Esta operación da una estructura de monoide (sin elemento neutro) en $L(X)$. Llamamos a $L(X)$ el *monoide libre sobre* X.

Si X es un conjunto unitario, $L(X)$ se identifica con $(\mathbb{N}, +)$. Si X tiene por lo menos dos elementos, pruebe que $L(X)$ no es conmutativo.

1.3 Subgrupos. Subgrupos normales

En general, dado un conjunto G, uno puede obtener toda una familia de otros conjuntos simplemente mirando los subconjuntos de G. Si además G tiene estructura de grupo, uno se puede preguntar cómo obtener "gratis", a partir de G, una familia de grupos de manera análoga a la situación conjuntista.

Definición 1.3.1. Dado un grupo $(G, \cdot)$, un *subgrupo* de G es un subconjunto $H \subseteq G$ tal que $(H, \cdot|_{H\times H})$ es un grupo o, equivalentemente, si

(a) $\cdot$ es cerrado en H, esto es, para todo $h_1, h_2 \in H$, se tiene que $h_1 \cdot h_2 \in H$;
(b) $e \in H$; y
(c) para todo $h \in H$, $h^{-1} \in H$.

Observación. La condición *(b)* implica que $H \neq \varnothing$, a su vez las condiciones *(a)* y *(c)* junto con $H \neq \varnothing$ implican la condición *(b)*, por lo tanto en la definición de subgrupo se puede cambiar *(b)* por $H \neq \varnothing$.

Ejemplos.
1. Si $n \in \mathbb{N}$, sea $G_n = \{w \in \mathbb{C} : w^n = 1\}$. Entonces $(G_n, \cdot)$ es un subgrupo de $(\mathbb{C} - \{0\}, \cdot)$.

2. Si $n \in \mathbb{N}$, el conjunto $n\mathbb{Z} = \{nk \ / \ k \in \mathbb{Z}\}$ de los múltiplos de n es un subgrupo de los enteros $(\mathbb{Z}, +)$.

3. Si $G = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \cdots, \overline{5}\}$, entonces $H_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ y $H_2 = \{\overline{0}, \overline{3}\}$ son subgrupos de G.

4. Si $(G, \cdot)$ es un grupo, G y $\{e\}$ son siempre subgrupos. Si p es un número primo y $G = \mathbb{Z}_p$ se verá fácilmente luego que estos dos subgrupos triviales son los únicos subgrupos que tiene $\mathbb{Z}_p$.

5. Sea $X = \{1, 2, 3, ..., n\}$ y $G = \mathcal{S}_n$ el conjunto de las permutaciones de X. Si $1 \leq i \leq n$, el conjunto de permutaciones que fijan el elemento i de X, esto es, $H_i = \{g \in G : g(i) = i\}$, es un subgrupo de G. ¿Cuántos elementos tiene G? ¿Cuántos elementos tiene H_i?

6. Sea $G = \mathrm{GL}_n(k)$ y sea $H = \{A \in G : \det A = 1\}$. Entonces H es un subgrupo de G.

7. Si H y K son subgrupos de G entonces $H \cap K$ es un subgrupo de G.

Dado un grupo G y un elemento $x \in G$, consideremos el conjunto $(x) = \{x^n : n \in \mathbb{Z}\}$. Se trata de un subgrupo de G, que puede ser finito o no. Llamaremos *orden de* x, y se notará $o(x)$, al orden de este subgrupo. En caso de ser finito, $o(x) = \min\{n \in \mathbb{N} : x^n = 1\}$.

Ejemplo. Si $G = \mathbb{Z}_6$, $o(\overline{0}) = 1$, $o(\overline{1}) = 6$, $o(\overline{2}) = 3$, $o(\overline{3}) = 2$, $o(\overline{4}) = 3$ y $o(\overline{5}) = 6$.

Observación. Si $x \in G$ es tal que $o(x) = n$ y $t \in \mathbb{Z}$ es tal que $x^t = e_G$, entonces n divide a t. En particular, para todo $x \in G$, se tiene que $o(x) = o(x^{-1})$.

Definición 1.3.2. Dado un grupo G, se llama *exponente* de G al mínimo del siguiente conjunto $A = \{s \in \mathbb{N} : x^s = 1 \text{ si } x \in G\}$.

Ejemplo. Si $G = \mathbb{Z}$ este conjunto es vacío, así que el exponente es, por definición, igual a $+\infty$.

Proposición 1.3.3. *Sea G un grupo finito. Entonces el conjunto A es no vacío. Además, el exponente de G es el mínimo común múltiplo de los órdenes de los elementos de G.*

Demostración. Sea $x \in G$. Si t es tal que $x^t = e$ entonces $o(x) \mid t$. Supongamos que $t = o(g)m$ con $m \in \mathbb{Z}$. Entonces $x^t = x^{o(x)m} = e$. Vemos que $o(x) \mid t \iff x^t = e$. Como G es finito, todo elemento tiene orden finito, y como G tiene una cantidad finita de elementos, tiene sentido considerar al mínimo común múltiplo s de los órdenes $o(x)$ con $x \in G$.

Es $x^s = e$ para todo $x \in G$, así que A es no vacío y G tiene exponente finito. Además, si m es tal que $x^m = e$ para todo $x \in G$ entonces claramente s divide a m. Luego s es el exponente de G. $\square$

Observemos que si H es un subgrupo de un grupo G, entonces para cada $x \in G$ el conjunto

$$xHx^{-1} = \{xhx^{-1} : h \in H\}$$

es también un subgrupo de G: en efecto, es

$$(xhx^{-1})(xh'x^{-1}) = x(hh')x^{-1}$$

y

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

De esta manera, a partir de un subgrupo H obtenemos otros, que llamaremos *conjugados* a H. No hay razón *a priori* para suponer que H coincide con sus subgrupos conjugados, aunque esto sí es cierto si por ejemplo el grupo G es conmutativo o, más generalmente, si los elementos de H conmutan con los de G.

Ejemplo. Sea $G = S_n$ y sea $\sigma \in G$ la permutación cíclica definida por

$$\sigma(i) = \begin{cases} i+1, & \text{si } i < n; \\ 1, & \text{si } i = n. \end{cases}$$

Sea además $H = \{id, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$. H es un subgrupo de G, pero no es cierto, en general, que si $x \in G$ entonces $xHx^{-1} = H$ (¡dé un ejemplo de esto!).

Definición 1.3.4. Un subgrupo H de un grupo G es *invariante* (o también *normal* o *distinguido*) si $xHx^{-1} = H$ para todo $x \in G$. Escribiremos $H \lhd G$.

Observaciones.
1. Sea $\{H_i\}_{i \in I}$ una familia de subgrupos de un grupo G. Entonces $\bigcap_{i \in I} H_i$ es también un subgrupo de G. Si además todos los H_i son invariantes en G, entonces $\bigcap_{i \in I} H_i$ es invariante.

2. Si H es un subgrupo de un grupo G, mostrar que $\bigcap_{x \in G} xHx^{-1}$ es un subgrupo invariante.

3. Si S es un subconjunto de G, sea

$$N_S = \{x \in G : xSx^{-1} = S\}.$$

N_S es un subgrupo de G al que llamamos el *normalizador* de S en G. Por ejemplo, si $a \in G$ y $S = \{a\}$, entonces se tiene que $N_S = \{x \in G : xa = ax\}$.

Si S es un subgrupo de G, se puede ver que S es también un subgrupo de N_S y $S \lhd N_S$. Además N_S es el subgrupo de G más grande con esa propiedad.

4. Sea

$$Z_G = \{x \in G : xg = gx \text{ para tdo } g \in G\}.$$

Z_G es un subgrupo de G. Llamamos a Z_G el *centro* de G. Se tiene $Z_G \lhd G$ y, además, cualquiera sea $S \subseteq G$, es $Z_G \subseteq N_S$.

5. Si G es un grupo cualquiera y $x, y \in G$, el *conmutador de x e y* es el elemento

$$[x, y] = xyx^{-1}y^{-1}.$$

Dejamos como ejercicio verificar que si $z \in G$, entonces

$$z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}].$$

Llamamos *subgrupo conmutador* o *subgrupo derivado*, y lo escribimos $[G, G]$, al subgrupo de G generado por los conmutadores. Tenemos entonces que $[G, G] \lhd G$.

1.4 Morfismos y cocientes

Así como la noción de conjunto está intrínsecamente ligada al concepto de función, pues una función es una forma de relacionar un conjunto con otro, para el caso de grupos — que son conjuntos provistos de una estructura de producto adicional — serán de importancia central las funciones entre grupos que "respeten" dicha estructura.

Definición 1.4.1. Sean $(G, \cdot_G)$ y $(G', \cdot_{G'})$ dos grupos. Una función $f : G \to G'$ es un *morfismo* (o también un *homomorfismo*) de grupos si para todo $g_1, g_2 \in G$ se tiene que

$$f(g_1 \cdot_G g_2) = f(g_1) \cdot_{G'} f(g_2).$$

Ejercicio. Un subconjunto H de un grupo G es subgrupo si y sólo si H admite una estructura de grupo tal que la función inclusion $i : H \hookrightarrow G$ es un morfismo de grupos.

Definición 1.4.2. Un *monomorfismo* es un morfismo inyectivo. Un *epimorfismo* es un morfismo suryectivo. Un *isomorfismo* es un morfismo biyectivo.

Notemos que el conjunto de morfismos de grupos $f : G \to G'$, que escribiremos $\mathrm{Hom}_{Gr}(G, G')$, es siempre no vacío: la función que a todo elemento de G le asigna el neutro de G' es trivialmente un morfismo de grupos, al que llamamos el "morfismo nulo".

Observaciones.
1. Un morfismo $f : G \to G'$ es un isomorfismo sii es monomorfismo y epimorfismo. En tal caso, la función inversa $f^{-1} : G' \to G$ también es un morfismo de grupos (¡verificarlo!).

2. Si f es un morfismo, entonces $f(e_G) = e_{G'}$: como $e_G = e_G e_G$, es $f(e_G) = f(e_G)f(e_G)$, así que

$$e_{G'} = f(e_G)(f(e_G))^{-1} = f(e_G)f(e_G)(f(e_G))^{-1} = f(e_G).$$

3. Si $f : G \to G'$ es un morfismo, entonces para cada $g \in G$ es $f(g^{-1}) = f(g)^{-1}$.

4. Un morfismo f es un monomorfismo sii

$$f(g) = e_{G'} \implies g = e_G.$$

Definición 1.4.3. Sea $f : G \to G'$ un morfismo de grupos. El *núcleo* de f es el conjunto

$$\mathrm{Ker}(f) = \{g \in G : f(g) = e_{G'}\}$$

y la *imágen* de f es el conjunto

$$\mathrm{Im}(f) = \{g' \in G' : \text{existe } g \in G \text{ tal que } f(g) = g'\}.$$

Se trata de subgrupos de G y de G', respectivamente.

Ejercicios.
1. Verificar que efectivamente $\mathrm{Ker}(f)$ e $\mathrm{Im}(f)$ son subgrupos de G y de G'. Verificar además que $\mathrm{Ker}(f) \lhd G$. Mostrar con un ejemplo que $\mathrm{Im}(f)$ no tiene porque ser invariante.

2. Sea $f : G \to G'$ como antes un morfismo de grupos y H' un subgrupo de G'. Verificar que $f^{-1}(H')$ es un subgrupo de G. Si además $H' \lhd G'$, entonces $f^{-1}(H') \lhd G$. En particular, como es $\{e\} \lhd G'$ resulta $\mathrm{Ker}(f) \lhd G$.

Las definiciones de monomorfismo y epimorfismo pueden ser enunciadas a través de estos subgrupos: un morfismo $f : G \to G'$ es un monomorfismo si y sólo si $\mathrm{Ker}(f) = \{e_G\}$ y es un epimorfismo si y sólo si $\mathrm{Im}(f) = G'$.

Ejemplos.
1. La aplicación exponencial $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$, dada por $\exp(x) = e^x$ para todo $x \in \mathbb{R}$, es un isomorfismo de grupos, cuyo inverso es la función logaritmo.

2. Determinemos los morfismos de $\mathbb{Z}_2$ a $\mathbb{Z}_4$.

Sea $f : \mathbb{Z}_2 \to \mathbb{Z}_4$ un morfismo de grupos. Sabemos que $f(\overline{0}) = \overline{0}$. ¿Cuánto vale $f(\overline{1})$? Como $\overline{0} = \overline{1} + \overline{1}$ entonces $f(\overline{1}) + f(\overline{1}) = \overline{0}$. Esto nos dice que $f(\overline{1})$ debe ser o bien cero o bien la clase de 2 en $\mathbb{Z}_4$. En cualquiera de los dos casos, la función así definida es un morfismo de grupos.

3. Si $f : \mathbb{Z}_2 \to \mathbb{Z}_3$ es un morfismo de grupos, entonces f es el morfismo nulo. (¡Verifíquelo!)

4. La proyección canónica $\pi : \mathbb{Z} \to \mathbb{Z}_n$ es un morfismo de grupos.

5. Dados un cuerpo k y $n \in \mathbb{N}$, la aplicación $f : \mathrm{GL}_n(k) \to k - \{0\}$ tal que $f(A) = \det(A)$ es un morfismo de grupos.

6. Sea $f : G_n \to \mathbb{Z}_n$ dado por $f(e^{\frac{2\pi i k}{n}}) = \overline{k}$. Entonces f es un isomorfismo de grupos.

Ejercicio. Definir un morfismo de grupos $f : S_3 \to S_3$ tal que $\mathrm{Im}(f) \not\lhd S_3$.

Vimos que si $f : G \to G'$ es un morfismo de grupos, entonces $\mathrm{Ker}(f) \lhd G$. Sin embargo, esto no es cierto para $\mathrm{Im}(f)$, como puede verse en el siguiente ejemplo:

Ejemplo. Sean k un cuerpo, $n \in \mathbb{N}$ y $A \in \mathrm{GL}_n(k)$ una matriz no escalar. Sea $f_A : \mathbb{Z} \to \mathrm{GL}_n(k)$ el morfismo de grupos definido por $f_A(r) = A^r$. Entonces la imagen de f_A es el subgrupo de $\mathrm{GL}_n(k)$ generado por A, que no es invariante.

El siguiente lema muestra que todo subgrupo normal de G es el núcleo de algún morfismo de G en algún grupo G'.

Lema 1.4.4. *Sea $H \lhd G$. Entonces existe un grupo G' y un morfismo de grupos $f : G \to G'$ tal que $H = \mathrm{Ker}(f)$.*

Demostración. Definimos una relación de equivalencia $\sim_H$ sobre G.

Si $x, y \in G$, diremos que $x \sim_H y$ sii $y^{-1}x \in H$. Dejamos como ejercicio mostra que, como H es un subgrupo, esto define en efecto una relación de equivalencia; notemos que si $H = \{e\}$ esta relación es simplemente la igualdad.

Consideramos el conjunto cociente $G/\sim_H$ y la aplicación natural

$$\begin{aligned} \pi : G &\to G/\sim_H \\ x &\mapsto \overline{x} \end{aligned}$$

donde $\overline{x} = \{y \in G : x \sim_H y\}$ es la clase de equivalecia de x.

Ponemos $G' = G/\sim_H$ y definimos una operación sobre G' de manera que

$$\overline{x} * \overline{y} = \overline{xy}.$$

Además, tomamos $f = \pi : G \to G'$. Queremos ver que G' es un grupo, que f es un morfismo de grupos y que $\mathrm{Ker}(f) = H$.

- *La operación $*$ está bien definida.* Sean x, x', y y y' tales que $\overline{x} = \overline{x'}$ y $\overline{y} = \overline{y'}$. Entonces existen $h_1, h_2 \in H$ tales que

  $$(x')^{-1}x = h_1, \qquad (y')^{-1}y = h_2,$$

  o, equivalentemente,

  $$x = x'h_1, \qquad y = y'h_2.$$

  Queremos ver que $\overline{x'y'} = \overline{xy}$ y para eso calculamos xy en términos de x' e y':

  $$\begin{aligned} xy &= x'h_1y'h_2 = x'(y'y'^{-1})h_1y'h_2 = x'y'(y'^{-1}h_1y')h_2 \\ &= x'y'h_3h_2, \end{aligned}$$

donde $h_3 = y'^{-1}h_1y'$, que es un conjugado de h_1. Como H es un subgrupo *invariante*, es $h_3 \in H$ y entonces $h_3h_2 \in H$. Por lo tanto, $xy \sim_H x'y'$ y, finalmente, $\overline{xy} = \overline{x'y'}$.

Notemos que si H no es invariante, el razonamiento anterior no es válido y no hay en general manera de dar al cociente G' una estructura de grupo compatible con la de G.

- *La operación definida en G' da una estructura de grupo*, es decir es asociativa, hay un elemento neutro y todo elemento tiene inverso. Dejamos esto como ejercicio al lector.
- *f es un morfismo de grupos y* $\mathrm{Ker}(f) = H$. Que f es un morfismo de grupos es inmediato a partir de su definición pues

$$f(xy) = \overline{xy} = \overline{x} * \overline{y} = f(x)f(y)$$

Calculamos ahora $\mathrm{Ker}(f)$:

$$\begin{aligned}\mathrm{Ker}(f) &= \{x \in G : f(x) = e_{G'}\}\\ &= \{x \in G : \overline{x} = \overline{e}\}\\ &= \{x \in G : x \sim_H e\}\\ &= \{x \in G : x \in H\}\\ &= H\end{aligned}$$

Esto completa la prueba. □

Definición 1.4.5. Si G es un grupo y $H \lhd G$ un subgrupo invariante, escribiremos G/H al grupo G' construido en la prueba del lema y lo llamaremos el *grupo cociente de G por H* (o G módulo H).

Notemos que la estructura de grupo de G/H proviene del hecho de que $H \lhd G$. Cuando H no es invariante, el conjunto cociente G/H es tan sólo un conjunto.

Ejemplos.
1. Sea $m\mathbb{Z} \subset \mathbb{Z}$. Se trata de un subgrupo de $(\mathbb{Z}, +)$ y $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

2. Consideremos el grupo $(\mathbb{R}, +)$ y el subgrupo $\mathbb{Z} \subset \mathbb{R}$. Es $\mathbb{Z} \lhd \mathbb{R}$ porque $\mathbb{R}$ es abeliano. Se obtiene entonces que $\mathbb{R}/\mathbb{Z}$ es un grupo isomorfo a $(S^1, \cdot) = \{z \in \mathbb{C} : |z| = 1\} \subset (\mathbb{C} - \{0\}, \cdot)$ y la proyección canónica es la aplicación

$$\overline{x} \in \mathbb{R}/\mathbb{Z} \mapsto e^{2i\pi x} \in S^1$$

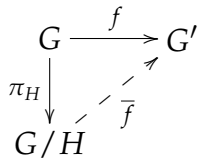
3. Si G es un grupo, entonces $G/\{e\} \cong G$ y $G/G \cong \{e\}$.

4. Sea $n \in \mathbb{N}$ y sea S_n el grupo de permutaciones de $\{1, \ldots, n\}$. Sea $i \in \{1, \ldots, n\}$ y sea H el subgrupo de S_n que consiste de las permutaciones que dejan fijo al elemento i. Entonces $S_n/H \cong S_{n-1}$.

Otra forma de describir al grupo cociente lo da la siguiente proposición, que presenta una propiedad de tipo universal que caracteriza completamente al cociente:

Proposición 1.4.6. *Sean G un grupo, $H \lhd G$ y sea $\pi_H : G \to G/H$ la proyección al cociente. Entonces para todo grupo G' y todo morfismo de grupos $f : G \to G'$ tal que $H \subseteq \mathrm{Ker}(f)$, existe un único morfismo de grupos $\overline{f} : G/H \to G'$ tal que $\overline{f} \circ \pi_H = f$.*

Esta situación se esquematiza con el siguiente diagrama:



Demostración. Mostremos separadamente la existenca y la unicidad.

Existencia. Si $\overline{x} \in G/H$, ponemos $\overline{f}(\overline{x}) = f(x)$. Esta aplicación está bien definida pues si $\overline{x} = \overline{x'}$, entonces ${x'}^{-1}x \in H \subseteq \mathrm{Ker}(f)$ y $f({x'}^{-1}x) = e'_G$. Esto implica que $f(x) = f(x')$.

Resulta claro también que $\overline{f}$ es un morfismo de grupos, pues

$$\overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y}).$$

Finalmente, la definición misma de $\overline{f}$ implica que $f = \overline{f} \circ \pi_H$.

Unicidad. La unicidad es una consecuencia de la sobreyectividad de π_H. Sean $\overline{f}_1, \overline{f}_2 : G/H \to G'$ morfismos de grupos tales que $\overline{f}_i \circ \pi = f$ para $i = 1, 2$. Entonces, si $\overline{x} \in G/H$, es

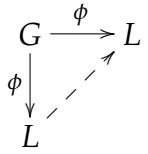
$$\overline{f}_1(\overline{x}) = \overline{f}_1(\pi(x)) = f(x) = \overline{f}_2(\pi(x)) = \overline{f}_2(\overline{x}),$$

así que $\overline{f}_1 = \overline{f}_2$. □

Observaciones.
1. Con las notaciones de la proposición anterior, $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$ y $\mathrm{Ker}(\overline{f}) = \pi_H(\mathrm{Ker}(f))$. En particular si f es un epimorfismo, entonces $\overline{f}$ también lo es, y si $H = \mathrm{Ker}(f)$ entonces $\overline{f}$ es un monomorfismo.

2. Sea G un grupo y $H \subset G$ un subgrupo normal. Supongamos que tenemos un grupo L y un morfismo de grupos $\phi : G \to L$ tal que $\mathrm{Ker}(\phi) = H$ y tal que para todo morfismo $f : G \to G'$ con $H \subseteq \mathrm{Ker}(f)$ existe un único morfismo $\hat{f} : L \to G'$ para el cual se tiene que $\hat{f} \circ \phi = f$. Queremos ver que existe un isomorfismo de grupos $L \cong G/H$.

Como $\mathrm{Ker}(\phi) = H$, existe un único $\overline{\phi} : G/H \to L$ tal que $\overline{\phi} \circ \pi_H = \phi$. Sabemos que $\mathrm{Ker}(\overline{\phi}) = \pi_H(\mathrm{Ker}(\phi) = \pi_H(H) = \{e\}$, así que $\overline{\phi}$ es monomorfismo. Para ver que $\overline{\phi}$ es también un epimorfismo, vamos a construir un inverso. Por hipótesis, existe un único morfismo $\hat{\pi}_H : L \to G/H$ tal que $\hat{\pi}_H \circ \phi = \pi_H$. Para verificar que $\hat{\pi}_H$ y $\overline{\phi}$ son inversos, notamos que una un único morfismo que hace conmutar el siguiente diagrama:



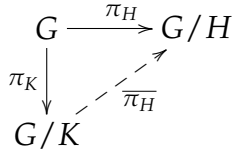
1.5 Teoremas de isomorfismo

Teorema 1.5.1. (Primer teorema de isomorfismo) *Sea $f : G \to G'$ es un morfismo de grupos, sea $H = \mathrm{Ker}(f)$ y consideremos la restricción $f : G \to \mathrm{Im}(f)$. Entonces $\overline{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ es un isomorfismo de grupos.*

Demostración. Basta observar que $\overline{f}$ es mono y epi. □

Teorema 1.5.2. (Segundo teorema de isomorfismo) *Sea G un grupo y sean H y K dos subgrupos normales de G tales que $K \subseteq H$. Entonces*

$K \lhd H$ y se tiene el siguiente diagrama conmutativo:



El morfismo $\overline{\pi_H}$ induce un isomorfismo

$$\frac{G/K}{H/K} \cong G/H.$$

Demostración. El morfismo $\overline{\pi_H}$ es claramente sobreyectivo, pues π_H lo es, y el núcleo de $\overline{\pi_H}$ es la imagen de H por π_K en G/K, es decir, $\mathrm{Im}(\overline{\pi_H}) = H/K$. Aaplicando ahora el primer teorema de isomorfismo a π_H se tiene que $\frac{G/K}{H/K} \cong G/H$. □

Ejemplo. Si consideramos los grupos aditivos $\mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$, entonces

$$\frac{\mathbb{C}/\mathbb{Z}}{\mathbb{R}/\mathbb{Z}} \cong \mathbb{C}/\mathbb{R} \cong \mathbb{R}.$$

Teorema 1.5.3. (Tercer teorema de isomorfismo) *Sea G un grupo y sean H y K subgrupos de G tales que $K \subseteq N_H$, esto es, tales que para todo $k \in J$ es $kHk^{-1} = H$.*

Si $HK = \{hk : h \in H, k \in K\}$, entonces HK es un subgrupo de G y $H \lhd HK$. Además, el morfismo de grupos $k \in K \mapsto \overline{k} \in HK/H$ induce un isomorfismo $K/(H \cap K) \cong HK/H$.

Demostración. HK es un subgrupo de G porque, por un lado,

$$(hk)(h'k') = hkh'(k^{-1}k)k' = \big(h(kh'k^{-1})\big)kk' \in HK,$$

ya que $kh'k^{-1} \in H$ y, por otro,

$$(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1}.$$

Es fácil ver que $H \lhd HK$, así que tiene sentido calcular HK/H. La aplicación $k \in K \mapsto \overline{k} \in HK/H$ es un morfismo de grupos sobreyectivo (¡verificarlo!) y su núcleo es el conjunto de los elementos de K que también están en H. El primer teorema da entonces un isomorfismo $K/(H \cap K) \cong HK/H$. □