y b de un grupo G, se tiene*

1. $(a^{-1})^{-1} = a$.
2. $(a * b)^{-1} = b^{-1} * a^{-1}$.

*Demostración.* El resultado sigue de manera muy natural de la unicidad del inverso. Debemos notar de la definición de grupo que

$$a^{-1} * \left(a^{-1}\right)^{-1} = e = a^{-1} * a,$$

y considerando que obtenemos la misma igualdad si invertimos lo papeles de $a$ y su inverso, debemos concluir que $(a^{-1})^{-1} = a$. De manera similar,

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * a^{-1} = e,$$

implica que lo expuesto en 2, comprobando el resultado. ■

Como se puede ver en la anterior proposición es relativamente incómodo escribir la operación del grupo cuando hay mas dos elementos involucrados. Por eso convendremos que $ab = a * b$ para simplificar nuestra discusión cuando esto no implique potenciales ambigüedades y cuando el grupo no esté escrito en notación aditiva.

**Definición 8.2.** Sea $a$ un elemento cualquiera de un grupo $G$. Definimos $a^0 = e$ y para un entero positivo $n$,

$$a^n = \underbrace{a * \cdots * a}_{n \text{ veces}}.$$

Además,

$$a^{-n} = \left(a^{-1}\right)^n.$$

Para un grupo en notación aditiva, los exponentes toman una notación completamente distinta: Para un entero no negativo $n$,

$$na = \underbrace{a + \cdots + a}_{n \text{ veces}}$$

y

$$(-n)a = n(-a).$$

Uno puede establecer una analogía directa con el caso de anillos, donde se definían de manera análoga usando la suma asociada al anillo. Sin embargo, cualquier resultado que se obtenga con exponentes se puede formular en notación aditiva sin mucho trabajo.

**Proposición 8.3.** *Sea $G$ un grupo y sean $a$ y $b$ elementos de éste. Para enteros $m$ y $n$ se cumple:*

1. *Si $ab = ba$, entonces $(ab)^n = a^n b^n$.*
2. *$(a^n)^m = a^{mn}$.*
3. *$a^m a^n = a^{m+n}$.*

*Demostración.* Se probará sólo 1), los otros incisos resultan idénticos a los probados en los naturales, enteros, reales, etc. y se dejan como ejercicio (8.3). Para probar 1) usaremos inducción para probar un resultado parcial. Primero, asumimos que $a$ y $b$ conmutan, en ese caso $(ab)^0 = e = a^0 b^0$; supongamos ahora $(ab)^n = a^n b^n$, entonces

$$\begin{aligned}(ab)^{n+1} &= (ab)^n (ab) \\ &= a^n b^n ab \\ &= (a^n a)(b^n b) \\ &= a^{n+1} b^{n+1}.\end{aligned}$$

Por inducción, se satisface para todo entero no negativo $n$, que $(ab)^n = a^n b^n$.

Para probar el resultado en los enteros negativos, debemos convencernos que $a^{-1}$ y $b^{-1}$ conmutan también (ejercicio 8.4) y suponiendo que $n$ es un entero positivo, la conclusión del párrafo anterior resulta en

$$\begin{aligned}(ab)^{-n} &= \left((ab)^{-1}\right)^n \\ &= \left(a^{-1}b^{-1}\right)^n \\ &= \left(a^{-1}\right)^n \left(b^{-1}\right)^n \\ &= a^{-n} b^{-n}.\end{aligned}$$

El resultado entonces sigue indistintamente para enteros positivos y negativos como afirma el resultado. ∎

Como se comentó con anterioridad, los grupos no son necesariamente conmutativos, lo que nos obliga a responder si existen grupos no abelianos. Desarrollaremos ahora un par de ejemplos estrechamente vinculados a la geometría que resultarán en nuestros ejemplos de grupos no abelianos.

## 8.2. Las permutaciones como un grupo

Hasta ahora, se han discutido de manera superficial algunos ejemplos que resultaron todos conmutativos. Sin embargo, históricamente el concepto de grupo aparece en la discusión de conjuntos de funciones. Presentaremos en esta sección un importante ejemplo considerando como piedra angular la composición de funciones denotada siempre por el símbolo $\circ$.

**Definición 8.3.** Sea $A$ un conjunto cualquiera. Por *una permutación* entenderemos una función biyectiva $\alpha\colon A \to A$. Al conjunto de las permutaciones sobre el conjunto $A$ lo denotaremos por $S_A$ y si $A = \{1, 2, \ldots, n\}$, escribiremos $S_n$.

Recordemos primero que la función identidad $\mathbb{1}_A\colon A \to A$ es una biyección. Además, para toda función biyectiva $\alpha\colon A \to A$, existe una función $\beta$ de forma que

$$\alpha \circ \beta = \beta \circ \alpha = \mathbb{1}_A;$$

a la función $\beta$ se le denota generalmente por $\alpha^{-1}$, esto junto a la asociatividad de la composición de funciones, nos permite afirmar el conjunto de permutaciones de un conjunto forma un grupo tomando $\mathbb{1}_A$ como la identidad del grupo y las funciones inversas como los inversos.

**Teorema 8.4.** *Para un conjunto cualquiera $A$, la pareja $(S_A, \circ)$ es un grupo.*

Es bien conocido el hecho que para un conjunto con $n$ elementos, existen exactamente $n!$ permutaciones de éste. Es además común interpretar las permutaciones como listas, por ejemplo si $A = \{1, \ldots, n\}$, una permutación $\alpha\colon A \to A$ genera una lista de los elementos de $A$ indicada como $i_1 = \alpha(1), \ldots, i_{n-1} = \alpha(n-1)$ y $i_n = \alpha(n)$. En esta lista aparecen todos los elementos de $A$ y ninguno está repetido por eso, se acostumbra escribir una permutación en *notación de dos filas*:

$$\alpha = \begin{pmatrix} 1 & \ldots & j & \ldots & n \\ \alpha(1) & \ldots & \alpha(j) & \ldots & \alpha(n) \end{pmatrix}.$$

Una ventaja de esta notación, es que la composición de permutaciones se puede realizar de modo visual, eliminando un poco el nivel de abstracción con el que comúnmente se discuten éstas.

**Definición 8.4.** El grupo $S_n$ es llamado *el grupo simétrico sobre n elementos*.

Es importante notar que la composición no es conmutativa, lo cual es fácil de probar usando la notación de dos filas: Sean

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{y} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

en ese caso

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

pero

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

lo que nos permite concluir que $\alpha \circ \beta \neq \beta \circ \alpha$ y con esto que el grupo simétrico sobre $n$ elementos resulta no conmutativo. Hemos entonces construido un ejemplo profundamente interesante de lo que constituye un grupo que resulta no es conmutativo. Este grupo presenta un sin fin de resultados, entre ellos el famoso teorema de Caley, que afirma que cualquier grupo es esencialmente un grupo de permutaciones mostrando que la falta de conmutatividad no representa una falta de propiedades sino todo lo contrario.

## 8.3. Los grupos euclideano y ortogonal

Un segundo ejemplo de grupo, también tiene como elementos a ciertas funciones y proviene de la geometría analítica. En ella, se definen un grupo especial de transformaciones en el plano que generan determinados invariantes: Las isometrías o transformaciones rígidas. Antes de comenzar es importante recapitular algunos conceptos que vamos a requerir en esta sección.

**Definición 8.5.** Para un punto $a = (a_1, a_2)$ de $\mathbb{R}^2$, se define *la norma de a* como

$$\|a\| = \sqrt{a_1^2 + a_2^2}.$$

En consecuencia, se define *la distancia entre los puntos* $a = (a_1, a_2)$ *y* $b = (b_1, b_2)$ como

$$\|a - b\|.$$

Los conceptos de norma y distancia juegan un rol importante en geometría lo mismo que el concepto de producto interno, los cuales están estrechamente vinculados.

**Definición 8.6.** Para los puntos $a = (a_1, a_2)$ y $b = (b_1, b_2)$ de $\mathbb{R}^2$ se define *el producto interno entre a y b*, como

$$\langle a, b\rangle = a_1 b_1 + a_2 b_2.$$

Estas dos operaciones pueden convertir un par de parejas ordenadas en un número real. La norma por un lado asocia la distancia del origen la punto a través del teorema de Pitágoras. El producto interno enmascara el ángulo entre los vectores asociados a los puntos que involucra, por ejemplo, si $\theta$ es el ángulo entre los puntos $a$ y $b$ del plano, entonces

$$\langle a, b\rangle = \|a\|\|b\| \cos\theta.$$

Además existe otra relación aparte de la identidad expuesta entre el producto interno y la norma. A decir $\langle a, a\rangle = \|a\|^2$. Estas identidades inspiran la siguiente definición.

**Definición 8.7.** Los puntos $a = (a_1, a_2)$ y $b = (b_1, b_2)$ en $\mathbb{R}^2$ se dicen *ortogonales entre sí* si

$$\langle a, b\rangle = 0.$$

Si además $\|a\| = 1$ y $\|b\| = 1$, diremos que son *ortonormales entre sí*.

Los vectores ortogonales constituyen un conjunto denominado *base* por el cual todo punto de $\mathbb{R}^2$ se puede expresar como una combinación lineal de cualquier conjunto ortogonal. Si los vectores además están normalizados está expresión toma una forma aún más sencilla. El siguiente teorema expone este resultado.

**Teorema 8.5.** *Sean a y b elementos de* $\mathbb{R}^2$ *ortonormales entre sí. Entonces, para cada c de* $\mathbb{R}^2$,

$$c = \langle c, a\rangle\, a + \langle c, a\rangle\, b.$$

*Demostración.* A falta de herramientas y por reducir los conceptos asociados, la prueba resulta larga y tediosa aunque completamente operativa. Comencemos tomando $a = (a_1, a_2)$ y $b = (b_1, b_2)$, en ese caso, como $a$ y $b$ son ortonormales entonces $\langle a, b\rangle = 0$, lo que implica que

$$a_1 b_1 + a_2 b_2 = 0. \tag{1}$$

Además, debemos tener $\|a\| = \|b\| = 1$ lo que se traduce en tener

$$a_1^2 + a_2^2 = 1 \tag{2}$$

y

$$b_1^2 + b_2^2 = 1 \tag{3}$$

Otra conclusión que podemos derivar es $a \neq (0,0)$ lo cual permite afirmar que $a_1 \neq 0$ o $a_2 \neq 0$. Si por un lado $a_1 \neq 0$, (1) implica

$$b_1 = -\frac{a_2 b_2}{a_1}$$

y sustituyendo en (3) obtenemos

$$1 = \frac{a_2^2 b_2^2}{a_1^2} + b_2^2 = \frac{b_2^2}{a_1^2},$$

de lo que sigue $b_2^2 = a_1^2$. De manera análoga, si $a_2 \neq 0$, entonces $b_1^2 = a_2^2$. En cualquier caso, por (2) y (3) obtenemos

$$a_1^2 + b_1^2 = a_2^2 + b_2^2 = 1. \tag{4}$$

Retomemos ahora nuestros casos originales: $a_1 \neq 0$ o $a_2 \neq 0$. Si asumimos $a_1 \neq 0$, en el párrafo anterior se mostró que $b_2^2 = a_1^2$ lo cual indica que tenemos las siguientes posibilidades $b_1 = a_1$ o $b_1 = -a_1$. Si $b_1 = a_1$ por (1) obtenemos $a_1(b_1 + a_2) = 0$ y como $a_1 \neq 0$ debemos tener $b_1 = -a_2$; además, también por (1), $b_2 = a_1$ por lo que $b = (-a_2, a_1)$. Por otro lado, si $b_1 = -a_1$, (1) implica $a_1(b_1 - a_2) = 0$, por tanto $b_1 = a_2$ y también $b_2 = -a_1$ por lo que $b = (a_2, -a_1)$. En conclusión si $a_1 \neq 0$ entonces $b = (-a_2, a_1)$ o $b = (a_2, -a_1)$, lo cual resulta igualmente cierto si $a_2 \neq 0$ (demuéstralo). Para cualquiera de éstas posibilidades sobre el valor de $b$, se tiene

$$a_1 a_2 + b_1 b_2 = 0. \tag{5}$$

Por último, tomamos $c = (c_1, c_2)$ y $x = (x_1, x_2) = \langle c, a \rangle a + \langle c, b \rangle b$. Desarrollando explícitamente los componentes, obtenemos

$$x_1 = \left(a_1^2 c_1 + a_1 a_2 c_2\right) + \left(b_1^2 c_1 + b_1 b_2 c_2\right) = \left(a_1^2 + b_1^2\right) c_1 + (a_1 a_2 + b_1 b_2) c_2$$

y

$$x_2 = \left(a_1 a_2 c_1 + a_2^2 c_2\right) + \left(b_1 b_2 c_1 + b_2^2 c_2\right) = \left(a_2^2 + b_2^2\right) c_2 + (a_1 a_2 + b_1 b_2) c_1.$$

Por las igualdades (4) y (5), debemos tener que $x_1 = c_1$ y $x_2 = c_2$ por lo que $x = c$ o, en otras palabras,

$$c = \langle c, a \rangle a + \langle c, a \rangle b.$$

■

El teorema anterior afirma que $c$ se puede expresar como una combinación lineal de $a$ y $b$ siempre y cuando estos sean ortonormales. Este tipo de vectores tienen ciertas invariantes respecto a un tipo especial de funciones que introducimos a continuación.

**Definición 8.8.** *Una isometría en el plano* es una función $\varphi\colon \mathbb{R}^2 \to \mathbb{R}^2$ que preserva la distancia, i.e., para cualesquiera puntos $a$ y $b$ en $\mathbb{R}^2$, se tiene

$$\|\varphi(a) - \varphi(b)\| = \|a - b\|.$$

Si además $\varphi(0,0) = (0,0)$, se dice que $\varphi$ es *una isometría central*.

Esta denominación para estas funciones puede resultar extraña, sin embargo son funciones muy conocidas:

- Sea $0 \leq \theta < 2\pi$. *Una rotación de $\theta$ grados sobre el origen* es una función $R_\theta\colon \mathbb{R}^2 \to \mathbb{R}^2$ definida como sigue: $R_\theta(0,0) = (0,0)$ y si $a \neq (0,0)$, expresamos el punto $a$ en coordenadas polares $(r_a, \theta_a)$ y $R_\theta(a)$ será el punto $(r_a, \theta_a + \theta)$ expresado en coordenadas cartesianas. Bajo esta descripción, no es difícil probar que las rotaciones son isometrías centrales.
- Sea $L$ una recta en el plano que pasa por el origen. *Una relexión sobre $L$* es una función $\rho_L\colon \mathbb{R}^2 \to \mathbb{R}^2$ que opera la siguiente forma: Si $a \in L$, entonces $\rho_L(a) = a$, pero si $a \notin L$ se debe primero encontrar la única linea $L'$ de forma que $L \cap L' \neq \varnothing$ y $a \in L'$; $\rho_L(a)$ será el único punto sobre la linea $L'$ de forma que $\|\rho_L(a)\| = \|a\|$. Por definición, cualquier reflexión sobre una recta que pasa por el origen es una isometría central.
- Sea $u$ un punto cualquiera de $\mathbb{R}^2$. *Una traslación sobre $u$* es una función $\tau_u\colon \mathbb{R}^2 \to \mathbb{R}^2$ definida simplemente como $\tau_u(a) = u + a$. Cualquier traslación es una isometría.

**Proposición 8.6.** *Todas las isometrías son funciones inyectivas.*

*Demostración.* Sea $\varphi$ una isometría. Para mostrar que es un función inyectiva suponemos que $\varphi(a) = \varphi(b)$ y en ese caso

$$\|a - b\| = \|\varphi(a) - \varphi(b)\| = 0.$$

Por tanto $a - b = (0,0)$ o en otras palabras $a = b$ y en consecuencia $\varphi$ es inyectiva. ∎

Todas las isometrías se pueden descomponer en isometrías mucho más simples: traslaciones e isometrías centrales. El siguiente teorema nos habilita para enfocarnos en estos tipos de isometrías, las cuales, estudiándolas con algo de detalle, nos permitirán obtener los resultados que buscamos. Es importante nunca perder de vista que el contenido que desarrollaremos es profundamente geométrico y que la intuición jugará un rol importante en entender no sólo los resultados sino las pruebas también.

**Lema 8.7.** *Si $\tau_u$ es una traslación, entonces $\tau_{-u}$ es su inversa. En otras palabras, las traslaciones son biyectivas y sus inversas son también traslaciones.*

*Demostración.* Al ser $\tau_u$ una traslación, ésta es una isometría y en consecuencia inyectiva por lo que basta mostrar que $\tau_{-u}$ es su inversa por la derecha pues las inversas laterales deben coincidir. Esto es sencillo, pues

$$\tau_u\left(\tau_{-u}(a)\right) = \tau_u(a - u) = a - u + u = a,$$

por lo que $\tau_u \circ \tau_{-u}$ es la función identidad, mostrando con esto que la función es sobreyectiva y por tanto biyectiva y en consecuencia $\tau_{-u}$ debe ser la inversa de $\tau_u$. ∎

**Teorema 8.8.** *Sea $\varphi$ una isometría. Entonces, existen una traslación $\tau$ y una isometría central $\gamma$ tales que*

$$\varphi = \tau \circ \gamma.$$

*Demostración.* Definimos primero $u = \varphi(0,0)$; en en ese caso, la función $\gamma = \tau_{-u} \circ \varphi$ es una isometría central pues es una composición de isometrías y además

$$(\tau_{-u} \circ \varphi)(0,0) = \tau_{-u}\left(\varphi(0,0)\right) = \tau_{-u}(u) = (0,0).$$

Como $\tau_{-u}$ es la inversa de la traslación $\tau_u$, podemos tomar $\tau = \tau_u$ y obtener

$$\varphi = (\tau \circ \tau_{-u}) \circ \varphi = \tau \circ \gamma.$$

La igualdad anterior es la descomposición que afirma el teorema. ∎

Las traslaciones por un lado, son lo suficientemente simples para sentirnos cómodos con ellas por lo que volcaremos nuestra atención a las isometrías centrales

**Lema 8.9.** *Si $\varphi$ es una isometría central, entonces $\|\varphi(a)\| = \|a\|$ para todo $a$ en $\mathbb{R}^2$.*

*Demostración.* Basta notar que

$$\|\varphi(a)\| = \|\varphi(a) - (0,0)\| = \|\varphi(a) - \varphi(0,0)\| = \|a - (0,0)\| = \|a\|,$$

probando nuestra afirmación. ∎

**Teorema 8.10.** *Una función $\varphi\colon \mathbb{R}^2 \to \mathbb{R}^2$ es una isometría central si y sólo si preserva el producto interno, i.e., para cualesquiera $a$ y $b$ elementos de $\mathbb{R}^2$ se cumple.*

$$\langle \varphi(a), \varphi(b) \rangle = \langle a, b \rangle$$

*Demostración.* Supongamos primero que $\varphi$ preserva el producto interno. Mostraremos primero que es una isometría: Sean $a$ y $b$ elementos cualquiera de $\mathbb{R}^2$, entonces

$$\begin{aligned}
\|\varphi(a) - \varphi(b)\|^2 &= \langle \varphi(a) - \varphi(b), \varphi(a) - \varphi(b) \rangle \\
&= \langle \varphi(a), \varphi(a) \rangle + 2\langle \varphi(a), \varphi(b) \rangle + \langle \varphi(b), \varphi(b) \rangle \\
&= \langle a, a \rangle + 2\langle a, b \rangle + \langle b, b \rangle \\
&= \langle a - b, a - b \rangle \\
&= \|a - b\|^2,
\end{aligned}$$

lo que implica que $\varphi$ es una isometría. Además

$$\begin{aligned}
\|\varphi(0,0)\|^2 &= \langle \varphi(0,0), \varphi(0,0) \rangle \\
&= \langle (0,0), (0,0) \rangle \\
&= 0,
\end{aligned}$$

lo que implica que $\varphi(0,0) = (0,0)$ permitiéndonos concluir que $\varphi$ es una isometría central.

Asumamos ahora que $\varphi$ es una isometría central. Como en particular $\varphi$ es una isometría, tenemos para cualesquiera $a$ y $b$ elementos de $\mathbb{R}^2$,

$$\langle \varphi(a) - \varphi(b), \varphi(a) - \varphi(b) \rangle = \|\varphi(a) - \varphi(b)\|^2 = \|a - b\|^2 = \langle a - b, a - b \rangle ,$$

desarrollando los productos de ambos lados, la anterior igualdad implica

$$\|\varphi(a)\|^2 - 2\langle \varphi(a), \varphi(b) \rangle + \|\varphi(b)\|^2 = \|a\|^2 - 2\langle a, b \rangle + \|b\|^2.$$

Como además la isometría es central, el lema anterior obliga a $\|\varphi(a)\|^2 = \|a\|^2$ y $\|\varphi(b)\|^2 = \|b\|^2$ y se debe tener

$$\langle \varphi(a), \varphi(b) \rangle = \langle a, b \rangle ,$$

mostrando con esto que $\varphi$ preserva el producto interno como deseábamos. ■

**Corolario 8.11.** *Si $a$ y $b$ son ortonormales, entonces $\varphi(a)$ y $\varphi(b)$ son ortonormales. En otras palabras, $\varphi$ preserva vectores ortnormales entre sí.*

*Demostración.* Esto es una consecuencia inmediata del teorema 8.10 pues si $\langle a, b \rangle = 0$, entonces

$$\langle \varphi(a), \varphi(b) \rangle = \langle a, b \rangle = 0.$$

Si además $\|a\| = \|b\| = 1$, entonces por el lema 8.9 $\|\varphi(a)\| = \|\varphi(b)\| = 1$. Mostrando con esto que $\varphi(a)$ y $\varphi(b)$ son ortonormales. ■

Estamos ahora en posición de probar que las isometrías centrales son en realidad funciones invertibles, lo cual puede no parecer sorprendente si se piensa geométricamente. Lo único que hacen éstas es mover nuestro punto de referencia mientras mantienen las distancias invariantes, i.e., sin deformaciones, el resultado de éstas operaciones será simplemente el cambio de origen y, quizá, el orden de las coordenadas. Al final acabamos con una copia del plano sin un cambio significativo. Esta idea es la que se plasma en la prueba.

**Lema 8.12.** *Sea $\varphi$ una isometría central y sean $\pi_1$ y $\pi_2$ las proyecciones del plano. Entonces, para todo punto $u$ de $\mathbb{R}^2$*

$$\varphi(u) = \pi_1(u)\varphi(1, 0) + \pi_2(u)\varphi(0, 1).$$

*Demostración.* Sean $e_1 = (1, 0)$ y $e_2 = (0, 1)$. Como $e_1$ y $e_2$ son ortonormales, de acuerdo al corolario 8.11, los vectores $\varphi(e_1)$ y $\varphi(e_2)$ también resultan ortonormales. En ese caso, según el teorema 8.5 podemos escribir $\varphi(u)$ como una combinación lineal de $\varphi(e_1)$ y $\varphi(e_2)$; explícitamente, si definimos $\alpha_1(u) = \langle \varphi(u), \varphi(e_1) \rangle$ y $\alpha_2(u) = \langle \varphi(u), \varphi(e_2) \rangle$ entonces

$$\varphi(u) = \alpha_1(u)\varphi(e_1) + \alpha_2(u)\varphi(e_2).$$

Basta entonces comprobar que las asignaciones $\alpha_1$ y $\alpha_2$ son las proyecciones del plano. En efecto, como $\varphi$ preserva el producto interno,

$$\alpha_1(u) = \langle \varphi(u), \varphi(e_1) \rangle = \langle u, e_1 \rangle = \pi(u)$$

y de la misma forma

$$\alpha_2(u) = \langle \varphi(u), \varphi(e_2) \rangle = \langle u, e_2 \rangle = \pi(u),$$

obteniendo con esto la expresión que afirma el lema. ■

**Teorema 8.13.** *Las isometrías centrales son biyectivas.*

*Demostración.* Sea $\varphi$ una isometría central. Usando el lema anterior y definiendo $h_1 = \varphi(1,0)$ y $h_2 = \varphi(0,1)$ podemos escribir

$$\varphi(u) = \pi_1(u)h_1 + \pi_2(u)h_2.$$

Usando esta expresión mostraremos que la función $\varphi$ es sobreyectiva.

Supongamos entonces $b$ como un punto cualquiera en el plano. Como $h_1$ y $h_2$ son ortonormales, expresamos

$$b = \langle b, h_1 \rangle h_1 + \langle b, h_2 \rangle h_2$$

y si definimos $a = (\langle b, h_1 \rangle, \langle b, h_2 \rangle)$, entonces

$$\begin{aligned} \varphi(a) &= \pi_1(a)h_1 + \pi_2(a)h_2 \\ &= \langle b, h_1 \rangle h_1 + \langle b, h_2 \rangle h_2 \\ &= b. \end{aligned}$$

Esto implica que todo elemento de $\mathbb{R}^2$ está en la imagen de $\varphi$, lo que nos permite concluir que ésta es sobreyectiva y en virtud de ser isometría es también inyectiva. En conclusión, $\varphi$ es biyectiva. ■

**Corolario 8.14.** *Todas las isometrías son biyectivas.*

*Demostración.* Por el teorema 8.8, una isometría se puede descomponer en una isometría central y una traslación. De acuerdo al corolario anterior las isometrías centrales son biyectivas, lo mismo que las traslaciones. Esto quiere decir que una isometría se puede expresar como la composición de dos funciones biyectivas por lo que ésta debe resultar de igual forma biyectiva. ■

Después de toda esta discusión, quizá innecesariamente larga, estamos al fin en posición de enunciar el resultado que buscamos permitiéndonos conectar el tema con los conceptos que nos interesan[1].

**Teorema 8.15.** *El conjunto de las isometrías junto a la composición forma un grupo.*

*Demostración.* La prueba consiste en hacer un resumen de los resultados expuestos. Como la composición de isometrías es una isometría (ejercicio 8.9), la composición define una operación binaria en el conjunto de isometrías, operación que debe ser asociativa pues la composición lo es.

Por otro lado, la función identidad funciona como la identidad del grupo por ser ésta trivialmente una isometría y en consecuencia estar dentro del conjunto en cuestión.

Por último, como todas las isometrías son biyectivas poseen una inversa, basta probar que ésta inversa es también una isometría. En efecto, si $\varphi$ es una isometría entonces, para cualesquiera puntos $a$ y $b$ en $\mathbb{R}^2$,

$$\begin{aligned} \|\varphi^{-1}(a) - \varphi^{-1}(b)\| &= \left\| \varphi\left(\varphi^{-1}(a)\right) - \varphi\left(\varphi^{-1}(b)\right) \right\| \\ &= \|a - b\| \end{aligned}$$

por lo que $\varphi^{-1}$ resulta una isometría, mostrando que cualquier isometría contiene una inversa en el conjunto de isometrías. Con esto, es posible concluir que el conjunto en cuestión es un grupo. ■

[1] Quizá no sea del todo inoportuno pedir un redoble de tambores…

**Corolario 8.16.** *El conjunto de las isometrías centrales forma un grupo con la composición.*

*Demostración.* La prueba es idéntica, sólo hay que notar que la identidad es una isometría central y que la inversa de una isometría central es de nueva cuenta una isometría central. ■

**Definición 8.9.** *El grupo euclideano del plano* es el conjunto de isometrías junto a la composición como operación y se denota por $E(\mathbb{R}^2)$. *El grupo ortogonal del plano* es el conjunto de isometrías centrales junto a la composición como operación y se denota por $O_2(\mathbb{R})$.

## Ejercicios

*Ejercicio* 8.1. Comprueba que los ejemplos posteriores a la definición 8.1 son en verdad grupos.

*Ejercicio* 8.2. Como debía sospecharse, hemos impuesto demasiadas condiciones a la definición de un grupo. En este ejercicio vamos a debilitar las condiciones para obtener un grupo sin comprometer la estructura. Sea $G$ un conjunto y sea $*$ una operación binaria sobre $G$ que satisfacen las siguientes condiciones:

- La operación $*$ es asociativa.
- Existe un elemento $e$ de forma que para todo $x$, se tiene $e * x = x$.
- Para cualquier elemento $x$ en $G$, existe $y$ en $G$ de forma que $y * x = e$.

Demuestra que $(G, *)$ es un grupo. Sugerencia: Observa que las condiciones no son las mismas que en la definición.

*Ejercicio* 8.3. Termina la prueba de la proposición 8.3 y formula el resultado en notación aditiva.

*Ejercicio* 8.4. En un grupo $G$, comprueba que si $a$ y $b$ conmutan, entonces $a^{-1}$ y $b^{-1}$ también lo hacen.

*Ejercicio* 8.5. Muestra que el producto interno en $\mathbb{R}^2$ satisface las siguientes identidades:

1. $\langle a, b\rangle = \langle b, a\rangle$.
2. $\langle ra, b\rangle = r\langle a, b\rangle$.
3. $\langle a + b, c\rangle = \langle a, c\rangle + \langle b, c\rangle$.
4. $\langle a, a\rangle \geq 0$.

*Ejercicio* 8.6. Demuestra que $\|a\| = 0$ si y sólo si $a = (0, 0)$.

*Ejercicio* 8.7. Usa un contraejemplo para mostrar que el producto interno no satisface las leyes de cancelación, i.e., no necesariamente $\langle a, c\rangle = \langle a, b\rangle$ y $a \neq (0, 0)$ implica que $b = c$.

*Ejercicio* 8.8. Muestra que las traslaciones son isometrías.

*Ejercicio* 8.9. Muestra que la composición de isometrías es una isometría.

*Ejercicio* 8.10. Demuestra que si $\varphi$ es una isometría central, entonces $\varphi^{-1}$ es una isometría central.

*Ejercicio* 8.11. Un subconjunto de $\Omega \subset \mathbb{R}^2$ se dice *un círculo* si existen un real $r > 0$ y un punto $a \in \mathbb{R}^2$ de forma que

$$\Omega = \left\{ x \in \mathbb{R}^2 \mid \|x - a\| = r \right\}.$$

El número $r$ se dice *el radio del círculo* mientras el punto $a$ se denomina *el centro del círculo*. Demuestra que sí $\varphi$ es una isometría, la imagen bajo $\varphi$ del conjunto $S^1$ es un círculo.

# Referencias

[RG04] Ramiréz-Galarza, Ana Irene: *Geometría analítica*. Las prensas de ciencias, 2ª edición, 2004.

[Rot05] Rotman, Joseph J.: *A first course in abstract algebra*. Pearson, 3ª edición, 2005.

Las notas anteriores juegan algunas veces a ser un simple resumen de lo que otros autores han presentado, otras menos a reinterpretarlo y en una cantidad ínfima de ocasiones intentan pobremente aumentalo. El único objectivo real al que sirven, es preparar el curso de Álgebra Superior II impartido en la carrera de Actuaría de la FES Acatlán. Su versión es, en consecuencia, susceptible a errores gramaticales, imprecisiones técnicas y cambios constantes.