Subgrupos normales, Grupo cociente y Teoremas de isomorfismos

Matemática Discreta 2 - IMERL
Facultad de Ingeniería - Universidad de la República

12/06/24 - Versión borrador

Índice general

Capítulo 1

Equivalencia definida por un subgrupo

1.1. Clases de equivalencia

Recordemos mediante un ejemplo el concepto de relación de equivalencia y clase de equivalencia. Consideremos el conjunto de los enteros $\mathbb{Z}$, y digamos que dos enteros a y b son "equivalentes", si se cumple que $a - b$ es múltiplo de tres. Es decir:

$$a \sim b \Leftrightarrow a - b = \dot{3}.$$

Por ejemplo: $10 \sim 4$, pues $10 - 4 = 6$, que es múltiplo de 3. También $10 \sim (-2)$, pues $10 - (-2) = 12$, que es múltiplo de 3. Al conjunto formado por todos los enteros que son equivalentes con 10, lo denominamos "clase de equivalencia" de 10, y lo denotamos mediante: $[10]$ o $\overline{10}$. Con la relación de equivalencia del ejemplo, la clase de equivalencia del 10 es:

$$[10] = \{b \in \mathbb{Z} \ / \ b \sim 10\} = \{b \in \mathbb{Z} \ / \ b = 10 + 3k, \ k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, 10, 13, \ldots\}.$$

Como se puede ver, esta clase es un subconjunto de los enteros, pero no contiene a todos los enteros. Por ejemplo, $2 \notin [10]$, pues $10 - 2 = 8$, que no es múltiplo de 3. Veamos cuáles son los enteros equivalentes con 2. Es decir: cuál es la clase de equivalencia del entero 2. Por definición, esta clase es:

$$[2] = \{b \in \mathbb{Z} \ / \ b = 2 + 3k, \ k \in \mathbb{Z}\} = \{\ldots, -7, -4, -1, 2, 5, 8, 14, \ldots\}.$$

Como podemos ver, ningún elemento de la clase de equivalencia $[2]$ pertenece a la clase $[10]$, y viceversa. Es decir: las clases son disjuntas: $[2] \cap [10] = \emptyset$. Por otro lado, existen enteros que no están en ninguna de estas dos clases. Por ejemplo: $3 \notin [2]$ y $3 \notin [10]$. Veamos cuál es la clase de equivalencia del 3:

$$[3] = \{b \in \mathbb{Z} \ / \ b = 3 + 3k, \ k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\}.$$

Al igual que antes, vemos que las clases son disjuntas dos a dos:

$$[2] \cap [10] = \emptyset, \quad [2] \cap [3] = \emptyset \quad [3] \cap [10] = \emptyset.$$

La novedad es que ahora cualquier entero pertenece a alguna de estas tres clases. Es decir:

$$[2] \cup [10] \cup [3] = \mathbb{Z}.$$

Decimos que la relación de equivalencia genera una "partición" del conjunto $\mathbb{Z}$ en clases de equivalencia (disjuntas dos a dos). La propiedad de partición obtenida en este ejemplo se cumple en general, para cualquier relación de equivalencia.

Ejercicio 1. *Consideremos la siguiente relación de equivalencia en $\mathbb{Z}$: $a \sim b \Leftrightarrow a - b = \dot{4}$.*

1. *Calcular las clases de equivalencia definidas por esta relación de equivalencia.*
2. *Verificar que las clases de equivalencia forman una partición de los enteros. Es decir:*
   - *para cualquier par de enteros no equivalentes, sus clases son disjuntas, y*
   - *la unión de todas las clases es $\mathbb{Z}$.*

1.2. Equivalencia definida por un subgrupo

En lo que sigue vamos a considerar relaciones de equivalencia entre elementos de un grupo G cualquiera. Estas relaciones las vamos a definir utilizando un subgrupo H de G. Esta es una idea que ya vimos durante la prueba del Teorema de Lagrange. Recordemos el enunciado de dicho teorema.

Teorema 1 (Teorema de Lagrange)**.** *Sea $(G, *)$ un grupo finito. Si $(H, *)$ es un subgrupo de G, entonces $|H|$ divide a $|G|$.*

No vamos a focalizarnos en el enunciado del Teorema de Lagrange, sino en la relación de equivalencia definida durante la prueba de dicho teorema. Al probar este teorema, vimos que un subgrupo H de G, permite definir una relación de equivalencia entre los elementos del grupo G. En concreto, definimos la relación de equivalencia de la siguiente forma:

$$\text{dados } g_1 \text{ y } g_2 \in G, \text{ decimos que } g_1 \sim g_2 \Leftrightarrow \exists\ h \in H \ /\ g_1 = h * g_2.$$

Multiplicando a ambos lados por g_2^{-1}, esto equivale a decir que:

$$g_1 \sim g_2 \Leftrightarrow g_1 * g_2^{-1} \in H.$$

Ambos criterios son equivalentes, y podemos usar uno o el otro según cuál sea más conveniente.

Ejemplo 1. *Consideremos el grupo de los enteros con la suma usual* $(G, *) = (\mathbb{Z}, +)$*, y el subgrupo formado por los enteros múltiplos de tres:* $(H, *) = (3\mathbb{Z}, +)$*. Este subgrupo permite definir la siguiente relación de equivalencia entre los enteros:*

$$a \sim b \Leftrightarrow \exists\ h \in 3\mathbb{Z}\ /\ a = h + b \Leftrightarrow a - b = h \in 3\mathbb{Z}.$$

Es decir: dos enteros a y b están relacionados si su resta es múltiplo de 3. Obtenemos entonces la misma relación de equivalencia del ejemplo visto al inicio.

La relación de equivalencia permite definir "clases de equivalencia", asociadas a los elementos de G. Como vimos al inicio, las clases de equivalencia son subconjuntos de G, definidos de la siguiente forma.

Definición 1 (Clase de equivalencia)**.** *Si* $g \in G$*, definimos la clase de equivalencia de* g*, y la denotamos mediante* $[g]$*, como el conjunto formado por todos los elementos de* G *que son equivalentes con* g*:*

$$[g] := \{f \in G\ /\ g \sim f\}.$$

En el caso particular en que la relación es la definida por un subgrupo H*, podemos expresar la clase de equivalencia de un elemento* $g \in G$ *de la siguiente forma:*

$$Hg = \{f \in G\ /\ f = h * g,\ \text{para algún } h \in H\} = \{h * g,\ h \in H\}.$$

Notar que modificamos la notación de la clase de equivalencia de g*, para dejar explícito cuál es el subgrupo* H *que induce la clase de equivalencia.*

Veamos un ejemplo más interesante de la relación de equivalencia inducida por un subgrupo.

Ejemplo 2. *Consideremos el grupo formado por las simetrías de un triángulo equilátero. Este es el grupo Diedral* D_3*, formado por:*

1. *las rotaciones con centro en el centro del triángulo, y sentido antihorario:* r_0 *de 0 grados (la identidad),* r_1 *de* 120^o*, y* r_2 *de* 240^o*, y*

2. *las reflexiones respecto a cada bisectriz:* s_1*,* s_2 *y* s_3 *(ver Figura 1.1).*

Es decir: $D_3 = \{id, r_1, r_2, s_1, s_2, s_3\}$*. La operación del grupo son las composiciones de las simetrías (pensadas como funciones).*

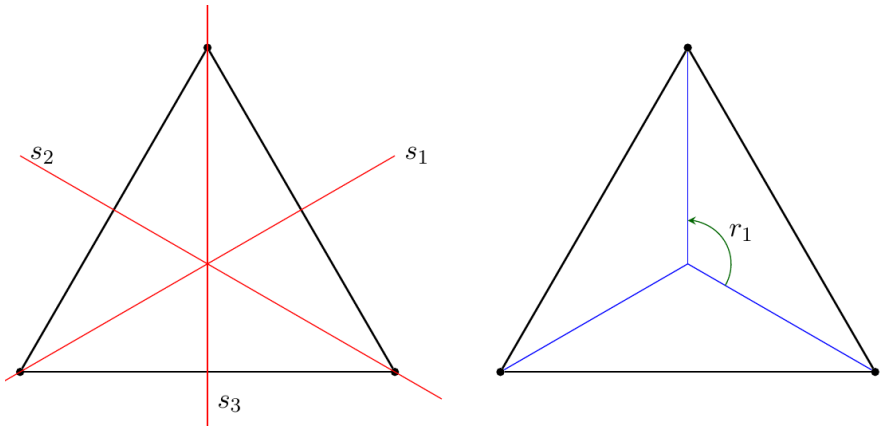

Figura 1.1: Simetrías de un triángulo equilátero.

Consideremos el subgrupo de D_3 formado por la identidad y una de las relfexiones: $H = \{id, s_1\}$. Por lo visto anteriormente, este subgrupo permite definir una relación de equivalencia entre los elementos del grupo. En concreto: dadas dos simetrías $g_1, g_2 \in D_3$, decimos que

$$g_1 \sim g_2 \Leftrightarrow \ \exists\ h \in H = \{id, s_1\}\ /\ g_1 = h \circ g_2.$$

Por ejemplo, es sencillo comprobar de forma geométrica que se cumple: $s_3 = s_1 \circ r_2$, con $s_1 \in H$. Por lo tanto: $s_3 \sim r_2$. Esto implica que s_3 y r_2 pertenecen a la misma clase de equivalencia. Supongamos ahora que queremos determinar cuáles son todas las simetrías relacionadas con r_2. Es decir, queremos calcular la clase de equivalencia de r_2. Por definición, esta clase está dada por el siguiente conjunto:

$$[r_2] = \{g \in G\ /\ g = h \circ r_2,\ \text{para algún } h \in H\} = \{h \circ r_2,\ h \in H\} = Hr_2.$$

Como H tiene solamente dos elementos, sólo tenemos que calcular dos composiciones:

$$[r_2] = Hr_2 = \{h \circ r_2,\ h \in H\} = \{id \circ r_2, s_1 \circ r_2\} = \{r_2, s_3\}.$$

Queda como ejercicio comprobar que las clases de equivalencia de este subgrupo son:

$$Hid = Hs_1 = \{id, s_1\} = H, \quad Hr_2 = Hs_3 = \{r_2, s_3\}, \quad Hr_1 = Hs_2 = \{r_1, s_2\}.$$

Notar que estas clases forman una partición del conjunto de simetrías D_3. Es decir:

1. *las clases distintas son disjuntas dos a dos:*

$$H \cap Hr_2 = \emptyset \quad H \cap Hr_1 = \emptyset \quad Hr_2 \cap Hr_1 = \emptyset,$$

2. *y la unión de las clases es todo D_3:*

$$D_3 = H \cup Hr_2 \cup Hr_1.$$

1.3. Clases laterales

Antes de terminar esta introducción, vamos a introducir un concepto que será clave en lo que sigue. Es el concepto de clases laterales. Para motivar este concepto, recordemos cómo definimos la relación de equivalencia inducida por un subgrupo:

$$\text{dados } g_1 \text{ y } g_2 \in G, \text{ decimos que } g_1 \sim g_2 \Leftrightarrow \exists\ h \in H\ /\ g_1 = h * g_2.$$

Como vimos, con esta relación, la clase de equivalencia de un elemento $g \in G$ es:

$$Hg = \{h * g,\ h \in H\}.$$

Es decir: la clase asociada a g, se construye multiplicando por g "a la derecha" a los elementos de H. ¿Qué ocurre si decidimos multiplicar por g a la izquierda? Es decir, qué ocurre si definimos la relación de equivalencia inducida por un subgrupo H, de la siguiente forma:

$$\text{dados } g_1 \text{ y } g_2 \in G, \text{ decimos que } g_1 \sim g_2 \Leftrightarrow \exists\ h \in H\ /\ g_1 = g_2 * h.$$

Con esta nueva relación de equivalencia, la clase de equivalencia de un elemento $g \in G$ se obtiene multiplicado por g "a la izquierda" del subgrupo H:

$$gH = \{g * h,\ h \in H\}.$$

Si el grupo es conmutativo, es claro que ambas definiciones son equivalentes, y por lo tanto las clases de equivalencia son iguales. Es decir:

$$Hg = gH,\ \forall\ g \in G.$$

Pero ¿qué ocurre si el grupo no es conmutativo? ¿Será posible que en dicho caso todas las clases de equivalencia coincidan por derecha y por izquierda? La respuesta es que sí, como veremos más adelante. Los subgrupos H cuyas clases de equivalencia al multiplicar por derecha y por izquierda son iguales, se denominan "subgrupos normales" (o invariantes). Este tipo de subgrupos será el objeto de nuestro estudio en los capítulos que siguen. En este contexto, las clases de equivalencia se denominan "clases laterales", por derecha y por izquierda; según si la relación de equivalencia inducida por H se define multiplicando por derecha o por izquierda.

Ejercicio 2. *Considere el grupo diedral D_3 del ejemplo anterior: $D_3 = \{id, r_1, r_2, s_1, s_2, s_3\}$, y el subgrupo formado por la identidad y una de las reflexiones: $H = \{id, s_1\}$. En el ejercicio anterior calculamos las clases de equivalencia por* ***derecha*** *Hg, para cada elemento $g \in H$.*

1. *Calcule las clases de equivalencia por* ***izquierda*** *de H.*
2. *Pruebe que H no es un subgrupo normal de D_3.*

Capítulo 2

Subgrupos normales y grupo cociente

En el capítulo anterior intentamos motivar el concepto de clases laterales y subgrupos normales mediante algunos ejemplos. Veamos ahora las definiciones formales de estos conceptos.

2.1. Clases laterales y Subgrupos normales

Definición 2 (Clases laterales)**.** *Sea $(G, *)$ un grupo, y sea $(H, *)$ un subgrupo de G. Para cada elemento $g \in G$, se define la clase lateral por* ***izquierda****, asociada a g, como el siguiente conjunto:*

$$gH = \{g * h,\ h \in H\}, \quad g \in G \text{ fijo.}$$

De forma similar, se define la clase lateral por ***derecha****, asociada a g, como:*

$$Hg = \{h * g,\ h \in H\}, \quad g \in G \text{ fijo.}$$

Cada clase lateral es un conjunto formado por elementos del grupo G.

Ejemplo 3. *Consideremos el conjunto formado por las matrices invertibles 2×2, que además son triangular superior:*

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ a, b, c \in \mathbb{R},\ ac \neq 0 \right\}.$$

Este conjunto forma un grupo con el producto usual de matrices. Consideremos el subgrupo

$$H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{R} \right\}.$$

Tomemos la matriz $g = \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix} \in G$. *La clase lateral por* ***izquierda*** *de* g, *es:*

$$gH = \left\{ \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 2 & 2x+3 \\ 0 & 5 \end{pmatrix},\ x \in \mathbb{R} \right\}.$$

La clase lateral por ***derecha*** *de la matriz* g, *es:*

$$Hg = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 2 & 3+5x \\ 0 & 5 \end{pmatrix},\ x \in \mathbb{R} \right\}.$$

Ejercicio 3. *En el ejemplo anterior, calcular las clases laterales por izquierda y por derecha de las siguientes matrices:*

1. $g = \begin{pmatrix} 2 & 5 \\ 0 & 5 \end{pmatrix}$.
2. $g = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
3. $g = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}$.

Definición 3 (Subgrupo normal)**.** *Sea* $(G, *)$ *un grupo, y sea* $(H, *)$ *un subgrupo de* G. *Decimos que* H *es un subgrupo normal (o invariante) de* G, *si las clases laterales por izquierda y por derecha coinciden, para todo elemento* $g \in G$. *Es decir, si se cumple:*

$$gH = Hg,\ \forall\ g \in G.$$

Observación 1. *Si* H *es un subgrupo normal de* G, *se denota:* $H \lhd G$

Ejemplo 4. *Sigamos con el ejemplo anterior, donde*

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ a, b, c \in \mathbb{R},\ ac \neq 0 \right\}, \quad H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{R} \right\}.$$

Para ver si el subgrupo H *es un subgrupo normal de* G, *tenemos que determinar si las clases laterales por izquierda y por derecha son el mismo conjunto, para todo elemento* $g \in G$. *Consideremos un elemento genérico* $g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$. *Ya vimos que la clase lateral por izquierda de* g, *es:*

$$gH = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} a & ax+b \\ 0 & c \end{pmatrix},\ x \in \mathbb{R} \right\}.$$

De igual forma podemos calcular la clase lateral por derecha de g, *que resulta ser:*

$$Hg = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right\} = \left\{ \begin{pmatrix} a & b+cy \\ 0 & c \end{pmatrix},\ y \in \mathbb{R} \right\}.$$

En este último caso denotamos la variable con la letra y, *en lugar de* x, *para facilitar el*

razonamiento siguiente.

Veamos que en este ejemplo las clases laterales de g son iguales, cualquiera sea el elemento $g \in G$ considerado. Es decir: veamos que H es un subgrupo normal de G. Para esto tenemos que probar la igualdad de conjuntos: $gH = Hg$. Una forma de hacerlo es probando la doble inclusión de los conjuntos. Es decir:

$$gH = Hg \quad \Leftrightarrow \quad gH \subset Hg \quad y \quad Hg \subset gH.$$

La primera inclusión equivale a probar:

$$gH = \left\{ \begin{pmatrix} a & ax+b \\ 0 & c \end{pmatrix},\ x \in \mathbb{R} \right\} \subseteq \left\{ \begin{pmatrix} a & b+cy \\ 0 & c \end{pmatrix},\ y \in \mathbb{R} \right\} = Hg.$$

Tomemos un elemento cualquiera de gH, que denotamos: $\begin{pmatrix} a & ax+b \\ 0 & c \end{pmatrix}$. Queremos ver que este elemento pertenece al conjunto Hg. Es decir, queremos ver que existe $y \in \mathbb{R}$, tal que:

$$\begin{pmatrix} a & ax+b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b+cy \\ 0 & c \end{pmatrix}.$$

Esto equivale a probar que existen $x, y \in \mathbb{R}$, tales que: $ax + b = b + cy$; lo cual a su vez equivale a probar que: $ax = cy$. Como $ac \neq 0$, sabemos que tanto a como c son no nulos. Por lo tanto, podemos despejar $y = \frac{a}{c}x$. Con este valor de y se obtiene la inclusión buscada. La otra inclusión se prueba de forma análoga. Por lo tanto, logramos probar que H es un subgrupo normal de G.

Ejercicio 4. *Dado un grupo G cualquiera, probar que los subgrupos triviales: $H = \{e\}$ y $H = G$, siempre son subgrupos normales de G.*

Ejercicio 5. *Si G es un grupo conmutativo, probar que cualquier subgrupo H de G es un subgrupo normal de G.*

2.1.1. Conjunto conjugado

Una definición equivalente de subgrupos normales, utiliza el concepto de "conjugación".

Definición 4 (Conjunto conjugado)**.** *Sea H un subgrupo de G. Dado $g \in G$, se define el conjugado de H, por el elemento g, como el siguiente conjunto:*

$$gHg^{-1} = \{ghg^{-1},\ h \in H\}.$$

Con esta definición, podemos dar la siguiente definición alternativa de subgrupo normal. Es inmediato ver que ambas definiciones son equivalentes.

Definición 5 (Subgrupo normal)**.** *Un subgrupo H es normal en G, si se cumple:*

$$H = gHg^{-1},\ \forall\ g \in G.$$

Es decir: H es subgrupo normal si coincide con todos sus conjuntos conjugados. Dicho de otra forma: H es subgrupo normal de G, si es "invariante" por la conjugación de todos los elementos de G. Esta es la razón por la que a los subgrupos normales también se los denomina ***subgrupos invariantes*** *(invariantes por la conjugación).*

El siguiente resultado permite simplificar el proceso de probar que un subgrupo es normal (o invariante). Su ventaja es que sólo requiere probar una inclusión de conjuntos, y no dos como hicimos en un ejemplo anterior.

Proposición 1. *Sea H un subgrupo de G. El subgrupo H es normal, sii se cumple:*

$$gHg^{-1} \subset H,\ \forall\ g \in G.$$

En particular, para probar la igualdad $gHg^{-1} = H$, basta con probar la inclusión en un sentido.

Este resultado es bastante sorprendente. Es decir: ¿cómo es posible que podamos probar una igualdad de conjuntos, solamente probando una de las inclusiones? La clave es que no estamos pidiendo una sola inclusión, sino una inclusión por cada elemento $g \in G$. En particular, como G es un grupo, estamos pidiendo la inclusión para todo g y su inverso g^{-1}, que también es un elemento de G. Los detalles se encuentran en la prueba a continuación.

Demostración. ($\Leftarrow$) Supongamos que se cumple la inclusión en un sentido: $gHg^{-1} \subset H,\ \forall\ g \in G$. Para probar que H es normal, basta con probar que se cumple la inclusión en el otro sentido: $H \subset gHg^{-1},\ \forall\ g \in G$. Por hipótesis:

$$gHg^{-1} \subset H,\ \forall\ g \in G.$$

En particular se cumple la inclusión para $g^{-1} \in G$. Es decir: $g^{-1}H(g^{-1})^{-1} \subset H$. Simplificando: $g^{-1}Hg \subset H$. Por lo tanto, dado $h \in H$, se cumple: $g^{-1}hg \in H$. Esto permite escribir:

$$h = g\left(g^{-1}hg\right)g^{-1},\ \text{con}\ g^{-1}hg \in H.$$

Esto prueba que $h \in gHg^{-1}$, para todo $h \in H$.

($\Rightarrow$) Esta es la parte más sencilla de la prueba. Supongamos que H es normal. Por definición, se cumple la igualdad de conjuntos: $gHg^{-1} = H,\ \forall\ g \in G$. Esto implica la inclusión buscada: $gHg^{-1} \subset H,\ \forall\ g \in G$.

□

2.2. Conjunto cociente y Grupo cociente

Vamos a definir ahora el concepto de **conjunto** cociente. Más adelante veremos bajo qué condiciones este conjunto se puede convertir en un **grupo** cociente.

2.2.1. Conjunto cociente

Definición 6 (Conjunto cociente)**.** *Sea $(G,*)$ un grupo, y sea $(H,*)$ un subgrupo de G. El conjunto cociente, que denotamos G/H, se define como el conjunto formado por las clases laterales por izquierda de H en G. Es decir:*

$$G/H = \{gH,\ g \in G\}.$$

El conjunto cociente G/H es un conjunto formado por conjuntos (las clases laterales).

Observación 2. *En la definición anterior optamos por definir el conjunto cociente mediante las clases laterales por izquierda. Sin embargo, podríamos haber optado por utilizar las clases laterales por derecha. Lo importante es que cuando el subgrupo H es normal, las clases laterales coinciden, y ambas definiciones son equivalentes.*

Ejemplo 5. *Retomemos el ejemplo anterior, donde*

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ a,b,c \in \mathbb{R},\ ac \neq 0 \right\}, \quad H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{R} \right\}.$$

Tomemos una matriz genérica del grupo: $g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$, con $ac \neq 0$. La clase lateral por ***izquierda*** *de g, es:*

$$gH = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} a & ax+b \\ 0 & c \end{pmatrix},\ x \in \mathbb{R} \right\}.$$

Por definición, el conjunto cociente es el conjunto formado por todas las clases laterales por izquierda. Por lo tanto:

$$G/H = \{gH,\ g \in G\} = \left\{ \left\{ \begin{pmatrix} a & ax+b \\ 0 & c \end{pmatrix},\ x \in \mathbb{R} \right\},\ a,b,c \in \mathbb{R},\ ac \neq 0 \right\}.$$

Hacemos notar nuevamente que el conjunto cociente es un conjunto formado por conjuntos (las clases laterales).

Veamos dos propiedades interesantes del conjunto cociente. La primera dice que todos los elementos del conjunto cociente (las clases laterales), tienen la misma cantidad de elementos. Además, esta cantidad coincide con la cantidad de elementos de H.

Proposición 2. *Sea G un grupo finito y H un subgrupo de G. Se cumple:*

$$|gH| = |H|, \ \forall \ g \in G.$$

Demostración. Sea $g \in G$ cualquiera. Por definición, la clase lateral por izquierda es el conjunto:

$$gH = \{g * h, \ h \in H\}.$$

Es decir: el conjunto gH se construye calculando una cantidad $|H|$ de productos, uno por cada elemento de H. Si logramos probar que estos productos son todos distintos entre sí, podremos concluir que gH tiene exactamente $|H|$ elementos. Supongamos por absurdo que existen $h_1, h_2 \in H$, con $h_1 \neq h_2$, y tales que: $g * h_1 = g * h_2$. Multiplicando a la izquierda por g^{-1}, se obtiene: $h_1 = h_2$. Esto es absurdo pues supusimos que h_1 y h_2 eran distintos. □

La segunda propiedad dice que la cantidad de elementos del conjunto cociente G/H, se puede calcular como el cociente de la cantidad de elementos de G y H. La prueba de esta segunda propiedad utiliza la propiedad anterior.

Proposición 3. *Sea G un grupo finito y H un subgrupo de G. Se cumple:*

$$|G/H| = \frac{|G|}{|H|}.$$

Notar que $\frac{|G|}{|H|}$ es un entero debido al Teorema de Lagrange.

Demostración. Por definición, la cantidad de elementos del conjunto cociente G/H es la cantidad de clases laterales (distintas) de G con respecto al subgrupo H. Sabemos que las clases laterales son una partición de G. Es decir: G es la unión disjunta de las clases laterales. Por lo tanto, podemos escribir:

$$G = H \cup (g_1 H) \ldots \cup (g_{l-1} H), \text{ con } l = |G/H| \text{ elementos en la unión.}$$

Como las clases son disjuntas, la cantidad de elementos de G es la suma de la cantidad de elementos de cada conjunto de la unión:

$$|G| = |H| + |g_1 H| + \ldots + |g_{l-1} H|, \text{ con } l = |G/H| \text{ sumandos.}$$

Finalmente, como cada una de estas clases tiene exactamente $|H|$ elementos, se obtiene:

$$|G| = |H| + \ldots + |H| = |H||G/H|.$$

□

2.2.2. Operación en el conjunto cociente

Nos gustaría definir una operación $\times$ en el conjunto cociente G/H, de forma que el par $(G/H, \times)$ sea un grupo. Para esto primero vamos a definir una operación candidata, y luego vamos a analizar bajo qué condiciones se obtiene un grupo con esta operación.

Definición 7 (Operación en el conjunto cociente)**.** *Sea $(G, *)$ un grupo y $(H, *)$ un subgrupo de G. Definimos la siguiente operación entre elementos del conjunto cociente:*

$$\times : G/H \times G/H \to G/H \quad / \quad (g_1 H) \times (g_2 H) = (g_1 * g_2)H.$$

Ejemplo 6. *Sigamos con el ejemplo anterior, donde*

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ a, b, c \in \mathbb{R},\ ac \neq 0 \right\}, \quad H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{R} \right\}.$$

Ya vimos que el conjunto cociente es:

$$G/H = \{gH,\ g \in G\} = \left\{ \left\{ \begin{pmatrix} a & ax+b \\ 0 & c \end{pmatrix},\ x \in \mathbb{R} \right\},\ a, b, c \in \mathbb{R},\ ac \neq 0 \right\}.$$

Tomemos los siguientes dos elementos de este conjunto cociente (notar que cada elemento es una clase lateral por izquierda de H, y por lo tanto un conjunto de elementos del grupo G):

$$g_1 H = \left\{ \begin{pmatrix} 2 & 2x+3 \\ 0 & 5 \end{pmatrix},\ x \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{R} \right\},\ g_1 = \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix}.$$

$$g_2 H = \left\{ \begin{pmatrix} 1 & x+4 \\ 0 & 2 \end{pmatrix},\ x \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} 1 & 4 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{R} \right\},\ g_2 = \begin{pmatrix} 1 & 4 \\ 0 & 2 \end{pmatrix}.$$

El producto de estos dos elementos, con la operación definida anteriormente, es:

$$g_1 H \times g_2 H = (g_1 * g_2)H = \left(\begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 0 & 2 \end{pmatrix} \right) H = \begin{pmatrix} 2 & 14 \\ 0 & 10 \end{pmatrix} H.$$

Es decir:

$$g_1 H \times g_2 H = \left\{ \begin{pmatrix} 2 & 14 \\ 0 & 10 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} 2 & 2x+14 \\ 0 & 10 \end{pmatrix},\ x \in \mathbb{R} \right\}.$$

Ejercicio 6. *En el ejemplo anterior, considere las matrices dadas por:*

$$g_1 = \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix}.$$

Calcular:

1. *las clases laterales por izquierda g_1H y g_2H.*

2. *el producto de las clases laterales: $g_1H \times g_2H$.*

Veamos otro ejemplo, que muestra que la operación anterior no siempre está bien definida.

Ejemplo 7. *Retomemos el ejemplo del grupo diedral D_3, formado por las simetrías de un triángulo equilátero: $D_3 = \{id, r_1, r_2, s_1, s_2, s_3\}$, y el subgrupo formado por la identidad y una de las reflexiones: $H = \{id, s_1\}$. Ya sabemos que las clases laterales por izquierda de H son:*

$$idH = s_1H = \{id, s_1\} = H, \quad r_1H = s_3H = \{r_1, s_3\}, \quad r_2H = s_2H = \{r_2, s_2\}.$$

Por lo tanto, el conjunto cociente G/H es por definición:

$$G/H = \{H, r_1H, r_2H\} = \{\{id, s_1\}, \{r_1, s_3\}, \{r_2, s_2\}\}.$$

Calculemos la operación entre las clases r_1H y r_2H. Por definición:

$$r_1H \times r_2H = (r_1 \circ r_2)\, H = idH = H.$$

Sin embargo, también sabemos que $r_1H = s_3H$. Por lo tanto, podemos calcular la operación anterior usando r_1H en lugar de s_3H (dado que son el mismo conjunto). Si hacemos esto obtenemos:

$$s_3H \times r_2H = (s_3 \circ r_2)\, H = s_2H \neq H = r_1H \times r_2H.$$

Ocurrió algo no deseado: el resultado de la operación depende del representante elegido para las clases laterales.

¿Qué podemos hacer para garantizar que la operación $\times$ en el conjunto cociente G/H esté bien definida? Como veremos a continuación, la respuesta a esta pregunta es la siguiente: pedir que el subgrupo H sea un subgrupo **normal** de G. Notar que en el ejemplo anterior el subgrupo H no es un subgrupo normal de D_3 (por ejemplo: $r_1H = \{r_1, s_3\} \neq Hr_1 = \{r_1, s_2\}$).

2.2.3. Grupo cociente

Veamos ahora bajo qué condiciones podemos garantizar que el conjunto cociente G/H y la operación $\times$ forman un grupo. Este es el resultado más importante del capítulo.

Teorema 2 (Grupo cociente)**.** *Sea $(G, *)$ un grupo, y sea $(H, *)$ un subgrupo de G. Consideremos el par $(G/H, \times)$, formado por el conjunto cociente, y la operación definida anteriormente. Si H es un subgrupo **normal** de G, entonces $(G/H, \times)$ es un grupo. Este se denomina grupo cociente de G sobre H.*

Demostración. 1. **Existencia de neutro.** Es sencillo ver que el neutro del cociente es la clase asociada al neutro del grupo G. Es decir: $e_{G/H} = e_GH$. En efecto, usando la

definición de la operación $\times$, se obtiene:

$$e_G H \times gH = (e_G * g)H = gH, \quad gH \times e_G H = (g * e_G)H = gH, \quad \forall\ g \in G.$$

2. **Existencia de inverso.** Dada una clase gH en el cociente, veamos que su inverso es la clase asociada al elemento inverso del grupo g^{-1}. Es decir: veamos que $(gH)^{-1} = g^{-1}H$. En efecto:

$$gH \times g^{-1}H = (g * g^{-1})H = e_G H = H, \quad g^{-1}H \times gH = (g^{-1} * g)H = e_G H = H.$$

3. **Asociativa.** Usando la propiedad asociativa de la operación $*$ del grupo G, se obtiene:

$$(g_1 H \times g_2 H) \times g_3 H = ((g_1 * g_2)H) \times g_3 H = ((g_1 * g_2) * g_3)\, H =$$

$$= (g_1 * (g_2 * g_3))\, H = g_1 H \times ((g_2 * g_3)H) = g_1 H \times (g_2 H \times g_3 H)\,,\ \forall\ g_1, g_2, g_3 \in G.$$

Parecería que con esto queda probado que el par $(G/H, \times)$ es un grupo. Sin embargo, en ningún momento utilizamos que el subgrupo H es normal. Parecería entonces que podemos eliminar esa hipótesis del teorema. El problema es el siguiente: si el subgrupo H no es normal, no podemos garantizar que la operación $\times$ esté bien definida. Esta es la razón por la que pedimos que el subgrupo H sea normal.

Operación bien definida. Veamos que si H es un subgrupo normal, entonces la operación $\times$ está bien definida. Esto quiere decir que el resultado de la operación no depende del representante elegido para cada clase lateral. En términos formales, queremos probar que se cumple lo siguiente:

$$\text{si } g_1 H = \overline{g_1} H \text{ y } g_2 H = \overline{g_2} H \text{ entonces: } g_1 H \times g_2 H = \overline{g_1} H \times \overline{g_2} H.$$

Por definición de la operación $\times$, esto equivale a probar que se cumple:

$$g_1 H = \overline{g_1} H \ \text{ y } \ g_2 H = \overline{g_2} H \Rightarrow (g_1 * g_2)H = (\overline{g_1} * \overline{g_2})H.$$

Como $g_1 H = \overline{g_1} H$, sabemos que existen $h_1, \overline{h_1} \in H$, tales que: $g_1 * h_1 = \overline{g_1} * \overline{h_1}$. Como H es un grupo, esto equivale a decir que existe $h = (\overline{h_1})^{-1} * h_1 \in H$, tal que: $g_1 = \overline{g_1} h$. En forma similar, podemos decir que existe $\overline{h} \in H$, tal que: $g_2 = \overline{g_2} * \overline{h}$. Por lo tanto, podemos reemplazar g_1 y g_2 por estas expresiones en términos de $\overline{g_1}$ y $\overline{g_2}$. De esta forma se obtiene:

$$(g_1 * g_2)H = \left((\overline{g_1} * h) * (\overline{g_2} * \overline{h})\right) H.$$

Ahora vamos a multiplicar por la identidad, escrita de la siguiente forma: $id = \overline{g_2} * (\overline{g_2}^{-1})$.

Con esto se obtiene:

$$(g_1 * g_2)H = \left((\overline{g_1} * \overline{g_2} * ((\overline{g_2})^{-1}) * h) * (\overline{g_2} * \overline{h})\right) H.$$

Ahora usamos la asociativa:

$$(g_1 * g_2)H = \left(\overline{g_1} * \overline{g_2} * ((\overline{g_2})^{-1} * h * \overline{g_2}) * \overline{h}\right) H = \left(\overline{g_1} * \overline{g_2} * \hat{h} * \overline{h}\right) H;$$

donde para la última igualdad definimos $\hat{h} = (\overline{g_2})^{-1} * h * \overline{g_2}$. Para finalizar, basta con probar que $\hat{h} \in H$; pues esto implica que $\hat{h} * h \in H$, lo cual a su vez implica que $\left(\overline{g_1} * \overline{g_2} * \hat{h} * \overline{h}\right) H = (\overline{g_1} * \overline{g_2})\, H$. Veamos entonces que $\hat{h} \in H$. Como H es **normal**, se cumple: $H = (\overline{g_2})^{-1} H \overline{g_2}$. En particular vale: $(\overline{g_2})^{-1} H \overline{g_2} \subset H$. Como $h \in H$, esto implica: $\hat{h} = (\overline{g_2})^{-1} * h * \overline{g_2} \in H$. $\square$

Capítulo 3

Teoremas de isomorfismos

Antes de estudiar esta sección, se sugiere estudiar la Sección 3.9 de las notas generales del curso [2], donde se introduce el tema de Homomorfismos (páginas 56 a 61). Recordamos a continuación la definición de **homomorfismo** de grupos (más adelante recordaremos la definición de **isomorfismo**).

Definición 8 (Homomorfismo de grupos)**.** *Consideremos dos grupos $(G, \cdot)$ y $(K, *)$. Decimos que una función $f : G \to K$ es un homomorfismo de grupos, si se cumple:*

$$f(g \cdot h) = f(g) * g(h), \quad \forall\ g, h \in G.$$

A un homomorfismo de grupos también se le suele llamar morfismo de grupos.

Intuitivamente, se puede pensar que los morfismos de grupos son funciones entre grupos, que además preservan la "estructura" de grupo (preservan la operación).

Ejemplo 8. *Consideremos la función $f : (\mathbb{Z}, +) \to (\mathbb{R}^*, \times)$, dada por: $f(n) = 2^n$. Es sencillo ver que esta función es un homomorfismo de grupos. En efecto:*

$$f(n + m) = 2^{n+m} = 2^n \times 2^m = f(n) \times f(m), \quad \forall\ n, m \in \mathbb{Z}.$$

Ejemplo 9. *Veamos un ejemplo de una función que no es un morfismo de grupos. Consideremos la función $f : (GL_n(\mathbb{R}), \cdot) \to (\mathbb{R}, +)$, que a cada matriz invertible le asocia su traza: $f(M) = traza(M)$. La condición para que esta función sea un homomorfismo de grupos, es:*

$$f(A \cdot B) = f(A) + f(B), \quad \forall\ A, B \in GL_n(\mathbb{R}).$$

Por definición de la función, esto equivale a que se cumpla:

$$traza(A \cdot B) = traza(A) + traza(B), \quad \forall\ A, B \in GL_n(\mathbb{R}).$$

Es sencillo encontrar dos matrices invertibles A y B que no cumplen con la condición anterior. Por ejemplo, si tomamos: $A = I_n$ y $B = -I_n$, donde I_n es la matriz identidad $n \times n$,

se obtiene:

$$traza(I \cdot (-I)) = traza(-I) = -n \quad \neq \quad traza(I) + traza(-I) = n + (-n) = 0.$$

Por lo tanto, concluimos que f no es un homomorfismo de grupos.

Ejercicio 7. *Considere la función $f : (\mathbb{R}^{n\times n}, +) \to (\mathbb{R}, +)$, que a cada matriz le asocia su traza: $f(M) = traza(M)$. Analizar si esta función es un homomorfismo de grupos.*

3.1. Núcleo e Imagen de un homomorfismo

Definición 9 (Núcleo de un homomorfismo)**.** *Sea $f : G \to K$ un homomorfismo de grupos. Denotemos el elemento neutro de K mediante e_K. Se define el núcleo de f como el conjunto:*

$$\ker(f) = \{g \in G \ / \ f(g) = e_K\} \subseteq G.$$

Observación 3. *En los cursos de álgebra lineal se define el núcleo de una transformación lineal entre espacios vectoriales $T : V \to W$, como el conjunto:*

$$\ker(T) = \{v \in V \ / \ T(v) = \vec{0}\} \subseteq V.$$

La definición de núcleo de un morfismo es similar a la definición de núcleo de una transformación lineal, cambiando el vector nulo $\vec{0}$ por el elemento neutro e_K.

En álgebra lineal se prueba que el núcleo de una transformación lineal siempre es un subespacio vectorial. De forma similar, vamos a probar que el núcleo de un morfismo siempre es un subgrupo. Mas aún, vamos a probar que el núcleo siempre es un subgrupo normal.

Proposición 4. *Sea $f : G \to K$ un homomorfismo de grupos. El núcleo $\ker(f) \subseteq G$ es un subgrupo normal de G.*

Demostración. Ejercicio de práctico. Hay que probar que es subgrupo y que es normal. □

Este resultado brinda un método para probar que un subgrupo es normal. Esto es: si queremos probar que H es un subgrupo normal, basta con probar que H es el núcleo de algún homomorfismo. La ventaja de este método es que no requiere calcular las clases laterales por derecha ni por izquierda. Ilustremos esto con un ejemplo.

Ejemplo 10. *Consideremos el grupo de las matrices invertibles, $n \times n$, con el producto usual de matrices. Este se denomina Grupo Lineal, y se denota $(GL_n(\mathbb{R}), \cdot)$. Un subgrupo importante de este grupo es el formado por las matrices invertibles con determinante igual a uno. Este se denomina Grupo Lineal Especial, y se denota mediante $SL_n(\mathbb{R})$. Es decir:*

$$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \ / \ \det(A) = 1\}.$$

Vamos a probar que $SL_n(\mathbb{R})$ es un subgrupo normal. Para esto consideremos el homomorfismo $f : GL_n(\mathbb{R}) \to \mathbb{R}^*$, tal que $f(A) = \det(A)$. El elemento neutro de $\mathbb{R}^*$ es el 1. Por lo tanto, el núcleo del homomorfismo es:

$$\ker(f) = \{A \in GL_n(\mathbb{R}) \ / \ f(A) = 1\} = \{A \in GL_n(\mathbb{R}) \ / \ \det(A) = 1\} = SL_n(\mathbb{R}).$$

Como el núcleo de un homomorfismo siempre es un subgrupo normal, esto prueba que $SL_n(\mathbb{R})$ es un subgrupo normal.

Observación 4. *El hecho de que el núcleo de un morfismo $f : G \to K$ sea un subgrupo normal de G, garantiza que el conjunto cociente $G/ker(f)$ forma un grupo junto con la operación $\times$ entre clases laterales.*

Definición 10 (Imagen de un homomorfismo)**.** *Sea $f : G \to K$ un homomorfismo de grupos. La imagen de f se define como:*

$$Im(f) = \{k \in K \ / \ \exists \ g \in G \text{ que cumple: } f(g) = k\} \subseteq K.$$

Es decir: es el conjunto de elementos de K que son "alcanzados" por la función f.

Ejemplo 11. *Consideremos el homomorfismo del ejemplo anterior: $f : GL_n(\mathbb{R}) \to \mathbb{R}^*$, tal que $f(A) = \det(A)$. Por definición, la imagen de f es:*

$$Im(f) = \{x \in \mathbb{R}^* \ / \ \exists \ A \in GL_n(\mathbb{R}) \text{ con } \det(A) = x\}.$$

Veamos que $Im(f) = \mathbb{R}^*$. Es decir: cualquier número real no nulo se puede expresar como el determinante de algún matriz invertible. En efecto, a cada $x \in \mathbb{R}^*$ le podemos asociar la siguiente matriz diagonal invertible:

$$A = \begin{pmatrix} x & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & & \dots & & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \quad / \quad \det(A) = x.$$

La imagen de un homomorfismo siempre es un subgrupo de K. Sin embargo, la imagen no siempre es un subgrupo normal. Esto es una diferencia importante con el núcleo, que como ya vimos siempre es un subgrupo normal.

Proposición 5. *Sea $f : G \to K$ un homomorfismo de grupos. La imagen $Im(f)$ es un subgrupo de K.*

Demostración. Ejercicio de práctico. □

Veamos un ejemplo de un homomorfismo cuya imagen no es un subgrupo normal.

Ejemplo 12. *Consideremos la función $f : \mathbb{Z}_2 \to D_3$, tal que: $f(\bar{0}) = id$ y $f(\bar{1}) = s_1$; donde s_1 es una simetría axial del triángulo equilatero (ver Figura 1.1). Queda como ejercicio probar que esta función es un homomorfismo.*

Por definición: $Im(f) = \{id, s_1\}$. Este es un subgrupo (el subgrupo generado por la simetría s_1). Sin embargo, $Im(f)$ no es un subgrupo normal de D_3. Para probar esto último, basta con encontrar un elemento $g \in D_3$, cuyas clases laterales sean distintas por izquierda y por derecha. Tomemos por ejemplo $g = r_1$, la rotación de ángulo 120 grados. Se cumple:

$$r_1 Im(f) = \{r_1, s_3\} \quad \neq \quad Im(f) r_1 = \{r_1, s_2\};$$

siendo s_2 y s_3 las otras dos simetrías axiales (ver Figura 1.1).

3.2. Teoremas de isomorfismos

Un isomorfismo de grupos es un caso particular de homomorfismo, en donde además pedimos que la función sea biyectiva.

Definición 11 (Isomorfismo de grupos)**.** *Consideremos dos grupos $(G, \cdot)$ y $(K, *)$. Decimos que una función $f : G \to K$ es un isomorfismo de grupos, si se cumple:*

1. *f es un homomorfismo de grupos, y*
2. *f es biyectiva (inyectiva y sobreyectiva).*

Ejemplo 13. *Consideremos la función $f : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$, tal que: $f(x) = e^x$. Queda como ejercicio probar que f es un homomorfismo de grupos. Veamos que además f es biyectiva, por lo que es un isomorfismo de grupos.*

1. *inyectiva:*
$$f(x) = f(y) \Leftrightarrow e^x = e^y \Leftrightarrow x = y.$$
2. *sobreyectiva: sea $y \in \mathbb{R}^+$, un número real positivo cualquiera. Queremos probar que existe $x \in \mathbb{R}$, tal que: $f(x) = y$. Para esto basta con despejar x aplicando el logaritmo:*
$$f(x) = y \Leftrightarrow e^x = y \Leftrightarrow x = \log(y).$$
Notar que el logaritmo está bien definido pues $y > 0$.

Ejemplo 14. *Consideremos la función $f : (\mathbb{Z}, +) \to (\mathbb{R}^+, \cdot)$, dada por: $f(n) = 2^n$. Es sencillo ver que esta función es un homomorfismo de grupos. Sin embargo, f no es una función sobreyectiva, por lo que no es un isomorfismo. En efecto, la imagen de f es el conjunto formado por las potencias de 2, por lo que f no alcanza a todos los valores reales positivos:*

$$Im(f) = \{\ldots, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3, \ldots, 2^n, \ldots\} \neq \mathbb{R}^+.$$

Cuando existe un **isomorfismo** entre dos grupos G y K, decimos que estos grupos son isomorfos, y denotamos: $G \simeq K$. En este caso existe una correspondencia biyectiva entre los elementos de ambos grupos (dada por el isomorfismo), que además preserva la operación. Por este motivo, dos grupos isomorfos se suelen concebir como el mismo grupo (aunque no lo sean). Los teoremas de isomorfismos permiten probar la existencia de isomorfismos entre ciertos grupos; mostrando así que estos grupos son "iguales" en lo que respecta a la teoría de grupos.

Antes de probar el Primer Teorema de Isomorfismos, veamos dos resultados que van a ser de utilidad para el enunciado y la prueba de este teorema.

Proposición 6. *Sea $f : G \to K$ un homomorfismo de grupos. Entonces f es inyectiva si y sólo si su núcleo es el grupo trivial: $Ker(f) = \{e_G\}$.*

Demostración. ($\Rightarrow$) : este es el sentido más sencillo. Si el homomorfismo es inyectivo, entonces en particular existe un único elemento $g \in G$ tal que: $f(g) = e_K$. Es decir, el núcleo está formado por un único elemento: $Ker(f) = \{g\}$. Por otro lado, por ser homomorfismo, sabemos que se debe cumplir: $f(e_G) = e_K$. Por lo tanto, se concluye que $g = e_G$, y $\ker(f) = \{e_G\}$.

($\Leftarrow$) Tenemos que probar que si $f(x) = f(y)$, entonces $x = y$. Vamos a utilizar la siguiente propiedad de un homomorfismo (cuya prueba queda como ejercicio): $(f(y))^{-1} = f(y^{-1})$. Usando esto, y la definición de homomorfismo, se tiene:

$$f(x) = f(y) \Leftrightarrow f(x)\,(f(y))^{-1} = e_K \Leftrightarrow f(x)f(y^{-1}) = e_K \Leftrightarrow f(xy^{-1}) = e_K.$$

Es decir: $xy^{-1} \in \ker(f) = \{e_G\}$. Por lo tanto: $xy^{-1} = e_G$; lo cual equivale a: $x = y$ □

Observación 5. *El resultado anterior es análogo al de los cursos de Álgebra Lineal, que dice que una transformación lineal $T : V \to W$ es inyectiva, si y sólo si su núcleo es el subespacio trivial: $Ker(T) = \{\vec{0}\}$.*

Ejemplo 15. *Consideremos la función $f : (\mathbb{Z}, +) \to (\mathbb{R}^+, \cdot)$, dada por: $f(n) = 2^n$. Ya vimos que esta función es un homomorfismo de grupos. Veamos que es inyectiva. El neutro de $(\mathbb{Z}, +)$ es 0, mientras que el neutro de $(\mathbb{R}^+, \cdot)$ es 1. Teniendo en cuenta esto, el núcleo de f es:*

$$\ker(f) = \{n \in \mathbb{Z} \ / \ f(n) = 1\} = \{n \in \mathbb{Z} \ / \ 2^n = 1\} = \{0\} = \{e_{\mathbb{Z}}\}.$$

Esto prueba que la función f es inyectiva.

Ejercicio 8. *Sea $f : G \to K$ un homomorfismo. Probar que se cumple:*

$$(f(x))^{-1} = f(x^{-1}),\ \forall\ x \in G.$$

La siguiente definición introduce una función con nombre propio, que será relevante para el Primer Teorema de Isomorfismos.

Definición 12 (Proyección canónica de un subgrupo)**.** *Dado un grupo G, y un subgrupo H, definimos la "proyección canónica", como la función que a cada elemento de G le asocia su clase lateral en el conjunto cociente G/H. Es decir:*

$$\Pi : G \to G/H \quad / \quad \Pi(g) = gH.$$

Notar que hay una proyección canónica por cada subgrupo.

Si el subgrupo es normal, entonces el conjunto cociente es un grupo. En este caso se puede probar que la proyección canónica es un homomorfismo. Más aún: el núcleo de este homomorfismo es el subgrupo normal que define la proyección. Esto muestra que todo subgrupo normal se puede ver como el núcleo de un homomorfismo.

Ejercicio 9. *Sea H un subgrupo normal. Probar que se cumple:*

1. *La proyección canónica $\Pi : G \to G/H$, es un homomorfismo de grupos.*
2. *El núcleo de Π es H.*

Veamos ahora el primer teorema de isomorfismos de grupos.

Teorema 3 (Primer Teorema de Isomorfismos)**.** *Sea $f : G \to K$ un homomorfismo de grupos. Sea $\Pi : G \to G/\ker(f)$ la proyección canónica al cociente por el subgrupo normal $\ker(f)$. Existe un único isomorfismo $\bar{f} : G/\ker(f) \to Im(f)$, tal que: $f = \bar{f} \circ \Pi$. Esta última igualdad se suele expresar diciendo que "el diagrama de la Figura 3.1 conmuta".*

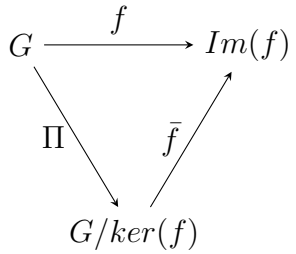

Figura 3.1: Primer Teorema de Isomorfismos.

Lo más relevante de este resultado, es que la existencia del isomorfismo implica que el grupo cociente $G/\ker(f)$ es isomorfo al grupo imagen $Im(f)$. Es decir: $G/\ker(f) \simeq Im(f)$. Esto quiere decir que ambos grupos son "iguales" en lo que respecta a la teoría de grupos.

Demostración. Consideremos dos grupos $(G, *)$ y $(K, \cdot)$. Para probar la existencia del isomorfismo, vamos a considerar la siguiente función como candidata a ser el isomorfismo buscado:

$$\bar{f} : G/ker(f) \to Im(f) \quad / \quad \bar{f}(gH) = f(g), \quad \text{con} \quad H = ker(f).$$

Veamos que esta función está bien definida y que además es un isomorfismo.

1. $\bar{f}$ **está bien definida**. Dado que $\bar{f}$ está definida en clases laterales, tenemos que probar que el valor $\bar{f}(gH)$ no depende del representante elegido para la clase lateral gH. Es decir, tenemos que probar que se cumple:

$$g_1H = g_2H \Rightarrow \bar{f}(g_1H) = \bar{f}(g_2H).$$

Por cómo es la definición de $\bar{f}$, esto equivale a probar que se cumple:

$$g_1H = g_2H \Rightarrow f(g_1) = f(g_2).$$

Para probar esto, la idea es usar que g_1 y g_2 están en la misma clase de equivalencia, para lograr escribir g_1 en función de g_2. Luego aplicar que f es un homomorfismo y que H es el núcleo de f.

Supongamos entonces que $g_1H = g_2H$. Esto es una igualdad de conjuntos, y equivale a la doble inclusión de los conjuntos. En particular: $g_1H \subseteq g_2H$. Entonces, para todo $h \in H$, existe $\hat{h} \in H$, tal que: $g_1h = g_2\hat{h}$. Despejando: $g_1 = g_2\hat{h}h^{-1}$. Ahora aplicamos f de ambos lados, y usamos que f es un homomorfismo:

$$f(g_1) = f(g_2\hat{h}h^{-1}) = f(g_2)f(\hat{h}h^{-1}).$$

Finalmente, como H es un subgrupo, podemos afirmar que $\hat{h}h^{-1} \in H$. Además, por definición, $H = ker(f)$. Es decir: $f(\hat{h}h^{-1}) = e_G$. Usando esto se obtiene la igualdad buscada: $f(g_1) = f(g_2)$.

2. $\bar{f}$ **es un homomorfismo**. Queremos probar que se cumple:

$$\bar{f}\left((g_1H)(g_2H)\right) = \bar{f}(g_1H)\bar{f}(g_2H), \quad \forall\ g_1H, g_2H \in G/\ker(f).$$

Para probarlo, primero usamos la definición del producto de clases laterales, y de la función candidata $\bar{f}$:

$$\bar{f}\left((g_1H)(g_2H)\right) = \bar{f}\left((g_1g_2)H\right) = f(g_1g_2).$$

Por otro lado, usando que f es un homomorfismo, y nuevamente la definición de $\bar{f}$:

$$f(g_1g_2) = f(g_1)f(g_2) = \bar{f}(g_1H)\bar{f}(g_2H).$$

3. $\bar{f}$ **es inyectiva**. Esto equivale a probar que el núcleo de $\bar{f}$ es el conjunto formado por el elemento neutro del grupo cociente $G/\ker(f)$. Es decir, queremos probar que se cumple: $\ker(\bar{f}) = \{\ker(f)\}$. Por definición de núcleo:

$$\ker(\bar{f}) = \{gH \in G/\ker(f)\ /\ \bar{f}(gH) = e_{Im(f)} = e_K\}.$$

A su vez, por definición: $\bar{f}(gH) = f(g)$. Por lo tanto, lo anterior equivale a:

$$\ker(\bar{f}) = \{gH \in G/ker(f) \ / \ f(g) = e_K\} = \{gH \in G/ker(f) \ / \ g \in ker(f)\}.$$

Recordemos que $H = \ker(f)$. Por lo tanto, por definición de clase lateral:

$$\ker(\bar{f}) = \{\{gh, \ h \in ker(f)\} \ / \ g \in ker(f)\} = \{ker(f)\}.$$

4. $\bar{f}$ **es sobreyectiva**. Sea $k \in Im(f)$. Por definición del conjunto imagen, existe $g \in G$, tal que: $k = f(g)$. Por lo tanto, por definición de $\bar{f}$, logramos probar que es sobreyectiva:

$$\forall \ k \in Im(f), \ \exists \ g \in G \ / \ k = f(g) = \bar{f}(gH).$$

□

Ejemplo 16. *Sean $(\mathbb{R}^*, \cdot)$ el grupo formado por el conjunto de los reales sin el cero, y $(\mathbb{R}^+, \cdot)$ el grupo formado por el conjunto de los reales positivos, ambos con la multiplicación usual.*

Vamos a probar que $\mathbb{R}^+$ es isomorfo al grupo cociente $\mathbb{R}^*/\{-1, 1\}$. Para esto basta con encontrar un homomorfismo $f : \mathbb{R}^* \to \mathbb{R}^+$, que cumpla: $Im(f) = \mathbb{R}^+$ y $ker(f) = \{-1, 1\}$. Veamos que la función valor absoluto cumple con lo buscado: $f(x) = |x|$.

1. *Es sencillo ver que f es un homomorfismo de grupos:*

$$f(xy) = |xy| = |x||y| = f(x)f(y), \ \forall \ x, y \in \mathbb{R}^*.$$

2. *Veamos que $Im(f) = \mathbb{R}^+$. Dado que f es siempre positiva en $\mathbb{R}^*$, se cumple: $Im(f) \subseteq \mathbb{R}^+$. Por otro lado, dado $x \in \mathbb{R}^+$, se cumple: $x = |x| = f(x)$. Esto último implica que f "alcanza" a todos los reales positivos.*

3. *Finalmente, veamos que $ker(f) = \{-1, 1\}$. El elemento neutro de $(\mathbb{R}^+, \cdot)$ es $e = 1$. Por lo tanto, por definición:*

$$\ker(f) = \{x \in \mathbb{R}^* \ / \ f(x) = 1\} = \{x \in \mathbb{R}^* \ / \ |x| = 1\} = \{-1, 1\}.$$

Por lo tanto, por el Primer Teorema de isomorfismos, se tiene:

$$\mathbb{R}^*/\{-1, 1\} = \mathbb{R}^*/ker(f) \simeq Im(f) = \mathbb{R}^+.$$

El siguiente resultado es consecuencia directa del Primer Teorema de Isomorfismos.

Corolario 1 (Teorema de órdenes)**.** *Sea $f : G \to K$ un homomorfismo de grupos. Entonces:*

$$|G| = |\ker(f)||Im(f)|.$$

Demostración. Vamos a probar únicamente el caso en que los grupos son de orden finito (el teorema vale aunque los grupos sean de orden infinito). Por el Primer Teorema de isomorfismos, los grupos $Im(f)$ y $G/\ker(f)$ son isomorfos. Esto implica que tienen la misma cantidad de elementos:

$$|Im(f)| = |G/\ker(f)|.$$

Por otro lado, por la Proposición 3, sabemos que el orden del cociente cumple:

$$|G/\ker(f)| = \frac{|G|}{|\ker(f)|}.$$

De estas dos igualdades se obtiene el resultado buscado. □

Observación 6. *Este último resultado es similar al teorema de las dimensiones visto en el curso de Álgebra Lineal. Este dice que si $T : V \to W$ es una transformación lineal (entre espacios vectoriales de dimensión finita), entonces:*

$$\dim(V) = \dim(Im(T)) + \dim(\ker(T)).$$

A continuación se enuncian los otros dos teoremas de isomorfismos. Estos se incluyen solamente a modo informativo, y no serán evaluados durante el curso.

Teorema 4 (Segundo teorema de isomorfismos)**.** *Sea G un grupo y sean H y K dos subgrupos* ***normales*** *de G, tales que: $K \subseteq H$. Entonces:*

1. *K es subgrupo normal de H (por lo que H/K es un grupo),*
2. *H/K es subgrupo normal de G/K (por lo que el cociente de ambos es un grupo), y*
3. *$\frac{G/K}{H/K}$ es isomorfo a G/H. Es decir:*

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

Demostración. Ver Teorema 1.5.2 de [1]. □

Teorema 5 (Tercer teorema de isomorfismos)**.** *Sea G un grupo y sean H y K dos subgrupos* ***normales*** *de G. Sea $HK = \{hk,\ h \in H,\ k \in K\}$. Entonces:*

- *HK es un subgrupo de G,*
- *H es un subgrupo* ***normal*** *de HK, y*
- *$K/(H \cap K) \simeq (HK)/H$.*

Demostración. Ver Teorema 1.5.3 de [1]. □

Bibliografía

[1] Anillos y sus categorías de representaciones (2007). Solotar, A., Farinati, M., Suárez-Álvarez, M. . Cuadernos de Matemática y Mecánica, IMAL (CONICET-UNL)-CIMEC (INTEC, CONICET-UNL). http://mate.dm.uba.ar/%7Easolotar/Publicaciones/libro.pdf.

[2] Notas de Matemática Discreta II (2016). Mariana Pereira, Claudio Qureshi, Gustavo Rama. Facultad de Ingeniería. Universidad de la República. Uruguay.

[3] Notas de teórico de Matemática Discreta 2 (2023, Semestre 2). Marco Pérez. Facultad de Ingeniería. Universidad de la República. Uruguay.