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 [**2**]

[**3**] [**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 $x = h_{n-1}g_n = h_n$. $\square$

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 $\sigma : X \longrightarrow X$.*

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.

$\square$

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. $\square$

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,* $\{e^{\frac{2\pi i k}{p^n}} \mid k, n \in \mathbb{N}^+\} \leq \mathbb{T}$.

[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 $H = K$. $\square$

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.

$SG1)$ Dado que para cualquier $\alpha \in \Lambda$ se tiene que $e \in H_\alpha$, entonces $e \in \bigcap_{\alpha\in\Lambda} H_\alpha$.

$SG2)$ 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. $\square$

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 $n \in \mathbb{N}$, $s_1, \ldots, s_n \in S$ y $k_1, \ldots, k_n \in \{-1, 1\}$. 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. $\square$

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 $\langle g^k \rangle = G$. $\square$

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. $\square$

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 $G = \mathbb{Z}_n$. $\square$

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.

$\square$

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 $X = \{1, \ldots, n\}$ 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 $S_n := S_{\{1,\ldots,n\}}$. 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 $\{1, \ldots, n\}$ 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. $\square$

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. $\square$

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.

$s_2 r = (12)(123) = (23)$. 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.

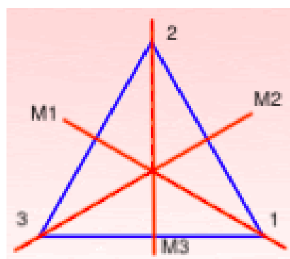


FIGURA 1.

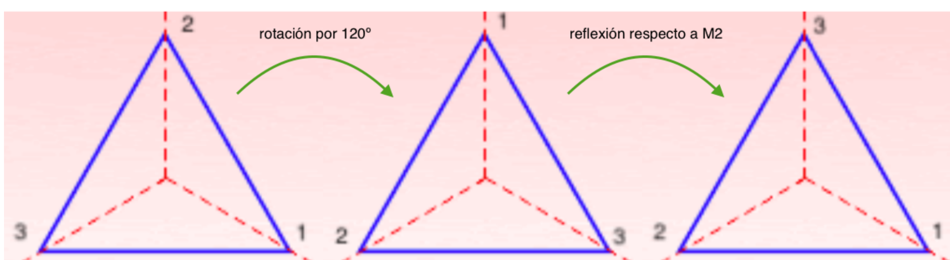


FIGURA 2.

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:*

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

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*

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

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 $1 \le i < j \le n$ 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,

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

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 $\mathbb{Z}[x_{\tau(1)}, \ldots, x_{\tau(n)}]$ por lo que al hacer el cambio de variable obvio se obtiene el resultado. $\square$

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. $\square$

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 $\tau_1, \ldots \tau_{2n+1}$ 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 $\tau_1, \ldots, \tau_{2n}$ transposiciones, entonces $sgn(\sigma) = (-1)^{2n} = 1$, de lo que se tiene el resultado. $\square$

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 $g \sim_H k$.

$\square$

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 $k \in [g]_{\sim_H}$. $\square$

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. $\square$

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 $a \cong a^p \mod p$. $\square$

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. $\square$

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. $\square$

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. $\square$

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:*

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

¿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* $g_1, \ldots, g_n \in G$ *entonces* $(g_1 \cdot \ldots \cdot g_n)^{-1} = g_n^{-1} \cdot \ldots \cdot g_1^{-1}$. *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* $G = \{e, a_1, \ldots, a_n\}$ *un grupo de orden* $n+1$ *donde el único elemento tal que* $x^2 = e$ *es* e. *Calcule* $a_1 \cdot \ldots \cdot a_n$.
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 $K_4 \subseteq S_4$ definido por $K_4 = \{(1),(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$ es un grupo abeliano. A este grupo se le conoce como el grupo de Klein.*[3]

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. $SU(n) \leq SL_n(\mathbb{C}) \leq GL_n(\mathbb{C})$

[3]Una notación alternativa para el grupo de Klein es V, la cual proviene del alemán “Vierergruppe” que significa grupo de cuatro elementos.

*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 $|D_n| = 2n$.*[4]
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?*

[4] 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 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?*

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:*

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

1. *Demuestre que* $\sim$ *es una relación de equivalencia en* $\{1,...,n\}$.
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 $H_1,\ldots,H_n$ clases laterales derechas (izquierdas) de subgrupos de G tales que $G = H_1 \cup \ldots \cup H_n$. 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* $\iota : H \to G$ *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. $\square$

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, $g_1 = h_1(1) = h_2(1) = g_2$. $\square$

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. $\square$

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 $\ln \circ \exp = 1_{(\mathbb{R},+)}$.*

[1] En teoría de categorías a los morfismos que cumplen la propiedad 3 de la proposición anterior se les conoce como isomorfismos y a los que cumplen 2 se les llama morfismos invertibles. Estos siempre coinciden y por lo tanto no se introducen ambos términos pues dicha distinción es innecesaria. Por otro lado, en 1 está oculto el hecho de que estos morfismos son cancelables por izquierda y derecha respecto a otros morfismos de grupos. Los morfismos que cumplen esta última propiedad se conocen como bimorfismos, sin embargo se reservará este concepto hasta el capítulo 5, donde se presentará una pequeña introducción a la teoría de categorías.

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

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 $f_1f_2^{-1} = \gamma_{g_1}\gamma_{g_2}^{-1} = \gamma_{g_1g_2^{-1}}$, luego, $f_1f_2^{-1} \in Int(G)$ 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

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

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 $f(x) = f_K(xK) = y$. $\square$

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 $\mathbb{Z} \cong G$. $\square$

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. $\square$

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. $\square$

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 $\phi : \mathscr{S}_H(G) \longrightarrow \mathscr{S}(G/H)$ 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 $\phi(\psi(L)) = L$. $\square$

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:*

$$\begin{tikzcd} X \arrow[r, "\iota"] \arrow[dr, "f"'] & F \arrow[d, dotted, "\overline{f}"] \\ & G \end{tikzcd}$$

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. $\square$

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. $\square$

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 $|X| = |Y|$. $\square$

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.

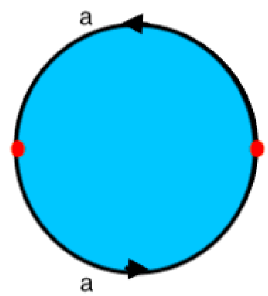
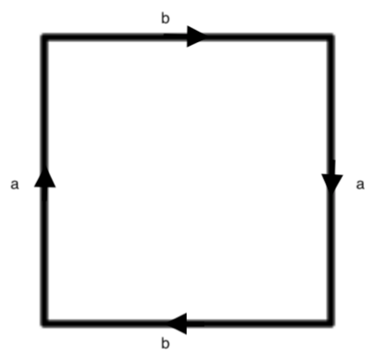


FIGURA 1.

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 $\square$

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 $(X \mid nuc(\phi))$. $\square$

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 $f : \{x\} \longrightarrow \mathbb{Z}_n$ dada por $f(x) = [1]$. Ahora por la propiedad universal del grupo libre existe un único morfismo de grupos $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ 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 $x = \overline{x_1 \ldots x_n}$ con $x_i \in X_G \cup X_H$. Por lo que $x = \overline{x_1} \ldots \overline{x_n}$ 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 $i_G(g_1)i_H(h_1)\ldots i_G(g_n)i_H(h_n)$ con $g_1, \ldots g_n \in G$ y $h_1, \ldots, h_n \in H$ 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 $i_G(g) = \bar{x}$ y si $x \in X_H$ entonces existe $h \in H$ $i_H(h) = \bar{x}$. Más aún, estos elementos son únicos. Por lo que para $x \in G*H$, se tiene que $x = \overline{x_1 \ldots x_n}$ 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. $\square$

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

$$\begin{aligned} \pi_\beta : \textstyle\prod_{\alpha\in\Lambda} G_\alpha &\to G_\beta \\ x &\mapsto x(\beta) \end{aligned}$$

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 $G = HK$. $\square$

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*

$$\begin{tikzcd}
\prod_{\alpha\in\Lambda} G_\alpha \arrow[r, "\pi_\alpha"] & G_\alpha \\
H \arrow[u, dotted, "f"] \arrow[ur, "f_\alpha"'] &
\end{tikzcd}$$

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 $g = f$. $\square$

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* $\iota : 2\mathbb{Z} \to \mathbb{Z}$ *la inclusión canónica. Demuestre que ninguna inversa izquierda de* ι *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*

$$\begin{tikzcd} G \arrow[r, "e"] \arrow[d, "f"'] & H \arrow[d, "g"] \\ K \arrow[r, "m"'] & L \end{tikzcd}$$

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

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

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* $Isom(\mathbb{R}^n) = \{f : \mathbb{R}^n \to \mathbb{R}^n \mid f$ *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_4.

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* $G \cong D_4$, *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*

$$\left(\prod_{\alpha\in\Lambda}G_\alpha\right)/\left(\prod_{\alpha\in\Lambda}N_\alpha\right)\cong\prod_{\alpha\in\Lambda}G_\alpha/N_\alpha.$$

EJERCICIO 128. *Sean G y H grupos y $f : H\to Aut(G)$ un morfismo de grupos. Se define la función $* : (G\times H)^2\to G\times H$ mediante la regla de correspondencia $(g_1,h_1)*(g_2,h_2)=(g_1f(h_1)(g_2),h_1h_2)$.*

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* $Aut(K_4) \cong S_3$.

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* $n = p^{n_1} \cdot ... \cdot p_r^{n_r}$ *es la descomposición en primos de* n. *Demuestre que si* G *y* H *son grupos abelianos de orden* n *tales que para todo* $i \in \{1, ..., r\}$, $G[p_i^{n_i}] \cong H[p_i^{n_i}]$, *entonces* $G \cong H$.

EJERCICIO 138. *Denótese por* C_l *al grupo cíclico de orden* l. *Sean* $n_1, ..., n_r, m_1, ..., m_s, p \in \mathbb{N}^+$ *con* p *primo,* $n_1 \geq ... \geq n_r$, $m_1 \geq ... \geq m_s$ *y* $\sum_{j=1}^{r} n_j = \sum_{j=1}^{s} m_j$. *Demuestre que* $C_{p^{n_1}} \times ... \times C_{p^{n_r}} \cong C_{p^{m_1}} \times ... \times C_{p^{m_s}}$ *si y sólo si* $r = s$ *y para toda* $i \in \{1, ..., r\}$, $C_{p^{n_i}} \cong C_{p^{m_i}}$.

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* $\alpha \in \Lambda$, $f \circ \iota_\alpha = f_\alpha$.

Capítulo 3

Grupos Simétricos

"Las matemáticas puras son, en su forma, la poesía de las ideas lógicas."

Albert Einstein.

1. Conjugados

DEFINICIÓN 1.1. *Sea G un grupo y $x, y \in G$. Se define la siguiente relación $x \sim y$, si existe $g \in G$ tal que $x = gyg^{-1}$. Se dice que x es conjugado de y en G*

PROPOSICIÓN 1.1. *Sea G un grupo. La relación ser conjugado es relación de equivalencia.*

DEMOSTRACIÓN. Sea $x \in G$, entonces $x = exe^{-1}$. Por lo tanto $x \sim x$.

Sean $x, y \in G$ con $x \sim y$, entonces existe $g \in G$ tal que $x = gyg^{-1}$. Por lo que $y = g^{-1}xg$. Por lo tanto $y \sim x$.

Sean $x, y, z \in G$ tales $x \sim y$ y $y \sim z$. Entonces existen $g, h \in G$ tales que $x = gyg^{-1}$ y $y = hzh^{-1}$. Sustituyendo tenemos que $x = ghzh^{-1}g^{-1} = ghz(gh)^{-1}$. Por lo que $x \sim z$. □

A la clase de equivalencia de x se le denotará x^G.

PROPOSICIÓN 1.2. *Sea G un grupo, $x, y \in G$. Entonces $o(xy) = o(yx)$.*

DEMOSTRACIÓN. Notamos $xy = x(yx)x^{-1}$. □

DEFINICIÓN 1.2. *Sea G un grupo. El centro de G, $Z(G)$, es el subconjunto de elementos de G que conmutan con todos los elementos de G.*

PROPOSICIÓN 1.3 (tarea). *Sea G un grupo. Entonces $Z(G) \trianglelefteq G$.*

PROPOSICIÓN 1.4 (tarea). *Sea G un grupo y $x \in G$. Entonces $x \in Z(G)$ si y sólo si $x^G = \{x\}$.*

DEFINICIÓN 1.3. *Sean G un grupo y $x \in G$. El centralizador de x en G, $C_G(x)$, es el subconjunto de elementos de G que conmutan con x.*

PROPOSICIÓN 1.5 (Tarea). *Sean G un grupo y $x \in G$. Entonces $C_G(x) \leq G$.*

PROPOSICIÓN 1.6. *Sean G un grupo y $x \in G$. Entonces $|x^G| = [G : C_G(x)]$. Más aún, si G es finito, $|x^G|$ es un divisor del orden de G.*

DEMOSTRACIÓN. Recordemos que $[G : C_G(x)] = |G/C_G(x)|$ y $G/C_G(x)$ aquí sólo denota las clases izquierdas, puesto que de primera instancia no sabemos que $C_G(x)$ es un subgrupo normal de G. Por lo que definimos $\phi \colon x^G \longrightarrow G/C_G(x)$ dada por $\phi(gxg^{-1}) = gC_G(x)$ para $gxg^{-1} \in x^G$. Primero hay que ver que ϕ esta bien definida. Si $gxg^{-1} = hxh^{-1}$ con $g, h \in G$, entonces $h^{-1}gx = xh^{-1}g$. Por lo que $h^{-1}g \in C_G(x)$. Por lo tanto $hC_G(x) = gC_G(x)$ y ϕ esta bien definida.

Sean $gxg^{-1}, hxh^{-1} \in x^G$ con $gC_G(x) = hC_G(x)$. Por lo que $h^{-1}g \in C_G(x)$. Entonces $h^{-1}gx(h^{-1}g)^{-1} = x$. Despejando $gxg^{-1} = hxh^{-1}$. Por lo tanto ϕ es inyectiva.

Para $g \in G$, tenemos que $\phi(gxg^{-1}) = gC_G(x)$. Por lo tanto ϕ es suprayectiva. Por lo tanto ϕ es una biyección. En el caso de que G sea finito, el resultado se sigue del teorema de Lagrange. $\square$

DEFINICIÓN 1.4. *Sean $H \leq G$ y $a \in G$. Entonces ponemos $H^a = aHa^{-1}$.El normalizador de H en G, $N_G(H)$, es el conjunto de $a \in G$ tales $H^a = H$.*

PROPOSICIÓN 1.7 (tarea). *Sean $H \leq G$. Entonces $H \trianglelefteq N_G(H)$. Más aún, $N_G(H)$ es el máximo subgrupo de G donde H es normal.*

De lo último se sigue que $H \trianglelefteq G$ si y sólo si $N_G(H) = G$.

PROPOSICIÓN 1.8 (tarea). *Sea G un grupo. Entonces N_G es un operador clausura.*

PROPOSICIÓN 1.9 (tarea). *Sean $H \leq G$ y $a,b \in G$. Entonces $H^a = H^b$ si y sólo si $b^{-1}a \in N_G(H)$.*

PROPOSICIÓN 1.10. *Sean $H \leq G$. Entonces $|H^G| = [G : N_G(H)]$. Más aún, si G es finito, entonces $|H^G|$ divide al orden de G.*

DEMOSTRACIÓN. Recordemos que $[G : N_G(H)] = |G/N_G(H)|$ y $G/N_G(H)$ aquí sólo denota las clases izquierdas, puesto que de primera instancia no sabemos que $N_G(H)$ es un subgrupo normal de G. Por lo que definimos $\phi : H^G \longrightarrow G/N_G(H)$ dada por $\phi(gHg^{-1}) = gN_G(H)$ para $gHg^{-1} \in H^G$. Primero hay que ver que ϕ esta bien definida. Si $gHg^{-1} = hHh^{-1}$ con $g,h \in G$, entonces $h^{-1}gH = xh^{-1}H$. Por lo que $h^{-1}g \in N_G(H)$. Por lo tanto $hN_G(H) = gN_G(H)$ y ϕ esta bien definida.

Sean $gHg^{-1}, hHh^{-1} \in H^G$ con $gN_G(H) = hN_G(H)$. Por lo que $h^{-1}g \in N_G(H)$. Entonces $h^{-1}gH(h^{-1}g)^{-1} = H$. Despejando $gHg^{-1} = hHh^{-1}$. Por lo tanto ϕ es inyectiva.

Para $g \in G$, tenemos que $\phi(gxg^{-1}) = gN_G(H)$. Por lo tanto ϕ es suprayectiva. Por lo tanto ϕ es una biyección. En el caso de que G sea finito, el resultado se sigue del teorema de Lagrange. □

2. Estructuras cíclicas en los grupos simétricos

El objetivo de esta sección es caracterizar el cuándo dos permutaciones $\sigma, \tau \in S_n$ son conjugadas en términos de la estructura cíclica de estas. Para esto es necesario puntualizar lo siguiente:

DEFINICIÓN 2.1. *Sean $\sigma, \tau \in S_n$. Decimos que σ y τ tienen la misma estructura cíclica si sus factorizaciones completas tienen el mismo número de r-ciclos para cada $r \in \mathbb{N}$.*

EJEMPLO 2.1. *Las permutaciones $\sigma, \tau \in S_6$ definidas mediante $\sigma = (123)(45)$ y $\tau = (145)(26)$ tienen la misma estructura cíclica.*

El concepto dado anteriormente está relacionado con el concepto de conjugación estudiado en la sección pasada. Para ver esto se requiere de un resultado previo.

LEMA 2.1. *Si $\sigma \in S_n$ es un r-ciclo, digamos $\sigma = (i_1 \cdots i_r)$, entonces para cualquier $\tau \in S_n$ se tiene que $\tau\sigma\tau^{-1} = (\tau(i_1) \cdots \tau(i_r))$. En particular todo conjugado de un r-ciclo es un r-ciclo.*

DEMOSTRACIÓN. Sea $\tau \in S_n$. La igualdad que se quiere probar es una igualdad de funciones en S_n, por lo que basta ver que estas tienen la misma regla de correspondencia. Para esto sea $j \in \{1, ..., n\}$. Se tienen dos casos:

Caso 1. Si $j = \tau(i_l)$ para algún $l \in \{1, ..., r\}$, entonces

$$\tau\sigma\tau^{-1}(j) = \tau\sigma(i_l) = \begin{cases} \tau(i_{l+1}), & \text{Si } l \in \{1, ..., r-1\} \\ \tau(i_1) & \text{Si } l = r \end{cases}$$

Luego es claro que $\tau\sigma\tau^{-1}(j) = (\tau(i_1) \cdots \tau(i_r))(j)$.

Caso 2. Si $j \neq \tau(i_l)$ para todo $l \in \{1, ..., r\}$, entonces $(\tau(i_1) \cdots \tau(i_r))(j) = j$. Por otro lado, como la hipótesis dice que $\tau^{-1}(j) \notin \{i_1, ..., i_r\}$, entonces $\tau^{-1}(j) \in fix(\sigma)$. Así, $\tau\sigma\tau^{-1}(j) = \tau\tau^{-1}(j) = j$, lo que prueba la igualdad. □

Retomando el ejemplo 2.1, se afirma que σ es conjugada con τ. Esto quiere decir que existe $\gamma \in S_6$ tal que

$$\sigma = \gamma\tau\gamma^{-1}.$$

Para determinar quién es γ se va a utilizar el resultado anterior, para lo que es necesario conocer la estructura cíclica de τ. Observe que:

$$\gamma\tau\gamma^{-1} = \gamma(145)(26)\gamma^{-1} = \gamma(145)\gamma^{-1}\gamma(26)\gamma^{-1} = (\gamma(1)\gamma(4)\gamma(5))(\gamma(2)\gamma(6))$$

Así, dado que se quiere que $\gamma\tau\gamma^{-1} = \sigma$, entonces se tiene que cumplir que

$$(\gamma(1)\gamma(4)\gamma(5)) = (123)$$
$$(\gamma(2)\gamma(6)) = (45)$$

Por lo que $\gamma(1) = 1$, $\gamma(4) = 2$, $\gamma(5) = 3$, $\gamma(2) = 4$ y $\gamma(6) = 5$. Además observe que $\gamma(3) = 6$ para que $\gamma \in S_6$. En notación cíclica

$$\gamma = (1)(24)(365) = (24)(365)$$

A manera de conclusión, la discusión anterior dice que las permutaciones del ejemplo 2.1 son conjugadas. Este es un hecho general, es decir, no sólo es válido para las permutaciones de dicho ejemplo y, de hecho el resultado caracteriza el cuando dos permutaciones tienen la misma estructura cíclica. Esto se muestra a continuación.

PROPOSICIÓN 2.1. *Sean $\sigma, \tau \in S_n$. Son equivalentes:*

1. σ *es conjugada a* τ.

2. σ *y* τ *tienen la misma estructura cíclica.*

DEMOSTRACIÓN. $1 \Rightarrow 2)$ Por hipótesis existe $\gamma \in S_n$ tal que $\sigma = \gamma\tau\gamma^{-1}$. Sea $\tau = \tau_1 \cdots \tau_k$ la factorización completa de τ. Observe que como $\sigma = (\gamma\tau_1\gamma^{-1}) \cdots (\gamma\tau_k\gamma^{-1})$, al ser cada τ_i un $r(i)$-ciclo, se deduce del lema anterior que $\gamma\tau_i\gamma^{-1}$ es un $r(i)$-ciclo. Además, cada uno de dichos ciclos son ajenos entre sí. Luego, por unicidad esta factorización es la factorización completa de σ, de lo que se deduce que σ y τ tienen el mismo número de r-ciclos para cada $r \in \mathbb{N}$, lo que concluye la prueba en esta dirección.

$2 \Rightarrow 1)$ Sean $\sigma = \sigma_1 \cdots \sigma_k$ y $\tau = \tau_1 \cdots \tau_k$ factorizaciones completas de σ y τ, donde observe que en estas existen el mismo número de factores por la hipótesis y además puede suponerse que para cada $i \in \{1, ..., k\}$, τ_i y σ_i son ciclos con la misma longitud. Luego, si $\tau_i = (j_1 \cdots j_{r(i)})$ y $\sigma_i = (k_1 \cdots k_{r(i)})$, entonces se define $\gamma(j_l) = k_l$ para cada $l \in \{1, ..., r_i\}$ y para cada $i \in \{1, ..., k\}$. De la definición es claro que $\gamma \in S_n$ y que $\gamma\tau\gamma^{-1} = \sigma$. $\square$

El resultado anterior permite dar una nueva caracterización del concepto de normalidad para el caso de grupos simétricos.

PROPOSICIÓN 2.2. *Sea* $H \leq S_n$. *Entonces* $H \trianglelefteq S_n$ *si y sólo si para cualquier* $\sigma \in H$, *todo* $\tau \in S_n$ *con la misma estructura cíclica que* σ *satisface que* $\tau \in H$.

DEMOSTRACIÓN. Es obvio del resultado anterior y la definición de normalidad. $\square$

EJEMPLO 2.2. *Considere el grupo de Klein* $K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$. *En los ejercicios del capítulo 1 se demostró que* $K_4 \leq S_4$. *Más aún, del resultado anterior se deduce que* $K_4 \trianglelefteq S_4$ *y además de esto último se deduce que* $K_4 \trianglelefteq A_4$. *Considere* $G := \langle (12)(34) \rangle \leq K_4$. *Dado que* $|G| = 2$, *entonces* $[K_4 : G] = 2$ *y por lo tanto* $G \trianglelefteq K_4$. *Esto dice que se tiene una cadena de subgrupos normales*

$$\{(1)\} \trianglelefteq G \trianglelefteq K_4 \trianglelefteq A_4 \trianglelefteq S_4.$$

Sin embargo se observa que $G \ntrianglelefteq S_4$ *pues* $(13)(12)(34)(13)^{-1} = (14)(23) \notin G$. *Esto proporciona un ejemplo de que la normalidad de subgrupos no es transitiva.*

Para concluir esta sección se van a realizar algunos resultados de carácter combinatorio. El primero de ellos tiene que ver con saber cuántos r-ciclos hay en S_n para $r \in \{1,...,n\}$. Para esto observe que para definir un r-ciclo hay que dar una sucesión de r elementos distintos del conjunto $\{1,...,n\}$, por lo que las formas de construir una de estas sucesiones es $n(n-1)...(n-r+1)$. Además recordemos que al tomar una de estas sucesiones, digamos $\{i_1,...,i_r\}$, representan el mismo ciclo las funciones

$$(i_1 i_2 \cdots i_r) = (i_2 i_3 \cdots i_r i_1) = ... = (i_r i_1 \cdots i_{r-1}).$$

Así, que se concluye que el número de r-ciclos en S_n es:

$$\frac{1}{r} n(n-1) \cdot ... \cdot (n-r+1) = \frac{1}{r} \frac{n!}{(n-r)!}.$$

EJEMPLO 2.3. *Como aplicación de la fórmula anterior observe que el número de triciclos en* S_4 *es* $\frac{1}{3}\frac{4!}{(4-3)!} = 8$. *De hecho observe que en este caso estos son:*

$$(123), (132), (234), (243), (314), (341), (412), (421).$$

Por supuesto que la importancia de la fórmula obtenida radica en el hecho de que para n "grande" esta proporciona una forma de saber cuántos r-ciclos hay sin necesidad de escribirlos de forma explícita. Un resultado interesante en torno al conteo realizado se presenta a continuación.

PROPOSICIÓN 2.3. *El grupo* A_4 *no tiene subgrupo de orden 6.*

DEMOSTRACIÓN. (T.L.Sheu) Argumentando por contradicción supóngase que uno de tales subgrupos existe y sea este G. Dado que $|A_4| = \frac{4!}{2} = 12$, entonces del teorema de Lagrange se deduce que $[A_4 : G] = 2$, por lo que $G \trianglelefteq A_4$ y para cualquier $\sigma \in A_4$, $\sigma^2 \in G$. En particular, si $\sigma \in A_4$ es un triciclo, entonces $\sigma = \sigma^4 = (\sigma^2)^2 \in G$, por lo que G debe tener como elementos a todos los triciclos de S_4, pero esto es una contradicción pues $|G| = 6$ y hay 8 triciclos en S_4. $\square$

Observe que la proposición anterior da un ejemplo (de hecho el primero en nuestro caso) de que el converso del teorema de Lagrange es falso ya que $|A_4| = 12$, $6|12$ pero no existe $G \leq A_4$ tal que $|G| = 6$. En el siguiente capítulo se verá que bajo ciertas condiciones dicho recíproco es cierto; estos resultados se conocen como el teorema de Cauchy y los teoremas de Sylow.

Por el momento, y para concluir la sección, se va a ver cómo determinar las estructuras que hay en S_4 desde la perspectiva de sus estructuras cíclicas. Respecto a r-ciclos hay 4 estructuras cíclicas posibles, donde en cada una de ellas se puede calcular el número de r-ciclos con la fórmula obtenida anteriormente. Observe que las estructuras restantes son necesariamente productos de transposiciones ajenas $(ij)(kl)$. Es claro que de estas hay 3

Representante de estructura cíclica	Número de conjugados
(1)	1
(12)	$\frac{1}{2}\frac{4!}{(4-2)!} = 6$
(123)	$\frac{1}{3}\frac{4!}{(4-3)!} = 8$
(1234)	$\frac{1}{4}\frac{4!}{(4-4)!} = 6$
$(12)(34)$	3

TABLA 1. Conteo de estructuras cíclicas en S_4.

Representante de estructura cíclica	Número de conjugados
(1)	1
(12)	$\frac{1}{2}\frac{5!}{(5-2)!} = \frac{1}{2}\frac{5!}{3!} = 10$
(123)	$\frac{1}{3}\frac{5!}{(5-3)!} = \frac{1}{3}\frac{5!}{3!} = 20$
(1234)	$\frac{1}{4}\frac{5!}{(5-4)!} = 30$
(12345)	$\frac{1}{5}\frac{5!}{(5-5)!} = 24$
$(12)(34)$	$\frac{1}{2}(\frac{5\cdot 4}{2}\cdot\frac{3\cdot 2}{2}) = 15$
$(123)(45)$	$\frac{5\cdot 4\cdot 3}{3}\cdot\frac{2\cdot 1}{2} = 20$

TABLA 2. Conteo de estructuras cíclicas en S_5.

Representante de estructura cíclica	Número de conjugados
(1)	1
(123)	20
(12345)	24
$(12)(34)$	15

TABLA 3. Conteo de estructuras cíclicas en A_5.

distintas (los elementos no triviales del grupo de Klein). Una forma combinatoria de obtener dicho conteo es al adaptar el conteo de r-ciclos realizados anteriormente pues para el factor (ij) hay $\frac{4\cdot 3}{2}$ elecciones y para (kl) hay $\frac{2\cdot 1}{2}$ posibilidades. Además, como $(ij)(kl) = (kl)(ij)$, el número de estas permutaciones es:

$$\frac{1}{2}\left(\frac{4\cdot 3}{2}\cdot\frac{2\cdot 1}{2}\right) = 3.$$

Los resultados se encuentran en la tabla 1 y es importante notar que esto da un total de 24 elementos como es de esperarse.

Este tipo de conteos pueden realizarse para otros casos, por ejemplo, para el caso de S_5 se muestra en la tabla 2 y, de este se deduce el correspondiente A_5 en la tabla 3.

3. Simplicidad de los grupos Alternantes

PROPOSICIÓN 3.1. *Sean $H \trianglelefteq G$ con índice primo p, $x, y \in G$ y $C_H(x) < C_G(x)$. Si x es conjugado de y en G, entonces x es conjugado de y en H.*

DEMOSTRACIÓN. Primero notamos que $C_H(x) = H \cap C_G(x)$ y aplicamos el segundo teorema de isomorfismo a $H \trianglelefteq G$ y a $C_G(x)$. Por lo que tenemos:

$$C_G(x)H/H \cong C_G(x)/C_G(x) \cap H = C_G(x)/C_H(x)$$

Por hipotesis sabemos que $C_H(x) < C_G(x)$. Por lo que $0 < |C_G(x)/C_H(x)| = [C_G(x)H : H]$. Por otro lado, $[G : C_G(x)H][C_G(x)H : H] = [G : H]$ que es primo y por lo anterior solo queda que $[C_G(x)H : H] = [G : H]$. Por lo tanto $C_G(x)H = G$.

Sea $g \in G$ tal que $x = gyg^{-1}$. Entonces $g = ha$ con $h \in H$ y $a \in C_H(x)$.

$$x = gyg^{-1} = hay(ha)^{-1} = hyh^{-1}$$

$\square$

PROPOSICIÓN 3.2. *A_5 es simple.*

DEMOSTRACIÓN. Primero veremos que todos los triciclos son conjugados en A_5. Esto es cierto en S_5. Por lo cual usaremos la proposición anterior. Sademos que $[S_5 : A_5] = 2$, por lo que A_5 es un subgrupo normal de índice primo. Consideremos $\alpha = (123)$ y notemos que $(45) \in C_{S_5}(\alpha)$ y $(45) \notin A_5$, por lo que la contención es propia, es decir, $C_{A_5}(\alpha) > C_{S_5}(\alpha)$. De aquí podemos concluir que $\alpha^{A_5} = \alpha^{S_5}$. Lo importante de destacar, es que el conjugado de un triciclo es un triciclo, pero acabamos de mostrar que obtenemos todos los triciclos al conjugar solamente por elementos pares. Esta clase de conjugación tiene 20 elementos.

Ahora queremos ver de nuevo que todos producto de dos transposiciones disjuntas son conjugadas en A_5, consideremos $\beta = (12)(34)$ y que $(12) \in C_{S_5}(\beta)$ y $(12) \notin A_5$. Usando la proposición tenemos que todos producto de dos transposiciones disjuntas son conjugadas en A_5. Esta clase de conjugación tiene 12 elementos.

Ahora consideremos $\gamma = (12345)$ que tiene 24 conjugados en S_5 y 12 en A_5. Puesto que los elementos de conmutan con γ tienen que ser sus potencias por lo que $|C_{A_5}(\gamma)| = 5 = |C_{S_5}(\gamma)|$. Por lo que

$$|\gamma^{S_5}| = [S_5 : C_{S_5}(\gamma)] = |S_5|/|C_{S_5}(\gamma)| = 60/5 = 12$$

y

$$|\gamma^{A_5}| = [A_5 : C_{A_5}(\gamma)] = |A_5|/|C_{A_5}(\gamma)| = 60/5 = 12$$

Por lo que concluimos que existen dos clases de conjugación de 5-ciclos en A_5 ambas con 12 elementos.

Recordemos que si $H \trianglelefteq G$, entonces $H = \bigcup_{x\in H} x^G$. Por lo que si $H \trianglelefteq A_5$ es propopio debe ser un divisor de 60 y tiene que tener un orden que sea la suma de 1 más una combinación de $12, 12, 15$ y 20. Es fácil ver que esta condición no sé cumple. Por lo que no exiten subgrupos no triviales.

□

PROPOSICIÓN 3.3. *Sea $H \trianglelefteq A_n$ con $n \geq 5$. Si H tiene un triciclo, entonces $H = A_n$.*

DEMOSTRACIÓN. Queremos probar que todos los triciclos son conjugados. Así si tiene un triciclo, tendrá a todos por normalidad y H es generado por todo los triciclos.

Para ver que los triciclos son conjugados lo haremos tomando como referencia (123) e (ijk). Si no disjuntos, entonces podemos decir que coinciden en k. Dejando fijos todos los simbolos posiblemente excepto $X = \{1, 2, 3, i, j\}$. Por lo que podemos pensar sin pérdida de generalidad que $(123), (ijk) \in A_X$. Como $A_X \cong A_5$, entonces (123) y (ijk) son conjugados en A_X y esto implica que también lo son en A_n.

Si (123) y (ijk) son disjuntos. Podemos usar el argumento anterior de la siguiente forma, (123) y $(3jk)$ son conjugados, y $(3jk)$ y (ijk) son conjugados. Por lo tanto (123) y (ijk) son conjugados. □

PROPOSICIÓN 3.4. *A_6 es simple.*

DEMOSTRACIÓN. Sea $e \neq H \trianglelefteq A_6$ y $\sigma \in H$ con $\sigma \neq 1$. Si σ fija algún $i = 1, \ldots 6$, entonces definimos $F_i = \{\alpha \in A_6 \mid \alpha(i) = i\}$. Es fácil ver que $F_i \cong A_5$ y que $\sigma \in H \cap F_i$. Por el segundo teorema de isomorfismo tenemos que $H \cap F_i \trianglelefteq F_i$, pero F_i es simple, por lo que la única opción es que $H \cap F_i = F_i$. Por lo que $F_i \leq H$. De aquí H contiene un triciclo y por la proposición anterior $H = A_6$.

Ahora si σ no fija a algún elemento, su estructura ccílica debe ser $(12)(3456)$ o $(123)(456)$. En el primer caso veemos que $\sigma^2 \in H$ y $\sigma^2 \neq 1$, y fija dos elementos, por lo que aplicamos el caso anterior. En el segundo caso, consideramos $\tau = (234)$. Como

$\sigma^{-1} \in H$ y H es normal, tenemos que $\tau\sigma^{-1}\tau^{-1} \in H$. En particular, $\sigma\tau\sigma^{-1}\tau^{-1} \in H$ este elemento no es 1 y fija a 1, por lo que regresamos al caso original. □

PROPOSICIÓN 3.5. *A_n es simple, para $n \geq 5$.*

DEMOSTRACIÓN. Sea $H \trianglelefteq A_n$ con $H \neq e$ y $\sigma \in H$ con $\sigma \neq 1$. Entonces existe $i = 1, \ldots, n$ tal que $\sigma(i) = j \neq i$. Si α es un triciclo que fija i y mueve a j, entonces:

$$\sigma(\alpha(i)) = \sigma(i) = j$$

y

$$\alpha(\sigma(i)) = \alpha(j) \neq j$$

De aquí $\sigma(\alpha\sigma^{-1}\alpha^{-1}) \neq 1$. Veamos que $\alpha\sigma^{-1}\alpha^{-1} \in H$ por que es H es normal, y que $\sigma(\alpha\sigma^{-1}\alpha^{-1}) \in H$. Por otro lado, como α es un triciclo, tenemos que $\sigma\alpha\sigma^{-1}$ es un triciclo y así $(\sigma\alpha\sigma^{-1})\alpha^{-1}$ es un producto de triciclos. Por lo que $\sigma\alpha\sigma^{-1}\alpha^{-1}$ mueve a lo más 6 símbolos, $i_1, \ldots, i_6$. Si F es el subgrupo de A_n que fija a los demás elementos, tenemos que $\sigma\alpha\sigma^{-1}\alpha^{-1} \in F \cap H$. Por el segundo teorema de isomorfismo $F \cap H \trianglelefteq F$ y es evidente $F \cong A_6$. Como A_6 es simple, y $H \cap F \neq e$, entonces $H \cap F = F$. De nuevo, H tiene que contener un triciclo y por lo tanto $H = A_n$. □

4. Teorema de Cayley

El teorema de Cayley (1878) es uno de los primeros y más emblemáticos teoremas de representación de grupos. De manera informal una representación de un grupo G es un morfismo de grupos con dominio G y codominio otro grupo que tenga una forma "concreta" como lo pueden ser un grupo de permutaciones, un grupo matricial o un grupo de endomorfismos de espacios vectoriales. La idea entonces es que dicho morfismo permite interpretar a los elementos de G como elementos de dichos grupos concretos, aunque es importante notar que el hecho de no pedir que dicho morfismo sea inyectivo hace que dicha representación pueda perder cierta información. Aún con este pequeño problema dichos morfismos son muy útiles y la idea de esta sección es dar los fundamentos para estudiar dichas representaciones en grupos de permutaciones.

Regresando al teorema de Cayley, este afirma que dado grupo G se puede ver como un subgrupo de un grupo de permutaciones. Esto se puede interpretar diciendo que:

¡el estudio de la teoría de grupos se puede llevar al estudio de los subgrupos de los grupos de permutaciones!

Entre otras cosas, con esta interpretación se deduce que el estudio de grupos de permutaciones puede ser muy complejo. Vale la pena mencionar que según Peter Johstone, esta interpretación atrasó un poco el desarrollo de la teoría de grupos en su momento [1], por lo que la forma más sana de entender este resultado es mediante la interpretación de que la idea de grupo queda totalmente determinada por el “álgebra de las sustituciones”.

PROPOSICIÓN 4.1. *(Cayley) Sea G un grupo. Entonces existe X un conjunto y $\rho : G \to S_X$ un monomorfismo. En particular si $|G| = n$, existe un monomorfismo $G \to S_n$.*

DEMOSTRACIÓN. Tome $X = G$ y defina $\rho : G \to S_G$ mediante la regla de correspondencia $\rho(g)(x) = gx$. Nótese que ρ está bien definido pues para cualquier $g \in G$, $\rho(g)^{-1} = \rho(g^{-1})$. Veamos que ρ es un morfismo. Sean $g, h \in G$. Así, para cualquier $x \in G$,

$$\rho(gh)(x) := (gh)x = g(hx) =: \rho(g)(hx) =: \rho(g)(\rho(h)(x)) = \rho(g)\rho(h)(x).$$

Luego, como $x \in G$ fue arbitrario, esto prueba la afirmación.

Para ver que ρ es mono, hay que ver que dicho morfismo es inyectivo, por lo que sea $g \in nuc(\rho)$. Así, $\rho(g) = 1_G$. Entonces al evaluar en el neutro, $g = ge = \rho(g)(e) = e$. Esto prueba la contención no trivial en la igualdad $nuc(\rho) = \{e\}$, de lo que se concluye la prueba de la primera afirmación.

Para concluir nótese que si $|G| = n$, $S_G \cong S_n$, de lo que se obtiene el resultado buscado al considerar la composición:

$$G \xhookrightarrow{\rho} S_G \xrightarrow{\cong} S_n$$

$\square$

Hay varias cosas que decir respecto a la proposición anterior. La primera tiene que ver con el hecho de que dicha representación ρ recibe un nombre especial pues resulta ser que en el caso de G finito, los elementos en su imagen son un tipo muy especial de permutaciones. Para esto se requiere introducir un nuevo concepto.

DEFINICIÓN 4.1. *Sea $\sigma \in S_n$. Decimos que σ es regular si $\sigma = (1)$ ó σ no tiene puntos fijos y es producto de ciclos ajenos de la misma longitud.*

[1] Ver la introducción de su libro "Stone spaces"

EJEMPLO 4.1. *Sea $\sigma \in S_4$ definido mediante $\sigma = (1234)$. Observe que son ejemplos de permutaciones regulares:*

$$\sigma$$
$$\sigma^2 = (13)(24)$$
$$\sigma^3 = (1432)$$
$$\sigma^4 = (1)$$

Nuevamente se insiste en que es muy importante definir el conjunto en el que una permutación es tomada ya que $(13)(24) \in S_4$ es regular, pero $(12)(24) \in S_n$ para $n \geq 5$ no es regular.

La importancia de este ejemplo radica en el hecho de que todas las permutaciones regulares se obtienen de esta forma. Se recomienda ver el ejercicio 192. Para nuestros fines el resultado que nos importa se presenta a continuación.

PROPOSICIÓN 4.2. *Para G finito, el morfismo $\rho : G \to S_n$ del teorema de Cayley satisface que para cualquier $g \in G$, $\rho(g) \in S_n$ es regular.*

DEMOSTRACIÓN. Supóngase que $\rho(g) \neq (1)$ y sea $\rho(g) = \sigma_1 \cdots \sigma_s$ la factorización completa de $\rho(g)$. Lo que se va a ver es que cada σ_i es un ciclo con la misma longitud. Para esto observe que $j \in sop(\sigma_i)$, se tiene que $sop(\sigma_i) = \{\rho(g^k)(j) \mid k \in \mathbb{N}\} = \{\rho(g^k)(j) \mid k \in \{0, ..., o(g)-1\}\}$. Así, $|sop(\sigma_i)| = o(g)$ y como este resultado no depende de $i \in \{1, ..., s\}$ se deduce que $|sop(\sigma_i)| = o(g)$ para cualquier $i \in \{1, ..., s\}$, de lo que se deduce el resultado. $\square$

En virtud a la proposición anterior, al morfismo $\rho : G \to S_G$ del teorema de Cayley se le suele llamar **representación regular izquierda** de G. De hecho se suele denotar $\rho =: L$ por la terminología obvia del inglés. Por otro lado también hay una representación regular derecha que va a ser el morfismo $\rho : G \to S_G$ definido por $\rho(g)(x) = xg^{-1}$. Observe que se multiplica por g^{-1} a la derecha en lugar de g para asegurar que ρ sea morfismo. Se recomienda ver el ejercicio 217.

Vamos a discutir un par de ejemplos concretos donde se estudia el morfismo que define el teorema de Cayley.

EJEMPLO 4.2. *Considere el grupo abeliano $(\mathbb{R}^n, +)$. El teorema de Cayley afirma que hay un monomorfismo $\rho : (\mathbb{R}^n, +) \to S_{\mathbb{R}^n}$. Observe que en este caso $\rho(a)(x) = x + a = T_a(x)$,* *es decir, $\rho(a)$ es la traslación por a en $\mathbb{R}^n$. Así, im$(\rho) = Tr(\mathbb{R}^n)$, por lo que en este caso se deduce que la representación regular izquierda induce el isomorfismo*

$$(\mathbb{R}^n, +) \cong Tr(\mathbb{R}^n).$$

EJEMPLO 4.3. *Considere el morfismo dado por el teorema de Cayley $\rho : \mathbb{Z}_n \to S_{\mathbb{Z}_n}$, donde $n \geq 2$ para no trivializar las cosas. Observe que por definición $\rho([k])([l]) = [k+l]$. Lo que se quiere ver es qué morfismo corresponde a ρ mediante el isomorfismo $S_{\mathbb{Z}_n} \cong S_n$. Para esto considere la biyección estándar $\mathbb{Z}_n \to \{1,...,n\}$ dada por $[k] \longmapsto k+1$.*[2] *Note que trivialmente $\rho([0]) = 1_{\mathbb{Z}_n}$. Por otro lado observe que $\rho([1]) : \mathbb{Z}_n \to \mathbb{Z}_n$ tiene por regla de correspondencia $\rho([1])([k]) = [k+1]$. Al usar la biyección mencionada esto dice que la regla de correspondencia de $\rho[1]$ como elemento de S_n es:*

$$\overline{\rho}([1])(1) = 2,\ \overline{\rho}([1])(2) = 3,\ ...,\ \overline{\rho}([1])(n-1) = n,\ \overline{\rho}([1])(n) = 1.$$

Es decir,

$$\overline{\rho}([1]) = (12\cdots n).$$

Así $\overline{\rho}[1]$ es un n-ciclo, que es un ejemplo de permutación regular en S_n. Además observe que como $\overline{\rho}$ es morfismo, $\overline{\rho}([k]) = (12\cdots n)^k$, luego im$(\overline{\rho}) = \langle(12\cdots n)\rangle$.

Esto dice que el encaje inducido por la representación regular izquierda $\overline{\rho} : \mathbb{Z}_n \to S_n$ es el que muestra el isomorfismo obvio de $\mathbb{Z}_n \cong \langle(12\cdots n)\rangle$.

A pesar de lo interesantes que son los ejemplos anteriores observe que el teorema de Cayley es en realidad un resultado teórico pues la representación no es la más fina. Así, como todo teorema de encaje, una vez que se tiene un resultado de existencia, nos gustaría obtener representaciones más finas. Vamos a darle sentido a esto: el teorema de Cayley afirma que A_5 se encaja como subgrupo de $S_{\frac{5!}{2}} = S_{60}$. Sin embargo observe que A_5 se encaja trivialmente en S_5 pues de hecho, $A_5 \trianglelefteq S_5$, de ahí que el encaje no es óptimo. Desde esta perspectiva vamos a buscar otros teoremas de este estilo, aunque como se verá estos perderán la noción de encaje para dar simplemente morfismos, aunque en la práctica estos pueden modificarse para obtener resultados de encajes. El primero de dichos resultado permite refinar el teorema de Cayley.

[2]Observe que cada biyección de $\mathbb{Z}_n$ con $\{1,...,n\}$ induce un isomorfismo $S_{\mathbb{Z}_n}$ con S_n, por lo que este resultado depende de la biyección que se está eligiendo.

PROPOSICIÓN 4.3. *Si $H \leq G$ tal que $[G:H]=n$, entonces existe un morfismo $\rho : G \to S_n$ con $nuc(\rho) \leq H$.*

DEMOSTRACIÓN. Considere el conjunto de clases laterales derechas, G/H. Ahora defina $\rho : G \to S_{G/H}$ como sigue: $\rho(g)(xH) = gxH$. Observe que como $\rho(g)$ es una función pues si $xH = yH$, entonces $y^{-1}x \in H$, luego $y^{-1}x = y^{-1}g^{-1}gx = (gy)^{-1}gx$, lo que implica que $gxH = gyH$ y prueba la afirmación. Además observe que $\rho(g) \in S_{G/H}$ pues es claro que $\rho(g)^{-1} = \rho(g^{-1})$.

Para concluir hay que ver que ρ es un morfismo, por lo que dados $g,h \in G$; se observa que $\rho(gh)(xH) = (gh)xH = g(hx)H = \rho(g)(hxH) = \rho(g)(\rho(h)(xH)) = \rho(g)\rho(h)(xH)$. Así, $\rho(gh) = \rho(g)\rho(h)$. Para concluir observemos que si $g \in nuc(\rho)$, entonces $\rho(g) = 1_{G/H}$. Esto implica que $gH = \rho(g)(H) = H$ y entonces $g \in H$. Por lo tanto $nuc(\rho) \subseteq H$.

Para concluir observe que como $|G/H| = n$, entonces $S_{G/H} \cong S_n$, de lo que se deduce el resultado. □

Observaciones:

1. Al morfismo ρ del teorema anterior se le conoce como **representación de G en las clases laterales (izquierdas) de H** por obvias razones.
2. Observe que si $H = \{e\}$, entonces el teorema anterior implica el teorema de Cayley para el caso de G un grupo finito.
3. Este resultado mejora el encaje de A_5 pues observe que A_5 tiene un subgrupo isomorfo a A_4. Dado que $[A_5, A_4] = 5$, existe un morfismo $\rho : A_5 \to S_5$ tal que $nuc(\rho) \leq A_4$. Dado que A_5 es simple, esto implica que $nuc(\rho) = \{(1)\}$, luego ρ es inyectivo y esto claramente mejora el encaje a lo que se espera.

Un resultado que se deduce del resultado anterior se presenta a continuación.

COROLARIO 4.1. *Un grupo infinito simple no tiene subgrupos propios de índice finito.*

DEMOSTRACIÓN. Si existe G grupo infinito simple con un subgrupo propio $H \lneq G$ tal que $[G:H] < \aleph_0$, entonces por la proposición anterior existe $\rho : G \to S_n$ morfismo, donde $n = [G:H]$ y $nuc(\rho) \subseteq H$. De la simplicidad y de la última contención se deduce que $nuc(\rho) = \{e\}$, así, ρ es un morfismo inyectivo. Luego, $|G| \leq |S_n| = n!$, lo que es una contradicción. □

Del resultado anterior se deduce módulo el ejercicio 207 que A_∞ no tiene subgrupos propios de índice finito. Esto muestra como los teorema de representación sirven para obtener información matemática de grupos concretos. Se presentarán algunos ejercicios es este estilo al final del capítulo.

Otro resultado que en una parte de su demostración usa nuevamente una representación en clases laterales, y que tiene que ver con la clasificación de los grupos con orden pequeño, se muestra a continuación.

PROPOSICIÓN 4.4. *Si G es un grupo de orden 6, entonces $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ ó $G \cong S_3$.*

DEMOSTRACIÓN. Dado que todo grupo de orden par tiene un elemento se orden 2, sea $g \in G$ uno de dichos elementos. La prueba se va a dividir en dos casos respecto a la conmutatividad de G.

Caso 1: G es abeliano. En tal caso, $\langle g \rangle \trianglelefteq G$. Por otro lado, dado que $|G/\langle g \rangle| = 3$, existe $h \in G$ con $o(h) = 3$. Nótese que nuevamente $\langle h \rangle \trianglelefteq G$ y que además $\langle g \rangle \langle h \rangle = G$. Dado que G es finito, entonces G es producto directo interno de los grupos $\langle g \rangle \cong \mathbb{Z}_2$ y $\langle h \rangle \cong \mathbb{Z}_3$. Luego, se deduce que $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

Caso 2: G no abeliano. Observe que en este caso $\langle g \rangle \ntrianglelefteq G$ pues en caso contrario se puede repetir el argumento del caso anterior y deducir que $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, lo cual es una contradicción pues G no es abeliano. Así, considere la representación en las clases laterales de $\langle g \rangle$, $\rho : G \to S_3$, donde $nuc(\rho) \subseteq \langle g \rangle$. Observe $nuc(\rho) \neq \langle g \rangle$ pues en caso contrario $\langle g \rangle \trianglelefteq G$ lo que es una contradicción, luego, $nuc(\rho) = \{e\}$. Esto dice que ρ es un morfismo inyectivo y dado que el dominio y codominio son finitos y tienen la misma cardinalidad, entonces ρ es un isomorfismo. $\square$

Continuando con lo teoremas de representación en grupos de permutaciones finitos se tiene el siguientes resultado.

PROPOSICIÓN 4.5. *Sea $H \leq G$. Entonces existe un morfismo $\rho : G \to S_X$ con X un conjunto y $nuc(\rho) \subseteq N_G(H)$*

DEMOSTRACIÓN. Sea $X = \{gHg^{-1} \mid g \in G\}$. Luego, se define $\rho : G \to S_X$ cuya regla de correspondencia es $\rho(g)(xHx^{-1}) = gxH(gx)^{-1}$. Observe que $\rho(g) : X \to X$ es una función trivialmente y además es una biyección pues $\rho(g)^{-1} = \rho(g^{-1})$. Además ρ es un morfismo pues para $g, h \in G$,

$$\rho(gh)(xHx^{-1}) = (gh)xH((gh)x)^{-1} = g(hx)H(g(hx))^{-1} = \rho(g)(hxH(hx)^{-1}) = \\ \rho(g)(\rho(h)(xHx^{-1})) = \rho(g)\rho(h)(xHx^{-1}).$$

Esto prueba que ρ es un morfismo. Para concluir, si $g \in nuc(\rho)$, entonces $\rho(g) = 1_X$. Luego $\rho(g)(eHe^{-1}) = eHe^{-1}$, es decir $gHg^{-1} = H$. Esto dice que $g \in N_G(H)$. □

Como es de esperarse el morfismo ρ del resultado anterior se conoce como la **representación de G en los conjugados de H**.

Hasta el momento las representaciones estudiadas se han considerado sobre el grupo de permutaciones, sin embargo, como se dijo en la introducción estas pueden ser en otros grupos. Por ejemplo, se deduce del teorema de Cayley:

PROPOSICIÓN 4.6. *Si G es un grupo con $|G| = n$ y k es cualquier campo, entonces existe un morfismo inyectivo $\rho : G \to GL_n(k)$.*

DEMOSTRACIÓN. Por el teorema de Cayley existe un morfismo inyectivo $\rho' : G \to S_n$. Del ejercicio 108 se deduce que $S_n \cong P(n,k)$, donde $P(n,k) \leq GL_n(k)$. Luego se tiene el morfismo inyectivo buscado de la composición

$$G \xhookrightarrow{\rho'} S_n \xrightarrow{\cong} P(n,k) \xhookrightarrow{\iota} GL_n(k)$$

□

A un morfismo como el del resultado anterior se le conoce como una **representación matricial del grupo G en el campo k** de grado n. De la misma forma a lo que sucedió anteriormente la representación anterior puede no ser muy fina ya que observe que el grupo de Hamilton, $\mathbb{H}$, admite una representación matricial de grado 8:

$$\rho : \mathbb{H} \to GL_8(\mathbb{C})$$

.

Sin embargo, se puede dar otra representación al considerar:

$$\rho : \mathbb{H} \to GL_2(\mathbb{C})$$
$$\rho(i) = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$$
$$\rho(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

la cual es fácil de ver cómo se extiende a $\mathbb{H}$ y de hecho esta representación es inyectiva.

Otro ejemplo se obtiene al observar que para el grupo de Klein el teorema da una representación $\rho : K_4 \to GL_4(k)$, sin embargo en el caso real hay una representación $\rho : K_4 \to GL_2(\mathbb{R})$ que se obtiene al extender la asignación

$$\rho((12)(23)) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\rho((13)(24)) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

El último ejemplo a presentar se obtiene al considerar $\mathbb{Z}_n$. El teorema anterior dice que hay un morfismo $\rho : \mathbb{Z}_n \to GL_n(k)$. Observe que si en k se toma ζ una raíz n-ésima de la unidad, se puede definir $\rho : \mathbb{Z}_n \to GL_1(k) = k^{\times}$ mediante $\rho([k]) = \zeta^k$.

La última proposición mencionada, y los ejemplos considerados después de esta, forman parte de un área de la matemática que se conoce como teoría de representaciones. Vamos a platicar algunas ideas en torno a esta interesante área que ha tenido importantes repercusiones en cuestiones geométricas y topológicas. Discutiremos brevemente el caso más simple: para grupos finitos.

Una **representación (lineal) de un grupo finito** G en un espacio vectorial finito dimensional complejo V, es un morfismo $\rho : G \to GL(V)$, donde $GL(V)$ es el grupo de automorfismos de V. Si ρ es inyectivo, se dice que la representación es **fiel**. Además a la dimensión de V se le conoce como la dimensión de la representación ρ.

Observe que toda representación matricial $\rho : G \to GL_n(k)$ da lugar a una representación lineal al usar el isomorfismo de grupos entre $GL_n(k)$ y $GL(k^n)$. Observe que con esta identificación la dimensión de las representaciones lineales y matriciales coinciden.

La teoría de representaciones es una teoría algebraica que combina ideas de teoría de grupos y álgebra lineal, por lo que hay muchas construcciones relativas a estas: el dual de una representación, el producto tensorial de representaciones, productos exteriores, productos directos, etc. Hay una noción de subrepresentación, morfismos de representaciones, isomorfismo de representaciones, etc. Muchas de las construcciones mencionadas tienen su idea en el álgebra lineal, pero con la teoría presentada se pueden motivar otras construcciones. Por ejemplo, si X es un conjunto finito y $\rho : G \to S_X$ es una representación, esto da lugar a una representación lineal pues si $V = k^{(X)}$, el espacio vectorial libre con base X, entonces se puede definir $\overline{\rho} : G \to GL(V)$ mediante la regla de correspondencia

$$\overline{\rho}(g)\left(\sum_{x\in X} \lambda_x \delta_x\right) = \sum_{x\in X} \lambda_x \delta_{\rho(g)(x)}$$

Esta representación $\overline{\rho}$ se conoce como representación regular pues esta corresponde al producto por la derecha con elementos de G, tal y como se ve del teorema de Cayley. Esto muestra que justamente hay otra forma de inspirar estas ideas que proviene de la teoría de grupos. Por desgracia la teoría de representaciones un toda un área de la matemática por lo que su estudio requiere realizar un curso completo, sin embargo, siempre que sea posible se platicarán ideas en torno a esta y con el desarrollo de la presente sección se espera que el lector haya notado el porque la idea de representar un grupo es interesante para la teoría de grupos misma y en la sección 6 de este capítulo se espera que lector vea porque esta idea se exporta más allá de la teoría de grupos.

5. G-conjuntos

DEFINICIÓN 5.1. *Sea G un grupo. Un G-conjunto X, es un conjunto X y una función* $\lambda\colon G\times X\longrightarrow X$. *Notacionalmente escribiremos* $gx:=\lambda(g,x)=gx$ *para toda* $g\in G$ *y* $x\in X$. *Esta tiene que cumplir:*

- $ex=x$ *para toda* $x\in X$.
- $(gh)x=g(hx)$ *para toda* $g,h\in G$ *y* $x\in X$.

También se dice G actua sobre X, esto porque a λ *se le llama una acción de G sobre X. El grado de un G-conjunto X es* $|X|$.

EJEMPLO 5.1. *Todo conjunto X es un* S_X*-conjunto con acción* $\sigma x:=\sigma(x)$ *para* $\sigma\in S_X$ *y* $x\in X$.

EJEMPLO 5.2. *Sea G un grupo, entonces G es un G-conjunto con la multiplicación.*

EJEMPLO 5.3. *Sea G un grupo, entonces G es G-conjunto con acción* $\lambda(g,a)=a^g$ *donde* $a^g:=gag^{-1}$ *para toda* $a,g\in G$.

EJEMPLO 5.4. *Sea G un grupo y X un G-conjunto. Entonces* $\mathscr{P}(X)$ *es un G-conjunto.*

EJEMPLO 5.5. *Sea G un grupo, entonces* $\mathscr{S}(G)$ *es un G-conjunto con la acción* $H^g:=gHg^{-1}$ *para* $H\leq G$ *y* $g\in G$.

La siguiente proposición nos dice que toda acción induce un morfismo de grupo.

PROPOSICIÓN 5.1. *Sea G un grupo y X un G-conjunto. Definimos* $\rho\colon G\longrightarrow S_X$ *dada por* $\rho(g)(x)=gx$ *para* $g\in G$ *y* $x\in X$. *Entonces* ρ *es un morfismo de grupos.*

DEMOSTRACIÓN. Para ver que esta bien definida, es decir, que $\rho(g)\in S_X$, basta notar que $\rho(g)\rho(g^{-1})=1_X=\rho(g^{-1})\rho(g)$.

Sean $g,h\in G$. Entonces:

$$\rho(gh)(x)=(gh)x=g(hx)=\rho(g)(hx)=\rho(g)(\rho(h)(x))=(\rho(g)\rho(h))(x)$$

para todo $x\in X$. Por lo que $\rho(gh)=\rho(g)\rho(h)$ y por lo tanto ρ es un morfismo de grupos.

□

De hecho, todo morfismo de grupos $\rho : G \longrightarrow S_X$ induce una acción.

PROPOSICIÓN 5.2. *Sea $\rho : G \longrightarrow S_X$ un morfismo de grupos. Entonces la función $\lambda : G \times X \longrightarrow X$ dada por $\lambda(g,x) = \rho(g)(x)$ con $g \in G$ y $x \in X$ es una acción.*

DEMOSTRACIÓN. Sean $e \in G$ y $x \in X$, entonces $ex = \rho(e)(x) = 1_X(x) = x$.

Sean $g, h \in G$ y $x \in X$, entonces:

$$(gh)x = \rho(gh)(x) = \rho(g)(\rho(h)(x)) = g(hx)$$

□

De hecho las dos construcciones son inversas una de la otra. [tarea]

El primer matemático en estudiar problemas de teoría de grupos fue Lagrange al considerar un polinomio en multiples variables $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ y su relación con el polinomio $f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ donde $\sigma \in S_n$. Puntualmente se pregunta cuantos polinomios distintos se pueden formar. Si ponemos $f^\sigma(x_1, \dots, x_n) := f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$, entonces la pregunta es cual es la cardinalidad de $S_n(f) := \{f^\sigma \mid \sigma \in S_n\}$. Si $S_n(f)$ tiene un único elemento decimos que f es una función simétrico.

Todo polinomio $p \in K[x]$ se puede ver como $p(x) = a_n \prod_{i=1}^n (x - r_i)$. Si $p = \sum_{i=0}^n a_i x^i$, entonces cada a_j es una función simétrica de $r_1, \dots, r_n$. El discrimintate de f, d_f, es el el número $(\prod_{i<j}(r_i - r_j))^2$. Si $D(x_1, \dots, x_n) = \prod_{i<j}(x_i - x_j)$. Tenemos que para toda $\sigma \in S_n$, $D^\sigma = sgn(\sigma)D$. De hecho podemos cambiar el punto de vista $S(f) = \{\sigma \in S_n \mid f^\sigma = f\}$. Más aún $Fix(f) \leq S_n$. De hecho f es una función simétrica si y sólo si $S(f) = S_n$.

DEFINICIÓN 5.2. *Si X es un G-conjunto y $x \in X$. Definimos la orbita de x, como $Gx := \{gx \in X \mid g \in G\}$*

PROPOSICIÓN 5.3 (tarea). *Sea X un G-conjunto. La relación $x \sim y$ para $x, y \in X$ si existe $g \in G$ tal que $gx = y$ es una ralación de equivalencia. Más aún, $[x] = Gx$.*

DEFINICIÓN 5.3. *Sea X un G-conjunto y $x \in X$. El estabilizador de x, G_x, son los elementos $g \in G$ tales que $gx = x$.*

PROPOSICIÓN 5.4. *Sea X un G-conjunto y $x \in X$. Entonces $G_x \leq G$.*

Sea $f \in K[x_1, \dots, x_n]$. Lagrange definió $f^* = \prod_{\sigma \in S_n} x - f^\sigma$. Lagrange definió el resolvente $\lambda(f)$ de f como el polinomio resultante de eliminar los factores redudantes de f^*. Entonces Lagrange propuso que $\partial\lambda(f) = n!/|S_n(f)|$. Esta formula es la razón por la que el teorema de Lagrange se llama así. La versión del teorema de Lagrange para grupos finitos muy probablemente fue demostrada por Galois.

EJEMPLO 5.6. *Si consideramos G como G-conjunto con la acción como conjugación. Entonces tenemos que $G_x = C_G(x)$.*

EJEMPLO 5.7. *Si consideramos $\mathscr{S}(G)$ como G-conjunto con la acción como conjugación. Entonces tenemos que $G_H = N_G(H)$ para $H \leq G$.*

De hecho el siguiente teorema generaliza las propsiciones que se vieron al principio del capítulo que eran muy similares.

PROPOSICIÓN 5.5 (Teorema de Orbita-Estabilizador). *Seas X un G-conjunto y $x \in X$. Entonces $|Gx| = [G : G_x]$*

PROPOSICIÓN 5.6. *Recordemos que $[G : G_x] = |G/G_x|$ y G/G_x aquí sólo denota las clases izquierdas, puesto que de primera instancia no sabemos que G_x es un subgrupo normal de G. Por lo que definimos $\phi : Gx \longrightarrow G/G_x$ dada por $\phi(gx) = gG_x$ para $gx \in Gx$. Primero hay que ver que ϕ esta bien definida. Si $gx = hx$ con $g, h \in G$, entonces $h^{-1}gx = x$. Por lo que $h^{-1}g \in G_x$. Por lo tanto $hG_x = gG_x$ y ϕ esta bien definida.*

Sean $gx, hx \in Gx$ con $gG_x = hG_x$. Por lo que $h^{-1}g \in G_x$. Entonces $h^{-1}gx = x$. Despejando $gx = hx$. Por lo tanto ϕ es inyectiva.

Para $g \in G$, tenemos que $\phi(gx) = gG_x$. Por lo tanto ϕ es suprayectiva. Por lo tanto ϕ es una biyección.

COROLARIO 5.1. *Sea X un G-conjunto con G finito. Entonces $|Gx| \mid |G|$ para toda $x \in X$.*

EJEMPLO 5.8. *Sean X un G-conjunto y Y un conjunto. Entonces Y^X el conjunto de funciones de X en Y es un G-conjunto con acción $(g\alpha)(x) := \alpha(gx)$ para toda $\alpha \in Y^X$ y $x \in X$.*

DEFINICIÓN 5.4. *Sea X un G-conjunto y Y un subconjunto de X. Decimos que Y es un G-subconjunto de X, si $gy \in Y$ para todoy $\in Y$ y $g \in G$. Notemos que todo G-conjunto X tiene dos G-subconjuntos $\emptyset$ y X*

EJEMPLO 5.9. *Sea X un G-conjunto y $x \in X$. Entonces Gx es un G-subconjunto de X.*

DEFINICIÓN 5.5. *Sea X un G-conjunto. Decimos que la acción es transitiva si X es simple. Es decir no tiene G-subconjuntos propios.*

DEFINICIÓN 5.6. *Decimos que un G-conjunto X es finito, si G y X es finito.*

PROPOSICIÓN 5.7 (Lema de Burnside). *Si X es un G-conjunto finito y N es el número de orbitas de X. Entonces*

$$N = \frac{1}{|G|} \sum_{g \in G} |F(g)|$$

donde $F(g) = \{x \in X \mid gx = x\}$.

DEMOSTRACIÓN. Notamos que:

$$\sum_{g\in G} |F(g)| = |\{(g,x) \in G \times X \times gx = x\}| = \sum_{x\in X} |G_x|$$

Esto por que:

$$\bigsqcup_{g\in G} F(g) \times \{g\} = |\{(g,x) \in G \times X \times gx = x\}| = \bigsqcup_{x\in X} G_x \times \{x\}$$

El teorema de Orbita-Estabilizador implica que $|Gx| = |G|/|G_x|$. Despejando $|G_x| = |G|/|Gx|$. Sustituyendo:

$$\sum_{x\in X} |G_x| = \sum_{x\in X} \frac{|G|}{|Gx|} = |G| \sum_{x\in X} \frac{1}{|Gx|}$$

Podemos separar a X en sus orbitas. Denotamos al conjunto de orbitas como X/G. Por lo que tenemos que:

$$\sum_{x\in X} \frac{1}{|Gx|} = \sum_{A\in X/G} \sum_{x\in A} \frac{1}{|A|} = \sum_{A\in X/G} 1 = |X/G|.$$

Sustituyendo tenemos la igualdad deseada. □

PROPOSICIÓN 5.8. *Si X es un G-conjunto finito transitivo con $|X| > 1$, entonces existe $g \in G$ con $F(g) = \emptyset$.*

DEMOSTRACIÓN. Por el lema de Burnside y usando que la acción es transitiva tenemos que:

$$1 = \frac{1}{|G|} \sum_{g\in G} |F(g)|$$

Notamos que $|F(e)| = |X| > 1$. Si todos los $F(g)$ son no vacíos, el lado derecho de la igualdad sobrepasa uno. □

6. Geometría

En esta sección se van a tocar diversos temas en torno al carácter geométrico/topológico de la teoría de grupos, con especial énfasis en la idea de acción de grupo. El objetivo de esto es mostrar mediante ejemplos como la idea de grupo es importante fuera del álgebra, por tal razón se van a evitar tecnicismos innecesarios ya que ante todo la sección tiene como fin ir dejando ideas por sobre el desarrollo de estas, ya que esto último requeriría herramientas fuera del álgebra que no pueden ser consideradas como requisitos del curso. La mentalidad adecuada con la que hay que leer esta sección se resume en una frase que Santiago López de Medrano suele repetir constantemente: “Hay que aprender a no entender”.

6.1. Sobre espacios de órbitas. La idea de acción tiene una fuerte interpretación geométrica pues con estas es posible construir espacios. Se va a estudiar esta afirmación mediante ejemplos.

Considérese la acción de $\mathbb{Z}$ en $\mathbb{R}^2$ dada por

$$\mathbb{Z} \times \mathbb{R}^2 \to \mathbb{R}^2$$
$$n \cdot (x,y) := (x+n,y).$$

Lo que se quiere describir es el espacio de órbitas, $\mathbb{R}^2/\mathbb{Z}$. Observe que $(x',y') \in \mathbb{Z}(x,y)$ si y sólo si existe $n \in \mathbb{Z}$ tal que $x' = x+n$ y $y' = y$. Esto dice que la órbita de un elemento está descrita por

$$\mathbb{Z}(x,y) = \{(x+n,y) \mid n \in \mathbb{Z}\}.$$

Al interpretar este resultado se obtiene que sobre el eje x dos puntos que difieran por un entero se consideran el mismo y lo mismo sucede con cualquier recta paralela a dicho eje. Luego observe que para obtener un conjunto de representantes basta con considerar la región $[0,1] \times \mathbb{R}$ donde además se cumple que para cualquier $y \in \mathbb{R}$, $(0,y) \sim (1,y)$. En la geometría esto dice que $\mathbb{R}^2/\mathbb{Z}$ corresponde a un cilindro infinito con una generatriz paralela al eje y (Ver figura 1).

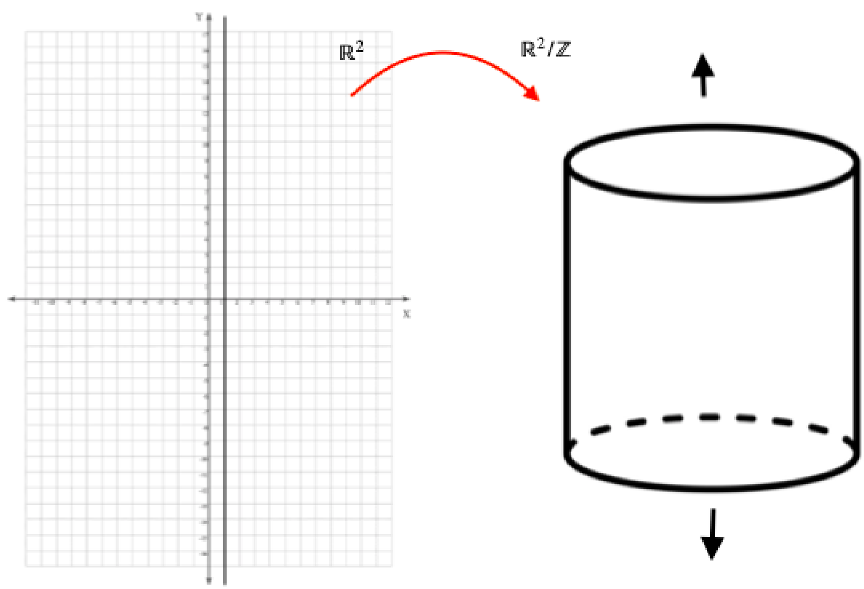


FIGURA 1. Espacio de órbitas $\mathbb{R}^2/\mathbb{Z}$.

Otros ejemplos básicos que son relevantes se mencionan a continuación, los cuales se presentarán con menos detalles.

EJEMPLO 6.1. *Si ahora se considera la acción $\mathbb{R}\times\mathbb{R}^2\to\mathbb{R}^2$ cuya regla de correspondencia es $r\cdot(x,y)=(x+r,y)$, $\mathbb{R}^2/\mathbb{R}$ es el eje y.*

EJEMPLO 6.2. *Para la acción $\mathbb{Z}\times\mathbb{R}\to\mathbb{R}$ cuya regla de correspondencia es $n\cdot x:=x+n$, se tiene que $\mathbb{R}/\mathbb{Z}$ es S^1, la circunferencia unitaria.*

EJEMPLO 6.3. *Respecto a la acción $\mathbb{Z}^2\times\mathbb{R}^2\to\mathbb{R}^2$ dada por $(n,m)\cdot(x,y)=(x+n,y+m)$, se tiene que $\mathbb{R}^2/\mathbb{Z}^2$ es el toro.*

EJEMPLO 6.4. *Al considerar $\mathbb{Z}_2\cong(\{-1,1\},\cdot)$, la acción $\mathbb{Z}_2\times S^n\to S^n$ dada por $\lambda\cdot x:=\lambda x$, se conoce como la acción* ***antípoda*** *y $S^n/\mathbb{Z}_2$ es el plano proyectivo real de dimensión n, $\mathbb{RP}^n$.*

Los ejemplos anteriores muestran uno de los usos comunes de las acciones que es la construcción de espacios como espacios de órbitas. En esta dirección hay teorías muy interesantes donde intervienen nociones de continuidad que llevan a un tratamiento topológico de estos conjuntos (acciones propiamente discontinuas y aplicaciones cubrientes) y al introducir nociones métricas pueden estudiarse ideas geométricas como curvatura, geodésicas, etc. Esta es la razón por la que se usó el término espacio pues dependiendo de lo que se quiera estudiar es la propiedad con la que se quiere equipar al conjunto de órbitas en cuestión.

Un caso particularmente interesante sucede al considerar G-conjuntos cuya acción es transitiva. Sea X uno de tales conjuntos. Si $x\in X$, considere el estabilizador de x, G_x. En general el estabilizador de un elemento no tiene por qué ser un subgrupo normal de grupo en cuestión, por lo que el conjunto de clases laterales G/G_x no tiene por qué ser un grupo. Sin embargo, siempre puede considerarse en dicho conjunto la acción de G. Observe que hay una asignación

$$f: G/G_x\to X$$
$$gG_x\mapsto g\cdot x$$

Esta asignación es una función pues $gG_x=hG_x$ si y sólo si, $h^{-1}g\in G_x$. Esto es equivalente a decir que $(h^{-1}g)\cdot x=x$, lo que es equivalente a decir que $g\cdot x=h\cdot x$. De hecho observe que de este argumento se deduce también que f es una función inyectiva. Además f es G-equivalente, es decir, respeta la acción pues:

$$f(h\cdot(gG_x))=f(hgG_x)=(hg)\cdot x=h\cdot(g\cdot x)=h\cdot f(gGx)$$

Para concluir, el hecho de que X tenga acción transitiva implica que f es suprayectiva, luego, f es un isomorfismo de G conjuntos (ver ejercicio 235).[3] Esto dice que como G-conjuntos X y G/G_x se pueden identificar. Veamos algunos ejemplos concretos de esto.

Algunos ejemplos de G-conjuntos con acción transitiva son:

EJEMPLO 6.5. *Para $n \geq 2$, S^{n-1} es un $O(n)$-conjunto con acción transitiva, donde la acción esta dada por el producto.*

En particular observe que $A \in O(n)_{e_1}$ si y sólo si $Ae_1 = e_1$, es decir, $A_{11} = 1$ y $A_{21} = \ldots = A_{n1} = 0$. Además, como $A^t e_1 = e_1$, entonces $A_{11} = 1$ y $A_{12} = \ldots = A_{1n} = 0$. Observe que esto permite definir un isomorfismo de grupos

$$O(n)_{e_1} \cong O(n-1).$$

Luego, el resultado demostrado implica que como $O(n)$-conjuntos se tiene el isomorfismo,

$$S^{n-1} \cong O(n)/O(n-1).$$

EJEMPLO 6.6. *Sea $H^+ = \{z \in \mathbb{C} \mid Im(z) = 0\}$, el semiplano superior. Hay una acción $SL_2(\mathbb{R}) \times H^+ \to H^+$ definida por*

$$A \cdot z = \frac{A_{11}z + A_{12}}{A_{21}z + A_{22}}.$$

Esta acción es transitiva y en este caso $SL_2(\mathbb{R})_i \cong SO(2)$. Por lo tanto, hay un isomorfismo de $SL_2(\mathbb{R})$-conjuntos,

$$H^+ \cong SL_2(\mathbb{R})/SO(2).$$

EJEMPLO 6.7. *Sea $\mathscr{P}$ el conjunto de matrices de $n \times n$ reales, simétricas y positivas definidas. Existe una acción transitiva.*

$$GL_n(\mathbb{R}) \times \mathscr{P} \to \mathscr{P}$$

$$A \cdot P = APA^t$$

.

En este caso $GL_n(\mathbb{R})_1 \cong O(n)$, por lo que hay un isomorfismo de $GL_n(\mathbb{R})$-conjuntos

[3] De hecho sí la acción es continua f en un isomorfismo de G-espacios

$$\mathscr{P} \cong GL_n(\mathbb{R})/O(n).$$

EJEMPLO 6.8. *Si V es $\mathbb{R}$-espacio vectorial de dimensión finita, una* ***retícula geométrica*** *Λ, es un subgrupo de V de la forma $\Lambda = \sum_{i=1}^{r} \mathbb{Z}v_i$, donde $\{v_1,\dots,v_r\} \subseteq V$ es linealmente independiente. Dicha retícula es completa si $r = n$.*

Sean $\mathscr{L}$ es el conjunto de retículas geométricas completas en $\mathbb{R}^2$ y $\mathscr{L}_1 \subseteq \mathscr{L}$ cuyos elementos satisfacen que los generadores de la retícula forman un paralelogramo de área 1.[4] *Observe que hay una acción transitiva canónica de $GL_2(\mathbb{R})$ en $\mathscr{L}$ y esta induce una acción transitiva de $SL_2(\mathbb{R})$ en $\mathscr{L}_1$. En este caso hay isomorfismos de G-conjuntos:*

$$\mathscr{L} \cong GL_2(\mathbb{R})/GL_2(\mathbb{Z}), \text{ con } G = GL_2(\mathbb{R})$$

$$\mathscr{L}_1 \cong SL_2(\mathbb{R})/SL_2(\mathbb{Z}), \text{ con } G = SL_2(\mathbb{R}).$$

EJEMPLO 6.9. *Para $k \in \{0,\dots,n\}$ sea $Gr_k(n)$ el conjunto de todos los subespacios vectoriales $k-$dimensionales de $\mathbb{R}^n$. Hay una acción $GL_n(\mathbb{R}) \times Gr_k(n) \to Gr_k(n)$, donde para $A \in GL_n(\mathbb{R})$ y $V \in Gr_k(n)$, si V tiene por base $\beta = \{e,\dots,e_k\}$, se define $A \cdot V = \langle Ae_1,\dots Ae_k\rangle$. Esta acción es transitiva. Más aún, este se restringe a una acción $O(n) \times Gr_k(n) \to Gr_k(n)$ la cual es transitiva también pues por el teorema de Gram-Schmidt todo espacio vectorial de dimensión finita tiene una base ortonormal.*

En este caso $Gr_k(\mathbb{R}^n) \cong GL_n(\mathbb{R})/GL_{k,n-k} \cong O(n)/(O(k) \times O(n-k))$, donde $GL_{k,n-k}$ es el subgrupo de $GL_n(\mathbb{R})$ de matrices por bloques de la forma $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$, donde $A \in M_k(\mathbb{R})$, $B \in M_{k\times n-k}(\mathbb{R})$, $C \in M_{n-k}(\mathbb{R})$.

Para concluir esta subsección es importante decir que cuando se pide que X sea un espacio y G un grupo con mayor estructura (de Lie), los G-conjuntos con acción transitiva se conocen como espacios homogéneos. Los ejemplos presentados pertenecen a dicha clase de espacios. Otra clase importante de G-conjuntos con acción transitiva son aquellos que tienen una acción libre. En el contexto de la geometría algebraica estos se conocen como G-**torsores**.

[4] A estas retículas se les conoce como unimodulares.

6.2. Grupos de simetrías. En 1872 Felix Klein da una importante conferencia, que se conoce como el *Programa de Erlangen*, en la que dice la famosa frase:

"La geometría es el estudio de los invariantes bajo un grupo de transformaciones"

La importancia de esta afirmación radica en el hecho de que aparece la noción de grupo, que fue introducida con fines algebraicos por Galois para tratar el conocido problema básico de la teoría de Galois respecto a la solubilidad de ecuaciones por radicales; y según Klein el estudio de la geometría debe realizarse usando este concepto. La idea de esta sección es vislumbrar un poco del sentido a esta frase.

Recordemos que en $\mathbb{R}^n$ hay una forma de medir distancias que canónicamente se hace con la métrica euclidiana. Tomando como motivación el problema de Erlangen debe existir un grupo de simetrías del espacio en sí mismo, es decir, cuyos elementos preservan dicha métrica. Dicho grupo se conoce como el **grupo Euclidiano** de dimensión n o el **grupo de isometrías** de $\mathbb{R}^n$, donde las notaciones comunes para este son $E(n)$ o $Isom(\mathbb{R}^n)$. En nuestro caso tomaremos la segunda de estas.

Según Klein, el estudio de la geometría euclidiana debe corresponder al estudio de dicho grupo. Esto es intuitivamente claro pues es bien sabido que $O(n) \leq Isom(\mathbb{R}^n)$ y en $O(n)$ están las rotaciones y reflexiones que son dos de los tipos de transformaciones más relevantes en la geometría euclidiana.

Más aún, el siguiente resultado es clave en el estudio de isometrías. Una prueba de la existencia se puede consultar en el libro "Álgebra Lineal" de Hugo Rincón, en las páginas 174-177. La unicidad es muy sencilla de demostrar.

PROPOSICIÓN 6.1. *Para toda $T \in Isom(\mathbb{R}^n)$, existen $A \in O(n)$ y $b \in \mathbb{R}^n$ tal que $T(x) = Ax + b$. Más aún, dicha representación es única.*

Observe que este resultado se puede usar para probar que $Isom(\mathbb{R}^n) \leq Aff(\mathbb{R}^n)$, por lo que esto dice que el estudio de la geometría afín contiene al estudio de la geometría Euclidiana, en el sentido de que todos los resultados que sean válidos en geometría afín lo son en geometría euclidiana.

Por otro lado, vale la pena comentar que dicho resultado de factorización se puede escribir de forma algebraica observando que hay una acción canónica $GL_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n$, la cual se restringe a una acción de $O(n)$. Al considerar ρ y ρ' las representaciones en $S_{\mathbb{R}^n}$ inducidas, respectivamente, el resultado anterior dice que hay un isomorfismos de grupos:

$$Isom(\mathbb{R}^n) \cong \mathbb{R}^n \times_{\rho'} O(n) =: \mathbb{R}^n \rtimes O(n).$$

Además por definición

$$Aff(\mathbb{R}^n) \cong \mathbb{R}^n \times_{\rho} GL_n(\mathbb{R}) =: \mathbb{R}^n \rtimes GL_n(\mathbb{R}).$$

Esta observaciones muestran la validez, de una forma muy concreta del enunciado base del problema de Erlangen que es relativo a $\mathbb{R}^n$. Pasemos a un estudio más local estudiando algunas ideas en torno a simetrías:

Sea $\Sigma \subseteq \mathbb{R}^n$ un politopo (envolvente convexa de un conjunto finito de puntos) con centro de gravedad en el origen. Observe que del grupo $Isom(\mathbb{R}^n)$, el subgrupo adecuado para estudiar las simetrías del politopo Σ es mediante el grupo $O(n)$, pues obviamente no va a haber invariancia ante traslaciones. Esto nos sugiere que se puede definir:

$$\mathscr{S}_n(\Sigma) = \{A \in O(n) \mid A \cdot \Sigma = \Sigma\},$$

donde observe que se usa la acción de $O(n) \times \mathbb{R}^n \to \mathbb{R}^n$ y $A \cdot \Sigma = \{Ax \mid x \in \mathbb{R}^n\}$.

Nótese que $\mathscr{S}_n(\Sigma) \leq O(n)$. Más aún, $\mathscr{S}_n(\Sigma)$ mide que tan simétrico es Σ pues no es difícil ver que si $\Sigma \subseteq \mathbb{R}^2$ es un triángulo equilátero, entonces $\mathscr{S}_2(\Sigma) \cong S_3$. En el caso en que Σ sea un triángulo isósceles, $\mathscr{S}_2(\Sigma) \cong \mathbb{Z}_2$. Además si Σ es un triángulo escaleno $\mathscr{S}_2(\Sigma) \cong \{e\}$. Hay un resultado de carácter general que permitirá relacionar $\mathscr{S}_n(\Sigma)$ con el grupo dihédrico, a saber:

PROPOSICIÓN 6.2. *Si Σ es un polígono regular de n vértices, entonces $\mathscr{S}_2(\Sigma)$ es un grupo de orden $2n$ generado por elementos R y S tales que $R^n = 1$, $S^2 = 1$ y $SRS = R^{-1}$.*

DEMOSTRACIÓN. Por regularidad nótese que el origen es el centro de gravedad de Σ y podemos suponer sin pérdida de generalidad que Σ tiene un vértice sobre el eje x. Observe que $\mathscr{S}_2(\Sigma)$ claramente finito pues $\mathscr{S}_2(\Sigma) \hookrightarrow S_n$, al identificar los vértices del polígono con los elementos $\{1,...,n\}$. Además observe que si $V = \{v_1,...,v_n\}$ son los vértices de Σ, entonces $\mathscr{S}_2(\Sigma)$ actúa en dicho conjunto de forma transitiva. Como el estabilizador de una arista tiene orden 2, entonces

$$|\mathscr{S}_2(\Sigma)| = [\mathscr{S}_2(\Sigma) : \mathscr{S}_2(\Sigma)_{v_1}] = 2n.$$

Si R es la rotación por $\frac{2\pi}{n}$ y S la reflexión por el eje x, entonces como $\mathscr{S}_2(\Sigma) \supseteq \langle R,S\rangle$, y dado que $R^n = 1$, $S^2 = 1$ y $SRS = R^{-1}$, se deduce que $\mathscr{S}_2(\Sigma) = \langle S,T\rangle$ pues el subgrupo tiene $2n$ elementos. □

La importancia del resultado anterior es que ahora se tiene un argumento formal para interpretar a D_n como el grupo de simetrías de un polígono regular de n-lados. Además, al grupo $\mathscr{S}_n(\Sigma)$ se le conoce como el **grupo de simetrías** del politopo Σ.

Un segundo ejemplo se da al querer estudiar el grupo de simetrías del cubo. Observe que este tiene que ser subgrupo de $O(3)$. Para esto observe que basta con analizar qué sucede con $SO(3)$ pues al componer un elemento de estos con $-I$, se obtienen todas las reflexiones que dejan invariantes al cubo. Para obtener dicho grupo note que dichas rotaciones mandan diagonales en diagonales y por lo tanto de esta observación no es difícil ver que entonces

$$\mathscr{S}_3(Cubo) \cong S_4 \times \mathbb{Z}_2.$$

Observe que si se quiere determinar el grupo correspondiente para el caso del octaedro, este se deduce del caso calculado para el cubo por dualidad. Los grupos de simetría de todos los sólidos platónicos[5] se muestran a continuación. Vale la pena mencionar que grupo de simetrías del icosaedro se deduce del dodecaedro nuevamente por dualidad (Ver figura 3).

$$\mathscr{S}_3(Tetraedro) = S_4$$

$$\mathscr{S}_3(Cubo) = \mathscr{S}_3(Octaedro) = S_4 \times \mathbb{Z}_2$$

$$\mathscr{S}_3(Dodecaedro) = \mathscr{S}_3(Icosaedro) = A_5 \times \mathbb{Z}_2$$

FIGURA 2.

Esta discusión es un bonito ejemplo de cómo se usa la teoría de grupos en la practica para resolver cuestiones geométricas pues observe que se involucran técnicas de las áreas en cuestión.

Regresando a asuntos generales, si $Pol(n)$ denota el conjunto de politopos en $\mathbb{R}^n$ con centro de gravedad en el origen, la asignación "grupo de simétrias" define una función

$$\mathscr{S}_n : Pol(n) \to Sub(O(n)).$$

Hay preguntas obvias que se pueden hacer respecto a funciones de este estilo, la primera de ellas es si esta es inyectiva. Desde la discusión de los sólidos platónicos se sabe que no. Otra respuesta posible es ver que:

[5]Estos son por definición poliedros convexos cuyas caras son polígonos regulares iguales entre sí, y en la que todos los ángulos sólidos son iguales entre sí. Un teorema famoso muestra que solamente hay cinco sólidos platónicos, estos se muestran en la 2

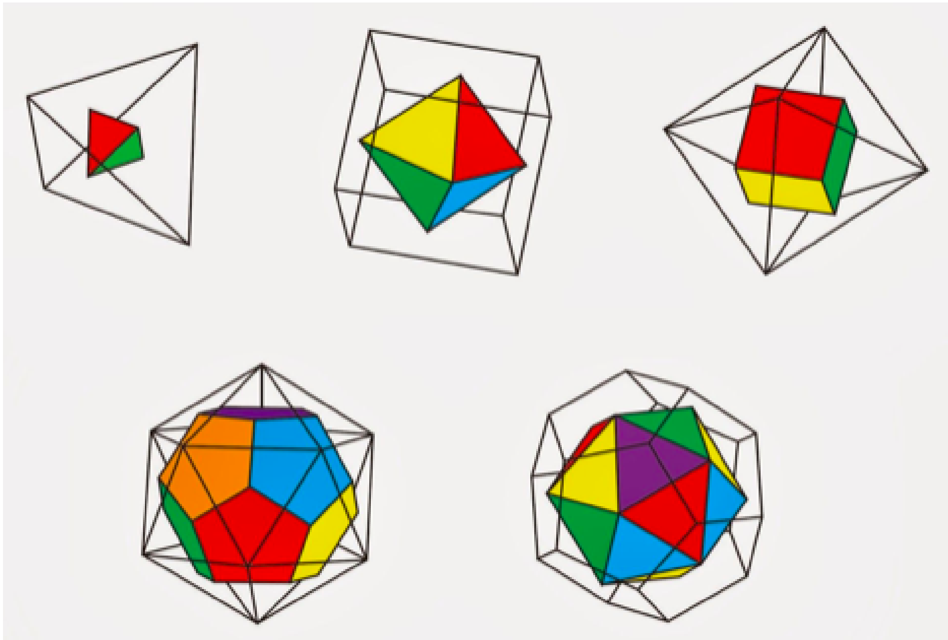


FIGURA 3. Dualidad en los sólidos platónicos

$$\mathscr{S}_2(Rombo) \cong \mathscr{S}_2(Rect\acute{a}ngulo) \cong K_4,$$

donde para ambos casos esto sucede pues los elementos en cada grupo son la reflexión respecto al eje x, la reflexión respecto al eje y y la rotación por $180°$ (ver figura 4). Al observar esto nótese que de la geometría se obtiene una observación obvia de la definición del grupo de Klein, pero que puede parecer no tan importante en un principio, esto es, que al aplicar dos de los elementos no triviales de dicho grupo, esto siempre da el tercer elemento no trivial. Observe que esto nos dice que el grupo de Klein tiene una presentación

$$(x, y \mid x^2, y^2, (xy)^2)$$

De esta presentación se deduce que $D_2 \cong K_4 \cong (\wp(\{a, b\}), \triangle)$.

Regresando a la función $\mathscr{S}_n$, respecto a la suprayectividad es importante observar que dado que para politopos $\mathscr{S}_n(\Sigma)$ es finito, dicha pregunta no tiene sentido en general, aunque permite plantear la cuestión interesante de saber si se pueden clasificar los subgrupos finitos de $O(n)$, y una vez hecho esto se puede refinar la pregunta a buscar suprayectividad respecto a los subgrupos finitos de $O(n)$. Este es un problema complicado en general. Por dar algunos ejemplos puede demostrarse que en el caso de $O(2)$ dichos subgrupos son D_{2n} y $\mathbb{Z}_n$. En el caso de $O(3)$ son D_{2n}, $\mathbb{Z}_n$, A_4, S_4 ó A_5.

Dichos teoremas de clasificación salen del alcance del curso, pero observe que esta última discusión muestra como el querer resolver problemas geométricos muchas veces nos

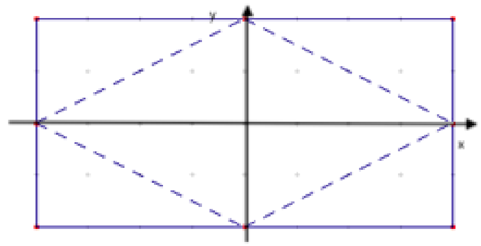


FIGURA 4.

lleva a plantear problemas algebraicos. Esta es una de las cuestiones fundamentales en áreas como la topología algebraica.

Para concluir esta sección es importante decir que esta idea de simetría es fructífera para definir grupos para estudiar espacios. Por ejemplo, el **espacio de Minkowski** es el espacio $\mathbb{R}^4$ con la métrica de Minkowski definida por

$$\eta((t_1,x_1,x_2,x_3),(t_2,y_1,y_2,y_3)) = -t_1t_2 + x_1y_1 + x_2y_2 + x_3y_3$$

Luego, se define el grupo $O(3,1)$, que se conoce como el **grupo de Lorentz**, como el conjunto de matrices $M_4(\mathbb{R})$ que preserva dicha métrica.[6] Observe que esta definición tiene una clara analogía con lo que sucede en el caso de $O(n)$ al recordar el teorema ($k = \mathbb{R}$):

PROPOSICIÓN 6.3. *Sea $T : V \to V$ una transformación lineal suprayectiva con V un k-espacio vectorial con producto interior. Son equivalentes:*

1. *T respeta el producto interior.*
2. *T respeta la norma.*
3. *T preserva conjuntos ortonormales.*
4. *T es invertible y $T^{-1} = T^*$.*

Más aún, si $\dim_k V < \aleph_0$, entonces se agregan a las equivalencias anteriores:

5 *Para cualquier $\beta \subseteq V$ base ortonormal, $[T^*]_\beta^\beta = ([T]_\beta^\beta)^{-1}$*
6 *Para cualquier $\beta \subseteq V$ base ortonormal, las columnas de $[T]_\beta^\beta$ forman una base ortonormal.*
7 *Para cualquier $\beta \subseteq V$ base ortonormal, los renglones de $[T]_\beta^\beta$ forman una base ortonormal.*

[6] El grupo de matrices $M_4(\mathbb{R})$ que preservan la métrica usual de $\mathbb{R}^4$ se conoce como el **grupo simpléctico**, $Sp(1)$.

DEMOSTRACIÓN. Ver el libro "Álgebra Lineal" de Hugo Rincón. Teoremas 79 y 80 en pp 174-177. $\square$

Como información adicional este grupo contiene las rotaciones espaciales de forma obvia y más aún contiene las transformaciones de Lorentz que mezclan el tiempo y las coordenadas espaciales, es decir,

$$\begin{pmatrix} \cosh\phi & -\sinh\phi & 0 & 0 \\ -\sinh\phi & \cosh\phi & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

El grupo $O(3,1)$ es importante en relatividad espacial. Más aún, imitando las ideas de grupo de isometrías de $\mathbb{R}^n$ se puede definir el grupo de todos los (difeomorfismos) del espacio de Minkowski que preservan intervalos espacio-temporales. Este es el importante **grupo de Poincaré** muy usado tanto en relatividad especial como en física de partículas.

Es importante decir que la idea de simetría que encierra el concepto de grupo es muy basta como lo muestran los ejemplos tratados. Hay una definición de grupo que carga con ambas nociones, conocida como grupo de Lie, los cuales reciben este nombre en honor al matemático noruego Sophus Lie. Esta teoría sale de nuestro alcance pues requiere ideas de geometría diferencial y hay que decir que a pesar de esto ya tenemos ejemplos de dichos grupos como lo son $\mathbb{T}$, $Tr(\mathbb{R}^n)$, $O(n)$, $SO(n)$, $U(n)$, $SU(n)$, $GL_n(\mathbb{R})$, $GL_n(\mathbb{C})$, etc.

7. Ejercicios

En lo que sigue G es un grupo y X un conjunto no vacío arbitrario. Además, $n,m \in \mathbb{N}$.

EJERCICIO 151. *Pruebe que si $G/Z(G)$ es cíclico entonces G es abeliano. Discutir lo que sucede con el recíproco de esta afirmación argumentando su respuesta.*

EJERCICIO 152. *Demuestre que para $n \geq 2$, $Z(U(n)) = Z(SU(n)) \cong \mathbb{Z}_n$.*

EJERCICIO 153. *Demuestre que:*

$$Z(D_n) = \begin{cases} \{(1)\}, & \text{Si } n \text{ es impar} \\ \langle r^{\frac{n}{2}} \rangle, & \text{Si } n \text{ es par} \end{cases}$$

Describir $D_n/Z(D_n)$ en cada caso. Además, use esto para demostrar que para todo $n \geq 2$, $D_{2n} \cong D_n \times \mathbb{Z}_2$.

EJERCICIO 154. *Demuestre que un grupo con un elemento de orden finito mayor a uno y dos clases de conjugación tiene orden dos.*

EJERCICIO 155. *Demuestre que si $f: G \to H$ es un epimorfismo entonces $f(Z(G)) \leq Z(H)$. Además pruebe que si f es un isomorfismo entonces $f(Z(G)) = Z(H)$.*

EJERCICIO 156. *Sean $H, K \leq G$ con índice finito. Demuestre que $H \cap K$ tiene índice finito.*

EJERCICIO 157. *Sea $H \leq G$ de índice finito. Demuestre que la intersección de todos los conjugados de H es un subgrupo normal de índice finito.*

EJERCICIO 158. *Sean $H, K \leq G$ con $([G:H],[G:K]) = 1$. Demuestre que $[G:H \cap K] = [G:H][G:K]$.*

EJERCICIO 159. *Sea $g \in G$ con G finito. Demuestre que si g^n tiene m conjugados y g tiene k conjugados, entonces $m|k$.*

EJERCICIO 160. *Sea G un grupo finito y $H \leq G$ tal que $[G:H] = 2$. Demuestre que $|x^H| = |x^G|$ ó que $|x^H| = \frac{1}{2}|x^G|$.*

EJERCICIO 161. *Demuestre que todo subgrupo normal de un grupo G es unión de clases de conjugación una de las cuales es $\{e\}$.*

EJERCICIO 162. *Supóngase que G es un grupo finito y H un subgrupo propio de G. Demuestre que $\bigcup_{g \in G} gHg^{-1}$ es un subconjunto propio de G.*

EJERCICIO 163. *Sea G un grupo y $x \in G$. Demuestre lo siguiente:*

1. *$x \in Z(G)$ si y sólo si $x^G = \{x\}$.*

2. *G es abeliano si y sólo si todas sus clases de conjugación tienen exactamente un elemento.*
3. $C_G(x) \leq G$.

EJERCICIO 164. *Se definen las relaciones $\sim, \sim_a \subseteq Sub(G) \times Sub(G)$ mediante:*

$$H \sim K, \text{ si existe } g \in G \text{ tal que } H = gKg^{-1}.$$

$$H \sim_a K, \text{ si existe } \varphi \in Aut(G) \text{ tal que } H = \varphi(K).$$

1. *Demuestre que ambas relaciones son de equivalencia y que $\sim \subseteq \sim_a$.*
2. *Demuestre que en ambas relaciones cualesquiera dos elementos en la misma clase de equivalencia tienen la misma cardinalidad.*
3. *Dar un ejemplo de un grupo tal que $\sim = \sim_a$.*
4. *Dar un ejemplo de un grupo tal que $\sim \subsetneq \sim_a$.*

EJERCICIO 165. *Sea G un grupo y $H, K \leq G$. Demuestre lo siguiente:*

1. *Si $G = HK$, entonces para todo $g \in G$ existe $k \in K$ tal que $H^g = H^k$.*
2. *Si $H, K \lneq G$ y $G = HK$, entonces H y K no son conjugados.*
3. *Si $H \lneq G$ entonces para todo $g \in G$, $G \neq HH^g$.*

EJERCICIO 166.

1. *Sea G un grupo de orden p^2 con $p \in \mathbb{N}$ primo. Demuestre que todo subgrupo de G es normal. Sugerencia: Usar el ejercicio 165.*
2. *Use el ejercicio 165 y el inciso anterior para demostrar que todo grupo de orden p^2, con $p \in \mathbb{N}$ primo, es abeliano.*

EJERCICIO 167. *Demuestre que $A, B \in GL_n(\mathbb{R})$ son conjugados si y sólo si $L_A = L_B$, donde L_A es la transformación lineal asociada a la matriz A.*

EJERCICIO 168. *Demuestre que* $SL_2(\mathbb{R})$ *y* $SU(1,1)$ *son conjugados como subgrupos de* $GL_2(\mathbb{C})$.[7]

EJERCICIO 169. *Demuestre lo siguiente:*

1. *Para cualesquiera* $a,x \in G$, $C_G(axa^{-1}) = aC_G(x)a^{-1}$.
2. *Si* $H \leq G$ *y* $x \in H$, *entonces* $C_H(x) = C_G(x) \cap H$.

EJERCICIO 170. *Supóngase que* $H \leq G$. *Demuestre lo siguiente:*

1. $H \trianglelefteq N_G(H)$. *Más aún,* $N_G(H)$ *es el máximo subgrupo de* G *donde* H *es normal.*
2. N_G *es un operador clausura.*
3. *Si* $a,b \in G$, *entonces* $H^a = H^b$ *si y sólo si* $b^{-1}a \in N_G(H)$.

EJERCICIO 171. *Demuestre lo siguiente:*

1. *Para cualesquiera* $a,x \in G$, $N_G(axa^{-1}) = aN_G(x)a^{-1}$.
2. *Si* $H \leq G$ *y* $x \in H$, *entonces* $N_H(x) = N_G(x) \cap H$.

DEFINICIÓN 7.1. *Una matriz* $A \in M_n(k)$ *es una matriz permutación generalizada si* A *tiene un único elemento no cero en cada renglón y cada columna. Denote por* $GP(n,k)$ *al conjunto de matrices de permutación generalizadas de* $n \times n$ *con coeficientes en* k.

EJERCICIO 172. *Demuestre lo siguiente:*

1. $GP(n,k) \leq GL_n(k)$. *Más aún, que* $P(n,k) \leq GP(n,k)$.[8]
2. *Si* $T \leq GL_n(k)$ *el subgrupo cuyos elementos son las matrices diagonales, entonces* $N_{GL_n(k)}(T) = GP(n,k)$.
3. $N_{GL_n(k)}(T)/T \cong S_n$.

EJERCICIO 173. *Sea* $H \leq G$ *con* H *finito. Demuestre que* $N_G(H) = \{a \in G \mid aHa^{-1} \leq H\}$. *¿Qué sucede con esta afirmación si* H *no es finito?*

---

[7]Ver ejercicio 104 para recordar la definición de $SU(1,1)$.

[8]Ver ejercicio 108 para recordar la definición de $P(n,k)$.

EJERCICIO 174. *Sea $H \leq G$. Demuestre que $|H^G| = [G : N_G(H)]$. Más aún, que cuando el orden de $|G|$ es finito, el orden de $|H^G|$ divide al orden de G.*

EJERCICIO 175. *Sea G un grupo infinito simple. Demuestre que si $x \in G$ y $H \leq G$ con $x \neq e$ y $H \neq \{e\}$, entonces x^G y H^G son infinitos.*

EJERCICIO 176. *Sea $H \trianglelefteq G$ y $K \leq H$. Supóngase que $Aut(H) = Int(H)$. Demuestre que $G = HN_G(K)$.*

EJERCICIO 177. *Sea $H \leq G$. Demuestre que existe un grupo L y morfismos $f, g : G \to L$ tales que $f|_H \neq g|_H$.*

EJERCICIO 178. *Sea G un grupo finito y $H \leq G$ tal que $|G| \nmid [G : H]!$. Demuestre que H tiene un subgrupo normal no trivial. Sugerencia: Usar una representación de G en las clases laterales de un subgrupo adecuado.*

EJERCICIO 179. *Sea G un grupo finito con H un subgrupo de índice p, donde p es mínimo divisor primo del orden de G. Demuestre que $H \trianglelefteq G$. Sugerencia: Examinar la prueba del teorema de representación de G en las clases laterales de un subgrupo.*

EJERCICIO 180. *Sea G un grupo simple infinito. Demuestre que todo subgrupo propio no trivial tiene una cantidad infinita de conjugados. Sugerencia: Usar el teorema de representación de un grupo en sus conjugados.*

EJERCICIO 181.

1. *Demuestre que para todo $n \in \mathbb{N}^+$ el conjunto $\{\sigma \in S_n \mid \sigma(n) = n\}$ es un subgrupo de S_n y que es isomorfo a S_{n-1}.*
2. *Con la misma notación de antes que se puede decir de $\{\sigma \in A_n \mid \sigma(n) = n\}$*
3. *Decir cuál es el resultado que se deduce según los incisos anteriores respecto a S_n y S_m, así como para A_n y A_m cuando $n \leq m$.*

EJERCICIO 182. *Sean X y Y conjuntos finitos.*

1. *Demuestre que $S_{X\sqcup Y} \cong S_X \times S_Y$.*
2. *Use la propiedad del inciso anterior para probar que $n!m!$ divide a $(n+m)!$ y de esto último que el producto de n enteros consecutivos es divisible por $n!$. Concluya que los coeficientes binomiales son enteros.*

EJERCICIO 183. *Sea $k \in \mathbb{N}$. Demuestre que un k-ciclo es par si y sólo si k es impar.*

EJERCICIO 184. *Sea σ un r-ciclo y $1 < k < r$. Demuestre que σ^k es un r-ciclo si y sólo si $(r,k) = 1$.*

EJERCICIO 185. *Demuestre que para $\sigma \in S_n$ se tiene que σ y σ^{-1} son conjugados.*

EJERCICIO 186. *Demuestre que $S_n = \langle (12), (12\cdots n) \rangle$.*

EJERCICIO 187. *Sean $\sigma, \tau \in S_5$ dados por $\sigma = (123)$ y $\tau = (25314)$*

1. *¿Es cierto que $S_5 = \langle \sigma, \tau \rangle$?*
2. *¿Es cierto que $A_5 = \langle \sigma, \tau \rangle$?*

EJERCICIO 188. *Demuestre que para $n \geq 3$, $Z(S_n) = \{(1)\}$.*

EJERCICIO 189.

1. *Determinar el número de morfismos de $\mathbb{Z}_6$ en S_5 que son inyectivos.*
2. *Determinar el número de morfismos de $\mathbb{Z}_6$ en S_5 con imagen de orden 3.*

DEFINICIÓN 7.2. *Sea $n \in \mathbb{N}^+$. Una partición de n es un conjunto $\{i_1, \ldots, i_r\} \subseteq \mathbb{N}^+$ tal que para todo $k \in \{1, \ldots, r-1\}$, $i_k \leq i_{k+1}$ y $n = \sum_{k=1}^{r} i_k$.*

EJERCICIO 190. *Demuestre que el número de clases de conjugación de S_n es igual al número de particiones de n.*

EJERCICIO 191. *Sea $k \leq n-2$ un número impar. Demuestre que todos los k-ciclos pertenecen a una misma clase de conjugación.*

EJERCICIO 192. *Sea $\sigma \in S_n$. Demuestre que σ es regular si y sólo si existe $\tau \in Sn$ un n-ciclo y $k \in \mathbb{N}$ tal que*

$$\sigma = \tau^k.$$

EJERCICIO 193. *Demuestre que si $\sigma \in S_n$ es un n-ciclo entonces $C_{S_n}(\sigma) = \langle \sigma \rangle$.*

EJERCICIO 194. *Demuestre que S_n no tiene subgrupos de índice t para $2 < t < n$.*

EJERCICIO 195. *Sean $p \in \mathbb{N}$ un primo, $\sigma \in S_p$ una transposición y $\tau \in S_p$ un p-cíclo. Demuestre que $S_p = \langle \sigma, \tau \rangle$.*

EJERCICIO 196. *Sea G un grupo de orden $2^k m$ con m impar. Demuestre que si G tiene un elemento de orden 2^k entonces el conjunto de todos los elementos de orden impar es un subgrupo normal.*

EJERCICIO 197. *Sea $G \leq S_n$ tal que:*

1. *Para todo par de enteros (k,m) existe $\sigma \in G$ tal que $\sigma(k) = m$.*
2. *Existe $\tau \in S_n$ una transposición tal que $\tau \in G$.*
3. *Existe $\alpha \in S_n$ un p-ciclo con $p \in \mathbb{N}$ primo tal que $p > \frac{n}{2}$ y $\alpha \in G$.*

Demuestre que $G = S_n$.

EJERCICIO 198. *Sea $H \leq S_n$. Demuestre que si H tiene una permutación impar entonces el orden de H es par ó la mitad de sus elementos son pares.*

EJERCICIO 199. *Sea $n > 4$ y $N \trianglelefteq S_n$ con $N \neq \{(1)\}$. Demuestre que $A_n \subseteq N$.*

EJERCICIO 200. *Supóngase que $n > 3$ y que $\sigma \in S_n$ que conmuta con todos los elementos del conjunto $\{\tau\sigma\tau^{-1} \mid \tau \in S_n$ es una transposición$\}$. Demuestre que $\sigma^2 = (1)$.*

EJERCICIO 201. *Demuestre que para $n \geq 3$. A_n está generado por los triciclos.*

EJERCICIO 202.

1. *Demuestre que $A_n = \langle\{\sigma^2 \mid \sigma \in S_n\}\rangle$*
2. *Use el inciso anterior para demostrar que $A_n \leq S_n$ es subgrupo característico (Ver definición 6.4).*

EJERCICIO 203. *Demuestre lo siguiente:*

1. *Para $n \geq 3$, $(S_n)' = A_n$*
2. *Para $n \geq 5$, $(A_n)' = A_n$*
3. *$(A_4)' = K_4$, con K_4 el grupo de Klein.*
4. *$(A_3)' = \{(1)\}$*

EJERCICIO 204. *Demuestre lo siguiente:*

1. *$(SL_2(\mathbb{F}_2))' = A_3$*
2. *$(SL_2(\mathbb{F}_3))' = \mathbb{H}$*

Usa estos resultados para decir escribir quién es $(SL_2(k))'$ y $(GL_n(k))'$ para cualquier $n \geq 2$ y k campo. (El ejercicio 70 completa la respuesta con los casos calculados en este ejercicio)

EJERCICIO 205. *Completar los detalles en la siguiente prueba de que A_n simple para $n \geq 5$.*

DEMOSTRACIÓN. (Por contradicción).
Supóngase que A_n tiene un subgrupo normal no trivial, entonces existe un subgrupo normal de A_n máximo, denótese a dicho grupo por M, y nótese que este grupo no es normal en S_n (¿Por qué?). De esto se deduce que existe una transposición $\tau \in S_n$ tal que $\tau M \tau^{-1} \neq M$ ya que ______.

Ahora se define el conjunto $X = \{\sigma \in S_n \mid \sigma M \sigma^{-1} = M\}$, que es un subgrupo de S_n y contiene a A_n (checar ambas afirmaciones). Además se tiene que $X = S_n$ ó que $X = A_n$ pues _____, y entonces se deduce que $X = A_n$ pues _____. Esto prueba que $A_n = N_{S_n}(M)$ y así toda transposición $\tau \in S_n$ satisface que $\tau M \tau^{-1} \neq M$.

Nótese que si $\tau, \sigma \in S_n$ son transposiciones, entonces $\sigma M \sigma^{-1} = \tau M \tau^{-1}$ pues _____. Entonces sea $\tau \in S_n$ una transposición fija y $\sigma_1, ..., \sigma_l \in S_n$ transposiciones, donde $l \in \mathbb{N}$ es par. Así se tiene la igualdad:

$$\sigma_1 ... \sigma_l \tau M \tau^{-1} \sigma_l ... \sigma_1 = \tau M \tau^{-1}, \tag{1}$$

pues _____. De esto se deduce que $\tau M \tau^{-1} \trianglelefteq A_n$ y de esta manera que $M \cap (\tau M \tau^{-1}) \trianglelefteq A_n$, pero dicho subgrupo no es A_n, así que A_n no está contenido en $\tau M \tau^{-1}$ (¿Por qué?).

Ahora si $\sigma \in S_n$ es una transposición, se tiene que

$$\sigma(M \cap (\tau M \tau^{-1}))\sigma^{-1} = \sigma M \sigma^{-1} \cap \sigma \tau M \tau^{-1} \sigma^{-1}. \tag{2}$$

(Argumentar esta igualdad). Y de esta manera se tiene que:

$$\sigma M \sigma^{-1} \cap \sigma \tau M \tau^{-1} \sigma^{1} = \tau M \tau^{-1} \cap M. \tag{3}$$

Como S_n está generado por las transposiciones, se deduce que $M \cap (\tau M \tau^{-1})$ es un subgrupo normal de S_n. Además se tiene que $M \cap (\tau M \tau^{-1}) = \{(1)\}$ pues _____.

Por otro lado, $M \tau M \tau^{-1}$ es un subgrupo normal de A_n y $M \tau M \tau^{-1}$ contiene propiamente a M (checa ambas afirmaciones), entonces por ser M un subgrupo normal no trivial máximo de A_n se deduce que $M(\tau M \tau^{-1}) = A_n$. Así todo elemento de M conmuta con todo elemento de $\tau M \tau^{-1}$ (checar esto).

Lo anterior permite deducir que todo elemento $\mu \in M$ conmuta con $\tau\mu\tau^{-1}$ y esto es válido para toda transposición $\tau \in S_n$. El ejercicio 200 dice que esto obliga a que $\mu^2 = (1)$ y esta conclusión es válida para toda $\mu \in M$.

Entonces M es un 2-grupo y como conjugar preserva órdenes, entonces $\tau M\tau^{-1}$ también es un 2-grupo. Además, como los elementos de M y de $\tau M\tau^{-1}$ conmutan (¿Por qué?), entonces A_n es un 2-grupo. Entonces todo elemento de A_n tiene orden 2 y esto es una contradicción pues _____ . $\square$

EJERCICIO 206. *Demuestre que si $n > 5$ entonces no existe una sucesión $H_0, \ldots, H_n$ de subgrupos de A_n tales que:*

1. *$H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n$.*
2. *$H_0 = \{(1)\}$, $H_n = A_n$ y para todo $k \in \{0, \ldots, n-1\}$, $H_k \neq H_{k+1}$.*
3. *Para todo $k \in \{0, \ldots, n-1\}$, H_{k+1}/H_k es abeliano.*

EJERCICIO 207. *Sea A_∞ el subgrupo de $S_\mathbb{N}$ generado por los triciclos.*[9] *Demuestre que A_∞ es simple.*

EJERCICIO 208. *Demuestre que para $n \geq 5$ los únicos subgrupos normales de S_n son $\{(1)\}$, A_n y S_n.*

EJERCICIO 209. *Demuestre que si $n \geq 3$ entonces A_n es el único subgrupo de S_n de orden $\frac{n!}{2}$.*

EJERCICIO 210. *Demuestre que K_4 es el único subgrupo normal propio no trivial de A_4.*

EJERCICIO 211. *Demuestre que A_5 no tiene un subgrupo de orden* 30*.*

[9] En este contexto un triciclo $\sigma \in S_\mathbb{N}$ es una función tal que $|sop(\sigma)| = 3$.

EJERCICIO 212. *Demuestre que A_4 es el único subgrupo normal propio de S_4.*

EJERCICIO 213.

1. *Demuestre que S_5 no tiene un subgrupo de orden 30.*
2. *Demuestre que S_5 no tiene un subgrupo de orden 40.*

EJERCICIO 214. *Demuestre que todo grupo finito puede ser incluido en un grupo el cual es generado por a lo más 2 elementos.*

EJERCICIO 215. *Sea G un subgrupo de S_n tal que contiene una permutación impar. Demuestre que $G\cap A_n$ tiene índice dos en G.*

EJERCICIO 216. *Demuestre que si G es un grupo finito simple y H es un subgrupo de G, entonces existe un morfismo inyectivo de grupos de G en el grupo simétrico S_H.*

EJERCICIO 217. *Dado $(G,\cdot)$ un grupo, se define el grupo opuesto de G, el que se denota por G^{op}, como sigue: como conjunto $G^{op} := G$. La operación*

$$*: G^{op}\times G^{op}\to G^{op}$$

$$g*h := hg$$

Demuestre lo siguiente:

1. *$(G^{op},*)$ es en efecto un grupo.*
2. *G es abeliano si y sólo si $(G,\cdot) = (G^{op},*)$.*
3. *Existe un morfismo de grupos $\rho : G^{op}\to S_G$.*

EJERCICIO 218. *Demuestre que $\mathbb{R}^2$ tiene estructura de $\mathbb{Z}$-conjunto con la función $\cdot : \mathbb{Z}\times\mathbb{R}^2\to\mathbb{R}^2$ definida por*

$$n\cdot(x,y) = (x+n,(-1)^n y).$$

¿Quién es $\mathbb{R}^2/\mathbb{Z}$?.

DEFINICIÓN 7.3. *Un conjunto X tiene una acción de un grupo G por la derecha si existe una función $\mu : X \times G \to X$, donde $xg := \mu(x,g)$, tal que:*

1. *Para cualquier $x \in X$, $xe = x$.*
2. *Para cualesquiera $x \in X$ y $g,h \in G$, $x(gh) = (xg)h$*

EJERCICIO 219. *Sea X un conjunto no vacío.*

1. *Demuestre que hay una correspondencia biyectiva entre morfismos de grupos $\rho : G \to S_X$ y acciones de grupo $G \times X \to X$.*
2. *Describir las acciones que corresponden segúns la biyección anterior a las representaciones regulares izquierdas, en clases laterales de un subgrupo y en clases de conjugación de un subgrupo.*
3. *Demuestre que hay una correspondencia biyectiva entre G-conjuntos y conjuntos con acciones derechas de G.*

DEFINICIÓN 7.4. *Para un G-conjunto X se define el conjunto de puntos fijos, el que se denota por $Fix_G(X)$, como $\{x \in X \mid gx = x\}$.*

EJERCICIO 220. *Para G y H grupos, defina $M_*(G,H)$ como el conjunto de funciones de G en H que preservan el neutro.*

1. *Defina la función $\cdot : G \times M_*(G,H) \to M_*(G,H)$ mediante $(g \cdot f)(x) := f(xg)f(g)^{-1}$. Demuestre que esta función está bien definida y es una acción de G en $M_*(G,H)$*
2. *Describir $Fix_G(M_*(G,H))$*

EJERCICIO 221. *Para G y H grupos, describir las acciones de $G \times H$ en un conjunto X en términos de acciones de G y H en dicho conjunto.*

EJERCICIO 222. *Sea X un $(G \times H)$-conjunto. Demuestre lo siguiente:*

1. *Existe un acción de H en X y además que G actúa en el conjunto de puntos fijos de dicha acción, $Fix_H(X)$.*
2. *Existe una acción de G en X y además H actúa en el conjunto de órbitas X/G.*

3. *Hay una biyección $Fix_H(X)/G$ y $Fix_H(X/G)$.*

EJERCICIO 223. *Sea X un G-conjunto. Demuestre que la relación $x \sim y$, si existe $g \in G$ tal que $gx = y$ es de equivalencia. Más aún, $[x] = Gx$.*

EJERCICIO 224. *Sea G considerado como G-conjunto con la multiplicación por la derecha. Demuestre que G tiene únicamente una órbita.*

EJERCICIO 225. *Sean X un G-conjunto, $x, y \in X$ y $g \in G$. Demuestre que si $gx = y$, entonces $G_y = gG_xg^{-1}$. Concluya que $|G_x| = |G_y|$.*

EJERCICIO 226. *Sea X un G conjunto y $G \to S_X$ su morfismo de grupos asociado. Demuestre que $\bigcap_{x \in X} G_x = nuc(G \to S_X)$.*

DEFINICIÓN 7.5. *Sea X un G-conjunto y $\cdot : G \times X \to X$ la acción de G en X. Se recuerda que dicha acción es:*

1. *transitiva si X no tiene G-subconjuntos triviales. En este caso se dice también que el G-conjunto es transitivo.*
2. *libre de puntos fijos si para todo $g \in G \setminus \{e\}$ y $x \in X$, $g \cdot x \neq x$.*

EJERCICIO 227. *Demuestre lo siguiente:*

1. *Una acción es libre de puntos fijos si y sólo si para todo $x \in X$, $G_x = \{e\}$.*
2. *Para un G-conjunto X son equivalentes:*
   - *La acción es transitiva.*
   - *Para cualesquiera $x, y \in X$ existe $g \in G$ tal que $y = g \cdot x$.*
   - *Para todo $x \in X$, $Gx = X$.*

EJERCICIO 228. *Sea X un G-conjunto. Demuestre lo siguiente:*

1. *Para todo $x \in X$, Gx es un G-conjunto transitivo.*

2. *Si G es finito y la acción es libre de puntos fijos, entonces para cualquier $x \in X$, $|Gx| = |G|$.*

EJERCICIO 229.

1. *Sea $G \leq S_X$ con X un conjunto tal que $|X| = n$. Demuestre que si G es abeliano y actúa transitivamente en X, entonces la acción es libre de puntos fijos. Deducir de esto que $[G : \{e\}] \leq n$.*
2. *Para toda $n \in \mathbb{N}^+$ exhibir un subgrupo de S_{3n} con orden 3^n.*
3. *Demuestre que si $G \leq S_n$ abeliano, entonces $|G| \leq 3^{\frac{n}{3}}$.*

EJERCICIO 230. *Demuestre que si $H \leq G$, entonces G actúa transitivamente en el conjunto de clases izquierdas de H y en el conjunto de conjugados de H.*

EJERCICIO 231. *Sea X un G-conjunto y $K = \bigcap_{x \in X} G_x$. Demuestre lo siguiente:*

1. *$K \trianglelefteq G$.*
2. *X es un G/K-conjunto.*
3. *Si X es un G-conjunto transitivo, entonces X es un G/K-conjunto transitivo.*

EJERCICIO 232. *Sea X un G-conjunto finito y $H \leq G$. Demuestre que si H actúa transitivamente en X entonces $HG_x = G$ para toda $x \in X$.*

DEFINICIÓN 7.6. *Para $n \in \mathbb{N}$ se define $S^n = \{x \in \mathbb{R}^{n+1} \mid \|x\| = 1\}$, donde $\|\_\|$ es la norma usual en $\mathbb{R}^{n+1}$.*

EJERCICIO 233. *Se define una función $\cdot : SO(n) \times S^{n-1} \to S^{n-1}$ mediante $A \cdot v = Av$.*

1. *Demuestre que la función anterior está bien definida y que hace de S^{n-1} un $SO(n)$-conjunto.*
2. *Demuestre que la acción definida es transitiva.*

EJERCICIO 234. *Sean $p \in \mathbb{N}$ un primo y el conjunto $X = \{(g_1, ..., g_p) \in G^p \mid g_1 \cdot ... \cdot g_p = e\}$. Se define una función $\cdot : \mathbb{Z}_p \times X \to X$ mediante:*

$$[0] \cdot (g_1, ..., g_p) = (g_1, ..., g_p),$$

y si $k \in \{1, ..., p-1\}$

$$[k] \cdot (g_1, ..., g_p) = (g_{p-(k-1)}, g_{p-(k-2)}, ..., g_1, ..., g_{p-k})$$

1. *Demuestre que la función anterior está bien definida.*
2. *Demuestre que la función anterior hace de X un G-conjunto.*

DEFINICIÓN 7.7. *Sean X y Y G-conjuntos. Una función $f : X \to Y$ es un morfismo de G-conjuntos si para cualesquiera $g \in G$ y $x \in X$, $f(g \cdot x) = g \cdot f(x)$.*

EJERCICIO 235. *Sea $f : X \to Y$ un morfismo de G-conjuntos. Demuestre que son equivalentes:*

1. *Existe $g : Y \to X$ morfismo de G-conjuntos tal que $f \circ g = 1_Y$ y $g \circ f = 1_X$*
2. *f es biyectiva.*

A un morfismo que cumple una de, y por lo tanto ambas de las condiciones en el resultado anterior se le conoce como isomorfismo de G-conjuntos.

EJERCICIO 236.

1. *Demuestre que todo grupo abeliano es un $\mathbb{Z}$-conjunto.*
2. *Sea $f : G \to H$ un morfismo de grupos con G y H grupos abelianos. Demuestre que f es un morfismo de $\mathbb{Z}$-conjuntos. ¿Cuándo es dicho morfismo un isomorfismo de $\mathbb{Z}$-conjuntos?*

EJERCICIO 237. *Sean $\alpha : G \to H$ y $\beta : G \to K$ morfismos de grupos. Considérese a H y K como G-conjuntos con la acción inducida por dichos morfismos y sea $f : H \to K$ un morfismo de grupos.*

1. *¿Qué condición debe satisfacer f para ser morfismo de G-conjuntos?*
2. *Probar que dicha condición caracteriza en este caso a los morfismos de G-conjuntos.*

EJERCICIO 238. *Sea $x \in X$ con X un G-conjunto. Demuestre que Gx es el $\subseteq$-mínimo G-subconjunto que tiene como elemento a x.*

DEFINICIÓN 7.8. *Sea X un G-conjunto y $\mathscr{P}$ una partición de X. Se dice que la partición $\mathscr{P}$ es estable por G si para todo $A \in \mathscr{P}$ se tiene que $gA = \{ga \mid a \in A\} \in \mathscr{P}$.*

EJERCICIO 239.

1. *Sea $X = \{1,2,3,4\}$ y $G = \langle (1234) \rangle$. Demuestre que la partición $\{\{1,3\},\{2,4\}\}$ es estable por G.*
2. *Sea $X = \{1,2,3,4\}$. Demuestre la partición $\{\{1,3\},\{2,4\}\}$ es estable por D_4.*
3. *Sea X un G-conjunto. Demuestre que las particiones $\{X\}$ y $\{\{x\}\}_{x \in X}$ son estables por G. A estas particiones se les conoce como particiones triviales.*
4. *Sea X un G-conjunto. Demuestre que $S \subseteq X$ es G-subconjunto si y sólo si S es unión de órbitas. Use esta propiedad para demostrar que si $H \leq G$, entonces $H \trianglelefteq G$ si y sólo si H es unión de clases de conjugación.*

DEFINICIÓN 7.9. *Sea X un G-conjunto. Se dice que G actúa primitivamente en X si las únicas particiones de X que son estables bajo G son las triviales.*

EJERCICIO 240.

1. *Demuestre que si G actúa en un conjunto X de manera primitiva entonces la acción es transitiva o para todo $x \in X$ y $g \in G$, $g \cdot x = x$.*
2. *Sea X un G-conjunto transitivo con al menos dos elementos y G finito. Demuestre que G no actúa de manera primitiva en X si y sólo si existe $A \subsetneq X$ con $|A| \geq 2$ tal que para todo $g \in G$, $gA = A$ ó $gA \cap A = \emptyset$.*[10]

[10] Un conjunto A que satisface esta condición se le llama un bloque.

3. *Sea X un G-conjunto transitivo con al menos dos elementos, G finito y $A \subsetneq X$ un bloque. Demuestre que para todo $x \in A$, $G_x \subsetneq G_A \subsetneq G$.*
4. *Sea X un G-conjunto transitivo con al menos dos elementos y G finito. Demuestre que G actúa primitivamente en X si y sólo si existe $x \in X$ tal que G_x es un subgrupo máximo de G.*

Capítulo 4

Teorema de Cauchy y los Teoremas de Sylow

"No se pueden aplicar las matemáticas mientras las palabras oscurezcan la realidad.."

Hermann Weyl.

La idea de estes capítulo es presentar los teoremas de Cauchy y Sylow. Si consideramos un grupo finito y los factores primos del orden del grupo, sería de esperarse que a menor número de factores más sencillo sea describir un grupo con tal orden.

1. Teorema de Cauchy

El caso más sencillo es cuando sólo se tiene un factor primo.

PROPOSICIÓN 1.1. *Sean G un grupo abeliano finito y p un primo. Si $p \mid |G|$, entonces G tiene un elemento de orden p*

DEMOSTRACIÓN. Si el orden de G es pm con $m \geq 1$. Procedemos a hacer inducción sobre m. El caso base $m = 1$, es trivial. Por que dado el caso se tendría que el orden de G es p y por lo tanto cíclio. Más aún, todo elemento no neutro tiene orden p.

Para el paso inductivo, sea $x \in G$ con orden $k > 1$. Si $p \mid k$, entonces $x^{\frac{k}{p}}$ tiene orden p. Por lo que supondremos que p no divide a k. Como G es abeliano entonces $H := \langle x \rangle$ es un subgrupo normal de G. Por lo que podemos considerar la proyección canónica $\pi\colon G \longrightarrow G/H$. Notamos que el orden de G/H es pm/k. Como p no divide a k, entonces m/k es un entero que cumple $m/k < m$. Aplicando la hipotesis de inducción a G/H cuyo orden es $p(m/k)$, tenemos que existe $yH \in G/H$ de orden p. Pero la proyección es suprayectiva, por lo que existe $z \in G$ tal que $\pi(z) = yH$. De aquí el orden de z es un múltiplo p y esto nos hace regresar al caso analogo que cuando $p \mid k$. $\square$

PROPOSICIÓN 1.2 (Teorema de Cauchy, Cauchy 1845). *Sean G un grupo finito y p un primo. Si $p \mid |G|$, entonces G tiene un elemento de orden p*

DEMOSTRACIÓN. Recordemos que para $x \in G$, tenemos que $|x^G| = [G : C_G(x)]$. Notemo que si x no esta en el centro de G, $x \notin Z(G)$, entonces $|x^G| > 1$. Por lo que se sigue que $|C_G(x)| < |G|$.

Si $p \mid |C_G(x)|$, entonces podemos proceder por inducción fuerte sobre $|G|$. Pensemoslo así. Si G es abeliano, entonces existe un elemento de orden p por la proposición pasada. En el caso de que no sea abeliano, debe de existir un elemento que no este en el centro. Por lo observado anterirormente $|C_G(x)| < |G|$. Si $p \mid C_G(x)$ para algún entonces por hipotesis de inducción tenemos un elemento de orde p en $C_G(x)$ y por lo tanto en G.

Sólo resta ver que pasa si $p \nmid C_G(x)$ para todo elemento que no este en el centro. Ahora como $|G| = [G : C_G(x)]|C_G(x)|$, entonces $p \mid [G : C_G(x)]$ por lema de euclides para no elemento que no este en el centro.

Por otro lado consideremos que $G = \bigsqcup_{x \in R_G} x^G$ donde R_G es una familia de representates de las clases de equivalencia y R_G^* es una familia de representates de las clases de equivalencia de elementos no centrales. Entonces:

$$|G| = \sum_{x \in R_G} |x^G| = |Z(G)| + \sum_{x \in R_G^*} [G : C_G(x)]$$

Como $|G|$ y $[G : C_G(x)]$ son divisibles por p. Entonces $p \mid |Z(G)|$. Recordando que $Z(G)$ es un grupo abeliano, entonces por la proposición anterior $Z(G)$ tiene un elemento de orden p y así G tiene un elemento de orden p. □

J. H. MCKAY. Definimos:

$$X := \{(g_1, \dots, g_p) \in G^p \mid g_1 \dots g_p = e\}$$

Evidentemente la elección de los primeros $p-1$ elementos determina el p-ésimo elemento, obligando a que el último sea el inverso del producto de los anteriores. Por lo que $|X| = |G|^{p-1}$. Notamos que X es un $\mathbb{Z}_p$-conjunto donde la acción $n(g_1, \dots, g_p) = (g_n, \dots, g_p, g_1, \dots, g_{n-1})$. Notemos que la acción esta bien definida asociando correctamente tenemos que si $ab = e$ entonces $ba = e$.

Ahora cada orbita tiene cardinalidad un divisor de p, por lo que tiene un elemento o p. Pero un elemento $(g_1, \dots, g_p)$ cuya orbita tiene un único elemento es por que todas sus entradas son iguales, es decir, $g = g_i$ para toda $i = 1, \dots, p$. Notamos que esto implica que $g^p = e$. Observamos que al menos hay un elemento con esta condición $(e, \dots, e)$. Por otro lado usando la partición de la acción y suponiendo que solo este elemento cumple el tener una rbita de un elemento, tenemos que:

$$|G|^{p-1} = |X| = 1 + kp$$

para algún natural k. Pero el orden de G es divisible por p, por lo que tendríamos que $p \mid 1+kp$. Lo cual es es una contradicción. Por lo cual debe existir otro elemento con orbita de un sólo elemento y por lo tanto de orden p $\square$

Rotman menciona que A. Mann le observo sobre esta demostración que en el caso de que el orden de G no sea divisible por p, esta sería un demostración del pequeño teorema de Fermat.

DEFINICIÓN 1.1. *Sean G un grupo y p un primo. Entonces G es un p-grupo, si todo sus elementos tienen orden una potencia de p.*

PROPOSICIÓN 1.3. *Sean G un grupo finito y p un primo. Entonces G es un p-grupo si y sólo si el orden de G es una potencia de p.*

DEMOSTRACIÓN. $\Rightarrow$) Si el orden no fuera una potencia de p, entonces existiera otro primo q que divide al orden del grupo. Por el teorema de Cauchy existe un elemento con ese orden contradiciendo que es un p-grupo.

$\Leftarrow$) El teorema de Lagrange $\square$

PROPOSICIÓN 1.4. *Sean G un grupo finito y p un primo. Si G es un p-grupo, entonces $Z(G) \neq e$.*

DEMOSTRACIÓN. Consideremos la ecuación de clase:

$$|G| = |Z(G)| + \sum_{x \in R_G^*} [G : C_G(x)]$$

Si $x \notin Z(G)$, entonces $C_G(x) < G$. Como $[G : C_G(x)]$ es un divisor del orden G, entonces $[G : C_G(x)]$ es una potencia de p. De la ecuación de clase tenemos que p divide al orden $Z(G)$. Por lo tanto $Z(G) \neq e$. $\square$

PROPOSICIÓN 1.5. *Sean G un grupo finito y p un primo. Si G tiene orden p^2, entonces G es abeliano.*

DEMOSTRACIÓN. Si G no es abeliano, entonces $Z(G) < G$. Por la proposición anterior concluimos $|Z(G)| = p$. Podemos considerar el grupo $G/Z(G)$ que tiene orden p por lo tanto es cíclico. Esto es una contradicción por que esto implica que G es abeliano. □

PROPOSICIÓN 1.6. *Sean G un grupo finito y p un primo. Si G es un p-grupo y $H < G$, entonces $H < N_G(H)$*

DEMOSTRACIÓN. Si H es normal en G, entonces $H < G = N_G(H)$. Supondremos que H no es normal, por lo cual tiene más de un congugado y si denotamos por X a su orbita bajo la acción de conjugación tenemos que $|X| > 1$. Más aún $|X| = [G : N_G(H)] = p^k$ con $k \geq 1$. Como G actúa por conjugación en X, también tenemos que lo hace H. Pero bajo esta acción la orbita de H tiene un sólo elemento. Como X tiene cardinalidad una potencia de p, entonces debe de existir almenos $p-1$ G-conjugados de H con orbita única bajo H. Con esto existe al menos uno, el caso $p = 2$ es el menor. Esto es, que existe $g \in G$ tal que $H^g \neq H$, y $(H^g)^a = H^g$ para todo $a \in H$. Por lo que $H^{g^{-1}ag} = H$ y $g^{-1}ag \in N_G(H)$ para toda $a \in H$. Recordando que $gHg^{-1} \neq H$, entonces existe $a \in H$ tal que $gag^{-1} \notin H$. Por lo tanto $H < N_G(H)$.

□

PROPOSICIÓN 1.7. *Sean G un grupo finito y p un primo. Si G es un p-grupo y $H \leq G$ es máximo, entonces $H \trianglelefteq G$ y $[G : H] = p$.*

DEMOSTRACIÓN. Como H es máximo, por la proposición anterior $N_G(H) = G$. Por lo tanto $H \trianglelefteq G$. Ahora sabemos que el índice de todo subgrupo máximo normal es un primo, en este caso por Lagrange debe ser p. □

PROPOSICIÓN 1.8. *Sean G un p-grupo finito connp un primo. Si k es el número de subgrupos de orden p, entonces $k \equiv 1 \mod p$*

DEMOSTRACIÓN. Empezamos viendo que los elementos de $Z(G)$ de orden p junto con e forman un subgrupo que tiene orden una potencia de p. Si llamamos a este grupo H, entonces tenemos que $|H| - 1 \equiv -1 mod p$. Si x es un elemento no central de orden p, entonces x^G tiene cardinalidad una potencia de p y sus elementos tienen orden p. De aquí se sigue que el número de elementos de orden p son congruentes con -1 módulo p. Realmente los no centrales con congruentes con 0 y los centrales con -1. Por lo que podemos decir que existen $mp-1$ elementos de orden p. Como la intersección de dos subgrupos distintos de orden p es trivial, entonces el número de elementos de orden p es $k(p-1)$. De aquí $k(p-1) = mp-1$ y $p \mid k(p-1)-(-1)$. Entonces $k(-1) \equiv -1 mod p$. Por lo tanto $k \equiv 1 \mod p$. □

PROPOSICIÓN 1.9. *Sean G un p-grupo finito connp un primo. Si k_s es el número de subgrupos de orden p^s, entonces $k_s \equiv 1 \mod p$*

DEMOSTRACIÓN. Sea H un subgrupo de orden p^s y $K_1,\ldots,K_a$ los subgrupos de orden p^{s+1} que lo contienen. Afirmamos que $a \equiv 1 mod p$. Todo subgrupo que normaliza a H esta contenido en $N_G(H)$. En particular por dos proposiciones anteriores H es normal en K_i, por lo que $K_i \leq N_G(H)$. Por el teorema de la correspondencia biyectiva y la proposición anterior se tiene que $a \equiv 1 mod p$.

Ahora sea K un subgrupo de orden p^{s+1}, y sean $H_1,\ldots,H_b$ sus subgrupos de orden p^s. De nuevo por dos proposiciones anteriores $H_i \trianglelefteq K$. Por otro lado $H_1H_2 = K$. Por la formula del producto tenemos que $|H_1 \cap H_2| = p^{s-1}$ y por lo que $[K : H_1 \cap H_2] = p^2$. Usando el segundo teorema de isomorfismo podemos considerar el grupo $K/H_1 \cap H_2$ que es abeliano por tener orden p^2. Como es generado por dos subgrupos $H_1/H_1 \cap H_2$ y $H_2/H_1 \cap H_2$ entonces no es cíclico. Más aún , $K/H_1 \cap H_2 \cong \mathbb{Z}_p^2$. Por lo que tiene p^2-1 elementos de orden p. De hecho tiene $p+1 = \frac{p^2-1}{p-1}$ subgrupos de orden p. Por el teorema de la correspondencia biyectiva hay $p+1$ subgrupos de K de orden p^s que contienen a $H_1 \cap H_2$. Supongamos que existe H_j tal que $H_1 \cap H_2$ no esta contenido en H_j. Entonces para $E_j = H_1 \cap H_J$ hay una nueva lista de $p+1$ subgrupos de orden p^s que contienen a E_j, uno de ellos H_1. De hecho $H_1 = E_j(H_1 \cap H_2)$ es el único subgrupo de ambas listas. Por lo cual se estan agragando realmente p elementos y hasta el momento se han contado $1+2p$ subgrupos. Si existe otro que no este contenido, se puede repetir este procedimos hasta contar $b = 1+mp$ subgrupos. Así $b \equiv 1 mod p$.

Ahora sean $H_1,\ldots,H_{k_s}$ todos los subgrupos de orden p^s y $K_1,\ldots,K_{k_{s+1}}$ todos los subgrupos de orden p^{s+1}. Para cada H_i hay a_i subgrupos d eorden p^{s+1} que lo contienen y para cada K_j hay b_j subgrupos que orden p^s que contiene. Tenemos que:

$$\sum_{i=1}^{k_s} a_i = \sum_{j=1}^{k_{s+1}} b_j$$

por ambas sumas cuentan las multiplicidades. Como $a_i \equiv 1 mod p$ y $b_j \equiv 1 mod p$. Entonces $\sum_{i=1}^{k_s} a_i \equiv k_s mod p$ y $\sum_{j=1}^{k_{s+1}} b_j \equiv k_{s+1} mod p$ por lo que $k_s \equiv k_{s+1} mod p$. Como sabemos que $k_s \equiv 1 mod p$ por recursión se sigue el resultado.

$\square$

2. Teoremas de Sylow

El teorema de Cauchy implica que si G es un grupo finito y $p \in \mathbb{N}$ es un número primo tal que $p \mid |G|$, G tiene un elemento de orden p y por lo tanto subgrupo de orden p. La importancia de este radica en el hecho de que nos proporciona un recíproco del teorema de Lagrange que como se vio en el capítulo anterior no es cierto en general pues A_4 no tiene un subgrupo de orden 6 y $6 \mid |A_4|$.

Continuando con este razonamiento, una segunda pregunta inmediata es qué sucede con otras potencias de p, es decir, si $|G| = p^k n$ con $(p,n) = 1$, ¿Existirá algún subgrupo de G de orden p^l para $l \in \{2,\ldots,k\}$? Vamos a analizar un ejemplo: Considere S_4 y observe que $|S_4| = 4! = 2^3 \cdot 3$. El teorema de Cauchy dice que existe un subgrupo de orden 3 de S_4, lo cual es obvio pues basta tomar el generado de cualquier triciclo en S_4, por ejemplo, $\langle (123) \rangle \leq S_4$. De la misma manera, el teorema de Cauchy también implica que existe un subgrupo de orden 2 y un ejemplo obvio es el generando de cualquier transposición, de forma concreta se puede considerar $\langle (12) \rangle \leq S_4$. Continuando con este análisis $4 \mid |S_4|$ y aunque el teorema de Cauchy no dice nada en este caso, hay ejemplos obvios de subgrupos de orden 4, a saber, el generando por cualquier 4-ciclo, por ejemplo, $\langle (1234) \rangle \leq S_4$. La pregunta se vuelve más interesante para $8 \mid |S_4|$, pues si este resultado es afirmativo, no se deduce de simplemente tomar algún r-ciclo como en los casos anteriores. Sin embargo el ejercicio 109 afirma que uno de tales subgrupos existe y que es isomorfo a D_4. De hecho este se puede obtener mediante intuición geométrica al recordar que D_4 es el grupo de simetrías de un cuadrado centrado en el origen el cual puede suponerse que tiene un vértice sobre el eje x, al etiquetar los vértices de este con los elementos $1,2,3$ y 4 (Ver figura 1). Luego, cada transformación que deje invariante al cuadrado, queda codificada con una permutación. De manera formal, si $S = (24) \in S_4$, que representa la reflexión respecto al eje x, y $T = (1234) \in S_4$, que representa la rotación por $90°$, se tiene que $D_4 \cong \langle S,T \rangle \leq S_4$ y $|\langle S,T \rangle| = 8$.

El hecho de que para todas las potencias de 2 que dividen al orden de S_4 exista un subgrupo con dicho orden es un resultado válido en general para cualquier primo que divida al orden de un grupo finito. Esta es la esencia del primer teorema de Sylow.

Además de dicho primer teorema hay otros dos (todos publicados en 1872) los cuales se discutirán al dar las definiciones adecuadas, pero antes de presentar dichos teoremas se requiere de un resultado previo que es el lema básico de esta sección.

LEMA 2.1. *Sean $p \in \mathbb{N}$ un número primo y G un p-grupo finito. Si $\cdot : G \times X \to X$ una acción finita, entonces*

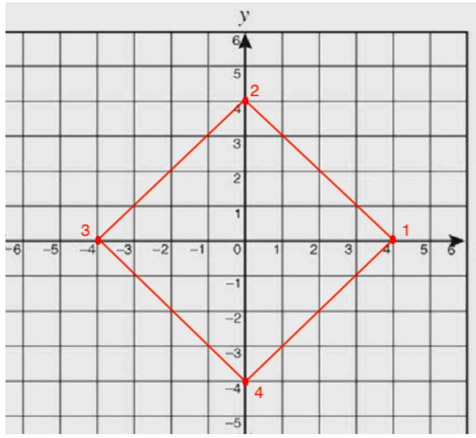


FIGURA 1.

$$|X| \equiv |Fix_G(X)| \mod p,$$

donde $Fix_G(X) = \{x \in X \mid \forall g \in G(gx = x)\}$.

DEMOSTRACIÓN. Considere uno de tales G-conjuntos X. Dado que las órbitas de la acción considerada son una partición de X, entonces $X = (\bigsqcup_{\theta \in X/G, |\theta|=1} \theta) \sqcup (\bigsqcup_{\theta \in X/G, |\theta|>1} \theta)$. Al calcular la cardinalidad se tiene que

$$|X| = \sum_{\theta \in X/G, |\theta|=1} |\theta| + \sum_{\theta \in X/G, |\theta|>1} |\theta|$$

Observe que el primer sumando es igual a $|Fix_G(X)|$. Por otro lado, considere $\theta \in X/G$ tal que $|\theta| > 1$. Del teorema órbita-estabilizador se deduce que $|\theta| = [G : G_x]$ para algún $x \in \theta$. Como G es un p-grupo, entonces $p \mid [G : G_x]$. Esto muestra que en la segunda suma, todos los términos son divisibles por p, luego, esta es congruente a $0 \mod p$, lo que demuestra el resultado. □

Como primera consecuencia del resultado anterior se tiene lo siguiente:

LEMA 2.2. *Si G es un grupo finito y H es un p-subgrupo de G, entonces*

$$[N_G(H) : H] \equiv [G : H] \mod p$$

DEMOSTRACIÓN. Tarea $\square$

Del resultado anterior se puede ahora deducir lo siguiente.

PROPOSICIÓN 2.1. *(Primer teorema de Sylow) Sean G un grupo finito y $p \in \mathbb{N}$ un número primo tal que $|G| = p^k n$ con $(p,n) = 1$. Entonces todo subgrupo de G que tiene orden p^l está contenido de manera normal en un subgrupo de orden p^{l+1}, donde $l \in \{0,...,k-1\}$. Por lo tanto G tiene un subgrupo de orden p^l para cualquier $l \in \{0,...,k\}$.*

DEMOSTRACIÓN. La prueba es un argumento recursivo de como obtener de un grupo de orden p^l uno de orden p^{l+1} con las propiedades deseadas.

Si $l = 0$, observe que el resultado se deduce el teorema de Cauchy. Así, sea $H \leq G$ con $|H| = p^l$, donde $l \in \{1,...,k-1\}$. Dado que $H \trianglelefteq N_G(H)$, entonces $N_G(H)/H$ es un grupo. Más aún, $|N_G(H)/H| = [N_G(H) : H]$ y como $[G : H] = p^{k-l}n$, donde $k-l \geq 1$, entonces $p \mid [G : H]$. Del lema anterior se deduce que $[N_G(H) : H] \equiv [G : H] \mod p$, entonces $p \mid [N_G(H) : H]$. Luego, al aplicar el teorema de Cauchy $N_G(H)/H$ tiene un subgrupo de orden p, que por el teorema de la correspondencia biyectiva es de la forma K/H con $K \leq N_G(H)$ y $H \trianglelefteq K$. Observe que por el teorema de Lagrange $|K| = [K : H]|H| = pp^l = p^{l+1}$, por lo que K es el grupo buscado. $\square$

El resultado anterior inspira la siguiente definición ya que observe que si $|G| = p^k \cdot n$ con $(p,n) = 1$ y p primo, del teorema anterior se deduce que un subgrupo $H \leq G$ tal que $|H| = p^k$, no puede estar contenido en otro p-subgrupo de G, es decir, es máximo. [1]

DEFINICIÓN 2.1. *Sean G un grupo y $p \in \mathbb{N}$ primo. Un **p-subgrupo de Sylow**, $P \leq G$, es un p-subgrupo máximo respecto al orden dado por la contención en la familia de p-subgrupos de G.*

Observaciones:

1. Del primer teorema de Sylow se deduce que en todo grupo finito, cualquier p-subgrupo está contenido en un p-subgrupo de Sylow. En particular, si $p \mid |G|$, G tiene un p-subgrupo de Sylow.

[1] Recuerde que para nosotros máximo es lo que la gente de habla hispana llama maximal (no hay un elemento por arriba de dicho elemento). Mientras que llamamos el mayor elemento a lo que la gente conoce como máximo (la mínima cota superior de un conjunto que pertenece al conjunto).

2. Si $|G| = p^k n$ con $(p,n) = 1$, entonces el orden de cualquier p-subgrupo de Sylow debe ser p^k.

EJEMPLO 2.1. *En el caso de S_4 nótese que un 2-grupo de Sylow es D_4, mientras que un 3-grupo de Sylow es $\langle(123)\rangle$.*

Es importante observar que la definición de p-subgrupo de Sylow está formulada para grupos sin ninguna hipótesis de finitud. Así, el primer teorema de Sylow solamente asegura la existencia de tales subgrupos en el caso finito. Un resultado que vale la pena comentar es que estos siempre existen cuando G tiene un p-subgrupo, independientemente de la hipótesis de finitud sobre G. Esto se demuestra a continuación.

PROPOSICIÓN 2.2. *Sea G un grupo. Todo p-subgrupo de G, está contenido en un p-subgrupo de Sylow.*

DEMOSTRACIÓN. Se usará el lema de Zorn: Sea $H \leq G$ un p-subgrupo. Considere

$$\mathscr{S} = \{K \leq G \mid K \text{ es } p\text{-subgrupo y } H \subseteq K\}.$$

Observe que $\mathscr{S} \neq \emptyset$ pues $H \in \mathscr{S}$. Además observe que $(\mathscr{S}, \subseteq)$ es un conjunto parcialmente ordenado.

Considere $\{K_\alpha\}_{\alpha\in\Lambda} \subseteq \mathscr{S}$ una cadena no vacía y tome $\bigcup_{\alpha\in\Lambda} K_\alpha \subseteq G$. Nótese que $\bigcup_{\alpha\in\Lambda} K_\alpha \leq G$ pues trivialmente $e \in \bigcup_{\alpha\in\Lambda} K_\alpha$ y si $g,h \in \bigcup_{\alpha\in\Lambda} K_\alpha$, entonces $g \in K_{\alpha_0}$ y $h \in K_{\alpha_1}$, para algunos $\alpha_0, \alpha_1 \in \Lambda$. Como la familia es una cadena, podemos suponer sin pérdida de generalidad que $K_{\alpha_0} \subseteq K_{\alpha_1}$ y así $g,h \in K_{\alpha_1}$; como $K_{\alpha_1} \leq G$, $gh^{-1} \in K_{\alpha_1}$ y así $gh^{-1} \in \bigcup_{\alpha\in\Lambda} K_\alpha$. Además observe que $H \subseteq \bigcup_{\alpha\in\Lambda} K_\alpha$ y $\bigcup_{\alpha\in\Lambda} K_\alpha$ es p-subgrupo. Esto prueba que $\bigcup_{\alpha\in\Lambda} K_\alpha$ es cota superior de $\{K_\alpha\}_{\alpha\in\Lambda}$. Luego, como la cadena fue arbitraria, el lema de Zorn implica que existe $P \in \mathscr{S}$ máximo y observe que dicho grupo es un p-grupo de Sylow buscado. $\square$

EJEMPLO 2.2. *Considere el grupo $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$. Para $p \in \mathbb{N}$ primo, observe que $\langle\{e^{\frac{2\pi ik}{p}} \mid k \in \mathbb{Z}\}\rangle \leq \mathbb{T}$. Dicho grupo tiene orden p y de hecho es isomorfo a $\mathbb{Z}_p$.*

El teorema anterior implica que $\mathbb{T}$ tiene un p-grupo de Sylow. En este ejemplo dicho p-grupo de Sylow es $\{e^{\frac{2\pi ik}{p^n}} \mid n \in \mathbb{N}^+,\ k \in \mathbb{Z}\}$.

Es importante decir que los teoremas clásicos de Sylow usan como hipótesis la finitud, por lo que aunque el resultado anterior es muy general, realmente nos vamos a concentrar en el caso finito.

Denote por $Syl_p(G)$ al conjunto de p-grupos de Sylow de G. Observe que dicho conjunto es cerrado bajo conjugación, es decir, el conjugado de cualquier p-subgrupo de Sylow es un p-subgrupo de Sylow (Ver Ejercicio 262). Más aún, el segundo teorema de Sylow dice que todos los grupos de Sylow de un grupo finito se obtienen de esta forma.

PROPOSICIÓN 2.3. *(Segundo teorema de Sylow) Sea G un grupo finito cuyo orden es divisible por un número primo $p \in \mathbb{N}$. Entonces, todos los p-subgrupos de Sylow de G son conjugados entre sí. En particular, cualesquiera dos p-subgrupos de Sylow de un grupo dado son isomorfismos.*

DEMOSTRACIÓN. Sean $P,Q \in Syl_p(G)$. Considere la acción $\cdot : P \times G/Q \to G/Q$ inducida por la restricción a P de la representación de G en las clases laterales de Q, es decir, $x \cdot gQ := xgQ$. Por el lema 2.1 se tiene que $|G/Q| \equiv |Fix_P(G/Q)| \mod p$. Dado que $p \nmid |G/Q|$, entonces $p \nmid |Fix_P(G/Q)|$ y en particular $Fix_P(G/Q) \neq \emptyset$.

Sea $gQ \in Fix_p(G/Q)$, entonces para cualquier $x \in P$, $xgQ = gQ$, es decir, para todo $x \in P$, $g^{-1}xg \in Q$. Esto dice que $g^{-1}Pg \subseteq Q$. Como hay una correspondencia biyectiva entre $g^{-1}Pg$ y P, así como entre P y Q, al ser todos los conjuntos finitos se deduce que $g^{-1}Pg = Q$, lo que demuestra la primera afirmación.

Para concluir, si $P,Q \in Syl_p(G)$, existe $g \in G$ tal que $P = gQg^{-1}$. Al considerar el morfismo de conjugación por g, $\gamma_g : G \to G$, se tiene que $(\gamma_g)|_Q : Q \to G$ es trivialmente inyectivo y como $im((\gamma_g)|_Q) = gQg^{-1} = P$, este es un isomorfismo entre P y Q. $\square$

Un resultado que se obtiene como coroalrio del resultado anterior caracteriza el hecho de cuando un grupo de Sylow es normal y como se va a ver, la condición es muy especial.

PROPOSICIÓN 2.4. *Un grupo finito G cuyo orden es divisible por un primo $p \in \mathbb{N}$ tiene un único p-subgrupo de Sylow P, si y sólo si $P \trianglelefteq G$.*

EJEMPLO 2.3. *Sean $p,q \in \mathbb{N}$ primos impares tales que $q \equiv 1 \mod p$. Nótese que el orden de $GL_2(\mathbb{Z}_q)$ es $(q^2-1)(q^2-q)$. Dado que $q = p^n m + 1$ con $(p,m) = 1$, $|GL_2(\mathbb{Z}_q)| =$*

$p^{2n}m'$ con $m' = m^2(p^n m+1)$. Luego, el primer teorema de Sylow implica que todo p-grupo de Sylow de $GL_2(\mathbb{Z}_q)$ tiene orden p^{2n}. Uno de tales p-subgrupos de Sylow es:

$$P = \left\{ \begin{pmatrix} a^{i\frac{q-1}{p^n}} & 0 \\ 0 & a^{j\frac{q-1}{p^n}} \end{pmatrix} \;\middle|\; a \in \mathbb{Z}_q \text{ es generador de } \mathbb{Z}_q^\times,\ i,j \in \mathbb{Z} \right\}$$

Observe que las raíces primitivas en $\mathbb{Z}_q$ tienen orden $q-1$. Esto implica que $a^{(q-1)/p^n}$ y todas sus potencias tienen orden una potencia de p. Así los elementos de P tiene orden una potencia p y $|P| = p^{2n}$. El argumento anterior muestra que P es un p-grupo de Sylow y además trivialmente es abeliano. Por el segundo teorema de Sylow todos los p-grupos de Sylow en $GL_2(\mathbb{Z}_q)$ son conjugados a P y así, todos son abelianos.

Observe que para el caso de S_4 el resultado anterior nos dice algo que ya conocíamos, a saber, que todos las triciclos son conjugados entre sí pues sus generados son los 3-subgrupos de Sylow de S_4. Nuevamente el ejemplo interesante viene al considerar D_4 pues en estos momentos no sabemos otros ejemplos de 2-grupos de Sylow en S_4 además de este. El último teorema de Sylow permite hacer un conteo de los p-subgrupos de Sylow de un grupo dado.

PROPOSICIÓN 2.5. *(Tercer teorema de Sylow) Sea G un grupo finito cuyo orden es divisible por un primo $p \in \mathbb{N}$. Si $n_p = |Syl_p(G)|$, entonces $n_p \mid |G|$ y $n_p \equiv 1 \mod p$.*

DEMOSTRACIÓN. Sea $X = Syl_p(G)$. Observe que por el segundo teorema de Sylow X es el conjunto de conjugados de $P_0 \in X$ fijo. Luego considere la representación de G en las clases de conjugación de $P_0 \in X$, $\rho' : G \to S_X$, y sea $\rho = \rho'|_{P_0} : P_0 \to S_X$ su restricción a P_0. Para la acción inducida, el lema 2.1 implica que $|X| \equiv |Fix_{P_0}(X)| \mod p$. Observe que trivialmente $P_0 \in Fix_{P_0}(X)$. Por otro lado, dado $Q \in Fix_{P_0}(X)$, para cualquier $g \in P_0$, $gQg^{-1} = Q$, de donde se deduce que $P_0 \subseteq N_G(Q)$. Esto implica que $P_0, Q \leq N_G(Q)$ y obviamente ambos son p-subgrupos de Sylow de $N_G(Q)$. Luego, por el segundo teorema de Sylow existe $g \in N_G(Q)$ tal que $P_0 = gQg^{-1} = Q$. Esto muestra que $|Fix_{P_0}(X)| = 1$. Al sustituir esto en la expresión del lema 2.1 se deduce que $n_p \equiv 1 \mod p$.

Para concluir observe que al considerar la acción de G en X, dado que por el segundo teorema de Sylow X es la órbita de P_0, al aplicar el teorema órbita-estabilizador se deduce que $n_p = |X| = [G : G_{P_0}] = [G : N_G(P_0)]$, de donde el teorema de Lagrange implica que $n_p \mid |G|$. $\square$

Observaciones:

1. Como escolio de la proposición anterior se obtiene que $|Syl_p(G)| = [G : N_G(P)]$ para cualquier $P \in Syl_p(G)$.
2. El hecho de que $|Syl_p(G)| \mid |G|$ y $|Syl_p(G)| \equiv 1 \mod p$, implica que si $|G| = p^k n$, entonces $|Syl_p(G)| \mid n$.

Las dos observaciones anteriores muestran una forma en la que es común encontrar el tercer teorema de Sylow en la literatura, a saber,

PROPOSICIÓN 2.6. *(Tercer teorema de Sylow -refinado-) Si $|G| = p^k n$ con $(p,n) = 1$ y $n_p := |Syl_p(G)|$, entonces:*

- $n_p \mid n$
- $n_p \equiv 1 \mod p$
- *Para cualquier $P \in Syl_p(G)$, $n_p = [G : N_G(P)]$*

A continuación se van a discutir algunos ejemplos. El primero tiene que ver con la pregunta que se plateó respecto a los 2-subgrupos de Sylow de S_4.

EJEMPLO 2.4. *En S_4, sea $n_2 = |Syl_2(S_4)|$. Por el tercer teorema de Sylow se tiene que $n_2|3$ y $n_2 \equiv 1 \mod 2$. Así, $n_2 \in \{1,3\}$. Observe que como $D_4 \ntrianglelefteq S_4$, pues D_4 no puede tener todas las estructuras cíclicas de sus elementos pues hay 6 transposiciones y 6 4-ciclos, lo que dan un total de 12 elementos y D_4 sólo tiene 8. Así, $n_2 = 3$.*

A pesar de que no conocemos los otros subgrupos, el segundo teorema nos permite obtenerlos pues basta con conjugar a D_4 con los elementos de S_4.

El siguiente ejemplo muestra que el tercer teorema de Sylow tiene como consecuencia el teorema de Wilson de teoría de números.

EJEMPLO 2.5. *(Teorema de Wilson) Sea $p \in \mathbb{N}$ primo. Considere S_p y observe que hay $|Syl_p(S_p)| = (\frac{p!}{p})\frac{1}{p-1}$ pues hay $\frac{p!}{p}$ p-ciclos en S_p y cada ciclo y sus potencias pertenecen a exactamente un p-grupo de Sylow, de ahí el factor $\frac{1}{p-1}$. Por tercer teorema de Sylow:*

$$(p-2)! \equiv 1 \mod p$$

Entonces,

$$(p-1)(p-2)! \equiv (p-1) \mod p$$

$$(p-1)! \equiv -1 \mod p$$

El último ejemplo a tratar tiene que ver con un teorema de clasificación, a saber, el de grupos de orden 15.

EJEMPLO 2.6. *Sea G grupo con $|G| = 15$. Sea $n_3 = |Syl_3(G)|$. Por el tercer teorema de Sylow $n_3|5$ y $n_3 \equiv 1 \mod 3$. La primera condición implica que $n_3 \in \{1,5\}$ pero $5 \equiv 2 \mod 3$, luego $n_3 = 1$. Entonces debe existir un único subgrupo de orden 3, el que tiene que ser normal. De manera análoga si $n_5 = |Syl_5(G)|$, el tercer teorema dice que en este caso $n_5|3$ y $n_5 \equiv 1 \mod 5$. La primer condición implica que $n_5 \in \{1,3\}$, de lo que se deduce que $n_5 = 1$, luego el único 5-subgrupo de Sylow es normal. Si $P \in Syl_3(G)$ y $Q \in Syl_5(G)$, como $(3,5) = 1$, $P \cap Q = \{e\}$ y luego $G \cong P \times Q \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$. Esto dice que hay único salvo isomorfismo grupo de orden 15.*

A manera de comentario se muestra uno de los análogos de los teoremas de Sylow en el caso infinito. Otras generalizaciones requieren algunas ideas topológicas como se puede ver por ejemplo en el libro de Serre “Topics in Galois theory”, donde se estudia el análogo para grupos profinitos.

PROPOSICIÓN 2.7. *Si $P \leq G$ es un p-subgrupo de Sylow tal que $\{gPg^{-1} \mid g \in G\}$ es finito, entonces todos p-subgrupo de Sylow es conjugado a P y además $|\{gPg^{-1} \mid g \in G\}| \equiv 1 \mod p$.*

3. Grupos de orden pequeño

El objetivo de esta sección es presentar una lista de todos los grupos de orden menor o igual a 15 salvo isomorfismo. Vale la pena comentar que ya se conocen algunos resultados al respecto pues como ejemplo de la aplicación del teorema de representación de un grupo en las clases laterales de un subgrupo se demostró que todo grupo de orden 6 es isomorfo a S_3 ó $\mathbb{Z}_2 \times \mathbb{Z}_3$ (Proposición 4.4).

Por otro lado, como ejemplo del uso de los teoremas de Sylow se demostró que si G es un grupo de orden 15, entonces $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$ (Ejemplo 2.6).

Para obtener el resultado de clasificación mencionado se van a realizar varios pasos que serán divididos en subsecciones, cada una de las cuales tiene un resultado general que permitirá obtener la clasificación buscada.

3.1. Grupos de orden primo. El primer paso no trivial en la clasificación buscada se obtiene al considerar dichos grupos. Para este caso no hay que desarrollar más herramienta de la considerada anteriormente por lo que el siguiente resultado da la clasificación buscada.

PROPOSICIÓN 3.1. *Si G es un grupo de orden $p \in \mathbb{N}$, con p primo, entonces G es cíclico. Por lo tanto $G \cong \mathbb{Z}_p$.*

DEMOSTRACIÓN. Sea $x \in G$ tal que $x \neq e$. Por el teorema de Lagrange $o(x) = p$, luego, $\langle x \rangle = G$. Esto demuestra la primera afirmación y la segunda se deduce del teorema de clasificación de grupos cíclicos (Ejemplo 2.2). $\square$

Observe que una prueba alterna del resultado anterior se obtiene al usar el teorema de Cauchy. Se ha elegido la prueba anterior por su simplicidad ya que esta se podía haber hecho simplemente con el material de los primeros dos capítulos.

En torno a la clasificación buscada, esto dice que hay un únicos grupos salvo isomorfismo de orden $2,3,5,7,11$ y 13, a saber: $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$ y $\mathbb{Z}_{13}$.

3.2. Grupos con orden el cuadrado de un primo. Para este paso el resultado se apoya en un famoso resultado que se presentó en la sección 1 de esté capítulo, a saber, que todo grupo de orden p^2 es abeliano. Recuerde que la prueba de este hecho se realizó usando la ecuación de clase; vale la pena mencionar que los ejercicios 165 y 166 dan una prueba artesanal de dicho resultado.

El resultado de clasificación buscado se presenta a continuación.

PROPOSICIÓN 3.2. *Si G es un grupo de orden p^2, entonces $G \cong \mathbb{Z}_{p^2}$ ó $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.*

DEMOSTRACIÓN. Sea $x \in G$ con $x \neq e$. Por el teorema de Lagrange $o(x) \in \{p, p^2\}$. Se van a estudiar ambos casos:

Caso 1: $o(x) = p^2$. Entonces $G = \langle x \rangle$ y por lo tanto $G \cong \mathbb{Z}_{p^2}$.

Caso 2: $o(x) = p$. Dado que por un resultado anterior G es abeliano, entonces $\langle x \rangle \trianglelefteq G$ y además $|G/\langle x \rangle| = p$. Esto implica que $G/\langle x \rangle$ es cíclico y entonces $G/\langle x \rangle = \langle y + \langle x \rangle \rangle$. Observe que $o(y) \in \{p, p^2\}$. Si $o(y) = p^2$, entonces $G = \langle y \rangle \cong \mathbb{Z}_{p^2}$. En caso contrario observe que por construcción $\langle x \rangle \cap \langle y \rangle = \{e\}$. Como G es finito, $G \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$. $\square$

Observe que la prueba anterior no usa material más allá del capítulo 2, salvo el hecho de que todo grupo de orden p^2 es abeliano. De ahí que este haya aparecido como ejercicio de dicho capítulo (Ejercicio 98).

Es importante notar que para que el resultado anterior muestre que en efecto únicamente hay dos representantes para las clases de isomorfismo para grupos de orden p^2, se tiene que ver que $\mathbb{Z}_{p^2}$ y $\mathbb{Z}_p \times \mathbb{Z}_p$ no son isomorfos. Esto es claro pues el primero de estos grupos es cíclico mientras que el segundo no lo es. Otra prueba de este hecho se puede hacer notando que $\mathbb{Z}_{p^2}$ tiene un elemento de orden p^2 (la clase del 1), mientras que todos los elementos no triviales de $\mathbb{Z}_p \times \mathbb{Z}_p$ tienen orden p.

Regresando a la clasificación que se busca esto da la lista de los grupos salvo isomorfismo para órdenes 4 y 9, a saber, en orden 4 se tiene a $\mathbb{Z}_2 \times \mathbb{Z}_2$ y $\mathbb{Z}_4$. En el caso de orden 9 se tienen $\mathbb{Z}_3 \times \mathbb{Z}_3$ y $\mathbb{Z}_9$.

3.3. Grupos con orden el producto de dos primos distintos. El siguiente paso es clasificar los grupos con orden de la forma pq con $p, q \in \mathbb{N}$ primos y $p > q$.

PROPOSICIÓN 3.3. *Si G es un grupo tal que $|G| = pq$ con $p > q$ y $p, q \in \mathbb{N}$ primos, entonces $G \cong \mathbb{Z}_{pq}$ ó G tiene una presentación de la forma $(g, h | g^p, h^q, hgh^{-1}g^{-m})$ con $m^q \equiv 1 \mod p$ y $m \not\equiv 1 \mod p$. Además si $q \nmid p-1$, el segundo caso no ocurre.*

DEMOSTRACIÓN. Por el teorema de Cauchy existe $g \in G$ con $o(g) = p$. Observe que $q = [G : \langle g\rangle] = [G : N_G(\langle g\rangle)][N_G(\langle g\rangle) : \langle g\rangle]$, de donde se deduce que alguno de los índices en el producto debe ser 1. Observe que como $\langle g\rangle$ es un p-grupo, entonces $[N_G(\langle g\rangle) : \langle g\rangle] \equiv [G : \langle g\rangle] \mod p = q \mod p$. Dado que $[N_G(\langle g\rangle) : \langle g\rangle] \leq q < p$, la congruencia implica que $[N_G(\langle g\rangle) : \langle g\rangle] = q$, de donde se deduce que $[G : N_G(\langle g\rangle)] = 1$, por lo que $N_G(\langle g\rangle) = G$. Esto prueba que $\langle g\rangle \trianglelefteq G$.

Por otro lado, usando nuevamente el teorema de Cauchy existe $h \in G$ con $o(h) = q$. Observe que $\langle h\rangle \leq G$ es un q-subgrupo de Sylow y si $n_q = |Syl_q(G)|$, entonces el tercer teorema de Sylow implica que $n_q | p$ y $n_q \equiv 1 \mod q$. Dado que la primera relación implica que $n_q \in \{1, p\}$, la prueba se va a dividir es esos dos casos:

Caso 1: $n_q = 1$. En tal caso $\langle h\rangle \trianglelefteq G$. Como $(p, q) = 1$, entonces $\langle g\rangle \cap \langle h\rangle = \{e\}$ y así por finitud de G, $G \cong \langle g\rangle \times \langle h\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

Caso 2: $n_q = p$. Entonces $q | p-1$ y además $\langle h\rangle \ntrianglelefteq G$. Dado que $\langle g\rangle \trianglelefteq G$, entonces $hgh^{-1} = g^m$ para algún $m \in \{0, ..., p-1\}$. Además $m \not\equiv 1 \mod p$ pues en caso contrario g y h conmutan y se regresa al caso abeliano, lo cual no puede suceder pues esto implicaría que $\langle h \rangle \trianglelefteq G$. Para concluir observe que por inducción se tiene que para cualquier $n \in \mathbb{N}^+$, $h^n g h^{-n} = g^{m^n}$. En particular $m^q \equiv 1 \mod p$.

Además observe que si $q \nmid p-1$, entonces $n_q \neq p$, por lo que $n_q = 1$ y así, el segundo caso no sucede. $\square$

El resultado anterior dice que bajo las hipótesis mencionadas existen a lo más dos clases de isomorfismo para grupos de orden pq. Para ver que los representantes dados son distintos, observe que cuando se tengan los dos casos que menciona el teorema los grupos en cuestión no son isomorfos pues $\mathbb{Z}_{pq}$ es cíclico y la presentación $(g,h|g^p,h^q,hgh^{-1}g^{-m})$ define un grupo no abeliano y por lo tanto no cíclico.

A continuación se va a aplicar el resultado anterior para continuar con la clasificación buscada. Aunque el caso de orden 6 se conoce, se va a ver como se deduce este del resultado anterior.

EJEMPLO 3.1. *Si G es un grupo con $|G| = 6 = 3 \cdot 2$, entonces $p = 3$ y $q = 2$. El resultado anterior implica que $G \cong \mathbb{Z}_6$ ó G tiene presentación $(g^3,h^2,hgh^{-1}g^{-m})$ con $m \not\equiv 1 \mod 3$ pero $m^2 \equiv 1 \mod 3$. Estas congruencias implican que $m = 2$. Así, la relación $hgh^{-1}g^{-m}$ es equivalente a $hgh = g^2 = g^{-1}$, es decir, $G \cong D_3$.*

Es importante decir que en la proposición 4.4 se probó que en el segundo caso $G \cong S_3$. No hay ninguna contradicción en el resultado obtenido pues $D_3 \cong S_3$ por ser estos grupos no abelianos de orden 6.

EJEMPLO 3.2. *Si G es un grupo con $|G| = 10 = 5 \cdot 2$, se tiene que $G \cong \mathbb{Z}_{10}$ ó G tiene presentación $(g^5,h^2,hgh^{-1}g^{-m})$ con $m \not\equiv 1 \mod 5$ y $m^2 \equiv 1 \mod 5$. La solución a este sistema de congruencias implica que $m = 4$. Luego, $G \cong D_5$ en el segundo caso.*

Nótese que los ejemplos anteriores son similares pues el orden de G es producto de 2 por un primo impar. De hecho el argumento de clasificación se puede englobar en un sólo resultado general, el cual se encuentra en el ejercicio 286.

El último ejemplo a tratar ya se había hecho antes. El punto es ver como se usa el resultado anterior para obtenerlo pues además, usa la hipótesis que elimina el segundo caso.

EJEMPLO 3.3. *Si G es un grupo con $|G| = 15 = 5 \cdot 3$, entonces nótese que $3 \nmid 4$, por lo que $G \cong \mathbb{Z}_{15}$.*

3.4. Casos especiales. Hasta el momento faltan dos casos para concluir con la clasificación, a saber, el de orden 8 y el de orden 12. Se tratará el de orden 8 y se dejará como ejercicio el de orden 12 (Ejercicios 287, 288 y 289). Ambas pruebas se dividen en dos casos que provienen del hecho de si G es o no abeliano.

PROPOSICIÓN 3.4. *Si G es un grupo abeliano con $|G| = 8$, entonces $G \cong \mathbb{Z}_8$, $G \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ ó $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.*

DEMOSTRACIÓN. Por el teorema de Lagrange los elementos no triviales de G deben tener órdenes $2, 4$ y 8. Si G tiene un elemento de orden 8, entonces $G \cong \mathbb{Z}_8$. Así, suponga que G no tiene elementos de orden 8. La prueba se va a hacer por casos:

Caso 1: Existe $g \in G$ con $o(g) = 4$. Observe que tiene que existir $h \in G \setminus \langle g \rangle$ con $o(h) = 2$ pues en caso contrario G tendría un elemento de orden 2, a saber g^2, así como 6 elementos de orden 4, lo cual es imposible. Por construcción $\langle g \rangle \cap \langle h \rangle = \{e\}$. Como G es finito y abeliano, esto implica que $G \cong \langle g \rangle \times \langle h \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Caso 2: Todos los elementos no triviales de G tienen orden 2. En este caso existe una acción de $\mathbb{Z}_2$ en G, que hace de G un $\mathbb{Z}_2$-espacio vectorial. Dado que dicho espacio vectorial debe tener dimensión finita pues G es finito, entonces $G \cong (\mathbb{Z}_2)^n$ para alguna $n \in \mathbb{N}$, donde este isomorfismo se da como $\mathbb{Z}_2$-espacios vectoriales y en particular como grupos. Al tomar la cardinalidad de ambos lados se deduce que $n = 3$, por lo que se concluye que como grupos $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Vale la pena mencionar que el resultado anterior se puede obtener como corolario de un teorema más general que se conoce como el Teorema Fundamental del los Grupos Abelianos Finitos. Dicho teorema se discutirá en el siguiente capítulo y por lo tanto la prueba del resultado anterior puede considerarse como un argumento artesanal. Sin embargo, encierra muchas ideas algebraicas interesantes por sí mismas, lo que hace que la prueba tenga su valor y tenga sentido exponerla.

Además observe que los grupos $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ y $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ no son isomorfos pues el primero es cíclico y los otros dos no. Respecto a los últimos dos, estos no pueden ser isomorfos pues todo elemento no trivial en $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ tiene orden 2, mientras que $\mathbb{Z}_4 \times \mathbb{Z}_2$ tiene elementos de orden 4, por ejemplo $(1, 0)$.

PROPOSICIÓN 3.5. *Si G es un grupo no abeliano de orden 8, entonces $G \cong \mathbb{H}$ ó $G \cong D_4$.*

DEMOSTRACIÓN. Observe que G no tiene elementos de orden 8 por ser no abeliano y además no todos los elementos tienen orden 2 pues en un grupo en el que todos los elementos tienen orden 2 es abeliano. Así, existe $g \in G$ de orden 4. Dado que $[G : \langle g \rangle] = 2$, entonces $\langle g \rangle \trianglelefteq G$ y de hecho $G/\langle g \rangle \cong \mathbb{Z}_2$. Luego, si $h \in G \setminus \langle g \rangle$, entonces $h^2 \in \langle g \rangle$, lo que implica que $h^2 \in \{e, g, g^2, g^3\}$. Si $h^2 = g$ ó $h^2 = g^3$, entonces $o(h) = 8$, lo que es una contradicción, por lo que las únicas posibilidades restantes son $h^2 = e$ ó $h^2 = g^2$.

Por otro lado, como $\langle g \rangle \trianglelefteq G$, $hgh^{-1} \in \langle g \rangle$ y así, $hgh^{-1} \in \{e, g, g^2, g^3\}$. Dado que $o(hgh^{-1}) = o(g)$, entonces $hgh^{-1} = g$ ó $hgh^{-1} = g^3$. No puede suceder que $hgh^{-1} = g$ pues como esto es equivalente a que $hg = gh$ y $G = \langle g, h \rangle$, entonces G sería abeliano, lo que es una contradicción.

Las observaciones hachas en los párrafos anteriores dan lugar a un par de casos.

Caso 1: $h^2 = g^2$ y $hgh^{-1} = g^3$. Observe que esto es una presentación de Q_8 y $Q_8 \cong \mathbb{H}$, con isomorfismo $f : Q_8 \to \mathbb{H}$ que se obtiene al extender $f(g) = i$ y $f(h) = j$.

Caso 2: $h^2 = e$ y $hgh^{-1} = g^3$. Observe que como $o(g) = 4$, la segunda ecuación es igual a $hgh = g^{-1}$, lo que da presentación de D_4 y por lo tanto $G \cong D_4$. $\square$

Es importante señalar que esta proposición se demuestra con material del capítulo 2, es por ello que se incluyó como un ejercicio (Ejercicio 110).

Para concluir con esta sección se va a presentar una tabla (tabla 1) donde aparecen todos los resultados obtenidos. Vale la pena mencionar que T denota al grupo $\langle g, h \mid g^6 = 1, h^2 = g^3 = (gh)^2 \rangle$. Por otro lado, observe que hay algunos datos curiosos que se pueden extraer de esta. Por ejemplo, que el grupo no cíclico con menor orden es $\mathbb{Z}_2 \times \mathbb{Z}_2$. Además, que el grupo no abeliano con menor orden es D_3.

4. Grupos Solubles

DEFINICIÓN 4.1. *Una serie normal de un grupo G es una sucesión de subgrupos de G,*

$$e = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

tales que $G_i \trianglelefteq G_{i+1}$ para $i = 0, \ldots, n-1$. Llamamos a n la longitud de la serie normal. A G_{i+1}/G_i los llamamos los grupos factor de la serie.

EJERCICIO 241. *La serie normal $e \leq A_n \leq S_n$.*

Orden	Representantes de las clases de isomorfismo
1	$\{e\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4,\ \mathbb{Z}_2\times\mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_2\times\mathbb{Z}_3,\ D_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8,\ \mathbb{Z}_4\times\mathbb{Z}_2,\ \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,\ \mathbb{H}, D_4$
9	$\mathbb{Z}_9,\ \mathbb{Z}_3\times\mathbb{Z}_3$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_{12},\ \mathbb{Z}_6\times\mathbb{Z}_2,\ A_4, D_6,\ T$
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

TABLA 1. Grupos de orden pequeño.

DEFINICIÓN 4.2. *Una serie normal se llama soluble si todos sus grupos factor son abelianos. Un grupo es soluble si tiene una serie soluble.*

EJERCICIO 242. *Todo grupo abeliano es soluble.*

EJERCICIO 243. *S_n es no soluble para $n \geq 5$.*

PROPOSICIÓN 4.1. *Sea G un grupo soluble. Entonces todo subgrupo de G es soluble.*

DEMOSTRACIÓN. Sea $H \leq G$ y $e = G_0 \leq G_1 \leq \cdots \leq G_n = G$ una serie soluble de G. Consideramos la serie

$$e = G_0 \cap H \leq G_1 \cap H \leq \cdots \leq G_n \cap H = G \cap H = H$$

Aplicando el segundo teorema de isomorfismo a $H \cap G_{i+1} \leq G_{i+1}$ y $G_i \trianglelefteq G_{i+1}$ tenemos que $H \cap G_i = (H \cap G_{i+1}) \cap G_i \trianglelefteq H \cap G_{i+1}$. Por lo que la tenemos una serie normal. También por el segundo teorema de isomorfismo tenenmos que:

$$(H \cap G_{i+1})/(H \cap G_i) \cong G_i(H \cap G_{i+1})/G_i \leq G_{i+1}/G_i$$

Por lo que $(H \cap G_{i+1})/(H \cap G_i)$ es un subgrupo de un grupo abeliano. Por lo que es abeliano y así la serie es soluble. Por lo tanto H es soluble. $\square$

PROPOSICIÓN 4.2. *Sea G un grupo soluble. Entonces todo grupo cociente de G es soluble.*

DEMOSTRACIÓN. Sea $H \leq G$, $\pi\colon G \longrightarrow G/H$ la proyección canónica y $e = G_0 \leq G_1 \leq \cdots \leq G_n = G$ una serie soluble de G. Consideramos la serie

$$e = \pi(G_0) \leq \pi(G_1) \leq \cdots \leq \pi(G_n) = G/H$$

Sea $\pi(x) \in \pi(G_i)$ con $x \in G_i$ y $\pi(y) \in \pi(G_{i+1})$ con $y \in G_{i+1}$. Entonces $yxy^{-1} \in G_i$ por lo que $\pi(y)\pi(x)\pi(y)^{-1} \in \pi(G_i)$. Por lo que la serie es normal. Consideramos los epimorfismos $G_i \longrightarrow \pi(G_{i+1})$ y $\pi(G_{i+1}) \longrightarrow \pi(G_{i+1})/\pi(G_i)$ y su composición $\phi\colon G_{i+1} \longrightarrow \pi(G_{i+1})/\pi(G_i)$. Como $G_i \leq nuc(\phi)$, entonces se induce un epimorfismo $\psi\colon G_{i+1}/G_i \longrightarrow \pi(G_{i+1})/\pi(G_i)$. Por lo que $\pi(G_{i+1})/\pi(G_i)$ es el cociente de un grupo abeliano y así es un grupo abeliano. Por lo tanto la sucesión es soluble y así G/H es soluble. □

PROPOSICIÓN 4.3. *Sea G un grupo y H un subgrupo normal de G tal que H y G/H es soluble. Entonces G es soluble.*

DEMOSTRACIÓN. Sea $e = G_0 \leq G_1/H \leq \cdots \leq G_n/H = G/H$ una serie soluble de G/H y $e = H_0 \leq H_1 \leq \cdots \leq H_m = H$ una serie soluble de H. La serie

$$e = H_0 \leq H_1 \leq \cdots \leq H_m \leq G_0 \leq G_1 \leq \ldots G_n = G$$

es soluble. □

COROLARIO 4.1. *Si G y H son grupos solubles. Entonces $G \times H$ es un grupo soluble.*

PROPOSICIÓN 4.4. *Sea p un primo. Entonces todo p-grupo finito es soluble.*

DEMOSTRACIÓN. Sea G un p-grupo finito. La prueba se hace sobre inducción sobre el orden de los p grupos finitos. Notemos que $Z(G) \neq e$ por lo que $G/Z(G)$ es un p-grupo con orden estrictamente menor que G. Por hipotesis de inducción $G/Z(G)$ es soluble y $Z(G)$ es soluble por ser abeliano. Por lo tanto G es soluble. □

DEFINICIÓN 4.3. *Sea G un grupo. Definimos los conmutadores altos de forma recursiva de la siguiente manera: $G^{(0)} = G$ y $G^{(n+1)} = (G^{(n)})'$. La serie derivada de G es:*

$$e \leq \ldots G^{(2)} \leq G^{(1)} \leq G$$

Recordemos que el conmutador G' de un grupo es el mínimo subgrupo normal de G tal que el cociente G/G' es abeliano. Por lo que en el caso de que exista un natural tal que $G^{(n)} = e$ entonces la serie derivada seria normal. Más aún, la serie seria soluble.

DEFINICIÓN 4.4. *Sea G un grupo. Decimos que G es nilpotente si existe un natural n tal que $G^{(n)} = e$.*

PROPOSICIÓN 4.5. *Sea G un grupo. Entonces G es nilpotente si y sólo si G es soluble.*

DEMOSTRACIÓN. La ida ya se explico por lo que solo falta el regreso. Si $e = G_0 \leq G_1 \leq \cdots \leq G_n = G$ es una serie solvable. Afirmamos que $G^{(n-i)} \leq G_i$ para $i = 0, \ldots, n$. Lo demostraremos por inducción sobre i. Si $i = 0$, entonces $G_0 = G = G^{(0)}$. Como G_i/G_{i-1} es abeliano, por la minimalidad del conmutador tenemos que $G_i' \leq G_{i-1}$. Por hipotesis de inducción $G^{(n-i)} \leq G_i$, de aquí $G^{(n-(i-1))} \leq G_i' \leq G_{i-1}$.

Por lo que concluimos que $G^{(n)} \leq G_0 = e$. Por lo tanto G es soluble. $\square$

5. Ejercicios

En esta parte de la tarea $p, q \in \mathbb{N}$ denotan números primos.

EJERCICIO 244. *Sea G un p-grupo finito y $H \trianglelefteq G$ no trivial. Demuestre que $H \cap Z(G) \neq \{e\}$.*

EJERCICIO 245. *Sea G un p-grupo finito y $H \trianglelefteq G$ de orden p. Demuestre que $H \leq Z(G)$.*

EJERCICIO 246. *Demuestre que si G es un grupo no abeliano de orden p^3, entonces el orden del centro es p y $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.*

EJERCICIO 247. *Sea G un p-grupo finito. Demuestre que el número de subgrupos normales de orden p^k es congruente a 1 módulo p.*

EJERCICIO 248. *Demuestre que si G es un grupo con $|G| = pm$ con $1 < m < p$, entonces G no es simple.*

EJERCICIO 249. *Sea G un p-grupo finito y X un G-conjunto finito tal que $(|X|, p) = 1$. Demuestre que existe $x \in X$ tal que para todo $g \in G$, $g \cdot x = x$.*

EJERCICIO 250. *Sea V un $\mathbb{Z}_p$-espacio vectorial de dimensión n, $n > 0$. Demuestre que si $G \leq GL_n(\mathbb{Z}_p)$ con $|G| = p^n$, entonces existe $v \in V$, $v \neq 0$, tal que para todo $g \in G$, $g \cdot v = v$.*

EJERCICIO 251. *Demuestre que en el ejercicio 137 la proposición recíproca también es cierta.*

EJERCICIO 252. *Complete los detalles en la siguiente prueba de que un grupo de orden p^2 es abeliano.*

DEMOSTRACIÓN. Como $|Z(G)| > 1$ (¿Por qué?) entonces $Z(G)$ tiene un subgrupo de orden p (¿Por qué?) y sea dicho subgrupo H. Si $a \in G \setminus H$, entonces $o(a) = p$ (¿Por qué?) y de esto se deduce que $C_G(a) = G$ ¿Por qué?. Así, se deduce que $a \in Z(G)$, de lo que se concluye que $Z(G) = G$ ¿Por qué?. Esto prueba que G es abeliano. □

EJERCICIO 253. *Sea G un p-grupo finito. Demuestre que G es cíclico si y sólo si G tiene un único subgrupo de índice p.*

EJERCICIO 254. *Sea G un p-grupo no abeliano de orden p^3. Demuestre que G contiene exactamente $p+1$ subgrupos máximos.*

EJERCICIO 255. *Si G es un grupo finito y H es un p-subgrupo de G, demuestre que*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}$$

EJERCICIO 256. *Sea $H \trianglelefteq G$ tal que H y G/H es un p-grupo. Demuestre que G es un p-grupo.*

EJERCICIO 257. *Sea* $\mathbb{Q}^{\times}$ *el grupo de unidades de* $\mathbb{Q}$ *y* $\mathbb{Z}^{\times} = \mathbb{Z} \setminus \{0\}$. *Describir algún* p*-grupo de Sylow de* $\mathbb{Q}^{\times}/\mathbb{Z}^{\times}$.

EJERCICIO 258. *Dar explícitamente un* p*-grupo de Sylow de* $GL_n(\mathbb{Z}_p)$.

EJERCICIO 259.

1. *Sean* G *un grupo finito y* $P \leq G$ *un* p*-subgrupo de Sylow de* G. *Demuestre que para cualquier* $H \leq G$, *existe* $g \in G$ *tal que* $H \cap gPg^{-1} \leq H$ *es un* p*-subgrupo de Sylow.*
2. *Usa el ejercicio 258 y el inciso anterior para demostrar que en un grupo finito, todo* p*-subgrupo se encuentra contenido en un* p*-subgrupo de Sylow.*
3. *Usar el ejercicio 258 y el inciso 1 para demostrar que cualesquiera dos* p*-grupos de Sylow de un grupo son conjugados.*

EJERCICIO 260. *Sea* G *un grupo con orden* $2^n p^m$ *con* $n \in \{1,2,3\}$, $m \in \mathbb{N}^+$ *y* p *impar. Demuestre que* G *es simple.*

EJERCICIO 261. *Demuestre que todo grupo simple de orden 60 es isomorfo a* A_5.[2]

EJERCICIO 262. *Sea* G *un grupo finito cuyo orden es un múltiplo de* p *y* $P \in Syl_p(G)$. *Demuestre que para todo* $g \in G$, $gPg^{-1} \in Syl_p(G)$.

EJERCICIO 263.

1. *Demuestre que si* $G \cong H$, *entonces* $Syl_p(G) = Syl_p(H)$.
2. *¿Es cierto el converso de la afirmación anterior?*

EJERCICIO 264. *Sea* G *un grupo abeliano finito. Demuestre lo siguiente:*

[2]Esto tiene como consecuencia que el grupo no cíclico simple con menor orden es A_5.

1. *Para cada número primo $p \in \mathbb{N}$ tal que $p \mid |G|$, existe exactamente un p-subgrupo de Sylow.*
2. *En G se satisface el recíproco del teorema de Lagrange, es decir, para todo $m \in \mathbb{N}$ tal que $m \mid |G|$, existe $H \leq G$ tal que $|H| = m$.*[3]

EJERCICIO 265. *Sea $H \leq G$ y $P \in Syl_p(G)$. Demuestre que si $N_G(P) \leq H$ entonces $N_G(H) = H$.*

EJERCICIO 266. *Sea $H \trianglelefteq G$ y $P \in Syl_p(G)$. Demuestre que $H \cap P \in Syl_p(H)$ y $HP/H \in Syl_p(G/H)$.*

EJERCICIO 267. *Sean G un grupo finito y $Q \trianglelefteq G$ un p-grupo. Demuestre que para todo $P \in Syl_p(G)$, $Q \leq P$.*

EJERCICIO 268. *Sean $p, q \in \mathbb{N}$ primos con $p < q$. Demuestre que:*

1. *Todo grupo de orden pq tiene un único subgrupo de orden q. Más aún dicho subgrupo es normal.*
2. *Si q no es congruente con $1 \mod p$ entonces G es cíclico.*

EJERCICIO 269. *Demuestre que no existe ningún subgrupo simple de orden 63.*

EJERCICIO 270. *Sea G un grupo de orden 50 con un único subgrupo de orden 2. Demuestre que G es abeliano.*

EJERCICIO 271. *Sea G un grupo tal que $|G| = pq$ con $3 \leq p$, $p < q$ y q el primo consecutivo a p. Demuestre que G es abeliano. ¿Qué sucede con esta afirmación si $3 \nleq p$?*

[3]Observe que este ejercicio dice que en los grupos abelianos finitos se cumple el recíproco del teorema de Lagrange.

EJERCICIO 272. *Sea G un grupo tal que* $|G| = p^2q$ *con* $3 \leq p$, $p < q$ *y q el primo consecutivo a p. Demuestre que G es abeliano. ¿Qué sucede con esta afirmación si* $3 \nleq p$*?*

EJERCICIO 273. *Sea G un grupo tal que* $|G| = (pq)^2$ *con* $5 \leq p$, $p < q$ *y q el primo consecutivo a p. Demuestre que G es abeliano. ¿Qué sucede con esta afirmación si* $5 \nleq p$*?*

EJERCICIO 274. *Sea G un grupo finito,* $H \leq G$ *y* $P \in Syl_p(G)$*. Demuestre que si* $N_G(P) \subseteq H$*, entonces* $N_G(H) = H$*. Pruebe también que* $N_G(N_G(P)) = N_G(P)$*.*

EJERCICIO 275. *Sea G un grupo de orden* 28*. Demuestre que si G tienen un subgrupo normal de orden* 4 *entonces G es abeliano.*

EJERCICIO 276. *Sea G un p-grupo finito y* $H \trianglelefteq G$ *con* $H \neq \{e\}$*. Demuestre que* $H \cap Z(G) \neq \{e\}$*.*

EJERCICIO 277. *Sea G un p-grupo finito. Demuestre que todo subgrupo normal de orden p está contenido en* $Z(G)$*.*

EJERCICIO 278. *Sea G un grupo de orden pq con* $p > q$ *y* $P \leq G$ *con orden p. Demuestre que* $P \trianglelefteq G$*.*

EJERCICIO 279. *Sea G un grupo de orden* p^n *y* $H \leq G$*. Demuestre que existe* $x \in G \setminus H$ *tal que* $H^x = H$*.*

EJERCICIO 280. *Sea G un grupo de orden* p^2q *con p y q primos. Demuestre que G no es simple.*

EJERCICIO 281. *Sea G un grupo finito,* $P \in Syl_p(G)$ *tal que* $P \subseteq Z(G)$*. Demuestre que existe* $N \trianglelefteq G$ *tal que* $P \cap N = \{e\}$ *y* $PN = G$*.*

EJERCICIO 282. *Sea G un grupo finito, $P \in Syl_p(G)$ y $H \trianglelefteq G$. Demuestre que si $P \trianglelefteq H$ entonces $P \trianglelefteq G$.*

EJERCICIO 283. *Demuestre que si G es un grupo no abeliano de orden p^3 entonces $Z(G) = [G,G]$.*

EJERCICIO 284. *Sea G un p-grupo finito y $H \leq G$ tal que $[G : H] = p^2$. Demuestre que $H \trianglelefteq G$ ó que H tiene p conjugados.*

EJERCICIO 285. *Sea G un p-grupo finito. Demuestre que G es cíclico si y sólo si $G/[G : G]$ es cíclico.*

EJERCICIO 286. *Demuestre que si $|G| = 2p$ con p primo, entonces $G \cong \mathbb{Z}_{2p}$ ó $G \cong D_p$.*

EJERCICIO 287. *Sea G un grupo de orden 12 con $G \ncong A_4$. Demuestre lo siguiente:*

1. *G tiene un elemento de orden 6.*
2. *G tiene un 3-subgrupo normal de Sylow.*
3. *G tiene exactamente 2 elementos de orden 3.*

EJERCICIO 288. *Demuestre que si G es un grupo abeliano de orden 12, entonces $G \cong \mathbb{Z}_{12}$ ó $G \cong \mathbb{Z}_6 \times \mathbb{Z}_2$.*

EJERCICIO 289. *Demuestre que si G es un grupo no abeliano de orden 12, entonces $G \cong A_4$, $G \cong D_6$ ó $G \cong T$. Sugerencia: Usar el ejercicio 287.*

EJERCICIO 290. *Demuestre que todo grupo abeliano es soluble.*

EJERCICIO 291. *Demuestre que S_n es no soluble para $n \geq 5$.*

EJERCICIO 292. *Demuestre que si todo subgrupo de Sylow de un grupo finito es cíclico, entonces dicho grupo es soluble.*

Capítulo 5

Grupos Abelianos

"Las matemáticas no permiten hipocresía ni vagueza."

Stendahl.

1. Ideas básicas de categorías

La idea de esta sección es introducir la noción de categoría y los conceptos más básicos en torno a esta teoría, haciendo énfasis en el caso de grupos y grupos abelianos, con el objetivo de generar el lenguaje básico sobre el que se va a trabajar en el presente capítulo. La forma más sana de leer esta sección es notar que muchos de los conceptos presentados se han desarrollado anteriormente en el curso, luego, lo que se está haciendo es extraer las ideas básicas que comparten estas y otras estructuras matemáticas usando como noción primitiva la idea de "morfismo o flecha".

1.1. Definiciones básicas.

DEFINICIÓN 1.1. *Una **categoría** $\mathscr{C}$ consta de una colección de objetos, denotada por $Obj(\mathscr{C})$, y una colección de morfismos o flechas, denotada por $Mor(\mathscr{C})$, así como de un par de funciones $d,c : Mor(\mathscr{C}) \to Obj(\mathscr{C})$, que se conocen como el dominio y codominio del morfismo en cuestión; donde todo $f \in Mor(\mathscr{C})$ con dominio A y codominio B se denota por $f : A \to B$.*

Si la clase de morfismos entre dos objetos A y B se denota por $Hom_{\mathscr{C}}(A,B)$, se cumple que:

1. *Para cada $A \in Obj(\mathscr{C})$ existe $1_A \in Hom_{\mathscr{C}}(A,A)$.*
2. *Dados $A,B,C \in Obj(\mathscr{C})$, existe una función $\circ : Hom_{\mathscr{C}}(B,C) \times Hom_{\mathscr{C}}(A,B) \to Hom_{\mathscr{C}}(A,C)$, $(g,f) \mapsto g \circ f$, a la que se le conoce como composición.*

Además, los datos anteriores satisfacen los siguientes axiomas:

A1) Para cada $f \in Hom_{\mathscr{C}}(A,B)$, $1_B \circ f = f = f \circ 1_A$.

A2) Para cualesquiera $f \in Hom_{\mathscr{C}}(A,B)$, $g \in Hom_{\mathscr{C}}(B,C)$ *y* $h \in Hom_{\mathscr{C}}(C,D)$, $h \circ (g \circ f) = (h \circ g) \circ f$.

NOTACIÓN 1.1.

- *Se escribirá* $A \in \mathscr{C}$ *para abreviar* $A \in Obj(\mathscr{C})$. *De hecho, en la gran mayoría de los casos se va a omitir la notación* Obj *para los objetos de una categoría, a no ser que por alguna razón sea necesario usarla.*
- *La composición de dos morfismos* f,g *se denotará* gf *en lugar de* $g \circ f$ *en la gran mayoría de ocasiones. El que se pida que la composición de esto sea asociativa implica que la composición no requiere paréntesis, como se vio al inicio del curso.*

Al adaptar la prueba que se hizo al inicio del curso donde se demostró que el neutro en un grupo es único, se deduce que el morfismo 1_A es único respecto a la propiedad A1. A este se le conoce como el **morfismo identidad** en el objeto A.

Vale la pena decir que hay una discusión enorme en torno a los fundamentos de la definición de categoría. Esta discusión se va a omitir no porque no sea importante, si no porque en estos momentos se quiere aprender esta herramienta y por lo tanto el objetivo es concentrarse en eso.[1] En esta dirección, la única observación que se va a hacer es que las categorías pueden ser colecciones que no son conjuntos[2] y por lo tanto se tienen dos definiciones que capturan la idea de "pequeñez".

DEFINICIÓN 1.2. *Una categoría* $\mathscr{C}$ *se llama* ***localmente pequeña*** *si para cualesquiera* $A,B \in \mathscr{C}$, $Hom_{\mathscr{C}}(A,B)$ *es un conjunto. Dicha categoría es* ***pequeña*** *si* $Obj(\mathscr{C})$ *es un conjunto.*[3]

A continuación se van a discutir algunos ejemplos de categorías.

[1]De hecho nuestra idea es aún más modesta pues queremos usar estos conceptos en el caso de grupos abelianos. Por otro lado, incluso en un primer curso de teoría de categorías esta discusión se suele postergar por el sencillo hecho de que hay que conocer la teoría para realmente entender dónde se encuentran los conceptos e ideas delicadas.

[2]Lo cual sigue siendo delicado pues depende de elegir una axiomática de la teoría de conjuntos, pero que en los ejemplos a tratar no será difícil de ver cuando una colección es un conjunto, incluso para alguien que sólo conozca los axiomas de ZFC.

[3]La definición de categoría pequeña dada en estas notas es la misma que da Borceaux en su "Handbook of categorical algebra" Vol 1.

EJEMPLO 1.1. *La categoría vacía que tiene por objetos al conjunto vacío y por morfismos al conjunto vacío. Esta categoría es pequeña y localmente pequeña.*

EJEMPLO 1.2. *La categoría de conjuntos,* ***Set****, con objetos los conjuntos y morfismos las funciones entre ellos. La composición es la composición usual de funciones al igual que las identidades. Esta categoría es localmente pequeña pero no pequeña.*

EJEMPLO 1.3. *La categoría de grupos,* ***Grp****, cuyos objetos son la clase de todos los grupos y con morfismos los morfismos de grupos. Observe que dado que la composición de morfismos de grupos es un morfismo de grupos y la identidad es un morfismo de grupos, entonces la composición es la composición usal de funciones. Nuevamente esta categoría es localmente pequeña pero no pequeña.*

EJEMPLO 1.4. *La categoría de grupos abelianos,* ***Ab****, cuyos objetos son los grupos abelianos y morfismos lo morfismos entre ellos. Esta categoría es localmente pequeña pero no pequeña.*

EJEMPLO 1.5. *La categoría de espacios vectoriales sobre un campo k,* ***k-Vec****, con las transformaciones lineales como morfismos y la composición usual de funciones.*

EJEMPLO 1.6. *La categoría de conjuntos parcialmente ordenados,* ***POSet****, con las funciones que preservan el orden.*

Nótese que en los ejemplos anteriores los objetos son siempre conjuntos con alguna estructura extra y los morfismos funciones que preservan dicha estructura. El siguiente ejemplo muestra que un morfismo no tiene porque ser una función.

EJEMPLO 1.7. *Sea G un grupo. Asociado a G se puede construir una categoría, que se denota por $\mathscr{B}G$, que tiene un único objeto, el cual se puede denotar por $*$, y cuyo única familia de morfismos $Hom_{\mathscr{B}G}(*,*) = G$. El producto del grupo es la composición de esta categoría y por lo tanto su neutro es la única identidad. Nótese que estas categorías son pequeñas y localmente pequeñas.*

Otro ejemplo que tiene el mismo formato que el anterior en el sentido de que asocia a una estructura algebraica una categoría, se presenta a continuación.

EJEMPLO 1.8. *Sea* $(P,\leq)$ *un conjunto parcialmente ordenado. A este conjunto se le puede asignar una categoría, que se denotará por* $\overline{P}$*, cuyos objetos son los elementos de* P*, y para* $x,y \in P$*,*

$$Hom_{\overline{P}}(x,y) = \begin{cases} \{f_{xy}\} & Si\ x \leq y \\ \emptyset & e.o.c. \end{cases}$$

En esta definición, los símbolos $\{f_{xy}\}$ *cumplen las propiedades* $f_{xy}f_{yz} = f_{xz}$ *(que expresa la transitividad del orden parcial) y* $f_{xx} = 1_x$ *(que expresa la simetría de dicho orden).*[4]

Esta categoría es pequeña y localmente pequeña.

Como se puede notar la idea de categoría parece ser subyacente en las estructuras algebraicas. Más aún, se pueden definir estructuras de categorías básicamente en cualquier estructura matemática, por supuesto que dichos ejemplos requieren saber de algunas otras cosas fuera del álgebra, cosa que no puede suponerse como requisito del curso y se aleja de los objetivos de este, por lo tanto no se tratarán. Sin embargo es importante estar consciente de la existencia de estos ejemplos que hacen ver un poco del gran alcance de la teoría de categorías como un lenguaje para axiomatizar estructuras matemáticas. De los ejemplos discutidos anteriormente básicamente nos quedaremos con tres que son los que se tratarán para dar ejemplos y en los que el lector siempre tiene que pensar cuando se da una definición, a saber, el caso de **Set**, **Grp** y **Ab**. Por supuesto que esto se hace para los fines del curso pues muchos de los ejemplos presentados anteriormente guardan ideas matemáticas muy interesantes , pero que sin embargo no da tiempo discutir pues no entran en los fines de este curso, pero que indudablemente se discuten en un curso de teoría de categorías.

A toda categoría $\mathscr{C}$, se le puede asociar otra categoría que se le conoce como su **categoría opuesta**, la que se va a denotar por $\mathscr{C}^{op}$, que se define de la siguiente manera:

$$Obj(\mathscr{C}^{op}) = Obj(\mathscr{C})$$
$$\text{Para } A,B \in \mathscr{C},\ Hom_{\mathscr{C}^{op}}(A,B) := Hom_{\mathscr{C}}(B,A)$$

Las defniciones anteriores fuerzan a como definir la composición pues si $f \in Hom_{\mathscr{C}^{op}}(A,B)$ y $g \in Hom_{\mathscr{C}^{op}}(B,C)$, entonces $f \in Hom_{\mathscr{C}}(B,A)$ y $g \in Hom_{\mathscr{C}}(C,B)$, por lo que $fg \in Hom_{\mathscr{C}}(C,A)$, y así, $fg \in Hom_{\mathscr{C}^{op}}(A,C)$. Por lo tanto, se define

$$\circ : Hom_{\mathscr{C}^{op}}(B,C) \times Hom_{\mathscr{C}^{op}}(A,B) \to Hom_{\mathscr{C}^{op}}(A,C)$$
$$(g,f) \mapsto fg$$

[4]De hecho observe que esto muestra que en realidad dicha categoría puede definirse a partir de un preorden.

La idea de la categoría opuesta puede parecer artificial en estos momentos, sin embargo, la siguiente discusión pretende mostrar una de las razones por las cuales es útil introducirla. Para esto recuerde que como se observó en el capítulo 2, en el caso de morfismos de grupos se tienen ciertas clases especiales de ellos. Estas definiciones provienen de la teoría de categorías y se presentan a continuación.

DEFINICIÓN 1.3. *Sea $\mathscr{C}$ una categoría. $f \in Hom_{\mathscr{C}}(A,B)$ es un:*

1. ***mono(morfismo)*** *si cumple la propiedad de cancelación por la izquierda respecto a morfismos en $\mathscr{C}$ que se puedan componer con f, es decir, para cualesquiera $g,h \in Hom_{\mathscr{C}}(C,A)$ tales que $fg = fh$, se tiene que $g = h$.*
2. ***epi(morfismo)*** *si cumple la propiedad de cancelación por derecha respecto a morfismos en $\mathscr{C}$ que se puedan componer con f, es decir, para cualesquiera $g,h \in Hom_{\mathscr{C}}(B,C)$ tales que $gf = hf$, se tiene que $g = h$.*
3. ***bimorfismo*** *si es mono y epi.*
4. ***mono(morfismo) que escinde*** *si tiene una inversa izquierda, es decir, existe $g \in Hom_{\mathscr{C}}(B,A)$ tal que $gf = 1_A$.*
5. ***epi(morfismo) que escinde*** *si tiene una inversa derecha, es decir, existe $g \in Hom_{\mathscr{C}}(B,A)$ tal que $fg = 1_B$.*
6. ***isomorfismo*** *si es mono que escinde y epi que escinde.*

Observaciones:

- En una categoría no vacía, cualquier clase de los morfismos definidos anteriormente es no vacía ya que la identidad en cualquier objeto pertenece a todas las clases anteriores.
- Si $f : A \to B$ es un mono, es usual escribir $f : A \rightarrowtail B$
- Si $f : A \to B$ es epi, es usual escribir $f : A \twoheadrightarrow B$

Lo que se quiere hacer en el resto de la sección es ver las relaciones entre los tipos especiales de morfismos de la definición anterior, así como algunas de las propiedades principales de estos. En el resto de esta sección $\mathscr{C}$ es una categoría.

PROPOSICIÓN 1.1. *Sea $f : A \to B$ un morfismo en $\mathscr{C}$. f es un isomorfismo si y sólo si es invertible, es decir, existe $g : B \to A$ en $\mathscr{C}$ tal que $fg = 1_B$ y $gf = 1_A$.*

DEMOSTRACIÓN. El regreso es obvio. Para la ida, dado que f es un isomorfismo, existen $g,h \in Hom_{\mathscr{C}}(B,A)$ tales que $gf = 1_A$ y $fh = 1_B$. Observe que si se prueba que $g = h$, el resultado queda demostrado. En efecto, observe que se tienen las igualdades

$$g = g1_B = g(fh) = (gf)h = 1_A h = h$$

□

Para las siguientes propiedades conviene hacer una observación fundamental, que es una de las razones por las que se introdujo la categoría opuesta.

PROPOSICIÓN 1.2. *Sea* $f \in Hom_{\mathscr{C}}(A,B)$.

1. f *es mono si y sólo si* $f \in Hom_{\mathscr{C}^{op}}(B,A)$ *es epi.*
2. f *es mono que escinde si y sólo si* $f \in Hom_{\mathscr{C}^{op}}(B,A)$ *es epi que escinde.*

DEMOSTRACIÓN. Respecto a la ida de la primera afirmación, sean $g,h \in Hom_{\mathscr{C}^{op}}(A,C)$ tales que $gf = hf$. Por definición de la categoría opuesta, esto implica que en $\mathscr{C}$ se cumple que $fg = fh$. Como f es mono, entonces es cancelable por la izquierda, lo que implica que $g = h$. Observe que el regreso de esta afirmación es similar.

La segunda afirmación es obvia. □

La importancia del resultado anterior radica en una interpretación muy potente a la hora de demostrar teoremas, pues esta dice que si un teorema es válido para monos, lo será para epis y viceversa. Lo mismo sucede con los conceptos de mono que escinde y epi que escinde. Este tipo de propiedades forman parte de uno de los metateoremas de la teoría de categorías que se conoce como principio de dualidad. Un ejemplo de esto se presenta en el siguiente resultado.

PROPOSICIÓN 1.3.

1. *Todo mono que escinde es mono.*
2. *Todo epi que escinde es epi.*
3. *Todo isomorfismo es bimorfismo.*

DEMOSTRACIÓN. Se va a probar simplemente la primera afirmación pues la prueba de la segunda es dual a esta y la tercera es un corolario claro de las anteriores. Sea $f \in Hom_{\mathscr{C}}(A,B)$ mono que escide, así como $g,h \in Hom_{\mathscr{C}}(C,A)$ tales que $fg = fh$. Dado que existe $r \in Hom_{\mathscr{C}}(B,A)$ tal que $rf = 1_A$, se deduce que

$$g = 1_A g = (rf)g = r(fg) = r(fh) = (rf)h = 1_A h = h$$

□

El resultado anterior muestra la comparación entre los conceptos dados, pero las afirmaciones recíprocas no son ciertas en general. Para esto se van a discutir algunos ejemplos.

EJEMPLO 1.9. *En **Set** los monos, monos que escinden y las funciones inyectivas coinciden. Lo mismo sucede con los epis, epis que escinden y funciones suprayectivas, así como con los bimorfismos, isomorfismos y funciones inyectivas.*

EJEMPLO 1.10. *En **Grp** y **Ab** los monomorfismos son los morfismos inyectivos de grupos, los epimorfismos son los morfismos suprayectivos de grupos y los bimorfismos son los isomorfismos, que a su vez son los morfismos biyectivos. Sin embargo, la inclusión $\iota : 2\mathbb{Z} \to \mathbb{Z}$ es un mono que no es un mono que escinde y la proyección $\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ es un epimorfismo que no es epi que escinde.*[5]

Vale la pena mencionar que en muchas categorías que vienen del álgebra sucede algo parecido al ejemplo anterior, es decir, aunque los monos que escinden y monos, así como los epis que escinden y los epis no coinciden, los bimorfismos y epimorfismos lo hacen. Esto sucede por el hecho de que en estas categorías la estructura "reconoce inversas", cosa que no sucede en general.[6]

La siguiente proposición da una forma muy común de encontrar isomorfismos en la práctica.

PROPOSICIÓN 1.4.

1. *Todo mono que es epi que escinde es isomorfismo.*
2. *Todo epi que es mono que escinde es isomorfismo.*

DEMOSTRACIÓN. Si $f \in Hom_{\mathscr{C}}(A,B)$ es mono y epi que escinde, existe $s \in Hom_{\mathscr{C}}(B,A)$ tal que $fs = 1_B$. Nótese que $f(sf) = (fs)f = 1_B f = f = f 1_A$. Al usar que f es cancelable por izquierda se deduce que $sf = 1_A$. La prueba de la segunda afirmación es dual. □

[5] Ver ejercicios 79 y 80

[6] Un ejemplo canónico se tiene en la categoría de espacios topológicos con su estructura usual, pues los isomorfismos son los homeomorfismos y los bimorfismos son las funciones continuas biyectivas. Con esta caracterización es una discusión usual de un curso de topología básico el dar ejemplos de funciones continuas y biyectivas que no son homeomorfismos, por ejemplo, la identidad de un conjunto (con al menos dos elementos) dotado con la topología discreta en el dominio y la topología indiscreta en el codominio.

Para concluir con esta sección, se va discutir una última de las propiedades básicas más útiles de los morfismos definidos respecto a la composición.

PROPOSICIÓN 1.5. *Cualquiera de las familias de morfismos definidas es cerrada bajo composición.*

DEMOSTRACIÓN. Por dualidad y de la definición, basta con probar los casos de mono y mono que escinde. Para el primer caso sean $f \in Hom_{\mathscr{C}}(A,B)$ y $g \in Hom_{\mathscr{C}}(B,C)$ monos y $h,k \in Hom_{\mathscr{C}}(D,A)$ tales que $(gf)h = (gf)k$. Entonces, $g(fh) = g(fk)$ y como g es mono, entonces $fh = fk$. Al usar que f es mono se deduce que $h = k$, lo que prueba el resultado.

Para el caso restante sean $f \in Hom_{\mathscr{C}}(A,B)$ y $g \in Hom_{\mathscr{C}}(B,C)$ monos que escinden. Entonces existen $h \in Hom_{\mathscr{C}}(B,A)$ y $k \in Hom_{\mathscr{C}}(C,B)$ tales que $hf = 1_A$ y $kg = 1_B$. Observe que $gf \in Hom_{\mathscr{C}}(A,C)$ y $hk \in Hom_{\mathscr{C}}(C,A)$. Además,

$$(hk)(gf) = h(kg)f = hf = 1_A,$$

esto prueba la afirmación. □

1.2. Productos y coproductos. En esta sección se van a introducir dos de las construcciones más famosas de la teoría de categorias.

DEFINICIÓN 1.4. *Sea $\{A_\alpha\}_{\alpha\in\Lambda}$ una colección de objetos en una categoría $\mathscr{C}$. El* ***producto*** *de dicha familia consta de un objeto, P, y una colección de morfismos, $\{\pi_\alpha : P \to A_\alpha\}_{\alpha\in\Lambda}$, con la propiedad de que dada cualquier otra familia de morfismos en $\mathscr{C}$, $\{f_\alpha : B \to A_\alpha\}_{\alpha\in\Lambda}$, existe un único morfismo $f : B \to P$ tal que para cualquier $\alpha \in \Lambda$, $\pi_\alpha f = f_\alpha$. Es decir, el siguiente diagrama conmuta para cada $\alpha \in \Lambda$:*

$$\begin{tikzcd} P \arrow[r, "\pi_\alpha"] & A_\alpha \\ B \arrow[u, dotted, "f"] \arrow[ur, "f_\alpha"'] & \end{tikzcd}$$

A esta última se le conoce como la ***propiedad universal del producto****.*

El ***coproducto*** *de la familia dada es el producto en la categoría opuesta cuando este exista.*

En la definición anterior se usan los artículos "el" para el producto y coproducto, lo cual sucede por el hecho de que si estos existen deben ser únicos (salvo isomorfismo).

PROPOSICIÓN 1.6. *Si el producto (coproducto) de una familia de objetos existe, este es único.*

DEMOSTRACIÓN. Canónica. □

En virtud de la proposición anterior, dada una familia de objetos en $\mathscr{C}$, $\{A_\alpha\}_{\alpha\in\Lambda}$, se tiene que:

1. Si el producto existe, al objeto producto se le denota por $\prod_{\alpha\in\Lambda} A_\alpha$ y a los morfismos π_α se les conoce como proyecciones canónicas del producto. Si $\Lambda = \{1,...,n\}$, el producto se suele denotar por $A_1 \times \cdots \times A_n$.
2. Dualmente, si el coproducto de dicha familia existe, a este se le denota por $\coprod_{\alpha\in\Lambda} A_\alpha$ y a los morfismos $\iota_\alpha : A_\alpha \to \coprod_{\alpha\in\Lambda} A_\alpha$ se les conoce como inclusiones canónicas. Además se tiene la notación correspondiente para cuando Λ es finito.
3. Hay que tener cuidado con el hecho de que los morfismos canónicos en un producto y coproducto pueden no ser epis y monos respectivamente. En el caso de la categoría de grupos sí se cumple esta dicha propiedad.

Observación: En el caso $\Lambda = \emptyset$, la propiedad universal del producto dice simplemente que el objeto producto satisface que dado cualquier otro objeto de la categoría, existe un único morfismo $f : A \to \prod_{\alpha\in\emptyset} A_\alpha$. En este caso a $\prod_{\alpha\in\emptyset} A_\alpha$ se le conoce como **objeto terminal** y se suele denotar por 1. Dualmente el coproducto vacío se conoce como **objeto inicial** y se denota por 0.

EJEMPLO 1.11. *En **Set** el producto es el producto usual y el coproducto es la unión ajena. El objeto inicial es $\emptyset$ y el terminal $\{*\}$.*

EJEMPLO 1.12. *En **Grp** el producto es el producto directo y el coproducto es el producto libre. En este caso el objeto inicial y terminal coinciden y son es grupo trivial.*[7]

EJEMPLO 1.13. *En **Ab** el producto es nuevamente el producto directo. El objeto inicial y terminal coinciden nuevamente y estos son el grupo trivial.*

[7]Cuando el objeto inicial y terminal coinciden, a este objeto se le conoce como objeto cero. Esta definición está justificada del ejemplo presente.

El caso del coproducto en la categoría de grupos abelianos no se deduce del de la categoría de grupos ya que el producto libre no es abeliano en general, incluso cuando se tomen grupos abelianos. Así, que queda abierta la pregunta de si existe el coproducto en la categoría de grupos abelianos. La respuesta es afirmativa y para su construcción considere $\{G_\alpha\}_{\alpha\in\Lambda}$ una familia de grupos abelianos no vacía. Considere $\prod_{\alpha\in\Lambda} G_\alpha$ y defina para $x \in \prod_{\alpha\in\Lambda} G_\alpha$ el soporte de dicho elemento, $sop(x)$, como el conjunto $\{\alpha \in \Lambda \mid x_\alpha \neq 0\}$. Defina

$$\bigoplus_{\alpha\in\Lambda} G_\alpha = \left\{ x \in \prod_{\alpha\in\Lambda} G_\alpha \;\middle|\; |sop(x)| < \aleph_0 \right\}.$$

Observe que $\bigoplus_{\alpha\in\Lambda} G_\alpha \leq \prod_{\alpha\in\Lambda} G_\alpha$ pues $sop(x^{-1}) = sop(x)$ y $sop(x+x') \subseteq sop(x) \cup sop(x')$. En particular $\bigoplus_{\alpha\in\Lambda} G_\alpha$ es un grupo abeliano y a este se le conoce como la **suma directa** de la familia $\{G_\alpha\}_{\alpha\in\Lambda}$. Observe que si Λ es finito, entonces $\bigoplus_{\alpha\in\Lambda} G_\alpha = \prod_{\alpha\in\Lambda} G_\alpha$.

Por otro lado, dado $\alpha \in \Lambda$, existe una función canónica $\iota_\alpha : G_\alpha \to \bigoplus_{\alpha\in\Lambda} G_\alpha$ definida mediante

$$\iota_\alpha(x)_\beta = \begin{cases} x, & \text{Si } \beta = \alpha \\ 0, & \text{En otro caso} \end{cases}$$

Observe que trivialmente ι_α es un morfismo de grupos. Más aún, se cumple lo siguiente:

PROPOSICIÓN 1.7. *Con las hipótesis y definiciones anteriores, sea $\{f_\alpha : G_\alpha \to H\}_{\alpha\in\Lambda}$ una familia de morfismos con H abeliano. Entonces existe un único $f : \bigoplus_{\alpha\in\Lambda} G_\alpha \to H$ tal que para cualquier $\alpha \in \Lambda$, $f \circ \iota_\alpha = f_\alpha$. Es decir, el siguiente diagrama conmuta para cada $\alpha \in \Lambda$:*

$$\begin{tikzcd} G_\alpha \arrow[r, "\iota_\alpha"] \arrow[dr, "f_\alpha"'] & \bigoplus_{\alpha\in\Lambda} G_\alpha \arrow[d, dotted, "f"] \\ & H \end{tikzcd}$$

DEMOSTRACIÓN. Dada la familia de las hipótesis, defina $f(x) := \sum_{\alpha\in\Lambda} f_\alpha(x_\alpha)$. Observe que esta función está bien definida pues $|sop(x)| < \aleph_0$. Además trivialmente esta función es un morfismo de grupos y más aún, $f \circ \iota_\alpha = f_\alpha$.

Supóngase que $g : \bigoplus_{\alpha\in\Lambda} G_\alpha \to H$ es un morfismo tal que para cualquier $\alpha \in \Lambda$, $g \circ \iota_\alpha = f_\alpha$. Para ver que f y g son iguales, basta ver que tienen la misma regla de correspondencia. Para esto observe que dado $x \in \bigoplus_{\alpha\in\Lambda} G_\alpha$, se tiene que $x = \sum_{\alpha\in\Lambda} \iota_\alpha(x_\alpha)$. Entonces,

$$g(x) = g(\sum_{\alpha\in\Lambda} \iota_\alpha(x_\alpha)) = \sum_{\alpha\in\Lambda} g(\iota_\alpha(x_\alpha)) = \sum_{\alpha\in\Lambda} f_\alpha(x_\alpha) =: f(x),$$

lo que concluye la prueba. □

Observe que el resultado anterior dice que la suma directa de la familia $\{G_\alpha\}_{\alpha\in\Lambda}$ satisface la propiedad universal del coproducto en la categoría de grupos abelianos. Observe que para esta construcción no se usa la notación estándar que viene de la teoría de categorías; esto es un detalle histórico que nosotros también asumiremos.

1.3. Funtores. La idea de funtor es muy importante en la teoría de categorías y en la matemática en general. Estos objetos pretenden axiomatizar la idea de morfismo entre categorías, lo que además muestra como las ideas de la teoría de categorías pueden usarse en las categorías en sí.

DEFINICIÓN 1.5. *Un **funtor** F entre las categorías $\mathscr{C}$ y $\mathscr{D}$, que notacionalmente se escribirá $F : \mathscr{C} \to \mathscr{D}$, consta de una asignación a nivel de objetos $F : Obj(\mathscr{C}) \to Obj(\mathscr{D})$ y una asignación en morfismos, donde para $f : A \to B$ en $\mathscr{C}$, se tiene $F(f) : F(A) \to F(B)$ es un morfismo en $\mathscr{D}$, sujeto a los siguientes axiomas:*

- *Para cualquier $A \in \mathscr{C}$, $F(1_A) = 1_{F(A)}$.*
- *Si $f : A \to B$ y $g : B \to C$ son morfismos en $\mathscr{C}$, entonces $F(gf) = F(g)F(f)$.*

Observación:

- Algunos autores llaman a estos funtores covariantes y dan una definición para funtores contravariantes que en la asignación en morfismos, giran el dominio y codominio, y por ende el axioma de la composición debe cambiarse de orden. Esta notación no se usará en estas notas pues con la categoría opuesta, un funtor contravariante de la categoría $\mathscr{C}$ en $\mathscr{D}$, es simplemente un funtor de $\mathscr{C}^{op}$ en $\mathscr{D}$ de acuerdo a la definición anterior.

EJEMPLO 1.14. *Para cualquier categoría $\mathscr{C}$, se puede definir el **funtor identidad** $1_{\mathscr{C}} : \mathscr{C} \to \mathscr{C}$, que en objetos y morfismos se comporta como la identidad.*

EJEMPLO 1.15. *Dado un objeto $A \in \mathscr{C}$, el funtor constante con valor A, $C_A : \mathscr{C} \to \mathscr{C}$, se define como aquel que a cualquier objeto le asigna el objeto A y, a cualquier morfismo el morfismo identidad en A.*

EJEMPLO 1.16. *Existe un funtor* $(\_)_{ab} : \boldsymbol{Grp} \to \boldsymbol{Ab}$ *conocido como el funtor de abelianización. Los detalles de este se pueden consultar en el ejercicio 85.*

Existen ejemplos muy generales de funtores que juegan un papel fundamental en la teoría de categorías. Para definirlos se requiere hacer una discusión: Sean $\mathscr{C}$ una categoría localmente pequeña y $A \in \mathscr{C}$. Se definen las asignaciones

$$h_A : \mathscr{C} \to \mathbf{Set},$$

que a nivel de objetos tiene por regla de correspondencia $h_A(B) = Hom_{\mathscr{C}}(A,B)$ y, a un morfismo $f : B \to C$, le asigna la función $h_A(f) : Hom_{\mathscr{C}}(A,B) \to Hom_{\mathscr{C}}(A,C)$, cuya regla de correspondencia es $h_A(f)(g) = fg$.

Así como

$$h^A : \mathscr{C}^{op} \to \mathbf{Set},$$

que a nivel de objetos tiene por regla de correspondencia $h^A(B) = Hom_{\mathscr{C}}(B,A)$, y a un morfismo $f : B \to C$ le asigna la función $h^A(f) : Hom_{\mathscr{C}}(C,A) \to Hom_{\mathscr{C}}(B,A)$, cuya regla de correspondencia es $h^A(f)(g) = gf$.

PROPOSICIÓN 1.8. *Con las hipótesis de la discusión previa, las asignaciones definidas son funtores.*

DEMOSTRACIÓN. Se va a realizar la prueba para el caso de h^A pues la prueba para h_A es análoga. Así, considérese $1_B : B \to B$ y nótese que $h^A(1_B) : Hom_{\mathscr{C}}(B,A) \to Hom_{\mathscr{C}}(B,A)$. Además, para $f \in Hom_{\mathscr{C}}(B,A)$, se tiene que $h^A(1_B)(f) = f1_B = f$. Por lo tanto, $h^A(1_B) = 1_{Hom_{\mathscr{C}}(B,A)}$.

Por otro lado, si $f \in Hom_{\mathscr{C}}(B,C)$, $g \in Hom_{\mathscr{C}}(C,D)$ y $h \in Hom_{\mathscr{C}}(D,A)$, entonces $h^A(gf)(h) = h(gf) = (hg)f = h^A(f)(hg) = h^A(f)h^A(g)(h)$. $\square$

NOTACIÓN 1.2. *Los funtores anteriores se conocen como los* ***funtores “hom” covariante y contravariante*** *en el objeto A respectivamente. También suelen llamarse* ***funtores representables*** *en el objeto A.*

Un ejemplo particularmente importante para nuestros fines se obtiene al considerar $\mathscr{C} = \mathbf{Ab}$. En este caso, el funtor “hom” covariante y contravariante se vuelven más especiales. Para esto se requieren hacer algunas observaciones previas.

PROPOSICIÓN 1.9. *Si $A,B \in$ **Ab**, entonces $Hom_{\boldsymbol{Ab}}(A,B)$ es un grupo abeliano.*[8]

DEMOSTRACIÓN. Dados $f,g \in Hom_{\mathbf{Ab}}(A,B)$, defina $f+g \in Hom_{\mathbf{Ab}}(A,B)$ mediante $(f+g)(a) = f(a)+g(a)$. Observe que dicha operación está bien definida pues B es abeliano, ya que dados $a,a' \in A$, se tiene que

$$
\begin{aligned}
(f+g)(a+a') &= f(a+a')+g(a+a') \\
&= (f(a)+f(a'))+(g(a)+g(a')) \\
&= (f(a)+g(a))+(f(a')+g(a')) \\
&= (f+g)(a)+(f+g)(a')
\end{aligned}
$$

Es sencillo ver que dicha operación satisface los axiomas de grupo. □

Dado $A \in \mathbf{Ab}$, el funtor "hom" contravariante, $h^A : \mathbf{Ab}^{op} \to \mathbf{Set}$, asigna a un morfismo de grupos $f \in Hom_{\mathbf{Ab}}(B,C)$ una función $h^A(f) : Hom_{\mathbf{Ab}}(C,A) \to Hom_{\mathbf{Ab}}(B,A)$ definida por $h^A(f)(g) = gf$. Más aún, dados $g,k \in Hom_{\mathbf{Ab}}(C,A)$, se tiene que

$$h^A(f)(g+k) = (g+k)f = gf+kf = h^A(f)(g)+h^A(f)(k)$$

Esto dice que con la estructura de grupo abeliano de la proposición anterior, $h^A(f)$ es un morfismo de grupos. Esto prueba la parte no trivial del siguiente resultado (para el caso contravariante).

PROPOSICIÓN 1.10. *Los funtores "hom" covariantes y contravariantes inducen para cada $A \in$ **Ab**, funtores:*

$$h_A : \boldsymbol{Ab} \to \boldsymbol{Ab}$$

$$h^A : \boldsymbol{Ab}^{op} \to \boldsymbol{Ab}$$

[8]Observe que la misma conclusión se obtiene si se pide solamente que B sea abeliano, donde en este caso la conclusión es respecto $Hom_{\mathbf{Grp}}(A,B)$.

2. Grupos Abelianos

Durante todo este los grupos serán abelianos por lo que pasaremos a la notación aditiva. En vez de expresar la operación con el producto se expresará por la suma. Para $S,T \subseteq G$ con G grupo, se escribirá $S+T$ en vez de ST. El neutro se denotará por 0. Las clases son de la forma $g+H$. Notamos que en el caso de una familia de subgrupos $\{H_i\}_{i\in I}$ de G, podemos definir la suma $\sum_{i\in I} H_i$ como el subgrupo de sumas finitas $\sum_{j=1}^{m} x_j$ con $x_j \in H_{i_j}$ para algún $i_j \in I$.

PROPOSICIÓN 2.1 (tarea). *Sea G un grupo y $\{H_i\}_{i\in I}$ una familia de subgrupos de G. Entonces la función $\pi\colon \bigoplus_{i\in I} H_i \longrightarrow \sum_{i\in I} H_i$ dada por $\pi(\phi) = \sum_{i\in I} \phi(i)$ para toda $\phi \in \bigoplus_{i\in I} H_i$ es un epimorfismo.*

DEFINICIÓN 2.1. *Sea G un grupo y $H \leq G$. Decimos que H es un sumando directo si existe $K \leq G$ tal que $H+K = G$ y $H \cap K = 0$.*

PROPOSICIÓN 2.2. *[tarea] Sea G un grupo y $H \leq G$. Son equivalentes:*

1. *H es sumando directo de G*
2. *Existes $K \leq G$ tal que todo $g \in G$ tiene una única expresión como $g = h+k$ con $h \in H$ y $k \in K$.*
3. *Existe un morfismo $s\colon G/H \longrightarrow G$ tal que $\pi s = 1_{G/H}$ donde $\pi\colon G \longrightarrow G/H$ es la proyección canónica.*
4. *Existe un morfismo $p\colon G \longrightarrow H$ tal que $pi = 1_H$ donde $i\colon H \longrightarrow G$ es la inclusión canónica.*

DEMOSTRACIÓN. $1) \Rightarrow 2)$ Como $G = H+K$ entonces todo $g \in G$ tiene una expresión $g = h+k$ con $h \in H$ y $k \in K$. Veamos la unicidad, suponemos que existe una segunda expresión $g = h'+k'$ con $h' \in H$ y $k' \in K$. Entonces $h+k = h'+k'$, de donde se sigue que $h-h' = k'-k \in H\cap K = 0$. Por lo que $h = h'$ y $k = k'$. Por lo tanto la expresión es única.

$2) \Rightarrow 3)$ Definimos $s(g+H) = k$ donde $h+k$ es la expresión de G. Veamos que esto no depende de la factorización. Si $g = h+k$ y $g' = h'+k'$ con $h,h' \in H$ y $k,k' \in K$ tal que $g+H = g'+H$. Entonces

$$k+H = h+k+H = g+H = g'+H = h'+k'+H = k'+H$$

Por lo que $k-k' \in H$ y de aquí $k-k'H\cap K = 0$. Se sigue que $k = k'$ Y la función esta bien definida. Calculando $\pi(s(g+H)) = \pi(k) = k+H = g+H$ para toda $g+H \in G/H$. Por lo tanto $\pi s = 1_{G/H}$.

3) $\Rightarrow$ 4) Considermos $q = s\pi \colon G \longrightarrow G$. Notemos que:

$$q^2 = qq = s\pi s\pi = s\pi = q$$

De aquí tenemos que si $e \colon im(q) \longrightarrow G$ es la inclusión canónica, entonces $qe = 1_{im(q)}$. Observemos que:

$$(1-q)^2 = 1 - 2q + q^2 = 1 - 2q + q = 1 - q$$

Por lo que analogamente si $\eta \colon im(1-q) \longrightarrow G$ es la inclusión canónica, entonces $(1-q)\eta = 1_{im(1-q)}$.

Basta ver que $im(1-q) = H$. Antes observemos que $nuc(q) = im(1-q)$ [tarea]

Para $h \in H$, tenemos que:

$$q(h) = s\pi(h) = s(h+H) = s(H) = 0$$

Por lo que el $H \subseteq nuc(q)$. Ahora sea $g \in nuc(q)$, entonces:

$$0 = q(g) = s\pi(g) = s(g+H)$$

Como s es monomorfismo, tenemos que $g + H = 0$. Lo que quiere decir que $g \in H$. Por lo tanto $nuc(q) = H$. $\square$

PROPOSICIÓN 2.3 (tarea). *Sea G un grupo y $\{H_i\}_{i\in I}$ una familia de subgrupos de G con $G = \sum_{i\in I} H_i$. Son equivalentes:*

1. *$\pi \colon \bigoplus_{i\in I} H_i \longrightarrow \sum_{i\in I} H_i$ es monomorfismo.*
2. *$\pi \colon \bigoplus_{i\in I} H_i \longrightarrow \sum_{i\in I} H_i$ es isomorfismo.*
3. *Todo elemento $x \in G$ no cero tiene una única expresión $\sum_{j=1}^{m} x_j$ con $x_j \in H_{i_j}$ para algún $i_j \in I$ con $x_j \neq 0$ para $j = 1, \dots m$.*
4. *Para todo $i \in I$, $H_i \cap \sum_{j\neq i} H_j = 0$.*

PROPOSICIÓN 2.4 (tarea). *Sea K un campo y V un K-espacio vectorial. Entonces V es isomorfo como grupo a $K^{(X)}$ para algún conjunto X.*

DEFINICIÓN 2.2. *Una sucesión de morfismo $\{f_i \colon G_i \longrightarrow G_{i+1}\}_{i=-\infty}^{\infty}$ es una sucesión exacta si $im(f_i) = nuc(f_{i+1})$ para todo $i \in \mathbb{Z}$. Una sucesión exacta corta es una sucesión exacta donde la lo más tres grupos son no triviales, por lo que se puede representar de la siguiente manera:*

$$0 \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow 0$$

Observamos que f es mono y G es epi.

DEFINICIÓN 2.3. *Una sucesión exacta corta* $0 \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow 0$ *decimos que se escinde si existe un morfismo* $h\colon G \longrightarrow G'$ *tal que* $hf = 1_{G'}$.

PROPOSICIÓN 2.5 (tarea). *Sea* $0 \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow 0$ *un sucesión exacta corta. Entonces la sucesión se escinde si y sólo si existe un morfismo* $l\colon G'' \longrightarrow G$ *tal que* $gl = 1_{G''}$

DEFINICIÓN 2.4. *Notacionalmente decir que las sucesiones* $0 \longrightarrow G' \xrightarrow{f} G$ *y* $G \xrightarrow{g} G'' \longrightarrow 0$ *son exactas nos referimos realemnte a las sucesiones exactas* $0 \longrightarrow G' \xrightarrow{f} G \xrightarrow{\pi} G/imf \longrightarrow 0$ *y* $0 \longrightarrow nuc(g) \xrightarrow{i} G \xrightarrow{g} G'' \longrightarrow 0$

EJEMPLO 2.1.

$$0 \longrightarrow p\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_p \longrightarrow 0$$

EJEMPLO 2.2.

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p} \mathbb{Z}_{p^2} \xrightarrow{\pi} \mathbb{Z}_p \longrightarrow 0$$

DEFINICIÓN 2.5. *Sea* G *un grupo y* $x_1, \ldots, x_n \in G$ *distinto de cero. Decimos que* $x_1, \ldots, x_n$ *son linealmente independientes si* $\sum_{i=1}^{n} m_i x_i = 0$ *con* $m_i \in \mathbb{Z}$*, entonces* $m_i x_i = 0$ *para* $i = 1, \ldots n$*. Sea* X *subconjunto de* G*. Decimos que* X *es linealmente independiente si todo subconjunto finito de* X *es linealmente independiente.*

PROPOSICIÓN 2.6. *Sea* G *un grupo y* X *un subconjunto de* G *que contiene al cero. Entonces* X *es linealmente independiente si y sólo si* $\langle X \rangle = \bigoplus_{x \in X} \langle x \rangle$.

DEMOSTRACIÓN. $\Rightarrow$) Notemos que siempre pasa que $\langle X \rangle = \sum_{x \in X} \langle x \rangle$. .Sea $x_0 \in X$ y $y \in \langle x_0 \rangle \cap \sum_{x \neq x_0} \langle .x \rangle$. Por lo que tenemos que $y = m_0 x_0$ y $y = \sum_{i=1} m_i x_i$ para algunas $x_i \in X \setminus \{x_0\}$ y $m_i \in \mathbb{Z}$ con $i = 0, \ldots, n$. De aquí́

$$m_0 x_0 - \sum_{i=1} m_i x_i = 0$$

Por la indepencia lineal, los $m_i x_i = 0$ para $i = 0, \ldots, n$. En particular, $y = m_0 x_0 = 0$. Por lo que $\langle x_0 \rangle \cap \sum_{x \neq x_0} \langle x \rangle = 0$.

$\Leftarrow$) Sean $x_1, \ldots, x_n \in X$ con $\sum_{i=1} m_i x_i = 0$. Entonces

$$m_j x_j = -\sum_{i \neq j} m_i x_i \in \langle x_j \rangle \cap \sum_{x \neq x_j} \langle x \rangle = 0$$

Por lo que $m_j x_j = 0$ para toda $j = 1, \ldots, n$. $\square$

DEFINICIÓN 2.6. *Sea G un grupo. Definimos la parte de torsión de G, $t(G)$, como el conjunto de los elementos orden finito. Los elementos de $t(G)$ se llaman elementos de torsión de G.*

PROPOSICIÓN 2.7. *Para todo grupo G, tG es un subgrupo de G.*

DEMOSTRACIÓN. El orden de 0 es finito. Si $a,b \in t(G)$ con $o(a) = n$ y $o(b) = m$, entonces $(m+n)(a+b) = 0$. Por lo que $o(a+b) \leq n+m$. Si $a \in G$, entonces $o(a) = o(-a)$. Por lo que si $a \in t(G)$, entonces $-a \in t(G)$. Por lo tanto $t(G) \leq G$. □

Observamos que si $f\colon G \longrightarrow H$ es un morfismo, entonces $f(t(G)) \subseteq t(H)$.

PROPOSICIÓN 2.8 (tarea). *La asignación t de grupos abelianos en grupos abelianos es un functor.*

DEFINICIÓN 2.7. *Sea G un grupo. Decimos que G es un grupo de torsión si $t(G) = G$. Decimos que G es libre de torsión si $t(G) = 0$.*

PROPOSICIÓN 2.9. *Sea G un grupo. Entonces $G/t(G)$ es un grupo libre de torsión.*

DEMOSTRACIÓN. Sea $x+t(G) \in t(G/t(G))$. Entonces existe un natural n tal que $n(x+t(G)) = 0$. Por lo que $nx \in tG$ De aquí existe un natural m tal que $nmx = 0$. Por lo tanto $x \in t(G)$ y $t(G/t(G)) = 0$. □

Una pregunta natural es si el subgrupo de torsión siempre es un sumando directo, pero esto es falso. Para esto ocuparemos la siguiente definición.

DEFINICIÓN 2.8. *Sea G un grupo, $x \in G$ y n un entero distinto de cero. Decimos que x es divisible por n, si existe $g \in G$ tal que $ng = x$.*

PROPOSICIÓN 2.10. *Sea P el conjunto de primos y $G = \prod_{p\in P} \mathbb{Z}_p$. Entonces $t(G)$ no es sumando directo de G.*

DEMOSTRACIÓN. Primero vemos que si $G = H \oplus t(G)$, entonces $H \cong G/t(G)$. Ahora notamos que para $q \in P$ y $\phi \in G$. Si $\phi \in G$ es divisible por q, entonces existe $\psi \in G$ tal que $q\psi = \phi$. En particular $\phi(q) = q\psi(q) = 0$. De aquí que si ϕ es divisible por todo primo, se sigue que $\phi = 0$.

Procedemos a ver que $G/t(G)$ tiene un elemento no cero que es divisible por todo primo, y así se tendría que H no puede ser isomorfo a $G/t(G)$. Consideramos $\phi \in G$ dado por $\phi(q) = 1$ para todo $q \in P$. En particular, ϕ tiene orden infinito, puesto que si $n\phi = 0$

tendríamos que $n\phi(q) = n1 = 0$ para todo $q \in P$. Por lo que $n = 0$. Por lo que $\phi \notin t(G)$ y $\phi + t(G) \neq 0$. Si q es un primo, entonces 1 es divisible por q en $\mathbb{Z}_p$ para $p \neq q$. Por lo que existe $g_p \in \mathbb{Z}_p$ tal que $qg_p = 1$ para toda $p \neq q$. Si ponemos a $g_q = 0$, podemos definir $\psi_q \in G$ como $\psi_q(p) = g_p$ para toda $p \in P$. De esta forma $\phi - q\psi \in t(G)$, puesto que en todas las entradas es cero excepto en q. Ahora:

$$q(\psi_q + t(G)) = q\psi_q + t(G) = \phi + t(G)$$

Por lo que $\phi + t(G)$ es divisible para toda $q \in P$. $\square$

DEFINICIÓN 2.9. *Sea p un primo y G un grupo. Definimos $T_p(G)$ como el conjunto de elementos g de G tal que que existe un natural n con $p^n g = 0$. A este conjunto lo llamamos la parte de p-torsión. También se le llama la componente p-primaria de G.*

PROPOSICIÓN 2.11. *La asignación T_p define un functor de la categoría de grupos en la categoría de grupos.*

PROPOSICIÓN 2.12 (Descomposición primaria). *Sea G un grupo finito. Entonces G es suma directa se sus componentes p-primarias*

DEMOSTRACIÓN. Como G es finito, entonces G tiene exponente n. Sea $n = p_1^{k_1} \dots p_m^{k_m}$ la descomposición en primos de n. Definimos $n_i = n/p^{k_i}$ y notamos que $(n_1, \dots, n_m) = 1$, es decir, estos números son primos relativos. Por lo que existen enteros $s_1, \dots, s_m \in \mathbb{Z}$ tales que $\sum_{i=1}^m s_i n_i = 1$. Por lo que se sigue que para $x \in G$, $x = \sum_{i=1}^m s_i n_i g$. Notamos que $p^{k_i} n_i s_i x = n s_i x = s_i 0 = 0$. Por lo que $n_i s_i x \in T_p(G)$. Por lo tanto $G = \sum_{i=1}^m T_{p_i}(G)$.

Sea $x \in T_{p_i}(G) \cap \sum_{j \neq i} T_{p_j}(G)$. Por un lado existe k_i tal que $p_i^{r_i} x = 0$ y por otro lado existen $x_j \in T_{p_j}(G)$ con $j \neq i$ tales que $x = \sum_{j \neq i} x_j$. Para cada x_j existe un natural r_j tal que $p_j^{r_j} x_j = 0$ para $j \neq i$. Si ponemos $r = \prod_{j \neq i} p_j^{r_j}$, entonces $(m, p_i^{r_i}) = 1$. Por lo que existen s y t enteros tales que $ms + p_i^{r_i} t = 1$. Por lo que $x = msx + p_i^{r_i} tx = 0 + 0 = 0$. Por lo tanto $T_{p_i}(G) \cap \sum_{j \neq i} T_{p_j}(G) = 0$. $\square$

PROPOSICIÓN 2.13. *Sea G un grupo de torsión. Entonces $G = \bigoplus_{p \in P} T_p(G)$.*

DEMOSTRACIÓN. Sea $x \in G$. Como G es un grupo de torsión, entonces existe un natural n tal que $nx = 0$. Sea $n = p_1^{k_1} \dots p_m^{k_m}$ la descomposición en primos de n. Definimos $n_i = n/p^{k_i}$ y notamos que $(n_1, \dots, n_m) = 1$, es decir, estos números son primos relativos. Por lo que existen enteros $s_1, \dots, s_m \in \mathbb{Z}$ tales que $\sum_{i=1}^m s_i n_i = 1$. Por lo que se sigue que para $x \in G$, $x = \sum_{i=1}^{m} s_i n_i g$. Notamos que $p^{k_i} n_i s_i x = n s_i x = s_i 0 = 0$. Por lo que $n_i s_i x \in T_p(G)$. Por lo tanto $G = \sum_{p \in P} T_p(G)$.

Sea $x \in T_{p_i}(G) \cap \sum_{j \neq i} T_{p_j}(G)$. Por un lado existe k_i tal que $p_i^{r_i} x = 0$ y por otro lado existen $x_j \in T_{p_j}(G)$ con $j \neq i$ tales que $x = \sum_{j \neq i} x_j$. Para cada x_j existe un natural r_j tal que $p_j^{r_j} x_j = 0$ para $j \neq i$. Si ponemos $r = \prod_{j \neq i} p_j^{r_j}$, entonces $(m, p_i^{r_i}) = 1$. Por lo que existen s y t enteros tales que $ms + p_i^{r_i} t = 1$. Por lo que $x = msx + p_i^{r_i} tx = 0 + 0 = 0$. Por lo tanto $T_{p_i}(G) \cap \sum_{j \neq i} T_{p_j}(G) = 0$. □

PROPOSICIÓN 2.14. *Sean G y H grupos de torsión. Entonces $G \cong H$ si y sólo si $T_p(G) \cong T_p(H)$ para toda $p \in P$.*

DEMOSTRACIÓN. $\Rightarrow$) Sea $f \colon G \longrightarrow H$ un isomorfismo. Como T_p es un funtor manda isomorfismos en isomorfismos.

$\Leftarrow$) Sea $\{f_p \colon T_p(G) \longrightarrow T_p(H)\}_{p \in P}$ una familia isomorfismos con la familia de sus inversa respectivas $\{g_p \colon T_p(H) \longrightarrow T_p(G)\}_{p \in P}$. Como $G = \bigoplus_{p \in P} T_p(G)$ y $H = \bigoplus_{p \in P} T_p(H)$. Definimos f como el morfimos inducido por la propiedad universal del coproducto de la familia $\{i_p^H f_p\}_{p \in P}$ y analogamente a g como el inducido por $\{i_p^G g_p\}_{p \in P}$. Se tiene que estos cumplen que $f i_p^G = i_p^H f_p$ y $g i_p^H = i_p^G g_p$. Notemos que

$$f g i_p^H = f i_p^G g_p = i_p^H f_p g_p = i_p^H 1_{T_p(H)}$$

y

$$g f i_p^G = g i_p^H f_p = i_p^G g_p f_p = i_p^G 1_{T_p(G)}$$

Por la unicidad de la propiedad universal tenemos que $fg = 1_H$ y $gf = 1_G$. Por lo tanto $G \cong H$. □

3. Grupos abelianos libres y proyectivos

En esta sección se van a analizar los conceptos de grupo abeliano libre así como el de grupo abeliano proyectivo, para los cuales se encontrará su relación. Asimismo se usará el material de esta sección para demostrar lo que se conoce como el Teorema Fundamental de los Grupos Abelianos Finitamente Generados.

3.1. Grupos abelianos libres. Como es de esperarse el concepto de grupo abeliano libre axiomatiza la idea de los grupos abelianos que tienen base. Este está relacionado con el concepto de grupo libre, sin embargo, en general dichos conceptos son diferentes. En esta subsección se va a ver esta relación, así como algunos resultados que comparten ambos conceptos. Es importante mencionar que en el caso de los grupos abelianos libres, muchos de los teoremas de grupos libres que son difíciles de demostrar tienen una prueba mas sencilla para estos. Dichas pruebas se discutirán en esta subsección.

DEFINICIÓN 3.1. *Un grupo abeliano F es* ***abeliano libre*** *si existe $X \subseteq F$ formado por elementos de orden infinito tal que $F \cong \bigoplus_{x\in X}\langle x\rangle$. A uno de tales subconjuntos X se le conoce como una base de F.*

Observaciones:

1. La definición anterior se suele parafrasear diciendo que los grupos abelianos libres son aquellos que son sumas directas de una familia de grupos cíclicos infinitos. Trivialmente, para cualquier conjunto X, el grupo $\mathbb{Z}^{(X)}$ es abeliano libre. Además se suele considerar $F = 0$ como el grupo abeliano libre con base $X = \emptyset$.[9]
2. Es muy importante mantener el nombre completo "grupo abeliano libre" para no confundir con los grupos libres estudiados en el capítulo 2, ya que estos tienen diferencias sustanciales y no son por lo general el mismo concepto. Esto se discutirá con más precisión posteriormente.
3. Si $X \subseteq F$ es base del grupo abeliano libre F, entonces por un resultado anterior todo elemento $g \in F$ se puede escribir de manera única como $g = \sum_{x\in X} m_x x$, con $m_x \in \mathbb{Z}$, que son todos cero salvo una cantidad finita de estos.
4. Los puntos 1 y 3 dicen que siempre es posible construir el grupo abeliano libre con base cualquier conjunto y que además este se puede identificar con el conjunto de combinaciones $\mathbb{Z}$-lineales (finitas) de elementos de X.

Tal y como sucedió con el concepto de grupo libre, el grupo abeliano libre tiene una propiedad categórica que lo determina salvo isomorfismo. Esta se presenta a continuación.

PROPOSICIÓN 3.1. *El grupo abeliano libre con base X, F, satisface la siguiente propiedad universal: Para todo grupo abeliano 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:*

$$\begin{tikzcd} X \arrow[r, "\iota"] \arrow[dr, "f"'] & F \arrow[d, dotted, "\overline{f}"] \\ & G \end{tikzcd}$$

DEMOSTRACIÓN. Quitando el caso obvio que ocurre cuando $X = \emptyset$, dado un grupo abeliano G y una función $f : X \to G$, defina $\overline{f} : F \to G$ mediante la regla de correspondencia $\overline{f}(\sum_{x\in X} m_x x) := \sum_{x\in X} m_x f(x)$. Por las observaciones anteriores $\overline{f}$ es una función, está bien definida y además claramente es un morfismo. Note que trivialmente se cumple que $\overline{f}|_X = f$.

[9]Recuerde que esto último es una cuestión que viene de la teoría de categorías.

Respecto a la unicidad, sea $g : F \to G$ otro morfismo tal que $g|_X = f$. Para ver que g coincide con $\overline{f}$ basta con ver que estos morfismos tienen la misma regla de correspondencia, para lo que observe que:

$$g(\sum_{x\in X} m_x x) = \sum_{x\in X} m_x g(x) = \sum_{x\in X} m_x f(x) =: \overline{f}(\sum_{x\in X} m_x x).$$

□

Retomando la observación realizada previamente a la proposición anterior, la propiedad universal anterior permite comenzar la comparación entre los conceptos de grupo libre y grupo abeliano libre, ya que esta muestra que si F es un grupo abeliano y es libre, entonces F es un grupo abeliano libre. Sin embargo, el regreso de la afirmación no es necesariamente cierto pues observe que la propiedad de extensión que da la propiedad universal correspondiente tiene una diferencia fundamental; mientras en el caso de grupos libres la extensión se hace respecto a cualquier función con codominio un grupo cualquiera, en el caso de los grupos abelianos libres se hace únicamente con funciones que tienen por codominio un grupo abeliano. Por otro lado, los grupos abelianos libres son sumas directas de grupos cíclicos infinitos, es decir, coproductos en la categoría de grupos abelianos de grupos cíclicos infinitos. Además, según el ejercicio 149, un grupo libre es producto libre de grupos cíclicos infinitos, es decir, un coproducto en la categoría de grupos. Esta última observación da la intuición de porqué estos conceptos no coinciden, ya que el coproducto en la categoría de grupos y en la categoría de grupos abelianos son distintos. En esta dirección, se tiene el siguiente resultado:

PROPOSICIÓN 3.2. *Sea $\{G_\alpha\}_{\alpha\in\Lambda}$ es una familia de grupos, entonces*

$$(*_{\alpha\in\Lambda} G_\alpha)_{ab} \cong \bigoplus_{\alpha\in\Lambda} (G_\alpha)_{ab}$$

DEMOSTRACIÓN. Lo que se va a ver es que $(*_{\alpha\in\Lambda} G_\alpha)_{ab}$ cumple la propiedad universal de $\bigoplus_{\alpha\in\Lambda}(G_\alpha)_{ab}$. Para esto, observe que si $\{\iota_\alpha : G_\alpha \to *_{\alpha\in\Lambda} G_\alpha\}_{\alpha\in\Lambda}$ es la familia de morfismos de inclusión de cada factor en el coproducto, entonces se tienen morfismos inducidos $\{(\iota_\alpha)_{ab} : (G_\alpha)_{ab} \to (*_{\alpha\in\Lambda} G_\alpha)_{ab}\}_{\alpha\in\Lambda}$. Para ver que $((*_{\alpha\in\Lambda} G_\alpha)_{ab}, (\iota_\alpha)_{ab})$ cumplen la propiedad universal mencionada, sea $\{f_\alpha : (G_\alpha)_{ab} \to H\}_{\alpha\in\Lambda}$ una familia de morfismos con H abeliano. Si $\pi_\alpha : G_\alpha \to (G_\alpha)_{ab}$ es el morfismo canónico de cada uno de los grupos de la familia en su abelianización, observe que $f_\alpha\pi_\alpha : G_\alpha \to H$, entonces por a propiedad universal del producto libre, existe un único morfismo de grupos $f' : *_{\alpha\in\Lambda} G_\alpha \to H$ tal que para cualquier $\alpha \in \Lambda$, $f'\iota_\alpha = f_\alpha\pi_\alpha$. Además, si $\pi : *_{\alpha\in\Lambda} G_\alpha \to (*_{\alpha\in\Lambda} G_\alpha)_{ab}$ es el morfismo canónico a la abelianización, existe un único morfismo $\hat{f} : (*_{\alpha\in\Lambda} G_\alpha)_{ab} \to H$ tal que $\hat{f}\pi = f'$.

Observe que por construcción $\hat{f}(\iota_\alpha)_{ab}\pi_\alpha = \hat{f}\pi\iota_\alpha = f'\iota_\alpha = f_\alpha\pi_\alpha$, como π_α es epi, entonces $\hat{f}(\iota_\alpha)_{ab} = f_\alpha$.

Para la unicidad, si $g : (*_{\alpha\in\Lambda}G_\alpha)_{ab} \to H$ es tal que para cualquier $\alpha \in \Lambda$, $g(\iota_\alpha)_{ab} = f_\alpha$, entonces $\hat{f}(\iota_\alpha)_{ab}\pi = g(\iota_\alpha)_{ab}\pi$, lo que implica que $\hat{f}\pi\iota_\alpha = g\pi\iota_\alpha$. Por la propiedad universal del producto libre, entonces $\hat{f}\pi = g\pi$, y como π es epi, entonces $\hat{f} = g$. $\square$

Esta discusión permite concluir lo siguiente:

PROPOSICIÓN 3.3. *Un grupo abeliano libre es libre si y sólo si es cíclico.*

Regresando a las analogías que existen entre los grupos libres y los grupos abelianos libres, lo que se quiere hacer es ver que la cardinalidad de la base de un grupo abeliano libre es un invariante de esta.

PROPOSICIÓN 3.4. *Sean F y F' grupos abelianos libres con bases X y Y respectivamente. Entonces, $F \cong F'$ si y sólo si $|X| = |Y|$.*

DEMOSTRACIÓN. El regreso de la afirmación es exactamente igual que en el caso libre, es decir, usando la propiedad universal, por lo que este se va a omitir. Para la ida supóngase que $F \cong F'$ y considere los grupos abelianos $V = F/2F$ y $W = F'/2F'$. Observe que en estos grupos abelianos hay una acción de $\mathbb{Z}_2$ que los dota con estructura de $\mathbb{Z}_2$-espacio vectorial. Considere los conjuntos $\beta = \{x+2F \mid x \in X\} \subseteq V$ y $\gamma = \{y+2F' \mid y \in Y\} \subseteq W$. Se afirma que estos son bases del espacio correspondiente. Para la prueba se va a tratar el caso de β pues para γ es análogo. En efecto, claramente β genera a V. Para la independencia lineal suponga que $\sum_{k=1}^{n}\lambda_k(x_k+2F) = 0+2F$, donde $\{x_1,\ldots,x_n\} \subseteq X$ y $\lambda_1,\ldots,\lambda_n$ son representantes de elementos en $\mathbb{Z}_2$. Dicha igualdad implica que $\sum_{k=1}^{n}\lambda_k x_k \in 2F$, de donde existen $x'_1,\ldots,x'_l \in X$ tales que $\sum_{k=1}^{n}\lambda_k x_k = \sum_{k=1}^{l}2m_k x'_k$, donde $m_1,\ldots,m_l \in \mathbb{Z}$. Por ser X base de F, se deduce que $l = n$ y que sin pérdida de generalidad puede suponerse que $x_k = x'_k$. Esto implica que para cualquier $k \in \{1,\ldots,n\}$, $\lambda_k = 2m_k$, lo que prueba que la clase de λ_k es cero en $\mathbb{Z}_2$, que es lo que se quería probar.

Para concluir, observe que $\dim_{\mathbb{Z}_2}(V) = |\{x+2F \mid x \in X\}| = |X|$ y análogamente $\dim_{\mathbb{Z}_2}(W) = |Y|$. Además observe que el isomorfismo de F y F' da lugar a un isomorfismo de $\mathbb{Z}_2$-espacios vectoriales entre V y W, luego, $|X| = \dim_{\mathbb{Z}_2}(V) = \dim_{\mathbb{Z}_2}(W) = |Y|$. $\square$

COROLARIO 3.1. *Cualesquiera dos bases de un grupo abeliano libre son equipotentes.*

La consecuencia directa del corolario anterior es que se puede definir el **rango de un grupo abeliano libre** F, el que se va a denotar por $rank_{\mathbb{Z}}(F)$, como el cardinal de cualquier base, el cual está bien definido por la proposición anterior. Observe además que si F y F' son grupos abelianos libres, entonces $F \oplus F'$ es un grupo abeliano libre con base la unión ajena de una base de F y una base de F'. Esto dice que,

$$rank_{\mathbb{Z}}(F \oplus F') = rank_{\mathbb{Z}}(F) + rank_{\mathbb{Z}}(F').$$

Es importante notar que la ecuación anterior es un claro análogo de la propiedad correspondiente para la dimensión de un espacio vectorial.

Además, observe que $rank_{\mathbb{Z}}(Z^{(X)}) = |X|$. Esto dice que la asignación rango de un grupo abeliano libre es suprayectiva al considerar como codominio la clase de todos los cardinales. En particular, la clase de grupos abelianos libres es propia.

Para concluir con la discusión del rango, se va a obtener una relación con el rango de un grupo libre. Esto se hace mediante el ejercicio 324, pues de este se deduce que

$$rank(F) = rank_{\mathbb{Z}}(F_{ab}).$$

Un argumento abstracto que muestra esta última afirmación se obtiene al usar el ejercicio 149, ya que si F es libre con base X, entonces $F \cong *_{x\in X}\langle x\rangle \cong *_{x\in X}\mathbb{Z}$. Así,

$$F_{ab} \cong (*_{x\in X}\mathbb{Z})_{ab} \cong \bigoplus_{\alpha\in X}\mathbb{Z}_{ab} \cong \bigoplus_{x\in X}\mathbb{Z} =: \mathbb{Z}^{(X)}.$$

Observe que de la relación anterior se puede demostrar que si F y F' son grupos libres, entonces

$$\begin{aligned} rank(F * F') &= rank_{\mathbb{Z}}((F * F')_{ab}) \\ &= rank_{\mathbb{Z}}(F_{ab} \oplus F'_{ab}) \\ &= rank_{\mathbb{Z}}(F_{ab}) + rank_{\mathbb{Z}}(F'_{ab}) \\ &= rank(F) + rank(F') \end{aligned}$$

Para concluir esta subsección vale la pena decir que como sucede en el caso libre, los grupos abelianos libres son importantes pues todo grupo abeliano se puede obtener como cociente de uno de estos. La prueba es básicamente igual que en el caso libre pues simplemente se usa la propiedad universal y tiene las mismas consecuencias, a saber, uno puede desarrollar una teoría de generadores y relaciones en el contexto abeliano. Sin embargo, para nuestros fines no es necesario desarrollar esta teoría.

3.2. Grupos abelianos proyectivos. El siguiente concepto que se va a trabajar en esta sección, se va a presentar con gran generalidad y se va a particularizar para el caso que nos interesa.

DEFINICIÓN 3.2. *Sea $\mathscr{C}$ una categoría. Decimos que $P \in \mathscr{C}$ es proyectivo si para cualesquiera morfismos $e : G \to H$ y $f : P \to H$, con e epi, existe un morfismo $g : P \to G$ tal que $eg = f$. Es decir, el siguiente diagrama conmuta*

$$\begin{tikzcd} & P \arrow[d, "f"] \arrow[dl, dotted, "g"'] \\ G \arrow[r, "e"'] & H \end{tikzcd}$$

Observación:

- El morfismo g de la definición no tiene porque ser único. Este tipo de propiedades donde no se tiene unicidad se suelen llamar propiedades universales débiles y observe que el no tener unicidad nos dice que estas no caracterizan a ningún objeto en especial, sino que son propiedades especiales que puede o no cumplir un objeto en una categoría.

De la definición anterior se deduce que un grupo abeliano es **proyectivo** si es un objeto proyectivo en la categoría de grupos abelianos. Así, el objetivo de esta sección es caracterizar dichos grupos. El primer paso en esta dirección, y que de hecho conecta la teoría con la subsección pasada, da los primeros ejemplos de objetos proyectivos.

PROPOSICIÓN 3.5. *Si F es un grupo abeliano libre, entonces F es proyectivo.*

DEMOSTRACIÓN. Observe que $F = 0$ cumple trivialmente la propiedad, por lo que suponga que F es no trivial. Considere morfismos $e : G \to H$ y $f : F \to H$ con e epimorfismo. Sea $X \subseteq F$ una base y observe que para cada $x \in F$, existe $g_x \in G$ tal que $e(g_x) = f(x)$, ya que en la categoría de grupos abelianos los epimorfismos son precisamente los morfismos suprayectivos. Dado que dicho elemento g_x no es necesariamente único, para cada $x \in X$ elija un único $g_x \in G$ con la propiedad mencionada. Observe que al definir la función $h : X \to G$ dada por $h(x) = g_x$, la propiedad universal del grupo abeliano libre implica que existe un único morfismo $\overline{h} : F \to G$ tal que $\overline{h}|_X = h$. Trivialmente se cumple que por construcción $e\overline{h} = f$, lo que concluye la prueba. $\square$

Es importante notar varias cosas de la proposición anterior. La primera es que en la prueba de esta se ve que el morfismo $\overline{g}$ no es único, pues si bien este es único cuando se fija una base, este depende de la base que se tome de F. Por otro lado, para la construcción de h

fue necesario usar el axioma de elección. Además observe que es sencillo adaptar la prueba anterior para ver que los grupos libres son objetos proyectivos en la categoría de grupos.

Anteriormente se mencionó que en una categoría un morfismo epi no tiene porque ser un epi que escinde. El siguiente resultado da una condición que tiene que ver con objetos proyectivos bajo la cual es válida dicha implicación.

PROPOSICIÓN 3.6. *Si $e : G \to P$ es un epimorfismo con $P \in \mathscr{C}$ proyectivo, entonces e es un epimorfismo que escinde.*

DEMOSTRACIÓN. Sea $e : G \to P$ epimorfismo con $P \in \mathscr{C}$ proyectivo. Al usar la propiedad que define a P para e como epimorfismo y $1_P : P \to P$, se deduce que existe $g : P \to G$ tal que $eg = 1_P$, lo que prueba la afirmación. $\square$

El siguiente resultado, que se deduce de los últimos dos, jugará un papel muy importante posteriormente, por lo que vale la pena enunciarlo.

COROLARIO 3.2. *Sea $H \leq G$ tal que G/H es abeliano libre. Entonces, $G \cong H \oplus G/H$.*

DEMOSTRACIÓN. Considere la proyección canónica $\pi : G \to G/H$, la cual es un epimorfismo. Como G/H es abeliano libre, entonces es proyectivo y así, π es un epimorfismo que escinde. Esto implica por un resultado anterior que $G \cong nuc(\pi) \oplus im(\pi) = H \oplus G/H$. $\square$

Uno de los resultados más importantes en los que se usa el corolario anterior, es un análogo al teorema de Nielsen-Schreir, pero para el caso de grupos abelianos libres. Este hace uso del teorema del buen orden y se presenta a continuación.

PROPOSICIÓN 3.7. *Si F es un grupo abeliano libre y $G \leq F$, entonces G es abeliano libre y además $rank_{\mathbb{Z}}(G) \leq rank_{\mathbb{Z}}(F)$.*

DEMOSTRACIÓN. Considere $\{x_k \mid k \in \Lambda\} \subseteq F$ una base, donde puede suponerse por el teorema del buen orden que Λ es bien ordenado. Defina para cada $k \in \Lambda$, $F'_k = \langle\{x_j \mid j < k\}\rangle$, $F_k = \langle\{x_j \mid j \leq k\}\rangle = F'_k \oplus \langle x_k\rangle$. Asimismo $G'_k = G \cap F'_k$ y $G_k = G \cap F_k$. Observe que $F = \bigcup_{k\in\Lambda} F_k$ y $G = \bigcup_{k\in\Lambda} G_k$. Dado que $G'_k = G \cap F'_k = G_k \cap F'_k$, entonces por el segundo teorema de isomorfismo y el teorema de la correspondencia biyectiva se tiene que:

$$G_k/G'_k = G_k/(G_k \cap F'_k) \cong (G_k + F'_k)/F'_k \leq F_k/F'_k \cong \mathbb{Z}$$

Esto dice que $G_k/G'_k = 0$ ó G_k/G'_k es cíclico infinito, lo que implica que $G_k = G'_k$ ó $G_k = G'_k \oplus \langle g_k \rangle$ por el corolario 3.2. Lo que se afirma es que G tiene por base $\{g_k\}$, donde observe que si se prueba esto, por la observación anterior se tiene que $rank_{\mathbb{Z}}(G) \leq |\Lambda| = rank_{\mathbb{Z}}(F)$, por lo que basta probar dicha afirmación.

Observe que dado que para cada $g \in G$ existe $k \in \Lambda$ tal que $g \in F_k$, al usar el hecho de que Λ es bien ordenado se puede definir $\mu(g) = \text{mín}\{k \in \Lambda \mid g \in F_k\}$. Considere $G^* = \langle \{g_k \mid k \in \Lambda\} \rangle \leq G$, donde en caso de que $G_k = G'_k$ defina $g_k = 0$. Si $G^* \lneq G$, entonces sea $\lambda = \text{mín}\{\mu(g) \mid g \in G \setminus G^*\}$ y considere $g \in G \setminus G^*$ tal que $\mu(g) = \lambda$. Entonces $g \in G \cap F_\lambda$, así que $g = a + mg_\lambda$ para $a \in G_\lambda$ y $m \in \mathbb{Z}$. Entonces $a \in G \setminus G^*$ y $\mu(a) < \lambda$, lo que sería una contradicción. Por lo tanto, $G = G^*$.

Para concluir la prueba, por un lema anterior basta con ver que las combinaciones de elementos en G son únicas, para lo cual basta con ver que si $\sum_{i=1}^n m_i g_{k_i} = 0$ con $k_1 < \cdots < k_n$, entonces cada $m_i = 0$. En efecto, si $m_n \neq 0$, entonces $m_n g_{k_n} \in \langle g_{k_n} \rangle \cap G'_{k_n} = 0$, lo que sería una contradicción. Así, G es abeliano libre. $\square$

Todos los resultado anteriores permiten caracterizar a los grupos abelianos proyectivos.

PROPOSICIÓN 3.8. *Los objetos proyectivos en la categoría de grupos abelianos son precisamente los grupos abelianos libres.*

DEMOSTRACIÓN. De la proposición 3.5 se deduce que basta con demostrar que todo grupo abeliano proyectivo es abeliano libre. En efecto, sea P uno de tales grupos. Observe que la función identidad, $1_P : P \to P$, da lugar a un morfismo de grupos $f : \mathbb{Z}^{(P)} \to P$ que es claramente un epimorfismo. Como P es proyectivo, entonces f es un epimorfismo que escinde, lo que dice que hay un morfismo $s : P \to \mathbb{Z}^{(P)}$ tal que $fs = 1_P$. Dado que s es mono, entonces $P \cong f(P)$ y $f(P) \leq \mathbb{Z}^{(P)}$. Dado que todo subgrupo de un grupo abeliano libre es abeliano libre, esto prueba que P es abeliano libre. $\square$

Por lo tanto, la proposición anterior dice que aunque los grupos abelianos proyectivos y los grupos abelianos libres tienen definiciones que aparentan ser distintas, estos son el mismo concepto. Además nótese que la prueba anterior se puede adaptar al caso no abeliano, lo que demuestra que en la categoría de grupos, los grupos proyectivos son precisamente los grupos libres.

Para concluir esta subsección se quiere discutir una caracterización más del concepto de proyectivo que tiene que ver solamente con la teoría de grupos abelianos y que es una caracterización con lenguaje categórico pues usa funtores representables, y que es una de las primeras ideas de álgebra homológica que se van a ver en el curso. Para esto se requiere del siguiente resultado:

LEMA 3.1. *Sea*

$$0 \longrightarrow G \xrightarrow{f} H \xrightarrow{g} K \longrightarrow 0$$

una sucesión exacta corta de grupos abelianos y $A \in \boldsymbol{Ab}$. Entonces, las siguientes sucesiones son exactas.

$$0 \longrightarrow h_A(G) \xrightarrow{h_A(f)} h_A(H) \xrightarrow{h_A(g)} h_A(K)$$

$$0 \longrightarrow h^A(K) \xrightarrow{h^A(g)} h^A(H) \xrightarrow{h^A(f)} h^A(G)$$

DEMOSTRACIÓN. Simplemente se va a demostrar que la primera sucesión es exacta pues para el segundo ejemplo la demostración es análoga. En efecto, la exactitud $h_A(G)$ es equivalente a probar que $h_A(f)$ es mono, lo que es equivalente a ver que el núcleo es cero. Sea $\alpha \in nuc(h_A(f))$. Entonces, $f\alpha = h_A(f)(\alpha) = 0$, lo que implica que $im(\alpha) \subseteq nuc(f) = \{0\}$, luego, $\alpha = 0$ y esto prueba la contención no trivial en la igualdad $nuc(h_A(f)) = \{0\}$.

Para la exactitud en $h_A(H)$, observe que es claro que $h_A(g)h_A(f) = h_A(gf) = h_A(0) = 0$, luego, $im(h_A(f)) \subseteq nuc(h_A(g))$. En lo que respecta a la contención restante, sea $\alpha \in nuc(h_A(g))$, es decir, $g\alpha = 0$. Esto implica que $im(\alpha) \subseteq nuc(g) = im(f)$, donde la igualdad se da por exactitud de la sucesión de la hipótesis. Así, observe que dado $x \in A$, $\alpha(x) = f(g_x)$ para algún $g_x \in G$. Además, como f es mono, dicho elemento g_x es único. Entonces esto permite definir una función $\beta : A \to G$ con la regla de correspondencia $\beta(x) = g_x$, si $\alpha(x) = f(g_x)$. Nótese que al ser α y f morfismos, se tiene que β lo es. Además, por construcción $\alpha = f\beta = h_A(f)(\beta)$, lo que prueba que $\alpha \in im(h_A(f))$, y concluye la prueba. □

A manera de comentario vale la pena decir que un funtor que cumple la propiedades del lema anterior, se conoce como funtor exacto izquierdo en el contexto del álgebra homológica. Si manda sucesiones exactas cortas a sucesiones exactas cortas a la derecha, se llamaría exacto derecho. Si dicho funtor mandara sucesiones exactas cortas en sucesiones exactas cortas, se llamaría exacto. Dejando de un lado esta terminología que tiene como propósito ir presentando conceptos muy importantes que aparecen en la teoría para irse familiarizando con ellos, el teorema buscado es:

PROPOSICIÓN 3.9. *Sea G un grupo abeliano. Las siguientes afirmaciones son equivalentes:*

1. *G es abeliano libre.*
2. *G es proyectivo.*
3. *$h_G : \boldsymbol{Ab} \to \boldsymbol{Ab}$ manda epimorfismos en epimorfismos*
4. *$h_G : \boldsymbol{Ab} \to \boldsymbol{Ab}$ manda sucesiones exactas cortas en sucesiones exactas cortas.*

DEMOSTRACIÓN. Se ha demostrado que 1 y 2 son equivalentes. Observe que 1 y 3 son equivalentes por definición. Para concluir 3 y 4 son equivalentes por el lema anterior. □

3.3. Un teorema fundamental. En esta sección se va a probar uno de los teoremas de estructura más importantes respecto a grupos abelianos finitamente generados. Su importancia es tal que se le conoce como el Teorema Fundamental de los Grupos Abelianos Finitamente Generados.

Para obtener este teorema se necesitan analizar algunos resultados respecto a grupos abelianos libres, así como un teorema de estructura para grupos finitos. Respecto a grupos abelianos libres ya no hay mucho que hacer pues ya se ha dedicado toda una subsección a ellos. Lo único que se necesita es un resultado que de entrada proporciona una fuente de ejemplos de grupos abelianos libres, el cual se presenta a continuación.

PROPOSICIÓN 3.10. *Todo grupo abeliano libre de torsión y finitamente generado, es abeliano libre.*

DEMOSTRACIÓN. La demostración es por inducción sobre el número de generadores de los grupos finitamente generados. Sea $G = \langle g_1, ..., g_n \rangle$ un grupo libre de torsión.

Base: $n = 1$. En este caso G es cíclico y como G es libre de torsión, entonces $G \cong \mathbb{Z}$, lo que concluye el resultado.

Paso inductivo: Supóngase que el resultado es válido para los grupos finitamente generados con menos de n generadores. Defina $H = \{g \in G \mid \exists m \in \mathbb{N}^+ (mg \in \langle g_n \rangle)\}$. Observe que $H \leq G$ y además G/H es libre de torsión ya que si $g + H \in t(G/H)$, entonces existe $k \in \mathbb{N}^+$ tal que $k(g+H) = 0 + H$, lo que implica que existe $m \in \mathbb{N}^+$ tal que $m(kg) \in \langle g_n \rangle$. Esto implica que $(mk)g \in \langle g_n \rangle$ y entonces $g \in H$, lo que implica que $g + H = 0 + H$ y prueba la afirmación.

Por otro lado G/H es finitamente generado y además tiene menos que n generadores, por lo que la hipótesis de inducción implica que G/H es abeliano libre, lo que implica que

$$G \cong H \oplus (G/H)$$

Para concluir con la prueba, basta con ver que H es abeliano libre. Para esto observe que como $H \cong G/(G/H)$, entonces H es finitamente generado. Por otro lado, observe que se puede definir una función $f : H \to \mathbb{Q}$, donde dado $g \in H$, se tiene que existen $m \in \mathbb{N}^+$ y $k \in \mathbb{Z}$ tales que $mg = kg_n$. En tal caso se define $f(g) = \frac{k}{m}$. Hay varias afirmaciones en torno a esta asignación.

Afirmación 1: f es función. Supóngase que $g \in H$ es tal que $mg = kg_n$ y $m'g = k'g_n$ para $m, m' \in \mathbb{N}^+$ y $k, k' \in \mathbb{Z}$. Entonces se tiene que $mm'g = mk'g_n$ y $m'mg = m'kg_n$, de donde $mk'g_n = m'kg_n$ y así $(mk' - m'k)g_n = 0$. Dado que G libre de torsión, entonces $mk' - m'k = 0$, lo que implica que $\frac{k'}{m'} = \frac{k}{m}$.

Afirmación 2: f es morfismo. Si $g, h \in H$ son tales que $mg = kg_n$ y $m'h = k'g_n$ para $m, m' \in \mathbb{N}^+$ y $k, k' \in \mathbb{Z}$, entonces $m'm(g+h) = (m'k + mk')g_n$. Así,

$$f(g+h) = \frac{m'k + mk'}{m'm} = \frac{k}{m} + \frac{k'}{m'} = f(g) + f(h)$$

Afirmación 3: f es monomorfismo. Si $g \in nuc(f)$, entonces $f(g) = 0$. Esto dice que $mg = 0$ para $m \in \mathbb{N}^+$. Dado que G es libre de torsión, esto implica que $g = 0$ y concluye la prueba.

Lo anterior prueba que H es isomorfo a un subgrupo finitamente generado de $\mathbb{Q}$. Haciendo la identificación de H con dicho subgrupo, supóngase que $H = \langle \frac{a_1}{b_1}, \ldots, \frac{a_l}{b_l} \rangle$. Entonces defina la asignación $h : H \to \mathbb{Z}$ tal que $h(x) = (\prod_{i=1}^{l} b_i)x$. Es claro que h es un morfismo de grupos inyectivo y así H se puede identificar con un subgrupo de $\mathbb{Z}$, el cual es abeliano libre y concluye la prueba. $\square$

El resultado buscado es:

PROPOSICIÓN 3.11. *(Teorema Fundamental de los Grupos Abelianos Finitamente Generados) Todo grupo abeliano finitamente generado es suma directa de grupos primarios y grupos ciclicos infinitos. El número de sumandos de cada uno de los grupos en cuestión, solamente depende del grupo en cuestión.*

DEMOSTRACIÓN. Sea G un grupo abeliano finitamente generado. Dado que G/tG es libre de torsión y finitamente generado, entonces G/tG es abeliano libre. Además, por el corolario 3.2, se deduce que

$$G \cong tG \oplus (G/tG)$$

Para concluir observe que dado que $tG \cong G/(G/tG)$, entonces tG es finitamente generado. Además, como los elementos en tG tienen orden finito, entonces tG es finito. Por lo tanto, tG es suma directa de grupos primarios. □

Es importante decir que puede refinarse el resultado anterior para conocer mejor la parte finita de dicha descomposición, que es la que proviene de las componentes primarias. Para esto se requiere de un resultado previo.

LEMA 3.2. *Si $G \leq F$ con F abeliano libre de rango n y $[F:G] < \aleph_0$, existen bases $\{x_1,\ldots,x_n\}$ bases de F y $\{g_1,\ldots,g_n\}$ de G tales que para cada $i \in \{1,\ldots,n\}$, $g_i \in \langle x_i \rangle$.*

DEMOSTRACIÓN. Tarea

□

El teorema de estructura buscado se muestra a continuación.

COROLARIO 3.3. *(Teorema de la base) Todo grupo abeliano finito es suma directa de grupos cíclicos finitos.*

DEMOSTRACIÓN. Sea G un grupo abeliano finito y nótese que $G \cong F/R$ con F un grupo abeliano libre finitamente generado y $R \leq F$ que trivialmente satisface que $[F:R] < \aleph_0$. Al usar el lema anterior se deduce que existen bases $\{x_1,\ldots,x_n\} \subseteq F$ y $\{y_1,\ldots,y_n\} \subseteq R$ tales que $y_i = k_i x_i$ para algún $k_i \in \mathbb{N}^+$. Entonces,

$$G \cong (\bigoplus_{i=1}^{n} \langle x_i \rangle)/(\bigoplus_{i=1}^{n} \langle y_i \rangle) \cong (\bigoplus_{i=1}^{n} \langle x_i \rangle)/(\bigoplus_{i=1}^{n} k_i \langle x_i \rangle) \cong \bigoplus_{i=1}^{n} \langle x_i \rangle / k_i \langle x_i \rangle \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{k_i}.$$

□

EJEMPLO 3.1. *El teorema de la base se puede usar para determinar los grupos abelianos de orden finito. Como ejemplo supóngase que se quieren determinar los posibles grupos abelianos de orden* 12*. El teorema anterior afirma que dado que* $12 = 2^2 \cdot 3$*, entonces al ser G productos de grupos cíclicos, las posibilidades que se tienen de la factorización son:*

$$\mathbb{Z}_{12}$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_3$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_6$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

Dado que $\mathbb{Z}_4 \oplus \mathbb{Z}_3 = \mathbb{Z}_{12}$ *y* $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$*, entonces las clases posibles son:*

$$\mathbb{Z}_{12} \text{ y } \mathbb{Z}_2 \oplus \mathbb{Z}_6$$

Este resultado empata con el ejercicio 288.[10]

Con los resultados anteriores se tiene todos los elementos para demostrar el teorema buscado.

De las observaciones anteriores se deduce que todo grupo finitamente generado se puede escribir de la forma

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_k},$$

donde $r = rank_{\mathbb{Z}}(G/tG)$ y $|tG| = \prod_{i=1}^{k} d_i$.

[10]Es común usar el símbolo de suma directa en lugar del de producto directo en el contexto abeliano cuando se tiene un producto finito. Esto se justifica en el hecho de que en la categoría de grupos abelianos los productos finitos y coproductos finitos coinciden.

4. Grupos Divisibles e Inyectivos

DEFINICIÓN 4.1. *Sea G un grupo. Decimos que G es divisible si para todo natural positivo n y $x \in G$, existe $g \in G$ tal que $ng = x$.*

EJEMPLO 4.1. *Los grupos $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son divisibles.*

EJEMPLO 4.2. *El grupo de los enteros $\mathbb{Z}$ no es divisible.*

EJEMPLO 4.3 (tarea). *Para todo natural n, $\mathbb{Z}_n$ no es divisible.*

De primera instancia parece complicado tener un grupo divisible de torsión. Pero estos existen aunque es un poco complicado de describirlos, como sea, estos tienen propiedades muy amigables que los hacen muy deseables.

DEFINICIÓN 4.2 (Grupo de Prufer). *Sea p un primo. Definimos $\mathbb{Z}_{p^\infty}$ como el grupo abeliano que tiene conjunto de generadores $\{x_i\}_{i=0}^{\infty}$ y relaciones $\{x_i - px_{i+1}\}_{i=0}^{\infty} \cup \{px_0\}$.*

PROPOSICIÓN 4.1 (tarea). *Sea p un primo. Entonces $\mathbb{Z}_{p^\infty}$ es un grupo de torsión.*

PROPOSICIÓN 4.2. *Sea p un primo. Entonces $\mathbb{Z}_{p^\infty}$ es divisble.*

DEMOSTRACIÓN. Sea $x \in \mathbb{Z}_{p^\infty}$ y k un natural positivo. Ponemos $x = \sum_{i=0}^{n} m_i \bar{x_i}$ notemos que por las relaciones podemos suponer que $0 \leq m_i < p$.

Primer caso $(k, p) = 1$. Entonces existen $s, t \in \mathbb{Z}$ tales que $sk + pt = 1$. Por lo que $ksm_n = m_n - ptm_n$ y de aquí

$$ksm_n\bar{x_n} = m_n\bar{x_n} - p\bar{x_n}tm_n = m_n\bar{x_n} - \bar{x_{n-1}}tm_n$$

Si ponemos $g_n = sm_n\bar{x_n}$, entonces procedemos a encontrar de forma análoga $g_{n-1} \in \mathbb{Z}_{p^\infty}$ tal que $kg_{n-1} = m_{n-1}\bar{x_{n-1}} - \bar{x_{n-1}}tm_n$. Notemos que esto lo podemos hacer usando la ecuación $sk + pt = 1$ y en cada paso agregamos un término a la ecución de índice menor inmediato. Hasta que se llega al término 0 donde el multiplicar por p anula el término extra y simplemente la ecuación queda resulta. Y tenemos que poniendo $g = \sum_{i=0}^{n} g_i$ se cumple que $kg = x$. □

PROPOSICIÓN 4.3. *Sea D un grupo divisible y $H \leq D$. Entonces D/H es divisible.*

DEMOSTRACIÓN. Sea n un natural positivo y $x + H \in D/H$. Entonces existe $g \in D$ tal que $ng = x$. Por lo que $n(g + H) = x + H$. Por lo tanto D/H es divisible. □

PROPOSICIÓN 4.4. *Sea $\{D_i\}_{i\in I}$ una familia de grupos divisible. Entonces $\prod_{i\in I} D_i$ es un grupo divisible.*

DEMOSTRACIÓN. Sean $\phi \in \prod_{i\in I} D_i$ y n un natural. Como cada D_i es divisible, entonces existe $g_i \in D_i$ tal que $ng_i = \phi(i)$. Si definimos $\psi \in \prod_{i\in I} D_i$ como $\psi(i) = g_i$ para toda $i \in I$. Entonces $n\psi = \phi$. Por lo tanto $\prod_{i\in I} D_i$ es divisible. □

PROPOSICIÓN 4.5 (tarea). *Sea $\{D_i\}_{i\in I}$ una familia de grupos divisible. Entonces $\bigoplus_{i\in I} D_i$ es un grupo divisible.*

PROPOSICIÓN 4.6 (tarea). *Sea $\{D_i\}_{i\in I}$ una familia de grupos. Si $\bigoplus_{i\in I} D_i$ o $\prod_{i\in I} D_i$ es un grupo divisible, entonces D_i es divisible para toda $i \in I$.*

DEFINICIÓN 4.3. *Sean G y H grupos. Decimos que G es H-inyectivo si para todo monomorfismo $\alpha\colon K \longrightarrow H$ y todo morfismo $f\colon K \longrightarrow G$ existe un morfismo $g\colon H \longrightarrow G$ con $g\alpha = f$. Decimos que G es inyecto si es H-inyectivo para todo grupo H.*

PROPOSICIÓN 4.7. *Sea D un grupo. Son equivalentes:*

1. *D es un grupo divisible.*
2. *$D = nD$ para todo natural positivo n.*
3. *$D = pD$ para todo primo p.*
4. *D es inyectivo.*
5. *D es $\mathbb{Z}$-inyectivo.*
6. *El funtor $Hom(\_,D)$ es exacto.*
7. *D es sumando directo de todo grupo del que es subgrupo.*

DEMOSTRACIÓN. $1 \iff 2)$ Es la definición de divisible en lenguaje de conjuntos.

$2 \Rightarrow 3)$ Es un caso particular

$3 \Rightarrow 2)$ Usamos la descomposición de todo natural en primos.

$4 \Rightarrow 2)$ Sean $x \in D$ y n natural positivo, y buscamos $y \in D$ con $ny = x$. Consideramos $H = \mathbb{Z}x$ el subgrupo de D generado por x, y la inclusión canónica $i\colon H \longrightarrow D$. Procedemos por casos, si H es infinito o finito.

Primer caso, H es infinito. Consideramos el morfismo $f\colon H \longrightarrow \mathbb{Z}$ inducido por $f(x) = n$, usando que H es libre de rango uno. Este morfismo f es monomorfismo. Como D es inyectivo, entonces existe un morfismo $h\colon \mathbb{Z} \longrightarrow D$ tal que $hf = i$. Ahora,

$$nh(1) = h(n) = h(f(x)) = i(x) = x$$

Poniendo $y = h(1)$, tenemos que $ny = x$.

Segundo caso, H es finito. Si $|H| = k$, entonces consideramos $K = \mathbb{Z}_{nk}$ y el morfismo canónico $f\colon H \longrightarrow K$ dado por $f(x) = n$. Tenemos que f esta bien definido y f es monomorfismo. Y de aquí la demostración es análoga al caso anterior.

$5 \Rightarrow 4)$ Sean G un grupo , H un subgrupo de G y $f\colon H \longrightarrow D$ un morfismo. Consideramos la familia $\mathscr{S} = \{(K,h) \mid H \leq K \leq G, h\colon K \longrightarrow D, h|_H = f\}$. Podemos asignarle un orden parcial a $\mathscr{S}$ dado por $(S,h) \leq (S',h')$ si $S \subseteq S'$ y $h'|_S = h$. [Tarea ver qu es orden parcial].

Consideramos una cadena ascendente $\{(S_i,h_i)\}_{i=1}^{\infty}$ en $\mathscr{S}$ y ponemos $\bar{S} = \bigcup_{i=1}^{\infty} S_i$ y $\bar{h} = \bigcup_{i=1}^{\infty} h_i$. Notamos que $\bar{h}$ esta bien definida puesto que esta familia $\{(S_i,h_i)\}_{i=1}^{\infty}$ es compatible, y cumple que $(\bar{S},\bar{h}) \in \mathscr{S}$. Ahora, en la familia $\mathscr{S}$ toda cadena ascendente es acotada, por lo que existe un máximo (L,g). Queremos ver que $L = G$.

Suponemos que $L < G$. Entonces existe $z \in G$ tal que $z \notin L$, y ponemos $L' = L + \mathbb{Z}z$. Procedemos por casos.

Si $L \cap \mathbb{Z}z = 0$, entonces $L' = L \oplus \mathbb{Z}z$ por lo que podemos considera el morfismo $g \oplus 0$ dado por la propiedad universal. Notamos que $(L', g \oplus 0) \in \mathscr{S}$ y $(L,g) < (L', g \oplus 0)$ lo cual es una contradicción a que (L,g) es máximo.

Si $L \cap \mathbb{Z}z \neq 0$. Entonces tomamos n el menor natural positivo tal que $nz \in L$. Consideramos el morfismo $g|_{L \cap \mathbb{Z}z}$ el cual por hipotesis se extiende a uno $a\colon \mathbb{Z}z \longrightarrow D$. De aquí $h + a\colon L' \longrightarrow D$ esta bien definida, y regresando al caso anterior tenemos una contradicción a que (L,g) es máximo. La contradiccióon viene de suponer que $L < G$. Por lo tanto $L = G$ y D es inyectivo.

$1 \Rightarrow 5)$ Sea n un natural positivo (el caso $n = 0$ es trivial), $i\colon n\mathbb{Z} \longrightarrow \mathbb{Z}$ la inclusión canónica y $f\colon n\mathbb{Z} \longrightarrow D$. Como de D es divisible, entonces existe $y \in D$ tal que $ny = f(n)$. Por lo que si ponemos $g(1) = y$, tenemos un morfismo $g\colon \mathbb{Z} \longrightarrow D$ tal que $gi = f$.

$4 \Rightarrow 6)$ Sea $\alpha\colon G' \longrightarrow G$ un monomorfismo. Queremos ver que $Hom(\alpha,D)\colon Hom(G,D) \longrightarrow Hom(G',D)$ es un epimorfismo. Sea $f \in Hom(G',D)$ entonces existe $g \in Hom(G,D)$ tal que $g\alpha = f$. Pero $Hom(\alpha)(g) = g\alpha = f$.

$6 \Rightarrow 7)$ Sea $\alpha\colon D \longrightarrow G$ un monomorfismo, como $Hom(\alpha,D)\colon Hom(G,D) \longrightarrow Hom(D,D)$ es un epimorfismo. Entonces existe $g\colon G \longrightarrow D$ tal que $g\alpha = 1_D$.

$7) \Rightarrow 4)$ [tarea] $\square$

DEFINICIÓN 4.4. *Sea G un grupo. Definimos la parte divisible de G como $d(G) := \sum\{im(f) \mid f\colon D \longrightarrow G, D$ divisible $\}$. Notamos que $d(G)$ es divisible y en particular sumando directo de G. Llamamos a G reducido si $d(G) = 0$.*

PROPOSICIÓN 4.8. *Sea G un grupo. Entonces $d(G/d(G)) = 0$.*

DEMOSTRACIÓN. Como $G = d(G) \oplus G/d(G)$. Entonces todo morfismo $f\colon D \longrightarrow G/d(G)$ con D divisible induce uno $f^*\colon D \longrightarrow G$. Por lo que $im(f) \subseteq G \cap G/d(G) = 0$. Por lo que $f = 0$ y $d(G/d(G)) = 0$. $\square$

DEFINICIÓN 4.5. *Sea n un natural. Definimos $G[n] = \{g \in G \mid ng = 0\}$.*

PROPOSICIÓN 4.9 (tarea). *Sea n un natural. Entonces la asignación $\_[n]$ es un funtor.*

PROPOSICIÓN 4.10. *Sea G y H grupos de p torsíon (p-primarios) divisibles. Entonces $G \cong H$ si y sólo si $G[p] \cong H[p]$.*

DEMOSTRACIÓN. $\Rightarrow$) Se sigue de la funtorialidad de $\_[p]$.

$\Leftarrow$) Sea $f\colon G[p] \longrightarrow H[p]$ un isomorfismo y su extensión en un monomorfismo $f^*\colon G[p] \longrightarrow H$. Entonces existe $\phi\colon G \longrightarrow H$ tal que $\phi|_{G[p]} = f^*$.

Para la inyectividad, consideramos $x \in G$ y queremos ver que $\phi(x) = 0$ implica $x = 0$. Procedemos por inducción n sobre el exponente del orden de x. Si $n = 1$, entonces $x \in G[p]$. Por lo que $0 = \phi(x) = f(x)$ y así $x = 0$. Suponemos que x tiene orden p^{n+1} y $\phi(x) = 0$. Entonces px tiene orden p^n. Por lo que $\phi(px) = p\phi(x) = p0 = 0$. Por hipotesis de inducción $px = 0$. Esto contradice que el orden de x sea p^{n+1}. Por lo que $x = 0$ y ϕ es inyectivo.

Para la suprayectividad, procedemos por inducción sobre n sobre la afirmación. Si $y \in H$ y tiene orden p^n, entonces $y \in im\phi$. Si $n = 1$, entonces $y \in H[p]$, entonces $y \in im(f) \subseteq im(\phi)$. Si $y \in H$ tiene orden p^{n+1}, entonces $p^n y$ tiene orden p. Por lo que $p^n y \in H[p]$. Entonces existe $x \in G$ tal que $\phi(x) = p^n y$. De aquí existe $g \in G$ tal que $p^n g = x$. Así $p^n(y - \phi(g)) = 0$ y por hipotesis de inducción existe $z \in G$ tal que $\phi(z) = y - \phi(g)$. Despejando $\phi(z+g) = y$. $\square$

PROPOSICIÓN 4.11 (tarea). *Si D es divisible y libre de torsión. Entonces D es un $\mathbb{Q}$ espacio vectorial.*

PROPOSICIÓN 4.12 (tarea). *Si D es divisible. Entonces $t(D)$ es divisible.*

PROPOSICIÓN 4.13 (tarea). *Si D es divisible. Entonces $T_p(D)$ es divisible para todo primo p.*

PROPOSICIÓN 4.14. *Todo grupo divisible D es suma directa de copias de $\mathbb{Q}$ y de $\mathbb{Z}_{p^\infty}$ corriendo por diferentes primos.*

DEMOSTRACIÓN. Como $t(D)$ es divisible. Entonces $D = t(D) \oplus D/t(D)$. De aquí, $D/t(D)$ es divisible y libre de torsión por lo que es una suma directa de copias de $\mathbb{Q}$.

Por otro lado para todo primo p, Tenemos que $T_p(D)[p]$ es un $\mathbb{Z}_{|}$-espacio vectorial. Digamos de dimensión λ. Notemos que $G_p = \mathbb{Z}_{p^\infty}^{\lambda}$ cumple que $G_p[p]$ es un $\mathbb{Z}_{|}$-espacio vectorial de dimensión λ. Por lo que $G_p \cong T_p(D)[p]$. Así $T_p(D) \cong G_p$. Recordamos que todo grupo de torsión es suma directa de sus partes de p-torsión. $\square$

PROPOSICIÓN 4.15. *Todo grupo es un subgrupo de un grupo divisible.*

DEMOSTRACIÓN. Sea G un grupo. Entonces $G = F/R$ con F libre. Como F es libre entonces $F = \mathbb{Z}^{(X)}$ para algún X conjunto. Entonces $F = \mathbb{Z}^{(X)} \leq \mathbb{Q}^{(X)}$. De aquí

$$G = F/R = \mathbb{Z}^{(X)}/R \leq \mathbb{Q}^{(X)}/R$$

$\square$

5. Producto tensorial

Una de las formas de introducir el producto tensorial es exactamente la misma que en el caso del álgebra lineal: una forma de transformar funciones “bilineales” en morfismos. Para esto lo primero que se tiene que definir es el concepto de bilineal.

DEFINICIÓN 5.1. *Una función $f : G \times H \to K$ es $\mathbb{Z}$-bilineal (o $\mathbb{Z}$-biaditiva) si:*

1. *Para cualquier $g \in G$, la función $f(g, \_) : H \to K$ es un morfismo de grupos.*
2. *Para cualquier $h \in H$, la función $f(\_, h) : G \to K$ es un morfismo de grupos.*

Observación: Como es común señalar, en esta construcción hay que tener cuidado con el concepto de $\mathbb{Z}$-bilineal respecto al de ser morfismo, ya que observe que tiene todo el sentido del mundo preguntarse si una función $f : G \times H \to K$ es morfismo de grupos, ya que $G \times H$ tiene una estructura canónica de grupo. El detalle es que ambas definiciones no tienen nada que ver una con la otra en general.

EJEMPLO 5.1. *La función $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ cuya regla de correspondencia es $f(x, y) = xy$, es $\mathbb{Z}$-bilineal.*

EJEMPLO 5.2. *De forma más general recuerde que todo grupo abeliano tiene una acción de $\mathbb{Z}$. Esta acción permite definir una función $f : \mathbb{Z} \times G \to G$ con regla de correspondencia $f(n,x) = nx$, la cual es $\mathbb{Z}$-bilineal.*

DEFINICIÓN 5.2. *Sean G y H grupos abelianos. Un producto tensorial de G y H consta de un grupo abeliano, T, y una función $\mathbb{Z}$-bilineal, $\tau : G \times H \to T$, que cumplen la siguiente propiedad universal: Para cualquier función $\mathbb{Z}$-bilineal, $f : G \times H \to K$, existe un único morfismo de grupos $\hat{f} : T \to K$ tal que $\hat{f}\tau = f$. Es decir, el siguiente diagrama conmuta:*

$$\begin{tikzcd} G \times H \arrow[r, "\tau"] \arrow[dr, "f"'] & T \arrow[d, dotted, "\hat{f}"] \\ & K \end{tikzcd}$$

Como es de esperarse, se tiene el siguiente resultado.

PROPOSICIÓN 5.1. *Si el producto tensorial de dos grupos existe, este es único.*

Más aún, el producto tensorial siempre existe.

PROPOSICIÓN 5.2. *Dados G y H grupos abelianos, su producto tensorial existe.*

DEMOSTRACIÓN. Considere el grupo abeliano libre con base $G \times H$, $\mathbb{Z}^{(G\times H)}$, así como $K = \langle \{(g+g',h) - (g,h) - (g',h), (g,h+h') - (g,h) - (g,h')\}_{g,g' \in G\ h,h' \in H} \rangle$. Sea $T = \mathbb{Z}^{(G\times H)}/K$ y $\tau : G \times H \to T$ el morfismo $\tau = \pi\iota$, donde $\iota : G \times H \to \mathbb{Z}^{(G\times H)}$ la inclusión canónica y $\pi : \mathbb{Z}^{(G\times H)} \to T$ la proyección canónica.

Es claro de la construcción que τ es $\mathbb{Z}$-bilineal. Para la propiedad universal sea $f : G \times H \to K$ una función $\mathbb{Z}$-bilineal. Observe que por la propiedad universal del grupo abeliano libre, existe un único morfismo $\overline{f} : \mathbb{Z}^{(G\times H)} \to K$ tal que $\overline{f}\iota = f$. Se afirma que $K \subseteq nuc(\overline{f})$. Para probar esto, basta ver que cada uno de los generadores de K pertenecen a $nuc(\overline{f})$. Sean $g, g' \in G$ y $h \in H$, entonces

$$\begin{aligned}\overline{f}((g+g',h)-(g,h)-(g',h)) &= \overline{f}(g+g',h)-\overline{f}(g,h)-\overline{f}(g',h)\\ &= f(g+g',h)-f(g,h)-f(g',h)\\ &= 0\end{aligned}$$

Además, observe que la prueba para los generadores restantes es análoga. Luego, por el lema previo al primer teorema de isomorfismo, existe un morfismo $\hat{f}: T \to K$ tal que $\hat{f}\pi = \overline{f}$.

Para concluir observe que por construcción $\hat{f}\tau = f$. Por otro lado, si existe un morfismo $g : T \to K$ tal que $g\tau = f$, entonces $(g\pi)\iota = (\hat{f}\pi)\iota$. De la propiedad universal del grupo abeliano libre, estas igualdades implican que $g\pi = \hat{f}\pi$, y por ser π un epimorfismo se deduce que $g = \hat{f}$. $\square$

En virtud de los últimos dos resultados, el producto tensorial de G y H se denota por $G\otimes_{\mathbb{Z}} H$, mientras que $\otimes := \tau$ y $g\otimes h := \otimes(g,h)$. Para simplificar la notación, a lo largo de estas notas se va a escribir $G\otimes H := G\otimes_{\mathbb{Z}} H$.

Observación: De acuerdo a las construcciones, nótese que si $x \in G\otimes H$, entonces $x = \sum_{i=1}^{n} g_i \otimes h_i$ para algunos $g_1,\dots,g_n \in G$ y $h_1,\dots,h_n \in H$. No es cierto en general que $x \in G\otimes H$ implique que existen $g \in G$ y $h \in H$ tales que $x = g\otimes h$.

Algunos ejemplos concretos de productos tensoriales usuales se presentan a continuación.

EJEMPLO 5.3.

1. *Para cualquier grupo abeliano G, $\mathbb{Z}\otimes G \cong G$.*
2. *Para cualquier grupo abeliano G y $n \in \mathbb{N}^+$, $\mathbb{Z}_n \otimes G \cong G/nG$.*
3. *Para $n,m \in \mathbb{N}^+$, $\mathbb{Z}_n \otimes \mathbb{Z}_m \cong \mathbb{Z}_{(n,m)}$.*

Existen dos formas consideradas canónicas para demostrar los isomorfismos anteriores, a saber: viendo que el objeto que se quiere ver es isomorfo al producto tensorial en cuestión satisface la propiedad universal de dicho producto tensorial, o dando el isomorfismo directo. Para ejemplificarlas se van a ver ambos argumentos para el primer ejemplo.

DEMOSTRACIÓN. (G satisface la propiedad universal de $\mathbb{Z}\otimes G$) Lo que se quiere ver es que G cumple la propiedad universal de $\mathbb{Z}\otimes G$, para lo que primero se tiene que dar una función $\mathbb{Z}$-bilineal, $\tau : \mathbb{Z}\times G \to G$, la cual es por supuesto la dada por la acción canónica de $\mathbb{Z}$ en G. Ahora veamos que (G,τ) cumple la propiedad universal que se quiere, para lo que hay que considerar $g : \mathbb{Z} \times G \to H$ una función $\mathbb{Z}$-bilineal. Defina $\hat{f} : G \to H$ mediante la regla de correspondencia $\hat{f}(x) = g(1,x)$. Observe que $\hat{f}$ es claramente un morfismo de grupos. Por otro lado, $\hat{f}\tau, f : \mathbb{Z} \times G \to G$, por lo que para la igualdad buscada, basta con ver que estas funciones tienen la misma regla de correspondencia. En efecto, para $(n,x) \in \mathbb{Z} \times G$, se tienen las igualdades

$$\hat{f}\tau(n,x) = \hat{f}(nx) := g(1,nx) = g(n,x).$$

Para ver que $\hat{f}$ es el único morfismo con la propiedad anterior, suponga que $h : \mathbb{Z} \times G \to H$ es otro morfismo tal que $h\tau = g$. Nuevamente basta con ver que h y $\hat{f}$ tienen la misma regla de correspondencia, para lo que se tienen las igualdades:

$$h(x) = h\tau(1,x) = g(1,x) =: \hat{f}(x).$$

Así, la unicidad salvo isomorfismo del producto tensorial implica que $\mathbb{Z} \otimes G \cong G$. $\square$

DEMOSTRACIÓN. (Dando el isomorfismo explícito) Sea $f : \mathbb{Z} \times G \to G$ la función definida por la acción canónica de $\mathbb{Z}$ en G, la cual es $\mathbb{Z}$-bilineal. Por la propiedad universal del producto tensorial, existe un único morfismo de grupos $\hat{f} : \mathbb{Z} \otimes G \to G$ tal que $\hat{f}\otimes = f$. Lo que se afirma es que $\hat{f}$ es un isomorfismo, para lo que usando la caracterización de los isomorfismos en la categoría de grupos abelianos, probar esto es equivalente a ver que $\hat{f}$ es una función biyectiva. En efecto, observe que como f es obviamente suprayectiva y $\hat{f}\otimes = f$, entonces $\hat{f}$ es suprayectiva. Para la inyectividad, sea $x \in nuc(\hat{f})$. Entonces, existen $n_1, \ldots, n_k \in \mathbb{Z}$ y $x_1, \ldots, x_k \in G$ tales que $x = \sum_{i=1}^k n_i \otimes x_i$ y además, $\hat{f}(x) = 0$. Dado que $\otimes$ es $\mathbb{Z}$-bilineal, entonces $x = \sum_{i=1}^k 1 \otimes n_i x_i = 1 \otimes \sum_{i=1}^k n_i x_i$. Por otro lado, $0 = \hat{f}(x) = \hat{f}(1 \otimes \sum_{i=1}^k n_i x_i) = \sum_{i=1}^k n_i x_i$. Al sustituir esta última igualdad en la última expresión obtenida para x, se tiene que $x = 1 \otimes 0 = 0$, donde la última igualdad se da pues $\otimes$ es $\mathbb{Z}$-bilineal.

Observe que esto muestra que $nuc(\hat{f}) = \{0\}$ y por lo tanto, $\hat{f}$ es inyectiva, lo que concluye la prueba. $\square$

El producto tensorial da lugar a un par de funtores asociados a cualquier grupo abeliano G:[11]

[11]Dado que $G \otimes H \cong H \otimes G$, en realidad ambos funtores son el mismo, sin embargo, se requeriría hablar de categorías de funtores para realmente poder justificar esta observación, cosa que no haremos.

$$G \otimes \_ : \mathbf{Ab} \to \mathbf{Ab}$$

$$\_ \otimes G : \mathbf{Ab} \to \mathbf{Ab}$$

La asignación a nivel de objetos es obvia en cada caso. Para la asignación a nivel de morfismos se va a hacer una construcción un poco más general.[12] Sean $f : G \to H$ y $g : G' \to H'$ morfismos entre grupos abelianos. Observe que se tiene una función $h : G \times G' \to H \otimes H'$ con regla de correspondencia $h(x,y) = f(x) \otimes g(y)$, la cual es $\mathbb{Z}$-bilineal. Al usar la propiedad universal del producto tensorial, existe un único morfismo, el que se va a denotar por $f \otimes g : G \otimes G' \to H \otimes H'$, tal que $(f \otimes g)\otimes = h$, es decir, para cualquier $x \in G$ y $y \in G'$, $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$.

Con esta construcción es fácil ver que las asignaciones:

$$(G \otimes \_)(f) := 1_G \otimes f$$

$$(\_ \otimes G)(f) := f \otimes 1_G$$

completan la definición de dichos funtores y, satisfacen los axiomas correspondientes.

Antes de pasar a la definición que se busca, es muy importante mencionar que el producto tensorial satisface una propiedad extra que en el caso de la teoría de conjuntos satisface el producto de dos objetos y que se parafrasea diciendo que "el producto transforma funciones de dos variables en una función de una variable con codominio un conjunto de funciones". Este importante principio es un ejemplo de uno de los conceptos más importantes de la teoría de categorías pues proporciona un ejemplo de lo que es una adjunción. Este se menciona a continuación.

PROPOSICIÓN 5.3. *Sean G, H, K grupos abelianos. Entonces existe un isomorfismo de grupos,*

$$Hom_{\boldsymbol{Ab}}(G \otimes_{\mathbb{Z}} H, K) \cong Hom_{\boldsymbol{Ab}}(G, Hom_{\boldsymbol{Ab}}(H,K)).$$

DEMOSTRACIÓN. Tarea $\square$

A continuación se da la definición fundamental de esta sección.

DEFINICIÓN 5.3. *Sea G un grupo abeliano. Decimos que G es plano si el funtor $G \otimes \_ : \boldsymbol{Ab} \to \boldsymbol{Ab}$ manda sucesiones exactas cortas en sucesiones exactas cortas.*

[12]De hecho esta construcción permite definir un funtor de dos variables, sin embargo, dado que no se comentó nada acerca de producto de categorías, no podemos dicho funtor.

Usando la misma filosofía que se usó en el caso de grupos proyectivos, los ejercicios 378 y 384 permiten demostrar lo siguiente:

PROPOSICIÓN 5.4. *Sea G un grupo abeliano. Son equivalentes:*

1. *G es plano.*
2. *El funtor $G\otimes\_ : \boldsymbol{Ab} \to \boldsymbol{Ab}$ manda monos en monos.*
3. *El funtor $\_\otimes G : \boldsymbol{Ab} \to \boldsymbol{Ab}$ manda sucesiones exactas cortas en sucesiones exactas cortas.*
4. *El funtor $\_\otimes G : \boldsymbol{Ab} \to \boldsymbol{Ab}$ manda monos en monos.*

EJEMPLO 5.4. *Todo grupo abeliano proyectivo es plano.*

DEMOSTRACIÓN. Dado que todo grupo abeliano proyectivo es libre, entonces observe que dado $f : H \to K$ un mono, se tiene que como $G = \mathbb{Z}^{(X)}$, entonces $1_G \otimes f : G\otimes H \to G\otimes K$ corresponde mediante los isomorfismos $G\otimes H \cong H^{(X)}$ y $G\otimes K \cong K^{(X)}$ al morfismo $\bigoplus_{x\in X} f : H^{(X)} \to K^{(X)}$, el cual es claramente inyectivo. $\square$

Es importante decir que $\mathbb{Q}$ es un grupo abeliano plano que no es proyectivo. Por otro lado, como sucedió respecto a los grupos proeyctivos e inyectivos, que tienen una caracterización usando un funtor exacto, los grupos planos también caracterizan un tipo especial de grupos, los cuales han estudiado ya y que se presentan en el siguiente resultado.

PROPOSICIÓN 5.5. *Un grupo abeliano finitamente generado es plano si y sólo si es libre de torsión.*

DEMOSTRACIÓN. $\Rightarrow$) Sea G un grupo plano y considere el morfismo de inclusión $\iota : \mathbb{Z} \to \mathbb{Q}$. Entonces, el morfismo $1_G \otimes \iota : G\otimes\mathbb{Z} \to G\otimes\mathbb{Q}$ es mono. Esto dice que $G \cong \mathbb{Z}\otimes G$ es isomorfo a un subgrupo de $\mathbb{Q}\otimes G \cong \mathbb{Q}\otimes G/t(G)$, y como $\mathbb{Q}\otimes G/t(G)$ es libre de torsión, entonces G lo es.

$\Leftarrow$) Al usar el teorema fundamental de los grupos abelianos finitamente generados y el hecho de que G es libre de torsión, se tiene que $G \cong \mathbb{Z}^r$. El resultado se deduce del ejemplo anterior pues este isomorfismo dice que G es proyectivo. $\square$

Es importante decir que la hipótesis de generación finita no se requiere, es decir, el resultado vale en general. De hecho observe que en la ida no se usó dicha hipótesis. En lo que respecta al regreso, se puede ver que la afirmación general se puede reducir a la demostrada viendo que todo grupo abeliano es colímite (de hecho límite directo) de la familia de sus subgrupos finitamente generados. Dado que en el curso no se han verán colímites, dicha prueba no se puede completar, por lo que simplemente se enuncia el caso finitamente generado.

6. Ejercicios

Se recuerda que en esta parte de la tarea todos los grupos serán abelianos, por lo que se usa notación aditiva. Además, $\mathscr{C}$ denota una categoría arbitraría.

EJERCICIO 293. *Dar un ejemplo de una categoría donde todo morfismo es un isomofismo*

EJERCICIO 294. *Demuestre que si $A,B \in \mathscr{C}$ y existe un isomorfismo entre A y B, entonces hay una correspondencia biyectiva entre los isomorfismos entre A y B y los automorfismos de A.*[13]

EJERCICIO 295. *Sean $f \in Hom_{\mathscr{C}}(A,B)$ y $g \in Hom_{\mathscr{C}}(B,C)$. Demuestre lo siguiente:*

1. *Si gf es mono, entonces f es mono.*
2. *Si gf es mono que escinde, entonces f es mono que escinde.*
3. *Si gf es epi, entonces g es epi.*
4. *Si gf es epi que escinde, entonces g es epi que escinde.*

EJERCICIO 296. *Sea G un grupo abeliano. Demuestre que se tienen los siguientes isomorfismos de grupos:*

1. $Hom_{\mathbf{Ab}}(\mathbb{Z},G) \cong G$
2. $Hom_{\mathbf{Ab}}(\mathbb{Z}_n,G) \cong G[n]$

[13]Un automorfismo en una categoría es un isomorfismo con el mismo dominio y codominio.

DEFINICIÓN 6.1. *Decimos que $A \in \mathscr{C}$ es un* ***generador*** *si siempre que existen dos morfismos $g,h \in Hom_{\mathscr{C}}(B,C)$ tales que $g \neq h$, entonces existe $f \in Hom_{\mathscr{C}}(A,B)$ tal que $gf \neq hf$. Dualmente decimos que $A \in \mathscr{C}$ es un cogenerador si A es un generador en la categoría opuesta.*

EJERCICIO 297.

1. *Usar la definición de la categoría opuesta para escribir una definición explícita de lo que es un cogenerador en una categoría explicando lo más detalladamente posible tu respuesta.*
2. *Demuestre que la categoría de grupos abelianos tiene un generador.*
3. *Demuestre que la categoría de grupos abelianos tiene un cogenerador.*

EJERCICIO 298. *Sean G y H grupos abelianos. Demuestre que $G \oplus H \cong H \oplus G$.*

EJERCICIO 299. *Sean G, H y K grupos abelianos. Demuestre que $G \oplus (H \oplus K) \cong (G \oplus H) \oplus K$.*

EJERCICIO 300. *Sean G, H, K grupos abelianos.*

1. *Supóngase que en una categoría $\mathscr{C}$ existen el producto y coproducto de cualesquiera dos objetos. Usar la propiedad universal del coproducto y del producto para demostrar que existe un morfismo de grupos $f : (G \times H) \coprod (G \times K) \to G \times (H \coprod K)$.*
2. *Usar el inciso anterior así como las definiciones del producto y coproducto de la categoría de grupos abelianos para obtener una regla de correspondencia explícita para dicho morfismo f. Argumenta tu respuestas.*
3. *Una categoría es distributiva si para cualesquiera tres objetos el morfismo construido en 1 es un isomorfismo. ¿Es la categoría de grupos abelianos una categoría distributiva?*

EJERCICIO 301. *Sea $\{G_\alpha\}_{\alpha \in \Lambda}$ una familia de grupos abelianos con Λ un conjunto. Demuestre que hay un isomorfismo en la categoría de grupos abelianos, $Hom_{\boldsymbol{Ab}}(G, \prod_{\alpha \in \Lambda} G_\alpha) \cong \prod_{\alpha \in \Lambda} Hom_{\boldsymbol{Ab}}(G, G_\alpha)$.*

EJERCICIO 302. *Sea* $\{G_\alpha\}_{\alpha\in\Lambda}$ *una familia de grupos abeliano con* Λ *un conjunto. Demuestre que hay un isomorfismo en la categoría de grupos abelianos* $Hom_{\boldsymbol{Ab}}(\bigoplus_{\alpha\in\Lambda} G_\alpha, G) \cong \prod_{\alpha\in\Lambda} Hom_{\boldsymbol{Ab}}(G, G_\alpha)$.

EJERCICIO 303. *Sea* $\{G_\alpha\}_{\alpha\in\Lambda}$ *una familia de grupos abelianos con* Λ *un conjunto y* $f : G \to \prod_{\alpha\in\Lambda} G_\alpha$ *un morfismo de grupos. Demuestre que* $nuc(f) = \bigcap_{\alpha\in\Lambda} nuc(\pi_\alpha f)$.

EJERCICIO 304. *Sea* $\{G_\alpha\}_{\alpha\in\Lambda}$ *una familia de grupos con* Λ *un conjunto y* $f : \bigoplus_{\alpha\in\Lambda} G_\alpha \to G$ *un morfismo de grupos. Demuestre que* $im(f) = \sum_{\alpha\in\Lambda} im(f\iota_\alpha)$

DEFINICIÓN 6.2. *Sea* $f : G \to H$ *un morfismo entre grupos abelianos. Un conúcleo de* f *es una pareja* (C, p) *con* C *un grupo abeliano y* $p : H \to C$ *un morfismo de grupos tales que* $p \circ f = 0$*. Además este satisface la siguiente propiedad universal: Para todo morfismo entre grupos abelianos* $g : H \to K$ *tal que* $g \circ f = 0$*, existe un único morfismo* $\hat{g} : C \to K$ *tal que* $\hat{g} \circ p = g$.

EJERCICIO 305.

1. *Demuestre que si existe un conúcleo de* f*, entonces este es único (salvo isomorfismo).*
2. *Demuestre que el conúcleo de un morfismo entre grupos abelianos siempre existe.*[14]
3. *Demuestre que* $f : G \to H$ *un morfismo de grupos es suprayectivo si y sólo si* $conuc(f) = 0$.

EJERCICIO 306. *Sean* $f : G \to H$ *y* $g : G \to K$ *morfismos entre grupos abelianos. Demuestre que existe un grupo abeliano* P *con morfismos* $i_1 : H \to P$ *y* $i_2 : K \to P$ *tales que* $i_1 \circ f = i_2 \circ g$ *y con la siguiente propiedad: Dado un grupo abeliano* L *con morfismos de grupos* $h_1 : H \to L$ *y* $h_2 : K \to L$ *tales que* $h_1 \circ f = h_2 \circ g$*, existe un único morfismo de grupos* $h : P \to L$ *tal que* $h \circ i_1 = h_1$ *y* $h \circ i_2 = h_2$.

---

[14] Por los dos incisos de este ejercicio el conúcleo de f se denotará por $conuc(f)$.

EJERCICIO 307. *Sea $F : \mathscr{C} \to \mathscr{D}$ un funtor y $f \in Hom_{\mathscr{C}}(G,H)$. Demuestre que si f es un isomorfismo, entonces $F(f) \in Hom_{\mathscr{D}}(F(G),F(H))$ es un isomorfismo. ¿Es cierto el recíproco de esta afirmación?*

EJERCICIO 308. *Sea G un grupo abeliano y $\{H_i\}_{i\in I}$ una familia de subgrupos de G. Demuestre que la función $\pi\colon \bigoplus_{i\in I} H_i \longrightarrow \sum_{i\in I} H_i$ dada por $\pi(\phi) = \sum_{i\in I} \phi(i)$ para toda $\phi \in \bigoplus_{i\in I} H_i$, es un epimorfismo.*

EJERCICIO 309. *Sea G un grupo abeliano y $\{H_i\}_{i\in I}$ una familia de subgrupos de G con $G = \sum_{i\in I} H_i$. Demuestre que son equivalentes:*

1. *$\pi\colon \bigoplus_{i\in I} H_i \longrightarrow \sum_{i\in I} H_i$ es monomorfismo.*
2. *$\pi\colon \bigoplus_{i\in I} H_i \longrightarrow \sum_{i\in I} H_i$ es isomorfismo.*
3. *Todo elemento $x \in G$ no cero tiene una única expresión $\sum_{j=1}^{m} x_j$ con $x_j \in H_{i_j}$ para algún $i_j \in I$ con $x_j \neq 0$ para $j = 1,\dots m$.*
4. *Para todo $i \in I$, $H_i \cap \sum_{j\neq i} H_j = 0$.*

EJERCICIO 310. *Sea $0 \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow 0$ un sucesión exacta corta. Demuestre que las siguientes afirmaciones son equivalentes:*

1. *Existe un morfismo $r\colon G \longrightarrow G'$ tal que $rf = 1_{G'}$*
2. *Existe un morfismo $l\colon G'' \longrightarrow G$ tal que $gl = 1_{G''}$*

EJERCICIO 311. *Demuestre que la asignación $t : \boldsymbol{Ab} \to \boldsymbol{Ab}$ que a cada grupo abeliano le asigna su subgrupo de torsión, es un funtor.*

EJERCICIO 312. *Sea G un grupo abeliano y $H \leq G$. Demuestre lo siguiente:*

1. *Si existe un morfismo $s\colon G/H \longrightarrow G$ tal que $\pi s = 1_{G/H}$ donde $\pi\colon G \longrightarrow G/H$ es la proyección canónica, y se define $q = s\pi$, entonces $nuc(q) = im(1-q)$.*
2. *Si existe un morfismo $p\colon G \longrightarrow H$ tal que $pi = 1_H$ donde $i\colon H \longrightarrow G$ es la inclusión canónica, entonces H es sumando directo de G.*

EJERCICIO 313. *Demuestre que para una sucesión exacta corta de grupos abelianos*

$$0 \longrightarrow G' \stackrel{\alpha}{\to} G \stackrel{\beta}{\to} G'' \longrightarrow 0$$

son equivalentes:

1. β *es epi que escinde.*
2. α *es mono que escinde.*
3. $im(\alpha)$ *es sumando directo de* G*.*
4. $nuc(\beta)$ *es sumando directo de* G*.*

EJERCICIO 314. *Sea la sucesión exacta de grupos abelianos*

$$G \stackrel{\alpha}{\to} H \stackrel{\beta}{\to} K \stackrel{\gamma}{\to} L$$

Demuestre que $H \cong im(\alpha) \oplus nuc(\gamma)$.

EJERCICIO 315. *Considérese una colección de subgrupos* $H' \leq H \leq G$ *y* $K' \leq K \leq G$*. Demuestre que hay una sucesión exacta corta de la forma*

$$0 \longrightarrow (H \cap K)/(H' \cap K') \longrightarrow H/H' \oplus K/K' \longrightarrow (H+K)/(H'+K') \longrightarrow 0$$

EJERCICIO 316. *Supóngase que en la siguiente diagrama en la categoría de grupos abelianos donde las sucesiones horizontales son exactas cortas y las flechas* f, g, h *hacen conmutar los cuadrados.*

$$\begin{tikzcd}
0 \arrow[r] & G \arrow[r] \arrow[d, "f"'] & H \arrow[r] \arrow[d, "g"'] & K \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & G' \arrow[r] & H' \arrow[r] & K' \arrow[r] & 0
\end{tikzcd}$$

Demuestre que:

1. *Si* f *y* h *son monomorfismos entonces* g *es monomorfismo.*
2. *Si* f *y* h *son epimorfismos entonces* g *es epimorfismo.*

3. Si f y h son isomorfismos entonces g es isomorfismo.

EJERCICIO 317. *Sea el siguiente diagrama en la categoría de grupos abelianos, donde las sucesiones horizontales son exactas y los cuadrados conmutan.*

$$\begin{tikzcd}
 & G \arrow[r, "\alpha"] \arrow[d, "f"'] & H \arrow[r] \arrow[d, "g"'] & K \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & G' \arrow[r] & H' \arrow[r, "\beta"'] & K' &
\end{tikzcd}$$

Demuestre que existe una sucesión exacta

$$nuc(f) \longrightarrow nuc(g) \longrightarrow nuc(h) \longrightarrow conuc(f) \longrightarrow conuc(g) \longrightarrow conuc(h)$$

Pruebe también que si α es mono, entonces la primera flecha en la sucesión es mono y que si β es epi la última flecha de la sucesión es epi.

EJERCICIO 318. *Demuestre que $t(G)$ es un grupo de torsión y $G/t(G)$ es un grupo libre de torsión.*

EJERCICIO 319. *Demuestre que a asignación que manda a cada grupo G en su componente p-primaria, da lugar a un funtor $T_p : \boldsymbol{Ab} \to \boldsymbol{Ab}$.*

EJERCICIO 320. *Sea $\{G_\alpha\}_{\alpha\in\Lambda}$ una familia de grupos con Λ un conjunto. Demuestre que $t(\bigoplus_{\alpha\in\Lambda} G_\alpha) \cong \bigoplus_{\alpha\in\Lambda} t(G_\alpha)$.*

EJERCICIO 321. *Demuestre que $\mathbb{Z}_n$ no es abeliano libre para todo $n > 1$.*

EJERCICIO 322. *Demuestre que $(\mathbb{Q}, +)$ no es abeliano libre.*

EJERCICIO 323. *(Baer-Specker) ¿Es $G = \prod_{i=0}^{\infty} \mathbb{Z} \cong \mathbb{Z}^{\mathbb{N}}$ un grupo abeliano libre?*

EJERCICIO 324. *Sea F un grupo libre con base X. Demuestre que F_{ab} es un grupo abeliano libre con base $\{x[F,F] \mid x \in X\}$.*

EJERCICIO 325. *Demuestre que en la categoría de conjuntos, todo elemento es proyectivo.*[15] *Usar esta afirmación para demostrar que en la categoría de conjuntos los epimorfismos y epimorfismos que escinden coinciden.*

DEFINICIÓN 6.3. *Un grupo abeliano G es un grupo de Whitehead si para cualesquiera grupo abeliano H y morfismos suprayectivos de grupos $f : H \to G$, existe $g : G \to H$ morfismo tal que $f \circ g = 1_G$.*

EJERCICIO 326. *Demuestre que todo grupo abeliano libre es un grupo de Whitehead. ¿Es cierta la proposición recíproca?*

EJERCICIO 327. *Sea $H \leq F$. Demuestre que si H y F/H son libres, entonces F es libre. De un contraejemplo para probar que el recíproco de esta proposición es falso.*

EJERCICIO 328. *Sea $n \in \mathbb{N}^+$ y una sucesión exacta de grupos abelianos libres de rango finito*

$$0 \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow 0$$

Demuestre que $\sum_{i=0}^{n}(-1)^i rank_{\mathbb{Z}}(F_i) = 0$.

EJERCICIO 329. *Sea G un grupo abeliano libre finitamente generado y $H \leq G$ tal que G/H es libre de torsión. Demuestre que $rank_{\mathbb{Z}}(G) = rank_{\mathbb{Z}}(H)$.*

[15] Vale la pena decir que en la prueba de esta afirmación se usa el axioma de elección. De hecho, se puede probar que el axioma de elección es equivalente a que todo conjunto sea proyectivo.

EJERCICIO 330. *Demuestre que si G es libre de torsión y tiene un subgrupo libre de índice finito, entonces G es libre.*

EJERCICIO 331.

1. *Sea $f \in Hom_{\mathscr{C}}(A,P)$ un mono que escinde con P proyectivo. Demuestre que A es proyectivo.*
2. *Sea $\{P_\alpha\}_{\alpha\in\Lambda}$ una familia de objetos proyectivos en una categoría $\mathscr{C}$ tal que el coproducto de dicha familia existe. Demuestre que $\coprod_{\alpha\in\Lambda} P_\alpha$ es proyectivo.*

EJERCICIO 332. *Para G y H grupos abelianos, demuestre que si $G\oplus H$ es proyectivo entonces G es proyectivo. Concluya que si para una familia de grupos $\{P_i\}_{i\in I}$ se tiene que $\bigoplus_{i\in I} P_i$ es proyectivo entonces para todo $i\in I$ se tiene que P_i es proyectivo.*

EJERCICIO 333. *Demuestre que si G es un grupo proyectivo entonces existe un grupo libre F tal que $G\oplus F\cong F$.*

EJERCICIO 334. *Sea*

$$0 \longrightarrow G \xrightarrow{f} H \xrightarrow{g} K \longrightarrow 0$$

una sucesión exacta corta de grupos abelianos y $A\in \boldsymbol{Ab}$. Demuestre que esta induce una sucesión exacta de la forma

$$0 \longrightarrow h^A(K) \xrightarrow{h^A(g)} h^A(H) \xrightarrow{h^A(f)} h^A(H)$$

EJERCICIO 335. *Demuestre que la sucesión siguiente es exacta*

$$G \xrightarrow{f} G' \xrightarrow{g} G'' \longrightarrow 0$$

si y sólo si para todo grupo abeliano A se tiene que la siguiente sucesión es exacta

$$0 \longrightarrow h^A(G'') \xrightarrow{h^A(g)} h^A(G') \xrightarrow{h^A(f)} h^A(G)$$

EJERCICIO 336. *Para $n \in \mathbb{N}^+$ considérese la sucesión exacta corta*

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\mu} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_n \longrightarrow 0$$

donde $\mu(x) = nx$ y $\pi(x) = [x]$. Por el ejercicio anterior esta induce una sucesión exacta

$$0 \longrightarrow Hom_{\mathbf{Ab}}(\mathbb{Z}_n, \mathbb{Z}) \xrightarrow{\pi^*} Hom_{\mathbf{Ab}}(\mathbb{Z}, \mathbb{Z}) \xrightarrow{\mu^*} Hom_{\mathbf{Ab}}(\mathbb{Z}, \mathbb{Z})$$

¿Quién es $conuc(\mu^*)$?

DEFINICIÓN 6.4. *Se dice que un conjunto $\{x_1, ..., x_n\}$ de elementos no cero en G es independiente si siempre que $\sum_{i=1}^n m_i x_i = 0$, con $m_i \in \mathbb{Z}$, se tiene que para todo $i \in \{1, ..., n\}$, $m_i x_i = 0$.*

EJERCICIO 337. *Demuestre las siguientes afirmaciones:*

1. *Si G es libre de torsión todo conjunto independiente es linealmente independiente (en el sentido usual, es decir, con escalares cero).*
2. *Si existe $p \in \mathbb{N}$ primo tal que $pG = 0$, entonces la noción de linealmente independiente en el sentido de grupos abelianos y linealmente independiente coinciden al pensar a G como $\mathbb{Z}_p$-espacio vectorial.*
3. *Si $\{x_1, ..., x_n\} \subseteq G$ es linealmente independiente con G un grupo p-primario y se define $\{y_1, ..., y_n\}$, donde $x_i = py_i$, entonces $\{y_1, ..., y_n\}$ es linealmente independiente.*
4. *Si $\{x_1, ..., x_n\} \subseteq G$ es linealmente independiente con G un grupo p-primario, entonces para todo $k_1, ..., k_n \in \mathbb{Z} \setminus \{0\}$ tales que $k_i x_i \neq 0$, se tiene que $\{k_1 x_1, ..., k_n x_n\}$ es linealmente independiente.*

EJERCICIO 338. *Demuestre que $\mathbb{Q}$ y $\mathbb{Z}_{p^\infty}$ no son finitamente generados.*

EJERCICIO 339. *Sea $H \leq G$. Demuestre que G es finitamente generado si y sólo si H y G/H son finitamente generados.*

EJERCICIO 340. *Sean G y H finitamente generados. Demuestre que* $G \cong H$ *si y sólo si* $G \oplus G \cong H \oplus H$.

EJERCICIO 341. *Demuestre lo siguiente: Si* $G \leq F$ *con F abeliano libre de rango n y* $[F:G] < \aleph_0$*, existen bases* $\{x_1,...,x_n\}$ *bases de F y* $\{g_1,...,g_n\}$ *de G tales que para cada* $i \in \{1,...,n\}$, $g_i \in \langle x_i \rangle$.

EJERCICIO 342. *Sean G, H y K finitamente generados. Demuestre que* $G \times H \cong G \times K$ *si y sólo si* $H \cong K$.

EJERCICIO 343. *Demuestre que un grupo proyectivo finitamente generado es libre.*

EJERCICIO 344. *Demuestre que si G es un grupo abeliano finito y* $|G|$ *es libre de cuadrados, entonces G es cíclico.*

EJERCICIO 345. *¿Es cierto que* $\mathbb{Q} \cong \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_k} \oplus \mathbb{Z}^n$ *para* $d_1,...,d_k \in \mathbb{N}^+$ *y* $n \in \mathbb{N}$*?.*

EJERCICIO 346. *Sea G un grupo abeliano finito no trivial. Demuestre que existen* $d_1,...,d_n \in \mathbb{N}^+$ *mayores a uno, tales que para cada* $i \in \{1,...,n-1\}$, $d_i | d_{i+1}$, *y*

$$G \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_n}.$$

Concluir que todo grupos abeliano finitamente generado se puede escribir de la forma $G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_n}$ *para* $d_1,...,d_n \in \mathbb{N}^+$ *mayores a uno tales que* $d_i | d_{i+1}$ *para cada* $i \in \{1,...,n-1\}$.

EJERCICIO 347. *Dmuestre que todo grupo abeliano finito no trivial, G, se puede escribir de la forma* $G \cong \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{k_n}}$*, donde* $k_1,...,k_n \in \mathbb{N}^+$ *y* $p_1,...,p_n \in \mathbb{N}$ *primos no necesariamente distintos entre sí.*

EJERCICIO 348. *Usar el Teorema Fundamental de los Grupos abelianos Finitamente Generados para demostrar que todo grupo abeliano de orden 30 es isomorfo a* $\mathbb{Z}_{30}$.

DEFINICIÓN 6.5. *Un grupo G es* ***indescomponible*** *si no existen $H, K \lneq G$ no triviales tales que $G \cong H \times K$.*

EJERCICIO 349. *Demuestre que todo grupo abeliano finito es indescomponible si y sólo si es cíclico de orden p, con $p \in \mathbb{N}$ un primo.*

EJERCICIO 350. *Demuestre que el funtor $h^{\mathbb{Q}/\mathbb{Z}} : \boldsymbol{Ab}^{op} \to \boldsymbol{Ab}$ satisface lo siguiente.*

1. *f es mono si y sólo si $h^{\mathbb{Q}/\mathbb{Z}}(f)$ es epi.*
2. *f es epi si y sólo si $h^{\mathbb{Q}/\mathbb{Z}}(f)$ es mono.*

EJERCICIO 351. *Pruebe que todo subgrupo propio de $\mathbb{Z}_{p^\infty}$ es finito y cíclico.*

EJERCICIO 352. *Sea p un primo. Demuestre que $\mathbb{Z}_{p^\infty}$ es un grupo de torsión y divisible.*

EJERCICIO 353. *Demuestre que $\mathbb{R}/\mathbb{Z} \cong \mathbb{T} \cong \prod_{p \in P} \mathbb{Z}_{p^\infty} \cong \mathbb{C}^* \cong \mathbb{R} \oplus \mathbb{Q}/\mathbb{Z}$, donde $P \subseteq \mathbb{N}$ es el conjunto de primos positivos.*

EJERCICIO 354. *Pruebe que un grupo de torsión no tiene sumandos directos si y sólo si es isomorfo a un subgrupo de $\mathbb{Z}_{p^\infty}$ para algún $p \in \mathbb{N}$ primo.*

EJERCICIO 355. *Demuestre que si a G se le encaja $\mathbb{Z}_{p^n}$ para toda $n \geq 1$ y ningún subgrupo propio de G tiene esta propiedad, entonces $G \cong \mathbb{Z}_{p^\infty}$.*

EJERCICIO 356. *Demuestre que todo grupo divisible libre de torsión tiene estructura de $\mathbb{Q}$-espacio vectorial.*

EJERCICIO 357. *Demuestre que todo grupo abeliano libre de torsión es una extensión de una suma directa de grupos cíclicos de un grupo divisible.*

EJERCICIO 358. *Demuestre que para* $\{G_i\}_{i\in I}$ *una familia de grupos abelianos se tiene que* $d(\bigoplus_{i\in I} G_i) \cong \bigoplus_{i\in I} d(G_i)$.

EJERCICIO 359. *Demuestre que si* $f : E \to D$ *es un epimorfismo con* E *divisible, entonces* D *es divisible. Use esta afirmación para probar que todo cociente de un grupo divisible es divisible.*

EJERCICIO 360. *Demuestre que si* $G \oplus H$ *es inyectivo entonces* G *es inyectivo.*

EJERCICIO 361. *Demuestre que* $\prod_{i\in I} E_i$ *es inyectivo si y sólo si para toda* $i \in I$, E_i *es inyectivo.*

EJERCICIO 362. *Sea* $\{D_i\}_{i\in I}$ *una familia de grupos divisibles. Demuestre que* $\bigoplus_{i\in I} D_i$ *es un grupo divisible.*

EJERCICIO 363. *Sea* $\{D_i\}_{i\in I}$ *una familia de grupos. Si* $\bigoplus_{i\in I} D_i$ *o* $\prod_{i\in I} D_i$ *es un grupo divisible, entonces* D_i *es divisible para toda* $i \in I$.

EJERCICIO 364. *Demuestre que la asignación* $d : \boldsymbol{Ab} \to \boldsymbol{Ab}$ *que a nivela de objetos asocia a cada grupo abeliano* G*, su parte divisible* $d(G)$*, es un funtor.*

EJERCICIO 365. *Demuestre que* $d(d(G)) = d(G)$ *y que* $d(G/d(G)) = 0$.

EJERCICIO 366. *Demuestre que si* G *es un grupo abeliano libre entonces* G *no es divisible.*

EJERCICIO 367. *Demuestre que si $D \leq G$ con D divisible entonces existe $H \leq G$ tal que $G = D \oplus H$.*

EJERCICIO 368. *Demuestre que dos grupos divisibles D y E son isomorfos si y sólo si $\dim_{\mathbb{Q}}(D/t(D)) = \dim_{\mathbb{Q}}(E/t(E))$ y $\dim_{\mathbb{Z}_p}(G[p]) = \dim_{\mathbb{Z}_p}(E[p])$ para todos los $p \in \mathbb{N}$ primos.*

EJERCICIO 369. *Sea $p \in \mathbb{N}$ un primo. Demuestre que un grupo G p-primario es divisible si y sólo si $pG = G$.*

EJERCICIO 370. *Demuestre que $G \cong H$ si y sólo si $d(G) \cong d(H)$ y $G/d(G) \cong H/d(H)$.*

EJERCICIO 371. *Demuestre que son equivalentes para un grupo G:*

1. *G es divisible.*
2. *Todo cociente no cero de G es infinito.*
3. *G no tiene subgrupos máximos.*

EJERCICIO 372. *Demuestre que si D y E son grupos divisibles tales que $D \oplus D \cong E \oplus E$ entonces $D \cong E$.*

EJERCICIO 373. *Demuestre lo siguiente:*

1. *Todo grupo libre de torsión se puede encajar en un $\mathbb{Q}-$espacio vectorial.*
2. *Si un conjunto máximo independiente de un grupo libre de torsión tiene n elementos, entonces G se encaja en un $\mathbb{Q}-$espacio vectorial de dimensión n.*

EJERCICIO 374. *Sea n un natural. Demuestre que la asignación $(\_)[n] : \textbf{Grp} \to \textbf{Grp}$ que a nivel de objetos asocia a G el grupo $G[n]$, es un funtor.*

EJERCICIO 375. *Demuestre que si D es divisible, entonces $t(D)$ es divisible.*

EJERCICIO 376. *Demuestre que si D es divisible, entonces $T_p(D)$ es divisible para todo primo p.*

EJERCICIO 377. *Demuestre que se tienen los siguientes isomorfismos donde G es un grupo abeliano cualquiera y $n,m \in \mathbb{N}^+$.*

1. $G \otimes \mathbb{Z}_n \cong G/nG$.
2. $\mathbb{Z}_n \otimes \mathbb{Z}_m \cong \mathbb{Z}_{(n,m)}$.

EJERCICIO 378. *Sean G y H grupos. Demuestre que $G \otimes H \cong H \otimes G$.*

EJERCICIO 379. *Sean G, H y K grupos. Demuestre que $G \otimes (H \otimes K) \cong (G \otimes H) \otimes K$.*

EJERCICIO 380. *Demuestre que para $\{G_i\}_{i \in I}$ una familia de grupos abelianos se tiene que $G \otimes (\bigoplus_{i \in I} G_i) \cong \bigoplus_{i \in I} G \otimes G_i$*

EJERCICIO 381. *Sean G, H, K grupos abelianos. Demuestre que existe un isomorfismo de grupos,*

$$Hom_{\boldsymbol{Ab}}(G \otimes_{\mathbb{Z}} H, K) \cong Hom_{\boldsymbol{Ab}}(G, Hom_{\boldsymbol{Ab}}(H, K)).$$

EJERCICIO 382. *Demuestre las siguientes afirmaciones:*

1. *El grupo abeliano $G \otimes_{\mathbb{Z}} \mathbb{Q}$ tiene estructura de $\mathbb{Q}$-espacio vectorial y además, existe un morfismo de grupos $\iota_1 : G \to G \otimes_{\mathbb{Z}} \mathbb{Q}$.*
2. *Existe un isomorfismo de grupos $G \otimes_{\mathbb{Z}} \mathbb{Q} \cong G/t(G) \otimes_{\mathbb{Z}} \mathbb{Q}$. ¿Es dicho isomorfismo un isomorfismo de $\mathbb{Q}$-espacios vectoriales?*
3. *Con la notación del ejercicio 1, dado cualquier morfismo de grupos $g : A \to B$ con B un $\mathbb{Q}$-espacio vectorial, existe una única transformación lineal $\hat{g} : G \otimes_{\mathbb{Z}} \mathbb{Q} \to B$ tal que $\hat{g}\iota_1 = g$.*

EJERCICIO 383. *Usar el ejercicio anterior para demostrar que existe un funtor* $(\_)_{\mathbb{Q}}$: $\boldsymbol{Ab} \to \mathbb{Q} - \boldsymbol{Vec}$. *A este funtor se le conoce como funtor de racionalización.*

EJERCICIO 384. *Demuestre que si la sucesión siguiente es exacta*

$$G \xrightarrow{f} G' \xrightarrow{g} G'' \longrightarrow 0$$

entonces para todo grupo abeliano H se tiene que la siguiente sucesión es exacta

$$G \otimes H \xrightarrow{f \otimes 1_H} G' \otimes H \xrightarrow{g \otimes 1_H} G'' \otimes H \longrightarrow 0$$

EJERCICIO 385. *Demuestre que toda imagen isomorfa de un grupo plano es un grupo plano.*

EJERCICIO 386. *Sea $\{G_i\}_{i \in I}$ es una familia de grupos abelianos con I un conjunto y supóngase que $G \cong \bigoplus_{i \in I} G_i$. Demuestre que G es plano si y sólo si para todo $i \in I$ se tiene que G_i es plano.*

DEFINICIÓN 6.6. *Para un grupo abeliano G se define el* ***subgrupo de Frattini*** *de G como $F(G) = \bigcap \{M \leq G \mid M$ es máximo$\}$.*

EJERCICIO 387. *Demuestre que $F(G) = \bigcap_{p \in \mathbb{P}} pG$, donde $\mathbb{P} \subseteq \mathbb{N}$ es el conjunto de primos positivos.*

EJERCICIO 388. *Sea $\{G_i\}_{i \in I}$ una familia de grupos con I un conjunto. Demuestre que $F(\bigoplus_{i \in I} G_i) \cong \bigoplus_{i \in I} F(G_i)$.*

EJERCICIO 389. *Sea G un grupo abeliano. Demuestre que para todo $p \in \mathbb{N}$ primo se tiene que $pG = \bigcap \{H \leq G \mid [G : H] = p\}$.*

EJERCICIO 390. *Demuestre que G es divisible si y sólo si $F(G) = G$.*

DEFINICIÓN 6.7. *Un grupo abeliano G se llama **acotado** si existe $n \geq 1$ tal que $nG = 0$.*

EJERCICIO 391. *Sea $G = \prod_{i \in I} G_i$ con cada G_i un subgrupo de torsión. Demuestre que si G es de torsión entonces G es acotado ó I es finito.*

DEFINICIÓN 6.8. *Se dice que $H \leq G$ es **puro** si para todo $n \in \mathbb{N}$ se tiene que $H \cap nG = nH$.*

EJERCICIO 392. *Demuestre que $t(G)$ es un subgrupo puro de G.*

EJERCICIO 393. *Demuestre que para G un grupo libre de torsión, $H \leq G$ es puro si y sólo si G/H es libre de torsión.*

DEFINICIÓN 6.9. *Un grupo abeliano se llama **simple-puro** si no tiene subgrupos puros propios.*

EJERCICIO 394. *Demuestre que si G es un grupo simple-puro entonces G se encaja en $\mathbb{Q}$ ó en $\mathbb{Z}_{p^\infty}$ para algún $p \in \mathbb{N}$ primo.*

EJERCICIO 395. *Demuestre que si G es abeliano de exponente acotado entonces G se descompone como suma directa de grupos cíclicos.*

EJERCICIO 396. *Sea $H \leq G$. Demuestre que H es puro si y sólo para todo K grupo, $H \otimes K \leq G \otimes K$.*

DEFINICIÓN 6.10. *Un grupo G es **fielmente plano** si es fiel y para todo H grupo abeliano tal que $G \otimes H = 0$ se tiene que $H = 0$.*

EJERCICIO 397. *Dar un ejemplo de un grupo plano que no sea fielmente plano.*

EJERCICIO 398. *Demuestre que las siguientes condiciones son equivalentes para un grupo G:*

1. *G es fielmente plano.*
2. *La sucesión siguiente es exacta*

$$H \xrightarrow{f} H' \xrightarrow{g} H''$$

si y sólo si la sucesión siguiente es exacta

$$G \otimes H \xrightarrow{1_G \otimes f} G \otimes H' \xrightarrow{1_G \otimes g} G \otimes H''$$

3. *G es plano y dado $f : H \to H'$ morfismo tal que $1_G \otimes f : G \otimes H \to G \otimes H'$ es el morfismo cero, se tiene que $f = 0$.*

EJERCICIO 399. *Un grupo abeliano G es fielmente plano si y sólo si G es libre de torsión y para todo $p \in \mathbb{N}$ primo se tiene que $pG \neq G$.*

EJERCICIO 400. *Demuestre que si G es un grupo plano y H un grupo fielmente plano entonces $G \oplus H$ es fielmente plano.*

EJERCICIO 401. *Sea la sucesión exacta corta*

$$0 \longrightarrow G \longrightarrow G' \longrightarrow G'' \longrightarrow 0$$

donde G y G'' son grupos reducidos. Demuestre que G' es reducido.

EJERCICIO 402. *Supóngase que existen $H, K \leq G$ y morfismos de grupos $f : H \to L$ y $g : K \to L$ tales que $f|_{H \cap K} = g|_{H \cap K}$. Demuestre que existe un único morfismo $h : H + K \to L$ que extiende a f y g.*

Capítulo 6

Introducción a la Cohomología de Grupos

“Las matemáticas son la música de la razón.”

James Joseph Sylvester.

1. Producto semidirecto

DEFINICIÓN 1.1. *Sean G y H grupos. Decimos que H es un G-módulo si existe un morfismo de grupos $\varphi : G \to Aut(H)$.*

Sean N un Q-módulo con morfismo de estructura $\varphi : Q \to Aut(N)$. Considere el producto $N \times Q$ y defina una operación binaria en dicho conjunto, $*$, como sigue:

$$(g,x) * (h,y) = (g\varphi(x)(h), xy)$$

Como se vio en el ejercicio 128, $(N \times Q, *)$ es un grupo cuyo neutro es el elemento (e,e) y $(g,x)^{-1} = (\varphi(x^{-1})(g^{-1}), x^{-1})$.

Dicho grupo se conoce como el **producto semidirecto** de N y Q, el cual se va a denotar por $N \rtimes_\varphi Q$. Otra notación usual es $N \times_\varphi Q$ y en algunos casos se suele omitir el morfismo de estructura y simplemente se escribe $N \rtimes Q$. En nuestro caso, para simplificar la notación no se usará el símbolo $*$ para el producto en $N \rtimes_\varphi Q$.

En el mismo ejercicio 128, se piede ver que $N \rtimes_\varphi Q$ tiene un subgrupo isomorfo a N, que como conjunto es $N \times \{e\}$, el cual es normal. Además, este grupo tiene un subgrupo isomorfo a Q que como conjunto es $\{e\} \times Q$, el cual no es necesariamente normal. Además, como la proyección en la segunda coordenada

$$\pi_2 : N \rtimes_\varphi Q \to Q$$

es un epimorfismo, entonces del primer teorema de isomorfismo se deduce que

$$(N \rtimes_\varphi Q)/N \cong Q$$

Por otro lado, observe que $N \rtimes_\varphi Q$ es el producto $N \times Q$ si y sólo si φ es trivial, es decir, es el morfismo constante con valor la identidad en N.

EJEMPLO 1.1. *Observe que hay una única estructura no trivial de $\mathbb{Z}_2$-modulo para $\mathbb{Z}_3$, $\varphi : \mathbb{Z}_2 \to Aut(\mathbb{Z}_3)$, donde $\varphi(1) = a^2$ con $\mathbb{Z}_3 = \langle a \rangle$. Dado que $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2$ tiene orden 6 y es claramente no abeliano, entonces $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2 \cong S_3$.*

EJEMPLO 1.2. *Considere $\mathbb{Z}_3 = \langle a \rangle$ y $\mathbb{Z}_4 = \langle x \rangle$. Sea $\varphi : \mathbb{Z}_4 \to Aut(\mathbb{Z}_3)$ el morfismo definido mediante $\varphi(x)(a) = a$, donde se está usando el isomorfismo $Aut(\mathbb{Z}_3) \cong U(\mathbb{Z}_3) \cong \mathbb{Z}_2$.*

Observe que $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ tiene orden 12. Además, al considerar $s := (a^2, x^2)$ y $t = (1, x)$, entonces se puede ver que $s^6 = e$ y $t^2 = s^3 = (st)^2$. Esto implica que $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4 \cong T$.

EJEMPLO 1.3. *Para $n \geq 3$, $D_n \cong \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$, donde $\varphi : \mathbb{Z}_2 \to Aut(\mathbb{Z}_n)$ es el morfismo $\varphi(-1)[x] = [-x]$, donde se usa que $\mathbb{Z}_2 \cong (\{-1, 1\}, \cdot)$. (Ver ejercicio 132)*

EJEMPLO 1.4. *Como se mencionó anteriormente, si $\rho : GL_n(\mathbb{R}) \to Aut(\mathbb{R}^n)$ es el morfismo inducido por la acción de $GL_n(\mathbb{R})$ en $\mathbb{R}^n$ y ρ' su restricción a $O(n)$, entonces se tienen los isomorfismos:*

$$Isom(\mathbb{R}^n) \cong Tr(\mathbb{R}^n) \rtimes_{\rho'} O(n)$$

$$Aff(\mathbb{R}^n) \cong Tr(\mathbb{R}^n) \rtimes_\rho GL_n(\mathbb{R})$$

En estos ejemplos se está usando el isomorfismo $\mathbb{R}^n \cong Tr(\mathbb{R}^n)$.

EJEMPLO 1.5. *(Ejercicio) Para k cualquier campo, se tiene que $GL_n(k) \cong k^* \rtimes_\varphi SL_n(k)$.*

Los ejemplos anteriores muestran la gran variedad de grupos que se pueden construir como productos semidirectos (sin contar los que son productos binarios, que son un caso especial de producto semidirecto). Hasta este momento, para ver que un grupo es producto semidirecto de un par de grupos, hay que encontrar el morfismo estructural que permita construir el producto semidirecto adecuado, lo cual puede ser no trivial. Uno de los objetivos de esta sección es dar una caracterización interna del producto semidirecto. Para esto hay que dar una discusión previa.

DEFINICIÓN 1.2. *Un subgrupo $H \leq G$ tiene un* ***pseudocomplemento*** *si existe $K \leq G$ tal que $H \cap K = \{e\}$ y $HK = G$.*

Observaciones:

1. Puede haber subgrupos que no necesariamente tengan un pseudocomplemento. Un ejemplo muy sencillo se obtiene al considerar para $p \in \mathbb{N}$ primo, $G = \mathbb{Z}_{p^2}$. Dado que existe $H \leq G$ con orden p, entonces H no puede tener un pseudocomplemento pues en caso contrario, dicho pseudocomplemento K implicaría que $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$, lo cual sabemos es imposible.
2. En caso de que un grupo tenga un pseudocomplemento, este puede no ser único.[1] Como ejemplo, observe que en $G = S_n$, todo subgrupo de orden 2, los cuales son generados por transposiciones, es complemento de A_n.
3. Si $N \trianglelefteq G$ con un pseudocomplemento, entonces este es único salvo isomorfismo como una consecuencia del segundo teorema de isomorfismo, ya que si Q es un pseudocomplemento, entonces

$$G/N = NQ/N \cong Q/(N \cap Q) \cong Q$$

Esto dice que todo pseudocomplemento es isomorfo a G/N.

Retomando el objetivo de esta sección, se requiere del siguiente resultado previo. Observe que este es un claro análogo de la proposición 2.2.

LEMA 1.1. *Sea $N \trianglelefteq G$. Las siguientes afirmaciones son equivalentes:*

1. *N tiene un pseudocomplemento en G.*
2. *Existe $Q \leq G$ tal que para cualquier $g \in G$, existe una única expresión $g = hx$ para únicos $h \in N$ y $x \in Q$.*
3. *Existe un morfismo $s : G/N \to G$ tal que $\pi s = 1_{G/K}$ (π es un epimorfismo que escinde).*
4. *Existe un morfismo $r : G \to G$ con $nuc(r) = N$ y para cualquier $x \in im(r)$, $r(x) = x$.*

DEMOSTRACIÓN. Se obtiene de adaptar la prueba de la proposición 2.2. □

A continuación se van a discutir los resultados principales de la presente sección.

PROPOSICIÓN 1.1. *Sea $\varphi : Q \to Aut(N)$ un morfismo. Si $G = N \rtimes_{\varphi} Q$, entonces N tiene un pseudocomplemento.*

[1] De esta observación se justifica el hecho de que la definición hable de un pseudocomplemento y no de un complemento

DEMOSTRACIÓN. Es claro que $N \cap Q = \{(e,e)\}$. Por otro lado, observe que dado $(g,x) \in G$, se tiene que $(g,e)+(e,x) = (g\varphi(e)(e), ex) = (g,x)$, lo que muestra la contención no trivial en la igualdad $NQ = G$. $\square$

El siguiente resultado dice que se satisface una especie de recíproco del resultado anterior.

PROPOSICIÓN 1.2. *Sea $N \trianglelefteq G$. Si existe un pseudocomplemento de N, Q, entonces $G \cong N \rtimes_\varphi Q$ para algún morfismo $\varphi : Q \to Aut(N)$.*

DEMOSTRACIÓN. Sea Q un pseudocomplemento de N. Defina $\varphi : Q \to Aut(N)$, mediante $\varphi(g)(x) = gxg^{-1}$, es decir, $\varphi = (\gamma_g)|_N$. De esta última observación se deduce que φ es morfismo y está bien definido por ser N normal. Así, se afirma que $G \cong N \rtimes_\varphi Q$. Para ver esto, defina $f : N \rtimes_\varphi Q \to G$ mediante $f(g,x) = gx$. Lo que se quiere ver es que f es un isomorfismo, para lo que se va a probar que este es un morfismo de grupos biyectivo.

En efecto, observe que por el lema 1.1 se deduce que todo $g \in G$ se escribe de forma única como $g = hx$ con $h \in N$ y $x \in Q$. Esta observación permite concluir que f es una función suprayectiva. Ahora veamos que f es un morfismo pues

$$\begin{aligned} f((g,x)(h,y)) &= f(g\varphi(x)(h), xy) \\ &= g\varphi(x)(h)xy \\ &= g(xhx^{-1})(xy) \\ &= (gx)(hy) \\ &= f(g,x)f(h,y) \end{aligned}$$

Para concluir, basta ver que f es un morfismo inyectivo, para lo que observe que dado $(g,x) \in nuc(f)$, se tiene que $gx = f(g,x) = e$, lo que implica por el lema 1.1 que $g = x = e$, de lo que se deduce la contención no trivial en la igualdad $nuc(f) = \{(e,e)\}$, lo que implica que f es inyectiva. $\square$

Observe que de la proposición anterior se puede justificar el por qué hay una notación para el producto semidirecto en el cual no se hace mención al morfismo estructural.

EJEMPLO 1.6. *De acuerdo a la observación dada en el ejercicio 405, se deduce de la proposición anterior que para $n \geq 3$, $S_n \cong A_n \rtimes \mathbb{Z}_2$.*

2. Cociclos

DEFINICIÓN 2.1. *Sea G un grupo y H un subgrupo de G. Una transversal (derecha) es un subconjunto T de G tal que $\{Ht\}_{t\in T}$ es una partición es de G, es decir, T contiene un único representante de las clases derechas de H en G.*

Notemos que por inducir una partición tenemos que todo $g \in G$ tiene una descomposición única $g = ht$ con $h \in H$ y $t \in T$

EJEMPLO 2.1. *Para $G = \mathbb{Z}$ y $H = 2\mathbb{Z}$, tenemos como ejemplos de transversales a $\{0,1\}$ y $\{28,35\}$.*

Si G es el producto semidirecto de H y K. Entonces K es una transversal de H en G.

DEFINICIÓN 2.2. *Sea $\pi\colon G \longrightarrow K$ un epimorfismo. Una función $l\colon K \longrightarrow G$ es un levantamiento si $\pi l = 1_K$. Esta función no tiene por que ser un morfismo. Notemos que la $T = im(l)$ es una transversal.*

PROPOSICIÓN 2.1. *Sea G una extensión de K por Q y $l\colon Q \longrightarrow G$ un levantamiento. Si K es un grupo abeliano, entonces la función $\theta\colon Q \longrightarrow Aut(K)$ dada por $\theta_x(a) = l(x)al(x)^{-1}$ es un morfismo de grupos. Más aún, si $l_*\colon Q \longrightarrow G$ es otra tranversal, entonces $l(x)al(x) = l_*(x)al_*(x)^{-1}$ para $a \in K$ y $a \in Q$.*

DEMOSTRACIÓN. Si consideramos $\gamma_g\colon G \longrightarrow G$ dado por $\gamma_g(x) = gxg^{-1}$ para toda $x \in G$, entonces $\gamma_g(K) = K$. Esto último por el hecho de que $K \trianglelefteq G$. Por lo que podemos restirngir y corestringir γ_g a K y llamamos este morfismo γ_g^K, y observamos que $\gamma_g^K \in Aut(K)$. Por lo cual podemos definir $\mu\colon G \longrightarrow Aut(K)$ dado por $\mu(g) = \gamma_g^K$. Como K es abeliano, entonces $K \leq nuc(\mu)$. Por lo que se induce un morfismo $\mu_K\colon G/K \longrightarrow Aut(K)$. Por el primer teorema de isomorfismo tenemos que $G/K \cong Q$, lo cual nos da el isomorfismo explicito $\lambda\colon Q \longrightarrow G/K$. Si $l\colon Q \longrightarrow G$ es una transversal, entonces $\lambda(x) = Kl(x)$. Si l_* es otra transversal, entonces $l(x)l_*(x)^{-1} \in K$. Por lo cual λ no depende de la transversal l. Si ponemos $\theta = \mu_K\lambda$. Entonces para $x \in Q$, tenemos que:

$$\theta_x = \mu_K\lambda(x) = \mu_K(Kl(x)) = \mu(l(x))$$

Para $a \in K$,

$$\theta_x(a) = \mu(l(x))(a) = l(x)al(x)^{-1}$$

$\square$

De lo anterior podemos concluir que K es un Q-conjunto.

DEFINICIÓN 2.3. *Decimos que una tripleta (Q,K,θ) es un dato si K es un grupo abeliano, Q es un grupo y $\theta\colon Q \longrightarrow Aut(K)$ es un morfismo. Decimos que un grupo G realiza el dato (Q,K,θ) si G es una extension de K por Q y cada transversal $l\colon Q \longrightarrow Q$ cumple que:*

$$xa = l(x)al(x)^{-1}$$

para $x \in Q$ y $a \in K$.

La proposición pasada nos dice que cada gupo G que sea una extensión de K por Q forma un dato que realiza G. El problema de la extensión es el siguiente, dado un dato (Q,K,θ) buscamos encontrar todos los grupos que realicen lel dato.

DEFINICIÓN 2.4. *Sea $\pi\colon G \longrightarrow Q$ un epimorfismo con nucleo K y $l\colon Q \longrightarrow G$ una transversal con $l(e) = e$. Una función $f\colon Q \times Q \longrightarrow K$ que cumple:*

$$f(x,y) = l(x)l(y)l(xy)^{-1}$$

es llamada un cociclo. El cociclo depende de la transversal l.

EJEMPLO 2.2. *En el caso en que G sea el producto semidirecto $K \rtimes_\theta Q$, entonces G consiste en las parejas $(a,x) \in K \times Q$ y producto dado por:*

$$(a,x)(b,y) = (ab^x, xy)$$

Si $l\colon Q \longrightarrow G$ es la transversal dada por $l(x) = (0,x)$, entonces l es un morfismo $l(x)l(y) = l(xy)$. En este caso su cociclo tiene que ser $f(x,y) = e$. Se puede pensar a un cociclo como una medida de G de que tanto se aleja de ser un producto semidirecto. Por lo que el también mide la obstrucción de la transversal l de ser un morfismo.

PROPOSICIÓN 2.2. *Sean $\pi\colon G \longrightarrow Q$ un epimorfismo con nucleo K, $l\colon Q \longrightarrow G$ una transversal tal que $l(e) = e$, y $f\colon Q \times Q \longrightarrow K$ su cociclo. Entonces:*

1. *$f(e,y) = e = f(x,e)$ para $x,y \in Q$.*

Identidad de cociclo *$f(x,y)f(xy,z) = xf(y,z)f(x,yz)$ para $x,y,z \in Q$.*

DEMOSTRACIÓN. 1. Calculando

$$f(e,y) = l(e)l(y)l(ey)^{-1} = el(y)l(y)^{-1} = e$$

y

$$f(x,e) = l(x)l(e)l(xe)^{-1} = l(x)el(x)^{-1} = e$$

para $x, y \in Q$.

2. Calculando

$$(l(x)l(y))l(z) = (f(x,y)l(xy))l(z) = f(x,y)f(xy,z)l(xyz)$$

y

$$\begin{aligned} l(x)(l(y)l(z)) &= l(x)(f(y,z)l(yz)) \\ &= l(x)f(y,z)l(x)^{-1}f(xy,z)l(xyz) \\ &= xf(y,z)f(xy,z)l(xyz) \end{aligned}$$

para $x, y, z \in Q$.

□

PROPOSICIÓN 2.3. *Dado un dato (Q,K,θ), una función $f\colon Q \times Q \longrightarrow K$ es un cociclo si y sólo*

$$xf(y,z)f(x,yx)^{-1}f(x,yz)f(x,y)^{-1} = e$$

y $f(x,e) = e = f(e,y)$ para todo $x, y \in K$. Más aún, existe G que realiza el dato y una transversal $l\colon Q \longrightarrow G$ que corresponde al cociclo f.

DEMOSTRACIÓN. Sea $G = K \times Q$ como conjunto y lo dotamos con la operación:

$$(a,x)(b,y) = (a(xb)f(x,y), xy)$$

para $(a,x),(b,y) \in K \times Q$.

Que G sea asociativa se sigue de la identidad de cociclo (tarea). El neutro es $(0,e)$. El inverso esta dado por:

$$(a,x)^{-1} = ((x^{-1}a)^{-1}(x^{-1}f(x,x^{-1}))^{-1}, x^{-1})$$

Definimos $\pi\colon G \longrightarrow Q$ como $\pi(a,x) = x$. Tenemos que π es un epimorfismo con nucleo $K \times e$. Obviamente K es isomorfo a $K \times e$. Por lo que K es normal en G y G es una extensión de K por Q. Falte ver que efectivamente G realiza el dato. Queremos ver que para cualquier transversal $l\colon Q \longrightarrow K$ tenemos que $ax = l(x)al(x)^{-1}$ con $x \in Q$ y $a \in K$. Para $x \in Q$ tenemos que $l(x) = (b,x)$ para algún $b \in K$. Así:

$$\begin{aligned} l(x)al(x)^{-1} &= (b,x)(a,e)(b,x)^{-1} \\ &= (b(ax),x)((x^{-1}b)^{-1}(x^{-1}f(x,x^{-1}))^{-1},x^{-1}) \\ &= (b(xa)(x(x^{-1}b)^{-1}(x^{-1}f(x,x^{-1}))^{-1}f(x,x^{-1}),e) \end{aligned}$$

Como K es abeliano entonces el último término se simplifica a (xa,e). Podemos identificar cualquier elemento xa con (xa,e) por lo cual G realiza el dato.

Si definimos la transversal $l\colon Q \longrightarrow K$ como $l(x) = (e,x)$ para $x \in Q$. Entonces el cociclo F satisface $F(x,y) = l(x)l(y)l(xy)^{-1}$. Pero haciendo cálculos concluimos que $F(x,y) = (f(x,y),e)$. Por lo que f es un cociclo.

□

Denotamos al grupo construido en la propositió anterior como G_f. Este realiza el dato (Q,K,θ) y tiene como cociclo f resultante de la transversal $l(x) = (e,x)$.

DEFINICIÓN 2.5. *Sea (Q,K,θ) un dato. Entonces $Z^2(Q,K,\theta)$ es conjunto de cociclos.*

PROPOSICIÓN 2.4. *Sea (Q,K,θ) un dato. Entonces $Z^2(Q,K,\theta)$ es un grupo abeliano.*

DEMOSTRACIÓN. La suma esta dada por $(f+g)(x,y) = f(x,y)+g(x,y)$ para $f,g \in Z^2(Q,K,\theta)$. El neutro es el cociclo correspondiente al producto semidirecto. □

Este grupo es relativamente muy grande. Dos transversales distintas dan a lugar cociclos distintos, pero a la misa extensión.

PROPOSICIÓN 2.5. *Sea G un grupo que realiza a $Z^2(Q,K,\theta)$ y sean l,l_* transversales con $l(e) = e = l_*(e)$ con cociclos f y f_*. Entonces existe una función $h\colon Q \longrightarrow K$ con $h(e) = e$ tal que $f_*(x,y)f(x,y)^{-1} = xh(y)h(xy)^{-1}h(x)$.*

Esta h es la que nos relaciona dos cociclos que realizan la misma extensión.

DEFINICIÓN 2.6. *Sea (Q,K,θ) un dato. Una cofrontera es una función $g\colon Q\times Q \longrightarrow K$ tal que existe una función $h\colon Q \longrightarrow K$ con $h(e) = e$ tal que $g(x,y) = xh(y)h(xy)^{-1}h(x)$. El conjunto de todas las cofronteras lo denotamos por $B^2(Q,K,\theta)$.*

PROPOSICIÓN 2.6. *Sea (Q,K,θ) un dato. Entonces $B^2(Q,K,\theta)$ es un subgrupo de $Z^2(Q,K,\theta)$.*

DEFINICIÓN 2.7. *Sea (Q,K,θ) un dato. Definimos*

$$H^2(Q,K,\theta) := Z^2(Q,K,\theta)/B^2(Q,K,\theta)$$

A este grupo lo llamamos el segundo grupo de cohomología.

3. Derivadas y el primer grupo de cohomología

En toda esta sección N es un grupo abeliano con estructura de Q-módulo dada por el morfismo $\varphi : Q \to Aut(N)$. En el lenguaje de la sección pasada, decir esto es equivalente a decir que se tiene un dato (Q,N,φ). Se usará la notación $xg := \varphi(x)(g)$. Además, por ser N un grupo abeliano, se usará notación aditiva para su operación, mientras que para Q se usará notación multiplicativa a no ser que se diga que Q es abeliano.

DEFINICIÓN 3.1. *Una* ***derivación o morfismo cruzado*** *es una función $d : Q \to N$ tal que para cualesquiera $x,y \in Q$,*

$$d(xy) = xd(y) + d(x).$$

EJEMPLO 3.1. *Dado $g \in N$, se define la función $d_g : Q \to N$ mediante la regla de correspondencia $d_g(x) = g - xg$. Esta función es una derivación ya que para $x,y \in Q$,*

$$d_g(xy) = g - (xy)g = x(g - yg) + (g - xg) = xd_g(y) + d_g(x).$$

A las derivaciones de la forma d_g se les conoce como ***derivaciones principales****. Observe que en particular $d_0 = 0$, es la derivación cero.*

Considere $Der(Q,N,\varphi)$ el conjunto de derivaciones $d : Q \to N$, asi como $PDer(Q,N,\varphi)$ el conjunto de derivaciones principales. La siguiente proposición dice que estos conjuntos tienen estructura de grupos abelianos.

PROPOSICIÓN 3.1. *El conjunto $Der(Q,N,\varphi)$ tiene estructura de grupo abeliano definiendo las operaciones de forma puntual. Además, con dicha estructura $PDer(Q,N,\varphi) \leq Der(Q,N,\varphi)$.*

DEMOSTRACIÓN. Para $d,d' \in Der(Q,N,\varphi)$, definir $d + d' : Q \to N$ mediante la regla de correspondencia $(d + d')(x) = d(x) + d'(x)$. Lo que se afirma es que $(Der(Q,N,\varphi),+)$ tiene estructura de grupo abeliano, para lo que primero se tiene que ver que $+$ está bien definida. En efecto, sean $d,d' \in Der(Q,N,\varphi)$. Para $x,y \in Q$,

$$\begin{aligned}(d+d')(xy) &:= d(xy)+d'(xy)\\ &= xd(y)+d(x)+xd'(y)+d'(x)\\ &= x(d(y)+d'(y))+(d(x)+d'(x))\\ &= x(d+d')(y)+(d+d')(x)\end{aligned}$$

Observe que la estructura de grupo abeliano de N se hereda a $Der(Q,N,\varphi)$ pues en este último conjunto la operación se definió de manera puntual, simplemente hay que observar que la derivación cero es el neutro en $Der(Q,N,\varphi)$ y que dada $d \in Der(Q,N,\varphi)$, $-d \in Der(Q,N,\varphi)$, lo cual es claro.

Para ver que $PDer(Q,N,\varphi) \leq Der(Q,N,\varphi)$, observe que la derivación cero es claramente principal. Por otro lado, si $d_g, d_h \in PDer(Q,N,\varphi)$, entonces observe que

$$(d_g - d_h)(x) = (g - xg) - (h - xh) = (g - h) - x(g - h) = d_{g-h}(x)$$

Esto prueba que $d_g - d_h \in PDer(Q,N,\varphi)$ y concluye la prueba de la afirmación. □

La proposición anterior permite dar la siguiente definición.

DEFINICIÓN 3.2. *Dado N un Q-módulo con N abeliano, se define el primer* ***grupo de cohomología*** *del dato* (Q,N,φ)

$$H^1(Q,N,\varphi) = Der(Q,N,\varphi)/PDer(Q,N,\varphi).$$

De la definición anterior no queda claro lo qué es el primer grupo de cohomología intuitivamente. Por supuesto que desde el punto de vista algebraico este mide qué tanto de aleja el grupo de derivaciones de ser el grupo de derivaciones principales. Con el propósito de ver la información que puede encerrar este grupo, se van a dar algunos resultados que permitan hacer algunos cálculos.

PROPOSICIÓN 3.2. *Suponga que $N \in$ **Ab** tiene estructura de Q-módulo trivial. Entonces, $H^1(Q,N,\varphi) \cong Hom_{\mathbf{Grp}}(Q,N)$.*

DEMOSTRACIÓN. Observe que en tal caso, para $g \in N$, $d_g(x) = g - xg = g - g = 0$. Esto dice que $PDer(Q,N,\varphi) = \{0\}$.

Por otro lado, observe que si $d \in Der(Q,N,\varphi)$, entonces para cualquier $x, y \in Q$, $d(xy) = xd(y) + d(x) = d(y) + d(x)$, por lo que esto dice que $d \in Hom_{\mathbf{Grp}}(Q,N)$. De hecho observe que trivialmente se tiene la contención en la otra dirección y por lo tanto, $Der(Q,N,\varphi) = Hom_{\mathbf{Grp}}(Q,N)$.

Esto permite concluir que:

$$H^1(Q,N,\varphi) \cong Der(Q,N,\varphi) = Hom_{\mathbf{Grp}}(Q,N)$$

□

Del resultado anterior y el ejercicio 72 se deducen los siguientes ejemplos particulares.

EJEMPLO 3.2. *Considere la acción trivial que hace de $\mathbb{Z}_{10}$ un $\mathbb{Z}_{21}$-módulo. Observe que $Hom_{\mathbf{Grp}}(\mathbb{Z}_{21}, \mathbb{Z}_{10}) = \{0\}$. Por lo tanto, en este caso:*

$$H^1(\mathbb{Z}_{21}, \mathbb{Z}_{10}, \varphi) \cong \{0\}.$$

EJEMPLO 3.3. *Considere la acción trivial que hace de $\mathbb{Z}_{12}$ un $\mathbb{Z}_{21}$-módulo. Observe que $Hom_{\mathbf{Grp}}(\mathbb{Z}_{21}, \mathbb{Z}_{12}) = \{f = 0, f = 4 \cdot \_\}$. Al considerar la estructura de grupo en este conjunto, se tiene que obviamente este es isomorfo a $\mathbb{Z}_2$. Por lo tanto, en este caso:*

$$H^1(\mathbb{Z}_{21}, \mathbb{Z}_{12}, \varphi) \cong \mathbb{Z}_2$$

EJEMPLO 3.4. *Cuando se considera la estructura trivial de $\mathbb{Z}_7$ como $\mathbb{Z}_{21}$-módulo, en este caso puede probarse que $Hom_{\mathbf{Grp}}(\mathbb{Z}_{21}, \mathbb{Z}_7)$ consta de todas las funciones que son producto con un representante de $\mathbb{Z}_7$. Esto dice que dicho grupo es cíclico con orden 7 y por lo tanto,*

$$H^1(\mathbb{Z}_{21}, \mathbb{Z}_7, \varphi) \cong \mathbb{Z}_7$$

Como se vio en la primera sección del presente capítulo, las estructuras de módulos para un par de grupos permiten construir el producto semidirecto de estos. La siguiente meta será la obtener algunos resultados que den herramientas para el cálculo del primer grupo de cohomología respecto su producto semidirecto.

Primero considere $G = N \rtimes_\varphi Q$. Si $\gamma : G \to G$ es un morfismo de estabilización, entonces observe que para cada $(g,x) \in G$,

$$\gamma(g,x) = (g + d(x), x)$$

Esto permite definir una función $d : Q \to N$ y más aún, $d \in Der(N,Q)$ al notar que:

$$\gamma((0,x)(0,y)) = \gamma(0,xy) = (d(xy),xy)$$

Por otro lado,

$$\gamma(0,x)\gamma(0,y) = (d(x),x)(d(y),y) = (d(x) + xd(y), xy)$$

La observación anterior da lugar a una asignación $f : A \to Der(Q,N,\varphi)$ mediante $f(\gamma) = d$, donde d es la derivación inducida por γ. Una pregunta interesante que se desprende de esta observación es si se puede decir algo de cuándo la derivada definida por un morfismo de estabilización es principal. La respuesta a esta pregunta se da en el siguiente resultado.

PROPOSICIÓN 3.3. *Para $G = N \rtimes_\varphi Q$, sea γ un morfismo de estabilización de G y $d \in Der(Q,N,\varphi)$ su derivación inducida. Entonces $d \in PDer(Q,N,\varphi)$ si y sólo si $\gamma \in Int(G)$.*

DEMOSTRACIÓN. $\Rightarrow$) Dado que existe $g \in N$ tal que $d = d_g$, entonces observe que

$$\begin{aligned}
(g,e)(h,x)(g,e)^{-1} &= (g+h,x)(-g,e) \\
&= (g+h-xg,x) \\
&= (h+d_g(x),x) \\
&= \gamma(h,x)
\end{aligned}$$

Esto demuestra que $\gamma = \gamma_{(g,e)}$.

$\Leftarrow$) Dado que $\gamma = \gamma_{(g,x)}$, observe que

$$\begin{aligned}
\gamma(0,y) &= (g,x)(0,y)(g,x)^{-1} \\
&= (g,xy)(-x^{-1}g,x^{-1}) \\
&= (g-xyx^{-1}g,xyx^{-1}) \\
&= (g-yg,y)
\end{aligned}$$

Como por otro lado $\gamma(0,y) = (d(y),y)$, entonces se deduce que $d(y) = g - yg$, lo que prueba la afirmación pues dice que $d = d_g$. $\square$

PROPOSICIÓN 3.4. *La función f es un isomorfismo de grupos entre A, el estabilizador de la extensión definida por (Q,N,φ), y $Der(Q,N,\varphi)$.*

DEMOSTRACIÓN. Para ver que f es morfismo, suponga que $\gamma,\gamma \in A$ tienen por derivaciones inducidas a $d,d' \in Der(Q,N,\varphi)$ respectivamente. Observe que para $(g,x) \in G$ se tiene que

$$\begin{aligned}
\gamma\gamma'(g,x) &= \gamma(g+d'(x),x) \\
&= (g+d'(x)+d(x),x) \\
&= (g+(d+d')(x),x)
\end{aligned}$$

Esto dice que $f(\gamma\gamma') = d+d'$, lo que prueba que f es un morfismo.

Para concluir la prueba, se va a ver que f es un biyectiva. Para la inyectividad observe que si $\gamma \in nuc(f)$, entonces $f(\gamma) = 0$, lo que implica que $\gamma = 1_G$. Esto prueba la contención no trivial en la igualdad $nuc(f) = \{1_G\}$, lo que dice que f es un morfismo inyectivo. Por otro lado, la suprayectividad se deduce del hecho de que dado $d \in Der(Q,N,\varphi)$, se tiene que $\gamma : G \to G$ definido por $\gamma(g,x) = (g+d(x),x)$, es un estabilizador y obviamente $f(\gamma) = d$. $\square$

El resultado buscado se presenta a continuación. Este dice que el primer grupo de cohomología se puede identificar como un subgrupo del grupo de automorfismos externos del producto semidirecto de los grupos en cuestión.

PROPOSICIÓN 3.5. *Para $G = N \rtimes_\varphi Q$, $H^1(Q,N,\varphi) \leq Aut(G)/Int(G)$.*

DEMOSTRACIÓN. Considere $f : A \to Der(Q,N,\varphi)$ el isomorfismo de la proposición anterior. Observe que por la proposición 3.3 se tiene que f induce un isomorfismo entre $A \cap Int(G) \to PDer(Q,N,\varphi)$. Luego,

$$\begin{aligned} H^1(Q,N,\varphi) &:= Der(Q,N,\varphi)/PDer(Q,N,\varphi) \\ &\cong A/(A \cap Int(G)) \\ &\cong (A + Int(G))/Int(G) \end{aligned}$$

Estos isomorfismos permiten dar la identificación buscada pues por el teorema de la correspondencia biyectiva, $(A + Int(G))/Int(G) \leq Aut(G)/Int(G)$. □

EJEMPLO 3.5. *Dado que $S_3 = \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2$, del resultado anterior se deduce que*

$$H^1(\mathbb{Z}_2, \mathbb{Z}_3, \varphi) \leq Aut(S_3)/Int(S_3)$$

Como se vio en el ejercicio 134 se tiene que $Aut(S_3) \cong S_3$. Por otro lado, se tiene que $Int(S_3) \cong S_3/Z(S_3) \cong S_3$. Luego, esto implica que

$$H^1(\mathbb{Z}_2, \mathbb{Z}_3, \varphi) \cong \{0\}$$

Para concluir se presentará un resultado que dice una interpretación en términos de extensiones para la situación en la que el primer grupo de cohomología sea trivial. Esta mejora el hecho de que dos pseudocomplementos de un subgrupo normal son isomorfos, dando un isomorfismo que puede considerarse canónico. Esta se va a escribir en notación aditiva en G para no confundir con la acción.

PROPOSICIÓN 3.6. *Si $G = N \rtimes_\varphi Q$ y $H^1(Q,N,\varphi) = 0$, entonces cualesquiera dos complementos de N son conjugados entre sí.*

DEMOSTRACIÓN. Sean C y C' complementos de N en G y considere $l : Q \to C$ y $l' : Q \to C'$ isomorfismos. Dado que C y C' son transversales en N de G, estos determinan cociclos $f, f' : Q \times Q \to N$, donde $l(x) + l(y) = f(x,y) + l(xy)$, y lo análogo para f'. Observe que como l y l' son morfismos, entonces $f = f' = 0$.

Por otro lado, por un lema anterior, la función $h : Q \to N$ con regla de correspondencia $h(x) = l'(x) - l(x)$, satisface que $f'(x,y) - f(x,y) = xh(y) - h(xy) + h(x)$. Esto implica que $h(xy) = x \cdot h(y) + h(x)$, lo que dice que $h \in Der(Q,N,\varphi)$, que al usar la hipótesis implica que $h \in PDer(Q,N,\varphi)$. Por lo tanto, existe $g \in N$ tal que $h = d_g$, lo que implica que

$l'(x) - l(x) = h(x) = g - xg$. De esto se deduce que $l'(x) = g + (-xg + l(x)) = g + l(x) - g$, lo que dice que $C' = g + C - g$, y que prueba la afirmación. $\square$

Para concluir, lo que se va a ver es que hay una forma de construir un funtor usando el primer grupo de cohomología. Para esto observe que si N es un Q-módulo y existe un morfismo de grupos $f : Q' \to Q$, entonces N adquiere una estructura de Q'-módulo al definir:

$$x \cdot g = f(x)g.$$

Considere entonces $f : Q' \to Q$ un morfismo de grupos y N un Q-módulo. Observe que si $d \in Der(Q,N,\varphi)$, la función $df \in Der(Q',N,\varphi f)$ ya que para $x,y \in Q'$,

$$df(xy) := d(f(xy)) = d(f(x)f(y)) = f(x)d(f(y)) + d(f(x)) = x \cdot df(x) + df(y).$$

Además, observe que si $d \in PDer(Q,N,\varphi)$, entonces $d = d_g$ para $g \in N$. Así, para $x \in Q$, se tiene que:

$$df(x) = d(f(x)) = g - f(x)g = g - x \cdot g.$$

Esto muestra que $df \in PDer(Q',N,\varphi f)$. Por lo tanto, se tiene un morfismo de grupos,

$$H^1(Q,N,\varphi) \to H^1(Q',N,\varphi f),$$

El cual se va a denotar por $H^1(N,f)$. Así, no es difícil ver que esto da lugar a un funtor

$$H^1(N,\_) : \mathbf{Grp}^{op} \to \mathbf{Ab}.$$

Como comentario final, en estos momentos el lector quizá pueda preguntarse en si se pueden definir grupos de n-cohomología para cuando $n \geq 3$. La respuesta es sí, sin embargo, para la construcción de estos se requiere de un formalismo que en estos momentos no se tiene, ya que estos se pueden construir a partir de la idea de funtor derivado. De hecho, todos los grupos de cohomología se pueden construir así, incluso los tratados en este capítulo, y estos son funtoriales automáticamente. En dicha teoría, las definiciones dadas en estas notas se vuelven teoremas, sin embargo, como se mencionó esta teoría sale de nuestro alcance y por ello es que no se abordó esta con toda generalidad y se tomó la perspectiva de hacer construcciones puntuales de algunos grupos, las cuales permiten decir varias cosas en dimensiones bajas pero que tienen el defecto de no verse cómo se extienden para los grupos de cohomología superior. Una segunda construcción se puede dar a partir de la topología algebraica usando la teoría de cohomología singular con coeficientes locales y la construcción del espacio clasificante de un grupo, por tal razón esta nuevamente sale de nuestro alcance.

4. Ejercicios

EJERCICIO 403. *Demuestre que si Q es un N-módulo con N y K solubles, entonces $N \rtimes_{\varphi} Q$ es soluble.*

EJERCICIO 404. *(Ejercicio) Para k cualquier campo, se tiene que $GL_n(k) \cong k^* \rtimes SL_n(k)$.*

EJERCICIO 405. *Sea $n \geq 3$. Demuestre que en S_n todo subgrupo generado por una transposición es un pseudocomplemento para A_n.*

EJERCICIO 406. *Demuestre que la asignación $H^1(N, \_) : \boldsymbol{Grp}^{op} \to \boldsymbol{Ab}$ es en efecto un funtor.*

Anexos

5. Retículas

DEFINICIÓN 5.1. *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 $x \leq z$*

Una notación común es escribir $(P, \leq)$ para un conjunto parcialmente ordenado con conjunto subyacente P y orden $\leq$.

EJEMPLO 5.1. *Sea X un conjunto. Entonces el conjunto potencia $\mathscr{P}(X)$ es un conjunto parcialmente ordenado con la contención $\subseteq$.*

DEFINICIÓN 5.2. *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 máximo es único y lo denotamos por $\bar{1}$.*

En el caso de $\mathscr{P}(X)$ su elemento máximo es X.

DEFINICIÓN 5.3. *Sea L un conjunto parcialmente ordenado. Decimos que L tiene un elemento mínimo x. Si para todo $y \in L$, $x \leq y$. Por la asimetría el elemento máximo es único y lo denotamos por $\bar{0}$.*

En el caso de $\mathscr{P}(X)$ su elemento mínimo es $\emptyset$.

DEFINICIÓN 5.4. *Sea L un conjunto parcialmente ordenado, $S \subseteq L$ y $a \in L$. Decimos que a es una cota superior de S, si $x \leq a$ para toda $x \in S$.*

En caso de S sea vacío, cualquier elemento de L es cota superior.

DEFINICIÓN 5.5. *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 5.1. *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 5.6. *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 5.7. *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 5.2. *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 5.8. *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 5.9. *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 5.1. *Sean L una retícula tal que existen todos los infimos. Entonces L es una retícula completa.*

DEFINICIÓN 5.10. *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 5.11. *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 5.12. *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.*

6. Lema de Zorn

El lema de Zorn, o Kuratowski-Zorn, es quizás el enunciado equivalente al axioma de elección que más se utiliza en álgebra pues permite garantizar la existencia de estructuras con alguna característica de maximalidad.

La meta de esta sección es enunciarlo, para lo cual se va a hacer una pequeña discusión.

DEFINICIÓN 6.1. *Sea $(P,\leq)$ un conjunto parcialmente ordenado y $S\subseteq P$. Decimos que S tiene un:*

1. *Elemento máximo si existe $x\in S$ tal que no existe $y\in S$ con la propiedad de que $x\lneq y$. En tal caso se dice que x es un elemento máximo.*
2. *Elemento mayor si existe $x\in S$ tal que para cualquier $y\in S$, $y\leq x$. En tal caso se dice que x es el mayor elemento de S.*

Es importante mencionar que en muchos libros de texto de habla hispana la primera de las definiciones presentadas se suele llamar elemento maximal y la segunda elemento máximo. La terminología seguida en estas notas es debida a Francisco Raggi quien comentaba que el término maximal es una mala traducción del inglés del concepto correspondiente. Mucha gente que pertenece a la escuela de Raggi usa la terminología, que es la que adoptaremos en estas notas.

Por otro lado el lector se imaginará como se definen los conceptos duales que son mínimo y menor elemento. Además recuerde que un conjunto puede tener muchos elementos máximos, pero tiene un único mayor elemento. Además, de que todo mayor elemento es un elemento máximo, pero el concepto de elemento máximo es más débil que el de elementos mayor, y lo análogo sucede con elementos mínimos y el menor elemento.

EJEMPLO 6.1. *Para $X=\{a,b,c\}$, si $P\subseteq\mathscr{P}(X)$ es el subconjunto formado por los subconjuntos propios de X, observe que $(P,\subseteq)$ es un conjunto parcialmente ordenado. Son elementos máximos los conjuntos $\{a,b\},\{a,c\},\{b,c\}$. Este conjunto parcialmente ordenado no tiene mayor elemento pero si tiene menor elemento a saber $\emptyset$. Observe que si $Q\subseteq\mathscr{P}(X)$ es el subconjunto formado por los subconjuntos propios de X no vacíos, se tienen los mismos máximos que antes pero ahora no hay menor elemento, sin embargo hay tres elementos mínimos $\{a\},\{b\},\{c\}$.*

EJEMPLO 6.2. *Considere $(\mathbb{N}\setminus\{0,1\},\leq)$, donde el orden está definido por:*

$$a\leq b,\text{ si } b|a.$$

Dicho conjunto parcialmente ordenado tiene como elementos máximos a cualquier primo positivo. Pero es obvio que no tiene un elemento mayor.

El ejemplo anterior hace ver que cuál es el problema en torno a por qué los elementos máximos no pueden ser el mayor elemento de un conjunto pues estos pueden ser no comparables. Por tal razón observe que en un conjunto totalmente ordenado ambos conceptos coinciden. Esto nos lleva a formular una definición general.

DEFINICIÓN 6.2. *Sea $(P, \leq)$ un conjunto parcialmente ordenado. Una cadena es un subconjunto $S \subseteq P$ que es totalmente ordenado, es decir, cualesquiera dos elementos de S son comparables.*

Retomando el ejemplo de $(\mathbb{N} \setminus \{0,1\}, \leq)$ observe que el conjunto $\{2^n \mid n \in \mathbb{N}\}$ es una cadena y que en esta el elemento máximo es 2, que es de hecho el elemento mayor en dicha cadena.

El ejemplo anterior muestra que en las cadenas de un conjunto parcialmente ordenado los conceptos de máximo y mayor elemento coinciden, lo que es más general que la afirmación correspondiente para el conjunto totalmente ordenado.

Una vez discutidos estos importantes y sutiles conceptos podemos enunciar el resultado que se quiere.

PROPOSICIÓN 6.1. *(Lema de Zorn) Cualquier conjunto parcialmente ordenado no vacío en el que toda cadena es acotada superiormente, tiene un elemento máximo.*

Para más información del lema de Zorn se recomienda consultar el libro “Axiom of Choice” de Horst Herrlich.

Bibliografía

[1] Michael Aschbacher. *Finite group theory*, volume 10. Cambridge University Press, 2000.

[2] J.S. Golan. *The Linear Algebra a Beginning Graduate Student Ought to Know*. Texts in the Mathematical Sciences. Springer, 2004.

[3] Joseph J Rotman. *An introduction to the theory of groups*, volume 148. Springer Science & Business Media, 2012.