Notas de Álgebra Moderna 1

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 [**?**]

Capítulo 1

Básico de Grupos

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

Stefan Banach.

1. Grupos

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

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

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

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

Entonces llamamos a G un grupo.

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

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

G1) La composición de funciones es asociativa.

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

G3) Sabemos que toda función biyectiva es invertible.

□

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

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

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

2. Subgrupos

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

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

SG1) $e \in H$

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

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

Algunas caracterizaciones se encuentran en el siguiente resultado:

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

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

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

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

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

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

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

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

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

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

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

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

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

□

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

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

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

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

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

[1] Se recomienda ver el ejercicio 25.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Grupos Cíclicos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Grupos de Permutaciones

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

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

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

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

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

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

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

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

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

□

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

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

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

$$|S_n| = n!$$

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

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

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

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

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

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

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

Respecto a la segunda notación hay que desarrollar teoría previa.

4.1. Notación cíclica.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TABLA 1.

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

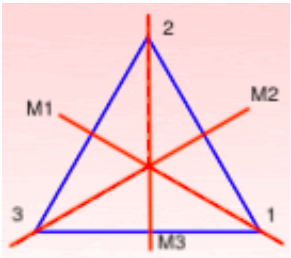

FIGURA 1.

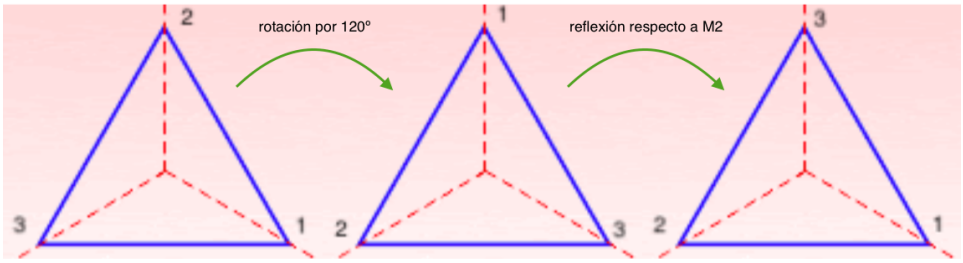

FIGURA 2.

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

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

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

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

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

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

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

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

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

Con lo anterior en mente se da el siguiente concepto.

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

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

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

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

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

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

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

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

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

DEMOSTRACIÓN. Claramente se tienen las siguientes igualdades,

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

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

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

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

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

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

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

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

lo que concluye la prueba. □

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

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

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

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

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

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

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

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

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

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

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

5. Teorema de Lagrange

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

De aquí que:

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

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

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

□

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

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

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

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

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

6. Subgrupos Normales y Grupo Cociente

Antes de dar la definición básica de la sección se va a probar un resultado previo que se obtiene al usar una generalización de las clases laterales. Sean $S, T \subseteq G$. Entonces se define el conjunto ST como $\{st \in G \mid s \in S, t \in T\}$.

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

DEMOSTRACIÓN. Lo primero que se observa es que HK no tiene porque tener estructura de de subgrupo. Se considera la función $f\colon H \times K \longrightarrow HK$ dada por $f(h,k) = hk$ para toda $h \in H$ y $k \in K$. 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. Por esto se tendría $H \times K = \bigcup_{x \in HK} f^{-1}(x)$. Si se toman las cardinalidades de ambos lados se tiene $|H||K| = \sum_{x \in HK} |H \cap K| = |HK||H \cap K|$.

Primero 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 $a = h(kb^{-1})$ y $b = (a^{-1}h)k$. También se tiene que $kb^{-1} = h^{-1}a$, de donde se pone $c = kb^{-1}$. Como se tiene que $c^{-1} = a^{-1}h$, se sigue la contención.

Sea $(hc, c^{-1}k)$ con $c \in H \cap K$. Entonces $f(hc, c^{-1}k) = x$. Se sigue la otra contención. La igualdad en la cardinalidad se sigue de ver que la función $g\colon H \cap K \longrightarrow f^{-1}(x)$ dada por $g(c) = (hc, c^{-1}k)$ para $c \in H \cap K$. □

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

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

El teorema básico de caracterización se presenta a continuación.

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

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

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

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

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

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

Vale la pena mencionar el siguiente resultado que está asociado a los conjuntos que permiten dar distintas caracterizaciones del concepto de normalidad. Este resultado es interesante pues en la sección anterior se vio que ni las clases laterales derechas ni las izquierdas de una subgrupo tenían estructura de subgrupo.

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

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

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

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

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

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

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

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

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

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

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

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

DEFINICIÓN 6.3. *Dado un grupo G, al subgrupo generado por todos los conmutadores de G se le llama como el subgrupo conmutador o subgrupo derivado de G. Este se denotará por G'.*

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 $g^{-1}g \in N$ 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. Además, observe que para $H \leq G$ el conjunto de clases laterales G/H tiene la estructura de grupo

$$g_1Hg_2H = g_1g_2H,$$

entonces $H \trianglelefteq G$ pues $gHg^{-1} \subseteq gHg^{-1}H = H$.

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. *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 6.8. *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 $O(n)/SO(n) = \{SO(n),\ A \cdot SO(n)\} = \langle A \cdot SO(n) \rangle$. En particular observe que $[O(n) : SO(n)] = 2$.*

EJEMPLO 6.9. *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.*

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 $g^{-1}Nh^{-1}N = h^{-1}Ng^{-1}N$, 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 $g,h \in N$, 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. □

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.

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 la cual tenemos que $x = hk \in L$- Por lo tanto $x \in HK \cap L$. □

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

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

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

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

8. Ejercicios

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

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

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

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

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

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

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

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

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

$\cdot$	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.

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.

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

EJERCICIO 6.

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

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

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

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

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

EJERCICIO 10. *Demuestre las siguientes afirmaciones:*

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

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

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

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

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

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

EJERCICIO 16.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $(n,m) = 1$.*

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 $\sigma = \tau_1 ... \tau_k$, donde $\tau_1, ..., \tau_k \in S_n$ 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 $\sim \subseteq \{1, ..., n\}^2$ mediante:*

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

1. *Demuestre que $\sim$ es una relación de equivalencia en $\{1, ..., n\}$.*
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 $r+\mathbb{Z}$ para $0 \leq r < n$.*
2. *Para $\mathbb{R} \leq \mathbb{C}$, las clases de $\mathbb{R}$ están dadas por $bi+\mathbb{R}$ con $b \in \mathbb{R}$.*

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

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

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

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

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

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

EJERCICIO 54.

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

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

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

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

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

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

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

EJERCICIO 61.

1. *Demuestre que la intersección de cualquier familia no vacía de subgrupos normales es un subgrupo normal.*
2. *Demuestre que dado cualquier conjunto, el subgrupo normal generado por dicho conjunto existe y es único.*
3. *Si el subgrupo normal generado por $S \subseteq G$ se denota por $\langle S \rangle_N$, ¿Existe alguna relación entre $\langle S \rangle_N$ y $\langle S \rangle$?*
4. *Demuestre que para cualquier $S \subseteq G$, $\langle S \rangle_N$ 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 $x \in N$.*

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.

Anexos

9. Retículas

DEFINICIÓN 9.1. *Sea P un conjunto y $\leq$ una relación sobre P. Decimos que P con $\leq$ es un conjunto parcialmente ordenado.*

1. *Para toda $x \in P$, $x \leq x$*
2. *Para todo $x, y \in P$, si $x \leq y$ e $y \leq x$, entonces $x = y$*
3. *Para todo $x, y, z \in P$, si $x \leq y$ e $y \leq z$, entonces $x \leq z$*

EJEMPLO 9.1. *Sea X un conjunto. Entonces el conjunto potencia $\mathscr{P}(X)$ es un conjunto parcialmente ordenado con la contención $\subseteq$.*

DEFINICIÓN 9.2. *Sea L un conjunto parcialmente ordenado. Decimos que L tiene un elemento máximo x. Si para todo $y \in L$, $y \leq x$. Por la asimetría el elemento maximo es único y lo denotamos por $\bar{1}$.*

En el caso de $\mathscr{P}(X)$ su elemento máximo es X.

DEFINICIÓN 9.3. *Sea L un conjunto parcialmente ordenado. Decimos que L tiene un elemento máximo x. Si para todo $y \in L$, $x \leq y$. Por la asimetría el elemento maximo es único y lo denotamos por $\bar{o}$.*

En el caso de $\mathscr{P}(X)$ su elemento mínimo es $\emptyset$.

DEFINICIÓN 9.4. *Sea L un conjunto parcialmente ordenado, $S \subseteq L$ y $a \in L$. Decimos que a es una cota superiorde S, si $x \leq a$ para toda $x \in S$.*

En caso de S sea vacío, cualquier elemento de L es cota superior.

DEFINICIÓN 9.5. *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 9.1. *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 9.6. *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 9.7. *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 9.2. *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 9.8. *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 9.9. *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 9.1. *Sean L una retícula tal que existen todos los ínfimos. Entonces L es una retícula completa.*

DEFINICIÓN 9.10. *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 9.11. *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 $z = y$.*

10. Lema de Zorn