Notas de Álgebra Moderna 1: Introducción a la teoría de Grupos

Facultad de Ciencias, UNAM

Frank Patrick Murphy Hernandez

Jaime García Villeda

Índice general

Introducción

"El álgebra es la oferta hecha por el diablo al matemático. El diablo dijo: Te daré esta potente máquina, que responderá cualquier cuestión. Todo lo que necesitas es darme tu alma. Deja la geometría y te daré esta maravillosa máquina."

Michael Atiyah.

"Cuando un matemático dice que algo es *fácil de ver* o *trivial*, significa que espera que saques un lápiz y una hoja de papel, y dediques un poco de tiempo (probablemente considerable) revisandolo por ti mismo."

Jonathan Golan [**1**]

Capítulo 1

Básico de Grupos

"Las matemáticas son la más bella y la más poderosa creación del espíritu humano "

Stefan Banach.

1. Grupos

DEFINICIÓN 1.1 (Grupo). *Sea G un conjunto no vacío con una función $*\colon G\times G\longrightarrow G$. Notacionalmente escribimos $gh := *(g,h)$ para $g,h\in G$. Si esta función cumple:*

G1) Para $g,h,k\in G$, $g(hk)=(gh)k$.

G2) Existe $e\in G$ tal que para cualquier $g\in G$, $ge=g=eg$. A un elemento que cumpla esta propiedad lo llamamos un neutro del grupo.

G3) Para todo $g\in G$, existe $h\in G$ tal que $gh=e=hg$. A un elemento que cumpla esta propiedad lo llamamos un inverso de g.

Entonces llamamos a G un grupo.

Notamos que formalmente un grupo es una pareja $(G,*)$ pero cuando la operación se sobrentienda simplemente denotaremos al grupo por G.

PROPOSICIÓN 1.1. *Sea G un grupo. Entonces G tiene un único neutro.*

DEMOSTRACIÓN. Sea $e'\in G$ otro neutro. Entonces

$$e=ee'=e'e=e'$$

□

Como el neutro de un grupo es único, lo denotaremos por e

PROPOSICIÓN 1.2. *Sea G un grupo y $g\in G$. Entonces g tiene un único inverso.*

DEMOSTRACIÓN. Si existen $h,k\in G$ tales que $gh=e=hg$ y $gk=e=kg$. Entonces $gh=gk$, y multiplicando por la izquierda con h y asociando tenemos que $h=k$. □

Como el inverso de $g\in G$ es único, lo denotaremos por g^{-1}.

PROPOSICIÓN 1.3. *Sea G un grupo y $g_1,\dots,g_n \in G$. Si definimos recursivamente $h_1 = g_1$ y $h_{k+1} = h_k g_{k+1}$, entonces cualquier producto de $g_1,\dots,g_n$ en este preciso orden es igual a h_n sin importar el orden en que se apliquen los parentesis.*

DEMOSTRACIÓN. La prueba se hace por inducción sobre todas las sucesiones de longitud n de G. Podemos suponer que $n > 2$ y que $x \in G$ es un producto de $g_1,\dots,g_n$. Por lo que lo podemos expresar como $x = yz$ donde $y = g_1 \dots g_i$ y $z = g_{i+1} \dots g_n$ con $i = 1,\dots,n-1$. Si $z = g_n$, entonces $x = h_n$. Si no, entonces $z = y'z'$. Por hipotesis de inducción entonces $z = wg_n$. De donde tenemos que $x = (yw)g_n$ y apicando la hipotesis de inducción de nuevo $x = h_{n-1}g_n = h_n$. □

EJEMPLO 1.1. *Los enteros con la suma* $(\mathbb{Z},+)$.

EJEMPLO 1.2. *Los racionales con la suma* $(\mathbb{Q},+)$.

EJEMPLO 1.3. *Los reales con la suma* $(\mathbb{R},+)$.

EJEMPLO 1.4. *Los complejos con la suma* $(\mathbb{C},+)$.

EJEMPLO 1.5. *Sea $n \in \mathbb{N}$. Los enteros módulo n con la suma* $(\mathbb{Z}_n,+)$.

EJEMPLO 1.6. *Los racionales sin el cero con el producto* $(\mathbb{Q}\setminus\{0\},*)$.

EJEMPLO 1.7. *Los reales sin el cero con el producto* $(\mathbb{R}\setminus\{0\},*)$.

EJEMPLO 1.8. *Los complejos sin el cero con el producto* $(\mathbb{C}\setminus\{0\},*)$.

DEFINICIÓN 1.2. *Sea G un grupo. Diremos que G es un grupo abeliano, si para todo $g,h \in G$ $gh = hg$. En el caso de los grupos abelianos usaremos notación aditiva, es decir, escribiremos $g+h$ en vez de gh.*

Hasta el momento todos los ejemplos que se han dado son grupos abelianos.

DEFINICIÓN 1.3. *Sea X un conjunto. Ponemos como S_X al conjunto de todas la funciones biyectivas $\sigma\colon X \longrightarrow X$.*

PROPOSICIÓN 1.4. *Sea X un conjunto. Entonces S_X es un grupo con la composición de funciones como operación.*

DEMOSTRACIÓN. Primero notamos que la composición de funciones biyectivas es una función biyectiva por lo que la operación esta bien definida.

G1) La composición de funciones es asociativa.

G2) Sabemos que la función identidad 1_X en X es una función biyectiva. Por lo que para $\sigma \in S_X$, $\sigma 1_X = \sigma = 1_X \sigma$.

G3) Sabemos que toda función biyectiva es invertible.

□

EJEMPLO 1.9. *Consideramos las funciones $f, g \in S_{\mathbb{R}}$ dadas por $f(x) = x+1$ y $g(x) = x^3$ para toda $x \in \mathbb{R}$. Por lo que tenemos $f(g(x)) = x^3 + 1 \neq (x+1)^3 = g(f(x))$ y que $S_{\mathbb{R}}$ no es un grupo abeliano.*

DEFINICIÓN 1.4. *Si G es un grupo finito. Entonces definimos su orden, $|G|$, como su cardinalidad. En caso de que G sea infinito, diremos que su orden es infinito.*

EJEMPLO 1.10. *Para n natural y K un campo. Las matrices invertibles de n por n con entradas en K, $GL_n(K)$, son un grupo no abeliano para $n \geq 2$.*

2. Subgrupos

En esta sección se van a estudiar los subconjuntos de un grupo que heredan la estructura de este, es decir, la noción de subgrupo.

DEFINICIÓN 2.1 (Subgrupo). *Sea G un grupo. Un subconjunto $H \subseteq G$ es un subgrupo, lo que se denotará por $H \leq G$, si satisface las siguientes propiedades:*

SG1) $e \in H$

SG2) Para cualesquiera $g, h \in H$, $gh^{-1} \in H$.

Observemos que la definición dada de subgrupo es muy compacta en el sentido de que la segunda propiedad permite deducir que los subgrupos son subconjuntos cerrados bajo inversos, es decir, si $H \leq G$ y $g \in H$, entonces $g^{-1} \in H$. Además, esta segunda condición también implica que los subgrupos son cerrados bajo producto, es decir, que si $g, h \in H$, entonces $gh \in H$. Estas últimas observaciones son importantes pues empatan con la discusión previa a la definición y nos dicen que un subgrupo es un subconjunto de un grupo que es grupo al restringir la operación de G. De hecho, esta afirmación es equivalente a la definición de subgrupo, la desventaja que tiene es que como esta es más teórica es un poco difícil de aplicar a la hora de hacer ejemplos, pero por otro lado permite ver que los subgrupos son en efecto grupos. Esta última observación es interesante pues en muchas ocasiones se puede demostrar que ciertos conjuntos con una operación son grupos al ver que estos son subgrupos de algún otro grupo ya conocido.

Algunas caracterizaciones se encuentran en el siguiente resultado:

PROPOSICIÓN 2.1. *Sea $H \subseteq G$ con G un grupo. Las siguientes afirmaciones son equivalentes:*

1. $H \leq G$
2. *H cumple las siguientes propiedades:*
   - $e \in H$.
   - *Para cualquier $g \in H$, $g^{-1} \in H$.*
   - *Para cualesquiera $g,h \in H$, $gh \in H$.*
3. *La restricción de la operación de G a H, define una estructura de grupo en H.*

DEMOSTRACIÓN. $1 \Rightarrow 2$) La primera propiedad a probar es exactamente $SG1$. Para la segunda se observa que dado $g \in H$, por $SG2$ se tiene que $g^{-1} = eg^{-1} \in H$. Para la última afirmación se consideran $g,h \in H$. Por la afirmación demostrada $h^{-1} \in H$. Luego, al aplicar $SG2$ esto implica que $gh = g(h^{-1})^{-1} \in H$, donde se ha usado el ejercicio 10.

$2 \Rightarrow 3$) La tercera propiedad dice que el rango de la restricción $*|_{H\times H} : H \times H \to G$ es H. Así, lo que resta checar es que $(H, *|_{H\times H})$ es un grupo. Para esto es claro que $G1$ se cumple pues esta propiedad se cumple más generalmente para los elementos de G. La propiedad $G2$ es consecuencia de la primera propiedad que define a H. Para concluir $G3$ es consecuencia de la segunda propiedad que cumple H.

$3 \Rightarrow 1$) Para ver que se cumple $SG1$ lo único que se tiene que ver es que si $e_H \in H$ es el neutro según la estructura de grupo de $(H, *|_{H\times H})$, entonces $e_H = e$. En efecto, ya que como $e_H = e_H^2$, el que esta igualdad se cumpla en G implica que $e_H = e$. Además, la prueba de la propiedad $SG2$ es obvia. □

EJEMPLO 2.1. *Para G un grupo, se tiene que $\{e\} \leq G$ y $G \leq G$. A estos subgrupos se les conoce como subgrupos triviales.*

EJEMPLO 2.2. *Sea k un campo. Observe que el conjunto $\{A \in M_n(k) \mid A \text{ es invertible}\}$ es un grupo cuya operación es el producto de matrices usual y el neutro es la matriz identidad. A este grupo se le conoce como el grupo general lineal y se le denotará por $GL_n(k)$. Ahora considere el conjunto $\{A \in M_n(k) \mid \det(A) = 1\}$, al que se le va a denotar por $SL_n(k)$. Dado que toda una matriz cuadrada es invertible si y sólo si su determinante es*

diferente de cero, esto implica que se tiene la contención de conjuntos $SL_n(k) \subseteq GL_n(k)$. De hecho,

Afirmación: $SL_n(k)$ es subgrupo de $GL_n(k)$.

DEMOSTRACIÓN. De acuerdo a la definición hay que probar dos propiedades:

SG1) Dado que la matriz identidad, I_n, satisface que $\det(I_n) = 1$, entonces esto implica que $I_n \in SL_n(k)$.

SG2) Sean $A, B \in SL_n(k)$. Para concluir que $AB^{-1} \in SL_n(k)$ se tiene que calcular el determinante de dicha matriz y ver que este es uno, por lo que se tiene que:

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(B)^{-1} = 1^{-1} = 1$$

□

Por lo tanto, se ha probado que $SL_n(k) \leq GL_n(k)$. Al grupo $SL_n(k)$ se le conoce como el grupo especial lineal.[1]

Continuando con la lista de ejemplos, los cuales se presentarán de aquí en adelante sin demostración, tenemos:

EJEMPLO 2.3. *Dado $n \in \mathbb{Z}$, se observa que $n\mathbb{Z} \leq \mathbb{Z}$, donde $n\mathbb{Z}$ es el conjunto de múltiplos de n. De hecho, se puede probar que todos los subgrupos de $(\mathbb{Z}, +)$ tienen esa forma (ver ejercicio 18)*

EJEMPLO 2.4. $\{-1, 1\} \leq (\mathbb{R} \setminus \{0\}, *)$

EJEMPLO 2.5. *Si se denota por $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$, entonces $\mathbb{T} \leq (\mathbb{C} \setminus \{0\}, *)$. A este subgrupo se le conoce como el subgrupo toro. Más aún, dado $p \in \mathbb{N}$ primo, $\{e^{\frac{2\pi ik}{p^n}} \mid k, n \in \mathbb{N}^+\} \leq \mathbb{T}$.*

[1] Se recomienda ver el ejercicio 25.

Regresando a la teoría general, de la definición es claro que no todo subconjunto de un grupo puede ser un subgrupo. Sin embargo, hay una forma de asociarle a cada subconjunto de un grupo un subgrupo, y además esta tiene una propiedad muy interesante pues dicha construcción es mínima en un sentido que se explicará a su debido tiempo.

DEFINICIÓN 2.2 (Subgrupo generado). *Sean G un grupo y $S \subseteq G$. Decimos que $H \leq G$ es el subgrupo generado por S, si:*

1. $S \subseteq H$
2. *Si $K \leq G$ tal que $S \subseteq K$, entonces $H \subseteq K$.*

La definición puede parafrasearse de la siguiente forma: La primera propiedad dice que el subgrupo generado por S debe contener a dicho conjunto. Esto intuitivamente dice que lo que se está haciendo es agregarle todo lo que le falta a S para ser un subgrupo, que según la caracterización de los subgrupos es agregar el neutro si S no lo tiene, cerrar bajo productos a todos los elementos de S así como los que se están agregando y, además poner un inverso para cada elemento. Por otro lado, la segunda condición dice que este subgrupo es mínimo con esta propiedad respecto a la contención, es decir, dice que si hay otro subgrupo de G que contiene a S, entonces el subgrupo generado debe quedarse contenido en ese otro subgrupo. Esta última propiedad permite demostrar la unicidad de dicho subgrupo en caso de que exista, por lo tanto esto justifica el por qué se usó la frase "el subgrupo generado" y a su vez permite ponerle una notación, a saber, el subgrupo generado por S se va a denotar por $\langle S \rangle$.

PROPOSICIÓN 2.2. *Sea G un grupo y $S \subseteq G$. Si el subgrupo generado de S existe, entonces este es único.*

DEMOSTRACIÓN. Supóngase que $H, K \leq G$ son subgrupos generados por S. Dado que $S \subseteq K$, entonces al usar la segunda propiedad que cumple H por ser subgrupo generado por S se deduce que $H \subseteq K$. Además, como el argumento es simétrico se deduce que $K \subseteq H$ y por lo tanto $H = K$. □

Con la proposición anterior ahora podemos preocuparnos por la existencia de dicho subgrupo. Para ver que este existe se va a hacer una construcción abstracta que de paso permite probar una afirmación teórica de carácter general que es muy recurrente en contextos algebraicos, esto es, que la noción de subgrupo es estable bajo intersecciones.

LEMA 2.1. *La intersección de cualquier familia no vacía de subgrupos de un grupo dado es un subgrupo.*

DEMOSTRACIÓN. Sea $\{H_\alpha\}_{\alpha\in\Lambda}$ una familia de subgrupos de un grupo G con $\Lambda \neq \emptyset$. Veamos que $\bigcap_{\alpha\in\Lambda} H_\alpha$ cumple los axiomas de la definición.

*SG*1) Dado que para cualquier $\alpha \in \Lambda$ se tiene que $e \in H_\alpha$, entonces $e \in \bigcap_{\alpha\in\Lambda} H_\alpha$.

*SG*2) Supóngase que $g,h \in \bigcap_{\alpha\in\Lambda} H_\alpha$. Dado que para cualquier $\alpha \in \Lambda$ se tiene que $g,h \in H_\alpha$, entonces para cualquier $\alpha \in \Lambda$, $gh^{-1} \in H_\alpha$, lo que implica que $gh^{-1} \in \bigcap_{\alpha\in\Lambda} H_\alpha$. □

Otra operación conjuntista que puede llegar a la mente en estos momentos es la unión de subgrupos. Para una discusión se esta con la perspectiva del lema anterior consultar el ejercicio 21.

PROPOSICIÓN 2.3. *Sea G un grupo. Dado un conjunto $S \subseteq G$, el subgrupo generado por S siempre existe.*

DEMOSTRACIÓN. Considere el conjunto $\mathscr{S} = \{H \leq G \mid S \subseteq H\}$. Es claro que $\mathscr{S} \neq \emptyset$ pues $G \in \mathscr{S}$. Luego, al considerar $\langle S\rangle := \bigcap \mathscr{S}$, es claro del lema anterior que $\langle S\rangle \leq G$ y además por construcción $S \subseteq \langle S\rangle$. Por otro lado, si $H \leq G$ tal que $S \subseteq H$, entonces $H \in \mathscr{S}$, por lo que $\langle S\rangle \subseteq H$ pues $\langle S\rangle$ es el ínfimo de la familia $\mathscr{S}$ con el orden definido por la contención. □

La construcción realizada tiene algunas propiedades generales las cuales se enuncian en el siguiente resultado.

PROPOSICIÓN 2.4. *Sean G un grupo y $S,T \subseteq G$. Se tienen las siguientes propiedades:*

1. $\langle\emptyset\rangle = \{e\}$
2. *Si* $S \subseteq T$, *entonces* $\langle S\rangle \subseteq \langle T\rangle$
3. $\langle\langle S\rangle\rangle = \langle S\rangle$
4. *S es un subgrupo si y sólo si* $\langle S\rangle = S$

DEMOSTRACIÓN. Dado que $\emptyset \subseteq \{e\}$, de la definición de subgrupo generado se tiene que $\langle\emptyset\rangle \subseteq \{e\}$, lo que obviamente implica la primera igualdad.

Para la segunda afirmación, si $S \subseteq T$, entonces $S \subseteq \langle T\rangle$ por transitividad de la contención. Por ser $\langle T\rangle$ es subgrupo, de la definición de subgrupo generado dicha contención implica que $\langle S\rangle \subseteq \langle T\rangle$.

Para la tercera igualdad, por definición de subgrupo generado se tiene que $\langle S\rangle \subseteq \langle\langle S\rangle\rangle$. Por otro lado como $\langle S\rangle \subseteq \langle S\rangle$ y $\langle S\rangle$ es un subgrupo, entonces por definición $\langle\langle S\rangle\rangle \subseteq \langle S\rangle$, donde estas contenciones implican la igualdad buscada.

Para la cuarta afirmación, respecto a la ida note primeramente que $S \subseteq \langle S\rangle$ por definición. Por otro lado $S \subseteq S$ y S es un subgrupo, lo que implica nuevamente por definición que $\langle S\rangle \subseteq S$, probando así la igualdad. Nótese que el regreso de la afirmación es obvio. □

Es importante notar que para la prueba de esta proposición no se usó la construcción con la que se definió el subgrupo generado, solamente se usaron los axiomas que lo definen. Esta característica muestra que la prueba dada es muy general.

Antes de continuar vale la pena hacer una pequeña discusión. Para esto denote por $Sub(G)$ al conjunto de subgrupos de G.[2] Luego, observe que la construcción generado permite definir una función cuyo dominio es el conjunto potencia de G y el codominio $Sub(G)$

$$\langle\_\rangle : \wp(G) \to Sub(G)$$

Observe que esta función no es inyectiva pues $\langle\emptyset\rangle = \langle\{e\}\rangle = \{e\}$. Además por la afirmación 4 de la proposición anterior se deduce que esta es suprayectiva. Al observar que $Sub(G) \subseteq \wp(G)$ tiene sentido preguntarnos por los puntos fijos de esta función, y precisamente la afirmación 4 de la proposición anterior dice que los puntos fijos son precisamente $Sub(G)$. Para concluir se recuerda que $\wp(G)$ es un conjunto parcialmente ordenado con la contención, por lo que $Sub(G)$ admite dicha estructura también. Por lo tanto, la propiedad 2 de la proposición dice que esta función preserva el orden. Este tipo de cuestiones de orden se discutirán a mayor profundidad en la sección 7 del presente capítulo.

Para concluir esta sección se va a obtener una descripción más tangible del subgrupo generado por un conjunto. Antes de esto se requieren algunas definiciones previas.

DEFINICIÓN 2.3. *Dado G un grupo y $g \in G$, se define recursivamente la función "elevar a la $n \in \mathbb{N}$" como sigue:*

1. $g^0 = e$
2. *Para todo $n \in \mathbb{N}$, $g^{n+1} = g^n g$*

Además esta función se puede extender para exponentes negativos al escribir $g^{-n} = (g^{-1})^n$

[2]Para los conjuntistas noten que esto es en efecto un conjunto

Algunas propiedades aritméticas básicas de la definición anterior se encuentran en el ejercicio 9.

DEFINICIÓN 2.4 (Palabras). *Sea $S \subseteq G$. Una palabra en S es un elemento de G de la forma*

$$s_1^{k_1} \cdots s_n^{k_n},$$

donde $n \in \mathbb{N}$, $s_1, ..., s_n \in S$ y $k_1, ..., k_n \in \{-1, 1\}$. Si $n = 0$ ó $S = \emptyset$, la palabra correspondiente se conoce como la palabra vacía y esta es por definición e.

PROPOSICIÓN 2.5. *Dado $S \subseteq G$, $\langle S \rangle$ es el conjunto de todas las palabras en S.*

DEMOSTRACIÓN. Si $S = \emptyset$, entonces $\langle S \rangle = \{e\}$ y por otro lado la única palabra que se puede formar es la palabra vacía que por definición es el neutro. Así, supóngase que $S \neq \emptyset$. Para probar la igualdad que se quiere observe que obviamente el conjunto de palabras en S contiene a S. Como el producto de dos palabras en S es una nueva palabra en S, salvo quizás reescribir algunos términos de esta, y como el inverso de una palabra en S sigue siendo una palabra en S (ejercicio 10), entonces el conjunto de palabras en S es un subgrupo de G y por lo tanto el generado por S está contenido en el conjunto de palabras en S. Por otro lado toda palabra en S claramente es elemento de $\langle S \rangle$, lo que da la igualdad buscada. □

EJEMPLO 2.6. *Dado $g \in G$, $\langle \{g\} \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Además, notacionalmente se escribirá $\langle g \rangle := \langle \{g\} \rangle$.*

DEFINICIÓN 2.5. *Sea G un grupo y $g \in G$. Definimos el orden de g, $o(g)$, como $|\langle g \rangle|$, cuando este cardinal es finito.*

3. Grupos Cíclicos

DEFINICIÓN 3.1. *Sea G un grupo. Decimos que G es cíclico si existe $g \in G$ tal que $G = \langle g \rangle$.*

EJEMPLO 3.1. *Los enteros $\mathbb{Z}$ son un grupo cíclico.*

EJEMPLO 3.2. *Los enteros módulo n $\mathbb{Z}_n$ son un grupo cíclico.*

Notamos que el elemento que genera al grupo cíclico no necesariamente es único, por ejemplo, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ y $\mathbb{Z}_3 = \langle 1 \rangle = \langle 2 \rangle$

PROPOSICIÓN 3.1. *Todo subgrupo de un grupo cíclico es cíclico.*

DEMOSTRACIÓN. Sea G grupo cíclico y $H \leq G$. Entonces existe $g \in G$ tal que $G = \langle g \rangle$. Sea n el mínimo natural positivo tal que $g^n \in H$. Afirmamos que $H = \langle g^n \rangle$. Es obvio que $\langle g^n \rangle \subseteq H$. Procedemos a demostrar la otra contención. Sea $h \in H$. Por pertenecer a G es una potencia de g, es decir, existe $m \in \mathbb{N}$ tal que $h = g^m$. Aplicamos en algoritmo de la división a m y n, por lo que existen $q \in \mathbb{Z}$ y $r \in \mathbb{N}$ tales que $m = nq + r$ con $0 \leq r < n$. Notemos que $g^r = g^{m-nq} = g^m g^{-nq} \in H$. Si $r > 0$, entonces se contradice la minimalidad de n, por lo que la única opción es que $r = 0$. Por lo tanto $h \in \langle g^n \rangle$. □

PROPOSICIÓN 3.2. *Sea G un grupo y $g \in G$ un elemento de orden n y $k \in \mathbb{Z}$ tal que $g^k = e$. Entonces $n \mid k$.*

DEMOSTRACIÓN. Aplicamos el algoritmos de la división a n y a k. Entonces existen $q \in \mathbb{Z}$ y $r \in \mathbb{N}$ tales que $k = nq + r$ con $0 \leq r < n$. Por lo que $g^r = g^{k-nq} = g^k g^{-nq} = e$. Si $r > 0$ entonces $\langle g \rangle$ tendría a lo más r elementos contradiciendo que tiene n. Por lo que $r = 0$ y $n \mid k$. □

PROPOSICIÓN 3.3. *Si G es un grupo cíclico finito de orden n. Entonces tiene un único subgrupo de orden d para todo d divisor de n.*

DEMOSTRACIÓN. Como G es cíclico entonces existe $g \in G$ con $G = \langle g \rangle$. Sea d divisor de n. Entonces existe $k \in \mathbb{N}$ tal que $dk = n$. Afirmamos que $\langle g^k \rangle$ es un subgrupo de orden d. En efecto, $(g^k)^d) = g^{kd} = g^n = e$, y este es el mínimo natural con respecto a esta propiedad, dado que si no lo fuese contradiría el hecho de que el orden de g es n.

Sea H otro subgrupo de orden d. Además sabemos que H es cíclico por el ejercicio ... . Por lo que $H = \langle h \rangle$ para algún $h \in G$. De esto, existe un $m \in \mathbb{N}$ tal que $g^m = h$. Entonces

$g^{md} = e$ y por la proposición anterior $n \mid md$. De donde existe $s \in \mathbb{Z}$ tal que $ns = md$. Si consideramos que $dk = n$, entonces $ks = m$. Por lo que $h = g^m = g^{ks}$. Por lo que $h \in \langle g^k \rangle$. De aquí $H \leq \langle g^k \rangle$. Como ambos subgrpos tienen orden d se sigue que son iguales. □

PROPOSICIÓN 3.4. *Si G es un grupo cíclico finito de orden n y $g \in G$ tal que $G = \langle g \rangle$. Entonces $\langle g^k \rangle = G$ si y sólo si $(k,n) = 1$.*

DEMOSTRACIÓN. $\Rightarrow$) Si $\langle g^k \rangle = G$, entonces existe $m \in \mathbb{N}$ tal que $g^{km} = g$. Por lo que $g^{km-1} = e$. Se sigue que $n \mid km - 1$. De donde $(k,n) = 1$.

$\Leftarrow$) Si $(k,n) = 1$, entonces existen $s,t \in \mathbb{Z}$ tales que $ks + nt = 1$. Por lo que $g = g^{ks+nt} = g^k s$. De aquí $g \in \langle g^k \rangle$ y por lo tanto $\langle g^k \rangle = G$. □

DEFINICIÓN 3.2. *Sea G un grupo cíclico. Denotamos por $Gen(G)$ el conjunto de generadores de G.*

PROPOSICIÓN 3.5. *Sea G un grupo. Entonces $G = \bigsqcup_{C \in \mathscr{C}(G)} Gen(C)$.*

DEMOSTRACIÓN. $\subseteq$) Sea $g \in G$. Entonces $\langle g \rangle \in \mathscr{C}(G)$ y $g \in Gen(\langle g \rangle)$. Por lo tanto $g \in \bigsqcup_{C \in \mathscr{C}(G)} Gen(C)$.

$\supseteq$) Notemos que para cada $C \in \mathscr{C}(G)$ tenemos que $Gen(C) \subseteq C \leq G$. Por lo tanto $\bigcup_{C \in \mathscr{C}(G)} Gen(C) \subseteq G$. Falta ver que la unión es disjunta. Sean $C_1, C_2 \in \mathscr{G}$ tales que $Cen(C_1) \cap Gen(C_2) \neq \emptyset$. Entonces existe $g \in Cen(C_1) \cap Gen(C_2)$. Por lo que $C_1 = \langle g \rangle = C_2$. Por lo tanto la unión es disjunta. □

DEFINICIÓN 3.3. *Definimos la ϕ de Euler como $\phi : \mathbb{N}^+ \longrightarrow \mathbb{N}$ dada por:*

$$\phi(n) := |\{1 \leq k \leq n \mid (k,n) = 1\}|$$

para toda $n \in \mathbb{N}^+$.

Observamos que $|Gen(\mathbb{Z}_n)| = \phi(n)$.

DEFINICIÓN 3.4. *Sea G un grupo . Denotamos por $\mathscr{C}(G)$ el conjunto de subgrupos cíclicos de G.*

PROPOSICIÓN 3.6. *Sea $n \in \mathbb{N}$. Entonces $n = \sum_{d \mid n} \phi(d)$.*

DEMOSTRACIÓN. Si G es un grupo. Entonces $G = \bigsqcup_{C \in \mathscr{C}(G)} Gen(C)$. Esto pasa en particular para $G = \mathbb{Z}_n$. □

PROPOSICIÓN 3.7. *Sea G un grupo finito de orden n. Si G tiene a lo más un subgrupo de orden d para cada d divisor de n, entonces G es cíclico.*

DEMOSTRACIÓN. Como $G = \bigsqcup_{C \in \mathscr{C}(G)} Gen(C)$. Entonces

$$n = |G| = \sum_{C \in \mathscr{C}(G)} |Gen(C)| \leq \sum_{d|n} \phi(d) = n$$

Por lo que G tiene que tener exactamente un subgrupo cíclico de orden d para todo d divisor de n. En particular para n. □

PROPOSICIÓN 3.8. *Sea G un grupo de orden n tal que para cada d divisor de n existe a lo más d elementos g tales que $g^d = e$. Entonces G tiene a lo más un subgrupo de orden d para cada d divisor de n.*

DEMOSTRACIÓN. Si H es un subgrupo de orden d, entonces $h^d = e$ para toda $h \in H$. Si existiesen más de un subgrupo de orden d entonces se tendría más de d elementos g tales que $g^d = e$. Contadiciendo la hipótesis. □

Notamos que estas son condiciones para que un grupo finito sea cíclico.

DEFINICIÓN 3.5. *Sea K un campo. Denotamos por K^* a $K \setminus \{0\}$ con estructura de grupo dada por la multiplicación*

COROLARIO 3.1. *Si K es un campo y G es un subgrupo finito de K^*. Entonces G es cíclico.*

DEMOSTRACIÓN. Si G tiene orden n y d es un divisor de n. Entonces el polinomio $x^d - 1 \in K[x]$ tiene a lo más d soluciones. Por lo que se cumplen las hipótesis de la proposición pasada. □

PROPOSICIÓN 3.9. *Si K es un campo finito. Entonces el grupo K^* es cíclico.*

Vale la pena mencionar que el resultado anterior es un corolario, pero dado a su bastas aplicaciones en cuestiones practicas le dejo el nombre proposición.

4. Grupos de Permutaciones

La pregunta de cuándo S_X es abeliano se presenta en el siguiente resultado. Se recomienda ver el ejercicio 47 para complementarlo.

PROPOSICIÓN 4.1. *Sea X un conjunto. Entonces S_X es un grupo abeliano si y sólo si $|X| < 3$.*

DEMOSTRACIÓN. $\Rightarrow$) (Por contrapositiva) Supóngase que $|X| \geq 3$. Luego sean $x_1, x_2, x_3 \in X$ elementos distintos. Para ver que S_X no es abeliano se van a construir dos elementos de este que no conmutan, por lo que sean $f, g : X \to X$ definidos mediante:

$$f|_{X\setminus\{x_2,x_3\}} = 1_{X\setminus\{x_2,x_3\}},\ f(x_2) = x_3 \text{ y } f(x_3) = x_2$$
$$g|_{X\setminus\{x_1,x_2\}} = 1_{X\setminus\{x_1,x_2\}},\ g(x_1) = x_2 \text{ y } g(x_2) = x_1$$

Observe que por definición es claro que $f, g \in S_X$. Más aún, $fg \neq gf$ ya que $fg(x_1) = x_3 \neq x_2 = gf(x_1)$.

$\Leftarrow$) Si $|X| < 3$, entonces se tienen tres casos:

C1) Si $|X| = 0$, entonces $X = \emptyset$ y así $S_X = \{1_\emptyset\}$, que es claramente abeliano.

C2) Si $|X| = 1$, entonces $X = \{*\}$ y por lo tanto $S_X = \{1_X\}$, que es claramente abeliano como en el caso anterior.

C3) Si $|X| = 2$, entonces supongamos que $X = \{a, b\}$. Luego $S_X = \{1_X, \tau\}$, donde $\tau(a) = b$ y $\tau(b) = a$ y en este caso también es claro que S_X es abeliano.

□

DEFINICIÓN 4.1. *Sea X un conjunto y $\sigma \in S_X$. Definimos el soporte de σ, $sop(\sigma)$, como los elementos $x \in X$ tales que $\sigma(x) \neq x$ y los puntos fijos de σ, $fix(\sigma)$, como los elementos $x \in X$ tales que $\sigma(x) = x$.*

Observamos que todo $\sigma \in S_X$ particiona a X con $\{sop(\sigma), fix(\sigma)\}$.

El estudio general de los grupos S_X puede ser difícil ya que como se verá posteriormente estos contienen una copia de cada grupo. En lugar de esto se va a particularizar nuestro estudio considerando $X = \{1, ..., n\}$ donde $n \in \mathbb{N}$, es decir, los conjuntos formados por los primeros n naturales empezando desde el 1. Es importante decir que incluso al hacer esto se están diciendo cosas de S_X para cualquier X finito pues posteriormente se dispondrá de la herramienta para ver que cuando dos conjuntos son biyectables estos producen el mismo grupo de permutaciones, luego, esto justificará la elección de los conjuntos tomados ya que estos son los representantes canónicos para modelos de finitud. En este caso es común denotar $S_n := S_{\{1,...,n\}}$. Más aún, es un hecho conocido de la combinatoria que

$$|S_n| = n!$$

Continuando con las particularidades obtenidas de esta reducción es importante discutir la existencia de dos notaciones usadas para representar las permutaciones de S_n. La primera de ellas es asociar una matriz $M_{2\times n}(\mathbb{Z})$ a cada elemento de S_n. Esta se construye al poner en el primer renglón cada uno de los elementos de $\{1, ..., n\}$ según el orden usual y debajo

de cada uno el valor que le corresponde para la permutación considerada. Así, si $\sigma \in S_n$, la matriz asociada tiene la forma:

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

Por ejemplo la permutación identidad $1_{\{1,...,n\}}$ se escribe

$$1_{\{1,...,n\}} = \begin{pmatrix} 1 & .... & n \\ 1 & ... & n \end{pmatrix}$$

Un ejemplo menos general se obtiene al considerar $\sigma \in S_3$ cuya regla de correspondencia es $\sigma(1) = 1$, $\sigma(2) = 3$ y $\sigma(3) = 2$, para la cual se escribe

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Respecto a la segunda notación hay que desarrollar teoría previa.

4.1. Notación cíclica.

DEFINICIÓN 4.2 (k-ciclo). *$\sigma \in S_n$ es un k-ciclo si existen $i_1, ..., i_k \in \{1, ..., n\}$ distintos tales que*

$$\sigma(i_1) = i_2, ..., \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$$

Mientras que $fix(\sigma) = \{1, ..., n\} \setminus \{i_1, ..., i_k\}$. En tal caso se escribe $\sigma = (i_1....i_k)$.

Observe que por definición los 1-ciclos son la permutación identidad y esta se denota por (1) aunque hay ocaciones que se suele escribir (k) para $k \in \{1, ..., n\}$. Por otro lado a los 2-ciclos se les conoce como transposiciones, mientras que a los 3-ciclos como triciclos.

Nótese que el último ejemplo de permutaciones discutido es una transposición y esta se escribe en notación cíclica por (23). Un ejemplo más elaborado se obtiene al considerar $\sigma \in S_6$ definido por

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

Es claro que esta permutación no es un ciclo. Sin embargo esta está formada por dos ciclos: el triciclo (123) y la transposición (45). Nótese entonces que σ se puede ver como la composición de estos dos ciclos por lo que σ se puede escribir en la notación cíclica mediante:

$$\sigma = (123)(45)$$

Este es un ejemplo de cómo escribir una permutación usando la segunda notación a la que se le conoce como cíclica. Vale la pena comentar que por el ejercicio 43 dicha descomposición no depende del orden en el que se escriben los factores, para lo que es necesario el siguiente concepto.

DEFINICIÓN 4.3 (Permutaciones ajenas). *Dos permutaciones $\sigma, \tau \in S_n$ son ajenas si $sop(\tau) \subseteq fix(\sigma)$ y $sop(\sigma) \subseteq fix(\tau)$.*

En estos momentos vamos a ver que toda permutación posee una descomposición como producto de ciclos, que es la segunda forma de representar una permutación.

PROPOSICIÓN 4.2. *Toda permutación es producto de ciclos ajenos*

DEMOSTRACIÓN. La prueba se va a hacer por inducción generalizada sobre la cardinalidad del soporte de las permutaciones. Sea $\sigma \in S_n$ y escribamos $k = |sop(\sigma)|$.

Base: $k = 0$. En este caso σ no mueve ningún elemento, es decir σ es la permutación identidad que es un 1-ciclo.

Paso inductivo: Supóngase que el resultado vale para las permutaciones cuyo soporte tiene cardinalidad menor a $k > 0$. Luego, sea $i_1 \in sop(\sigma)$ y definimos $i_{l+1} := \sigma^l(i_1)$ para $l \in \mathbb{N}$. Ya que $\{i_l \mid l \in \mathbb{N}\} \subseteq \{1, ..., n\}$, sea $r \in \mathbb{N}$ el mínimo índice tal que $i_{r+1} \in \{i_1, ..., i_r\}$. Observe que por ser σ una biyección se tiene que $\sigma(i_r) = i_1$. Si $r = n$ entonces $\sigma = (i_1 ... i_r)$ por lo que σ es un r-ciclo. En caso contrario note que se puede definir $\sigma' \in S_n$ mediante $\sigma'|_{\{i_1,...,i_r\}} = 1_{\{i_1,...,i_r\}}$ y $\sigma'|_{\{1,...,n\}\setminus\{i_1,...,i_r\}} = \sigma|_{\{1,...,n\}\setminus\{i_1,...,i_r\}}$. Luego se tiene que $\sigma = (i_1 ... i_r)\sigma'$ y $|sop(\sigma')| < k$, por lo que la hipótesis inductiva implica que σ' tiene descomposición como producto de ciclos ajenos. Para concluir nótese que como $(i_1 ... i_r)$ y σ' son ajenas, la descomposición es la buscada. □

Para poder establecer el teorema de unicidad que se espera es necesario controlar las factorizaciones por ciclos para que estas no sean artificiales.

DEFINICIÓN 4.4 (Factorización completa). *Una factorización completa de una permutación $\sigma \in S_n$ es una factorización como producto de ciclos ajenos que contiene un 1-ciclo (i) por cada $i \in fix(\sigma)$.*

Nótese que la definición anterior es la que logra hacer el trabajo buscado ya que no pueden agregarse identidades arbitrarias y además cada elemento en $\{1,...,n\}$ pertenece exactamente a un ciclo. Además realmente la única parte que falta probar es la unicidad de la factorización ya que la existencia se deduce de la proposición anterior.

PROPOSICIÓN 4.3. *La factorización completa de una permutación $\sigma \in S_n$ es única salvo el orden en el que ocurren los factores.*

DEMOSTRACIÓN. Supóngase que $\sigma = \sigma_1 \cdots \sigma_l = \tau_1 \cdots \tau_s$ son factorizaciones completas de σ, donde observe que podemos quitar los 1-ciclos presentes pues estos son identidades y aparecen exactamente los mismos es cada una de las factorizaciones pues estos son puntos fijos de σ. Además supongamos sin pérdida de generalidad que $l \leq s$. Considere entonces $i_1 \in sop(\sigma_l)$ y observe que como σ_l es ajeno con $\sigma_1, ..., \sigma_{l-1}$, entonces para cualquier $k \in \mathbb{N}$, $\sigma^k(i_1) = \sigma_l^k(i_1)$. Por otro lado observe que existe un único $\tau_{j(l)}$ tal que $i_1 \in sop(\tau_{j(l)})$ y, dado que todas las permutaciones de la segunda factorización son ajenas entre sí, podemos suponer sin pérdida de generalidad que $\tau_{j(l)} = \tau_s$ por el ejercicio 43. Observe que nuevamente para cualquier $k \in \mathbb{N}$ se tiene que $\sigma^k(i_1) = \tau_s^k(i_1)$, lo que implica que $\tau_s^k(i_1) = \sigma_l^k(i_1)$. Más aún, como τ_s y σ_l son ciclos, esto implica que $\tau_s = \sigma_l$ y por lo tanto la igualdad $\sigma_1 \cdots \sigma_l = \tau_1 \cdots \tau_s$ implica que $\sigma_1 \cdots \sigma_{l-1} = \tau_1 \cdots \tau_{s-1}$. Observemos que el argumento anterior puede repetirse hasta obtener la igualdad $(1) = \tau_1 \cdots \tau_{s-l}$, de donde es claro que $s = l$ pues en otro caso al aplicar nuevamente el ejercicio 43 se tendría que $\tau_1 = ... = \tau_{s-l} = (1)$, lo cual es imposible pues inicialmente se habían eliminado todos los 1-ciclos. Esto concluye la prueba. □

Para concluir la sección vamos a ver que S_3 tiene como subgrupo al grupo de simetrías de un triángulo equilátero lo cual además de mostrar la importancia de los grupos de permutaciones, nos permitirá dar un poco de práctica a la notación cíclica. Observemos que uno de tales triángulos tiene dos tipos de simetrías: rotaciones por múltiplos de 120° y reflexiones respecto a las medianas del triángulo. Estas transformaciones pueden codificarse mediante elementos de S_3 pues si se numeran los vértices del triángulo, cada una de estas transformaciones se puede codificar con una permutación de los vértices (ver figura 1). Por ejemplo, si r es la rotación por 120°, esta está codificada por el triciclo (123) pues esta dice que el primer vértice va al segundo, el segundo al tercero y el tercero al primero. Luego observe que la rotación por 240° corresponde a $r^2 = (123)(123) = (132)$ y la rotación por 360° es la identidad pues $r^3 = (1)$. Por otro lado la reflexión respecto a la mediatriz $M1$ está codificada por la transposición $s_1 = (23)$, respecto a la mediatriz $M2$ por $s_2 = (12)$ y respecto a $M3$ por $s_3 = (13)$. De manera geométrica nótese que el hacer una rotación de 120° y después una reflexión respecto a $M2$ esto da como resultado la reflexión respecto a la mediatriz $M1$ (ver figura 2). Esto se obtiene de manera algebraica pues

$\circ$	(1)	r	r^2	s_1	s_2	s_3
(1)	(1)	r	r^2	s_1	s_2	s_3
r	r	r^2	(1)	s_2	s_3	s_1
r^2	r^2	(1)	r	s_3	s_1	s_2
s_1	s_1	s_3	s_2	(1)	r^2	r
s_2	s_2	s_1	s_3	r	(1)	r^2
s_3	s_3	s_2	s_1	r^2	r	(1)

TABLA 1.

$s_2r = (12)(123) = (23)$. Las operaciones restantes se muestran en la tabla 1. Adaptando esta idea uno puede considerar el grupo de simetrías de un n-gono regular como subgrupo de S_n.

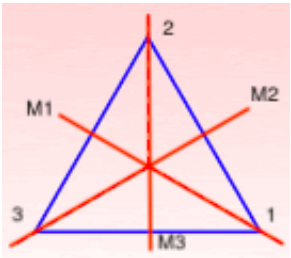


FIGURA 1.

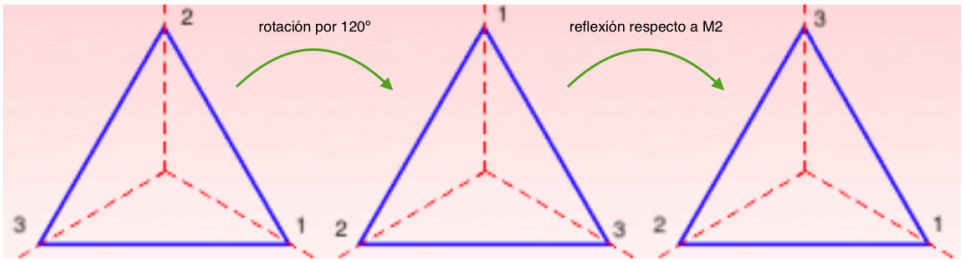


FIGURA 2.

4.2. El signo de una permutación. Continuando con la teoría general existe una asignación que se le puede hacer a cualquier permutación. Para definirla se requieren de algunos conceptos previos.

DEFINICIÓN 4.5. *Para $n \in \mathbb{N}$ se define el polinomio de Vandermonde, el que se denota por $V(x_1,...,x_n) \in \mathbb{Z}[x_1,...,x_n]$, como:*

$$V(x_1,...,x_n) = \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

Además, dada $\sigma \in S_n$ se define el polinomio $V^\sigma(x_1,...,x_n) \in \mathbb{Z}[x_1,...,x_n]$ mediante

$$V^\sigma(x_1,...,x_n) := V(x_{\sigma(1)},...,x_{\sigma(n)})$$

EJEMPLO 4.1. *Considere $\sigma \in S_4$ dado por $\sigma = (123)$. De la definición se tiene que*

$$\begin{aligned} V^\sigma(x_1,...,x_4) &:= \prod_{1 \leq i < j \leq 4} (x_{\sigma(j)} - x_{\sigma(i)}) \\ &= (x_{\sigma(2)} - x_{\sigma(1)})(x_{\sigma(3)} - x_{\sigma(1)})(x_{\sigma(4)} - x_{\sigma(1)})(x_{\sigma(3)} - x_{\sigma(2)})(x_{\sigma(4)} - x_{\sigma(2)})(x_{\sigma(4)} - x_{\sigma(3)}) \\ &= (x_3 - x_2)(x_1 - x_2)(x_4 - x_2)(x_1 - x_3)(x_4 - x_3)(x_4 - x_1) \\ &= V(x_1,...,x_4) \end{aligned}$$

Observe que $V^\sigma(x_1,...,x_n)$ siempre es un múltiplo del polinomio de Vandermonde cuyos únicos coeficientes posibles son 1 ó -1 pues por ser $\sigma \in S_n$ biyectiva, cada término $x_j - x_i$ del polinomio de Vandermonde tiene su correspondiente en $V^\sigma(x_1,...,x_n)$ con a lo más un cambio de signo para lo cual hay que analizar casos pues dados $1 \leq i < j \leq n$ se tiene:

C1) $i, j \in fix(\sigma)$: la afirmación es obvia.
C2) $i \in fix(\sigma)$ y $j \in sop(\sigma)$: existe $k \in \{1,...,n\}$ tal que $\sigma(k) = j$. Observe que $k \neq i, j$. Entonces se tienen posibilidades $i > k$ o $i < k$. En el primer caso se tiene el término $x_i - x_j$ en $V^\sigma(x_1,...,x_n)$ y en el segundo caso $x_j - x_i$; en cualquier caso se tiene el resultado.
C3) $j \in fix(\sigma)$ y $i \in sop(\sigma)$: Es análogo al anterior.
C4) $i, j \in sop(\sigma)$: existen $k, l \in \{1,...,n\}$ tales que $\sigma(k) = i$ y $\sigma(l) = j$. Entonces $k \neq l$ y como esto implica que $k < l$ ó $k > l$, este caso se concluye como antes.

Con lo anterior en mente se da el siguiente concepto.

DEFINICIÓN 4.6. *Dado $\sigma \in S_n$, se define el signo de dicha permutación, el que se denota por $sgn(\sigma)$, mediante:*

$$sgn(\sigma) = \frac{V^\sigma(x_1,...,x_n)}{V(x_1,...,x_n)}$$

Por la observación previa a la definición se observa que esto da lugar a una función

$$sgn : S_n \to \{-1, 1\}$$

Nótese que esta función es suprayectiva cuando $n \geq 2$. Por lo tanto, esto permite dar una partición de S_n. A las permutaciones con signo 1 se les llama pares y a las permutaciones con signo -1 se les llama impares.

EJEMPLO 4.2. *Para* $(1) \in S_n$ *es claro que* $sgn(1) = 1$. *Además, para cualquier* $\tau \in S_n$ *transposición se tiene que* $sgn(\tau) = -1$. *También observe que del último ejemplo, para* $(123) \in S_4$ *se tiene que* $sgn(123) = 1$.

Vale la pena comentar que el tratamiento de la función signo dado no es canónico. La mayoría de las definiciones canónicas tienen que ver con un estudio más profundo de la estructura cíclica de una permutación, a saber, después de probar que toda permutación se descompone como producto de ciclos, el siguiente paso es descomponer todo ciclo como producto de transposiciones y entonces definir el signo usando la paridad del número de transposiciones que conforman una permutación. Por supuesto que esto requiere más trabajo pues hay que probar la independencia de la paridad en las descomposiciones de una permutación, lo que puede ser un poco trabajoso. Además, la siguiente proposición también cuesta algo de trabajo de demostrar en dicho contexto pues hay que hacer algunos pasos previos, sin embargo, con la definición presentada todo se vuelve muy sencillo.

PROPOSICIÓN 4.4. *Para cualesquiera* $\sigma, \tau \in S_n$ *se cumple que*

$$sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$$

DEMOSTRACIÓN. Claramente se tienen las siguientes igualdades,

$$sgn(\sigma\tau) = \frac{V^{\sigma\tau}(x_1, ..., x_n)}{V(x_1, ..., x_n)} = \frac{V^{\sigma\tau}(x_1, ..., x_n)}{V^{\tau}(x_1, ..., x_n)} \frac{V^{\tau}(x_1, ..., x_n)}{V(x_1, ..., x_n)}$$

Es claro que el segundo cociente es por definición $sgn(\tau)$. En lo que respecta al primer cociente observe que este es igual a $sgn(\sigma)$ ya que estos polinomios se pueden considerar en el anillo $\mathbb{Z}[x_{\tau(1)}, ..., x_{\tau(n)}]$ por lo que al hacer el cambio de variable obvio se obtiene el resultado. □

Un corolario directo de esta proposición es que el signo de una permutación es el mismo que el de su inversa. Un hecho mucho más importante es el siguiente.

PROPOSICIÓN 4.5. *Defina* $A_n := \{\sigma \in S_n \mid sgn(\sigma) = 1\} \subseteq S_n$. *Entonces* $A_n \leq S_n$.

DEMOSTRACIÓN. Vamos a ver que A_n satisface las propiedades que definen a los subgrupos.

SG1) Anteriormente se dijo que $sgn(1) = 1$ por lo que $(1) \in A_n$.

SG2) Sean $\sigma, \tau \in A_n$. Entonces se tiene que,

$$sgn(\sigma\tau^{-1}) = sgn(\sigma)sgn(\tau^{-1}) = sgn(\tau) = 1,$$

lo que concluye la prueba. □

DEFINICIÓN 4.7. *Al subgrupo $A_n \leq S_n$ se le conoce como el grupo alternante en n letras.*

Como último resultado teórico de la sección lo que se quiere calcular el orden de A_n. Quitando los casos triviales que es $n = 0, 1$, supóngase que $n \geq 2$. Así, considere la transposición $(12) \in S_n$. Luego, defina la función:

$$\begin{gathered} f : A_n \to S_n \setminus A_n \\ \sigma \mapsto (12)\sigma \end{gathered}$$

Dado que la función signo es multiplicativa nótese que esta función está bien definida. Además es claramente inyectiva y suprayectiva pues $(12)^2 = (1)$. Así, esto dice que la cardinalidad de las permutaciones pares e impares es la misma. Entonces, dado que $S_n = A_n \sqcup (S_n \setminus A_n)$, entonces $2|A_n| = |S_n|$. Por lo tanto se ha demostrado que

PROPOSICIÓN 4.6. *Para cualquier $n \geq 2$, $|A_n| = \frac{n!}{2}$.*

Para terminar con esta sección se va a dar una interpretación a la función signo que dado que fue definida de forma abstracta, puede ser que no se tenga tan claro lo que "mide esta función". Para esto recordemos que toda $\sigma \in S_n$ tiene una factorización completa que es única. Luego, quitando los 1-ciclos que corresponden a los puntos fijos de dicha permutación, dicha permutación se puede expresar como un producto de ciclos. La forma genérica de un r-ciclo ($r \geq 2$) es $(i_1 ... i_r)$. El siguiente paso es observar que cualquiera de estos ciclos se escribe como un producto de transposiciones ya que quitando el caso obvio de $r = 2$ se deduce que:

$$(i_1 ... i_r) = (i_1 i_r) \cdots (i_1 i_3)(i_1 i_2)$$

Esto nos dice que toda permutación se puede ver como un producto de transposiciones. Dicho de forma más elaborada observe que este resultado dice que el subgrupo generado por todas las transposiciones es S_n. Esta observación es lo que permite darle una interpretación a los elementos de A_n y por lo tanto a la definición signo.

PROPOSICIÓN 4.7. *Sea $\sigma \in S_n$. Entonces $\sigma \in A_n$ (σ es par) si y sólo si σ se descompone como el producto de una cantidad par de transposiciones.*

DEMOSTRACIÓN. $\Rightarrow$) Por contrapositiva: Si $\sigma = \tau_1 \cdots \tau_{2n+1}$ para alguna $n \in \mathbb{N}$ y $\tau_1, ...\tau_{2n+1}$ transposiciones, entonces $sgn(\sigma) = sgn(\tau_1)\cdots sgn(\tau_{2n+1}) = (-1)^{2n+1} = -1$, luego $\sigma \notin A_n$.

$\Leftarrow$) Si $\sigma = \tau_1 \cdots \tau_{2n}$ para alguna $n \in \mathbb{N}$ y $\tau_1, ..., \tau_{2n}$ transposiciones, entonces $sgn(\sigma) = (-1)^{2n} = 1$, de lo que se tiene el resultado. □

5. Teorema de Lagrange

DEFINICIÓN 5.1. *Sean G un grupo y $H \leq G$. Definimos la relación en G dada por: $g \sim_H h$, si $gh^{-1} \in H$ para toda $g, h \in G$.*

PROPOSICIÓN 5.1. *Sean G un grupo y $H \leq G$. Entonces $\sim_H$ es una relación de equivalencia.*

DEMOSTRACIÓN.
- Sea $g \in G$. Entonces $gg^{-1} = e \in H$. Por lo tanto $g \sim_H g$.
- Sean $g, h \in G$ tales que $g \sim_H h$. Entonces $gh^{-1} \in H$. De aquí $hg^{-1} = (gh^{-1})^{-1} = \in H$. Por lo tanto $h \sim_H g$.
- Sean $g, h, k \in G$ tales que $g \sim_H h$ y $h \sim_H k$. Entonces $gh^{-1}, hk^{-1} \in H$. Se sigue que $gk^{-1} = gh^{-1}hk^{-1} \in H$. Por lo tanto $g \sim_H k$.

□

DEFINICIÓN 5.2. *Sean G un grupo, $g \in G$ y $H \leq G$. Ponemos $gH := \{gh \in G \mid h \in H\}$ y $Hg := \{hg \in G \mid h \in H\}$. A gH se le llama una clase izquierda de G y Hg se le llama una clase derecha.*

Notamos que en general ni gH ni Hg tienen estructura excepto cuando $g = e$ y $gH = Hg = e$.

También vemos que no necesariamente $gH = Hg$. Por ejemplo $G = S_3$, $H = \{1, (12)\}$ y $g = (13)$. Tenemos que $gH = \{(13), (123)\}$ y $Hg = \{(13), (132)\}$. Por lo que $gH \neq Hg$. Es importante observar que si el grupo es abeliano, siempre se tiene que $gH = Hg$.

EJEMPLO 5.1. *Sea $G = \mathbb{Z}$ y $H = n\mathbb{Z}$. Notamos que $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, puesto que la relación $a \cong b \mod n$ quiere decir que $n \mid b - a$. Pero esto es lo mismo que decir $b - a \in n\mathbb{Z}$. De nuevo esto es $b \sim_{n\mathbb{Z}} a$ en la nueva notación. Un caso punual de clases es cuando $n = 2$, por que tenemos que $\mathbb{Z}_2$ tiene dos clases, los pares $2\mathbb{Z}$ y los impares $2\mathbb{Z} + 1$.*

PROPOSICIÓN 5.2. *Sean G un grupo, $g \in G$ y $H \leq G$. Entonces $[g]_{\sim_H} = Hg$.*

DEMOSTRACIÓN. $\subseteq$) Sea $k \in [g]_{\sim_H}$. Entonces $k \sim_H g$. De aquí $kg^{-1} \in H$. Por lo que $k = (kg^{-1})g \in Hg$. Por lo tanto $k \in Hg$.

$\supseteq$) Sea $k \in Hg$. Entonces existe $h \in H$ tal que $k = hg$. Se tiene que $kg^{-1} = h \in H$. Por lo que $k \sim_H g$. Por lo tanto $k \in [g]_{\sim_H}$. □

De forma analoga se puede definir la relación $g_H \sim h$ si $g^{-1}h \in H$ para toda $g,h \in H$. Esta relación de nuevo sería de equivalencia. Y tendremos la proposición analoga.

PROPOSICIÓN 5.3. *Sean G un grupo, $g \in G$ y $H \leq G$. Entonces $[g]_{H\sim} = gH$.*

COROLARIO 5.1. *Sean G un grupo, $g,h \in G$ y $H \leq G$. Entonces $Hg = Hh$ si y sólo $gh^{-1} \in H$.*

COROLARIO 5.2. *Sean G un grupo, $g,h \in G$ y $H \leq G$. Entonces $gH = hH$ si y sólo $g^{-1}h \in H$.*

COROLARIO 5.3. *Sean G un grupo y $H \leq G$. Entonces dos clases izquierdas (derechas) son identicas o disjuntas.*

Notacionalmente vamos a denotar a $G/_H \sim$ por G/H. Esto puede sonar un poco arbitrario por que la notación G/H ya no hace referencia al lado de las clases. En general no habrá confusión como se verá en la siguiente sección. Independientemente para la siguiente proposición necesitaremos hacer la distinción.

PROPOSICIÓN 5.4. *Sean G un grupo y $H \leq G$. Entonces $|G/_H \sim| = |G/\sim_H|$.*

DEMOSTRACIÓN. Definimos $\phi\colon G/_H \sim \longrightarrow G/\sim_H$ como $\phi(gH) = Hg^{-1}$ para toda $gH \in G/_H \sim$. Antes que nada tenemos que ver que esta bien definida, puesto que esta definida en los representantes. Si $gH = hH$, entonces $g^{-1}h \in H$. De aquí $h^{-1}g = (g^{-1}h)^{-1} \in H$, por lo que $\phi(hH) = Hh^{-1} = Hg^{-1} = \phi(gH)$ y por lo tanto ϕ esta bien definida.

De forma analoga podemos definir $\psi\colon G/\sim_H \longrightarrow G/_H \sim$ como $\psi(Hg) = g^{-1}H$ para toda $Hg \in G/\sim_H$. Igualmente esta bien definida, ahora

$$\phi(\psi(Hg)) = \phi(g^{-1}H) = H(g^{-1})^{-1} = Hg$$

para toda $Hg \in G/\sim_H$, y

$$\psi(\phi(gH)) = \psi(Hg^{-1}) = (g^{-1})^{-1}H = gH$$

para toda $Hg \in G/_H \sim$. Por lo que ϕ y ψ son inversas. □

Notamos que lo primero que se nos ocurre es definir $\phi(gH) = Hg$ pero de esta forma no se puede demostrar que esta bien definida.

DEFINICIÓN 5.3. *Sean G un grupo y $H \leq G$. Definimos el índice de G en H, $[G:H]$, es el número de clases laterales $|G/H|$.*

Observamos que por la proposición anterior el índice no depende si se toman clases izquierdas o derechas.

El siguiente teorema es inspirado en el trabajo de Lagrange (1770), aunque lo más probable es que fuese demostrado por Galois.

PROPOSICIÓN 5.5 (Teorema de Lagrange). *Sea G un grupo finito y $H \leq G$. Entonces $|H| \mid |G|$. Más aún, $|G| = [G:H]|H|$.*

DEMOSTRACIÓN. Como G es finito, entonces G/H es finito. De hecho podemos elegir $k = [G:H]$ representantes $g_1, \ldots, g_k \in G$ tales que $G/H = \{g_1H, \ldots, g_kH\}$. Sabemos G/H es una partición, por lo que:

$$G = \bigsqcup_{i=1}^{k} g_iH$$

De aquí que:

$$|G| = |\bigsqcup_{i=1}^{k} g_iH| = \sum_{i=1}^{k} |g_iH|$$

Solo basta ver que $|g_iH| = |g_jH|$ para $i, j = 1, \ldots, k$. Así que sin perdida de generalidad podemos suponer que $g_1 = e$ y ver que $|H| = |gH|$. Definimos $\phi\colon H \longrightarrow gH$ dado por $\phi(h) = gh$ para toda $h \in H$. Veamos que es inyectiva, sean $h, h' \in H$ tales que $\phi(h) = \phi(h')$. Entonces $gh = gh'$. Por lo que $h = h'$ y ϕ es inyectiva. Por otro lado, para $gh \in gH$ con $h \in H$, tenemos que $\phi(h) = gh$ por lo que la función es suprayectiva y por lo tanto biyectiva. Así todas las clases tiene el mismo número de elementos. Regresenado a la ecuación antes mencionada:

$$|G| = \sum_{i=1}^{k} |g_iH| = \sum_{i=1}^{k} |H| = k|H| = [G:H]|H|$$

□

COROLARIO 5.4. *Sea G un grupo finito y $g \in G$. Entonces $o(g) \mid |G|$.*

COROLARIO 5.5. *Sea p un primo y G un grupo de orden p. Entonces G es cíclico.*

DEMOSTRACIÓN. Por el teorema de Lagrange, G tiene subgrupos de orden 1 o de orden p. En ambos casos es único. Y se aplica la proposición que dice que si tiene a lo más un subgrupo de orden d para cada divisor del orden n, entonces el grupo es cíclico. □

COROLARIO 5.6 (Pequeño Teorema de Fermat). *Si p es un primo y $a \in \mathbb{Z}$. Entonces* $a \cong a^p \mod p$

DEMOSTRACIÓN. Sea $G = \mathbb{Z}_p^*$. Notemos que $|G| = p-1$. Entonces $[a^{p-1}] = [a]^p = [1]$. Multiplicando por a, tenemos que $[a^p] = [a]$. Por lo tanto $a \cong a^p \mod p$. □

6. Subgrupos Normales y Grupo Cociente

Antes de dar la definición básica de la sección se va a probar un resultado previo que se obtiene al usar una generalización de las clases laterales. Sean $S, T \subseteq G$. Entonces se define el conjunto ST como $\{st \in G \mid s \in S, t \in T\}$. Es importante observar que incluso en el caso en que se consideren $H, K \leq G$, el conjunto HK no tiene porque tener estructura de grupo pues si se considera $G = S_3$, $H = \langle(12)\rangle$ y $K = \langle(13)\rangle$, entonces $HK = \{(1),(12),(13),(132)\}$, que no e subgrupo pues $(13)(12) = (123) \notin HK$ (ver ejercicio 58).

PROPOSICIÓN 6.1. *Sean $H, K \leq G$ finitos. Entonces $|HK||H \cap K| = |H||K|$.*

DEMOSTRACIÓN. Considérese la función $f\colon H \times K \longrightarrow HK$ dada por $f(h,k) = hk$. Se busca demostrar que para toda $x \in HK$, $|f^{-1}(x)| = |H \cap K|$. Esto por que el conjunto de las imágenes inversas forman una partición del dominio y así se tendría que como $H \times K = \bigcup_{x \in HK} f^{-1}(x)$, si se toman las cardinalidades de ambos lados, entonces se tiene $|H||K| = \sum_{x \in HK} |H \cap K| = |HK||H \cap K|$.

Para esto, dado $x \in HK$ observe que existen $h \in H$ y $k \in K$ tales que $hk = x$. Por lo que se demostrará que $f^{-1}(x) = \{(hc, c^{-1}k) \in H \times K \mid c \in H \cap K\}$.

Sea $(a,b) \in f^{-1}(x)$. Entonces $ab = x = hk$, por lo que $h^{-1}a = kb^{-1}$. Defina $c = kb^{-1}$ y observe que la última igualdad implica que $c \in H \cap K$. Además, $a = h(kb^{-1}) = hc$ y como $c^{-1} = (h^{-1}a)^{-1} = a^{-1}h$, entonces $b = (a^{-1}h)k = c^{-1}k$. Esto prueba la contención de izquierda a derecha.

Para la contención de derecha a izquierda sea $(hc, c^{-1}k)$ con $c \in H \cap K$. Entonces $f(hc, c^{-1}k) = hk = x$, lo que muestra la otra contención.

Para concluir note que la igualdad buscada se sigue de ver que la función $g : H \cap K \longrightarrow f^{-1}(x)$ dada por $g(c) = (hc, c^{-1}k)$ es claramente inyectiva por cancelación y suprayectiva por la descripción de $f^{-1}(x)$ dada anteriormente. □

Después de dicho resultado preliminar se presenta la definición básica de la sección.

DEFINICIÓN 6.1. *Sea $H \leq G$. Se dice que H es un subgrupo normal de G, lo que se denota por $H \trianglelefteq G$, si para todo $h \in H$ y $g \in G$, $ghg^{-1} \in H$.*

El teorema básico de caracterización se presenta a continuación.

PROPOSICIÓN 6.2. *Sea $H \leq G$. Son equivalentes:*

1. *$H \trianglelefteq G$.*
2. *Para todo $g \in G$, $gHg^{-1} \subseteq H$.*
3. *Para todo $g \in G$, $gHg^{-1} = H$.*
4. *Para todo $g \in G$, $gH = Hg$.*

DEMOSTRACIÓN. $1 \Rightarrow 2)$ Es claro de la definición. De hecho observe que las afirmaciones son equivalentes de forma directa.

$2 \Rightarrow 3)$ Sea $g \in G$. Por un lado la hipótesis implica que $gHg^{-1} \subseteq H$. Por otro lado, al aplicar la hipótesis a $g^{-1} \in G$ se tiene que $g^{-1}Hg \subseteq H$. Observe que esta contención implica que $H \subseteq gHg^{-1}$ pues para $h \in H$ se tiene que $g^{-1}hg \in H$ por lo que $h = g(g^{-1}hg)g^{-1} \in gHg^{-1}$. Por lo tanto se concluye que $gHg^{-1} = H$.

$3 \Rightarrow 4)$ Dado $x \in gH$, existe $h \in H$ tal que $x = gh$. Luego, $x = (ghg^{-1})g$ y como $ghg^{-1} \in H$ por hipótesis, entonces $x \in Hg$, lo que prueba que $gH \subseteq Hg$. Además, como la prueba de la otra contención es análoga esta se va a omitir.

$4 \Rightarrow 1)$ Sean $g \in G$ y $x \in H$. Dado que por hipótesis $gx \in Hg$, existe $y \in H$ tal que $gx = yg$, de donde se observa que $gxg^{-1} = y \in H$. Como los elementos tomados fueron arbitrarios esto concluye la prueba. □

Vale la pena mencionar el siguiente resultado que está asociado a los conjuntos que permiten dar distintas caracterizaciones del concepto de normalidad.

PROPOSICIÓN 6.3. *Sean $H \leq G$ y $g \in G$. Entonces $gHg^{-1} \leq G$.*

DEMOSTRACIÓN. Vamos a ver que se cumplen las dos propiedades de la definición.

SG1) Dado que $e \in H$, entonces $e = geg^{-1} \in gHg^{-1}$.

SG2) Sean $x, y \in gHg^{-1}$. Luego, existen $h,k \in H$ tales que $x = ghg^{-1}$ y $y = gkg^{-1}$. Entonces observe que $xy^{-1} = (ghg^{-1})(gk^{-1}g^{-1}) = ghk^{-1}g^{-1}$. Dado que $hk^{-1} \in H$, entonces $xy^{-1} \in gHg^{-1}$, lo que concluye la prueba. □

EJEMPLO 6.1. *Dado G grupo,* $\{e\} \trianglelefteq G$ *y* $G \trianglelefteq G$.

EJEMPLO 6.2. *Para todo* $n \in \mathbb{N}$, $A_n \trianglelefteq S_n$

EJEMPLO 6.3. *Para cualquier* $n \geq 1$, $SO(n) \trianglelefteq O(n)$, *donde* $O(n) = \{A \in M_n(\mathbb{R}) \mid AA^* = I_n\}$ *y* $SO(n) = \{A \in O(n) \mid \det(A) = 1\}$.

EJEMPLO 6.4. *Todo subgrupo de un grupo abeliano es normal. Sin embargo esto no caracteriza a los grupos abelianos pues los cuaternios es un ejemplo de un grupo donde todos sus subgrupos son normales pero este no es abeliano (Ejercicio 57).*

Para el siguiente ejemplo se requiere plantear una definición de carácter general.

DEFINICIÓN 6.2 (Conmutadores). *Para* $g,h \in G$, *se define el conmutador de estos elementos, el que se denota por* $[g,h]$, *como el elemento en G*

$$[g,h] = ghg^{-1}h^{-1}$$

El conjunto formado por todos los conmutadores no es necesariamente un grupo (ver ejercicio 68). Esto nos lleva a plantear el siguiente concepto:

DEFINICIÓN 6.3. *Dado un grupo G, al subgrupo generado por todos los conmutadores de G se le llama como el subgrupo conmutador o subgrupo derivado de G. Este se denotará por* G' *aunque otra notación usual es* $[G,G]$.

Notemos que si G es abeliano si y sólo si $G' = \{e\}$. Por otro lado, conectando con la teoría que hasta el momento se ha estudiado, se tiene lo siguiente.

EJEMPLO 6.5. *Dado un grupo G,* $G' \trianglelefteq G$.

Como en la sección anterior denote por G/H al conjunto de clases laterales izquierdas $\{gH \mid g \in G\}$. Este conjunto no tiene necesariamente estructura de grupo pues si se considera $H = \langle(12)\rangle \leq S_3$, entonces

$$(123)H(132)H = \{(1),(23),(12),(132)\}$$

Por lo tanto este conjunto no puede ser una clase lateral izquierda pues estas tienen cardinalidad 2. En particular la estructura de grupo que se nos puede ocurrir dar en general no funciona, esto es, el producto que se obtiene al hacer el producto de los representantes en cuestión, donde el problema radica en el hecho de que el producto depende se los representantes elegidos ya que los axiomas de grupo se cumplen de manera inmediata. La noción de subgrupo normal es importante pues con esta se puede dar la estructura de grupo mencionada a G/H.

PROPOSICIÓN 6.4. *Si $N \trianglelefteq G$, entonces el producto canónico da estructura de grupo a G/N. Además este grupo tiene cardinalidad $[G:N]$.*

DEMOSTRACIÓN. Observemos que el producto es una función para lo que supónga que $gN = g'N$ y $kN = k'N$. Lo que se quiere probar es que $(gN)(kN) = (g'N)(k'N)$, es decir, $gkN = g'k'N$. Más aún, observe que esto es equivalente a ver que $(gk)^{-1}g'k' \in N$. En efecto, $(gk)^{-1}g'k' = k^{-1}g^{-1}g'k' = (k^{-1}g^{-1}g'k)(k^{-1}k')$, donde dado que $N \trianglelefteq G$ se deduce que $k^{-1}g^{-1}g'k \in N$ pues $k^{-1}k' \in N$ por hipótesis, mientras que $k^{-1}k' \in N$ por hipótesis, luego, el resultado se sigue del hecho de que N es un subgrupo.

Verificar que se cumplen los axiomas de grupo es obvio por la definición del producto dada, donde el neutro es $eN = N$ y $(gN)^{-1} = g^{-1}N$. Además, por definición $|G/N| = [G:N]$. □

De aquí en adelante siempre que se hable del grupo cociente nos estaremos refiriendo a la estructura de la proposición anterior a no ser que se diga lo contrario.

EJEMPLO 6.6. *El ejemplo canónico de grupo cociente se obtiene al considerar $H \leq (\mathbb{Z},+)$. Por uno de los ejercicios existe $n \in \mathbb{N}$ tal que $H = n\mathbb{Z}$. En este caso $\mathbb{Z}/H = \mathbb{Z}/n\mathbb{Z}$ que es por definición $\mathbb{Z}_n$.*

EJEMPLO 6.7. *Para los subgrupos normales triviales de un grupo G, los grupos G/G y $G/\{e\}$ son como conjuntos $G/G = \{G\}$ y $G/\{e\} = \{g\{e\} \mid g \in G\}$.*

EJEMPLO 6.8. *Como se vio anteriormente para $n \geq 2$ se tiene que $A_n \trianglelefteq S_n$, por lo que S_n/A_n es un grupo. Además, de acuerdo a la proposición anterior y por el teorema de Lagrange se tiene que $|S_n/A_n| = 2$. Luego, se observa que para $(12) \in S_n$, se tiene que $(12)A_n \neq A_n$, por lo que $S_n/A_n = \{A_n,\ (12)A_n\} = \langle (12)A_n \rangle$.*

EJEMPLO 6.9. *De manera análoga al ejemplo anterior para $n \geq 2$ se tiene que $SO(n) \trianglelefteq O(n)$. Luego, dado $A \in O(n) \setminus SO(n)$ se tiene que $O(n)/SO(n) = \{SO(n),\ A \cdot SO(n)\}$. En particular observe que $[O(n) : SO(n)] = 2$.*

EJEMPLO 6.10. *Un ejemplo teórico muy importante se obtiene al considerar el grupo cociente G/G'. A este ejemplo se le conoce como la abelianización del grupo G. Esta se va a denotar por G_{ab}.*

Para concluir esta sección vamos a hacer algunos comentarios al respecto de cuándo G/N es abeliano, pues resulta que esto se puede caracterizar con una propiedad que tiene que ver con el subgrupo derivado. La idea en el fondo de esta proposición es el prototipo de una serie de teoremas que permiten establecer una correspondencia entre propiedades del grupo cociente y ciertos subgrupos que contienen al denominador del cociente, enunciado que es la base de lo que se conoce como el teorema de la correspondencia biyectiva y que será estudiado hasta el siguiente capítulo.

PROPOSICIÓN 6.5. *Sea $N \trianglelefteq G$. Entonces G/N es abeliano si y sólo si $G' \subseteq N$.*

DEMOSTRACIÓN. $\Rightarrow$) Basta ver que N contiene todos los conmutadores de elementos de G. Así, sean $g,h \in G$. Por ser G/N abeliano $(g^{-1}N)(h^{-1}N) = (h^{-1}N)(g^{-1}N)$, igualdad que es equivalente a $g^{-1}h^{-1}N = h^{-1}g^{-1}N$. Pero esto sucede si y sólo si $(h^{-1}g^{-1})^{-1}(g^{-1}h^{-1}) \in N$, es decir, $[g,h] \in N$.

$\Leftarrow$) Dados $g,h \in G$, se tiene que $[g^{-1},h^{-1}] \in N$, es decir, $g^{-1}h^{-1}gh \in N$. Esto es equivalente a decir que $ghN = hgN$, de lo que se deduce el resultado. $\square$

Observe que por ejemplo, como aplicación del resultado anterior y uno de los ejemplos previos, al ser S_n/A_n abeliano, se deduce que $(S_n)' \subseteq A_n$. Resulta ser que esta contención es de hecho una igualdad, sin embargo, en este momento la prueba de ello no está a nuestro alcance pues se requieren algunos resultados de estructura cíclica los cuales se verán posteriormente. Luego, observe que suponiendo este resultado S_n/A_n es la abelialización de S_n.

Esta última observación muestra que podemos realmente dar pocos ejemplos explícitos de subgrupos conmutadores y abelianizaciones pues nos falta desarrollar herramienta. Otros ejemplos se discutirán al avanzar en los temas, aunque a este nivel se puede realizar el ejercicio 70.

Para concluir esta sección vale la pena mencionar que existe el concepto de subgrupo normal generado por un conjunto. Las ideas en torno a este son esencialmente las mismas de la definición de subgrupo generado pues dicho subgrupo es por definición el $\subseteq$-mínimo subgrupo normal que contiene al conjunto en cuestión. La construcción de este se realiza al notar que la propiedad de normalidad es preservada bajo intersecciones de subgrupos normales. Además este tiene una caracterización en término de palabras (Para algunos detalles al respecto se recomienda el ejercicio 61). Por otro lado se puede construir el máximo subgrupo de G en el que un subgrupo H es normal, a este grupo se le conoce como el normalizador. SIn embargo, este no se tratará aquí pues resultará ser más útil en el capítulo 3 y por lo tanto su estudio se va a posponer.

7. Retícula de Subgrupos

DEFINICIÓN 7.1. *Sea G un grupo. Denotamos por por $\mathscr{S}(G)$ el conjunto de subgrupos de G. Notamos que $\mathscr{S}(G) \subseteq \mathscr{P}(G)$. Por lo que la contención le hereda la estructura de conjunto parcialmente ordenado.*

Como la intersección de subgrupos es un subgrupo, entonces los ínfimos de $\mathscr{P}(G)$ resultan ser los de $\mathscr{S}(G)$.

PROPOSICIÓN 7.1. *Sea G un grupo. Entonces $\mathscr{S}(G)$ es una retícula completa*

PROPOSICIÓN 7.2. *Sea G un grupo y $\{H_i\}_{i\in I} \subseteq \mathscr{S}(G)$. Entonces $\bigvee_{i\in I} H_i = \langle \bigcup_{i\in I} H_i \rangle$.*

PROPOSICIÓN 7.3. *Sean G un grupo, $H, K \leq G$ con K normal. Entonces $HK \leq G$.*

DEMOSTRACIÓN. Primero $e = ee \in HK$.

Sean $h_1k_1, h_2k_2 \in HK$ con $h_1, h_2 \in H$ y $k_1, k_2 \in K$. Entonces:

$$\begin{aligned}(h_1k_1)(h_2k_2)^{-1} &= h_1k_1k_2^{-1}h_2^{-1} \\ &= h_1(h_2^{-1}h_2)k_1k_2^{-1}h_2^{-1} \\ &= h_1h_2^{-1}k_3 \in HK\end{aligned}$$

Donde $h_3 := h_2k_1k_2^{-1}h_2^{-1} \in K$, por ser K normal. □

PROPOSICIÓN 7.4. *Sean G un grupo, $H, K \leq G$ con K normal. Entonces $H \vee K = HK$.*

DEMOSTRACIÓN. Notamos que $H \leq HK$ y $K \leq HK$.

Sea $L \leq G$ tal que $H, K \leq L$. Entonces para toda $h \in H$ y $k \in K$, tenemos que $h, k \in L$. De donde $hk \in L$, por lo que $HK \leq L$. Por lo tanto $H \vee K = HK$. □

PROPOSICIÓN 7.5. *Sea G un grupo, $H, K, L \leq G$ con $H \leq L$. Entonces $HK \cap L = H(K \cap L)$.*

DEMOSTRACIÓN. $\Rightarrow$) Sea $x \in HK \cap L$. Entonces $x \in L$ y existen $h \in H$ y $k \in K$ tales $x = hk$. Como $k = h^{-1}x$ y $h \in H \leq L$, se sigue que tenemos $k \in L$. Por lo que $k \in K \cap L$. Por lo tanto $x = hk \in H(K \cap L)$.

$\Leftarrow$) Sea $x \in H(K \cap L)$. Entonces $x = hk$ with $h \in H$ and $k \in K \cap L \leq K$. Por lo que $x \in HK$. Por otro lado $h \in H \leq L$ y $k \in L \cap K \leq L$, de lo cual tenemos que $x = hk \in L$- Por lo tanto $x \in HK \cap L$. □

Esta última igualdad es como subconjuntos, esto ultimos no tienen por que tener estructura de subgrupos.

DEFINICIÓN 7.2. *Sea G un grupo. Denotamos por $\mathscr{N}$ la clase de subgrupos normales de G.*

COROLARIO 7.1. *Sea G un grupo. Entonces $\mathscr{N}(G)$ es una retícula modular.*

COROLARIO 7.2. *Sea G un grupo abeliano. Entonces $\mathscr{S}(G)$ es una retícula modular.*

8. Ejercicios

En todos los ejercicios G denota un grupo arbitrario y e su elemento neutro.

EJERCICIO 1. *Se define la función $\hat{+} : [0,1) \times [0,1) \to [0,1)$ mediante la regla de correspondencia:*

$$x \hat{+} y = \begin{cases} x + y, & \text{Si } x + y < 1. \\ x + y - 1, & \text{Si } 1 \leq x + y \end{cases}$$

¿Qué axiomas de grupo satisface $([0,1), \hat{+})$?

EJERCICIO 2. *Sea S un conjunto y $*$ una operación en S que satisface las siguientes dos propiedades:*

1. *Para cualesquiera $a,b \in S$, $a*b = b*a$.*
2. *Para cualesquiera $a,b \in S$, $a*(a*b) = b$.*

Sea $o \in S$ un elemento fijo y se define una nueva operación en S mediante la regla $a+b = o*(a*b)$.

- *Demuestre que $+$ es conmutativa y que tiene un elemento neutro.*
- *Demuestre que para $a,b \in S$ la ecuación $x+a=b$ tiene una única solución en S.*
- *Demuestre que $+$ es asociativa si y sólo si para todo $a,b,c \in S$, $c*(o*(a*b)) = a*(o*(b*c))$.*
- *Concluya que $(S,+)$ es un grupo si y sólo si para todo $a,b,c \in S$, $c*(o*(a*b)) = a*(o*(b*c))$. De un ejemplo de un conjunto S con una operación $*$ que satisfaga 1 y 2, pero tal que $(S,+)$ no tenga estructura de grupo.*

EJERCICIO 3. *Sea G un conjunto no vacío con una función $* : G \times G \to G$ tal que:*

G1') Para cualesquiera $g,h,k \in G$, $g(hk) = (gh)k$

G2') Existe $e \in G$ tal que para cualquier $g \in G$, $ge = g$

G3') Para cualquier $g \in G$ existe $h \in G$ tal que $gh = e$,

donde $gh := *(g,h)$.

Demuestre lo siguiente:

1. *Si $g \in G$ es tal que $gg = g$, entonces $g = e$*
2. *Si $g,h \in G$ son tales que $gh = e$, entonces $hg = e$*
3. *Para cualquier $g \in G$, $eg = g$*

Concluir que un conjunto con una operación que cumple G1' a G3' es un grupo y viceversa.

EJERCICIO 4. *El **grupo de Hamilton** o **grupo de cuaternios** , $\mathbb{H}$, consta de un conjunto con 8 elementos $\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$ satisfaciendo las reglas que se muestran en la tabla de multiplicación (tabla 1)*

Demuestre que el grupo de Hamilton es en efecto un grupo y que este es no abeliano. Además, determine cada uno de los órdenes de los elementos que forman a dicho grupo.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

TABLA 2.

EJERCICIO 5. *Demuestre que el conjunto de unidades de un anillo es un grupo multiplicativo.*

EJERCICIO 6.

1. *Hallar un ejemplo de un grupo infinito en el cual existe exactamente un elemento de orden 2.*
2. *Dar un ejemplo de un grupo infinito en el cual todo elemento, salvo el neutro, tiene orden 2.*

EJERCICIO 7. *Sean $g,h,k \in G$. Demuestre que si $gh = gk$ o $hg = kg$, entonces $h = k$.*

EJERCICIO 8. *Demuestre que para $g \in G$, la función $L_g : G \to G$, llamada la traslación izquierda por g, dada por $L_g(x) = gx$, es una biyección. Además, pruebe que para cualesquiera $g,h \in G$, $L_g L_h = L_{gh}$.*

EJERCICIO 9. *Demuestre que para todo $g \in G$ y cualesquiera $n,m \in \mathbb{Z}$ se tiene que:*

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

EJERCICIO 10. *Demuestre las siguientes afirmaciones:*

1. *Si $g \in G$, entonces $(g^{-1})^{-1} = g$.*
2. *Si $g_1, ..., g_n \in G$ entonces $(g_1 \cdot ... \cdot g_n)^{-1} = g_n^{-1} \cdot ... \cdot g_1^{-1}$. Deduzca que para todo $n \in \mathbb{Z}$, $(g^{-1})^n = (g^n)^{-1} = g^{-n}$.*

EJERCICIO 11. *Sean $g, h \in G$ tales que $gh = hg$. Demuestre que para todo $n \in \mathbb{Z}$, $(gh)^n = g^n h^n$.*

EJERCICIO 12. *Sea G un grupo tal que para todo $g \in G$, $g^2 = e$. Demuestre que G es abeliano.*

EJERCICIO 13. *Sea G un grupo, $g \in G$ y $n, m \in \mathbb{Z}$ primos relativos. Demuestre que si $g^m = e$ entonces existe un $h \in G$ tal que $g = h^n$.*

EJERCICIO 14. *Decir si la siguiente afirmación es verdadera ó falsa, dando una demostración ó un contraejemplo según sea el caso: Si $g, h \in G$ son tales que existen $n, m \in \mathbb{N}^+$ con la propiedad de que $g^n = h^m = e$, entonces existe $k \in \mathbb{N}^+$ tal que $(gh)^k = e$.*

EJERCICIO 15. *Sean $g, h \in G$ tales que $gh = hg$, $g^n = e$ y $h^m = e$. Demuestre que $(gh)^{[n,m]} = e$.*

EJERCICIO 16.

1. *Supóngase que $G = \{e, a_1, ..., a_n\}$ un grupo de orden $n+1$ donde el único elemento tal que $x^2 = e$ es e. Calcule $a_1 \cdot ... \cdot a_n$.*
2. *Concluya del inciso anterior que si $p \in \mathbb{N}$ es primo entonces $(p-1)! \equiv -1 \mod p$.*

EJERCICIO 17. *Sea H un subconjunto de G. Demuestre que H es un subgrupo si y sólo si $H \neq \emptyset$ y para cualesquiera $g, h \in H$, $gh^{-1} \in H$.*

EJERCICIO 18. *Demuestre que H es un subgrupo de $(\mathbb{Z},+)$ si y sólo si $H = n\mathbb{Z}$ para un único $n \in \mathbb{N}$.*

EJERCICIO 19. *Sea $n \in \mathbb{N}^+$. Demuestre que el conjunto $\{e^{\frac{2\pi ik}{n}} \mid k \in \mathbb{N}\}$ es un grupo multiplicativo y calcule su orden.*

EJERCICIO 20. *Demuestre que $K \subseteq S_4$ definido por $K = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ es un grupo. A este grupo se le conoce como el grupo de Klein.*

EJERCICIO 21. *Sean H, K subgrupos de G.*

1. *Pruebe con un ejemplo que en general $H \cup K$ no es subgrupo de G.*
2. *Demuestre que $H \cup K \leq G$ si y sólo si $H \subseteq K$ o $K \subseteq H$.*

EJERCICIO 22. *Sea G un grupo y H un subgrupo propio de G. Demuestre que $\langle G \setminus H \rangle = G$.*

EJERCICIO 23. *Sean $S, T \subseteq G$. Demuestre que $\langle S \cap T \rangle \subseteq \langle S \rangle \cap \langle T \rangle$. Muestre con un ejemplo que la igualdad no se tiene necesariamente.*

EJERCICIO 24. *Pruebe que si H y K son subgrupos de G, entonces $HK = \{hk \mid h \in H,\ k \in K\}$ es un subgrupo de G si y sólo si $HK = KH$.*

EJERCICIO 25. *Definamos los conjuntos $U(n) = \{A \in M_n(\mathbb{C}) \mid AA^* = I_n\}$ y $SU(n) = \{A \in U(n) \mid \det(A) = 1\}$. Demuestre lo siguiente:*

1. *$SU(n) \leq U(n) \leq GL_n(\mathbb{C})$*
2. *$SU(n) \leq SL_n(\mathbb{C}) \leq GL_n(\mathbb{C})$*

*A los grupos $U(n)$ se les conoce como el **grupo unitario** y a $SU(n)$ como el **grupo especial unitario**. Sus versiones análogas con coeficientes reales se denotan por $O(n)$ y $SO(n)$ y se conocen como los grupos ortogonales y especial ortogonal respectivamente.*

EJERCICIO 26. *Sea G un grupo y sea $D_n = \langle \{r,s \mid o(r) = n,\ o(s) = 2,\ srs^{-1} = r\} \rangle \leq G$ con $n \in \mathbb{N}^+$.*

1. *Demuestre que existen $x, y \in G$ tales que $D_n = \langle \{x,y \mid o(x) = n,\ o(y) = 2,\ (xy)^2 = e\} \rangle$*
2. *Demuestre que $|D_n| = 2n$.*[3]
3. *Pruebe que el grupo de Klein se puede escribir como D_2 con $G = S_4$*
4. *Considere las matrices:*

$$r_k = \begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix}$$

$$s_k = \begin{pmatrix} \cos\frac{2\pi k}{n} & \sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & -\cos\frac{2\pi k}{n} \end{pmatrix}$$

Pruebe que usando estas matrices se puede construir un modelo para D_n donde $G = O(2)$

EJERCICIO 27. *Sea G un grupo y defina $Q_{2^{n+1}} = \langle \{x,y \mid o(x) = 2^n,\ x^{2^{n-1}} = y^2,\ xyx = y\} \rangle \leq G$.*

1. *Calcule el orden de $Q_{2^{n+1}}$*
2. *Construir un modelo de Q_8 con $G = SL_2(\mathbb{C})$.*

EJERCICIO 28. *Si G es un grupo finito de orden par, demostrar que el número de elementos de orden 2 es impar. ¿Qué sucede con esta afirmación si el grupo tiene orden impar?*

EJERCICIO 29. *Sea G un grupo de orden impar. Demostrar que para cada $x \in G$ existe $y \in G$ tal que $y^2 = x$. ¿Es dicho elemento es único?. ¿Qué sucede con la afirmación si el orden de G es par?*

[3] Usualmente hay dos notaciones para este tipo de grupos pues es además de la presentada en común escribir D_{2n} en lugar de D_n indicado que este grupo tiene $2n$ elementos.

EJERCICIO 30. *Sea G un grupo finito y H un subconjunto de G. Demuestre que H es un subgrupo de G si y sólo si $e \in H$ y para cualesquiera $g,h \in H$, $gh \in H$. ¿Qué sucede con esta afirmación si se quita la hipótesis de que G sea finito?*

EJERCICIO 31. *Demuestre que si G es un grupo finito y con un número par de elementos, entonces existe un elemento $g \in G$, con $g \neq e$, tal que $g^2 = e$.*

EJERCICIO 32. *Demuestre lo siguiente:*

1. *Si G tiene orden n y $g \in G$, entonces $g^n = e$.*
2. *Dado $g \in G$ el $o(g)$ es el mínimo natural positivo tal que $g^{o(g)} = e$.*

EJERCICIO 33. *Sea $g \in G$. Demuestre que para todo $h \in G$ el orden de g coincide con el orden de hgh^{-1}.*

EJERCICIO 34. *Demuestre que si $g \in G$ tiene orden n y $n = mk$ con $m,k \in \mathbb{N}^+$, entonces g^k tiene orden m.*

EJERCICIO 35. *Supóngase que G es un grupo cíclico generado por g con orden n. Demuestre que g^k genera G si y sólo si $(k,n) = 1$.*

EJERCICIO 36. *Sean $p,k \in \mathbb{N}$ primos relativos. Demuestre que $k^{\phi(p)} \equiv 1 \mod p$.*

EJERCICIO 37. *Si G es un grupo cíclico de orden n y $H,K \leq G$. Demuestre que $H \leq K$ si y sólo el orden de H divide al orden de K. ¿Qué sucede con esta afirmación si G no es cíclico?.*

EJERCICIO 38. *Demuestre que un grupo cíclico con exactamente un generador puede tener a lo más dos elementos.*

EJERCICIO 39. *Demuestre que si G es un grupo cíclico infinito, entonces todo subgrupo de G diferente al subgrupo neutro tiene orden infinito.*

EJERCICIO 40. *Demuestre que $\mathbb{Z} \times \mathbb{Z}$ no es cíclico.*

EJERCICIO 41. *Demuestre que $\mathbb{Z}_n \times \mathbb{Z}_m$ es cíclico de orden nm si y sólo si $(n,m) = 1$.*

DEFINICIÓN 8.1. *Un grupo $G \neq \{e\}$ es simple si sus únicos subgrupos normales son $\{e\}$ y G.*

EJERCICIO 42.

1. *Sea $n \in \mathbb{N}$ con descomposición en factores primos $n = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$, donde todos los factores son positivos. Demuestre que el número de subgrupos de $\mathbb{Z}_n$ es $\prod_{j=1}^{k}(n_j + 1)$.*
2. *Demuestre que $\mathbb{Z}_n$ es simple si y sólo si n es primo.*

EJERCICIO 43.

1. *Demuestre que si $\sigma, \tau \in S_n$ son ajenos, entonces $\sigma\tau = \tau\sigma$.*
2. *Demuestre que si $\sigma, \tau \in S_n$ son ajenos y $\sigma\tau = (1)$, entonces $\sigma = \tau = (1)$.*
3. *Demuestre que el orden de un r-cíclo es precisamente r.*
4. *Sea $\sigma \in S_n$ tal que $\sigma = \tau_1 \ldots \tau_k$, donde $\tau_1, \ldots, \tau_k \in S_n$ son cíclos ajenos. Demuestre que el orden de σ coincide con el mínimo común múltiplo de los ordenes de todos los τ_i.*

EJERCICIO 44. *Sean $n \in \mathbb{N}^+$ y $H \leq S_n$. Se define la relación $\sim \subseteq \{1, \ldots, n\}^2$ mediante:*

$$j \sim k, \text{ si existe } \sigma \in H \text{ tal que } \sigma(j) = k.$$

1. *Demuestre que $\sim$ es una relación de equivalencia en $\{1, \ldots, n\}$.*

2. *Describir el conjunto cociente cuando* $H = (1)$ *y cuando* $H = S_n$.

EJERCICIO 45. *Considérese* $\sigma = (12)(123)$ *y* $\tau = (143)$ *en* S_5. *¿Es cierto que* $S_5 = \langle \sigma, \tau \rangle$*?*.

EJERCICIO 46. *Considérese* $\sigma \in S_9$ *definido por*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$$

Calcule σ^{3015}.

EJERCICIO 47. *Demuestre que* S_n *es cíclico si y sólo si* $n \in \{0,1,2\}$.

EJERCICIO 48. *Demuestre lo siguiente:*

1. *Para* $n\mathbb{Z} \leq \mathbb{Z}$ *con* $n \in \mathbb{N}$, *las clases laterales de* $n\mathbb{Z}$ *están dadas por* $r + n\mathbb{Z}$ *para* $0 \leq r < n$.
2. *Para* $\mathbb{R} \leq \mathbb{C}$, *las clases de* $\mathbb{R}$ *están dadas por* $bi + \mathbb{R}$ *con* $b \in \mathbb{R}$.

EJERCICIO 49. *Sea* G *un grupo finito y* $K \leq H \leq G$. *Demuestre que* $[G : K] = [G : H][H : K]$.

EJERCICIO 50. *Sean* $H, K \leq G$ *y para* $a \in G$ *se define el conjunto* $HaK = \{hak \mid h \in H, k \in K\}$.

1. *Demuestre que el conjunto* $\{HaK \mid a \in G\}$ *es una partición de* G.
2. *Demuestre que si* G *es finito y* $G = \bigcup_{i=1}^{n} Ha_iK$, *entonces* $[G : K] = \sum_{i=1}^{n} [H : H \cap a_iKa_i^{-1}]$.
3. *Con la igualdad del inciso anterior pruebe al teorema de Lagrange.*

EJERCICIO 51. *Supóngase que existen $H_1, ..., H_n$ clases laterales derechas (izquierdas) de subgrupos de G tales que $G = H_1 \cup ... \cup H_n$. Demuestre que G se puede cubrir con una unión de clases laterales derechas (izquierdas) H_i de subgrupos de índice finito en G.*

EJERCICIO 52. *Demuestre que si H es un subgrupo de G con índice 2, entonces para todo $a \in G$, $a^2 \in H$.*

EJERCICIO 53. *Sea G un grupo y $H \leq G$ tal que $[G : H] = 2$. Demuestre que $H \trianglelefteq G$.*

EJERCICIO 54.

1. *Supóngase que G es un grupo finito y que $H, K \leq G$. Demuestre que si $|H|, |K| > \sqrt{|G|}$, entonces $|H \cap K| > 1$.*
2. *Sean $p, q \in \mathbb{N}$ primos distintos con $p > q$ y supóngase que $|G| = pq$. Demuestre que G tiene a lo más un subgrupo de orden p.*

EJERCICIO 55. *Sea G un grupo y $H, K \leq G$ con orden finito tales que $(|H|, |K|) = 1$. Demostrar que $H \cap K = \{e\}$.*

EJERCICIO 56. *Demuestre que para todo campo K y para todo $n \in \mathbb{N}^+$, $SL_n(K) \trianglelefteq GL_n(K)$.*

EJERCICIO 57. *Demuestre que todo subgrupo del grupo de cuaternios es normal.*

EJERCICIO 58. *Demuestre que si $H, K \trianglelefteq G$, entonces $HK \trianglelefteq G$.*

EJERCICIO 59. *Sea $H \leq G$ tal que si $Hg \neq Hk$ entonces $gH \neq kH$. Demuestre $H \trianglelefteq G$.*

EJERCICIO 60. *Sea G un grupo y $H \leq G$. Demuestre que $H \trianglelefteq G$ si y sólo si para cualesquiera $g, h \in G$, $gh \in H$ si y sólo si $hg \in H$.*

EJERCICIO 61.

1. *Demuestre que la intersección de cualquier familia no vacía de subgrupos normales es un subgrupo normal.*
2. *Demuestre que dado cualquier conjunto, el subgrupo normal generado por dicho conjunto existe y es único.*
3. *Si el subgrupo normal generado por $S \subseteq G$ se denota por $N^G(S)$, ¿Existe alguna relación entre $N^G(S)$ y $\langle S \rangle$?*
4. *Demuestre que para cualquier $S \subseteq G$, $N^G(S)$ es el conjunto de palabras en el conjunto $\{gsg^{-1} \mid g \in G,\ s \in S\}$.*

EJERCICIO 62. *Supóngase que G es un grupo finito y que $H \trianglelefteq G$ tal que $(|H|, [G : H]) = 1$. Demuestre que H el único subgrupo con esta propiedad.*

EJERCICIO 63. *Sea G un grupo finito para el que existe $n \in \mathbb{N}$ con $n > 1$ tal que para todo $g, h \in G$, $(gh)^n = g^n h^n$. Se definen $G[n] = \{g \in G \mid g^n = e\}$ y $G^n = \{g^n \mid g \in G\}$. Demuestre que $G[n], G^n \trianglelefteq G$ y que $|G^n| = [G : G[n]]$.*

EJERCICIO 64. *Supóngase que $H \trianglelefteq G$ con índice n y $x \in G$ tal que $x^m = e$ con $(n, m) = 1$. Demuestre que $x \in H$.*

EJERCICIO 65. *Sean $H \leq K \trianglelefteq G$ con K un grupo cíclico finito. Demuestre que $H \trianglelefteq G$.*

EJERCICIO 66. *Sea G un grupo y $\mathscr{P}$ una partición de G. Supóngase que $\mathscr{P}$ es un grupo bajo la operación $* : \mathscr{P} \times \mathscr{P} \to \mathscr{P}$ que satisface que para todo $a, b \in G$, $[a]_{\mathscr{P}} * [b]_{\mathscr{P}} = [xy]_{\mathscr{P}}$.*

1. *Demuestre que $[e]_{\mathscr{P}} \trianglelefteq G$.*
2. *Demuestre que como subgrupos $\mathscr{P} = G/[e]_{\mathscr{P}}$.*

EJERCICIO 67. *Sea G un grupo y $H \trianglelefteq G$ un grupo con índice n. Demuestre que para toda $g \in G$, $g^n \in H$. De un ejemplo donde se vea que esto puede ser falso si se quita la hipótesis de normalidad.*

EJERCICIO 68. *Dar un ejemplo de un grupo tal que el conjunto de conmutadores no es un subgrupo.*

EJERCICIO 69. *Discutir en cada una de las siguientes cadenas de subgrupos cuáles de los subgrupos en cuestión son normales, dando una demostración en caso afirmativo ó un contraejemplo en caso negativo*

- $SO(n) \leq O(n) \leq GL_n(\mathbb{R})$
- $SO(n) \leq SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$

Sugerencia: Ver el ejercicio 25 para las definiciones.

EJERCICIO 70. *Sea k un campo con $k \neq \mathbb{F}_2, \mathbb{F}_3$. Demuestre que:*

1. *Para $n \geq 2$, $(GL_n(k))' = SL_n(k)$*
2. *Para $n \geq 3$, $(SO(n))' = SO(n)$*

Capítulo 2

Morfismos

"La esencia de las matemáticas yace en su libertad"

Georg Cantor.

1. Morfismos

La idea de esta sección es definir el concepto de función entre grupos que preserva la estructura. Este proceso puede considerarse el análogo a lo que sucede en álgebra lineal, donde la idea de las transformaciones lineales es que estas funciones entre espacios preservan dicha estructura. Esto es útil desde el punto de vista ver como se comparan los espacios y de manera mucho más importante permite establecer un criterio de cuándo dos de ellos pueden considerarse con el mismo. En nuestro caso, el concepto que permitirá hacer esto es:

DEFINICIÓN 1.1. *Sean G y H grupos. Una función $f : G \to H$ es un morfismo de grupos si para cualesquiera $x, y \in G$,*

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

Es muy importante notar que en la definición anterior se están trabajando con dos operaciones distintas ya que para los elementos $x, y \in G$, el producto $xy \in G$, mientras que $f(x)f(y) \in H$. Sin embargo, para no cargar la notación y dado que en la práctica quedará clara la operación entre los grupos considerados, se conservará esta forma de escribir las operaciones ya que resulta engorroso enfatizar las operaciones, aunque en algunos ejemplos puede ser que se indiquen al escribir los grupos en cuestión como parejas ordenadas. Otro importante abuso de notación que se usará frecuentemente es que al decir "$f : G \to H$ es un morfismo" se tiene que sobreentender que G y H son grupos.

Antes de pasar a discutir ejemplos, se va a probar una proposición que nos dice que efectivamente el concepto de morfismo preserva la estructura de grupo. Esta observación tiene sentido pues la definición esta formulada únicamente usando las operaciones de los grupos en cuestión, sin embargo, en la definición de grupo intervienen otros elementos como lo son el neutro y los inversos. Precisamente el resultado dice que estos se preservan.

PROPOSICIÓN 1.1. *Sea $f : G \to H$ un morfismo de grupos. Entonces,*

1. $f(e) = e$

2. *Para cualquier* $g \in G$, $f(g^{-1}) = f(g)^{-1}$.

DEMOSTRACIÓN. Para la primera afirmación se observa que como $e^2 = e$, entonces $f(e)^2 = f(e)$, lo que implica la afirmación.

En lo que respecta a la segunda afirmación, sea $g \in G$. Dado que $gg^{-1} = e = g^{-1}g$, al aplicar f y usar que esta es morfismo se tiene que $f(g)f(g^{-1}) = e = f(g^{-1})f(g)$, donde es importante observar que para llegar a estas igualdades se ha usado la afirmación 1.

Así, por unicidad del inverso se deduce que $f(g)^{-1} = f(g^{-1})$. □

Es importante observar que como corolario del resultado anterior más un argumento por inducción entera se deduce que para $f : G \to H$ un morfismo y cualquier $g \in G$, se tiene que para todo $n \in \mathbb{Z}$,

$$f(g^n) = f(g)^n$$

Por otro lado, es claro también de la definición que la composición de morfismos es un morfismo.

A continuación se presentan algunos ejemplos.

EJEMPLO 1.1. *En el capítulo anterior se vio que la función signo es multiplicativa. Observe que esto se puede traducir diciendo que para* $n \geq 1$ *la función signo,*

$$sgn : (S_n, \circ) \to (\{-1, 1\}, \cdot),$$

es un morfismo de grupos.

EJEMPLO 1.2. *La función determinante da lugar a los tres siguientes morfismos de grupos donde k es un campo.*

$$\det : GL_n(k) \to k \setminus \{0\}$$

$$\det : O(n) \to \{-1, 1\}$$

$$\det : U(n) \to \mathbb{T}$$

EJEMPLO 1.3. *Observe que* $(\mathbb{R}^+,\cdot) \leq (\mathbb{R}\setminus\{0\},\cdot)$. *Son morfismos de grupos las funciones logaritmo (natural) y exponencial:*

$$\ln : (\mathbb{R}^+,\cdot) \to (\mathbb{R},+)$$

$$\exp : (\mathbb{R},+) \to (\mathbb{R}^+,\cdot)$$

EJEMPLO 1.4. *Las funciones valor absoluto real y norma compleja son morfismos*

$$|\_| : (\mathbb{R}\setminus\{0\},\cdot) \to (\mathbb{R}^+,\cdot)$$

$$\|\_\| : (\mathbb{C}\setminus\{0\},\cdot) \to (\mathbb{R}^+,\cdot)$$

EJEMPLO 1.5. *Considere la función* $f : \{-1,1\} \to \mathbb{Z}_2$ *definida mediante:* $f(-1) = 1$ *y* $f(1) = 0$. *Esta función es un morfismo de grupos.*

Todos los ejemplos mostrados hasta ahora son con grupos concretos. Se continua la lista con algunos ejemplos más abstractos.

EJEMPLO 1.6. *Para* G *un grupo y* $g \in G$, *defina* $f : \mathbb{Z} \to G$ *mediante la regla de correspondencia* $f(n) = g^n$. *De las leyes de los exponentes se deduce que* f *es un morfismo.*

EJEMPLO 1.7. *Sea* $H \leq G$.

1. *La función inclusión* $\imath : H \to G$ *es un morfismo. Observe que en particular la identidad* $1_G : G \to G$ *es un morfismo.*
2. *Si* $H \trianglelefteq G$, *entonces la función proyección canónica* $\pi : G \to G/H$ *es un morfismo.*

Como el lector podrá imaginarse, existen muchos ejemplos de morfismos, tantos que podríamos escribir un libro únicamente con estos. Dejaremos esta tarea para avanzar con la teoría. En esta dirección el siguiente paso es definir algunos conjuntos distinguidos asociados a un morfismo.

DEFINICIÓN 1.2. *Sea* $f : G \to H$ *un morfismo. Se definen:*

1. *El núcleo de f, el que se denotará por $nuc(f)$, como el conjunto $\{x \in G \mid f(x) = e\}$.*
2. *La imagen de f, la que se denotará por $im(f)$, como $f(G)$.*

Los conjuntos anteriores en realidad tienen estructura como lo muestra el siguiente resultado.

PROPOSICIÓN 1.2. *Sea $f : G \to H$ un morfismo. Entonces,*

1. $nuc(f) \trianglelefteq G$
2. $im(f) \leq H$

DEMOSTRACIÓN. Para la primera afirmación hay que demostrar dos cosas, la primera que $nuc(f) \leq G$ y la segunda la normalidad de dicho subgrupo.

Para la primera afirmación observe que obviamente $e \in nuc(f)$. Por otro lado, si $g,h \in nuc(f)$, entonces $f(gh^{-1}) = f(g)f(h)^{-1} = ee^{-1} = e$, es decir, $gh^{-1} \in nuc(f)$. Esto demuestra que $nuc(f) \leq G$. Respecto a la normalidad, sean $g \in G$ y $h \in nuc(f)$. Luego, $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)ef(g)^{-1} = e$. Así $ghg^{-1} \in nuc(f)$ y esto prueba que $nuc(f) \trianglelefteq G$.

Para la segunda afirmación, observe que obviamente $e \in im(f)$ pues $f(e) = e$. Por otro lado, dados $h_1, h_2 \in im(f)$, existen $g_1, g_2 \in G$ tales que $h_1 = f(g_1)$ y $h_2 = f(g_2)$. Así, $h_1h_2^{-1} = f(g_1)f(g_2)^{-1} = f(g_1g_2^{-1})$. Entonces $h_1h_2^{-1} \in im(f)$ y esto concluye la prueba. □

Hay varias observaciones que se pueden hacer respecto al resultado anterior. La primera de ellas tiene que ver con que la imagen no necesariamente es un subgrupo normal del codominio (Ejercicio 74). La segunda observación es que el hecho de que el núcleo de un morfismo sea un subgrupo normal nos da una forma de probar en muchos ejemplos particulares la normalidad de ciertos subgrupos. Por ejemplo, consideremos el morfismo

$$sgn : S_n \to \{-1, 1\}$$

Observe que por definición $nuc(sgn) = A_n$. Así, el resultado anterior proporciona una segunda demostración de que para cualquier $n \geq 1$, $A_n \trianglelefteq S_n$.

Otro ejemplo muy interesante es que los morfismos determinante del ejemplo 1.2 implican que:

$$SL_n(k) \trianglelefteq GL_n(k)$$

$$SO(n) \trianglelefteq O(n)$$

$$SU(n) \trianglelefteq U(n)$$

Un ejemplo interesante que es nuevo pues no se ha tratado antes se obtiene al considerar para $n \in \mathbb{N}^+$, $Aff(\mathbb{R}^n)$ el conjunto de transformaciones afines, es decir,

$$Aff(\mathbb{R}^n) = \{T : \mathbb{R}^n \to \mathbb{R}^n \mid \exists A \in GL_n(\mathbb{R}) \exists b \in \mathbb{R}^n (T(x) = Ax + b)\}$$

Es muy sencillo ver que $Aff(\mathbb{R}^n) \leq S_{\mathbb{R}^n}$ y que la representación de los elementos en $Aff(\mathbb{R}^n)$ es única. Además, observe que se puede definir un morfismo

$$f : Aff(\mathbb{R}^n) \to GL_n(\mathbb{R})$$
$$f(Ax+b) = A$$

Observemos que $(Ax+b) \in nuc(f)$ si y sólo si $A = I_n$, es decir, $nuc(f) = Tr(\mathbb{R}^n)$, el conjunto de traslaciones. Luego, la afirmación anterior prueba que:

$$Tr(\mathbb{R}^n) \trianglelefteq Aff(\mathbb{R}^n).$$

Después de la gran variedad de ejemplos que se pueden obtener por este método, resulta ser que se tiene una equivalencia de conceptos, es decir, el concepto de normalidad queda determinado por la idea de núcleo. Para esto se recomienda ver el ejercicio 84.

1.1. Monos, epis e isos. En álgebra lineal la introducción de la idea de núcleo permite dar la caracterización de ciertas transformaciones lineales. En nuestro caso se tiene un resultado análogo.

PROPOSICIÓN 1.3. *Sea $f : G \to H$ un morfismo. Las siguientes afirmaciones son equivalentes:*

1. *f es inyectiva.*
2. *$nuc(f) = \{e\}$*
3. *f es cancelable por la izquierda respecto a morfismos de grupos.*

DEMOSTRACIÓN. $1 \Rightarrow 2$) Dado que $\{e\} \subseteq nuc(f)$, lo que se va a probar es la contención restante. Sea $g \in nuc(f)$, entonces $f(g) = e$. Dado que $f(e) = e$, entonces $f(g) = f(e)$, y como f es inyectiva, $g = e$, lo que termina la demostración.

$2 \Rightarrow 3$) Sean $h_1, h_2 : K \longrightarrow G$ morfismos de grupos tales que $f \circ h_1 = f \circ h_2$. Lo que se quiere probar es que $h_1 = h_2$, para lo que es suficiente con ver que estas funciones tienen la misma regla de correspondencia por tener el mismo dominio y codominio. Para esto sea $k \in K$. Dado que $f \circ h_1 = f \circ h_2$, entonces $f(h_1(k)) = f(h_2(k))$, lo que implica que $f(h_1(k)h_2(k)^{-1}) = e$. Esto dice que $h_1(k)h_2(k)^{-1} \in nuc(f)$, por lo que de la hipótesis

se deduce que $h_1(k)h_2(k)^{-1} = e$, es decir, $h_1(k) = h_2(k)$. Como el elemento tomado fue arbitrario, esto concluye la prueba.

$3 \Rightarrow 1$) Lo que se va a probar es que si $g_1, g_2 \in G$ son tales que $f(g_1) = f(g_2)$, entonces $g_1 = g_2$. Así, observe que se pueden definir morfismos $h_1, h_2 : \mathbb{Z} \longrightarrow G$ dados por $h_1(n) = g_1^n$ y $h_2(n) = g_2^n$. Luego, la igualdad $f(g_1) = f(g_2)$ y un argumento de inducción entera implican que $f \circ h_1 = f \circ h_2$. Como f es cancelable por izquierda respecto a morfismos, esto implica que $h_1 = h_2$. Así, $g_1 = h_1(1) = h_2(1) = g_2$. □

En virtud de la proposición anterior a los morfismos inyectivos se les conoce como **monomorfismos**, o en breve **monos**, ya que la condición 3 es precisamente la definición de este tipo de morfismos desde la perspectiva de la teoría de categorías. La afirmación correspondiente para los morfismos suprayectivos se presenta en el ejercicio 78, donde en virtud a la afirmación 2 se les llama **epimorfismos** o **epis**. En esta dirección es importante mencionar que en el caso conjuntista la noción de inyectividad es también equivalente a la existencia de una inversa izquierda y, la de suprayectividad a la existencia de una inversa derecha, sin embargo, en el caso de la teoría de grupos esto no sucede ni para el caso de morfismos inyectivos (ejercicio 79) ni para los morfismos suprayectivos (ejercicio 80).

En este momento el siguiente paso es dar la definición de aquellos morfismos que nos permiten identificar dos grupos, es decir, considerarlos como el mismo. Desde el punto de vista intuitivo es razonable pensar que esto sucede con los morfismos biyectivos pues estos establecen una correspondencia biyectiva entre los elementos de los grupos en cuestión y al sumar el hecho de ser morfismo esto dice que la operación del dominio no solamente se preserva, sino que está representada exactamente en el codominio. Esta intuición resulta ser correcta y nuevamente la justificación de este nombre proviene de la teoría de categorías. Dicho resultado se presenta a continuación.

PROPOSICIÓN 1.4. *Sea $f : G \to H$ un morfismo de grupos. Son equivalentes:*

1. *f es biyectiva.*
2. *Existe un morfismo de grupos $g : H \to G$ tal que $f \circ g = 1_H$ y $g \circ f = 1_G$.*
3. *f tiene una inversa izquierda que es un morfismo de grupos y una inversa derecha que es un morfismo de grupos.*

DEMOSTRACIÓN. $1 \Rightarrow 2$) Supóngase que f es biyectiva. Luego, de la teoría de conjuntos se sabe que existe la inversa de f, $f^{-1} : H \longrightarrow G$, la cual satisface que $f \circ f^{-1} = 1_H$ y $f^{-1} \circ f = 1_G$. Así, lo que resta probar es que $f^{-1} : H \longrightarrow G$ es un morfismo. En efecto, sean $h_1, h_2 \in H$. Al ser f biyectiva, existen únicos $g_1, g_2 \in G$ tales que $f(g_1) = h_1$ y $f(g_2) = h_2$. Luego,

$$f^{-1}(h_1h_2) = f^{-1}(f(g_1)f(g_2)) = f^{-1}(f(g_1g_2)) = g_1g_2 = f^{-1}(h_1)f^{-1}(h_2)$$

Dado que los elementos tomados fueron arbitrarios, esto prueba que f^{-1} es un morfismo.

$2 \Rightarrow 3)$ Obvio.

$3 \Rightarrow 1)$ De las hipótesis se tiene que como todo morfismo es en particular una función, entonces dado que f tiene una inversa izquierda resulta que f es inyectiva y de la afirmación correspondiente a la derecha se deduce que f es suprayectiva. Así, f es biyectiva. □

Dado la importancia del concepto mencionado vale la pena puntualizarlo.[1]

DEFINICIÓN 1.3. *Un morfismo $f : G \to H$ que cumple una de, y por lo tanto todas las afirmaciones de la proposición pasada, se conoce como un* ***isomorfismo****. Dados grupos G y H, si existe un isomorfismo entre G y H, se dirá que dichos grupos son isomorfos y esto se va a denotar por $G \cong H$.*

Observe que es inmediato de la definición ver que si $f : G \to H$ es un isomorfismo, entonces $f^{-1} : H \to G$ lo es. Por otro lado, la composición de isomorfismos es un isomorfismo. Estas observaciones se pueden resumir como sigue:

PROPOSICIÓN 1.5. *La relación de "ser isomorfos" es de equivalencia en la clase de todos los grupos.*

Ahora vamos a discutir algunos ejemplos particulares.

EJEMPLO 1.8. *Observe que del ejemplo 1.3 se deduce que $(\mathbb{R}^+, \cdot) \cong (\mathbb{R}, +)$ ya que $\exp \circ \ln = 1_{(\mathbb{R}^+,\cdot)}$ y $\ln \circ \exp = 1_{(\mathbb{R},+)}$.*

EJEMPLO 1.9. *Del ejemplo 1.5 se deduce que $(\{-1, 1\}, \cdot) \cong (\mathbb{Z}_2, +)$.*

[1] En teoría de categorías a los morfismos que cumplen la propiedad 2 de la proposición anterior se les conoce como isomorfismos y a los que cumplen 3 se les llama bimorfismos. En nuestro caso no hay distinción entre estos y por lo tanto no se introducen estos términos.

EJEMPLO 1.10. *Nótese que hay un único grupo con un elemento, a este se le llama el grupo neutro y se denotará por* $\{e\}$. *En particular para cualquier grupo G,*

$$G/G \cong \{e\}$$

EJEMPLO 1.11. *Para cualquier grupo G,* $G/\{e\} \cong G$.

Observe que se puede definir para cualquier $n \geq 2$ la función $f : \{-1,1\} \to S_n/A_n$ cuya regla de correspondencia es

$$f(1) = A_n$$
$$f(-1) = (12)A_n$$

es un isomorfismo. Al combinar esto con el ejemplo 1.9 se deduce que para $n \geq 2$:

$$S_n/A_n \cong \{-1,1\} \cong \mathbb{Z}_2$$

Por un argumento similar se puede probar que

$$O(n)/SO(n) \cong \mathbb{Z}_2$$

Muchos de los ejemplos discutidos en la parte de morfismos inducen un isomorfismo, resultado que se conoce como el primer teorema de isomorfismo y se verá en la siguiente sección. Uno de los ejemplos que se deducen de dicho teorema tiene que ver con estos últimos grupos mencionados ya que en el primer capítulo se dijo que S_n/A_n y $O(n)/SO(n)$ son cíclicos de orden 2 y como se vio ambos grupos son isomorfos a $\mathbb{Z}_2$. Dicha justificación de por medio será vista en la siguiente sección.

1.2. Automorfismos. Existen dos tipos especiales de morfismos que básicamente se obtienen de tomar el dominio y codominio como el mismo grupo.

DEFINICIÓN 1.4.

1. *Un morfismo* $f : G \to G$ *se llama un endomorfismo del grupo G.*
2. *Un endomorfismo que además es un isomorfismo se conoce como automorfismo. El conjunto de automorfismos se denota por* $Aut(G)$.

Observe que para cualquier grupo G, $Aut(G) \subseteq S_G$. Más aún $Aut(G) \leq S_G$. Una pregunta obvia en si $Aut(G)$ tiene elementos no triviales (diferentes a la identidad) ya que está claro que $Aut(G) \subsetneq S_G$. La afirmación siguiente dice que siempre es posible construir elementos en $Aut(G)$ posiblemente no triviales.

PROPOSICIÓN 1.6. *Para G un grupo y $g \in G$, la función $\gamma_g : G \to G$ con regla de correspondencia $\gamma_g(x) = gxg^{-1}$, es un automorfismo.*

DEMOSTRACIÓN. Sean $x_1, x_2 \in G$. Entonces $\gamma_g(x_1x_2) = gx_1x_2g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = \gamma_g(x_1)\gamma_g(x_2)$. Esto prueba que γ_g es un endomorfismo.

Para ver que γ_g es biyectiva se puede probar esto directamente o notar que $(\gamma_g)^{-1} = \gamma_{g^{-1}}$ □

Los morfismos definidos juegan un papel muy importante en la teoría.

DEFINICIÓN 1.5. *Se dice que $f \in Aut(G)$ es interno si existe $g \in G$ tal que $f = \gamma_g$.*

Observe que 1_G es un automorfismo interno pues $1_G = \gamma_e$. Por otro lado, si $f \in Aut(G)$ es interno, el elemento $g \in G$ tal que $f = \gamma_g$ no es en general único. Esto se deduce de observar que si G es abeliano, entonces $\forall g \in G$, $\gamma_g = 1_G$, luego basta con tomar G abeliano con $| G | \geq 2$ para dar un ejemplo que demuestre la última afirmación.

Escribamos por $Int(G)$ al conjunto de automorfismos internos. Observe que $Int(G) \subseteq Aut(G)$. Más aún,

PROPOSICIÓN 1.7. *Para cualquier grupo G, $Int(G) \trianglelefteq Aut(G)$.*

DEMOSTRACIÓN. Para demostrar la afirmación primero veamos que $Int(G) \leq Aut(G)$. Para esto, como $1_G \in Int(G)$, sean $f_1, f_2 \in Int(G)$. Entonces existen $g_1, g_2 \in G$ tales que $f_1 = \gamma_{g_1}$ y $f_2 = \gamma_{g_2}$. Así, observe que $f_1 f_2^{-1} = \gamma_{g_1}\gamma_{g_2}^{-1} = \gamma_{g_1 g_2^{-1}}$, luego, $f_1 f_2^{-1} \in Int(G)$ y esto prueba la afirmación.

Para concluir sea $f \in Aut(G)$ y $\gamma_g \in Int(G)$. Dado $x \in G$ observe que,

$$(f\gamma_g f^{-1})(x) = f(gf^{-1}(x)g^{-1}) = f(g)ff^{-1}(x)f(g^{-1}) = f(g)xf(g)^{-1} = \gamma_{f(g)}(x).$$

Esto prueba que $f\gamma_g f^{-1} = \gamma_{f(g)}$ y por lo tanto $f\gamma_g f^{-1} \in Int(G)$, lo que demuestra la normalidad. □

Esta afirmación nos permite hacer dos cosas. La primera es ver que como en particular $Int(G)$ es un grupo, la función

$$\begin{array}{c}\gamma_{\square} : G \to Int(G) \\ g \to \gamma_g\end{array}$$

es un epimorfismo. Observe que $g \in nuc(\gamma_{\square})$ si y sólo si $\gamma_g = 1_G$, es decir, si para todo $x \in G$, $gxg^{-1} = x$, condición que es equivalente a decir que para todo $x \in G$, $gx = xg$. Esto dice que el elemento g conmuta con todos los elementos del grupo.

Dado que $nuc(\gamma_{\square}) = \{g \in G : \forall x \in G(gx = xg)\}$, se deduce que dicho conjunto es un subgrupo normal de G. Este grupo se conoce como el **centro** de G y se denota por $Z(G)$.

Más aún, como consecuencia del primer teorema de isomorfismo de la siguiente sección se verá que hay un isomorfismo

$$G/Z(G) \cong Int(G)$$

Por otro lado, una segunda pregunta obvia es qué sucede con el grupo $Aut(G)/Int(G)$. Para esta pregunta no se puede dar un resultado de carácter general pues dicho grupo depende del grupo en cuestión. Este grupo se conoce como el **grupo de automorfismos externos de** G. Algunos ejemplos de este se obtienen al observar que si G es abeliano, $Int(G) = \{1_G\}$. Luego, $Aut(G)/Int(G) \cong Aut(G)$. De forma concreta se sabe que $Aut(\mathbb{Z}) \cong \mathbb{Z}_2$ y $Aut(\mathbb{Z}n) \cong (U(\mathbb{Z}_n), \cdot)$ con $U(\mathbb{Z}_n)$ el grupo de unidades del anillo $\mathbb{Z}n$ (Ver ejercicios 130 y 131).

2. Teoremas de Isomorfismo

LEMA 2.1. *Sean $f : G \longrightarrow H$ un morfismo, $K \trianglelefteq G$ y $K \leq nuc(f)$. Entonces $f_K : G/K \longrightarrow H$ dada por $f_K(xK) = f(x)$ para toda $xK \in G/K$ esta bien definida y es un morfismo. Más aún, f_K es monomorfismo si y sólo si $K = nuc(f)$. También tenemos que; f es un epimorfismo si y sólo si f_K es un epimorfismo.*

DEMOSTRACIÓN. Sean $g, h \in G$ tales que $gK = hK$. Entonces $g^{-1}h \in K \leq nuc(f)$. Por lo que $f(g^{-1}h) = e$ y se sigue que $f(g) = f(h)$. Por lo tanto $f_K(gK) = f_K(hK)$ y f_K esta bien definida.

Sean $gK, hK \in G/K$. Entonces

$$f_K(gKhK) = f_K(ghK) = f(gh) = f(g)f(h) = f_K(gK)f_K(hK)$$

Por lo que f_K es un morfismo.

Si f_K es un monomorfismo, entonces $nuc(f_K) = \{K\}$. Sea $g \in nuc(f)$. Entonces $f_K(gK) = f(g) = e$. Por lo que $gK \in nuc(f_K)$ y $gK = K$. De donde $g \in K$. Por lo tanto $nuc(f) = K$.

Si $K = nuc(f)$ y $gK \in nuc(f_K)$. Entonces $f(g) = f_K(gK) = e$. Por lo que $g \in nuc(f) = K$. Así $gK = K$. Por lo tanto $nuc(f_K) = \{K\}$ y f_K es un monomorfismo.

$\Rightarrow$) Sea $y \in H$, entonces existen $x \in G$ tal que $f(x) = y$. Por lo que $f_K(xK) = f(x) = y$.

$\Leftarrow$) Sea $y \in H$ entonces existe $xK \in G/K$ tal que $f_K(xK) = y$. Por lo tanto $f(x) = f_K(xK) = y$. □

COROLARIO 2.1 (Primer Teorema de Isomorfismo). *Sea $f\colon G \longrightarrow H$ un morfismo. Entonces $G/nuc(f) \cong im(f)$.*

EJEMPLO 2.1. *Sea n un natural y $sgn\colon S_n \longrightarrow \{1,-1\}$. Notemos que $nuc(sgn) = A_n$ y esto es la definición de A_n. Por lo que por el primer teorema de isomorfismo $S_n/A_n \cong \mathbb{Z}_2$.*

EJEMPLO 2.2. *Sea G es un grupo cíclico.*

1. *Si G es finito, entonces $G \cong \mathbb{Z}_n$ para alguna $n \in \mathbb{N}^+$.*
2. *Si G es infinito, entonces $G \cong \mathbb{Z}$*

DEMOSTRACIÓN. Dado que G es cíclico, existe $g \in G$ tal que $G = \langle g \rangle$. Luego, considere el morfismo $f : \mathbb{Z} \to G$ definido mediante $f(n) = g^n$. Observe que este morfismo es un epimorfismo, por lo que del primer teorema del isomorfismo se deduce que

$$\mathbb{Z}/nuc(f) \cong G.$$

Observe que si G es finito, entonces sea $n = |G|$. Observe que $o(g) = n$. Así, dado que $g^n = e$, entonces $n \in nuc(f)$, de lo que se deduce que $n\mathbb{Z} \subseteq nuc(f)$. Por otro lado observe que si $m \in nuc(f)$, entonces $g^m =: f(m) = e$. Luego, como $o(g) = n$, se tiene que $n|m$, es decir, que $m \in n\mathbb{Z}$. Este argumento prueba que $nuc(f) = n\mathbb{Z}$, de lo que se deduce al usar el primer teorema de isomorfismo que $\mathbb{Z}_n \cong G$.

Por otro lado, al considerar G infinito, se tiene que $nuc(f) = 0$, pues en caso contrario existe $n \in nuc(f)$ con $n \neq 0$, lo que implica que $g^n = e$. Esto es una contradicción pues el orden de g es infinito. Por lo tanto, se deduce del primer teorema de isomorfismo que $\mathbb{Z} \cong G$. □

LEMA 2.2 (tarea). *Sea G un grupo, $K \leq G$ y $N \trianglelefteq G$. Si $N \leq K$ entonces $N \trianglelefteq K$.*

PROPOSICIÓN 2.1 (Segundo Teorema de Isomorfismo). *Sean G un grupo, $H \leq G$ y $N \trianglelefteq G$. Entonces $NH/N \cong H/(N \cap H)$.*

DEMOSTRACIÓN. Definimos una función $\phi\colon H \longrightarrow NH/N$ dada por $\phi(x) = xN$ para toda $x \in H$. Primero veamos que es un morfismo. Sean $x, y \in H$. Entonces:

$$\phi(xy) = xyN = xNyN = \phi(x)\phi(y)$$

Por otro lado, para $xhN \in NH/N$ con $x \in N$ y $h \in H$. Tenemos que

$$\phi(h) = hN = Nh = Nxh = xhN$$

Por lo que ϕ es suprayectiva.

Afirmación $nuc(\phi) = N \cap H$.

$\subseteq$) Sea $x \in nuc(\phi)$. Entonces $N = \phi(x) = xN$. Por lo que $x \in N$. Ya teníamos que $x \in H$ por ser parte del dominio. Por lo tanto $x \in N \cap H$.

$\supseteq$) Sea $x \in N \cap H$. Entonces $\phi(x) = xN = N$. Por lo tanto $x \in nuc(\phi)$.

Aplicando el primer teorema de isomorfismo, obtenemos el segundo teorema de isomorfismo. □

Notemos que anteriormente ya se había demostrado que para $H, K \leq G$ tenemos que $|HK||H \cap K| = |H||K|$. En el caso de que H y K sean finitos, tendríamos que $|HK|/|K| = |H|/|H \cap K|$. Este hecho se puede interpretar como una versión débil del segundo teorema, puesto que no se tiene un morfismo de grupos, si no una función biyectiva.

PROPOSICIÓN 2.2 (Tercer Teorema de Isomorfismo). *Sean G un grupo, $K, N \trianglelefteq G$ con $K \leq N$. Entonces $(G/K)/(N/K) \cong G/N$.*

DEMOSTRACIÓN. Notemos primero que $K \trianglelefteq N$ esto por que $K \trianglelefteq G$. La siguiente afirmación es que $N/K \trianglelefteq G/K$.

Sean $gK \in G/K$ y $xK \in N/K$. Entonces $gxg^{-1} \in N$. Por lo que $gKxK(gK)^{-1} = gxg^{-1}K \in N/K$. Por lo tanto $N/K \trianglelefteq G/K$.

Definimos $\phi\colon G/K \longrightarrow G/N$ dado por $\phi(xK) = xN$ para toda $xK \in G/N$. Notemos que si $\pi\colon G \longrightarrow G/N$ es la proyección canónica y como $K \subseteq N = nuc(\pi)$, entonces $\pi_K = \phi$. Con esto vemos que ϕ esta bien definida y es un morfismo de grupos. También como π es epimorfismo, tenemos que ϕ es un epimorfismo.

Afirmamos que $nuc(\phi) = N/K$.

$\subseteq$) Sea $xK \in N/K$ tal que $N = \phi(xK) = xN$. De aquí $x \in N$ por lo que $xK \in N/K$.

$\supseteq$) Sea $xK \in N/K$, entonces $\phi(xK) = xN = N$. Por lo que $xK \in nuc(\phi)$.

Por lo que usando el primer teorema de isomorfismo llegamos al resultado. □

DEFINICIÓN 2.1. *Sea G un grupo y $H \leq G$. Definimos $\mathscr{S}_H(G) := \{K \in \mathscr{S}(G) \mid H \leq K\}$.*

PROPOSICIÓN 2.3 (Teorema de la correspondencia biyectiva). *Sea G un grupo y $H \trianglelefteq G$. Entonces $\phi\colon \mathscr{S}_H(G) \longrightarrow \mathscr{S}(G/H)$ dada por $\phi(K) = K/H$ para $K \in \mathscr{S}_H(G)$ es un función monótona biyectiva.*

DEMOSTRACIÓN. Daremos la inversa de ϕ. Definimos $\psi\colon \mathscr{S}(G/H) \longrightarrow \mathscr{S}_H(G)$ dada por $\psi(L) = \cup L$ para $L \in \mathscr{S}(G/H)$. Afirmamos que $\cup L$ es un subgrupo de G.

Notamos que $e \in H \subseteq \cup L$. Sean $x, y \in \cup L$. Entonces existen $g, h \in G$ tales que $x \in gH$ y $y \in hH$. Por lo que usando la normalidad de H:

$$xy \in (gH)(h^{-1}H) = g(Hh^{-1})H = gh^{-1}HH = gh^{-1}H \subseteq \cup L$$

Por lo tanto $\cup L \leq G$.

Sea $K \in \mathscr{S}_H(G)$, entonces:

$$\psi(\phi(K)) = \psi(K/H) = \cup K/H = K$$

Por ser K/H una partición de K.

Sea $L \in \mathscr{S}(G/H)$, entonces:

$$\phi(\psi(L)) = \phi(\cup L) = (\cup L)/H$$

Afirmamos que $(\cup L)/H = L$.

$\subseteq$) Sea $xH \in (\cup L)/H$ con $x \in \cup L$. Entonces $x \in gH$ para algún $gH \in L$. Por lo que existe $h \in H$ con $x = gh$. De aquí $xH = ghH = gH$. Por lo tanto $xH \in L$.

$\supseteq$) Sea $gH \in L$. Entonces $g \in gH \subseteq \cup L$. Por lo tanto $gH \in (\cup L)/H$.

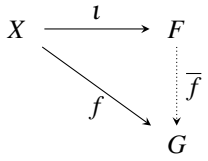
Por lo que $\phi(\psi(L)) = L$. □

EJEMPLO 2.3. *Sabemos que los subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$. Más aún, $n\mathbb{Z} \leq m\mathbb{Z}$ si y sólo si $m \mid n$. Como $\mathbb{Z}_n$ es $\mathbb{Z}/n\mathbb{Z}$ entonces sus subgrupos son de la forma $m\mathbb{Z}/n\mathbb{Z}$ con $m \mid n$, es decir, son de la forma $m\mathbb{Z}_n$ con $m \mid n$. Por ejemplo, los subgrupos de $\mathbb{Z}_6$ son $0, 3\mathbb{Z}_6, 2\mathbb{Z}_6$ y $\mathbb{Z}_6$.*

3. Grupos Libres

Los grupos libres son aquellos que tienen una base. La definición de estos está inspirada en la caracterización del concepto de base del álgebra lineal, la cual se conoce como la propiedad universal de las bases, que permite extender funciones de la base en transformaciones lineales.

DEFINICIÓN 3.1. *Sea F un grupo. Decimos que F es un grupo libre con base X si existe $X \subseteq F$ tal que para todo grupo G y toda función $f : X \to G$, existe un único morfismo $\overline{f} : F \to G$ tal que $\overline{f}\,|_X = f$, es decir, el siguiente diagrama conmuta:*



La propiedad de extensión de funciones a morfismos de grupos es un ejemplo de lo que se conoce como una propiedad universal pues esta caracteriza (salvo isomorfismo) al objeto que se está definiendo, en este caso el grupo libre con base X. Antes de demostrar esto, y con la notación de la definición, nótese que si se denota por G^X al conjunto de funciones de X en G y por $Hom(F,G)$ al conjunto de morfismos de grupos de F en G, dicha propiedad universal da lugar a una función

$$\begin{aligned} G^X &\to Hom(F,G) \\ f &\mapsto \overline{f} \end{aligned}$$

Luego, la propiedad universal dice que esta función es una biyección.

Tal y como sucede en álgebra lineal vale la pena enfantizar el hecho de que usando funciones en sentido de conjuntos uno puede obtener morfismos entre F y G, más aún, todos estos morfismos se pueden construir de esta forma. Observe que de hecho la inversa de la función mencionada anteriormente se da por precomposición por ι,

$$\iota^* : Hom(F,G) \to G^X$$

Vamos a ver que dicha propiedad universal caracteriza al grupo libre.

PROPOSICIÓN 3.1. *Si el grupo libre con base en un conjunto existe, este es único (salvo isomorfismo).*

DEMOSTRACIÓN. Supóngase que F y F' son grupos libres con base un conjunto X. De la propiedad universal de F aplicada a la función $\iota' : X \to F'$, existe un único morfismo $f : F \to F'$ tal que $f|_X = \iota'$. Por otro lado, al usar la propiedad correspondiente para F' respecto a ι, existe un único morfismo $g : F' \to F$ tal que $g|_X = \iota$. Lo que resta probar es que $f \circ g = 1_{F'}$ y $g \circ f = 1_F$, para lo cual se va a probar la primera igualdad pues la segunda se deduce de forma análoga. Para esto, como $f \circ g, 1_{F'} : F' \to F'$, basta ver, por la propiedad universal de F' aplicada a ι', que $(f \circ g)|_X = \iota'$, lo cual es claro pues

$(f \circ g)|_X = (f \circ g) \circ \iota' = f \circ \iota = f|_X = \iota'$. De esto se deduce la igualdad y se concluye la prueba. □

En virtud a la proposición anterior, si un grupo es libre con base X, este se puede denotar mediante $F := F(X)$. Discutamos un par de ejemplos.

EJEMPLO 3.1. *El grupo neutro $\{e\}$ es libre con base $\emptyset$.*

EJEMPLO 3.2. *Para $n \in \mathbb{N}^+$, el grupo $(n\mathbb{Z}, +)$ es un grupo libre. Observe que una base de este es $\{n\}$, sin embargo, $\{-n\}$ es otra base.*

EJEMPLO 3.3. *Ningún grupo finito no trivial puede ser libre ya que los elementos de una base tienen siempre orden infinito.*

DEMOSTRACIÓN. Sea F un grupo libre con base X. Defina la función $f : X \to \mathbb{Z}$ como la función constante con valor 1. Luego, al ser F libre, existe un único morfismo $\overline{f} : F \to \mathbb{Z}$ tal que $\overline{f}|_X = f$. Sea $x \in X$ y supóngase que $x^n = e$ para algún $n \in \mathbb{N}$. Entonces,

$$n = n\overline{f}(x) = \overline{f}(x^n) = \overline{f}(e) = 0$$

Esto prueba que la única potencia a la que x da el neutro es cero, entonces x debe tener orden infinito. □

El tercer ejemplo muestra que no todo grupo es libre. En lo que respecta al segundo ejemplo, su importancia es que nos permite ver que como es de esperarse la existencia de una base para un grupo libre no es única. Sin embargo, hay un invariante asociado a dichas bases que es la cardinalidad de la base. La demostración general de este hecho requiere conocer algunos resultados de aritmética cardinal, y dado que el curso de teoría de conjuntos no es obligatorio no podemos suponer que el lector los conozca. El mejor resultado que se puede dar sin suponer esto es el siguiente:

PROPOSICIÓN 3.2. *Si X y Y son bases de un grupo F y una de ellas es finita, entonces la otra también lo es y además $|X| = |Y|$.*

DEMOSTRACIÓN. Sin pérdida de generalidad podemos suponer que $|X| < \aleph_0$. Observe que de la propiedad universal se deduce que se tienen las siguientes biyecciones

$$\mathbb{Z}_2^X \cong Hom(F, \mathbb{Z}_2) \cong \mathbb{Z}_2^Y$$

Al tomar cardinales dicha biyección implica que

$$2^{|X|} = 2^{|Y|}$$

Esto prueba que $|Y| < \aleph_0$ pues X es finito. Más aún, esta igualdad de números naturales implica que $|X| = |Y|$. □

Para el lector interesado es importante decir que la prueba en el caso infinito usa el hecho de que si F es un grupo generado por X y X es infinito, entonces $|F| = |X|$, de donde es obvio el resultado.

Como corolario de esta proposición se deduce que:

COROLARIO 3.1. *Sean X y Y conjuntos. Entonces, $F(X) \cong F(Y)$ si y sólo si $|X| = |Y|$.*

El resultado anterior dice que el cardinal de la base de un grupo es un invariante. Luego, permite definir una asociación que a cada grupo libre F le asocia un cardinal denotado por $rank(F)$, que se conoce como el **rango** de F, y está definido como el cardinal de cualquier base.

EJEMPLO 3.4.

1. $rank(\{e\}) = 0$
2. $rank(\mathbb{Z}) = 1$

Por el momento esta quedará como una pequeña curiosidad, sin embargo, en el tema de grupos abelianos proyectivos esta se va a ver desde otra perspectiva.

Una vez que se ha visto el problema de la unicidad de grupos libres, podemos pasar al problema de la existencia, es decir, ver que para cualquier conjunto X existe un grupo libre con base dicho conjunto.[2] Para esto se requiere realizar una construcción, que como en el caso $X = \emptyset$ el grupo libre con base en dicho conjunto es el grupo trivial, vamos a realizar suponiendo que $X \neq \emptyset$.

[2]Observe que esto dice que la función rango toma todos los cardinales. En particular la clase de todos los grupos es propia.

Sea X un conjunto y considere X^{-1} un conjunto que tiene un elemento por cada elemento de X, donde se denota por x^{-1} al elemento asociado a $x \in X$. Observe que esto dice que X y X^{-1} son biyectables. Además considere un conjunto con un único elemento $\{e\}$ y considere la unión ajena $X \sqcup \{e\} \sqcup X^{-1}$. Si $x \in X$, denote por

$$x^1 := x$$
$$x^0 := e$$

.

DEFINICIÓN 3.2. *Una palabra en X es una sucesión $w \in (X \sqcup \{e\} \sqcup X^{-1})^{\mathbb{N}}$ con soporte finito, es decir, existe $n \in \mathbb{N}$ tal que $w_i = e$ para todo $i > n$. En particular, la sucesión constante con valor e se conoce como la palabra vacía y se denota por e.*

Existe una notación que permite empatar la definición de palabra dada con la del caso de grupos ya que toda palabra tiene una única representación

$$w = x_1^{k_1} x_2^{k_2} \cdot \ldots \cdot x_n^{k_n},$$

con $x_i \in X$, $k_i \in \{-1,0,1\}$ y $k_n \in \{-1,1\}$.

Dado que las palabras son sucesiones, hay una noción clara de igualdad entre ellas. Además hay una noción de longitud de palabras la cual es por definición 0 para la palabra vacía y en caso de que $w = x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$, la longitud de w es n.

Inspirados nuevamente en lo que sucede para el caso de grupos, dada una palabra $w = x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$, el inverso de esta palabra se define como $w^{-1} = x_n^{-k_n} \cdot \ldots \cdot x_1^{-k_1}$.

Observe que hasta este momento todas las definiciones anteriores están inspiradas en sus análogos de la teoría de grupos. La siguiente serie de definiciones son especiales para el concepto de palabra introducido en esta sección.

DEFINICIÓN 3.3.

1. *Una palabra w en X es reducida si w es la palabra vacía ó $w = x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ donde $k_i \in \{-1,1\}$ y no existe $i \in \{1,\ldots,n-1\}$ tal que $(x_i^{k_i})^{-1} = x_{i+1}^{k_{i+1}}$.*
2. *Una subpalabra de una palabra w es una subsucesión de esta formada por términos adyacentes dos a dos ó la palabra vacía.*

Algunas observaciones que se deducen inmediatamente de las definiciones anteriores se encuentran en el siguiente resultado.

PROPOSICIÓN 3.3.

1. *En la notación introducida, si $w = x_1^{k_1} \ldots x_n^{k_n}$ es una palabra, entonces las subpalabras de w son la palabra vacía ó tienen la forma $x_i^{k_i} \ldots x_j^{k_j}$ donde $1 \leq i \leq j \leq n$.*

2. *Si v es una subpalabra de w, existen subpalabras w' y w'' tales que $w = w'vw''$.*
3. *Una palabra no vacía w es reducida si y sólo si no contiene subpalabras de la forma x^0 ó $x^{-k}x^k$.*

El siguiente paso en la construcción de grupo libre es la definición de un producto.

Dadas palabras $w = x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ y $u = y_1^{l_1} \cdot \ldots \cdot y_m^{l_m}$ estas se pueden concatenar para definir una palabra

$$w * u = x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} y_1^{l_1} \cdot \ldots \cdot y_m^{l_m}.$$

Sin embargo, esta operación no define un producto en el conjunto de palabras reducidas en X pues $w * u$ puede no ser reducida.

EJEMPLO 3.5. *Supóngase que $X = \{a,b\}$. Considere las palabras en X, $w := aba$ y $u := a^{-1}b^{-1}$. Observe que ambas palabras son reducidas y su concatenación está dada por*

$$w * u = abaa^{-1}b^{-1}.$$

Esta no es reducida pues contiene la subpalabra aa^{-1}.

Intuitivamente, en la concatenación $w * u$ a uno le gustaría reducir aa^{-1} pues en un grupo $aa^{-1} = e$ y así $abaa^{-1}b^{-1} = abeb^{-1} = abb^{-1} = ae = a$.

Para definir el producto que nos interesa hay que axiomatizar estás reducciones, lo que nos llevará a definir el **producto de yuxtaposición**. Esto se hace como sigue: Dadas palabras reducidas w y u, existe una subpalabra de ambas (posiblemente vacía) tal que $w = w'v$ y $u = v^{-1}u'$. En el ejemplo anterior note que $w = a(ba)$ y $u = (ba)^{-1}$. El hacer esto no asegura que $w' * u'$ sea reducida pues en el ejemplo anterior $w = (ab)a$ y $u = (a^{-1})b^{-1}$, pero abb^{-1} no es reducida. Así, se quiere que además de que $w = w'v$ y $u = v^{-1}u^{-1}$, $w' * u'$ sea reducida. Así, se define el producto de yuxtaposición o de w con u por

$$wu = w' * u'$$

EJEMPLO 3.6. *Para $X = \{a,b\}$ y la palabra $w = a(ba)$ y $u = a^{-1}b^{-1} = (ba)^{-1}$,*

$$wu = a.$$

Por definición el producto de yuxtaposición es una operación binaria en el conjunto de palabras reducidas. Con esto se puede ahora probar la existencia de grupos libres. Además es de esperarse por la discusión anterior que el candidato al grupo libre con base un conjunto X es el conjunto de palabras reducidas en dicho conjunto. Sin embargo, al pensar en la prueba de esta afirmación la asociatividad del producto de yuxtaposición es un proceso muy engorroso ya que habría que analizar muchos casos. Entonces la prueba de este hecho se va a hacer usando un "truco" que está basado en un teorema que estudiaremos después (Teorema de Cayley).

PROPOSICIÓN 3.4. *Dado un conjunto X, existe el grupo libre con base X.*

DEMOSTRACIÓN. (Truco de van der Waerden) Como antes supongamos que $X \neq \emptyset$ pues dicho caso es obvio. Sea F el conjunto de palabras reducidas en el conjunto X. Para cada $x \in X$ defina funciones $|x^k| : F \to F$, donde $k \in \{-1, 1\}$, cuya regla de correspondencia es:

$$|x^k|(x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}) = \begin{cases} x^k x_1^{k_1} \ldots x_n^{k_n}, & \text{Si } (x^k)^{-1} \neq x_1^{k_1} \\ x_2^{k_2} \ldots x_n^{k_n}, & \text{e.o.c.} \end{cases}$$

Observemos que $|x^k| \circ |x^{-k}| = |x^{-k}| \circ |x^k| = 1_F$, lo que dice que estas funciones son biyectivas y que $|x^k|^{-1} = |x^{-k}|$, en particular $\{|x| \ : \ x \in X\} \subseteq S_F$. Luego, considere G el subgrupo generado por $\{|x| : x \in X\} \subseteq S_F$. De la observación anterior y la descripción del subgrupo generado por un conjunto en término de palabras, un elemento $g \in G$ se puede escribir como:

$$g = |x_1^{k_1}| \circ \ldots \circ |x_n^{k_n}|,$$

con $k_i \in \{-1, 1\}$ y, en dicha descomposición no existe $i \in \{1, \ldots, n-1\}$ tal que $|x_i^{k_i}|^{-1} = |x_{i+1}^{k_{i+1}}|$. Note que esta es claramente única pues S_F es un grupo. Lo que se afirma es que G es grupo libre con base $\{|x| : x \in X\}$. Para esto lo primero que hay que observar es que se tiene una función de inclusión obvia $\iota : \{|x| \ : \ x \in X\} \to G$. Para ver que G cumple la propiedad universal del grupo libre sea $f : \{|x| : x \in X\} \to H$ una función con H un grupo. Por la expresión única de los elementos en G se define $\overline{f} : G \to H$ mediante

$$\overline{f}(|x_1^{k_1}| \circ \ldots \circ |x_n^{k_n}|) = f(|x_1|)^{k_1} \cdot \ldots \cdot f(|x_n|)^{k_n}.$$

Para ver que $\overline{f}$ es un morfismo sean w y u palabras reducidas en $\{|x| : x \in X\}$. Así, si $w = w' \circ v$ y $u = v^{-1} \circ u'$ con $w' \circ u'$ reducida, entonces dado que w' y v son reducidas se deduce que $\overline{f}(w) = \overline{f}(w')\overline{f}(v)$ y, por el mismo argumento $\overline{f}(u) = \overline{f}(v)^{-1}\overline{f}(u')$. Así, observe que por definición $wu = w' \circ u'$ y entonces $\overline{f}(wu) = \overline{f}(w')\overline{f}(u')$. Por otro lado $\overline{f}(w)\overline{f}(u) = \overline{f}(w')\overline{f}(v)\overline{f}(v)^{-1}\overline{f}(u') = \overline{f}(w')\overline{f}(u')$, lo que prueba la igualdad. Además es claro que $\overline{f}|_{\{|x| : x \in X\}} = f$ y la unicidad de $\overline{f}$ es clara, lo que concluye la afirmación.

Para concluir la prueba, observe que hay una biyección

$$g : G \to F$$
$$(|x_1|^{k_1} \circ \ldots \circ |x_n|^{k_n}) \mapsto x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$$

Luego, dado que G es un grupo libre, entonces F tiene una única estructura de grupo que hace de la función anterior una biyección (ejercicio 90), de donde por la discusión previa es claro que dicho producto en F es el producto de yuxtaposición y además que F es un grupo libre con base $g(\{|x| : x \in X\}) \subseteq F$. Más aún, observe que g induce una biyección entre $\{|x| : x \in X\}$ y X, por lo que la base de F es X. □

Observe que pos construcción el grupo libre con base X es en particular generado por X. Por otro lado, hay un resultado teórico muy interesante que se explotará en la siguiente sección y que tiene gran importancia.

PROPOSICIÓN 3.5. *Todo grupo es cociente de un grupo libre.*

DEMOSTRACIÓN. Sea G un grupo y considere X un conjunto con un elemento por cada $g \in G$, el cual se va a denotar por x_g. Considere la función $f : X \to G$ definida mediante $f(x_g) = g$. Por la propiedad universal del grupo libre existe un único morfismo de grupos

$$\overline{f} : F(X) \to G$$

tal que $\overline{f}|_X = f$.

Observe que $\overline{f}$ es un epimorfismo por construcción, así, por el primer teorema de isomorfismo se deduce que

$$F(X)/nuc(\overline{f}) \cong G,$$

de lo que se deduce el resultado. □

EJEMPLO 3.7. *Se recuerda que para $n \geq 2$ se define $D_n = \langle \{r,s \mid o(r) = n,\ o(s) = 2,\ srs = r^{-1}\} \rangle$, para el cual se construyó un modelo en el ejercicio 26 para $G = O(2)$. Observe que dicho grupo se puede escribir de la forma $D_n = \langle \{r,s \mid o(r) = n,\ o(s) = 2,\ (sr)^2 = e\} \rangle$. Considere F el grupo libre con base $X = \{x,y\}$ y el morfismo $f : F(X) \to D_n$ definido mediante $f(x) = r$ y $f(y) = s$. Sean $R = \{x^n, y^2, (yx)^2\} \subseteq F(X)$ y N el subgrupo*

normal generado por dicho conjunto R. Observe que $N \subseteq nuc(f)$. Así, al considerar la proyección canónica

$$\pi : F(X)/N \to (F(X)/N)/(nuc(f)/N),$$

esta es un epimorfismo. Por el tercer teorema de isomorfismo el codominio es isomorfo a $F(X)/nuc(f)$. Además, por el primer teorema de isomorfismo se tiene esto induce un epimorfismo

$$\tilde{\pi} : F(X)/N \to D_n$$

Observe que $|D_n| = 2n$ y además, del ejercicio 26 se deduce que $|F(X)/N| = 2n$, por lo que $\tilde{\pi}$ es un isomorfismo.

En virtud del ejemplo anterior note que la importancia de este resultado es que da una construcción formal a grupos como D_n, $Q_{2^{n+1}}$ y de hecho esto vale para cualquier grupo. Esto se va a discutir con mayor detalle en la siguiente sección.

En lo que respecta al problema dual una pregunta obvia es: ¿Qué sucede con los subgrupos de grupo libre?. La respuesta es un teorema muy famoso:

PROPOSICIÓN 3.6. *(Nielsen - Schreir) Todo subgrupo de un grupo libre es libre.*

La demostración de este teorema está fuera de nuestro alcance pues usa hechos no triviales de carácter conjuntista, a saber, que el subgrupo es bien ordenado y además se usa un argumento de inducción transfinita para construir el conjunto que es base de dicho subgrupo. El lector interesado puede consultar por ejemplo el libro "Axiom of Choice" de Horst Herrlich. Por otro lado hay pruebas de carácter topológico las cuales también salen de nuestro alcance pues usan la idea de aplicación cubriente. Para esta se puede consultar el libro de Rotmann "Algebraic topology".

Para concluir esta sección vamos a comentar unas interpretación topológico/geométrica en torno a los grupos libres. Este tiene que ver con lo que se conocen como superficies (combinatorias) y la reducción de palabras tiene por lo tanto un significado geométrico que permiten dar un teorema de clasificación de superficies. Este trabajo se debe a J.Conway y es el caso particular del problema de la palabra en álgebra.

Considérese el disco de la figura 1 donde los ejes que forman la frontera tienen una orientación. Luego, a^{-1} se interpreta como la trayectoría a recorrida en signo contrario. Con esto, una palabra indica una forma de pegar las trayectorias. Así, la palabra aa^{-1} corresponde a una esfera 2-dimensional. El caso de la palabra aa es un plano proyectivo pues para obtener la superficie que dicha palabra representa hay que quitar el interior de dicho disco.

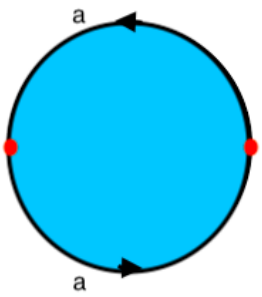
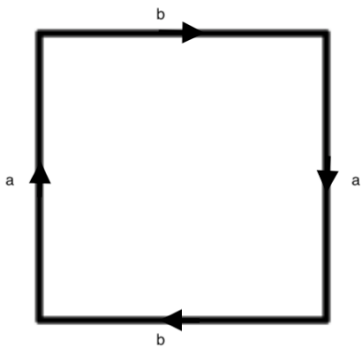


FIGURA 1.

Otro ejemplo se obtiene de considerar la figura 2 donde la palabra $aba^{-1}b^{-1}$ representa un toro y *aabb* una botella de Klein. Observe que la primera palabra en el grupo libre representa al conmutador $[a,b]$.



2.png

FIGURA 2.

Con esto en mente observe que el hecho de que un producto de n-conmutadores representa un n-toro y el hecho de un producto de conmutadores no sea un conmutador dice que un n-toro no es equivalente a un toro. Usando estas ideas uno puede convencerse de la correspondencia geométrica de las palabras en cuestión mostrada en la tabla 1.

Palabra en $X = \{a_i, b_i\}_{i\in\mathbb{N}^+}$	Superficie
$a_1a_1^{-1}$	S^2
a_1a_1	$\mathbb{RP}^1$
$a_1b_1a_1^{-1}b_1^{-1}$	$T = S^1 \times S^1$ (Toro)
$a_1a_1b_1b_1$	Botella de Klein
$[a_1,b_1][a_2,b_2]$	T^2 (2-toro)
$a_1a_1a_2a_2a_3a_3$	3-crosscaps

TABLA 1. Correspondencia entre palabras y algunas superficies (combinatorias)

4. Generadores y Relaciones

DEFINICIÓN 4.1. *Sea G un grupo y S un subcojunto de G. Definimos la clausura normal (clausura conjugada) de S en G como el subgrupo generado por $\{gsg^{-1} \mid s \in S, g \in G\}$. Lo denotamos por $N^G(S)$.*

PROPOSICIÓN 4.1. *Sea G un grupo y S un subcojunto de G. Entonces $N^G(S) \trianglelefteq G$.*

DEMOSTRACIÓN. Sin pérdida de generalidad suponemos que todos los inversos de S estan en S, esto es, $S^{-1} \subseteq S$. Un elemento x de $N^G(S)$ es de la forma $g_1s_1g_1^{-1}\dots g_ns_ng_n^{-1}$ para $g_1,\dots,g_n \in G$ y $s_1,\dots,s_n \in S$. Sea $h \in G$, entonces:

$$hxh^{-1} = hg_1s_1g_1^{-1}\dots g_ns_ng_n^{-1}h^{-1} = (hg_1)s_1(hg_1)^{-1}\dots(hg_n)s_n(hg_n)^{-1}$$

Por lo que $hxh^{-1} \in N^G(S)$. □

PROPOSICIÓN 4.2. *Sea G un grupo. Entonces $N^G\colon \mathscr{S}(G) \longrightarrow \mathscr{S}(G)$ es un operador cerradura, esto es, idempotente, inflatorio y monotono.*

DEMOSTRACIÓN. Tarea □

PROPOSICIÓN 4.3. *Sea G un grupo y S subconjunto de G. Entonces $\langle S\rangle \leq N^G(S)$.*

DEMOSTRACIÓN. Tarea □

PROPOSICIÓN 4.4. *Sea G un grupo y $\{N_i\}_{i\in I}$ una familia de subgrupos normales de G. Entonces $\bigcap_{i\in I} N_i \trianglelefteq G$.*

DEMOSTRACIÓN. Tarea □

PROPOSICIÓN 4.5. *Sea G un grupo y S un subconjunto de G. Entonces $N^G(S) = \bigcap\{N \trianglelefteq G \mid S \subseteq N\}$.*

DEMOSTRACIÓN. Tarea □

DEFINICIÓN 4.2. *Sea G un grupo. Una presentación de G es una pareja $(X \mid R)$ donde X es un conjunto y $R \subseteq F(X)$ tales que $G \cong F(X)/N^{F(X)}(R)$. Al conjunto X lo llamamos generadores y al conjunto R relaciones. En caso de que $X = \{x_1, \ldots, x_n\}$ y $R = \{r_1, \ldots, r_m\}$ sean finitos, escribiremos $(x_1, \ldots, x_n \mid r_1, \ldots, r_m)$ en vez de $(X \mid R)$. Decimos que G es finitamente generado si tiene una presentación con X finito, decimos que es finitamente relacionado si tiene una presentación con R finito y decimos que es finitamente presentado si tiene una presentación con X y R finitos.*

PROPOSICIÓN 4.6. *Todo grupo tiene una presentación.*

DEMOSTRACIÓN. Sabemos que todo grupo es cociente de in grupo libre por lo que existe X conjunto y $\phi : F(X) \longrightarrow G$ epimorfismo. Por el primer teorema de isomorfismo tenemos que $G \cong F(X)/nuc(\phi)$. Por lo tanto G tiene una representación $(X \mid nuc(\phi))$. □

EJEMPLO 4.1. *Todo grupo libre $F(X)$ tiene una presentación $(X \mid \emptyset)$. Por lo que todo grupo libre es finitamente relacionado.*

EJEMPLO 4.2. *Si $G = \mathbb{Z}_n$ con n natural. Entonces G tiene una representación $(x \mid x^n)$. Vemos que podemos definir una función $f\colon \{x\} \longrightarrow \mathbb{Z}_n$ dada por $f(x) = [1]$. Ahora por la propiedad universal del grupo libre existe un único morfismo de grupos $\phi\colon \mathbb{Z} \longrightarrow \mathbb{Z}_n$ tal que $\phi|_{\{x\}} = f$. Aquí estamos usado el hecho de que $F(\{x\}) = \mathbb{Z}$. Notamos que $nuc(\phi) = n\mathbb{Z}$ y por el primer teorema de isomorfismo tnemos el resultado. Vemos que la relación x^n realmente significa que $x^n = e$. Puntualmente $F(\{x\})$ es un grupo abeliano, así que todos sus subgrupos son abelianos. De este hecho tenemos que $N^{\mathbb{Z}}(\{x^n\}) = \langle x^n \rangle$. Ahora bien:*

$$(x\langle x^n \rangle)^n = x^n \langle x^n \rangle = \langle x^n \rangle$$

Aquí radica parte de la belleza de los cocientes, por que me ayudan a poner o inducir relaciones que busco. Veamos que yo quiero un grupo generado por un elemento y que ese elemento elevado a la n sea el neutro. Como tal mi grupo no esta generado por x si no por $x\langle x^n \rangle$. Veamos que usando el clásico $x \in H$ si y sólo si $xH = H$. Veamos que la última parte equivale a decir en el grupo cociente que xH es el neutro de G/H. La condición es medio tramposa puesto que una vex que entendemos que para ser neutro, basta con que el representante pertenezca al subgrupo, podemos ver inmediatamente que esta condición es trivial puesto que el elemento es un generador en este caso $x^n \in \langle x^n \rangle$.

EJEMPLO 4.3 (Tarea). *Si $G = \mathbb{Z}_{pq}$ con p y q primos relativos. Entonces G tiene una representación $(x,y \mid x^p, y^q, [x,y])$. Aquí tenemos dos generadores y tres relaciones. Este ejempo es interesante por que la representación de un grupo no es única, puesto que por el ejemplo anterior G también se puede representar como $(x \mid x^{pq})$. Por otro lado $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Vesmos que las primeras dos relaciones reflejan las copias de $\mathbb{Z}_p$ y $\mathbb{Z}_q$. Analicemos la tercera, primero llamemos $H = N^G(x^p, y^p, [x,y])$. Ahora veamos que:*

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

Por lo que $xyH = yxH$. Entonces la relación $[x,y]$ realmente lo que quiere decir es $xy = yx$.

EJEMPLO 4.4. *El grupo dihedrico D_n de orden $2n$ tiene representación $(r,R \mid r^n, R^2, (rR)^2)$.*

EJEMPLO 4.5. *El grupo dihedrico infinito D_∞ tiene representación $(r,R \mid R^2, (rR)^2)$.*

EJEMPLO 4.6. *El grupo $GL_2(\mathbb{Z})$ tiene representación $(x,y,z \mid xyxy^{-1}x^{-1}y^{-1}, (xyx)^4, z^2, (zx)^2, (zy)^2)$.*

El definir un grupo por una presentación forma parte de la teoría de grupos combinatoria, e historicamente es la motivación de Whitehead de la teoría simple de homotopía.

4.1. El problema de Burnside.

DEFINICIÓN 4.3. *Sea G un grupo. Decimos que G es periodico si todo elemento tiene orden finito.*

Originalmente el problema de Burnside decía que si un grupo periodico finitamente generado esta obligado a ser finito. Este problema fue planteado por William Burnside en 1902 y en 1964 Golod y Safarevich dieron un contraejemplo. En este contraejemplo los ordenes de los elementos no estaban acotados, es decir, el grupo no tenía exponente finito. Por lo que se plante el problema de Burnside acotado. Que planta que todo grupo periodico finitamente generado y con exponente finito tiene que ser finito.

DEFINICIÓN 4.4. *El grupo libre de Burnside de rango m y exponente n, de notado por $B(m,n)$ es el grupo con m generadores y todo elemento cumple que $x^n = e$.*

El problema de Burnside acotado es equivalente a que todo $B(m,n)$ sea finito. Notemos que $B(1,n) \cong \mathbb{Z}_n$.

PROPOSICIÓN 4.7 (tarea). *Sea m un natural. Entonces $B(m,2) \cong \mathbb{Z}_2^m$.*

Sea sabe que para todo m natural, $B(m,3), B(m,4)$ y $B(m,4)$ son finitos. Hasta donde sabemos $B(2,5)$ es un problema abierto saber si es finito.

Sin embargo, este problema también tiene respuesta negativa, Vasilievich demostró en 1994 que para $m > 1$ y $n \geq 2^{48}$ par y divisible por 2^9 se tiene que $B(m,n)$ es infinito.

4.2. Producto Libre.

DEFINICIÓN 4.5. *Sean G y H grupos con representaciones $(X_G \mid R_G)$ y $(X_H \mid F_H)$, respectivamente. Su producto libre, denotado por $G*H$, es el grupo cuya representación es $(X_G \sqcup X_H \mid R_G \sqcup R_H)$.*

PROPOSICIÓN 4.8 (tarea). *Sean X y Y conjuntos. Entonces $F(X)*F(Y) \cong F(X \sqcup Y)$.*

PROPOSICIÓN 4.9 (tarea). *Sean G y H grupos. Entonces $G*H \cong H*G$.*

Consideramos que la composición de morfismos canónicos $\phi : F(X_G) \longrightarrow F(X_G \sqcup X_H) \longrightarrow G*H$. Afirmamos que $nuc(\phi) = N^{F(X_G)}(R_G)$.

$\subseteq$) Sea $x \in nuc(\phi) \subseteq F(X_G)$. Entonces:

$$N^{F(X_G \sqcup X_H)}(R_G \sqcup R_H) = \phi(x) = xN^{F(X_G \sqcup X_H)}(R_G \sqcup R_H)$$

Por lo que $x \in N^{F(X_G \sqcup X_H)}(R_G \sqcup R_H) \cap F(X_G) = N^{F(X_G)}(R_G)$.

$\supseteq$) Sea $x \in N^{F(X_G)}(R_G) \subseteq N^{F(X_G \sqcup X_H)}(R_G \sqcup R_H)$. Entonces $x \in nuc(\phi)$.

Por lo que podemos definir $i_G = \phi_{nuc(\phi)} : G \longrightarrow G*H$ que es un monomorfismo. Analogamente definimos $i_H : H \longrightarrow G*H$.

PROPOSICIÓN 4.10. *Sean G y H grupos. Entonces $G*H = \langle im(i_G) \cup im(i_H) \rangle$.*

DEMOSTRACIÓN. Sea $x \in G*H$. Entonces $x = \overline{x_1 \dots x_n}$ con $x_i \in X_G \cup X_H$. Por lo que $x = \overline{x_1} \dots \overline{x_n}$ con $\overline{x_i} \in im(i_G) \cup im(i_H)$. Por lo tanto $G*H \subseteq \langle im(i_G) \cup im(i_H) \rangle$ □

PROPOSICIÓN 4.11. *Sean G y H grupos. Entonces todo elemento $e \neq x \in G*H$ tiene una expresión única como $i_G(g_1)i_H(h_1) \dots i_G(g_n)i_H(h_n)$ con $g_1, \dots g_n \in G$ y $h_1, \dots, h_n \in H$ permitiendo solamente que $g_1 = e$ y $h_n = e$.*

DEMOSTRACIÓN. Obsevamos que si $x \in X_G$ entonces existe $g \in G$ tal que $i_G(g) = \overline{x}$ y si $x \in X_H$ entonces existe $h \in H$ $i_H(h) = \overline{x}$. Más aún, estos elementos son únicos. Por lo que para $x \in G*H$, se tiene que $x = \overline{x_1 \dots x_n}$ para algunos $x_i \in X_G \cup X_H$. Si $\overline{x_1} \notin X_G$ o $\overline{x_n} \notin X_H$, entonces podemos escribir $x = i_G(e)x$, $x = xi_H(e)$ o $x = i_G(e)xi_H(e)$ según sea el caso. Si $x_i, x_{i+1} \in X_G$ o $x_i, x_{i+1} \in X_H$ podemos sustituirlo por $y_i \in X_G$ o $y_i \in X_H$ segun sea el caso. Esto sucede puesto que existe $g_i, g_{i+1} \in G$ tales que $i_G(g_i) = \overline{x_i}$ y $i_G(g_{i+1}) = \overline{x_{i+1}}$. Por lo que:

$$\overline{x_i x_{i+1}} = i_G(g_i)i_G(g_{i+1}) = i_G(g_i g_{i+1})$$

Considerando el caso análogo para H y por un argumento inductivo podemos deducir la factorización propuesta.

La unicidad es tarea □

PROPOSICIÓN 4.12. *Sean G y H grupos y $f_G : G \longrightarrow K$ y $f_H : H \longrightarrow K$ morfismos de grupo. Entonces existe un único morfismo de grupos $f : G*H \longrightarrow K$ tal que $fi_G = f_G$ y $fi_H = f_H$.*

DEMOSTRACIÓN. Definimos

$$f(i_G(g_1)i_H(h_1)\dots i_G(g_n)i_H(h_n)) = f_G(g_1)f_H(h_1)\dots f_G(g_n)f_H(h_n)$$

para $i_G(g_1)i_H(h_1)\dots i_G(g_n)i_H(h_n) \in G*H$. Esta función esta bien definida por la unicidad de la factorización.

Que es morfismo, es tarea.

Notamos que $fi_G = f_G$ y $fi_H = f_H$ es por construcción.

Por último como $G*H = \langle im(i_H) \sqcup im(i_G)\rangle$, el morfismo f es único. □

5. Producto directo

Sea $\{G_\alpha\}_{\alpha\in\Lambda}$ una familia de grupos no vacía. A nivel de conjuntos se puede considerar el producto cartesianos generalizado,

$$\prod_{\alpha\in\Lambda} G_\alpha = \left\{ x : \Lambda \to \bigcup_{\alpha\in\Lambda} G_\alpha \;\middle|\; \forall \alpha \in \Lambda (x(\alpha) \in G_\alpha) \right\}$$

Puede definirse una operación binaria en este conjunto usando el hecho de que cada elemento en la familia $\{G_\alpha\}_{\alpha\in\Lambda}$ es un grupo pues para $x, y \in \prod_{\alpha\in\Lambda} G_\alpha$, se define $xy \in \prod_{\alpha\in\Lambda} G_\alpha$ como la función tal que para cada $\alpha \in \Lambda$, $(xy)(\alpha) := x(\alpha)y(\alpha)$.

Observe que esta operación da una estructura de grupo a $\prod_{\alpha\in\Lambda} G_\alpha$ pues la asociatividad se deduce de la asociatividad en cada grupo. El neutro en la función $e : \Lambda \to \bigcup_{\alpha\in\Lambda} G_\alpha$, que en cada $\alpha \in \Lambda$, $e(\alpha) = e \in G_\alpha$, donde para no cargar la notación no se distinguen los neutros de cada uno de los elementos G_α. Para concluir, dado $x \in \prod_{\alpha\in\Lambda} G_\alpha$, observe que x^{-1} está dado para que en cada $\alpha \in \Lambda$, $(x^{-1})(\alpha) = x(\alpha)^{-1}$.

Esto muestra que $\prod_{\alpha\in\Lambda} G_\alpha$ tiene una estructura de grupo. Ahora observe que para $\beta \in \Lambda$ se puede considerar la función

$$\begin{array}{c} \pi_\beta : \prod_{\alpha\in\Lambda} G_\alpha \to G_\beta \\ x \mapsto x(\beta) \end{array}$$

Esta función es un ejemplo de morfismo de grupos. Además,

$$nuc(\pi_\beta) = \left\{ x \in \prod_{\alpha\in\Lambda} G_\alpha \;\middle|\; x(\beta) = e \right\}.$$

Dado que π_β es claramente suprayectiva, por el primer teorema de isomorfismo se concluye que

$$\left(\prod_{\alpha\in\Lambda} G_\alpha\right)/nuc(\pi_\beta) \cong G_\beta$$

En particular, para el caso $\Lambda = \{1,2\}$ se deduce que $G_1 \times \{e\} \trianglelefteq G_1 \times G_2$, $\{e\} \times G_2 \trianglelefteq G_1 \times G_2$ y $(G_1 \times G_2)/(\{e\} \times G_2) \cong G_1$. Dado que claramente $G_1 \times \{e\} \cong G_1$ y $\{e\} \times G_2 \cong G_2$, esto dice que $G_1 \times G_2$ tiene una copia de G_1 y G_2 como subgrupos normales.

Observe que de hecho $\prod_{\alpha\in\Lambda} G_\alpha$ tiene una copia de cada G_α como subgrupo normal adaptando el argumento anterior.

EJEMPLO 5.1. *Si $n,m \in \mathbb{N}^+$ son tales que $(n,m) = 1$, $\mathbb{Z}_n \times \mathbb{Z}_m$ en cíclico de orden nm por un ejercicio del capítulo 1 (ejercicio 41). Luego, por uno de los corolarios del primer teorema de isomorfismo se concluye que $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$.*

En particular observe que se conocen tres grupos de orden 6: $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_6$ y S_3. Así, el resultado dice que esencialmente hay 2 pues $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. Además $S_3 \ncong \mathbb{Z}_6$ pues S_3 no es abeliano y $\mathbb{Z}_6$ sí.

Hay algunas observaciones que vale la pena realizar antes de continuar con la teoría general. La primera es que dado que de la teoría de conjuntos el producto vacío es un conjunto unitario, el producto vacío puede definirse como el grupo neutro, por lo que se tiene la definición del producto de cualquier familia de grupos $\{G_\alpha\}_{\alpha\in\Lambda}$. Al tomar en cuenta esto se puede dar propiedades de productos finitos analizando el caso binario y el producto vacío. Con esta filosofía los siguientes resultados están escritos en el caso binario.

PROPOSICIÓN 5.1. *Si G es un grupo y $H,K \trianglelefteq G$ tales que $HK = G$ y $H \cap K = \{e\}$, entonces $G \cong H \times K$.*

DEMOSTRACIÓN. Se define la función $f : H \times K \to G$ que tiene por regla de correspondencia $f(h,k) = hk$. Para ver que f es un isomorfismo se va a probar que f es un morfismo biyectivo.

Afirmación: f es morfismo. En efecto, dados (h_1,k_1), $(h_2,k_2) \in H \times K$,

$$f((h_1,k_1)(h_2,k_2)) = f(h_1h_2,k_1k_2) = (h_1h_2)(k_1k_2) = h_1(k_1k_1^{-1})h_2k_1(h_2^{-1}h_2)k_2 = f(h_1,k_1)k_1^{-1}h_2k_1h_2^{-1}f(h_2,k_2)$$

Observe que estas igualdades prueban la afirmación si $k_1^{-1}h_2k_1h_2^{-1} = e$. Para esto observe que como $H \trianglelefteq G$, $k_1^{-1}h_2k_1 \in H$, de donde $(k_1^{-1}h_2k_1)h_2^{-1} \in H$. Por otro lado $h_2k_1h_2^{-1} \in K$ pues $K \trianglelefteq G$ y así $k_1^{-1}(h_2k_1h_2^{-1}) \in K$. Esto ultimo prueba que $k_1^{-1}h_2k_1h_2^{-1} \in H \cap K = \{e\}$, lo que prueba el resultado.

Para ver que f es inyectiva sea $(h,k) \in nuc(f)$, entonces $hk = e$. Así, como $h = k^{-1}$, se deduce que $h \in H \cap K = \{e\}$. Luego, $h = e$ y además como $k^{-1} = e$, $k = e$. Por lo tanto $(h,k) = (e,e)$. Esto prueba la contención no trivial de la igualdad de conjuntos $nuc(f) = \{(e,e)\}$, lo que muestra la inyectividad de f.

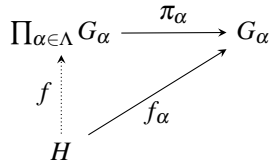
Para concluir observe que f es suprayectiva pues por hipótesis $G = HK$. □

Es importante decir que en muchos textos la definición de $H \times K$ como el producto cartesiano con la estructura de grupo dada se le conoce como **producto directo externo**, nombre que es claro de la construcción de este pues se recuerda que este tiene una copia de H y K. Por otro lado el resultado anterior permite definir una versión interna que se define diciendo que G es **producto directo interno** de H y K si $H,K \trianglelefteq G$, $H \cap K = \{e\}$ y $HK = G$. Así, observe que esta distinción es superflua pues el resultado anterior dice que si G es producto directo interno de H y K, entonces es producto directo externo. Más aún, por el ejercicio 124 se deduce que si G es producto directo externo de un par de grupos, este se puede ver como un producto directo interno. Por tal razón no se harán distinciones entre estos.

Otra cosa que es importante decir es que la definición de producto directo interno es el análogo a la definición de suma directa de espacios, por lo que esta discusión no debe ser rara para el lector. Se recomiendan los ejercicios 122 y 123 para apoyar esta idea.

Regresando a asuntos generales se va a probar el siguiente resultado que caracteriza dicha construcción. El trasfondo de esto es nuevamente un resultado de la teoría de categorías.

PROPOSICIÓN 5.2. *(Propiedad universal del producto) Sea $\{G_\alpha\}_{\alpha\in\Lambda}$ una familia de grupos. Dada una familia de morfismos $\{f_\alpha : H \to G_\alpha\}_{\alpha\in\Lambda}$, existe un único morfismo $f : H \to \prod_{\alpha\in\Lambda} G_\alpha$ tal que para cualquier $\alpha \in \Lambda$, $\pi_\alpha \circ f = f_\alpha$. Es decir, el siguiente diagrama conmuta*



DEMOSTRACIÓN. Sea $\{f_\alpha : H \to G_\alpha\}_{\alpha\in\Lambda}$ una familia de morfismos. Para definir f, dado $x \in H$, $f(x)(\alpha) := f_\alpha(x)$. Veamos que f es un morfismo. Para esto sean $x_1, x_2 \in H$. Dado $\alpha \in \Lambda$,

$$f(x_1x_2)(\alpha) = f_\alpha(x_1x_2) = f_\alpha(x_1)f_\alpha(x_2) = f(x_1)(\alpha)f(x_2)(\alpha) = (f(x_1)f(x_2))(\alpha)$$

Como $\alpha \in \Lambda$ fue arbitrario se deduce que $f(x_1x_2) = f(x_1)f(x_2)$, lo que concluye la prueba de la afirmación.

Dado $\alpha \in \Lambda$, observe que como $\pi_\alpha \circ f$, $f_\alpha : H \to G_\alpha$, para la igualdad que se quiere probar basta ver que estas funciones tienen la misma regla de correspondencia. Sea $x \in H$, entonces $(\pi_\alpha \circ f)(x) = f(x)(\alpha) := f_\alpha(x)$, lo que implica la igualdad.

Para la unicidad supóngase que $g : H \to \prod_{\alpha\in\Lambda} G_\alpha$ es un morfismo tal que para cualquier $\alpha \in \Lambda$, $\pi_\alpha \circ g = f_\alpha$. Para ver que $g = f$ basta ver que f y g tienen la misma regla de correspondencia por lo que dado $x \in H$, para cualquier $\alpha \in \Lambda$, $g(x)(\alpha) = (\pi_\alpha \circ g)(x) = f_\alpha(x) =: f(x)(\alpha)$. Así, como $x \in H$ fue arbitrario, se concluye que $g = f$. □

La propiedad anterior conceptualmente es obvia, sin embargo al pensar en abstracto permite demostrar proposiciones sin hacer uso de la construcción explícita de $\prod_{\alpha\in\Lambda} G_\alpha$ pues como sucedió en el caso del grupo libre esta propiedad caracteriza a este objeto. Por ejemplo, de esta es claro que $\prod_{\alpha\in\emptyset} G_\alpha = \{e\}$. Otras propiedades que se pueden deducir es que $G \times (H \times K) \cong (G \times H) \times K$ ó $G \times H \cong H \times G$. Este tipo de ideas debe irse madurando y forman el núcleo básico de la teoría de categorías. Uno de los objetivos de este curso es ir desarrollando algunas ideas en turno a esta intuición.

6. Ejercicios

EJERCICIO 71. *Sea $f : (\mathbb{Q}, +) \to (\mathbb{Z}, +)$ un morfismo de grupos. Demuestre que $f = 0$.*

DEFINICIÓN 6.1. *Para G y H grupos se define $Hom(G,H) = \{f : G \to H \mid f$ es morfismo de grupos$\}$.*

EJERCICIO 72.

1. *Demuestre que si $f \in Hom(\mathbb{Z}_n, \mathbb{Z}_m)$ entonces existe $r \in \mathbb{Z}$ tal que $f(x) = rx$ donde el orden de r en $\mathbb{Z}_n$ divide a (n,m).*
2. *Describir explícitamente el $Hom(\mathbb{Z}_{21}, \mathbb{Z}_7)$.*
3. *Describir explícitamente el $Hom(\mathbb{Z}_{21}, \mathbb{Z}_{10})$.*
4. *Describir explícitamente el $Hom(\mathbb{Z}_{21}, \mathbb{Z}_{12})$.*

EJERCICIO 73. *Sea $f : G \to H$ un morfismo de grupos. Demuestre lo siguiente:*

1. *Si $K \leq G$, entonces $f(K) \leq H$.*
2. *Si $K \leq H$, entonces $f^{-1}(K) \leq G$.*

EJERCICIO 74. *Dar un ejemplo de un morfismo de grupos tal que la imagen no sea un subgrupo normal.*

EJERCICIO 75. *Sea $f : G \to H$ un morfismo de grupos. Demuestre que si $K \trianglelefteq G$ entonces $f(K) \trianglelefteq im(f)$.*

EJERCICIO 76. *Sea G un grupo finito y supóngase que existe $n > 1$ tal que la función $f : G \to G$ dada por $f(x) = x^n$ es un morfismo. Demuestre que $im(f) \trianglelefteq G$.*

EJERCICIO 77. *Demuestre que G es un grupo abeliano si y sólo si la función $f : G \to G$ definida mediante $f(x) = x^{-1}$ es un endomorfismo de grupos.*

EJERCICIO 78. *Sea $f : G \to H$ un morfismo. Demuestre que son equivalentes:*

1. *f es suprayectiva.*
2. *f es cancelable por la derecha respecto a morfismos de grupos.*

EJERCICIO 79. *Sea $\imath : 2\mathbb{Z} \to \mathbb{Z}$ la inclusión canónica. Demuestre que ninguna inversa izquierda de $\imath$ es un morfismo de grupos.*

EJERCICIO 80. *Sea $\pi : \mathbb{Z} \to \mathbb{Z}_2$ la proyección canónica. Demuestre que ninguna inversa derecha de π es un morfismo de grupos.*

EJERCICIO 81. *Sea $f : G \to H$ un morfismo de grupos y $g \in G$. Demuestre lo siguiente:*

1. *Si g tiene orden finito, entonces $f(g)$ tiene orden finito y además $o(f(g))|o(g)$.*
2. *Si f es un isomorfismo y g tiene orden infinito, entonces $f(a)$ también tiene orden infinito.*
3. *¿Qué sucede con la afirmación anterior si se quita la hipótesis de que f sea un isomorfismo?*

EJERCICIO 82. *Sean X, Y dos conjuntos equipotentes. Demuestre que $S_X \cong S_Y$. Usar este resultado para probar que si X es un conjunto finito, existe $n \in \mathbb{N}$ tal que $S_X \cong S_n$.*

EJERCICIO 83. *Sea $f : G \to H$ un morfismo de grupos. Demuestre que $f^{-1}(f(g)) = g \cdot nuc(f) = nuc(f) \cdot g$.*

EJERCICIO 84. *Sea $N \leq G$. Demuestre que $N \trianglelefteq G$ si y sólo si existe $f : G \to H$ un morfismo tal que $nuc(f) = N$.*

EJERCICIO 85. *Demuestre las siguientes afirmaciones:*

1. *Si $f : G \to H$ es un morfismo de grupos con H abeliano, entonces existe un único morfismo de grupos $\overline{f} : G_{ab} \to H$ tal que $\overline{f} \circ \pi_{G_{ab}} = f$, donde $\pi_{G_{ab}}$ es la proyección de G en su abelianización.*
2. *Dado $f : G \to H$ un morfismo de grupos, este induce un morfismo de grupos $f_{ab} : G_{ab} \to H_{ab}$.*

EJERCICIO 86. *Sean $f : G \to H$ y $g : H \to L$ morfismos de grupos con g un epimorfismo. Demuestre que si $nuc(g) \subseteq nuc(f)$, entonces existe un único morfismo de grupos $h : L \to H$ tal que $f = h \circ g$. Demuestre además que $im(f) = im(h)$ y que $nuc(h) = g(nuc(f))$. ¿Cuándo es h inyectiva?*

EJERCICIO 87. *Demuestre lo siguiente:*

1. *El grupo de Klein y $\mathbb{Z}_2 \times \mathbb{Z}_2$ son isomorfos.*
2. *$\mathbb{Z}_2 \times \mathbb{Z}_2$ y $\mathbb{Z}_4$ no son isomorfos.*

EJERCICIO 88. *Demuestre que:*

1. *D_2 y el grupo de Klein son isomorfos.*
2. *D_3 y S_3 son isomorfos.*

EJERCICIO 89. *Sea G un grupo finito. Demuestre que si existen $g,h \in G$ elementos de orden 2, entonces $\langle g,h\rangle \cong D_n$ para algún $n \in \mathbb{N}$.*

EJERCICIO 90. *Sea $f : G \to X$ una función biyectiva con X un conjunto. Demuestre que existe una única estructura de grupo en X que hace de f un isomorfismo.*

EJERCICIO 91. *Con las hipótesis y notación del ejercicio 2 sean $o, o' \in S$ y $(S,+)$, $(S,+')$ los grupos asociados a dichos elementos, es decir, supóngase que $+$ y $+'$ con asociativas. Demuestre que $(S,+) \cong (S,+')$.*

EJERCICIO 92. *Sea $f : G \to H$ un morfismo de grupos, $K \trianglelefteq G$ y $L \trianglelefteq H$. Supóngase además que $f(K) \subseteq L$, demuestre lo siguiente:*

1. *f induce un morfismo de grupos $\overline{f} : G/K \to H/L$.*
2. *Si f es un isomorfismo y $f(K) = L$, entonces $\overline{f}$ es un isomorfismo.*

EJERCICIO 93. *Demuestre que si $G \cong H$ entonces G y H tienen la misma cantidad de elementos con orden d, donde $d \in \mathbb{N}^+$.*

EJERCICIO 94. *Demuestre que dos grupos cíclicos son isomorfos si y sólo si tienen el mismo orden.*

EJERCICIO 95. *Demuestre las siguientes afirmaciones:*

1. *Existe un grupo I tal que para todo grupo G existe un único morfismo de grupos $f : I \to G$. Además, que dicho grupo I es único (salvo isomorfismo) con esa propiedad.*
2. *Existe un grupo F tal que para todo grupo G existe un único morfismo de grupos $g : G \to F$. Pruebe que F también es único.*

EJERCICIO 96.

1. *Sea $f : G \to H$ un morfismo de grupos. Demuestre que existen $g : G \to K$ un epimorfismo y $h : K \to H$ un monomorfismo tales que $f = h \circ g$.*
2. *Supóngase que se tiene un diagrama conmutativo de morfismos de grupos*

$$\begin{array}{ccc} G & \xrightarrow{e} & H \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ K & \xrightarrow[m]{} & L \end{array}$$

donde e es epi y m es mono. Demuestre que existe un único morfismo $h : H \to K$ tal que $h \circ e = f$ y $m \circ h = g$.

EJERCICIO 97. *Sea $f : G \to H$ un morfismo de grupos con $G \neq \{e\}$ y G simple. Demuestre que f es mono.*

EJERCICIO 98. *Sea $p \in \mathbb{N}$ primo y G un grupo abeliano de orden p^2. Demuestre que $G \cong \mathbb{Z}_{p^2}$ ó $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.*[3]

EJERCICIO 99. *Sea $f : G \to H$ un morfismo de grupos. Demuestre lo siguiente:*

1. *La función $\imath : nuc(f) \to G$ es un monomorfismo.*
2. *Si $g : K \to G$ es un morfismo de grupos tal que $im(g) \subseteq nuc(f)$, entonces existe un único $h : K \to nuc(f)$ morfismo de grupos tal que $\imath \circ h = g$.*

[3]Más adelante se va a probar que todos los grupos de orden p^2 son abelianos por lo que esta hipótesis es superflua, sin embargo se requiere para realizar el ejercicio.

EJERCICIO 100. *Sean $f : G \to H$ y $g : K \to H$ morfismos de grupos. Demuestre que existe un grupo P con morfismos $p_1 : P \to G$ y $p_2 : P \to K$ tales que $f \circ p_1 = g \circ p_2$ y con la siguiente propiedad: Dado un grupo L con morfismos de grupos $h_1 : L \to G$ y $h_2 : L \to K$ tales que $f \circ h_1 = g \circ h_2$, existe un único morfismo de grupos $h : L \to P$ tal que $p_1 \circ h = h_1$ y $p_2 \circ h = h_2$.*

EJERCICIO 101. *Considere los conjuntos $G, H \subseteq M_2(\mathbb{R})$ definidos por*

$$G = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \;\middle|\; x \in \mathbb{R} \right\}$$

$$H = \left\{ \begin{pmatrix} \cosh x & \sinh x \\ \sinh x & \cosh x \end{pmatrix} \;\middle|\; x \in \mathbb{R} \right\}$$

Demuestre lo siguiente:

1. *$G, H \subseteq GL_2(\mathbb{R})$. Más aún, $G, H \leq GL_2(\mathbb{R})$.*
2. *$(\mathbb{R}, +) \cong G \cong H$*

EJERCICIO 102. *Demuestre los siguientes isomorfismos:*

1. *$(\mathbb{R}^*, \cdot)/\mathbb{Z}_2 \cong (\mathbb{R}^+, \cdot)$.*
2. *Para todo campo k, $GL_n(k)/SL_n(k) \cong k \setminus \{0\}$.*

EJERCICIO 103. *Demuestre que $\mathbb{T} \cong SO(2)$.*

EJERCICIO 104. *Considere el conjunto $SU(1,1) = \left\{ \begin{pmatrix} z & w \\ \overline{w} & \overline{z} \end{pmatrix} \;\middle|\; \|z\|^2 - \|w\|^2 = 1 \right\} \subseteq M_2(\mathbb{C})$.*

Demuestre lo siguiente:

1. *$SU(1,1) \leq GL_2(\mathbb{C})$.*
2. *$SL_2(\mathbb{R}) \cong SU(1,1)$.*

EJERCICIO 105.

1. *Sea* $Isom(\mathbb{R}^n) = \{f : \mathbb{R}^n \to \mathbb{R}^n \mid f \text{ es isometría suprayectiva}\}$. *Demuestre que* $Isom(\mathbb{R}^n) \leq S_{\mathbb{R}^n}$.
2. *Demuestre que* $Tr(\mathbb{R}^n) \trianglelefteq Isom(\mathbb{R}^n)$ *y que* $Isom(\mathbb{R}^n)/Tr(\mathbb{R}^n) \cong O(n)$.

EJERCICIO 106. *Sea* $G = \mathbb{R}^{[0,1]}$ *como grupo aditivo definiendo la operación de manera puntual. Demuestre que para todo* $a \in [0,1]$ *el conjunto* $N_a = \{f \in G \mid f(a) = 0\}$ *es un subgrupo normal de* G *y además* $G/N_a \cong (\mathbb{R}, +)$.

EJERCICIO 107. *Sea* V *un* k*-espacio vectorial. Defina*

$$GL(V) = \{T : V \to V \mid T \text{ es un automorfismo de espacios vectoriales}\}.$$

Demuestre lo siguiente:

1. $GL(V) \leq S_V$.
2. *Si* $\dim_k(V) < \aleph_0$, *entonces existe* $n \in \mathbb{N}$ *tal que* $GL(V) \cong GL_n(k)$.

EJERCICIO 108. *Sea* $n \in \mathbb{N}^+$ *y* k *un campo. Defina el conjunto* $P(n,k) := \{A \in M_n(k) \mid \exists \sigma \in S_n (A^i = e_{\sigma(i)})\}$, *donde* A^i *denota la* i*-ésima columna de la matriz* A *y* $\{e_1, ..., e_n\}$ *es la base canónica de* k^n.

Demuestre lo siguiente:

1. $P(n,k) \leq GL_n(k)$.
2. $P(n,k) \cong S_n$

EJERCICIO 109. *Demuestre que* S_4 *tiene un subgrupo isomorfo a* D_8.

EJERCICIO 110. *Demuestre que* $SL_2(\mathbb{C})$ *tiene un subgrupo isomorfo al grupo de Hamilton* $\mathbb{H}$.

EJERCICIO 111. *Demuestre que si* G *es un grupo no abeliano de orden* 8 *entonces* $G \cong \mathbb{H}$ *ó* $G \cong D_8$, *donde* $\mathbb{H}$ *es el grupo de Hamilton.*

EJERCICIO 112. *Demuestre lo siguiente:*

1. $D_n' = \langle r^2 \rangle$
2. $\mathbb{H}' = \{-1, 1\} \cong \mathbb{Z}_2$

EJERCICIO 113. *Sean $H \trianglelefteq G$ y $K, N \in S_H(G)$. Demuestre las siguientes afirmaciones:*

1. *$K \leq N$ si y sólo si $K/H \leq N/H$*
2. *Si $K \leq N$, entonces $[N : K] = [N/H; K/H]$*
3. *$K \trianglelefteq N$ si y sólo si $K/H \trianglelefteq N/H$*
4. *H es máximo si y sólo si G/H es simple.*[4]

EJERCICIO 114. *Sean $H, K \leq G$ y H^*, K^* subgrupos normales de H y K respectivamente. Demuestre las siguientes afirmaciones.*

1. $H^*(H \cap K^*) \trianglelefteq H^*(H \cap K)$.
2. $K^*(H^* \cap K) \trianglelefteq K^*(H \cap K)$.
3. $H^*(H \cap K)/H^*(H \cap K^*) \cong K^*(H \cap K)/K^*(H^* \cap K) \cong H \cap K/(H^* \cap K)(H \cap K^*)$.

EJERCICIO 115. *Sean $N \leq H, K \leq G$ tales que $N \trianglelefteq G$. Demuestre lo siguiente:*

1. $(H \wedge K)/N = (H/N) \wedge (K/N)$.
2. $(H \vee K)/N = (H/N) \vee (K/N)$.

EJERCICIO 116. *Sea $H \leq G$. Demuestre lo siguiente:*

1. *H es un subgrupo máximo respecto a ser normal si y sólo si G/H es simple.*
2. *Sea $H \trianglelefteq G$ un subgrupo máximo de G, entonces el orden de G/H es finito y un primo.*

DEFINICIÓN 6.2. *Sean $f : G \to H$ y $g : H \to K$ morfismos de grupos. Se dice que la pareja (f, g) es exacta en H si $nuc(g) = im(f)$. Además, la pareja es una sucesión exacta corta si las parejas $(\{e\} \to G, f)$, (f, g) y $(g, K \to \{e\})$ son exactas.*

[4] Ver definición 8.1.

EJERCICIO 117. *Sea $p \in \mathbb{N}$ un primo. Se definen las funciones $f : \mathbb{Z}_p \to \mathbb{Z}_{p^2}$ mediante $f(x) = px$ y $g : \mathbb{Z}_{p^2} \to \mathbb{Z}_p$ mediante $g(x) = x$. Demuestre las siguientes afirmaciones.*

1. *f y g están bien definidas y son morfismos de grupos.*
2. *La pareja (f,g) es una sucesión exacta corta.*
3. *¿Existe $f' : \mathbb{Z}_{p^2} \to \mathbb{Z}_p$ morfismo tal que $f' \circ f = 1_{\mathbb{Z}_p}$?.*
4. *¿Existe $g' : \mathbb{Z}_p \to \mathbb{Z}_{p^2}$ morfismo tal que $g' \circ g = 1_{\mathbb{Z}_{p^2}}$?.*

EJERCICIO 118. *Sea G un grupo y $H, K \leq G$ tales que $[G : H]$ y $[G : K]$ son finitos y primos relativos. Demuestre que $G = HK$.*

EJERCICIO 119. *Demuestre que si $n, m \in \mathbb{N}^+$ son tales que $(n,m) = 1$, entonces $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$. Concluya que si $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ es la descomposición en primos de n entonces $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}}$.*

EJERCICIO 120. *Sea G es un grupo y $H \leq G$ es un subgrupo simple con $[G : H] = 2$. Demuestre que H es el único subgrupo normal no trivial de G ó que existe $K \trianglelefteq G$ de orden 2 tal que la función $f : K \times H \to G$ dada por $f(k,h) = kh$ es un isomorfismo.*

EJERCICIO 121. *Sea G un grupo finito, $H \trianglelefteq G$ y $K \trianglelefteq G$ tales que $|G| = |H||K|$. Demuestre que si $H \cap K = \{e\}$ o $HK = G$, entonces $G \cong H \times K$.*

EJERCICIO 122. *Sean H y K subgrupos de un grupo G y tales que para todo $h \in H$ y $k \in K$, $hk = kh$. Demuestre que si todo elemento de G tiene una única descomposición como producto de un elemento de H y uno de K entonces $G \cong H \times K$.*

EJERCICIO 123. *Sean $H, K \trianglelefteq G$. Demuestre que $HK = G$ y $H \cap K = \{e\}$ si y sólo si para todo $g \in G$, existen una única expresión $g = hk$ con $h \in H$ y $k \in K$.*

EJERCICIO 124. *Sean G y H grupos. Demuestre lo siguiente:*

1. $(G\times\{e\})(\{e\}\times H) = G\times H$
2. $(G\times\{e\})\cap(\{e\}\times H) = \{(e,e)\}$
3. *$G\times H$ es abeliano si y sólo si G y H son abelianos.*

EJERCICIO 125. *Se define la función $\Delta: G\to G\times G$ mediante $\Delta(a) = (a,a)$. Demuestre las siguientes afirmaciones:*

1. *Δ es un monomorfismo.*
2. *$\Delta(G)\trianglelefteq G\times G$ si y sólo si G es abeliano.*
3. *G es abeliano si y sólo si el producto $\cdot : G\times G\to G$ es un morfismo.*

EJERCICIO 126. *Sean G y H grupos. Decir si las siguientes afirmaciones son verdaderas ó falsas dando una demostración o un contraejemplo según sea el caso:*

1. *Dados $G'\leq G$ y $H'\leq H$, $G'\times H'\leq G\times H$.*
2. *Todo subgrupo de $G\times H$ se obtiene como el producto de dos subgrupos, es decir, si $K\leq G\times H$, entonces existen $G'\leq G$ y $H'\leq H$ tales que $K = G'\times H'$.*

EJERCICIO 127. *Sean $\{G_\alpha\}_{\alpha\in\Lambda}$ una familia de grupos y para cada $\alpha\in\Lambda$, $N_\alpha\trianglelefteq G_\alpha$. Demuestre que $\prod_{\alpha\in\Lambda} N_\alpha\trianglelefteq\prod_{\alpha\in\Lambda} G_\alpha$ y además*

$$\Big(\prod_{\alpha\in\Lambda} G_\alpha\Big)/\Big(\prod_{\alpha\in\Lambda} N_\alpha\Big)\cong\prod_{\alpha\in\Lambda} G_\alpha/N_\alpha.$$

EJERCICIO 128. *Sean G y H grupos y $f: H\to Aut(A)$ un morfismo de grupos. Se define la función $*: (G\times H)^2\to G\times H$ mediante la regla de correspondencia $(g_1,h_1)*(g_2,h_2) = (g_1 f(h_1)(g_2), h_1h_2)$.*

1. *Demuestre que $(G\times H,*)$ es un grupo. Este grupo se va a denotar por $G\times_f H$.*
2. *Demuestre que existe $G'\trianglelefteq G\times_f H$ tal que $G\cong G'$.*
3. *Demuestre que existe $H'\leq G\times_f H$ tal que $H\cong H'$.*

EJERCICIO 129. *Sea $K\trianglelefteq G$ y $H\leq G$ tales que $KH = G$ y $K\cap H = \{e\}$. Demuestre que existe $f: H\to Aut(K)$ un morfismo de grupos tal que $G\cong K\times_f H$.*

EJERCICIO 130. *Demuestre que* $Aut(\mathbb{Z}) = \{1_{\mathbb{Z}}, -1_{\mathbb{Z}}\}$.

EJERCICIO 131. *Sea* $n \in \mathbb{N}^+$. *Demuestre que* $Aut(\mathbb{Z}_n) \cong (U(\mathbb{Z}_n), \cdot)$, *donde* $U(\mathbb{Z}_n)$ *es el grupo de unidades de* $\mathbb{Z}_n$.

EJERCICIO 132. *Sea* $n \geq 3$. *Demuestre que* $D_n \cong \mathbb{Z}_n \times_f \mathbb{Z}_2$ *para algún* $f : \mathbb{Z}_2 \to Aut(\mathbb{Z}_n)$.

EJERCICIO 133. *Demuestre que* $Aut(K) \cong S_3$.

EJERCICIO 134. *Demuestre que* $Aut(S_3) \cong S_3$.

EJERCICIO 135. *Considerese el grupo aditivo* $\mathbb{Z}_p^n$ *con* $n \in \mathbb{N}^+$. *Demuestre que el grupo de automorfismos de* $\mathbb{Z}_p^n$ *coincide con el grupo de automorfismos de* $\mathbb{Z}_p^n$ *como* $\mathbb{Z}_p$*- espacio vectorial.*

DEFINICIÓN 6.3. *Una estructura algebraica es rígida si el único automorfismo en dicha estructura es la identidad.*

EJERCICIO 136. *Demuestre que si* G *es un grupo rígido entonces* $|G| \leq 2$.

EJERCICIO 137. *Con la notación de ejercicio 63 supóngase que* $n = p^{n_1} \cdot \ldots \cdot p_r^{n_r}$ *es la descomposición en primos de n. Demuestre que si* G *y* H *son grupos abelianos de orden n tales que para todo* $i \in \{1, \ldots, r\}$, $G[p_i^{n_i}] \cong H[p_i^{n_i}]$, *entonces* $G \cong H$.

EJERCICIO 138. *Denótese por* C_l *al grupo cíclico de orden l. Sean* $n_1, \ldots, n_r, m_1, \ldots, m_s, p \in \mathbb{N}^+$ *con p primo,* $n_1 \geq \ldots \geq n_r$, $m_1 \geq \ldots \geq m_s$ *y* $\sum_{j=1}^{r} n_j = \sum_{j=1}^{s} m_j$. *Demuestre que* $C_{p^{n_1}} \times \ldots \times C_{p^{n_r}} \cong C_{p^{m_1}} \times \ldots \times C_{p^{m_s}}$ *si y sólo si* $r = s$ *y para toda* $i \in \{1, \ldots, r\}$, $C_{p^{n_i}} \cong C_{p^{m_i}}$.

DEFINICIÓN 6.4. *$H \leq G$ se llama característico si para todo $f \in Aut(G)$, $f(H) = H$.*

EJERCICIO 139.

1. *Demuestre que $H \leq G$ es característico si y sólo si para todo $f \in Aut(G)$, $f(H) \subseteq H$.*
2. *Demuestre que si $H \leq G$ es característico, entonces $H \trianglelefteq G$.*
3. *De un ejemplo de un subgrupo normal que no sea característico.*

EJERCICIO 140. *Demuestre que si $M, N \leq G$ son subgrupos característicos, entonces $MN \leq G$ es característico.*

EJERCICIO 141. *Demuestre que si $N \trianglelefteq G$ y $M \leq N$ es un subgrupo característico, entonces $M \trianglelefteq G$.*

EJERCICIO 142. *Sea $PSL_2(\mathbb{Z})$ el grupo de transformaciones de Möbius con coeficientes enteros y determinante 1 y $f : SL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z})$ la transformación canónica que a cada matriz le asocia su transformación de Möbius.*

1. *Demuestre que f es un morfismo de grupos.*
2. *Demuestre que si $\Gamma_1 \leq SL_2(\mathbb{Z})$, entonces $nuc(f|_{\Gamma_1}) = \{Id, -Id\}$.*
3. *Demuestre que no existe $\Gamma_1 \leq SL_2(\mathbb{Z})$ tal que $-Id \notin \Gamma_1$ y $f(\Gamma_1) = PSL_2(\mathbb{Z})$.*

EJERCICIO 143. *Sea $n \in \mathbb{N}^+$ y denótese por* $\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a \equiv 1 \mod n, b \equiv 0 \mod n, c \equiv 0 \mod n, d \equiv 1 \mod n \right\}$.

1. *Demuestre que $\Gamma(n) \leq SL_2(\mathbb{Z})$.*
2. *Demuestre que $SL_2(\mathbb{Z})/\Gamma(n) \cong SL_2(\mathbb{Z}_n)$.*

EJERCICIO 144. *Usar la propiedad universal del grupo libre para demostrar que si los conjuntos X y Y con biyectables, entonces $F(X) \cong F(Y)$.*

EJERCICIO 145. *Demuestre que* $PSL(2,\mathbb{Z}) \cong \langle a,b \mid a^2 = b^3 = e \rangle$

EJERCICIO 146. *Se recuerda que* $D_\infty = \langle r,s \mid s^2 = e, srs = r^{-1} \rangle$. *Demuestre que* $D_\infty \cong \mathbb{Z}_2 * \mathbb{Z}_3$

EJERCICIO 147. *Demuestre que* $B(m,2) \cong \mathbb{Z}_2^m$.

EJERCICIO 148. *Sean* G,H,K *grupos. Demuestre que:*

1. $G * H \cong H * G$
2. $G * (H * K) \cong (G * H) * K$

DEFINICIÓN 6.5. *Para una familia de grupos* $\{G_\alpha\}_{\alpha\in\Lambda}$ *donde cada* G_α *tiene una presentación* $(X_\alpha|R_\alpha)$, *defina el producto libre de dicha familia, el que se va a denotar por* $*_{\alpha\in\Lambda} G_\alpha$, *como el grupo que tiene por presentación* $(\bigsqcup_{\alpha\in\Lambda} X_\alpha | \bigsqcup_{\alpha\in\Lambda} R_\alpha)$.

EJERCICIO 149. *Sean* X *y* Y *conjuntos. Demuestre que:*

1. $F(X) * F(Y) \cong F(X \sqcup Y)$
2. *Todo grupo libre se puede escribir como el producto libre de una familia de grupos libres de rango 1.*

EJERCICIO 150. *Demuestre que el producto libre de una familia de grupos satisface las siguientes propiedades, resultado que se conoce como la propiedad universal:*

1. *Existe una familia de monomorfismos* $\{\iota_\beta : G_\beta \to *_{\alpha\in\Lambda} G_\alpha\}_{\beta\in\Lambda}$.
2. *Dada cualquier familia de morfismos de grupos* $\{f_\beta : G_\beta \to H\}$, *existe un único morfismo de grupos* $f : *_{\alpha\in\Lambda} G_\alpha \to H$ *tal que para cualquier* $\alpha \in \Lambda$, $f \circ \iota_\alpha = f_\alpha$.

Anexos

7. Retículas

DEFINICIÓN 7.1. *Sea P un conjunto y $\leq$ una relación sobre P. Decimos que P con $\leq$ es un conjunto parcialmente ordenado.*

1. *Para toda $x \in P$, $x \leq x$*
2. *Para todo $x, y \in P$, si $x \leq y$ e $y \leq x$, entonces $x = y$*
3. *Para todo $x, y, z \in P$, si $x \leq y$ e $y \leq z$, entonces $x \leq z$*

EJEMPLO 7.1. *Sea X un conjunto. Entonces el conjunto potencia $\mathscr{P}(X)$ es un conjunto parcialmente ordenado con la contención $\subseteq$.*

DEFINICIÓN 7.2. *Sea L un conjunto parcialmente ordenado. Decimos que L tiene un elemento máximo x. Si para todo $y \in L$, $y \leq x$. Por la asimetría el elemento maximo es único y lo denotamos por $\bar{1}$.*

En el caso de $\mathscr{P}(X)$ su elemento máximo es X.

DEFINICIÓN 7.3. *Sea L un conjunto parcialmente ordenado. Decimos que L tiene un elemento máximo x. Si para todo $y \in L$, $x \leq y$. Por la asimetría el elemento maximo es único y lo denotamos por $\bar{o}$.*

En el caso de $\mathscr{P}(X)$ su elemento mínimo es $\emptyset$.

DEFINICIÓN 7.4. *Sea L un conjunto parcialmente ordenado, $S \subseteq L$ y $a \in L$. Decimos que a es una cota superiorde S, si $x \leq a$ para toda $x \in S$.*

En caso de S sea vacío, cualquier elemento de L es cota superior.

DEFINICIÓN 7.5. *Sea L un conjunto parcialmente ordenado, $S \subseteq L$ y $a \in L$. Decimos que a es el supremo de S, si a es la menor cota superior, es decir, si a cumple:*

- *Para todo $x \in S$, $x \leq a$.*
- *Si $b \in L$ es tal que para todo $x \in S$ tenemos que $x \leq b$, entonces $a \leq b$*

NOTACIÓN 7.1. *Sean L una retícula, $S \subseteq L$ y $x, y \in L$. Denotamos por $\bigvee S$ al supremo de S. En caso de que $S = \{x, y\}$, ponemos $x \vee y$ para denotar al supremo.*

En caso de S sea vacío, $\bigvee S = \bar{0}$.

DEFINICIÓN 7.6. *Sea L un conjunto parcialmente ordenado, $S \subseteq L$ y $a \in L$. Decimos que a es una cota inferior de S, si $a \leq x$ para toda $x \in S$.*

En caso de S sea vacío, cualquier elemento de L es cota inferior.

DEFINICIÓN 7.7. *Sea L un conjunto parcialmente ordenado, $S \subseteq L$ y $a \in L$. Decimos que a es el ínfimo de S, si a es la menor cota inferior, es decir, si a cumple:*

- *Para todo $x \in S$, $a \leq x$.*
- *Si $b \in L$ es tal que para todo $x \in S$ tenemos que $b \leq x$, entonces $b \leq a$*

NOTACIÓN 7.2. *Sean L una retícula, $S \subseteq L$ y $x, y \in L$. Denotamos por $\bigwedge S$ al ínfimo de S. En caso de que $S = \{x, y\}$, ponemos $x \wedge y$ para denotar al ínfimo.*

En caso de S sea vacío, $\bigwedge S = \bar{1}$.

DEFINICIÓN 7.8. *Sea L un conjunto parcialmente ordenado. Decimos que L es una retícula, si para todo $x, y \in L$ $x \wedge y$ y $x \vee y$ existen.*

DEFINICIÓN 7.9. *Una retícula L es completa si todo subconjunto S de L, $\bigvee S$ y $\bigwedge S$ existen.*

Tenemos que $\mathscr{P}(X)$ es una retícula completa.

PROPOSICIÓN 7.1. *Sean L una retícula tal que existen todos los ínfimos. Entonces L es una retícula completa.*

DEFINICIÓN 7.10. *Una retícula L es modular, si $a \leq b$ implica $a \vee (x \wedge b) = (a \vee x) \wedge b$ para cualesquiera $a, b, x \in L$.*

DEFINICIÓN 7.11. *Sean L una retícula, y $x, y \in L$. Decimos que y es un pseudocomplemento de x si:*

- *$x \wedge y = \bar{0}$.*
- *Si $z \in L$ es tal que $z \wedge x = \bar{0}$ y $y \leq z$, entonces $z = y$.*

DEFINICIÓN 7.12. *Para $(P,\leq)$ un conjunto parcialmente ordenado, una función $f : P \to P$ es un operador:*

1. *monótono si f es una función monótona, es decir, para cualesquiera $x,y \in P$ tales que $x \leq y$, se tiene que $f(x) \leq f(y)$.*
2. *idempotente si $f \circ f = f$.*
3. *inflatorio si para cualquier $x \in P$, $x \leq f(x)$.*
4. *cerradura si es monótono, idempotente e inflatorio.*

8. Lema de Zorn

Bibliografía

[1] J.S. Golan. *The Linear Algebra a Beginning Graduate Student Ought to Know*. Texts in the Mathematical Sciences. Springer, 2004.