Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Departamento de Matemática - Escuela de Ciencias Exactas y Naturales
**COMPLEMENTOS DE MATEMÁTICA II**
Licenciatura en Ciencias de la Computación - Año 2023
Docentes: Francisco Vittone - Mauro Lucci - Delfina Martin

---

# Unidad 5: Grupos.

---

## 1. Propiedades básicas de un grupo - Repaso

Los grupos constituyen sin dudas el concepto algebráico más importante en matemática. Esto se debe fundamentalmente a que cuando estudiamos cualquier estructura matemática, es necesario definir una noción de equivalencia que nos permita clasifficar los objetos respecto de la estructura que estamos estudiando. Por ejemplo, si estamos estudiando álgebra lineal, ¿cuándo son equivalentes dos espacios vectoriales? O si estamos considerando conjuntos ordenados, o retículos, ¿Cuándo son equivalentes? Esta noción de equivalencia deberá ser tal que estudiar las propiedades de la estructura que estamos considerando en cualquier representante de la clase, las propiedades que obtengamos deben valer para cualquier otro elemento de la clase. Ya hemos visto que para llevar a cabo esta clasificación es fundamental el concepto de *isomorfismo*. Pero además, los isomorfismos de cualquier estructura (de espacios vectoriales, de retículos, de monoides, de grupos, etc.) forman siempre un grupo, y los invariantes de este nuevo grupo de isomorfismos constituyen los elementos que interesa estudiar respecto de esa estructura.

A lo largo de esta unidad nos porponemos por lo tanto estudiar la estructura de grupo en más profundidad. Comencemos recordando que si $G$ es un conjunto con una operación $\cdot : G \times G \to G$, decimos que $G$ es un **grupo** si:

G1) la operación $\cdot$ es asociativa;

G2) existe un elemento neutro $e \in G$ para $\cdot$;

G3) todo elemento $g \in G$ admite un elemento inverso, denotado por $g^{-1}$.

Si además la operación es conmutativa, $(G, \cdot)$ se denomina un **grupo abeliano**.

Definición **1.** *El cardinal de $G$ se denomina **orden** del grupo $G$ y se denota $o(G)$.*

**Notación 1.** *A partir de aquí denotaremos por $\cdot$ a una operación genérica en un grupo cualquiera. Si $g_1, g_2 \in G$, denotaremos por $g_1 g_2$ al producto $g_1 \cdot g_2$ (es decir, la yuxtaposición de dos elementos representa su producto). Más aún, si trabajamos con dos grupos abstractos distintos $G$ y $G'$ denotaremos por $\cdot$ la operación en ambos grupos, aunque sean operaciones distintas, a menos que tratemos con algún caso concreto.*

En la unidad anterior vimos que a partir de uno o más grupos podemos construir nuevos grupos. Los procedimientos generales son:

1. **Considerar subgrupos de** $G$. Recordemos que dado un subconjunto $H \subset G$, $H$ es un subgrupo de $G$ si se verififca cualquiera de las siguientes propiedades equivalentes:
   - $H$ es cerrado para $\cdot$, $e \in H$ y $g^{-1} \in H$ para cada $g \in H$.
   - $(H, \cdot)$ es un grupo.
   - Para todo $g_1, g_2 \in H$, $g_1 g_2^{-1} \in H$.
2. **Construir grupos producto**. En este caso partimos de dos grupos $(G, \cdot)$ y $(G', \cdot)$. Entonces $G_1 \times G_2$ es un nuevo grupo cuya operación es
   $$(g_1, g_1') \cdot (g_2, g_2') = (g_1 g_2, g_1' g_2')$$
   denominado **grupo producto** de $G_1$ y $G_2$.
3. **Construir un grupo cociente**. Aquí tenemos un grupo $(G, \cdot)$ y una relación de equivalencia $\sim$ en $G$ tal que $\cdot$ se induce al cociente $G/\sim$. Entonces $G/\sim$ es un nuevo grupo, denominado **grupo cociente**

La construcción del grupo cociente no siempre es posible, esto es, puede ocurrir que un grupo $G$ no admita ninguna relación de equivalencia no trivial (esto es $=$ o la relación $G \times G$). Nos ocuparemos de estos temas en las próximas secciones).

Recordemos que la asociatividad permite definir además la "potencia" de un elemento del grupo sin preocuparnos por el orden en el cual operamos:

**Definición:** Sean $(G, \cdot)$ un grupo y $a \in G$. Se definen:

- $a^0 = e$
- para cada $n \in \mathbb{N}$, $a^n$ se define inductivamente como $a^n = a^{n-1} \cdot a$.
- para cada $k \in \mathbb{Z}$ con $k < 0$, se define $a^k = (a^{-1})^{-k}$.

Antes de continuar, hagamos algunas observaciones sobre cómo interpretar el símbolo $a^n$. De modo intuitivo, $a^n$ (para $n \in \mathbb{N}$) representa operar iteradamente $a$ con sí mismo $n$ veces. Ya hemos notado como la notación "$\cdot$" para la operación es una convención abstracta, pero no debe hacernos pensar que se trate de un "producto" en el sentido que lo conocemos para los conjuntos numéricos. En un grupo donde esté definida otra operación la definición anterior debe interpretarse adecuadamente. Consideremos un grupo cualquiera donde esté definida una suma (por ejemplo $\mathbb{Z}$, $\mathcal{M}_n, \mathbb{Z}_p$, etc.). Entonces cada item de la definición anterior se leerá:

$$0a = 0, \quad na = (n-1)a + a, \quad ka = (-k)(-a) \tag{1}$$

respectivamente. Se trata símplemente de replicar la definición de $a^n$ para un grupo que utiliza, por comodidad o porque así lo permite la operación en él definida, una **notación aditiva** (es decir, donde la operación se simboliza con $+$ en vez de $\cdot$).

Como ya hemos probado en la Práctica 4, la potencia en un grupo verifica:

Teorema **2.** *Sea $G$ un grupo y $a \in G$. Para cada $m, n \in \mathbb{Z}$, se verifican:*

1. $a^n a^m = a^{n+m}$;
2. $(a^n)^m = a^{nm}$.

*En notación aditiva:*

1. $na + ma = (n+m)a$;
2. $m(na) = (mn)a$.

## 2. Subgrupos cíclicos. Subgrupos generados por un subconjunto de un grupo.

**Notación 3.** *Usaremos la notación $H < G$ para indicar que $H \subset G$ es un subgrupo de $G$.*

Uno de los primeros problemas que surgen es el siguiente. Si $X$ es un subconjunto de $G$ que no es un subgrupo. ¿Cuál es el menor subgrupo de $G$ que contiene a $X$?

Comencemos con el caso más sencillo. Supongamos que tenemos un elemento $a \in G$ cualquiera. ¿Cuál es el menor subgrupo de $G$ que contiene a $a$? Si $H$ es un subgrupo de $G$ que contiene a $a$, debe contener además a $a^{-1}$ y como la operación es cerrada en $H$, $H$ deberá contener a cualquier potencia $a^k$ con $k \in \mathbb{Z}$. Esto es, si $H < G$ es tal que $a \in H$, entonces

$$\langle a \rangle := \{a^k \,:\, k \in \mathbb{Z}\} \subset H.$$

Por otra parte, de las propiedades del teorema 2 tenemos que si $u$, $v$ son elementos de $\langle a \rangle$, existen $k_1, k_1 \in \mathbb{Z}$ tales que $u = a^{k_1}$, $v = a^{k_2}$ y por lo tanto

$$uv^{-1} = a^{k_1} a^{-k_2} = a^{k_1 - k_2} \in \langle a \rangle.$$

Concluimos que $\langle a \rangle$ es un subgrupo de $G$ que contiene a $a$ y está contenido en cualquier otro subgrupo de $G$ que contiene a $a$. Esto es, $\langle a \rangle$ es un mínimo del poset $(\mathcal{S}_a(G), \subseteq)$ donde $\mathcal{S}_a(G)$ es el conjunto de subgrupos de $G$ que contienen a $a$. Decimos por esto que $\langle a \rangle$ es el **menor subgrupo de** $G$ que contiene a $a$.

Definición **2.** *Sea $G$ un grupo y $a \in G$.*

- *El subgrupo $\langle a \rangle$ de $G$ dado por $\langle a \rangle = \{a^k \,:\, k \in \mathbb{Z}\}$ (o $\langle a \rangle = \{ka \,:\, k \in \mathbb{Z}\}$ en notación aditiva) se denomina **subgrupo cíclico** de $G$ generado por $a$.*
- *Si existe $a \in G$ tal que $G = \langle a \rangle$, $G$ se dice un **grupo cíclico** y $a$ es un **generador de** $G$.*

- *Se define el* ***orden*** *del elemento $a \in G$ como el orden (es decir el cardinal) del subgrupo cíclico $\langle a \rangle$ generado por $a$.*

Ejemplos **1.** 1. Consideremos el grupo $(\mathbb{Z}, +)$. Como estamos trabajando con notación aditiva, recordemos que si $a \in \mathbb{Z}$, $\langle a \rangle = \{ka : k \in \mathbb{Z}\}$ (en este caso, y es algo que sólo ocurre en los conjuntos numéricos, la notación $ka$ coincide con el producto usual en $\mathbb{Z}$, pero en otros grupos esto no ocurre y no debe hacernos pensar que $ka$ representa una nueva operación en el grupo).

Observemos que $\langle 1 \rangle = \{k1 : k \in \mathbb{Z}\} = \mathbb{Z}$. Luego $\mathbb{Z}$ es cíclico y $1$ es un generador de $\mathbb{Z}$. Pero también tenemos

$$\langle -1 \rangle = \{k(-1) : k \in \mathbb{Z}\} = \{s1 : s \in \mathbb{Z}\} = \langle 1 \rangle = \mathbb{Z}$$

y por lo tanto $-1$ también es un generador de $\mathbb{Z}$. Vemos así que un grupo cíclico puede tener más de un generador.

Es fácil ver que $\mathbb{Z}$ no puede tener otros generadores. En efecto, si $a \neq \pm 1$ es un número entero, entonces $\langle a \rangle$ es el subgrupo de $\mathbb{Z}$ formado por los múltiplos de $a$, que claramente no es todo $\mathbb{Z}$. Nuevamente, es fácil ver que para cualquier $a \in \mathbb{Z}$, los únicos generadores del subgrupo cíclico $\langle a \rangle$ son $a$ y $-a$.

2. El caso de $\mathbb{Z}$ no es un caso particular, en el sentido que **si $a$ es un generador de un grupo cíclico $G$, $a^{-1}$ también es un generador**. En efecto, si $G = \langle a \rangle$, entonces

$$\langle a^{-1} \rangle = \{(a^{-1})^k : k \in \mathbb{Z}\} = \{a^{-k} : k \in \mathbb{Z}\} = \{a^s : s \in \mathbb{Z}\} = G.$$

3. Consideremos ahora el grupo $(\mathbb{Z}_m, +)$ de los enteros módulo $m$ con la suma. En este caso, si $\overline{a} \in \mathbb{Z}_m$, $k\overline{a} = \overline{ka}$. Luego

$$\langle \overline{1} \rangle = \{k\overline{1} : k \in \mathbb{Z}\} = \{\overline{k} : k \in \mathbb{Z}\} = \mathbb{Z}_m$$

con lo cual $\mathbb{Z}_m$ es un grupo cíclico y $\overline{1}$ es un generador. También $-\overline{1} = \overline{m-1}$ es un generador de $\mathbb{Z}_m$, pero en este caso puede haber más generadores aún.

Consideremos antes de hacer el análisis general dos ejemplos puntuales: $\mathbb{Z}_5$ y $\mathbb{Z}_8$.

Comencemos por $\mathbb{Z}_8 =, \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$. Sus subgrupos cíclicos son:

- $\langle \overline{0} \rangle = \{\overline{0}\}$ (el grupo trivial)
- $\langle \overline{1} \rangle = \mathbb{Z}_8$
- $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$
- $\langle \overline{4} \rangle = \{\overline{0}, \overline{4}\}$
- $\langle \overline{6} \rangle = \langle -\overline{2} \rangle = \langle \overline{2} \rangle$.
- $\langle \overline{7} \rangle = \langle -\overline{1} \rangle = \mathbb{Z}_8$.

Observemos que en el caso de $\langle \overline{2} \rangle$, hemos cortado cuando obtenemos $\overline{6}$, pues en efecto el próximo elemento sería $\overline{8} = \overline{0}$, el siguiente $\overline{10} = \overline{2}$, y así los elementos se repiten cíclicamente. Lo mismo ocurre con $\langle \overline{4} \rangle$ y $\langle \overline{6} \rangle$. Hemos dejado afuera del análisis, a propósito, los grupos cíclicos generados por $\overline{3}$ y $\overline{5}$.

Observemos que:

$$\langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}, \ldots\} = \{\overline{0}, \overline{3}, \overline{6}, \overline{1}, \overline{4}, \overline{7}, \overline{2}, \overline{5}\} = \mathbb{Z}_8$$

Es decir que $\overline{3}$ es un generador de $Z_8$. En el proceso anterior podríamos haber parado mucho antes. En efecto, como $3\overline{3} = \overline{9} = \overline{1}$, resulta que $\overline{1} \in \langle\overline{3}\rangle$ y por lo tanto $Z_8 = \langle\overline{1}\rangle \subset \langle\overline{3}\rangle$. Luego no hay otra opción que $\langle\overline{3}\rangle = \mathbb{Z}_8$.

Con el subgrupo cíclico generado por $\overline{5}$ ocurre algo parecido: $3 \cdot \overline{5} = \overline{15} = \overline{7}$, con lo cual $\overline{7} \in \langle\overline{5}\rangle$ y por lo tanto $\langle\overline{7}\rangle \subset \langle\overline{5}\rangle$. Pero $\langle\overline{7}\rangle = \mathbb{Z}_8$, con lo cual $\langle\overline{5}\rangle = \mathbb{Z}_8$ (otra forma de probarlo sería simplemente observar que $\overline{5} = -\overline{3}$ y por lo tanto generan el mismo subgrupo cíclico).

Concluimos que los generadores de $\mathbb{Z}_8$ son $\overline{1}$, $\overline{3}$, $\overline{5} = -\overline{3}$ y $\overline{7} = -\overline{1}$.

Veamos ahora qué ocurre en $\mathbb{Z}_5$. En este caso es claro que $\overline{1}$ y $\overline{4} = -\overline{1}$ son generadores. Pero además, como $2 \cdot \overline{2} = \overline{4}$, resulta $\overline{4} \in \langle\overline{2}\rangle$ y por lo tanto $\mathbb{Z}_5 = \langle\overline{4}\rangle \subset \langle\overline{2}\rangle$ y entonces $\overline{2}$ es un generador de $\mathbb{Z}_5$. Por otro lado, $2 \cdot \overline{3} = \overline{6} = \overline{1}$, con lo cual $\overline{1} \in \langle\overline{3}\rangle$ y por lo tanto $\overline{3}$ también es un generador de $\mathbb{Z}_5$.

Analizando ambos casos, observamos que en $\mathbb{Z}_8$ los generadores son $\overline{1}$, $\overline{3}$ y $\overline{7}$, mientras que en $\mathbb{Z}_5$, todos los elementos distintos de $\overline{0}$ son generadores. El hecho de que $5$ sea un número primo y que todos los generadores de $\mathbb{Z}_8$ sean las clases de elementos coprimos con $8$ no es casual. Analicemos qué ocurre en el caso general:

Consideremos ahora $\mathbb{Z}_m$ para $m \in \mathbb{N}$ cualquiera. Supongamos que $\overline{a}$ es un generador de $\mathbb{Z}_m$. Observemos que con los mismos argumentos que en los ejemplos concretos anteriores, $\overline{a}$ es generador de $\mathbb{Z}_m$ si y sólo si $\overline{1} \in \langle\overline{a}\rangle$, o sea, si y sólo si existe $k \in \mathbb{Z}$ tal que $k \cdot \overline{a} = \overline{1}$. Pero esto a su vez ocurre si y sólo si $ka - 1$ es múltiplo de $m$. Concluimos que

$$\begin{aligned} \overline{a} \text{ es generador de } \mathbb{Z}_m &\iff \exists\, k, k' \in \mathbb{Z} : ka - 1 = k'm \iff \exists\, k, k'' \in \mathbb{Z} : ka + k''m = 1 \\ &\iff mcd(a, m) = 1. \end{aligned}$$

Es decir, $\overline{a}$ es un generador de $\mathbb{Z}_m$ si y sólo si $a$ y $m$ son coprimos.

4. Sea $G_n = \{z \in \mathbb{C} : z^n = 1\}$ el conjunto de raices $n$-ésimas de la unidad, para cada $n \in \mathbb{N}$. Si $z_1, z_2 \in G_n$, entonces $(z_1 \cdot z_2)^n = z_1^n z_2^n = 1$, es decir, el producto usual de números complejos es una operación cerrada en $G_n$. Además el elemento neutro, $1$, pertenece a $G_n$ y por lo tanto $(G_n, \cdot)$ es un monoide. Claramente si $z \in G_n$, entonces $(z^{-1})^n = 1/z^n = 1$ con lo cual todo elemento de $G_n$ admite un inverso en $G_n$. Concluimos que $(G_n, \cdot)$ es un grupo. Ahora bien, si $z$ es una raíz $n$-ésima de $1$, $z$ admite una representación en forma polar de la forma $z_k = 1_{\frac{2k\pi}{n}}$ para $0 \leq k \leq n-1$. Tomemos $z_1 = 1_{\frac{2\pi}{n}}$. Entonces

$$z_1^2 = 1_{\frac{4\pi}{n}} = z_2, \quad z_1^3 = 1_{\frac{6\pi}{n}} = z_3, \ \cdots, z_1^k = 1_{\frac{2k\pi}{n}} = z_k.$$

Por lo tanto $z_1$ es un generador de $G_n$, y $G_n$ es un grupo cíclico abeliano finito de orden $n$. Más aún, $G_n$ es un subgrupo cíclico finito del círculo $(S^1, \cdot)$.

Lema **4.** *Todo subgrupo $H$ de $(\mathbb{Z}, +)$ es cíclico. Además $H = \langle 0\rangle = \{0\}$ o bien $H = \langle m\rangle$, donde $m$ es menor entero positivo de $H$.*

*Demostración.* Si $H \neq \langle 0 \rangle$, entonces $S = H \cap \mathbb{N}$ es no vacío (pues al ser subgrupo, debe contener cada elemento y su opuesto, y uno de ellos es positivo). Por el principio del bueno orden, $S$ tiene un elemento mínimo, digamos $m$. En particular $m \in H$ y por lo tanto $\langle m \rangle \subset H$. Recíprocamente, si $h \in H$ podemos aplicar el algoritmo de la división para dividir $h$ por $m$ y obtener $h = qm + r$, con $0 \leq r < m$. Como $h$ y $qm$ son elementos de $H$, deberemos tener $r = h + (-qm) \in H$. Si $r > 0$, entonces $r \in S$. Pero esto es absurdo pues $r < m$. Luego debe ser $r = 0$ y por lo tanto $h \in \langle m \rangle$. □

Pasemos ahora a analizar la existencia del menor subgrupo que contenga a un subconjunto $X$ cualquiera de un grupo $G$.

Lema **5.** *Sea $G$ un grupo y $H_1$, $H_2$ subgrupos de un grupo $G$. Entonces $H_1 \cap H_2$ es un subgrupo de $G$. Más generalmente, si $\{H_i\}_{i \in I}$ es una familia de subgrupos de $G$, entonces $\bigcap_{i \in I} H_i$ es un subgrupo de $G$.*

*Demostración.* Observemos que $e \in H_1 \cap H_2$ y por lo tanto $H_1 \cap H_2 \neq \emptyset$. Sean $a, b \in H_1 \cap H_2$. Entonces en particular $a, b \in H_1$ y por lo tanto $ab^{-1} \in H_1$. De la misma manera, $a, b \in H_2$ y por lo tanto $ab^{-1} \in H_2$. Luego $ab^{-1} \in H_1 \cap H_2$. Concluimos que $H_1 \cap H_2 < G$. Dejamos como ejercicio la prueba de que la intersección generalizada de subgrupos es un subgrupo. □

Teorema **6.** *Sea $G$ un grupo y sea $X \subset G$.*

1. *Existe un único subgrupo $H$ de $G$ que contiene a $X$ y tal que para cada $H' < G$ con $X \subset H'$, resulta $H \subset H'$.*

2. *Los elementos del subgrupo $H$ del item anterior son de la forma*

$$a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} \tag{2}$$

*con $k \in \mathbb{N}$, $n_j \in \mathbb{Z}$ y $a_j \in X$ para cada $j = 1, \ldots, k$.*

*Demostración.* 1. Sea $S = \{K < G : X \subset K\}$ la familia de subgrupos de $G$ que contienen a $X$. Observemos que $S \neq \emptyset$ pues $G \in S$. Pongamos

$$H = \bigcap_{K \in S} K.$$

Entonces $H$ es un subgrupo de $G$ por el Lema 5 y claramente $X \subset H$. Además si $H'$ es un subgrupo de $G$ que contiene a $X$, entonces $H' \in S$ y por lo tanto $H \subset H'$.

2. Sea $K = \{a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} : k \in \mathbb{N},\ n_j \in \mathbb{Z},\ a_j \in X\ \forall\, j = 1, \ldots, k\}$ y sea $H$ la intersección de todos los subgrupos de $G$ que contienen a $X$, como en el item anterior. Observemos primero que $K$ es un subgrupo de $G$. Sean $x = a_1^{n_1} \cdots a_k^{n_k}$ e $y = b_1^{m_1} \cdots b_r^{m_r}$ dos elementos arbitrarios de $K$. Observemos que $y^{-1} = b_r^{-m_r} \cdots b_2^{-m_2} b_1^{-m_1}$ y por lo tanto $xy^{-1}$ es claramente de la forma (2), con lo cual $xy^{-1} \in K$. Luego $K < G$ y $X \subset K$, de donde $H \subset K$. Por otro lado, como $H$ contiene a todos los elementos de $X$ y la operación del grupo es cerrada en $H$, $H$ deberá contener necesariamente a todos los elementos de la forma (2), y por lo tanto $K \subset H$. Concluimos que $K = H$ como queríamos probar.

□

Definición **3.** *Sea $G$ un grupo y $X \subset G$ un subconjunto cualquiera. El menor subgrupo de $G$ que contiene a $X$ definido en el Teorema 6 se denomina* ***subgrupo generado por*** *$X$ y se denota $\langle X \rangle$.*

Observación **1.** *Si $X = \{a\}$ consta de un único elemento, es claro que el subgrupo generado por $\{a\}$ es el subgrupo cíclico generado por $a$.*

Ejemplo **2.** Hemos visto que en $(\mathbb{Z}, +)$ todo subgrupo es cíclico. Consideremos $X = \{2, 3\}$. Entonces debe existir $a \in \mathbb{Z}$ tal que $\langle X \rangle = \langle a \rangle$. Ahora bien, $1 = 3 - 2 \in \langle \{2, 3\} \rangle$. Luego $\langle X \rangle = \langle 1 \rangle = \mathbb{Z}$. Más generalmente, puede verse que $\langle \{n, n+1\} \rangle = \mathbb{Z}$.

Ejercicio **1.** *Si $m, n \in \mathbb{Z}$, ¿cuál es el subgrupo generado por $\{n, m\}$?*

## 3. Grupo cociente. Subgrupos normales.

Hemos visto que si $G$ es un grupo y $\sim$ es una relación de equivalencia en $G$ tal que la operación del grupo se induce al cociente, entonces $G/\sim$ es nuevamente un grupo. Nos ocuparemos en esta sección de estudiar cómo son estas relaciones de equivalencia.

Recordemos que en $G/\sim$ el elemento neutro es $[e]$, es decir, la clase del elemento neutro de $G$, y el inverso de $[a]$ es $[a^{-1}]$.

Comencemos con nuestro caso paradigmático, el grupo $(\mathbb{Z}, +)$. Supongamos que $\sim$ es una relación de equivalencia en $\mathbb{Z}$ tal que la suma se induce al cociente $\mathbb{Z}/\sim$, y por lo tanto $\mathbb{Z}/\sim$ es un grupo. Esto es, cada vez que $k_1 \sim k_1'$ y $k_2 \sim k_2'$ entonces $k_1 + k_2 \sim k_1' + k_2'$. Ya hemos visto en la unidad anterior que un ejemplo de este tipo de relaciones es la congruencia módulo $m$ y el grupo cociente que se obtiene es $(\mathbb{Z}_m, +)$. Veamos ahora si existen otras relaciones de equivalencai $\sim$ en $\mathbb{Z}$ que permitan definir un grupo $(\mathbb{Z}/\sim, +)$.

Consideremos la clase de equivalencia $H$ del $0$. Esto es,

$$H = [0] = \{x \in \mathbb{Z} : x \sim 0\}.$$

Veamos primero que $H$ es un subgrupo de $G$:

- Claramente $0 \in [0]$, con lo cual $0 \in H$.
- Si $k_1, k_2 \in H$, entonces $k_1 \sim 0$, $k_2 \sim 0$ y como la suma se induce al cociente, $k_1 + k_2 \sim 0 + 0 = 0$. Esto es, $k_1 + k_2 \in H$ y por lo tanto $H$ es un subconjunto cerrado para $+$.
- Finalmente, si $k \in H$, veamos que $-k \in H$. Observemos que como $k \sim 0$ y $-k \sim -k$, entonces $k + (-k) \sim 0 + (-k)$, esto es, $0 \sim -k$ y por lo tanto $-k \in H$.

Luego $H$ es un subgrupo de $\mathbb{Z}$ y por el Lema 4, $H$ debe ser el grupo cíclico generado por algún elemento $m \in \mathbb{Z}$. Esto es, $H = \langle m \rangle$.

Tomemos ahora $k_1 \sim k_2$ cualesquiera. Como $-k_2 \sim -k_2$, resulta

$$k_1 - k_2 \sim k_2 - k_2 = 0 \implies k_1 - k_2 \in H = \langle m \rangle$$

y recíprocamente, si $k_1 - k_2 \in H$, entonces $k_1 - k_2 \sim 0$ pero $k_2 \sim k_2$ de donde $(k_1 - k_2) + k_2 \sim 0 + k_2$, o sea $k_1 \sim k_2$.

Concluimos que

$$k_1 \sim k_2 \;\Leftrightarrow\; k_1 - k_2 \in \langle m \rangle \;\Leftrightarrow\; k_1 - k_2 \text{ es múltiplo de } m \;\Leftrightarrow\; k_1 \equiv k_2\,(m).$$

O sea que las únicas relaciones de equivalencia en $\mathbb{Z}$ tales que $\mathbb{Z}/\sim$ es un grupo son las congruencias módulo algún entero $m$, y por lo tanto los únicos grupos cocientes que se obtienen a partir de $\mathbb{Z}$ son los grupos $\mathbb{Z}_m$.

Veremos a continuación que en un grupo arbitrario $G$, las únicas relaciones de equivalencia que permiten definir un grupo cociente $G/\sim$ provienen también de algún subgrupo de $G$, como ocurre con $\mathbb{Z}$ y $\mathbb{Z}_m$.

Lema **7.** *Sea $G$ un grupo y sea $\sim$ una relación de equivalencia tal que $G/\sim$ es un grupo (con la operación inducida). Entonces:*

1. *$H = [e]$ es un subgrupo de $G$.*
2. *para cada $x, y \in G$,*
$$x \sim y \iff xy^{-1} \in H$$
3. *para cada $x, y \in G$,*
$$x \sim y \iff x^{-1}y \in H.$$

*Demostración.* 1. Observemos que $e \in H$ y que si $k_1, k_2 \in H$, entonces $k_1 \sim e$, $k_2 \sim e$ y por lo tanto

$$k_1 \cdot k_2 \sim e \cdot e = e \implies k_1 \cdot k_2 \in H.$$

Luego $H$ es cerrado para la operación de $G$ y contiene a la identidad. Finalmente, si $k \in H$, $k \sim e$, y como $k^{-1} \sim k^{-1}$ resulta

$$k \cdot k^{-1} \sim e \cdot k^{-1} \implies e \sim k^{-1} \implies k^{-1} \in H.$$

Concluimos que $H < G$.

2. Supongamos que $x \sim y$. Entonces como $y^{-1} \sim y^{-1}$, resulta $x \cdot y^{-1} \sim y \cdot y^{-1} = e$, con lo cual $xy^{-1} \in H$. Recíprocamente, si $xy^{-1} \in H$, entonces $xy^{-1} \sim e$ y como $y \sim y$, resulta $(xy^{-1}) \cdot y \sim e \cdot y$, o sea $x \sim y$.

3. Es análoga al item anterior y se deja como ejercicio.

□

El Lema 7 nos dice entonces que si $\sim$ es una relación de equivalencia en $G$ tal que $G/\sim$ es un grupo, existe un subgrupo $H$ de $G$ tal que la relación está dada por cualquiera de las dos definiciones equivalentes dadas en los items 2 y 3.

Una pregunta natural es si para cualquier subgrupo $H$ de $G$ la relación de equivalencia definida como en los items 2 o 3 es tal que $G/\sim$ sea un grupo. Lo que ocurre en $\mathbb{Z}$ puede hacernos pensar que la respuesta

es afirmativa, pero no debemos olvidar que $(\mathbb{Z}, +)$ tiene una propiedad particular que no comparten todos los grupos: $(\mathbb{Z}, +)$ es un grupo abeliano.

Para intentar dar una respuesta a nuestra pregunta, consideremos un subgrupo $H$ cualquiera y definamos las siguientes relaciones en $G$:

Definición **4.** *Sea $G$ un grupo y $H$ un subgrupo. Sean $a, b \in G$, decimos que $a$ es* ***congruente a derecha*** *con $b$* ***módulo*** *$H$, y lo denotamos $a \equiv_r b\,(H)$, si $ab^{-1} \in H$. Decimos que $a$ es* ***congruente a izquierda*** *con $b$* ***módulo*** *$H$, y lo denotamos $a \equiv_l b\,(H)$, si $a^{-1}b \in H$.*

Lema **8.** *Sea $G$ un grupo y $H$ un subgrupo de $G$ entonces las congruencias a izquierda y a derecha módulo $H$ son relaciones de equivalencia en $G$. Más aún, para cada $a \in G$,*

- *la clase de equivalencia de $a$ por $\equiv_r$ es $[a]_r = Ha = \{ha : h \in H\}$*
- *la clase de equivalencia de $a$ por $\equiv_l$ es $[a]_l = aH = \{ah : h \in H\}$*

*Demostración.* Probaremos el lema para $\equiv_r$, la prueba para $\equiv_l$ es análoga y se deja como ejercicio.

Veamos primero que $\equiv_r$ es una relación de equivalencia. Como $H$ es un subgrupo de $G$, $e \in H$ y por lo tanto para cada $a \in G$ se verifica $aa^{-1} = e \in H$, con lo cual $a \equiv_r a\,(H)$ y $\equiv_r$ es reflexiva.

Si ahora tenemos $a, b \in G$ tales que $a \equiv_r b(H)$, o sea $ab^{-1} \in H$, nuevamente como $H$ es un subgrupo el inverso de este elemento debe estar en $H$. Por lo tanto $(ab^{-1})^{-1} = ba^{-1} \in H$ con lo cual $b \equiv_r a\,(H)$ y entonces $\equiv_r$ es simétrica.

Finalmente, si $a \equiv_r b\,(H)$ y $b \equiv_r c\,(H)$, entonces $ab^{-1} \in H$, $bc^{-1} \in H$ y como la operación en $H$ es cerrada, resulta $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$. Luego $a \equiv_r c\,(H)$ y por lo tanto $\equiv_r$ es transitiva.

Encontremos ahora la clase de equivalencia $[a]_r$ de $a$ por $\equiv_r$.

Si $h \in H$, entonces $a(ha)^{-1} = h^{-1} \in H$, con lo cual $a \equiv_r (ha)\,(H)$. Esto es, $Ha \subset [a]_r$.

Si ahora $b \in [a]_r$, sea $h = ab^{-1}$, entonces $h \in H$ y $b = h^{-1}a \in Ha$, de donde $[a]_r \subset Ha$. □

Ejemplos **3.**

1. Volviendo al caso de la definición de $\mathbb{Z}_m$, podemos observar que si $H = \langle m \rangle$, entonces $a \equiv b\,(m)$ si $a$ es congruente a derecha con $b$ módulo $H$. En este caso, $a$ es también congruente a izquierda módulo $H$, puesto que si $a - b$ es un ḿutliplo de $m$, $-a + b = -(a - b)$ también lo es.

2. Vimos en el Lema 7 que si $\sim$ es una relación de equivalencia en un grupo $G$ tal que $G/\sim$ es un grupo, entonces $H = [e]$ es tal que la congruencia a izquierda y a derecha módulo $H$ coinciden.

3. Veamos ahora que en general estas congruencias no tienen por qué coincidir. Consideremos el grupo $Gl(2)$ de matrices invertibles $2 \times 2$ y el subgrupo $O(2) = \{A \in Gl(2) : A^tA = Id\}$ (dejamos como ejercicio probar que $O(2)$ es un subgrupo). Consideremos las matrices $A = \begin{pmatrix} \sqrt{2} & 1/\sqrt{2} \\ 0 & 1/\sqrt{2} \end{pmatrix}$ y $B = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ en $Gl(2)$. Tenemos entonces

$$AB^{-1} = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} \in O(2), \quad A^{-1}B = \begin{pmatrix} \sqrt{2} & 1/\sqrt{2} \\ -\sqrt{2} & 0 \end{pmatrix} \notin O(2)$$

con lo cual $A \equiv_r B\,(O(2))$ pero $A$ no es congruente a izquierda con $B$ módulo $O(2)$.

En función del Lema 7, si la congruencia a derecha e izquierda módulo un subgrupo $H$ de $G$ no coinciden, entonces estas relaciones no pueden inducir una estructura de grupo en el conjunto cociente. Sin embargo, cuando $\equiv_r = \equiv_l$ entonces la operación del grupo siempre se induce al cociente:

Teorema **9.** *Sea $H$ un subgrupo de un grupo $G$ tales que la congruencia a izquierda módulo $H$ y la congruencia a derecha módulo $H$ coinciden. Sea $\sim = \equiv_r = \equiv_l$. Entonces la operación del grupo se induce al cociente $G/\sim$, que por lo tanto es un grupo.*

*Demostración.* En este caso tendremos una relación de equivalencia $\sim$ en $G$ definida por

$$a \sim b \iff ab^{-1} \in H \iff a^{-1}b \in H.$$

Veamos que entonces la operación del grupo se induce al cociente $G/\sim$. Para ello sean $a, b, a', b' \in G$ tales que $a \sim a'$ y $b \sim b'$. Sólo debemos probar que $ab \sim a'b'$, o sea, que $(ab)(a'b')^{-1} \in H$.

Ahora bien, $(ab)(a'b')^{-1} = a(bb'^{-1})a'^{-1}$. Como $b \sim b'$, $bb'^{-1} \in H$, es decir, existe $h \in H$ tal que $bb'^{-1} = h$. Luego

$$(ab)(a'b')^{-1} = aha'^{-1}$$

Por otra parte, $ah \in aH = [a]_l$. Pero como la congruencia a derecha e izquierda módulo $H$ coinciden, $[a]_l = [a]_r = Ha$. Con lo cual existirá $h' \in H$ tal que $ah = h'a$. Luego

$$(ab)(a'b')^{-1} = aha'^{-1} = h'aa'^{-1}$$

Finalmente, como $a \sim a'$, $aa'^{-1} \in H$ de donde concluimos que $(ab)(a'b')^{-1} \in H$ y entonces $ab \sim a'b'$ como queríamos probar. □

En resumen, uniendo los resultados del Lema 7 y del Teorema 9, tenemos:

Teorema **10.** *Sea $\sim$ una relación de equivalencia en $G$. Entonces $G/\sim$ es un grupo con la operación que se induce de $G$ si y sólo si existe un subgrupo $H$ de $G$ para el cual $\sim = \equiv_r = \equiv_l$ módulo $H$.*

Definición **5.** *Un subgrupo $N$ de un grupo $G$ para el cual las congruencias a derecha e izquierda módulo $N$ coinciden se denomina un **subgrupo normal** de $G$. Se denota $N \triangleleft G$. El subgrupo cociente $G/\sim$, donde $\sim$ es la congruencia a derecha o izquierda módulo $N$, se denota por $G/N$.*

Teorema **11** (Caracterización de los subgrupos normales)**.** *Sea $G$ un grupo y $N$ un subgrupo de $G$. Entonces son equivalentes:*

1. *$N$ es un subgrupo normal de $G$.*
2. *para cada $a \in G$, $aN = Na$.*
3. *para cada $a \in G$, $aNa^{-1} \subset N$, donde $aNa^{-1} = \{ana^{-1} : n \in N\}$.*
4. *para cada $a \in G$, $aNa^{-1} = N$.*

*Demostración.* La equivalencia entre 1 y 2 es inmediata del Lema 8 y de la definición de subgrupo normal.

A partir de 2, el item 3 también se deduce fácilmente: si $n \in N$, como $aN = Na$, existe $n' \in N$ tal que $an = n'a$, de donde $ana^{-1} = n' \in N$. O sea, para $n \in N$ arbitrario, $ana^{-1} \in N$, de donde $aNa^{-1} \subset N$.

Supongamos que vale 3 y veamos que vale 4. Sólo resta probar que $N \subset aNa^{-1}$ para cada $a \in G$. Fijemos por lo tanto $a \in G$ y sea $n \in N$ cualquiera. Pongamos $n' = a^{-1}na$. Observemos que $n' = bnb^{-1}$, para $b = a^{-1} \in G$. Como por hipótesis $bNb^{-1} \subset N$ para cualquier $b \in G$, concluimos que $n' \in N$. Luego $n = an'a^{-1} \in aNa^{-1}$ como queríamos ver.

Veamos finalmente que si $aNa^{-1} = N$ para cada $a \in G$, entonces $N$ es un subgrupo normal de $G$, o equivalentemente que $aN = Na$ para cada $a \in G$. En efecto, sea $n \in N$. Entonces $ana^{-1} = n' \in N$, de donde $an = n'a$. Concluimos que $an \in Na$, o sea, $aN \subset Na$. Con un razonamiento análogo (aplicando la hipótesis a $a^{-1}$ en vez de $a$), se obtiene $Na \subset aN$, lo que completa la prueba. □

Ejemplos **4.**

1. Cualquier subgrupo de un grupo abeliano $G$ es normal. En efecto, tomemos un subgrupo $N$ cualquiera de $G$ y fijemos $a \in G$ cualquiera. Si $n \in N$ es arbitrario, entonces $an = na$, de donde $ana^{-1} = n \in N$. O sea, $aNa^{-1} \subset N$.

2. Consideremos el subgrupo cíclico $K$ generado por $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ en $S_3$ (el grupo de biyecciones de $\{1, 2, 3\}$ en sí mismo). Entonces puede verse que $K$ es un subgrupo normal de $S_3$ (ejercicio). Observemos que $S_3$ no es abeliano.

3. Sea $AGl(n)$ el conjunto de transformaciones afines de $\mathbb{R}^n$, o sea, de la forma $f : \mathbb{R}^n \to \mathbb{R}^n$ dada por $f(x) = Ax + b$ donde $A \in Gl(n)$ es una transformación lineal invertible y $b \in \mathbb{R}^n$ es un vector fijo. Es fácil ver que las transformaciones afines son biyectivas, y por lo tanto $AGl(n) \subset \mathcal{B}(\mathbb{R}^n)$, el conjunto de biyecciones de $\mathbb{R}^n$. Veamos que es un subgrupo. Para ello observemos que

$$f(x) = y \;\Leftrightarrow\; Ax + b = y \;\Leftrightarrow\; x = A^{-1}y - A^{-1}b$$

con lo cual $f^{-1}(x) = A^{-1}x + b'$, con $b' = -A^{-1}b$. Luego si $g(x) = Bx + c$, tenemos

$$g \circ f^{-1}(x) = BA^{-1}x + (Bb' + c).$$

Como $BA^{-1}$ es una matriz invertible y $Bb' + c \in \mathbb{R}^n$, resulta $g \circ f^{-1} \in AGl(n)$.

Luego $(AGl(n), \circ)$ es un grupo. Sea $T(\mathbb{R}^n)$ el conjunto de traslaciones, o sea transformaciones de la forma $T_v(x) = x + v$. Es fácil ver que $T_v^{-1} = T_{-v}$ y por lo tanto $T_w \circ T_v^{-1} = T_{w-v} \in T(\mathbb{R}^n)$. Luego $T(\mathbb{R}^n)$ es un subgrupo de $AGl(n)$. Veamos que es un subgrupo normal. Si $f \in AGl(n)$ está dada por $f(x) = Ax + b$ y $T_v$ es una traslación cualquiera, entonces

$$f \circ T_v \circ f^{-1}(x) = A(A^{-1}x + b' + v) = x + Ab' + Av = T_{-b+Av} \in T(\mathbb{R}^n).$$

Concluimos que $fT(\mathbb{R}^n)f^{-1} \subset T(\mathbb{R}^n)$.

Una forma simple de obtener subgrupos normales es a través del núcleo de un homomorfismo.

Recordemos que si $G$ y $G'$ son dos grupos, un homomorfismo de $G$ en $G'$ es una función $f : G \to G'$ tal que

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

para cada $x, y \in G$. En teoría de grupos algunos homomorfismos reciben nombres particulares:

- Si $f$ es un homomorfismo inyectivo, se denomina un **monomorfismo**.
- Si $f$ es un homomorfismo sobreyectivo, se denomina un **epimorfismo**.
- Si $f$ es un homomorfismo biyectivo, se denomina un **isomorfismo**, y si $G' = G$ $f$ se dice un **automorfismo**.

Teorema **12.** *Sea $f : G \to G'$ un homomorfismo y sea $\ker(f) = \{x \in G : f(x) = e_{G'}\}$ el núcleo de $f$. Entonces:*

1. *$\ker(f)$ es un subgrupo normal de $G$.*
2. *$f$ es un monomorfismo si y sólo si $\ker(f) = \{e_G\}$.*

*Demostración.* 1. Sea $f : G \to G'$ un homomorfismo de grupos. Veamos primero que $\ker(f)$ es un subgrupo de $G$. En efecto, si $g_1, g_2 \in \ker(f)$ entonces

$$f(g_1 g_2^{-1}) = f(g_1)f(g_2^{-1}) = f(g_1)f(g_2)^{-1} = e_{G'}e_{G'}^{-1} = e_{G'} \implies g_1 g_2^{-1} \in \ker(f).$$

Para ver que $\ker(f)$ es un subgrupo normal de $G$, consideremos $a \in G$ cualquiera y $b \in \ker(f)$. Entonces $f(aba^{-1}) = f(a)f(b)f(a)^{-1} = f(a)e_{G'}f(a)^{-1} = e_{G'}$. Luego $aba^{-1} \in \ker(f)$.

2. Supongamos que $f : G \to G'$ es un monomorfismo. Entonces si $g \in \ker(f)$, $f(g) = e_{G'}$. Pero $f(e_G) = e_{G'}$ y como $f$ es inyectivo deberá ser $g = e_G$. Luego $\ker(f) = \{e_G\}$.

   Recíprocamente, supongamos que $\ker(f) = \{e_G\}$. Sean $a, b \in G$ tales que $f(a) = f(b)$. Entonces

$$f(a)f(b)^{-1} = e_{G'} \implies f(a)f(b^{-1}) = e_{G'} \implies f(ab^{-1}) = e_{G'} \implies ab^{-1} \in \ker(f).$$

   Luego $ab^{-1} = e_G$, o sea $a = b$ y entonces $f$ es inyectiva.

□

Para poder construir más ejemplos de grupos cociente necesitamos de un resultado fundamental, el denominado *Primer Teorema de Isomorfismo*:

Teorema **13** (Primer Teorema de Isomorfismo)**.** *Si $f : G \to H$ es un epimorfismo, entonces $G/\ker(f)$ es isomorfo a $H$.*

*Demostración.* Supongamos que $f : G \to H$ es un epimorfismo y construyamos la aplicación

$$\overline{f} : G/\ker(f) \to H$$

dada por $\overline{f}(\overline{a}) = f(a)$.

Veamos primero que $\overline{f}$ está bien definida, esto es, si $a \equiv b\,(\ker(f))$ entonces $f(a) = f(b)$. En efecto, si $a \equiv b\,(\ker(f))$, entonces $ab^{-1} \in \ker(f)$. Luego

$$f(ab^{-1}) = e_H \;\Rightarrow\; f(a)f(b)^{-1} = e_H \;\Rightarrow\; f(a) = f(b).$$

Como $f$ es un epimorfismo, $\overline{f}$ también será una aplicación sobreyectiva (pues dado $h \in H$, si $a \in G$ es tal que $f(a) = h$, entonces $\overline{f}(\overline{a}) = f(a) = h$).

Veamos entonces que $\overline{f}$ es un monomorfismo. Primero, tenemos que

$$\overline{f}(\overline{a} \cdot \overline{b}) = \overline{f}(\overline{ab}) = f(ab) = f(a)f(b) = \overline{f}(\overline{a})\overline{f}(\overline{b})$$

y por lo tanto $\overline{f}$ es un homomorfismo. Por otra parte,

$$\overline{a} \in \ker(\overline{f}) \;\Leftrightarrow\; \overline{f}(\overline{a}) = f(a) = e_H \;\Leftrightarrow\; a \in \ker(f) = \overline{e} \;\Leftrightarrow\; \overline{a} = \overline{e}.$$

Luego $\ker(\overline{f}) = \{\overline{e}\}$ como queríamos ver. □

Ejemplos **5.**

1. Consideremos el homomorfismo $f : \mathbb{Z} \to \mathbb{Z}_m$ tal que $f(k) = \overline{k}$. Entonces es claro que $f$ es un epimorfismo y $f(k) = \overline{0}$ si y sólo si $k$ es múltiplo de $m$, es decir, $\ker f = \langle m \rangle$. Luego $\mathbb{Z}_m \cong \mathbb{Z}/\langle m \rangle$. En realidad el isomorfismo $\overline{f}$ construido en la demostración del Teorema 13 es la identidad.

2. Sea $H = \langle i \rangle$ el subgrupo cíclico de $(\mathbb{C}^*, \cdot)$ generado por la unidad imaginaria $i$. Consideremos la función $f : \mathbb{Z} \to H$ dada por $f(k) = i^k$. Entonces es claro que $f$ es sobreyectiva. Más aún, $f$ es un homomorfismo de grupos. En efecto,

   $$f(k_1 + k_2) = i^{k_1+k_2} = i^{k_1} i^{k_2} = f(k_1)f(k_2).$$

   Luego $f$ es un epimorfismo. Además $\ker(f) = \{k \in \mathbb{Z} : i^k = 1\} = \{4k : k \in \mathbb{Z}\} = \langle 4 \rangle$. Luego

   $$\langle i \rangle \cong \mathbb{Z}/\langle 4 \rangle = \mathbb{Z}_4.$$

3. Consideremos la circunferencia $S^1$ con el producto inducido por $\mathbb{C}^*$. Hemos visto que la aplicación $f : \mathbb{R} \to S^1$ dada por $f(\theta) = \cos(2\pi\theta) + i\,\mathrm{sen}(2\pi\theta)$ es un epimorfismo. Por lo tanto $S^1$ es isomorfo a $\mathbb{R}/\ker(f)$. Ahora bien, $\theta \in \ker(f)$ si y sólo si $\cos(2\pi\theta) + i\,\mathrm{sen}(2\pi\theta) = 1$, lo que ocurre si y sólo si $\theta = k$ para $k \in \mathbb{Z}$. Luego $\ker(f) = \mathbb{Z}$ y por lo tanto $S^1 \cong \mathbb{R}/\mathbb{Z}$,

4. Consideremos la aplicación $\pi : AGl(n) \to Gl(n)$ dada por $\pi(f) = A$, donde $f(x) = Ax + b$. Observemos que $\pi$ es un homomorfismo. En efecto, si $f(x) = Ax+b$ y $g(x) = Bx+c$, entonces $f \circ g(x) = ABx+Ac+b$, y por lo tanto $\pi(f \circ g) = AB = \pi(f)\pi(g)$. Claramente es un epimorfismo, pues dada $A \in Gl(n)$, $f(x) = Ax \in AGl(n)$ y $\pi(f) = A$. Finalmente, si $f(x) = Ax + b$ tenemos que

   $$f \in \ker(\pi) \;\Leftrightarrow\; \pi(f) = A = Id \;\Leftrightarrow\; f(x) = x + b$$

   o sea, $\ker(\pi) = T(\mathbb{R}^n)$. Luego $Gl(n) \cong AGl(n)/T(\mathbb{R}^n)$.

## 4. Propiedades y clasificación de los grupos cíclicos.

En esta sección afrontaremos por primera vez un problema de clasificación, Ya hemos mencionado repetidamente que en el estudio de cualquier estructura algebraica la noción de isomorfismo nos permite clasificar estas estructuras, es decir, dividirlas en clases de equivalencia cuyos elementos comparten propiedades comunes. Sin embargo en general es un problema muy dificil (si no imposible) describir un representante particular de cada una de estas clases. En el caso de los grupos cíclicos el problema es relativamente sencillo. Como veremos a continuación, un grupo cíclico es isomorfo a $\mathbb{Z}$ o es isomorfo a algún $\mathbb{Z}_m$.

Teorema **14.** *Sea $f : G \to G'$ un homomorfismo de grupos. Si $G$ es un grupo cíclico, entonces $f(G)$ es un subgrupo cíclico de $G'$ cuyos generadores son las imágenes de los generadores de $G$.*

*Demostración.* Supongamos que $G$ es cíclico y $a$ es un generador de $G$. Hemos visto en la práctica $4$ que $f(G)$ es un subgrupo de $G'$. Veamos que $f(G) = \langle f(a)\rangle$. En efecto, dado $k \in \mathbb{Z}$, $f(a)^k = f(a^k) \in f(G)$, luego $\langle f(a)\rangle \subset f(G)$.

Recíprocamente, si $g' \in f(G)$ existe $g \in G$ tal que $f(g) = g'$. Pero como $G = \langle a\rangle$, existirá $k \in \mathbb{Z}$ tal que $g = a^k$. Luego $g' = f(a^k) = f(a)^k \in \langle f(a)\rangle$.

Dejamos como ejercicio probar que si $b'$ es cualquier otro generador de $\langle f(a)\rangle$, entonces existe $b \in G$ tal que $f(b) = b'$ y $b$ es un generador de $G$. □

Corolario **15.** *Sea $f : G \to G'$ un isomorfismo de grupos. Entonces para cada $a \in G$, $o(a) = o(f(a))$.*

*Demostración.* Como $f$ es un isomorfismo, por el Teorema 14 es fácil ver que $f : \langle a\rangle \to \langle f(a)\rangle$ es un isomorfismo. Luego los dos grupos tienen el mismo cardinal, y por lo tanto el orden de $a$ y de $f(a)$ coindicen. □

Teorema **16.** *Sea $G$ un grupo cíclico. Entonces $G$ es isomorfo a alguno de los siguientes grupos:*

1. *$(\mathbb{Z}, +)$ si $o(G)$ es infinito.*
2. *$(\mathbb{Z}_m, +)$, para algún $m \in \mathbb{N}$, si $o(G) = m$.*

*Demostración.* Sea $G$ un grupo cíclico y sea $a$ un generador de $G$. Consideremos la aplicación $f : \mathbb{Z} \to G$ dada por $f(a) = a^k$. Es fácil ver que $f$ es un homomorfismo de grupos y claramente $f$ es sobre, por la definición misma de grupo cíclico.

Si $\ker(f) = \{0\}$, entonces $f$ es además un monomorfismo y por lo tanto un isomorfismo. Es decir, $G \cong \mathbb{Z}$.

Supongamos entonces que $\ker(f)$ no es trivial. Por el Lema 4 $\ker f = \langle m\rangle$ para algún $m \in \mathbb{Z}$. Luego $G \cong \mathbb{Z}/\langle m\rangle = \mathbb{Z}_m$.

En este caso, podemos dar explícitamente el isomorfismo siguiendo la prueba del Teorema 13:

$$\overline{f} : \mathbb{Z}_m \to G, \quad \overline{f}(\overline{k}) = a^k.$$

□

Corolario **17.** *Todo subgrupo de un grupo cíclico es cíclico.*

*Demostración.* Supongamos que $G$ es cíclico, $a$ es un generador de $G$ y consideremos el epimorfismo $f : \mathbb{Z} \to G$ dado por $f(k) = a^k$. Si $< G$ es un subgrupo de $G$, entonces $S' = f^{-1}(S)$ es un subgrupo de $\mathbb{Z}$. Como $S = f(S')$ y $S'$ es cíclico por el Teorema 4, $S$ debe ser un subgrupo cíclico por el Teorema 14. □

Ya hemos notado que un grupo cíclico puede tener más de un generador. Estudiaremos el problema de establecer los posibles generadores de un grupo cíclico a la luz del isomorfismo con $(\mathbb{Z}, +)$ o $(\mathbb{Z}_m, +)$. Recordemos que:

- En $\mathbb{Z}$, los únicos generadores son $1$ y $-1$.
- En $\mathbb{Z}_m$, $\overline{k}$ es un generador si y sólo si $mcd(k, m) = 1$.

Teorema **18.** *Sea $G = \langle a \rangle$ un grupo cíclico. Entonces*

1. *Si $G$ es infinito, $a$ y $a^{-1}$ son los únicos generadores de $G$.*
2. *Si $G$ es finito de orden $m$, entonces $a^k$ es un generador de $G$ si y sólo si $(k : m) = 1$.*

*Demostración.*

1. Supongamos que $G = \langle a \rangle$ es un grupo cíclico de orden infinito generado por $a \in G$. Entonces siguiendo la prueba del Teorema 16 tenemos que $f : \mathbb{Z} \to G$ dado por $f(k) = a^k$ es un isomorfismo.

   Por el Teorema 14, los únicos generadores de $G$ son $f(1)$ y $f(-1)$. Como $a = f(1)$, el otro generador es $f(-1) = f(1)^{-1} = a^{-1}$.

2. Supongamos ahora que $G = \langle a \rangle$ es un grupo cíclico de orden finito $m$. Nuevamente, tenemos un isomorfismo $f : \mathbb{Z}_m \to G$ dado por $f(\overline{k}) = a^k$. Por el Teorema 14, los generadores de $G$ son $f(\overline{k})$ tales que $mcd(k, m) = 1$. En particular, como $a = f(\overline{1})$, los generadores de $G$ son los elemenos de la forma $a^k$ con $mcd(k, m) = 1$.

□

Corolario **19.** *Si un grupo cíclico $G$ tiene orden $p$, con $p$ primo, entonces $G$ no tiene subgrupos propios.*

*Demostración.* Si $G$ es cíclico de orden $p$, entonces es isomorfo a $\mathbb{Z}_p$. Por lo tanto basta probar que $\mathbb{Z}_p$ no tiene subgrupos propios.

Supongamos que $S$ es un subgrupo de $\mathbb{Z}_p$. Entonces por el Corolario 17 $S$ debe ser un subgrupo cíclico de $\mathbb{Z}_p$. Es decir, existe $\overline{a} \in \mathbb{Z}_p$ tal que $S = \langle \overline{a} \rangle$. Pero en $\mathbb{Z}_p$ todo elemento $\overline{k} \neq \overline{0}$ es un generador de $\mathbb{Z}_p$. Luego $S = \langle \overline{0} \rangle = \{\overline{0}\}$ o $S = \mathbb{Z}_p$. □

El análisis desarrollado hasta acá debería habernos convencido que para estudiar cualquier propiedad de un grupo cíclico basta conocer las propiedades de los grupos aditivos $\mathbb{Z}$ y $\mathbb{Z}_m$.

Nos interesa ahora caracterizar el orden de un elemento $a$ de un grupo $G$ cualquiera, no necesariamente cíclico. Por definición, $o(a)$ es el orden del subgrupo cíclico generado por $a$, $H = \langle a \rangle \subset G$. Tenemos:

Teorema **20.** *Sea $G$ un grupo y $a \in G$.*

1. *$a$ tiene orden infinito si y sólo si vale: [$a^k = e$ si y sólo si $k = 0$]. En ese caso, los elementos $a^k$ con $k \in \mathbb{Z}$ son todos distintos entre sí.*

2. *$a$ tiene orden finito si y sólo si existe $m \in \mathbb{N}$ tal que $a^m = e$. En este caso, $o(a) = \min\{k \in \mathbb{N} : a^k = e\}$ y $a^r = a^s$ si y sólo si $r \equiv s\,(m)$. Es decir, $\langle a \rangle = \{e, a, a^2, \cdots, a^{o(a)-1}\}$.*

*Demostración.* 1. Supongamos que $a \in G$ tiene orden infinito. Entonces $H = \langle a \rangle$ es un grupo cíclico de orden infinito y existe un isomorfismo $f : \mathbb{Z} \to H$ tal que $f(1) = a$.

Observemos que $k1 = 0$ si y sólo si $k = 0$. Como $f(1) = a$, tenemos que $a^k = f(k1) = e$ si y sólo si $k1 \in \ker(f) = \{0\}$, si y sólo si $k = 0$.

Supongamos ahora que $a \in G$ es tal que $a^k = e$ si y sólo si $k = 0$. Veamos que $a$ tiene orden infinito. Supongamos por el contrario que $a$ tiene orden finito $m$. Entonces $H = \langle a \rangle$ es isomorfo a $\mathbb{Z}_m$ y existe un isomorfismo $f : \mathbb{Z}_m \to H$ tal que $f(\overline{1}) = a$. Como $m\overline{1} = \overline{m} = \overline{0}$, tenemos $a^m = f(m\overline{1}) = f(\overline{0}) = e$, lo que contradice la hipótesis. Luego $o(a)$ es infinito.

Finalmente, como $a^k = f(k1)$ para el isomorfismo $f : \mathbb{Z} \to H$, resulta claro que todos los elementos de la forma $a^k$ son distintos entre sí.

2. Supongamos ahora que $a \in G$ es un elemento de orden finito $m$. De la última parte de la demostración del item anterior tenemos que $a^m = e$. Veamos que $m$ es efectivamente el mínimo de los $k \in \mathbb{Z}$ que verifican $a^k = e$. En efecto, consideremos un isomorfismo $f : \mathbb{Z}_m \to \langle a \rangle$ tal que $f(\overline{1}) = a$. Como $k\overline{1} = \overline{0}$ si y sólo si $k$ es un múltiplo de $m$, tendremos que $a^k = e$ si y sólo si $k$ es un múltiplo de $m$. En particular, cualquier valor $k \in \mathbb{N}$ tal que $a^k = e$ verifica $k > m$ y por lo tanto $m = o(m) = \min\{k \in \mathbb{N} : a^k = e\}$.

Recíprocamente, si existe $m \in \mathbb{N}$ tal que $a^m = e$, entonces $a$ no puede tener orden infinito por el item anterior, y por lo tanto $a$ tiene orden finito. De la parte anterior de la prueba, resulta que el orden de $a$ es el mínimo $m$ con esta propiedad.

La última afirmación es inmediata del isomorfismo entre $\langle a \rangle$ y $\mathbb{Z}_m$. Dejamos los detalles como ejercicio.

□

Ejemplos **6.** 1. Consideremos $\mathbb{Z}_{10}$. Entonces $\overline{k}$ será un generador de $\mathbb{Z}_{10}$ si $mcd(k, 10) = 1$. O sea, los generadores de $\mathbb{Z}_{10}$ son $\overline{1}$, $\overline{3}$, $\overline{7}$ y $\overline{9}$. Por lo tanto los posibles subgrupos propios de $\mathbb{Z}_{10}$ son los subgrupos cíclicos generados por $\overline{2}$, $\overline{4}$, $\overline{5}$, $\overline{6}$ y $\overline{8}$.

Observemos que $o(\overline{2}) = 5$. En efecto, $1 \cdot \overline{2} = \overline{2}$, $2 \cdot \overline{2} = \overline{4}$, $3 \cdot \overline{2} = \overline{6}$, $4 \cdot \overline{2} = \overline{8}$ y $5 \cdot \overline{2} = \overline{10} = \overline{0}$. O sea $5$ es el menor entero $k$ tal que $k\overline{2} = \overline{0}$. Por lo tanto, en $\mathbb{Z}_{10}$, $\langle \overline{2} \rangle \cong \mathbb{Z}_5$. En particular, como $5$ es primo, de este isomorfismo conlcuimos que cualquier elemento en $\langle \overline{2} \rangle$ es un generador de $\langle \overline{2} \rangle$. En particular, como $\overline{4}, \overline{6}, \overline{8} \in \langle \overline{2} \rangle$, tendremos que

$$\langle \overline{2} \rangle = \langle \overline{4} \rangle = \langle \overline{6} \rangle = \langle \overline{8} \rangle \cong \mathbb{Z}_5.$$

Sólo nos queda explorar que ocurre $\overline{5}$. Aqui tendremos $2 \cdot \overline{5} = \overline{0}$ y por lo tanto $o(\overline{5}) = 2$. En este caso, $\langle \overline{5} \rangle \cong \mathbb{Z}_2$.

Concluimos que cualquier subgrupo propio de $\mathbb{Z}_{10}$ es isomorfo a $\mathbb{Z}_5$ o a $\mathbb{Z}_2$.

2. Consideremos el grupo $G_n = \{z \in \mathbb{C} :, z^n = 1\}$ de las raices $n$-ésimas de la unidad. Vimos que $G$ es un grupo cíclico de orden $n$, y por lo tanto $G_n \cong \mathbb{Z}_n$. Si $z_1 = 1_{\frac{2\pi}{n}}$, $z_1$ es un generador de $G_n$. Recordemos $G_n = \{z_1, \cdots, z_n\}$ y que $z_1^k = z_k$. Luego los generadores de $G_n$ son aquellos $z_k$ tales que $k$ y $n$ son coprimos.

   Por ejemplo, si $n$ es primo, cualquier raíz $n$-ésima de $1$ es un generador de $G_n$. Si $n = 4$, los generadores son $z_1$ y $z_3$, etc.

3. Consideremos el grupo $\mathrm{Aut}(\mathbb{Z})$ de automorfismos de $\mathbb{Z}$. En particular, como $\mathbb{Z}$ es un grupo cíclico generado por $\pm 1$ y un automorfismo envía generadores en generadores, tendremos que $f(1) = 1$ o $f(1) = -1$. Observemos que el valor de $f(1)$ determina completamente $f$, pues $f(k) = f(k \cdot 1) = kf(1)$. Es decir, si conocemos $f(1)$ sabemos quién es $f$. Por lo tanto hay sólo dos automorfismos posibles, $f_1$ tal que $f_1(1) = 1$, en cuyo caso $f_1(k) = k$ y por lo tanto $f_1 = Id$, o $f_2$ tal que $f_2(1) = -1$, en cuyo caso $f_2(k) = -k$, o sea $f_2 = -Id$. Observemos que $f_2 \circ f_2 = f_1$ y por lo tanto $\mathrm{Aut}(\mathbb{Z})$ es un grupo cíclico de orden $2$, cuyo generador es $f_2 = -Id$. Concluimos que $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

   Observemos que un grupo con dos elementos, digamos $G = \{e, a\}$ debe ser automaticamente isomorfo a $\mathbb{Z}_2$, pues $a^2 = e$ (no puede ser $a^2 = a$ pues podríamos cancelar y obtendríamos $a = e$).

4. Consideremos ahora el grupo $\mathrm{Aut}(\mathbb{Z}_4)$. Nuevamente $f$ queda determinado por $f(\overline{1})$. Como $\overline{1}$ es un generador de $\mathbb{Z}_4$, $f(\overline{1})$ también debe ser un generador, y por lo tanto tenemos nuevamente dos opciones: $f_1(\overline{1}) = \overline{1}$, o sea $f_1 = Id$, o $f_2(\overline{1}) = \overline{3}$. Luego $\mathrm{Aut}(\mathbb{Z}_4) = \{Id, f_2\} \cong \mathbb{Z}_2$.

5. Consideremos finalmente el grupo $\mathrm{Aut}(\mathbb{Z}_5)$. Aquí cualquier elemento es un generador, y por lo tanto tenemos cuatro posibles automorfismos: $f_1 = Id$, $f_j$, $j = 2, 3, 4$ tal que $f_j(\overline{1}) = \overline{j}$. Tomemos $f_3$ e intentemos determinar $f_3^k$. Tendremos

   *a*) $f_3^2(\overline{1}) = f_3 \circ f_3(\overline{1}) = f_3(\overline{3}) = f_3(3 \cdot \overline{1}) = 3 \cdot f_3(\overline{1}) = \overline{9} = \overline{4}$. Como $f_3^2$ es un automorfismo, está determinado por su valor en $\overline{1}$ y por lo tanto $f_3^2 = f_4$.

   *b*) $f_3^3(\overline{1}) = f_3 \circ f_4(\overline{1}) = f_3(\overline{4}) = 4 \cdot f_3(\overline{1}) = \overline{12} = \overline{2}$. Luego $f_3^3 = f_2$.

   *c*) Finalmente, $f_3^4(\overline{1}) = f_3 \circ f_2(\overline{1}) = f_3(\overline{2}) = 2 \cdot f_3(\overline{1}) = \overline{6} = \overline{1}$, luego $f_3^4 = Id = f_1$.

   Concluimos que $f_3$ es un elemento de orden $4$, y $\langle f_3 \rangle = \mathrm{Aut}(\mathbb{Z}_5)$, con lo cual $\mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4$.

Ejercicio **2.** *Probar que si $p$ es primo,* $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$.

## 5. El teorema de Lagrange y algunas aplicaciones

Retomemos las congruencias a derecha e izquierda módulo un subgrupo $H$ de un grupo $G$. Recordemos que $a \equiv_r b\,(H)$ si $ab^{-1} \in H$ y la clase de equivalencia de $a$ es $[a]_r = Ha$, y que $a \equiv_l b\,(H)$ si $a^{-1}b \in H$ y la clase de equivalencia de $a$ es $[a]_l = aH$.

Estas clases suelen denominarse **coclases a derecha e izquierda** respectivamente determinadas por el subgrupo $H$.

Hemos visto que $[a]_r = [a]_l$ para cada $a \in G$ si y sólo si $H$ es un subgrupo normal de $G$. Por lo tanto, para un subgrupo genérico $H$ de $G$, estas clases no conciden. Sin embargo, tienen algunas propiedadades comunes:

Teorema **21.** *Sea $H$ un subgrupo de un grupo $G$. Entonces:*

1. *El cardinal de cada coclase (a derecha o izquierda) coincide con el cardinal de $H$.*
2. *Un subgrupo $H$ de $G$ determina la misma cantidad de coclases a derecha que a izquierda en $G$ (es decir, el cardinal de los conjuntos cociente $G/\equiv_r$ y $G/\equiv_l$ es el mismo).*

*Demostración.* 1. Consideremos la función $\varphi : [a]_r \to H$ tal que $\varphi(b) = ba^{-1}$. Como cada $b \in [a]_r$ es de la forma $b = ha$ para algún $h \in H$, resulta claro que $\varphi$ está bien definida. Además es sobre, pues para cada $h \in H$, $ha \in [a]_r$ es tal que $\varphi(ha) = h$. Finalmente, $\varphi$ es inyectiva: si $\varphi(b) = \varphi(c)$, entonces $ba^{-1} = ca^{-1}$ y entonces $b = c$. Luego $\varphi$ es una biyección y por lo tanto el cardinal de $[a]_r$ coincide con el cardinal de $H$. De manera análga se prueba el resultado para $[a]_l$.

2. Sea ahora $\Psi : G/\equiv_r \to G/\equiv_l$ dada por $\Psi([a]_r) = [a^{-1}]_l$. Veamos primero que $\Psi$ está bien definida. Sean $a, b \in G$ tales que $a \equiv_r b$, o sea, $ab^{-1} \in H$. Entonces $(ab^{-1})^{-1} \in H$ con lo cual $ba^{-1} \in H$. Pero $ba^{-1} = (b^{-1})^{-1}(a^{-1})$ con lo cual $b^{-1} \equiv_l a^{-1}$. Es decir, $[a]_r = [b]_r$ entonces $[a^{-1}]_l = [b^{-1}]_l$. Una vez que hemos probado que $\Psi$ está bien definida, es fácil ver (y lo dejamos como ejercicio) que $\Psi$ es biyectiva, y por lo tanto $G/\equiv_r$ y $G/\equiv_l$ tienen el mismo cardinal.

□

Todo grupo $G$ es la unión disjunta de las clases de equivalencia (a derecha o izquierda) dadas por la congruencia módulo $H$, siendo $H$ un subgrupo cualquiera de $G$. Las clases a derecha y a izquierda que determina $H$ pueden ser distintas, pero la cantidad de ellas es la misma. El número de clases distintas que determina un grupo $H$ juega un rol particular en el estudio sobre todo de grupos finitos. Se denomina **índice de $H$ en $G$** y se denota $[G : H]$.

El siguiente resultado establece una relación entre el orden de un grupo $G$ y de un subgrupo $H$ con el índice $[G : H]$. En particular, nos permitirá hacer una previsión sencilla sobre los posibles órdenes de los elementos de $G$:

Teorema **22** (Lagrange)**.** *Sea $H$ un subgrupo de un grupo $G$. Entonces $o(G) = [G : H]o(H)$. En particular, si $G$ es finito, entonces para cada $a \in G$, $o(a)$ divide a $o(G)$.*

*Demostración.* Elijamos un representante $a_i$ de cada clase de $\equiv_r$ módulo $H$, donde $i \in I$, siendo $I$ un conjunto de índices cuyo cardinal es $[G : H]$. Luego

$$G = \bigcup_{i \in I} Ha_i.$$

Como $a_i$ y $a_j$ son representantes de clases distintas si $i \neq j$, se tiene que en este caso $Ha_i \cap Ha_j = \emptyset$. Luego

$$o(G) = \sum_{i \in I} |Ha_j| = \sum_{i \in I} o(H) = o(H)[G : H]$$

como queríamos probar.

En el caso que $H = \langle a \rangle$, se tiene que $o(H) = o(a)$, y por lo tanto si $o(G)$ es finito, $o(a)$ debe dividir a $o(G)$. □

A partir del Teorema de Lagrange podemos generalizar el resultado del Corolario 19:

Teorema **23.** *Todo grupo de orden primo es cíclico y no tiene subgrupos propios.*

*Demostración.* Si $G$ es un grupo de orden primo $p$, entonces todo elemento $a \in G$ debe dividir a $p$. Luego su orden es $1$ o $p$. El único elemento de orden $1$ en un grupo es la identidad. Por lo tanto, todo elemento de $G$ tiene orden $p$, y por lo tanto $G$ es el grupo cíclico generado por $a$. □

Para finalizar esta Unidad analizaremos algunas aplicaciones de la teoría de grupos a la teoría de números analizando algunas propiedades de la aritmética modular.

Teorema **24** (Pequeño Teorema de Fermat)**.** *Sea $p$ un número primo. Entonces para todo entero $a$ no divisible por $p$ resulta $a^{p-1} \equiv 1\,(p)$.*

*Demostración.* Si $a$ no es divisible por $p$, entonces $\overline{a} \neq \overline{0}$. Luego $\overline{a}$ es un elemento del grupo multiplicativo $(\mathbb{Z}_p^*, \cdot)$, que es un grupo de orden $p - 1$. Por el Teorema de Lagrange, $o(\overline{a})$ divide a $p - 1$, es decir, existe $k \in \mathbb{N}$ tal que $p - 1 = ko(\overline{a})$ . Como $\overline{a}^{o(\overline{a})} = \overline{1}$, tenemos $a^{o(\overline{a})} \equiv 1\,(p)$ y por lo tanto $(a^{o(\overline{a})})^k \equiv 1\,(p)$ o sea $a^{p-1} \equiv 1\,(p)$. □

Como consecuencia inmediata del Teorema 24 obtenemos el siguiente corolario. Es interesante notar que ambos enunciados son en realidad equivalentes. Dejamos la prueba como **ejercicio**.

Corolario **25.** *Sea $p$ un número primo y $a \in \mathbb{Z}$ cualquiera. Entonces $a^p \equiv a\,(p)$.*

Ejemplo **7.** Aplicaremos el Pequeño Teorema de Fermat (PTF) para calcular de manera sencilla el resto de dividir $27^{2154}$ por $11$. Observemos que como $11$ es primo y $11 \nmid 27 = 3^3$, del PTF tendremos que $27^{10} \equiv 1\,(11)$. Pero entonces $27^{k10} \equiv 1^k\,(11)$ para cualquier $k \in \mathbb{Z}$. Escribamos $2154$ como $2154 = 215 \cdot 10 + 4$. Luego $27^{2154} = 27^{215 \cdot 10} \cdot 27^4$. Como $27^{215 \cdot 10} \equiv 1\,(11)$, resulta $27^{2154} \equiv 27^4\,(11)$. Ahora bien, $r_{11}(27) = 5$ y por lo tanto $27^4 \equiv 5^4\,(11)$. Ahora, $5^4 = 25^2$ y como $25 \equiv 3\,(11)$ tenemos

$$27^{2154} \equiv 27^4 \equiv 5^4 \equiv 25^2 \equiv 3^2 \equiv 9\,(11).$$

Concluimos que $r_{11}(27^{2154}) = 9$. □

Un segundo resultado fundamental de la aritmética modular es el denominado *Teorema Chino del Resto*. Este resultado permite resolver sistemas de ecuaciones lineales en congruencia:

$$\begin{cases} x & \equiv a_1 \, (m_1) \\ x & \equiv a_2 \, (m_2) \\ \vdots & \quad \vdots \\ x & \equiv a_r \, (m_r) \end{cases} \tag{3}$$

No es de esperar que estos sistemas tengan siempre solución. Consideremos por ejemplo el siguiente sistema simple:

$$\begin{cases} x & \equiv 2 \, (4) \\ x & \equiv 7 \, (10) \end{cases}$$

Si un tal $x$ existiese, debería ser de la forma $x = 4k_1 + 2$ y $x = 10k_2 + 7$ para algún par de enteros $k_1$ y $k_2$. Esto implica que existen enteros tales que

$$4k_1 + 2 = 10k_2 + 7 \quad \Leftrightarrow \quad 2(2k_1 - 5k_2) = 5$$

lo cual claramente no puede ocurrir, puesto que el lado izquierdo de la igualdad es siempre un número par, y el lado derecho es siempre impar.

Intentaremos desarrollar primeramente un criterio para determinar cuándo el sistema tiene solución. Más aún, a nivel de la aritmética modular, encontrar una solución de este sistema no significa simplemente encontrar un entero $x$ que las satisfaga a todas, sino que nuestro objetivo será determinarlo unívocamente múdulo algún entro $m$. Esto es, pretendemos reducir el sistema de ecuaciones a una ecuación lineal del tipo

$$x \equiv x_0 \, (m)$$

para algún $x_0$ y algún $m$.

Teorema **26** (Teorema Chino del Resto)**.** *Sean $m_1, m_2, \ldots, m_r$ números naturales coprimos dos a dos y sea $m$ su producto. Si $a_1, a_2, \ldots, a_r$ son números enteros cualesquiera, existe solución al sistema (3) y está unívocamente determinada módulo $m$. Esto es, si $x_0$ es una solución cualquiera de (3), entonces $x$ satisface $x \equiv x_0 \, (m)$. En particular, existe un único $x_0 \in \mathbb{Z}$ solución de (3) tal que $0 \leq x_0 < m$.*

*Demostración.* Comencemos suponiendo que $a_2 = a_3 = \cdots = a_r = 0$. Es decir, tenemos un sistema

$$S_1) \begin{cases} x & \equiv a_1 \, (m_1) \\ x & \equiv 0 \, (m_2) \\ \vdots & \quad \vdots \\ x & \equiv 0 \, (m_r) \end{cases}$$

Veamos que $S_1$ tiene solución. Sea $m' = m_2 \cdot m_3 \cdots m_r$. Observemos que $mcd(m', m_1) = 1$, pues de otra manera un divisor común debería dividir simultáneamente a $m_1$ y a alguno de los otros $m_j$, $j \geq 2$, (dado que los $m_j$ son coprimos dos a dos), y esto no puede ocurrir pues $mcd(m_1, m_j) = 1$ para cada $j = 2, \ldots, r$.

En particular, $m'$ es invertible en $\mathbb{Z}_{m_1}^*$. Por lo tanto existirá $v' \in \mathbb{Z}$ tal que $m'v' \equiv 1\,(m_1)$. Observemos que $m_j \mid m'v'$ para cada $j \geq 2$ pues $m_j \mid m'$. Luego $m'v' \equiv 0\,(m_j)$ para cada $j \geq 2$. Pongamos $x_1 = a_1 m'v'$. Tendemos entonces

$$m'v' \equiv 0\,(m_j) \;\Rightarrow\; x_1 \equiv 0\,(m_j), \quad \text{para todo } j = 2, \ldots, r.$$

Además

$$m'v' \equiv 1\,(m_1) \;\Rightarrow\; x_1 = a_1 m'v' \equiv a_1\,(m_1).$$

Luego $x_1$ es una solución de $S_1$.

De manera análoga podemos encontrar una solución $x_j$ de cada uno de los sistemas $S_j$ dados por

$$S_j) \begin{cases} x & \equiv a_j\,(m_j) \\ x & \equiv 0\,(m_i) \quad \forall\, i \neq j \end{cases}$$

Si ahora ponemos

$$x_0 = \sum_{j=1}^{r} x_j$$

tenemos que

$$x_j \equiv a_j\,(m_j), \quad x_i \equiv 0\,(m_j)\ \forall\, i \neq j \;\Rightarrow x_0 \equiv a_j\,(m_j).$$

Como esto es válido para cada $j$, tenemos que $x_0$ es solución de (3). Luego, tenemos que el sistema que estamos considerando es equivalente a un sistema más simple:

$$\begin{cases} x & \equiv a_1\,(m_1) \\ x & \equiv a_1\,(m_2) \\ \vdots & \quad\vdots \\ x & \equiv a_r\,(m_r) \end{cases} \iff \begin{cases} x & \equiv x_0\,(m_1) \\ x & \equiv x_0\,(m_2) \\ \vdots & \quad\vdots \\ x & \equiv x_0\,(m_r) \end{cases} \tag{4}$$

Veamos que este sistema es equivalente a la ecuación lineal $x \equiv x_0\,(m)$.

Observemos que si $x \equiv x_0\,(m)$, entonces $m \mid x - x_0$. Como $m_j \mid m$ resulta $m_j \mid x - x_0$ y por lo tanto $x \equiv x_0\,(m_j)$ para cada $j = 1 \ldots, r$. Esto es, $x$ es solución de (4).

Si ahora $x$ es solución de (4), tenemos que $m_j \mid x - x_0$ para cada $j = 1, \ldots, r$ . Como $mdc(m_i, m_j) = 1$ para cada $i \neq j$, tenemos que $m \mid x - x_0$ y por lo tanto $x \equiv x_0\,(m)$.

Concluimos que la solución del sistema está unívocamente determinada módulo $m$. Observando que $x_0 \equiv r_m(x_0)\,(m)$, vemos que hay una única solución entera $x_0' = r_m(x_0)$ tal que $0 \leq x_0' < m$. □

La prueba del Teorema Chino del Resto es constructiva y nos da un modo de encontrar una solución del sistema 3. Sin embargo, para ello necesitamos en cada paso encontrar el inverso de un elemento $\overline{a}$ en el monoide $\mathbb{Z}_m^*$, donde $a$ y $m$ son coprimos. Para ello recurrimos al denominado algoritmo de Euclides:

Teorema **27** (Algoritmo de Euclides)**.** *Sean $a, b \in \mathbb{N}$. Aplicamos reiteradamente el algoritmo de la división como sigue:*

$$\begin{aligned} a &= q_1 b + r_1 & 0 < r_1 < b \\ b &= q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 & 0 < r_3 < r_2 \end{aligned}$$

$$\dots$$

$$r_i = q_{i+2}r_{i+1} + r_{i+2} \quad 0 < r_{i+2} < r_{i+1}$$

$$\dots$$

$$\begin{aligned} r_{k-3} &= q_{k-1}r_{k-2} + r_{k-1} \quad 0 < r_{k-1} < r_{k-2} \\ r_{k-2} &= q_k r_{k-1} + r_k \qquad\quad 0 < r_{k-1} < r_{k-2} \\ r_{k-1} &= q_{k+1}r_k. \end{aligned}$$

*Entonces $r_k$, el último resto no nulo, es el máximo común divisor de $a$ y $b$.*

*Demostración.* Observemos primero que el algoritmo termina en una cantidad finita de pasos puesto que para cada $i$, $0 \leq r_{i+1} < r_i$ y por lo tanto en algún momento el resto debe ser cero (si no deberían existir infinitos números naturales menores que un número natural dado). Por otro lado, si recorremos el proceso anterior hacia arriba tenemos: $r_k \mid r_{k-1}$, y como $r_k \mid r_k$, y por lo tanto $r_k$ divide a $r_{k-2}$. Subiendo un renglón y aplicando la misma propiedad, vemos que $r_k$ divide a $r_{k-3}$. Siguiendo así hacia arriba, llegamos a que $r_k \mid b$ y $r_k \mid a$.

Supongamos ahora que $c \mid a$ y $c \mid b$. Entonces del primer renglón del algoritmo, $c \mid r_1$. Del segundo renglón tenemos $c \mid b$ y $c \mid r_1$, entonces $c \mid r_2$. Siguiendo así hacia abajo, llegamos a que $c \mid r_k$ como queríamos probar. □

Ejemplo **8.** Consideremos el sistema

$$S) \begin{cases} x \equiv 4\,(8) \\ x \equiv 10\,(35) \\ x \equiv 1\,(3) \end{cases}$$

La demostración del Teorema Chino del Resto nos da un modo de obtener una solución particular, y a partir de ella todas las soluciones del sistema $S$. Debemos considerar tres sistemas:

$$S_1) \begin{cases} x \equiv 4\,(8) \\ x \equiv 0\,(35) \\ x \equiv 0\,(3) \end{cases}, \quad S_2) \begin{cases} x \equiv 0\,(8) \\ x \equiv 10\,(35) \\ x \equiv 0\,(3) \end{cases}, \quad S_3) \begin{cases} x \equiv 0\,(8) \\ x \equiv 0\,(35) \\ x \equiv 1\,(3) \end{cases}$$

Sea $m_1' = 35 \cdot 3 = 105$. Tenemos que encontrar $v_1'$ tal que $m_1'v_1' \equiv 1\,(8)$. Comencemos observando que $105 = 13 \cdot 8 + 1$ y entonces $105 \equiv 1\,(8)$. Por lo tanto $v_1' = 1$ y $x_1 = m_1'v_1'a_1 = 105 \cdot 4 = 420$. Observemos que efectivamente

$$420 = 12 \cdot 35, \quad 420 = 140 \cdot 3, \quad 420 = 52 \cdot 8 + 4$$

y por lo tanto $x_1 \equiv 4\,(8)$, $x_1 \equiv 0\,(35)$, $x_1 \equiv 0\,(3)$. O sea que $x_1$ es solución de $S_1$. Para hallar las soluciones de $S_2$ consideremos $m_2' = 8 \cdot 3 = 24$. Encontremos $v_2'$ tal que $24v_2' \equiv 1(35)$. Recordemos que $v_2'$ es el coeficiente de $24$ que se obtiene aplicando el algoritmo de Euclides para encontrar $mcd(24, 35)$. Tenemos:

$$\begin{aligned} 35 &= 24 \cdot 1 + 11 \\ 24 &= 11 \cdot 2 + 2 \\ 11 &= 5 \cdot 2 + 1 \end{aligned}$$

de donde

$$1 = 11 - 5 \cdot 2 = 11 - 5 \cdot (24 - 11 \cdot 2) = -5 \cdot 24 + 11 \cdot 11 = -5 \cdot 24 + 11 \cdot (35 - 24) = -16 \cdot 24 + 11 \cdot 35.$$

Luego $v_2' = -16$ y $x_2 = 24 \cdot (-16) \cdot 10 = -3840$. De manera análoga se obtiene una solución $x_3 = 280$ de $S_3$. Luego una solución $x_0$ de $S$ es

$$x_0 = 420 - 3840 + 280 = -3140.$$

Ahora bien, $m = 8 \cdot 25 \cdot 3 = 840$, y por lo tanto la única solución $x_0'$ con $0 \leq x_0' < m$ es $r_{840}(-3140) = 220$. Concluimos finalmente que las soluciones de $S$ están caracterizadas por $x \equiv 220\,(840)$.

Ejemplo **9.** Para vender una enciclopedia cuyo precio es menor a \$10.000 una librería ofrece los siguientes planes de pago:

1. anticipo de \$200 y cuotas mensuales de \$180.
2. anticipo de \$300 y cuotas mensuales de \$250.
3. anticipo de \$370 y cuotas mensuales de \$490.

¿Cuál es el precio total de la enciclopedia?
*Solución:* Supongamos que $P$ es el precio de la obra. Entonces cualquiera de los planes se calcula mediante la fórmula $P = a + cn$, donde $a$ es el anticipo, $c$ es el monto de cada cuota y $n$ es el número de cuotas, que claramente varía de plan a plan. Por lo tanto nuestras incógnitas son $P$ y $n_1$, $n_2$, $n_3$, donde $n_i$ es el número de cuotas del plan $i$. En principio pareciera que tenemos un sistema de ecuaciones a coeficientes enteros (denominadas *ecuaciones diofánticas*) en las incógnitas $P$, $n_1$, $n_2$, $n_3$. Pero si observamos mejor, vemos que

$$P - a = cn \quad \Leftrightarrow \quad P \equiv a\,(c).$$

Es decir, reduciendo el problema a un sistema de ecuaciones en congruencia podemos obviar las incógnitas $n_i$, cuyo valor estará determinado una vez que conozcamos $P$ (aunque en el enunciado del problema no se pide hallar la cantidad de cuotas de cada plan). Debemos entonces resolver

$$S) \begin{cases} P & \equiv 200\,(180) \\ P & \equiv 300\,(250) \\ P & \equiv 370\,(490) \end{cases}$$

Lo primero que debemos observar es que $180$, $250$ y $490$ no son coprimos dos a dos (pues $10$ es un divisor común de todos). Sin embargo, observemos que

$$y \equiv kn\,(km) \;\Leftrightarrow\; y - kn = lkm \;\Leftrightarrow \frac{y}{k} - n = lm \;\Leftrightarrow \frac{y}{k} \equiv n\,(m)$$

Pongamos entonces $x = P/10$. Tenemos que $P$ será solución de $S$ si y sólo si $x$ es solución de

$$S') \begin{cases} x & \equiv 20\,(18) \\ x & \equiv 30\,(25) \\ x & \equiv 37\,(49) \end{cases}$$

En este caso $18$, $25$ y $49$ sí son primos relativos dos a dos, pues $18 = 2 \cdot 3^2$, $25 = 5 \cdot 5$, $49 = 7 \cdot 7$. Siguiendo el procedimiento del ejemplo anterior obtenemos que $22430$ es una solución de $S'$. En este caso $m = 22050$ y es fácil comprobar que $22430 \equiv 380\,(22050)$. Con lo cual $x_0 = 380$ es la solución más pequeña que podemos encontrar. Observemos que cualquier otra solución diferirá de $x_0$ en un múltiplo de $22050$ y por lo tanto $x_0$ es la única solución menor que $1000$. Luego $P = 3800$ es la única solución de $S$ menor que $10000$

Ejemplo **10. El algoritmo de encriptación RSA.** El algoritmo RSA es una forma muy sencilla de encriptar datos que se utiliza aún hoy. Se basa en la existencia de dos claves: una clave pública que todos conocen y con la cual pueden cifrar sus mensajes, y una clave privada que se utiliza para descifrarlos.

Supongamos que una persona $A$ decide mandar un mensaje a una persona $B$, y quiere que sólo $B$ lo pueda leer. La persona $B$ elige dos número primos $p$ y $q$ y considera un número $e < (p-1)(q-1)$ que sea coprimo con $(p-1)(q-1)$. En un principio sólo $B$ conoce estos tres números, pero comunica a $A$ los números $e$ y $n = pq$. El par $(n, e)$ constituye la clave pública, a la que todos tienen acceso. A los fines prácticos, para que el algoritmo sea eficiente, los números $p$, y $q$ y $e$ deben ser muy grandes (en general se utilizan núneros de más de 170 cifras). Para ejemplificarlo, tomemos los siguientes números:

$$p = 3,\ q = 11,\ n = pq = 33,\ (p-1)(q-1) = 20,\ e = 7.$$

Ahora $A$ convierte su mensaje en un número $M < n$ y lo transforma en el único número $c < n$ tal que $c \equiv M^e\,(n)$. En vez de enviar el mensaje $M$ completo, envía sólo el número $c$ que $B$ deberá descifrar. Supongamos siguiendo con el ejemplo que el mensaje sin cifrar es $M = 15$. Entonces

$$M^e = 15^7 \equiv 27\,(33)$$

con lo cual el mensaje cifrado es $c = 27$.

Observemos que en el camino alguien podría hacker el mensaje, y así tendría acceso al número $c$. No entendría lo que $A$ efectivamente está enviando porque el mensaje está cifrado. Aún teniendo acceso a la clave pública $(n, e)$, debería hallar $M$ tal que $c \equiv M^e\,(n)$. Ahora bien, si este problema en una ecuación normal se resuelve de manera sencilla aplicando la raíz $e$-ésima a $c$ para recuperar $M$, en la aritmética modular esto no es cierto. Como ejemplo podemos observar que $1 \equiv 2^2\,(3)$, pero no es cierto que $\sqrt{1} \equiv 2\,(3)$. En nuestro ejemplo, $\sqrt[7]{27}$ ni siquiera es un número entero.

Para descifrar el mensaje $B$ utiliza la clave privada, que está dada por el único $d < ((p-1)(q-1))$ tal que $ed \equiv 1\,((p-1)(q-1))$. Observemos que como el $e$ elegido originalmente es coprimo con el módulo, el número $d$ buscado siempre existe. En nuestro ejemplo, $d = 3$, pues $de = 21 \equiv 1\,(20)$.

Ahora bien, como $de \equiv 1\,((p-1)(q-1))$ tenemos que

$$de = \lambda(p-1)(q-1) + 1 = \lambda_1(p-1) + 1 = \lambda_2(q-1) + 1$$

donde $\lambda_1 = \lambda(q-1)$ y $\lambda_2 = \lambda(p-1)$. Por lo tanto

$$c^d = M^{de} = (M^{p-1})^{\lambda} M \equiv M\,(p)$$

pues por el Pequeño Teorema de Fermat $M^{p-1} \equiv 1\,(p)$. Con el mismo argumento resulta $c^d \equiv M\,(q)$. Es decir que $M$ es solución del sistema

$$\begin{cases} x = c^d\,(p) \\ x = c^d\,(q) \end{cases}$$

que por el Teorema Chino del resto es única módulo $n = pq$.

En nuestro ejemplo, $c^d = 27^3 = 19683 \equiv 15\,(33)$.

Observemos que como $n = pq$ y la factorización en números primos es única, conociendo $n$ debería ser sencillo recuperar los primos $p$ y $q$. La eficacia de este algoritmo se basa en que en realidad es muy difícil factorizar un número muy grande en factores primos. □