Universidad de El Salvador
Facultad de Ciencias Naturales y Matemática
Escuela de Matemática
Licenciatura en Matemática

Trabajo de Tesis Titulado:

RECUBRIMIENTO DE UN LAZO POR MEDIO DE SUBLAZOS.

Presentado por:
Juan Antonio Rivera Menjivar, RM18039

Asesorado por:
Dra. Ingrid Carolina Martínez Barahona

Ciudad Universitaria, 21 de noviembre de 2024

UNIVERSIDAD DE EL SALVADOR

M.Sc. Juan Rosa Quintanilla
Rector

Dra. Evelyn Beatriz Farfán
Vicerrectora Académica

M.Sc. Roger Armando Arias
Vicerrector Administrativo

Lic. Pedro Rosalío Escobar Castaneda
Secretario General

Lic. Carlos Amílcar Serrano Rivera
Fiscal General

Lcda. Ana Ruth Avelar
Defensora de los Derechos Universitarios

Facultad de Ciencias Naturales y Matemática

Dr. Luis Gilberto Parada Gómez
Decano

Dr. José Nerys Funes Torres
Vicedecano

Lcda. Angela Gudelia Portillo de Pérez
Secretaria de la Facultad

Escuela de Matemática

Dr. Dimas Noé Tejada Tejada
Director

Lcda. Claudia Patricia Corcio
Secretaria

Tribunal Evaluador

Dra. Ingrid Carolina Martínez Barahona
Asesora de Tesis

Dr. Riquelmi Salvador Cardona Fuentes
Jurado

MSc. José René Palacios Barrera
Jurado

Agradecimientos

A mis padres, Blanca Rubia Menjivar de Rivera y Alvaro de Jesús Rivera Galdamez, por el apoyo que siempre me brindaron para lograr mis objetivos y metas.

A Manuel Cubías, por su apoyo durante la completitud de mi carrera universitaria, por sus consejos que ayudaron mantener siempre fijos mis objetivos y permanecer perseverante y constante en mi crecimiento personal y educativo.

A mis amigos y compañeros, que durante toda la carrera me ayudaron cada uno a su manera, para poder culminar este proceso, guiados por el deseo de superación y el amor común por las matemáticas.

A mi asesora Dra. Ingrid Carolina Martínez Barahona, por la dedicación, compromiso y conocimientos que me ha transmitido a lo largo de la realización de este trabajo de graduación, por ser mi guia no solo en este trabajo, si no que durante toda la carrera, por ser una de las y los mejores docentes de los cuales he tenido la oportunidad de aprender.

A mi jurado: Dr. Riquelmi Salvador Cardona Fuentes y MSc. José René Palacios Barrera, por la revisión y recomendaciones de ideas para la correcion y mejoramiento del trabajo final.

Índice general

INTRODUCCIÓN

Este trabajo de investigación presenta la estructura algebraica de lazo, una generalización de los grupos, la cual no es necesariamente asociativa, pero se mantiene la existencia de un elemento neutro e inversos. Los lazos, junto con los cuasigrupos, forman una clase de estructuras algebraicas no asociativas que, a pesar de su aparente simplicidad, presentan una amplia y compleja organización interna. A lo largo de este trabajo se explora los fundamentos de la teoría de lazos y su relación con la teoría de grupos, se introducen conceptos importantes como los recubrimientos por sublazos, y se adaptan resultados clásicos de la teoría de grupos al contexto de estructuras no asociativas.

El principal objetivo es estudiar como los lazos pueden ser descompuestos y cubiertos por medio de sublazos. Esta idea de recubrimiento, que en teoría de grupos ha sido ampliamente estudiada, especialmente a partir de los trabajos de Bernhard Neumann, se traslada de manera similar al ámbito de teoría de lazos, con esto en mente, es necesario un desarrollo de propiedades básicas de los lazos, lo que nos lleva a estudiar la teoría de cuasigrupos y su comportamiento bajo operaciones binarias no asociativas, lo cual nos permite profundizar en el análisis de las descomposiciones internas de los lazos, proporcionando nuevas perspectivas sobre como estas estructuras algebraicas pueden organizarse y ser descompuestas en componentes más simples.

El trabajo comienza con una revisión de las definiciones básicas en teoría de grupos, que servirán como punto de partida para el estudio de teoría de los lazos. Estos conceptos permiten no solo comprender la organización interna de los grupos, sino también como estos pueden ser descompuestos y cubiertos por subconjuntos más pequeños, lo que sienta las bases para el estudio de los lazos.

En el segundo capítulo se presentan algunas de las estructuras algebraicas que son generalizaciones de grupos, las cuales son, magmas, cuasigrupos y lazos, así como varias de sus propiedades y algunos ejemplos que nos permiten ver como se estructuran estos conjuntos. Los magmas siendo un conjunto con una operación binaria cerrada, los cuasigrupos definidos por la existencia de soluciones únicas para las ecuaciones de la forma $a * x = b$ y $y * a = b$ y finalmente un lazo, el cual es un cuasigrupo que además posee un elemento neutro o identidad, lo que lo aproxima más a la estructura de un grupo, pero sin la necesidad de ser asociativo. Al igual que en teoría de grupos, en este capítulo se estudian las subestructuras de lazo como sublazos, especialmente el núcleo y centro, analizando su comportamiento y estructura dentro del lazo.

En álgebra moderna, el estudio de las subestructuras siempre resulta de suma importancia, en el capítulo 3, los sublazos nos permiten analizar las descomposiciones en clases laterales, adaptando las nociones que en teoría de grupos son clásicas. El concepto de índice de un sublazo se convierte en una parte crucial para entender como los lazos pueden ser estructurados y organizados. La descomposición de un lazo en clases laterales permite dividir su estructura en partes más simples, facilitando su análisis y proporcionando una idea más clara de su estructura interna.

Finalmente, en el capítulo 4, la idea de descomposición nos lleva a plantearnos nuevos conceptos, tales como los recubrimientos finitos y los $n-$recubrimientos para lazos, en los cuales se muestran formas de recubrir un lazo mediante una colección de sublazos, de manera análoga a como un grupo puede ser cubierto por subgrupos. Con esta idea de recubrimientos surge la necesidad de verificar si el Lema de Neumann, un resultado clave en la teoría de grupos, se cumple para los lazos, con esto, se caracterizan los lazos que pueden admitir un recubrimiento finito, siendo este el objetivo principal de este trabajo. La noción de recubrimiento no solo permite descomponer un lazo, sino también entender mejor su comportamiento global a partir del análisis de sus subestructuras.

Capítulo 1

Definiciones algebraicas básicas

En este capítulo se presentan algunas definiciones básicas de teoría de grupos, así como algunas de sus propiedades, las cuales nos ayudarán a comprender los conceptos a estudiar posteriormente en este trabajo.

1.1. Definiciones básicas de grupos y algunas propiedades

Definición 1.1.1. *Un grupo es un par $(G, *)$, donde G es un conjunto no vacío y " $*$ " es una ley de composición interna definida en G,*

$$\begin{aligned} G \times G &\to G \\ (x, y) &\mapsto x * y \end{aligned}$$

tal que verifica las siguientes propiedades:

1. *Asociativa: Para todo $x, y, z \in G$, $(x * y) * z = x * (y * z)$.*
2. *Existencia de elemento neutro: Existe $e \in G$ tal que, para todo $x \in G$ $e * x = x * e = x$.*
3. *Existencia de elemento simétrico (inverso): Para cada $x \in G$ existe $x' \in G$ tal que $x * x' = x' * x = e$.*

Cuando no existe riesgo de confusión con la operación interna que estemos utilizando, diremos simplemente que G es un grupo. Asimismo, escribiremos ab en vez de $a * b$.

Definición 1.1.2. *Si en un grupo G se verifica la propiedad conmutativa, es decir, $xy = yx$ para todo $x, y \in G$, diremos que G es un grupo conmutativo o abeliano.*

Lema 1.1.1. *Sea G un grupo, se verifica lo siguiente:*

1. *El elemento neutro e del grupo G es único.*
2. *Para cada $x \in G$, existe un único simétrico $x' \in G$.*

Demostración.

1. Supongamos que e_1, e_2 son elementos neutros en G. Se verifica que

$$e_1 = e_1 e_2 = e_2.$$

2. Supongamos que x' y x" son elementos simétricos de x en G. Se verifica que

$$x' = x'e = x'(xx'') = (x'x)x'' = ex'' = x''. \quad \square$$

Observación 1.1.1. *Siempre que no exista riesgo de confusión, el elemento simétrico de $x \in G$, que hemos demostrado que es único, lo denotaremos por x^{-1}.*

Lema 1.1.2. *Sea G un grupo, se verifica lo siguiente:*

1. $(xy)^{-1} = y^{-1}x^{-1}$, $\forall x, y \in G$.
2. $(x^{-1})^{-1} = x$, $\forall x \in G$.
3. $e^{-1} = e$.

Demostración

1. $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = 1$. De igual forma se demuestra que $(y^{-1}x^{-1})(xy) = 1$. Ahora, al ser único el simétrico de un elemento, se tiene el resultado.
2. Como $x^{-1}x = xx^{-1} = e$, por tanto, podemos afirmar que $(x^{-1})^{-1} = x$.
3. Como $ee = e$, tendremos que $e^{-1} = e$. $\square$

Ejemplo 1.1.1. *Los números reales con la operación suma $(\mathbb{R}, +)$ forman un grupo donde el elemento identidad es el 0 y para todo $x \in \mathbb{R}$, su inverso es $-x$.*

Ejemplo 1.1.2. *El grupo de 4 de Klein, $V = \{e, a_1, a_2, a_3\}$, es un grupo formado por cuatro elementos, donde cada uno de ellos es inverso de sí mismo. Este posee la siguiente tabla de Cayley*

$*$	e	a_1	a_2	a_3
e	e	a_1	a_2	a_3
a_1	a_1	e	a_3	a_2
a_2	a_2	a_3	e	a_1
a_3	a_3	a_2	a_1	e

Definición 1.1.3. *Si G es un grupo y $m \in \mathbb{Z}$, definimos las potencias enteras de un elemento $a \in G$ como sigue:*

$$a^m = \begin{cases} \overbrace{a \cdots a}^{(m)} & Si\ m > 0, \\ e & Si\ m = 0, \\ \overbrace{a^{-1} \cdots a^{-1}}^{(m)} & Si\ m < 0. \end{cases}$$

En el caso de un grupo abeliano $(G, +)$, si $m > 0$, tenemos $a^m = \overbrace{a + \cdots + a}^{(m)} = ma$.

De la definición anterior se desprende el siguiente resultado, cuya demostración es inmediata.

Proposición 1.1.1. *Sean G un grupo, $a \in G$ y $m, n \in \mathbb{Z}$. Se verifica lo siguiente:*

1. $a^m a^n = a^{m+n}$.
2. $(a^m)^n = a^{mn}$.

Proposición 1.1.2. *Sean $(G_1, *)$ y $(G_2, +)$ dos grupos. Definimos en el conjunto $G_1 \times G_2$ la operación $(a_1, a_2) \bullet (b_1, b_2) = (a_1 * b_1, a_2 + b_2)$. Se verifica que $(G_1 \times G_2, \bullet)$ es un grupo.*

Demostración.
Veamos que se verifican las condiciones necesarias para ser grupo

1. La operación $\bullet$ es una operación interna, ya que para todo $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$, se tiene que $a_1, b_1 \in G_1$ y $a_2, b_2 \in G_2$. Por tanto, $a_1 * b_1 \in G_1$ y $a_2 + b_2 \in G_2$. De ahí que $(a_1, a_2) \bullet (b_1, b_2) = (a_1 * b_1, a_2 + b_2) \in G_1 \times G_2$.
2. La propiedad asociativa en $G_1 \times G_2$ es consecuencia inmediata de la asociatividad en G_1 y G_2.

3. Existencia de elemento neutro. El elemento $(1_{G_1}, 1_{G_2})$ es el elemento neutro, ya que para todo $(a_1, a_2) \in G_1 \times G_2$, se tiene que $(a_1, a_2) \bullet (1_{G_1}, 1_{G_2}) = (1_{G_1}, 1_{G_2}) \bullet (a_1, a_2) = (a_1, a_2)$.

4. Existencia de elemento simétrico. Dado un elemento $(a_1, a_2) \in G_1 \times G_2$, se tiene que $(a_1, a_2) \bullet (a_1^{-1}, a_2^{-1}) = (1_{G_1}, 1_{G_2}) = (a_1^{-1}, a_2^{-1}) \bullet (a_1, a_2)$. Por tanto, el elemento $(a_1^{-1}, a_2^{-1}) \in G_1 \times G_2$ es el elemento simétrico de (a_1, a_2). □

A este grupo se le denomina el producto directo de G_1 y G_2.

Definición 1.1.4. *Sean $(G_1, *)$ y $(G_2, +)$ dos grupos y $f\colon G_1 \to G_2$ una aplicación, se dice que f es un **homomorfismo de grupos** si preserva las operaciones, es decir, $\forall x, y \in G_1$, se cumple:*

$$f(x * y) = f(x) + f(y).$$

Definición 1.1.5. *Sean $(G_1, *)$ y $(G_2, +)$ dos grupos y $f\colon G_1 \to G_2$ una aplicación, se dice que f es un **isomorfismo de grupos** si es homomorfismo de grupos y además, es biyectiva.*

Nota. Dos grupos son homomorfos (isomorfos) si existe un homomorfismo (isomorfismo) entre ellos.

Definición 1.1.6. *Sea G un grupo y X un conjunto. Decimos que G actúa sobre X o que hay una acción de G sobre X, o simplemente que X es un* G-conjunto *si existe una función $G \times X \to X$, $(g, x) \mapsto g \cdot x$ que satisface los siguientes axiomas.*

1. *$e \cdot x = x$ para todo x en X, donde e es el elemento identidad del grupo G.*
2. *$g \cdot (h \cdot x) = (gh) \cdot x$ para todo x en X, todo g, h en G (gh denota el producto en G de los elementos g y h).*

Definición 1.1.7. *Sean x, y en un conjunto X, decimos que x está relacionado con y y escribimos $x \sim y$ si existe g en G tal que $g \cdot x = y$.*

Observación 1.1.2. *Notemos que la relación anterior es una relación de equivalencia:*

1. *Reflexiva: $e \cdot x = x$, donde e denota el elemento identidad de G.*
2. *Simetría: si $g \cdot x = y$ entonces $g^{-1} \cdot y = x$.*
3. *Transitividad: si $g \cdot x = y$ y $h \cdot y = z$ entonces $(hg) \cdot x = z$.*

Las clases de equivalencia bajo esta relación de equivalencia se denominan órbitas de G en X o simplemente órbitas, si G y X quedan claros en el contexto.

Definición 1.1.8. *Sea $x \in X$, la órbita que lo contiene se define como $Gx := \{g \cdot x \ \ | g \in G\}$.*

Observación 1.1.3. *Recordar que las clases de equivalencia que determina una relación de equivalencia sobre un conjunto A forman una partición para dicho conjunto.*

1.2. Subgrupos

La noción de subobjeto, en álgebra moderna, posee un valor esencialmente importante por la preservación de propiedades en subconjuntos, es decir, por restricción de problemas elementales a partes más simples.

Definición 1.2.1. *Dados $(G, *)$ un grupo y H un subconjunto no vacío de G, diremos que H es un subgrupo de G si H es un grupo respecto de la misma operación que dota a G de estructura de grupo y se denota como $H \leq G$.*

Proposición 1.2.1. *Dado $(G, *)$ un grupo. H un subconjunto no vacío de G es subgrupo de G si y sólo si:*

1. *Para cualesquiera $x, y \in H$ se tiene $xy \in H$.*
2. *El elemento neutro e de G pertenece a H.*

3. *Para todo $x \in H$ se tiene que su simétrico $x^{-1} \in H$.*

Demostración.
($\Longleftarrow$) Es inmediato, ya que basta observar que la condición (1) nos dice que la operación $*$ es interna en H, la condición (2) afirma que e es el elemento neutro de H, y la condición (3) dice que todo elemento de H tiene inverso perteneciente también a H. Por tanto, sólo nos falta ver que se verifica la propiedad asociativa. Pero si $x, y, z \in H$, entonces $x, y, z \in G$ y por tanto,

$$x(yz) = (xy)z. \quad \square \tag{1.1}$$

($\Longrightarrow$)
Si H es subgrupo de $(G, *)$, tenemos que $(H, *)$ es un grupo, por tanto, se verifica:

(1) La operación $*$ es interna en H y así para cualquier par de elementos $x, y \in H$ se tiene que $xy \in H$.

(2) Sea e_H el elemento neutro en H, por tanto, para todo $x \in H$ se tiene

$$xe_H = e_H x = x$$

pero, por otra parte, como $x \in G$, también se tiene

$$xe = ex = x$$

donde e es el elemento neutro de G, por tanto, para todo $x \in H$ se verifica $xe_H = xe$ y de ahí que $e_H = e$.

(3) Sea $x' \in H$ el simétrico de x, luego se tiene que $xx' = x'x = e$. Por tanto, x' es el simétrico de x en G y así, por la unicidad del elemento simétrico, $x^{-1} = x' \in H$. $\square$

La siguiente proposición caracteriza de modo sencillo la condición de ser subgrupo.

Proposición 1.2.2. *Sean G un grupo y H un subconjunto no vacío de G. Las siguientes proposiciones son equivalentes:*

1. *H es subgrupo de G.*

2. *Para cada par de elementos $x, y \in H$, se tiene $xy^{-1} \in H$.*

Demostración.
$(1) \implies (2)$: Sean $x, y \in H$. Por la **Proposición 1.2.1** (3), $y^{-1} \in H$. Por tanto, $x, y^{-1} \in H$ y por la **Proposición 1.2.1** (1) se tiene el resultado.

$(2) \implies (1)$: Veremos que H verifica las tres condiciones de la **Proposición 1.2.1**:

(2) Como H es no vacío, existe al menos un elemento $x \in H$. Por tanto, se tiene que $e = xx^{-1} \in H$.
(3) Como $e \in H$, para todo $y \in H$ se tiene que $y^{-1} = ey^{-1} \in H$.
(1) Dados $x, y \in H$, como $y^{-1} \in H$ por el apartado (3), se tiene $xy = x(y^{-1})^{-1} \in H$. $\square$

Observación 1.2.1. *Dado un grupo G, los conjuntos $\{e\}$ y G son subgrupos de G y son los llamados subgrupos triviales del grupo G.*

Definición 1.2.2. *Llamaremos subgrupos propios de un grupo G, a aquellos subgrupos distintos de $\{e\}$ y G.*

Ejemplo 1.2.1. *Los subgrupos del grupo $(\mathbb{Z}, +)$ son los conjuntos de la forma $m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$, para cada entero m no negativo.*

Proposición 1.2.3. *Sean G un grupo. Si H_1, H_2 son subgrupos de G entonces $H_1 \cap H_2$ es subgrupo de G.*

Demostración.
$H_1 \cap H_2 \neq \emptyset$, ya que $e \in H_1 \cap H_2$ dado que $e \in H_1$ y $e \in H_2$ por ser subgrupos. Sean $x, y \in H_1 \cap H_2$ arbitrarios, como $x, y \in H_1$ y $x, y \in H_2$ por definición de intersección, luego $y^{-1} \in H_1, y^{-1} \in H_2$, y $xy^{-1} \in H_1, xy^{-1} \in H_2$ por ser H_1, H_2 subgrupos, entonces $xy^{-1} \in H_1 \cap H_2$. Por tanto, por la **Proposición 1.2.2** $H_1 \cap H_2$ es subgrupo de G. $\square$

Análogamente, se prueba que dado un grupo G y una familia $\{H_i\}_{i \in I}$ de subgrupos de G, $\bigcap_{i \in I} H_i$ también es subgrupo de G.

Se acaba de probar que la intersección de dos subgrupos es un subgrupo, ¿será que una unión de subgrupos arbitrarios es un subgrupo?

Consideremos el grupo $(\mathbb{R}^2, +)$ y consideremos los subgrupos $H_1 = \{(a, 0)/a \in \mathbb{R}\}$ y $H_2 = \{(0, b)/b \in \mathbb{R}\}$. Se verifica que $H_1 \cup H_2$ no es subgrupo de $\mathbb{R}^2$, ya que no es cerrado, sean $(1, 0) \in H_1$, $(0, 1) \in H_2$, entonces $(1, 0) + (0, 1) = (1, 1)$, pero $(1, 1)$ no pertenece ni a H_1 ni a H_2, por tanto, no pertenece a $H_1 \cup H_2$.

Proposición 1.2.4. *Sean G un grupo y H_1, H_2 subgrupos de G, $H_1 \cup H_2$ es subgrupo de G si y sólo si $H_1 \subset H_2$ ó $H_2 \subset H_1$.*

Demostración.
($\Longleftarrow$) Si $H_1 \subset H_2$ entonces $H_1 \cup H_2 = H_2$ que es subgrupo por hipótesis.
Análogamente se cumple si $H_1 \subset H_2$.

($\Longrightarrow$)
Por contradicción, supongamos que $H_1 \not\subset H_2$ y $H_2 \not\subset H_1$, sean $x \in H_1 - H_2$ y $y \in H_2 - H_1$, estos conjuntos son no vacíos, pues $H_1 \not\subset H_2$ y $H_2 \not\subset H_1$). Como $x \in H_1$ se sigue que $x \in H_1 \cup H_2$ y lo mismo para y. Por tanto, $xy \in H_1 \cup H_2$ por ser este subgrupo, por hipótesis. Luego, $xy \in H_1$ o $xy \in H_2$. Si $xy \in H_1$ entonces $xy = h$ para algún $h \in H_1$. Como H_1 es subgrupo, $y = x^{-1}h \in H_1$ ya que $x \in H_1$. Luego, $y \in H_1$ contrario a que $y \in H_2 - H_1$ como se había elegido. Así se prueba que $xy \notin H_1$, pero análogamente se prueba que $xy \notin H_2$, Por lo que tenemos una contradicción. $\square$

1.3. Índice de un subgrupo y subgrupo normal.

La finitud en el número de elementos de un grupo es importante para distinguir grupos, no sólo por el aspecto contable, sino también por las propiedades inherentes a un grupo en virtud de su cardinal.

Definición 1.3.1. *Sea G un grupo. Al cardinal de un subgrupo H de G se le llama orden de H y lo denotamos por $o(H)$. En particular, al número de elementos de G se llama orden de G. Un grupo es finito cuando $o(G) < \infty$. En caso contrario, decimos que el grupo G es infinito.*

Sean G un grupo y $H \subseteq G$ un subgrupo. Definimos en G las siguientes relaciones binarias:

1. $\forall x, y \in G \qquad xR_H y \Longleftrightarrow xy^{-1} \in H$,
2. $\forall x, y \in G \qquad xR^H y \Longleftrightarrow x^{-1}y \in H$.

Lema 1.3.1. *Con la notación anterior, las relaciones binarias R_H, R^H son relaciones de equivalencia sobre G.*

Demostración.
Lo demostraremos para R_H, para R^H es análogo.

- Reflexiva: Para todo $x \in G$ se tiene que $xx^{-1} = e \in H$, por tanto, $xR_H x$.
- Simétrica: Sean $x, y \in G$, tales que $xR_H y$ entonces $xy^{-1} \in H$. Pero al ser H un subgrupo, se tiene que $\left(xy^{-1}\right)^{-1} \in H$. Por tanto $yx^{-1} \in H$, y de ahí que $yR_H x$.

- Transitiva: Sean $x, y, z \in G$ tales que $xR_H y$ e $yR_H z$, entonces $xy^{-1} \in H$ e $yz^{-1} \in H$. Por tanto, al ser H un subgrupo, $xz^{-1} = \left(xy^{-1}\right)\left(yz^{-1}\right) \in H$ y de ahí que $xR_H z$. $\square$

Dado $a \in G$, denotemos por $[a]_H$ y $[a]^H$ respectivamente las clases de equivalencia que las relaciones R_H, R^H determinan en G. Asimismo, los conjuntos cocientes serán denotados por G/R_H, G/R^H respectivamente.

Lema 1.3.2. *Con la notación anterior, se verifica que* $[a]_H = \{ha : h \in H\}$ *y* $[a]^H = \{ah : h \in H\}$.

Demostración.
Notemos que

$$Ha = \{ha : h \in H\}$$

donde $a \in G$. Se trata de demostrar que $[a]_H = Ha$. Si $y \in [a]_H$ entonces $yR_H a$, por tanto $ya^{-1} \in H$. Así, existe $h \in H$ tal que $ya^{-1} = h$, y de aquí que $y = ha$, con $h \in H$. Por tanto $y \in Ha$. Recíprocamente, sea $y \in Ha$. Luego existe $h \in H$, tal que $y = ha$, con lo cual $ya^{-1} = h \in H$. Así, $yR_H a$ y $y \in [a]_H$. Por lo tanto $[a]_H = Ha$. $\square$

Definición 1.3.2. *Las clases de equivalencia Ha y aH se llaman respectivamente clases laterales por la derecha y por la izquierda de G módulo H.*

Lema 1.3.3. *Sea G un grupo, y H un subgrupo de G. Los conjuntos G/R_H y G/R^H tienen el mismo cardinal.*

Demostración.
Para demostrar que los conjuntos G/R_H y G/R^H tienen el mismo cardinal, estableceremos una aplicación biyectiva entre ellos. Definimos

$$\begin{aligned} f\colon G/R_H &\to G/R^H \\ Ha &\mapsto a^{-1}H. \end{aligned}$$

Se verifica que:

1. f está bien definida y es inyectiva, ya que, dados $a, b \in G$, tenemos

$$\begin{aligned} Ha = Hb &\iff [a]_H = [b]_H \\ &\iff aR_H b \\ &\iff ab^{-1} \in H \\ &\iff \left(a^{-1}\right)^{-1} b^{-1} \in H \\ &\iff a^{-1} R^H b^{-1} \\ &\iff \left[a^{-1}\right]^H = \left[b^{-1}\right]^H \\ &\iff a^{-1}H = b^{-1}H \\ &\iff f(Ha) = f(Hb). \end{aligned}$$

2. f es sobreyectiva, ya que para todo $bH \in G/R^H$, existe $Hb^{-1} \in G/R_H$ tal que $f\left(Hb^{-1}\right) = bH$.

Por tanto, $card\,(G/R_H) = card\,\left(G/R^H\right)$. $\square$

Definición 1.3.3. *Sea G un grupo y sea H un subgrupo de G.*

1. *Si G/R_H (y por tanto G/R^H) es un conjunto infinito, decimos que H es un subgrupo de G de índice infinito.*
2. *Si G/R_H (y por tanto G/R^H) es finito, se llama índice de H en G, y lo denotamos por $[G : H]$, al cardinal (común) de los conjuntos G/R_H y G/R^H. En este caso decimos que H es un subgrupo de G de índice finito.*

Lema 1.3.4. *Sea H un subgrupo de G, y sea $x \in G$. Las aplicaciones*

$$\begin{aligned} f\colon H &\to Hx \\ h &\mapsto hx \end{aligned} \qquad\qquad \begin{aligned} g\colon H &\to xH \\ h &\mapsto xh \end{aligned}$$

son biyectivas.

Demostración.
Haremos la demostración para la aplicación f. De igual forma se demuestra que g es biyectiva.

- f es inyectiva, ya que si $f(h_1) = f(h_2)$ entonces $h_1 x = h_2 x$. Por tanto, $h_1 = h_2$.
- f es sobreyectiva, ya que para todo $hx \in Hx$, existe $h \in H$ tal que $f(h) = hx$. $\square$

Del **Lema 1.3.4**, tenemos que:

1. Dado $x \in G$, existe una biyección entre Hx y xH. Sin embargo, estos pueden ser diferentes.
2. Si $o(H)$ es finito, se verifica que $card(Hx) = card(xH) = card(H) = o(H)$.

Definición 1.3.4. *sea G un grupo, H un subgrupo de G y g un elemento cualquiera de G:*

1. *$gH = \{gh : h \in H\}$ es una clase lateral izquierda de H en G.*
2. *$Hg = \{hg : h \in H\}$ es una clase lateral derecha de H en G.*

Proposición 1.3.1. *Sean G un grupo y sea H un subgrupo de G. Las siguientes condiciones son equivalentes:*

1. *$Ha = aH$ para cada $a \in G$.*
2. *$H = a^{-1}Ha$ para cada $a \in G$.*
3. *Para cada par de elementos $a, b \in G$ tales que $ab \in H$ entonces $ba \in H$.*

Demostración.
$(1) \implies (2)$: Si $y \in a^{-1}Ha$ entonces $y = a^{-1}ha$, con $h \in H$. Así tenemos que $ay = ha$, de donde $ay \in Ha$. Pero por hipótesis $Ha = aH$, luego existe $h' \in H$ tal que $ay = ah'$, de donde $y = h'$. Así $y \in H$. Con esto hemos demostrado que $a^{-1}Ha \subseteq H$.
Recíprocamente, sea $h \in H$, se sigue que $ah \in aH$. Por hipótesis tenemos que $aH = Ha$, luego existe $h' \in H$ tal que $ah = h'a$, o lo que es lo mismo, $h = a^{-1}h'a$. Por tanto, $H \subseteq a^{-1}Ha$.

$(2) \implies (3)$: Sean $a, b \in G$, tales que $ab \in H$. Luego $ba = \left(a^{-1}a\right)(ba) = a^{-1}(ab)a \in a^{-1}Ha = H$.

$(3) \implies (1)$: Si $x \in Ha$ entonces $x = ha$ para algún $h \in H$, por tanto $xa^{-1} = h \in H$. Así, aplicando la hipótesis, $a^{-1}x \in H$, es decir, existe $h' \in H$ tal que $a^{-1}x = h'$, de donde $x = ah' \in aH$. Por consiguiente $Ha \subseteq aH$. La otra inclusión se demuestra de forma análoga. $\square$

Definición 1.3.5. *Dado un grupo G y $H \leq G$, al conjunto X conformado por exactamente un representante de cada clase lateral derecha de H se denomina transversal derecha de H en G, de igual manera se define una transversal izquierda de H en G.*

Definición 1.3.6. *Diremos que un subgrupo H de un grupo G es subgrupo normal, y se denotará por $H \triangleleft G$, si verifica una cualquiera y por tanto, todas las condiciones de la **Proposición 1.3.1**.*

Proposición 1.3.2. *(Cociente por un Grupo Normal) Sea G un grupo, H un subgrupo normal de G. El conjunto de las clases laterales izquierdas (que coincide con el conjunto de las clases laterales derechas) tiene una estructura de grupo respecto a la operación definida por*

$$(aH) * (bH) := abH.$$

*Simbolizaremos a ese grupo por G/H y lo llamaremos el **grupo cociente** de G por (el subgrupo) H o G módulo H.*

Demostración.
La definición de normal garantiza que la operación definida en el enunciado está bien definida en el conjunto de las clases laterales. El neutro para la operación es la clase del neutro $H = eH$, ya que $eHxH = exH = xH = xeH = xHeH$. La asociatividad sigue de, $xH(yHzH) = xH(yzH) = x(yz)H = (xy)zH = xyHzH = (xHyH)zH$. Análogamente, $xHx^{-1}H = xx^{-1}H = eH = H = eH = (x^{-1}x)H = x^{-1}HxH$. Lo que prueba que la clase $x^{-1}H$ es la inversa de la clase xH. □

1.4. Recubrimiento de grupos por subgrupos (Resultados).

Decimos que un grupo tiene un recubrimiento por subgrupos si es la unión teórica de conjuntos de subgrupos propios, y si el conjunto de subgrupos es finito, se dice que el recubrimiento es finito. Tales recubrimientos han sido ampliamente estudiados en teoría de grupos y recientemente se han planteado problemas análogos para anillos y para semigrupos (conjunto con una operación cerrada y asociativa) se discutieron en [HAL97; LJJ01], respectivamente. Con esto, se tienen los siguientes resultados.

Teorema 1.4.1. *Un grupo es la unión teórica de tres subgrupos propios si y solo si el grupo tiene una imagen homomórfica al grupo de cuatro de Klein.*

Bernhard Neumann en [Neu54a; Neu54b] investigó los recubrimientos por clases laterales. El siguiente teorema, a menudo llamado **Lema de Neumann**, es una clave para muchos de los resultados en teoría de grupos. Particularmente se enuncia una caracterización de los grupos que tienen recubrimientos finitos como corolario del siguiente teorema.

Teorema 1.4.2. *Sea $G = \bigcup_{i=1}^{k} giHi$, donde $H_1, ..., H_k$ son subgrupos (no necesariamente distintos) de G. Si omitimos de la unión cualquier clase lateral g_iH_i para la cual $[G : H_i]$ sea infinito, la unión de las clases laterales restantes sigue siendo todo G.*

Corolario 1.4.1. *Un grupo tiene un recubrimiento finito por subgrupos si y sólo si tiene una imagen homomórfica no cíclica finita.*

Observación 1.4.1. *Notamos que en el **Teorema 1.4.2**, si consideramos a $g_i = e$ para todo $i = 1, ..., k$, entonces se tiene que G es unión de subgrupos.*

Ejemplo 1.4.1. *El grupo de cuatro de Klein, $V = \{e, a_1, a_2, a_3\}$, admite una descomposición de tres subgrupos. Consideremos los conjuntos $V_i = \{e, a_i\}$, se verifica que V_i es subgrupo de V, por ser a_i su propio inverso para $i = 1, 2, 3$, por lo tanto, tenemos que*

$$V = V_1 \cup V_2 \cup V_3.$$

Ejemplo 1.4.2. *El grupo cuaternión $Q_8 = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$ el cual tiene la siguiente tabla de Cayley.*

$*$	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

Este es la unión de tres subgrupos propios. Una prueba directa es ver que $Q_8 = H_1 \cup H_2 \cup H_3$, donde $H_1 = \langle \mathbf{i} \rangle$, $H_2 = \langle \mathbf{j} \rangle$, $H_3 = \langle \mathbf{k} \rangle$.

Capítulo 2

Cuasigrupos y Lazos

Este capítulo se centrará en dar una introducción al estudio de estructuras algebraicas no asociativas, con el objetivo de extender algunas analogías respecto a definiciones y propiedades presentadas en teoría de grupos y verificar su comportamiento en estructuras algebraicas más generales.

2.1. Magmas, cuasigrupos y lazos.

Una operación binaria (cerrada) en un conjunto no vacío G es simplemente una aplicación $\alpha\colon G \times G \to G$. Siempre que α sea una operación binaria sobre G y a, b y c sean miembros de G tales que $\alpha(a, b) = c$, no dudaremos en emplear cualquiera de los recursos de notación comunes y útiles para registrar esta información. Por ejemplo, podemos escribir $a + b = c,\ a * b = c,\ a \div b = c$, etc., y dependiendo de la notación seleccionada, podemos llamar a c la "suma", "producto", "cociente", etc., de a y b. En el presente capítulo y los posteriores, se va a emplear la notación " $*$ " o "producto" y, por lo tanto, a escribir $a * b = c$ para $\alpha(a, b) = c$ e incluso a referirnos, informalmente, a $(*)$ en lugar de α como la operación binaria en G.

Definición 2.1.1. *Un magma es un par $(G, *)$, donde G es un conjunto no vacío, y $(*)$ una operación binaria cerrada sobre G, es decir $\forall a, b \in G, a * b \in G$.*

Definición 2.1.2. *Sea $(G, *)$ Un magma y sea $a \in G$ cualquier elemento fijo, las aplicaciones,*

$$L_a\colon G \to G \qquad\qquad R_a\colon G \to G$$
$$x \mapsto a * x \qquad\qquad x \mapsto x * a$$

Para todo $x \in G$, se denominan traslaciones izquierda y derecha respectivamente.

Definición 2.1.3. *Un magma $(G, *)$ es llamado cuasigrupo si las traslaciones L_a y R_a son biyecciones para todo $a \in G$.*

Proposición 2.1.1. *Dado un magma $(G, *)$, las siguientes condiciones son equivalentes,*

1. *$(G, *)$ es un cuasigrupo.*
2. *Para todo $a, b \in G$ las ecuaciones $a * x = b, y * a = b$ tienen solución única.*

Demostración.
$1 \implies 2$
Es claro ya que si $(G, *)$ es cuasigrupo entonces las traslaciones L_a y R_a son biyecciones para todo $a \in G$, luego, dado que $b \in G$, se tiene que existen únicos $x, y \in G$ tal que $L_a(x) = b$ y $R_a(y) = b$, esto implica que las ecuaciones $a * x = b$ y $y * a = b$ tienen solución única.

$2 \implies 1$
También es claro, ya que si las ecuaciones $a * x = b$ y $y * a = b$ tienen solución única, $x, y \in G$ son únicos,

y esto implica que para todo $a \in G$, las traslaciones $L_a \colon G \to G$ y $R_a \colon G \to G$ son biyecciones. $\square$

Teorema 2.1.1. *Sea $(G, *)$ un cuasigrupo. Se tienen las siguientes propiedades:*

1. *Para $(a, b) \in G \times G$ existe un único $(x, y) \in G \times G$ tal que $a * x = y * a = b$ (solubilidad única).*
2. *Para $a, x, y \in G, a * x = a * y$ implica que $x = y$ (cancelación izquierda).*
3. *Para $a, x, y \in G,\ x * a = y * a$ implica que $x = y$ (cancelación por la derecha).*

Demostración.
(1) se probó en la **Proposición 2.1.1**, por otro lado, **(2), (3)** se desprenden de la biyectividad de L_a, R_a respectivamente, vistas en la **Definición 2.1.2**. De **1** se puede ver fácilmente que para cada elemento $a \in (G, *)$ existe una identidad local única izquierda (derecha) $l_a(r_a)$ tal que $l_a * a = a(a * r_a = a)$. Diferentes elementos pueden tener diferentes identidades locales. $\square$

Aunque **1,2,3** del **Teorema 2.1.1** son condiciones necesarias para que un magma $(G, *)$ sea un cuasigrupo, sólo la condición **1** es, en general, una condición necesaria y suficiente para $(G, *)$ ser un cuasigrupo. Sin embargo, en presencia de la finitud, tenemos lo siguiente.

Teorema 2.1.2. *Sea $(G, *)$ un magma finito, las siguientes afirmaciones son equivalentes:*

1. *$(G, *)$ es un cuasigrupo.*
2. *$L_a : G \to G$ y $R_a : G \to G$ son inyectivas para todo $a \in G$.*
3. *$L_a : G \to G$ y $R_a : G \to G$ son sobreyectivas para todo $a \in G$.*
4. *Las leyes de cancelación de derecha e izquierda son válidas para $(G, *)$.*
5. *Cada elemento de G aparece una vez y sólo una vez en cada fila y en cada columna de una tabla de Cayley para $(G, *)$.*

Demostración.
Primero recordemos que dado un conjunto finito G y cualquier aplicación $\alpha \colon G \to G$, α es inyectiva si y solo si es sobreyectiva.

$1 \implies 2$. Si G es un cuasigrupo, se tiene que L_a y R_a son biyectivas, por tanto, son inyectivas para todo $a \in G$.

$2 \implies 3$. Si $L_a \colon G \to G$ y $R_a \colon G \to G$ son inyectivas para todo $a \in G$, como G es finito, se cumple que $L_a : G \to G$ y $R_a \colon G \to G$ son sobreyectivas para todo $a \in G$.

$3 \implies 4$. Dado que $L_a \colon G \to G$ y $R_a \colon G \to G$ son sobreyectivas, cualquier elemento de G puede escribirse como $x * a$ o $a * x$, para algún $x \in G$. Con esto, las ecuaciones $a * x = b$ y $x * a = b$ tienen solución única, para $a, b \in G$. Así se cumple la ley de cancelación por izquierda y derecha.

$4 \implies 5$. Supongamos que un elemento a aparece dos veces en una fila, entonces existe $b \in G$ tal que $a = b * c$ y $a = b * d$, pero esto contradice la ley de cancelación por la izquierda, de igual manera se verifica que si un elemento aparece dos veces en una columna, se contradice la ley de cancelación por la derecha.

$5 \implies 1$. Si cada elemento aparece una sola vez en cada fila o columna, se asegura que las ecuaciones $a * x = b$ y $y * a = b$ tienen solución única. $\square$

Definición 2.1.4. *Un magma $(G, *)$ es conmutativo si $L_a = R_a$ para todo $a \in G$.*

Definición 2.1.5. *Un magma $(G, *)$ es asociativo si $R_{a*b}(x) = R_b(R_a(x))$ para todo $a, b, x \in G$.*

Definición 2.1.6. *Si $(G, *)$ es un magma y sea $e \in G$, que e es un elemento de identidad izquierdo (derecho) para $(G, *)$ significa que $L_e : G \to G$ ($R_e : G \to G$) es la aplicación identidad de G. También que e sea un elemento identidad para $(G, *)$ significa que e es un elemento de identidad izquierdo y derecho para $(G, *)$.*

Algunos de los conceptos recién definidos están relacionados como se indica a continuación:

Teorema 2.1.3. *Si $(G, *)$ es un cuasigrupo asociativo, $(G, *)$ necesariamente tiene un elemento de identidad único.*

Demostración.
Como G no es vacío, hay al menos un elemento a en G. Ahora, por **Teorema 2.1.1** existe $e \in G$ tal que $a * e = a$, sea b cualquier elemento en G, de nuevo por el **Teorema 2.1.1** existe $y \in G$ tal que $y * a = b$. De ello se deduce que $R_e(b) = b * e = (y * a) * e = R_e(R_a(y)) = R_{a*e}(y) = R_a(y) = y * a = b$ (obsérvese cómo se usa la asociatividad aquí). Por tanto, $R_e : G \to G$ es la aplicación de identidad en G, por lo que e es un elemento de identidad derecho para $(G, *)$.

Ahora, sea b cualquier elemento en G. Tenemos $b * b = (b * e) * b = R_b(R_e(b)) = R_{e*b}(b) = b * (e * b)$ (una vez más se utiliza la asociatividad). Por cancelación por la izquierda (ver **Teorema 2.1.1**) observamos que $b * b = b * (e * b)$ implica $b = e * b$. Esto es cierto para todo $b \in G$, luego $L_e(b) = b$ para todo $b \in G$. Pero que $L_e : G \to G$ sea la aplicación identidad en G significa que e es un elemento identidad izquierdo para $(G, *)$.
Así, e es un elemento identidad para $(G, *)$ y, de hecho, es el único (ver Ejercicio I.1.I en [Pfl90]) . □

No es cierto que un cuasigrupo con un elemento identidad tenga que ser asociativo. Considere el siguiente ejemplo:

Ejemplo 2.1.1. *Sea $G = \{1, 2, 3, 4, 5\}$ y sea $(*)$ dado por*

*	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	3	2	1

*Según el **Teorema 2.1.2**, el sistema binario $(G, *)$ es un cuasigrupo, ya que cada elemento de G aparece una vez y exactamente una vez en cada fila y en cada columna. Claramente, 1 es el elemento identidad, pero $(G, *)$ no es asociativo, ya que $R_{3*4}(3) \neq R_4(R_3(3))$.*

En vista del **Teorema 2.1.3**, se tiene la siguiente definición.

Definición 2.1.7. *Si un magma $(G, *)$ es un grupo entonces $(G, *)$ es un cuasigrupo asociativo.*

Así, los grupos son precisamente aquellos cuasigrupos que son asociativos y, por tanto, también tienen un elemento identidad.

Consideremos ahora aquellos cuasigrupos que poseen un elemento identidad, sin ser necesariamente asociativos.

Definición 2.1.8. *Un magma $(G, *)$ es llamado lazo si es un cuasigrupo y además $(G, *)$ posee un elemento neutro (identidad).*

Por tanto, los grupos son aquellos lazos que son asociativos. El **Ejemplo 2.1.1** muestra que existen lazos que no son grupos.

Definición 2.1.9. *Un cuasigrupo (lazo) $(G, *)$ es conmutativo si $(G, *)$ es conmutativo de acuerdo con la **Definición 2.1.4**.*

Proposición 2.1.2. *Sea $(G, *)$ un cuasigrupo que posee elemento identidad e, se cumple lo siguiente:*

1. *Para todo $a \in G$, se tiene que existen únicos $x, y \in G$ tal que $a * x = y * a = e$ (existencia de inversos por izquierda y derecha).*

2. *$(G, *)$ siempre cumple los axiomas de grupo, excepto la asociatividad.*

Demostración.

1. Dado que $(G, *)$ es cuasigrupo con identidad, es decir, $e \in G$, luego por la **Proposición 2.1.1**, tomando $b = e$, las ecuaciones $a * x = e$ y $y * a = e$ tienen solución única, entonces $a * x = y * a = e$ (existencia de inversos por izquierda y derecha).

2. Es no vacío y la operación es cerrada por ser un magma.
   a) Por hipótesis $e \in G$ (existencia de identidad).
   b) De 1. para todo $a \in G$, se tiene el resultado.

□

Ejemplo 2.1.2. *Sea $G = \{1, 2, 3, 4, 5\}$ y sea $(\circ)$ dada por*

$\circ$	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	1
3	3	4	5	1	2
4	4	5	1	2	3
5	5	1	2	3	4

$(G, \circ)$ es un ejemplo de lazo conmutativo, que también resulta ser un grupo. (El lazo $(G, *)$ del **Ejemplo 2.1.1** no es conmutativo).

Sea $(G, *)$ un cuasigrupo. Según la definición misma de cuasigrupo (ver **Definición 2.1.3**), todas las traslaciones $L_a \colon G \to G$ y $R_a \colon G \to G$, para todo $a \in G$, son biyecciones de G. Como tal, todas tienen aplicaciones inversas $L_a^{-1} \colon G \to G$ y $R_a^{-1} \colon G \to G$ que no son necesariamente traslaciones. (Por ejemplo, para $a \in G$ no hay garantía, en general, de que haya $b \in G$ de modo que $L_a^{-1} = L_b$ ó $R_a^{-1} = R_b$). Dadas estas aplicaciones inversas, se definen las operaciones binarias $(\backslash)$ y $(/)$ para el conjunto G. Sea

$$x \backslash y = L_x^{-1}(y) \text{ y } x/y = R_y^{-1}(x)$$

para todo $x,\ y \in G$. Tenga en cuenta que $x \backslash y = z$ si y sólo si $x * z = y$, y que $x/y = z$ si y sólo si $z * y = x$. Con esto, es fácil ver que $(G, \backslash)$ y $(G, /)$ también son cuasigrupos:
La existencia y unicidad de soluciones para $a/w = b,\ x/a = b,\ a \backslash y = b,\ z \backslash a = b$ se deriva de la existencia y unicidad de soluciones para $b * w = a,\ b * a = x,\ a * b = y,\ z * b = a$, respectivamente, en el cuasigrupo $(G, *)$.
Los cuasigrupos $(G, \backslash)$ y $(G, /)$ se denominan conjugados de $(G, *)$.

Utilizando las operaciones $(/)$ y $(\backslash)$ a veces resulta ventajoso dar una definición diferente para un lazo:

Definición 2.1.10. *Un **lazo** $(G, *, /, \backslash)$ es un conjunto G junto con tres operaciones binarias $(*)$, $(/)$, $(\backslash)$ tales que*

1. *$a * (a \backslash b) = b,\ (b/a) * a = b$ para todo $a, b \in G$,*

2. *$a \backslash (a * b) = b,\ (b * a)/a = b$ para todo $a, b \in G$,*

3. *$a \backslash a = b/b$ para todo $a, b \in G$.*

2.2. Subcuasigrupos y sublazos.

Sea $(G, *)$ un magma. Recuerde de la Sección 2.1 que $x * y = \alpha(x, y)$ para alguna $\alpha\colon G \times G \to G$. Ahora bien, para cualquier subconjunto H no vacío de G es cierto que $\emptyset \neq H \times H \subseteq G \times G$. Por lo tanto, se puede considerar la restricción β de α a $H \times H$. Es decir, $\beta(x, y) = \alpha(x, y)$ para todo $(x, y) \in H \times H$. Así H es un magma relativo a β sólo si el rango de β es un subconjunto de H, y es sólo cuando esto ocurre que consideramos a H como un submagma del magma $(G, *)$. Tomando esto en cuenta, es conveniente dejar que " $*$ " cumpla dos funciones,

$$x * y = \alpha(x, y) = \beta(x, y)$$

para todo $(x, y) \in H \times H$.

Con lo anterior, que un subconjunto H no vacío de G sea un submagma de un magma $(G, *)$ significa que $(H, *)$ es en sí mismo un magma.

Consideremos lo siguiente: Sea $G = \mathbb{R}$, el conjunto de todos los números reales, sea $H = \mathbb{R}^+$, el conjunto de todos los números reales no negativos, y sea $(-)$ la operación binaria de la resta ordinaria. Así $\emptyset \neq H \subset G$, pero H no es un submagma del magma $(G, -)$. Por otro lado, debe quedar claro que H es un submagma del magma $(G, +)$, donde " $+$ " denota suma ordinaria.

Nos interesa algo un poco más específico en esta sección. En el contexto previsto en los párrafos anteriores, formulamos lo siguiente.

Definición 2.2.1. *Un subconjunto H no vacío de un conjunto G es un subcuasigrupo (sublazo, subgrupo) de un cuasigrupo $(G, *)$ si $(H, *)$ es un cuasigrupo (lazo, grupo).*

Siempre que $(G, *)$ sea un cuasigrupo, recuerde de la **Sección 2.1** que $(G, /)$ y $(G, \backslash)$ también son cuasigrupos. Luego, con las concesiones de notación hechas al comienzo de esta sección tenemos el siguiente resultado útil.

Teorema 2.2.1. *Sea $(G, *)$ un cuasigrupo. Un subconjunto H no vacío de G es un subcuasigrupo de $(G, *)$ si y sólo si $(H, *)$,$(H, /)$ y $(H, \backslash)$ son magmas.*

Demostración.
La necesidad es clara. En cuanto a la suficiencia, supongamos que $(H, *)$, $(H, /)$, y $(H, \backslash)$ son magmas. Ahora sea $a, b \in H$. Como $a, b \in G$ existe un único $x \in G$ de modo que $a * x = b$, lo cual nos lleva a que $x = a\backslash b$, luego $x \in H$ ya que $a, b \in H$ y $(H, \backslash)$ es un magma. El hecho de que x sea el único elemento en H tal que $a * x = b$ es obvio ya que $(G, *)$ es un cuasigrupo. Asimismo, dado que $(H, /)$ es un magma, podemos demostrar que existe un único $y \in H$ tal que $y * a = b$. Por lo tanto, $(H, *)$ es un cuasigrupo y así H es un subcuasigrupo de $(G, *)$. $\square$

Dado que estamos interesados en los lazos, se incluye el siguiente teorema, aunque se ve fácilmente que es poco más que un corolario del teorema anterior.

Teorema 2.2.2. *Sea $(G, *)$ un lazo. Un subconjunto H no vacío de G es un sublazo del lazo $(G, *)$ si y sólo si $(H, *)$, $(H, /)$ y $(H, \backslash)$ son magmas.*

Demostración.
La necesidad es obvia. En cuanto a la suficiencia, sean $(H, *)$, $(H, /)$ y $(H, \backslash)$ magmas. Luego, según el **Teorema 2.2.1**, queda claro que H es un subcuasigrupo de $(G, *)$. Por tanto, $(H, *)$ es un cuasigrupo. Dado que $(G, *)$ es un lazo, $(G, *)$ tiene un elemento identidad, digamos e. Como $H \neq \emptyset$ existe $a \in H$, claramente $(a/a) * a = a = e * a$, por cancelación por la derecha en $(G, *)$ (ver **Teorema 2.1.1**) vemos que $a/a = e$. Pero $(H, /)$ es un magma, por lo que $e \in H$, evidentemente e es un elemento identidad para $(H, *)$, y nuestra demostración está completa. (Véase también el Ejercicio 1.2.A. en [Pfl90]) $\square$

Encontraremos conveniente escribir $H \leq G$ para indicar que H es un sublazo de un lazo $(G, *)$. Obviamente, sólo podemos utilizar este recurso de notación cuando sabemos por el contexto exactamente que lazo $(G, *)$ se está considerando.

Los dos teoremas anteriores resultan muy familiares en presencia de asociatividad. De hecho, resulta que si que $\emptyset \neq H \subseteq G$ entonces H es un subgrupo de un grupo $(G, *)$ si y sólo si $(H, /)$ es un magma. En concreto tenemos lo siguiente:

Proposición 2.2.1. *Si H es un sublazo de un lazo $(G, *)$, se tiene que $(H, *)$ y $(G, *)$ comparten el mismo elemento de identidad.*

Demostración. Sea e el elemento identidad en $(G, *)$ y e_1 el elemento identidad en $(H, *)$, luego $e_1 * e_1 = e_1, e * e_1 = e_1$ se sigue que $e * e_1 = e_1 * e_1$, por lo tanto $e = e_1$ por cancelación a la izquierda (ver **Teorema 2.1.1**). $\square$

Teorema 2.2.3. *Sea $(G, *)$ un grupo, para cualquier subconjunto H no vacío de G las siguientes afirmaciones son equivalentes:*

1. *$(H, *)$ es un grupo.*
2. *$(H, /)$ y $(H, \backslash)$ son magmas.*
3. *H es un subgrupo de $(G, *)$.*
4. *$H \leq G$.*

Demostración.
$1 \implies 2$. Dado que $(H, *)$ es un grupo, este es cerrado, tiene inversos, elemento identidad y es asociativo bajo la operación $(*)$.
Como H es grupo, es no vacío. Ahora sean $x, y \in H$ arbitrarios, luego $x \backslash y = z$ si y sólo si $x * z = y$ pero como $x \in H$, se tiene que existe su inverso, de manera que $z = x^{-1} * y \in H$ por ser grupo, con esto $(H, \backslash)$ es cerrado y por tanto es un magma. Análogamente se prueba que $(H, /)$ es magma.

$2 \implies 3$. Como $(H, \backslash)$ y $(H, /)$ son magmas son cerrados bajo $(\backslash)$ y $(/)$, además H es no vacío.
Ahora, sean $x, y \in H$, $x * y^{-1} = z$ si y sólo si $z * y^{-1} = x$, pero esto es cierto si y sólo si $x/y = z \in H$ por ser magma, luego $x * y^{-1} \in H$. Por tanto H es subgrupo de G.

$3 \implies 4$ Por definición de subgrupo. Ver **Definición 1.2.1**.
$4 \implies 1$ Por definición de subgrupo. Ver **Definición 1.2.1**. $\square$

Teorema 2.2.4. *Sea $(G, *)$ un cuasigrupo (lazo, grupo), sea $\emptyset \neq S \subseteq G$, y sea T cualquier conjunto no vacío de subcuasigrupos (sublazos, subgrupos) de $(G, *)$ con $S \subseteq H$ siempre que $H \in T$. Se tiene que $\bigcap_{H \in T} H$ es un subcuasigrupo (sublazo, subgrupo) de $(G, *)$ con $\emptyset \neq S \subseteq \bigcap_{H \in T} H$.*

Demostración.
Por conveniencia, sea $D = \bigcap_{H \in T} H$. Es claro que $S \subseteq D \subseteq G$. Además, $D \neq \emptyset$ ya que $S \neq \emptyset$ luego $\emptyset \neq D \subseteq G$. Ahora sean $a, b \in D$, se sigue que $a, b \in H$ para todos los $H \in T$. Dado que cada $H \in T$ es un subcuasigrupo de $(G, *)$, sabemos que cada uno de $(H, *)$, $(H, /)$, $(H, \backslash)$ es un magma (ver **Teorema 2.2.2**). Por lo tanto, $a * b \in H$, $a/b \in H$ y $a \backslash b \in H$ para todos los $H \in T$. En consecuencia, $a * b$, a/b y $a \backslash b$ son todos elementos de D. Por tanto, $(D, *)$, $(D, /)$ y $(D, \backslash)$ son magmas. Por el **Teorema 2.2.2** se deduce que D es un subcuasigrupo de $(G, *)$.

Ahora, supongamos que $(G, *)$ es un lazo y que H es un sublazo de $(G, *)$ siempre que $H \in T$. Sea e el elemento identidad de $(G, *)$. Por la **Proposicion 2.2.1** está claro que $e \in H$ para todos los $H \in T$. Luego $e \in D$ y se deduce fácilmente que el subcuasigrupo D de $(G, *)$ es un sublazo del lazo $(G, *)$.

Si $(G, *)$ es un grupo y si cada H en T es un sublazo de $(G, *)$ entonces del párrafo anterior se desprende claramente que D es un sublazo de $(G, *)$. Pero con $(G, *)$ asociativo también lo es $(D, *)$. Por tanto, D es

un subgrupo de $(G, *)$. $\square$

Ahora sea $(G, *)$ un cuasigrupo (lazo, grupo), sea $\emptyset \neq S \subseteq G$ y sea T el conjunto de todos los subcuasigrupos (sublazos, subgrupos) de $(G, *)$ que tienen S como subconjunto. Claramente $T \neq \emptyset$ ya que $G \in T$. Por tanto, podemos aplicar el Teorema 1.2.5 y deducir que $\bigcap_{H \in T} H$ es un subcuasigrupo (sublazo, subgrupo) de $(G, *)$ con $S \subseteq \bigcap_{H \in T} H$. Usaremos $\langle S \rangle$ para denotar la intersección $\bigcap_{H \in T} H$ y se tiene la siguiente definición:

Definición 2.2.2. *Sea $(G, *)$ un cuasigrupo (lazo, grupo), sea $\emptyset \neq S \subseteq G$, y sea T el conjunto de todos los subcuasigrupos (sublazos, subgrupos) de $(G, *)$ tales que $S \subseteq H$ siempre que $H \in T$. El subcuasigrupo (sublazo, subgrupo) $\langle S \rangle$ de $(G, *)$ se llama subcuasigrupo (sublazo subgrupo) generado por S.*

El conjunto $\langle S \rangle$ es el subcuasigrupo (sublazo, subgrupo) más pequeño del cuasigrupo (lazo, grupo) $(G, *)$ que contiene a S como subconjunto. En el caso de grupos, recuerde que se dispone de una caracterización muy constructiva de la generación. En el caso de que $\langle S \rangle = G$ decimos que S genera $(G, *)$ o que S es un conjunto generador para $(G, *)$. Siempre que S sea un conjunto con un único elemento $S = \{a\}$ para algún $a \in G$, acordaremos escribir $\langle a \rangle$ en lugar de $\langle \{a\} \rangle$.

Se dice que un cuasigrupo $(G, *)$ es monogénico (se prefiere la palabra cíclico si $(G, *)$ es un grupo) siempre que $G = \langle a \rangle$ para algún $a \in G$. De manera más general, un cuasigrupo $(G, *)$ se genera de manera finita siempre que $G = \langle S \rangle$ para algún subconjunto finito S de G.

Aunque un cuasigrupo $(G, *)$ podría no satisfacer una propiedad P, aún podría satisfacerlo "localmente" en el siguiente sentido: Un cuasigrupo $(G, *)$ satisface la propiedad P localmente significa que todo subcuasigrupo finitamente generado de $(G, *)$ satisface P.

Observación 2.2.1. *Notemos que dado un lazo $(G, *)$ los elementos del sublazo generado por un elemento $a \in G$, son potencias de a, es decir, $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$ dado que si $a \in H$, con $H \leq G$ entonces todas las potencias de a también están en H, por la cerradura de la operación $*$, por tanto, si $T = \{H \leq G | a \in H\}$ entonces $\langle a \rangle = \bigcap_{H \in T} H = \{a^n | n \in \mathbb{Z}\}$.*

Definición 2.2.3. *Un cuasigrupo $(G, *)$ es potencia-asociativo si $(\langle a \rangle, *)$ es un grupo para cada $a \in G$.*

Definición 2.2.4. *Un cuasigrupo $(G, *)$ es di-asociativo si $(\langle a, b \rangle, *)$ es un grupo para todo $a, b \in G$, con a y b no necesariamente distintos.*

Observación 2.2.2. *Cualquier cuasigrupo $(G, *)$ que sea di-asociativo es automáticamente potencia-asociativo porque $\langle a \rangle = \langle a, a \rangle$ para todo $a \in G$.*

Sea $(G, *)$ un lazo, y e su elemento identidad, sean x^λ y x^ρ esos elementos únicos en G tales que $x^\lambda * x = x * x^\rho = e$ para cada $x \in G$.

Definición 2.2.5. *Un lazo $(G, *)$ tiene la **propiedad de inverso derecho** si satisface las identidades $y * y^\rho = e$ y $(x * y) * y^\rho = x$.*

Definición 2.2.6. *Un lazo $(G, *)$ es **potencia alternativo derecho** si $(x * y^i) * y^j = x * y^{i+j}$ se cumple para todos los enteros i, j.*

Observación 2.2.3. *Nóte que si un lazo es potencia alternativo derecho entonces tiene la propiedad de inverso derecho.*

Definición 2.2.7. *Un **lazo de Bol derecho** es un lazo que satisface la identidad de Bol derecha $x((yz)y) = ((xy)z)y$ y un **lazo de Bol izquierdo** es un lazo que satisface la identidad de Bol izquierda $(x(yx))z = x(y(xz))$.*

Definición 2.2.8. *Un lazo de Moufang es un lazo que es un lazo Bol derecho e izquierdo.*

Teorema 2.2.5. *Si $(G, *)$ es un lazo de Bol derecho entonces:*

(i) *$(G, *)$ satisface la propiedad de inverso derecho,*

(ii) $y^\lambda = y^\rho$ *para todo* $y \in G$.

Demostración.

(i) Sea $z = y^\rho$ en la identidad de Bol derecha. Luego, $((x * y) * y^\rho) * y = x * ((y * y^\rho) * y) = x * y$ para todo $x, y \in G$. Por lo tanto, $(x * y) * y^\rho = x$ para todo $x, y \in G$.

(ii) Sea $z = y^\lambda$ en la identidad de Bol derecha. Se tiene que $((x*y)*y^\lambda)*y = x*((y*y^\lambda)*y)$ para todo $x, y \in G$. Ahora, usando la propiedad inverso derecho y el hecho de que $y = (y^\lambda)^\rho$, obtenemos que $x*y = x*((y*y^\lambda)*y)$ para todo $x, y \in G$. Por lo tanto $y*y^\lambda = e$ y así, $y^\lambda = y^\rho$ para todo $y \in G$. □

A partir de acá, cuando se trate de lazos de Bol, consideremos $x^\lambda = x^\rho = x^{-1}$.

Definición 2.2.9. *Si* x *es un elemento de un lazo de Bol derecho* $(G, *)$ *y* n *es un entero no negativo. Definimos* x^n *recursivamente por* $x^0 = e$ *y* $x^n = x^{n-1} * x$ *para* $n > 0$*. Para cualquier entero negativo* n*, definimos* x^n *por* $x^n = (x^{-1})^{|n|}$.

Lema 2.2.1. *Si* $(G, *)$ *es un lazo de Bol derecho entonces*

$$x * y^n = (x * y^{n-1}) * y = (x * y) * y^{n-1} \tag{2.1}$$

para todo $x, y \in G$ *y todos los enteros* n.

Demostración.

Por inducción. Se cumple para $n = 0$ y para $n = 1$. Ahora, asumamos que, para $k > 1$,

$$x * y^k = (x * y^{k-1}) * y = (x * y) * y^{k-1} \tag{2.2}$$

para todo $x, y \in G$ (en particular, $y^k = y^{k-1} * y = y * y^{k-1}$ para todo $y \in G$). Luego,

$$x * y^{k+1} = x * (y^k * y) = x * ((y * y^{k-1}) * y) = ((x * y) * y^{k-1}) * y = (x * y^k) * y$$

para todo $x, y \in G$. Luego, reemplazando x por $x * y$ en 2.2, obtenemos

$$(x * y) * y^k = ((x * y) * y^{k-1}) * y = x * ((y * y^{k-1}) * y) = x * (y^k * y) = x * y^{k+1}$$

para todo $x, y \in G$. Por lo tanto, 2.1 se cumple para todos los enteros $n \geq 0$.

Ahora, para todos los enteros $n > 0$ y para todo $x, y \in G$, aplicando 2.1 a x y y^{-1} obtenemos

$$x * (y^{-1})^{n+1} = (x * (y^{-1})^n) * y^{-1} = (x * y^{-n}) * y^{-1}$$

y aplicando 2.1 a xy y y^{-1} obtenemos

$$(x * y) * (y^{-1})^{n+1} = ((x * y) * y^{-1}) * (y^{-1})^n = x * y^{-n}.$$

Por lo tanto, $x * y^{-n} = (x * y^{-n-1}) * y = (x * y) * y^{-n-1}$. □

Proposición 2.2.2. *Si* $(G, *)$ *es un lazo de Bol entonces es potencia alternativo derecho.*

Demostración.
El resultado deseado es claro para $n = 0$ y, por el **Lema 2.2.1**, también se cumple para $n = 1$.
Ahora supongamos cierto para cualquier entero $n > 1$, $(x * y^m) * y^n = x * y^{m+n}$ se cumple para todos los enteros m y para todos $x, y \in G$. Por el **Lema 2.2.1**, $x * y^{m+n+1} = (x * y^{m+n}) * y = ((x * y^m) * y^n) * y = (x * y^m) * y^{n+1}$ para todos $x, y \in G$ y para todos los enteros m y todos los enteros no negativos n. (En particular, para uso posterior, $(y^n)^{-1} = y^{-n}$ para todos los enteros no negativos n y para todos $y \in G$). Reemplazando m por $m - n$, tenemos $(x * y^{m-n}) * y^n = x * y^m$.
Por lo tanto, $(x * y^{m-n}) = (x * y^m) * (y^n)^{-1} = (x * y^m) * y^{-n}$ para todos los enteros $n \geq 0$, todos los enteros m, y para todos $x, y \in G$.
En particular, $y^m * y^n = y^{m+n}$ para todos $y \in G$ y todos los enteros m y n. □

Proposición 2.2.3. *Sea $(G,*)$ un lazo. Si $(G,*)$ es de Bol derecho entonces es potencia-asociativo.*

Demostración.
Sean $x,y,z \in \langle a\rangle$ arbitrarios, para todo $a \in G$. Se tiene que $x = a^m, y = a^n, z = a^p$, para algunos enteros m,n,p. Por la **Proposición 2.2.2**, $(x*y)*z = (a^m*a^n)*a^p = a^m*a^{n+p} = a^m*(a^m*a^p) = x*(y*z)$, por lo tanto $(\langle a\rangle,*)$ es asociativo. □

2.3. Núcleo y centro de un cuasigrupo.

Sea $(G,*)$ un magma y sea $a \in G$. A veces, el papel que desempeña a como miembro de $(G,*)$ puede describirse o caracterizarse por el comportamiento de las traslaciones $L_a\colon\ G \to G$ *y* $R_a\colon\ G \to G$, que se introdujeron en la **sección 2.1**.

Definición 2.3.1. *Sea $(G,*)$ un magma y sea $a \in G$, a es nuclear izquierdo (medio, derecho) en $(G,*)$ si $L_{a*x}(y) = L_a(L_x(y))$ $(L_{x*a}(y) = L_x(L_a(y)), R_{x*a}(y) = R_a(R_x(y)))$ para todo $x,y \in G$. Además, a es nuclear en $(G,*)$ si a es nuclear izquierdo, medio y derecho en $(G,*)$.*

Proposición 2.3.1. *Sea $(G,*)$ un magma y sea $a \in G$. Las siguientes afirmaciones son equivalentes:*

1. *a es nuclear por la izquierda,*
2. *$a*(x*y) = (a*x)*y$ para todo $x,y \in G$,*
3. *$L_a(R_x(y)) = R_x(L_a(y))$ para todo $x,y \in G$.*

Demostración.
$1 \Longrightarrow 2$. Si a es nuclear izquierdo entonces $L_{a*x}(y) = L_a(L_x(y)$, es decir $(a*x)*y = a*(x*y)$, para todo $x,y \in G$.
$2 \Longrightarrow 3$. Si $a*(x*y) = (a*x)*y$ para todo $x,y \in G$ entonces $L_a(R_x(y)) = a*(y*x) = (a*y)*x = R_x(L_a(y))$.
$3 \Longrightarrow 1$. Si $L_a(R_x(y)) = R_x(L_a(y))$ para todo $x,y \in G$, basta con desarrollar ls aplicaciones en la igualdad y se tiene el resultado. □

La proposición anterior corresponde al Ejercicio 1.3.A en [Pfl90], la prueba de los Ejercicios 1.3.B y I.3.C también en [Pfl90] es análoga a la anterior.

Definición 2.3.2. *Sea $(G,*)$ un magma. El núcleo izquierdo N_λ (núcleo medio N_μ, núcleo derecho N_ρ) de $(G,*)$ es el conjunto de todos los elementos nucleares izquierdos (medios, derechos) en $(G,*)$ y el núcleo N de $(G,*)$ viene dado por $N = N_\lambda \cap N_\mu \cap N_\rho$.*

En vista de las definiciones anteriores y los Ejercicios 1.3.A, I.3.B y I.3.C, queda claro que

$$\begin{aligned} N_\lambda &= \{a \in G \mid a*(x*y) = (a*x)*y,\ x,y \in G\},\\ N_\mu &= \{a \in G \mid (x*a)*y = x*(a*y),\ x,y \in G\},\\ N_\rho &= \{a \in G \mid (x*y)*a = x*(y*a),\ x,y \in G\}\ . \end{aligned}$$

No hay garantía de que existan elementos nucleares izquierdos, medios o derechos y por lo tanto, cualquiera de $N_\lambda,\ N_\mu,\ N_\rho, N$ bien podría estar vacío.

Ejemplo 2.3.1. *sea $A = \{1,2,3\}$ y defina $(*)$ mediante la tabla de Cayley:*

$*$	1	2	3
1	1	1	2
2	1	1	2
3	2	2	2

Aquí los tres $N_\lambda,\ N_\mu$ y N_ρ son vacíos. En efecto

Para $a = 1$:

$$L_{1*2}(3) = L_1(3) = 2$$
$$L_1(L_2(3)) = L_1(2) = 1$$
$$\Rightarrow \exists x, y \in G \textit{ tal que } L_{a*x}(y) \neq L_a(L_x(y))$$
$$\therefore 1 \notin N_\lambda.$$

Para $a = 2$:

$$L_{2*1}(3) = L_1(3) = 2$$
$$L_2(L_1(3)) = L_2(2) = 1$$
$$\Rightarrow \exists x, y \in G \textit{ tal que } L_{a*x}(y) \neq L_a(L_x(y))$$
$$\therefore 2 \notin N_\lambda.$$

Para $a = 3$:

$$L_{3*1}(2) = L_2(2) = 1$$
$$L_3(L_2(1)) = L_3(1) = 2$$
$$\Rightarrow \exists x, y \in G \textit{ tal que } L_{a*x}(y) \neq L_a(L_x(y))$$
$$\therefore 3 \notin N_\lambda.$$

Con esto verificamos que $N_\lambda = \emptyset$, análogamente se verifica que N_μ y N_ρ son vacíos.

Teorema 2.3.1. *Sea $(G, *)$ un magma. Si N_λ $(N\mu,\ N\rho)$ no es vacío entonces $N_\lambda(N_\mu,\ N_\rho)$ es un submagma de $(G, *)$.*

Demostración. Supongamos que $N_\lambda \neq \emptyset$, y sea $a, b \in N_\lambda$. Vemos que

$$L_{(a*b)*x} = L_{L_{a*b}(x)} = L_{L_a(L_b(x))} = L_{a*(b*x)} = L_a(L_{b*x}) = L_a(L_b(L_x)) = L_{a*b}(L_x)$$

para todo $x \in G$, por lo que $a*b$ es nuclear izquierdo de acuerdo con la **Definición 2.3.1**. De ello se deduce que N_λ es un submagma de $(G, *)$. De manera similar se puede demostrar que $N\mu$ y N_ρ, son submagmas de $(G, *)$ siempre que no sean vacíos. □

Es claro (ver Ejercicio I.3.F en [Pfl90]) que siempre que $N_\lambda(N_\mu, N_\rho)$ es un submagma de un magma $(G, *)$, de hecho, es un submagma asociativo de $(G, *)$. Si el magma $(G, *)$ es un cuasigrupo, podemos decir más sobre los núcleos, como se indica a continuación:

Teorema 2.3.2. *Sea $(G, *)$ un cuasigrupo.*

(i) Si $N_\mu \neq \emptyset$ entonces N_μ es un subgrupo de $(G, *)$ y el elemento identidad e de $(N_\mu, *)$ es el elemento identidad de $(G, *)$.

(ii) Si $N_\lambda \neq \emptyset$ entonces N_λ es un subgrupo de $(G, *)$ y el elemento identidad de $(N_\lambda, *)$ es un elemento identidad a la izquierda de $(G, *)$.

(iii) Si $N_\rho \neq \emptyset$ entonces N_ρ es un subgrupo de $(G, *)$ y el elemento identidad de $(N_\rho, *)$ es un elemento identidad a la derecha de $(G, *)$.

Demostración.
(i) Suponga que $N_\mu \neq \emptyset$, y sea $a \in N_\mu$. Dado que $(G, *)$ es un cuasigrupo, existe un único elemento identidad local a la derecha $e \in G$ tal que $a * e = a$. También tenemos que $(x * a) * e = x * (a * e) = x * a$ para todo $x \in G$ (ya que $a \in N_\mu$). Pero cada elemento $y \in G$ es de la forma $x * a$, así que tenemos $y * e = y$ para todo $y \in G$, luego e es un elemento identidad a la derecha para $(G, *)$.
Ahora para $x \in G$ sean x^λ y x^ρ elementos únicos en G tales que $x^\lambda * x = x * x^\rho = e$. Vemos que $a * a^\rho = e = e * e = e * (a * a^\rho) = (e * a) * a^\rho$ (ya que $a \in N_\mu$), pero $(G, *)$ es cancelativo, así que $a * a^\rho = (e * a) * a^\rho$ implica que $e * a = a$. Luego, $a * x = (e * a) * x = e * (a * x)$ para todo $x \in G$. Cada elemento $y \in G$ es de la forma $a * x$ y por lo tanto $y = e * y$ para todo $y \in G$. Así, e es también un elemento identidad a la izquierda para $(G, *)$. Por tanto, e debe ser el elemento identidad para $(G, *)$.

Dado que e es el elemento identidad para $(G, *)$, se tiene que $(x * e) * y = x * y = x * (e * y)$ para todo $x, y \in G$, así, $e \in N_\mu$. Ahora, para todo $b \in N_\mu$ tenemos que $b^\lambda * (b * b^\lambda) = (b^\lambda * b) * b^\lambda = e * b^\lambda = b^\lambda = b^\lambda * e$ y así, por cancelación, se sigue que $b * b^\lambda = e = b * b^\rho$. Nuevamente, por cancelación se prueba que $b^\lambda = b^\rho$. Para conveniencia, definamos b^{-1} como $b^{-1} = b^\lambda = b^\rho$ para todo $b \in N_\mu$.

Ahora, para todo $b \in N_\mu$ y para todo $x \in G$ se cumple que $((x * b) * b^{-1}) * b = (x * (b * b^{-1})) * b = (x * e) * b = x * b$, pero notamos que cada $y \in G$ es de la forma $x * b$. Así, $(y * b^{-1}) * b = y$ para todo $y \in G$, luego $R_b = R_{b^{-1}}$ para todo $b \in N_\mu$. Examinando la expresión $b * (b^{-1} * (b * x))$, se deduce de manera similar que $L_b = L_{b^{-1}}$ para todo $b \in N_\mu$. Sean $b, c \in N_\mu$, con la información anterior obtenemos que $c/b = R_b^{-1}(c) = R_{b^{-1}}(c) = c * b^{-1}$ y que $b * c = L_b^{-1}(c) = L_{b^{-1}}(c) = b^{-1} * c$. Pero sabemos que $b^{-1} \in N_\mu$ (ver arriba) y así, por el **Teorema 2.1.2**, se deduce que c/b y $b\backslash c$ están ambos en N_μ, por tanto $(N_\mu, *)$, $(N_\mu/)$, y $(N_\mu\backslash)$ son magmas. Por el **Teorema 2.2.2** concluimos que N_μ es un subcuasigrupo de $(G, *)$. Pero $(N_\mu, *)$ también es asociativo y tiene un elemento identidad e, que se demostró que es el elemento identidad para $(G, *)$. Esto completa nuestra prueba de (i).

(ii) Sea $N_\lambda \neq \emptyset$ y sea $a \in N_\lambda$, dado que $(G, *)$ es un cuasigrupo, existe un único elemento $e \in G$ tal que $a * e = a$. Se sigue que $a * ((e * x) * y) = (a * (e * x)) * y = ((a * e) * x) * y = (a * x) * y = a * (x * y) = (a * e) * (x * y) = a * (e * (x * y))$ para todo $x, y \in G$ (observe como hemos repetido el uso de $a \in N_\lambda$). Pero por cancelación $a * ((e * x) * y) = a * (e * (x * y))$ implica que $(e * x) * y = e * (x * y)$. Luego, tenemos $e \in N_\lambda$. Ahora, para todo $x \in G$ también tenemos $a * (e * x) = (a * e) * x = a * x$ y por cancelación, obtenemos $e * x = x$. Así, e es un elemento identidad a la izquierda para $(G, *)$. Para todo $b \in N_\lambda$ tenemos $(b * e) * a = b * (e * a) = b * a$ (ya que e es un elemento identidad a la izquierda para $(G, *)$). Concluimos, por cancelación, que $b * e = b$ para todo $b \in N_\lambda$, luego e es el elemento identidad para $(N_\lambda, *)$.

Sea $b \in N_\lambda$, y sea b^λ y b^ρ tal como en la prueba de (i). Es decir,si b^λ y b^ρ son esos elementos únicos en G tales que $b^\lambda * b = b * b^\rho = e$ entonces $e * b = b = b * e = b * (b^\lambda * b) = (b * b^\lambda) * b$ y por cancelación, tenemos que $b * b^\lambda = e$. Pero b^ρ es el único elemento en G tal que $b * b^\rho = e$, así, $b^\lambda = b^\rho$. Por lo tanto, definamos b^{-1} como $b^{-1} = b^\lambda = b^\rho$ para todo $b \in N_\lambda$.

Para $b \in N_\lambda$ y $x, y \in G$ tenemos $b * (b^{-1} * (x * y)) = (b * b^{-1}) * (x * y) = e * (x * y) = x * y$ (ya que e es un elemento identidad a la izquierda para $(G, *)$). Pero $x * y = (e * x) * y = ((b * b^{-1}) * x) * y = (b * (b^{-1} * x)) * y = b * ((b^{-1} * x) * y)$, por tanto, $b * ((b^{-1} * x) * y) = b * ((b^{-1} * x) * y)$ y por cancelación, $b^{-1} * (x * y) = (b^{-1} * x) * y$. Así, $b^{-1} \in N_\lambda$ cuando $b \in N_\lambda$.

Para $b, c \in N_\lambda$ tenemos $(R_b^{-1}(c)) * b = c = c * e = c * (b^{-1} * b) = (c * b^{-1}) * b$ y $b * L_b^{-1}(c)) = c = e * c = (b * b^{-1}) * c = b * (b^{-1} * c)$, ahora por cancelación tenemos que $R_b^{-1}(c) = c * b^{-1}$ y $L_b^{-1}(c) = b^{-1} * c$ para todo $a, b \in N_\lambda$, ahora c/b y $b\backslash c$ están en N_λ cuando $b, c \in N_\lambda$, pero sabemos que $b^{-1} \in N_\lambda$. Usando el **Teorema 2.1.2** y el hecho de que $b^{-1} \in N_\lambda$ cuando $b \in N_\lambda$, concluimos que $(N_\lambda, *)$, $(N_\lambda\backslash)$ y $(N_\lambda/)$ son magmas.

(iii) La prueba es análoga a **(ii)**. Sin embargo, debe tomarse en cuenta que **(iii)** es dual de **(ii)** en el siguiente sentido: para $x, y \in G$, tomemos $x \cdot y = y * x$ tomemos en cuenta que $(G, \cdot)$ también es un cuasigrupo. Ahora N_ρ, que es el núcleo derecho de $(G, *)$, es claramente el núcleo izquierdo de $(G, \cdot)$. Ahora aplicando **(ii)** a $(G, \cdot)$, se tiene el resultado. $\square$

Consideremos el siguiente ejemplo:

Ejemplo 2.3.2. *Sea $G = \{e, x, y\}$ con $|G| = 3$ y sea $(*)$ definida por la tabla de Cayley*

$*$	e	x	y
e	e	x	y
x	y	e	x
y	x	y	e

Se tiene que $(G, *)$ es un cuasigrupo, $N_\lambda = \{e\}$, e es un elemento identidad a la izquierda para $(G, *)$, pero e no es un elemento identidad para $(G, *)$. Así, cuando $(G, *)$ es un cuasigrupo que no es un lazo, uno

no puede esperar mejorar las afirmaciones (ii) y (iii) del **Teorema 2.3.2**. Por supuesto, si $(G, *)$ es un lazo, sabemos que $(G, *)$ comparte su elemento identidad con cada uno de sus sublazos.

Teorema 2.3.3. *Si $(G, *)$ es un lazo entonces los núcleos N_λ, N_μ y N_ρ son subgrupos de $(G, *)$.*

Demostración.
Sea e el elemento identidad de $(G, *)$. Está claro que $e \in N_\lambda \cap N_\mu \cap N_\rho$. Por tanto, cada uno de los núcleos no es vacío y solo es necesario recurrir al **Teorema 2.3.2**. □

Definición 2.3.3. *Sea $(G, *)$ un magma. El centro Z de $(G, *)$ viene dado por*

$$Z = \{a \in N \mid L_a = R_a\},$$

donde N es el núcleo de $(G, *)$.

Es evidente que un elemento $a \in G$ pertenece al centro Z de un magma $(G, *)$ si y sólo si

$$a * (x * y) = (a * x) * y, \quad (x * a) * y = x * (a * y), \quad (x * y) * a = x * (y * a), \quad \text{y} \quad a * x = x * a$$

para todo $x, y \in G$. Los siguientes resultados son consecuencias de los **Teoremas 2.3.1,2.3.2, 2.3.3**.

Teorema 2.3.4. *Sea $(G, *)$ un magma con núcleo N y centro Z. Si N y Z no son vacíos entonces ambos son submagmas de $(G, *)$, siendo Z un submagma conmutativo de $(N, *)$.*

Demostración.
Como N no es vacío, por el **Teorema 2.3.1** se tiene que N es un magma. Ahora si $a, b \in Z$ entonces $L_{a*b}(y) = L_a(L_b(y)) = R_a(R_b(y)) = R_{b*a}(y) = R_{a*b}(y)$, ya que $a, b \in Z \subseteq N$ entonces Z es cerrado bajo $(*)$, por tanto $(Z, *)$ es submagma de $(G, *)$. Además, es conmutativo por la **Definición 2.1.4** . □

Teorema 2.3.5. *Sea $(G, *)$ un cuasigrupo con núcleo N y centro Z. Si N no es vacío entonces Z no es vacío y N y Z son subgrupos de $(G, *)$, siendo Z un subgrupo conmutativo de $(N, *)$.*

Demostración.
Dado que N es no vacío, se sigue que es subgrupo $(G, *)$ por el **Teorema 2.3.2**, ahora $e \in N$ (elemento identidad), pero $L_e = R_e$, por tanto $e \in Z$ y por el **Teorema 2.3.4**, se tiene el resultado. □

Teorema 2.3.6. *Si $(G, *)$ es un lazo con núcleo N y centro Z entonces N y Z son subgrupos de $(G, *)$, siendo Z un subgrupo conmutativo de $(N, *)$.*

Demostración.
Consecuencia directa de **Teorema 2.3.5**. □

Capítulo 3

Índices de sublazos y descomposición de clases laterales.

En teoría de grupos resulta de mucha importancia el estudio de subgrupos y el análisis del comportamiento de las clases laterales respectivas a dichos subgrupos, dado que ellas nos permiten definir otras estructuras que resultan ser de suma importancia, tales como subgrupos normales y grupo cociente, además se sabe que las clases laterales respecto a un subgrupo forman no solo un recubrimiento para el grupo, si no que también forman una partición del mismo. En este capítulo se presenta un estudio similar al realizado en teoría de grupos. Dado un lazo G y un sublazo H, se pretende entender como se comportan las clases laterales módulo H, principalmente bajo que condiciones podemos obtener una partición de G mediante estas clases laterales, así como algunas de sus propiedades.

3.1. Clases laterales y descomposición de clases laterales.

Parte de lo que se sabe sobre los subcuasigrupos o sublazos es simplemente una generalización manifiesta de ciertos resultados estándar de la teoría de grupos. A continuación se presenta una de esas generalizaciones. Tiene que ver con clases laterales, descomposiciones de clases laterales y resultados tipo Lagrange.

Sea $(G, *)$ un lazo y sea $H \leq G$ (es decir, H es un sublazo de $(G, *)$). Sea $a \in G$, definimos aH y Ha por

$$aH = \{a * h \,|h \in H\} \text{ y } Ha = \{h * a \,|h \in H\}.$$

Claramente, aH y Ha son subconjuntos de G. Cualquier subconjunto de G formado de esta manera se llama clase lateral de H o clase lateral módulo H. Específicamente, formulamos lo siguiente.

Definición 3.1.1. *Sea $(G, *)$ un lazo, sea $H \leq G$ y sea $K \subseteq G$. Se dice que K es una clase lateral izquierda (derecha) módulo H si que $K = aH$ ($K = Ha$) para algún $a \in G$.*

Lema 3.1.1. *Sea $(G, *)$ un lazo, si H y K son sublazos de G entonces para todo $x \in G$, se cumple que $x(H \cap K) = xH \cap xK$.*

Demostración.
Claramente, $x(H \cap K) \subseteq xH \cap xK$. Sea $y \in xH \cap xK$, entonces $y = xh = xk$ para algún $h \in H$ y $k \in K$. Al cancelar, obtenemos $h = k \in H \cap K$. □

Corolario 3.1.1. *Si G es un lazo y H_i son sublazos de G para $i = 1, ..., n$ entonces $x(\bigcap_{i=1}^{n} H_i) = \bigcap_{i=1}^{n} xH_i$, para todo $x \in G$.*

Demostración.
Por inducción, notamos que se cumple para $n = 2$ por **Lema 3.1.1**, asumamos cierto para n, es decir $x(\bigcap_{i=1}^{n} H_i) = \bigcap_{i=1}^{n} xH_i$, para todo $x \in G$. Probar para $n + 1$:

$$\left(\bigcap_{i=1}^{n+1} xH_i\right) = \left(\bigcap_{i=1}^{n} xH_i\right) \cap xH_{n+1} = x\left(\bigcap_{i=1}^{n} H_i\right) \cap xH_{n+1} = x\left(\bigcap_{i=1}^{n} H_i \cap H_{n+1}\right) = x\left(\bigcap_{i=1}^{n+1} H_i\right)$$

□

Observación 3.1.1. *Recuerde de teoría de conjuntos que P es una partición de un conjunto no vacío G significa que*

1. $P \subseteq 2^G$.
2. $X \neq \emptyset$ *siempre que* $X \in P$.
3. $G = \bigcup_{X \in P} X$.
4. $X = Y$ *siempre que* $X \in P$ *y* $Y \in P$ *y* $X \cap Y \neq \emptyset$.

Definición 3.1.2. *Sea $(G, *)$ un lazo y sea $H \leq G$. $(G, *)$ tiene una descomposición de clases laterales izquierda (derecha) módulo H si el conjunto P de todas las clases laterales izquierdas (derechas) módulo H es una partición de G.*

Sea $(G, *)$ el lazo dado en el **Ejemplo 2.1.1** y sea $H = \{1, 2\}$. Claramente $H \leq G$ y las clases laterales izquierdas módulo H son las siguientes: $1H = \{1, 2\}$, $2H = \{1, 2\}$, $3H = \{3, 5\}$, $4H = \{3, 4\}$, $5H = \{4, 5\}$. Por inspección queda claro que el conjunto P de las clases laterales izquierdas módulo H no constituye una partición de G (nótese que $3H \cap 4H \neq \emptyset$, pero $3H \neq 4H$). Por lo tanto, $(G, *)$ no tiene una descomposición lateral izquierda módulo H.

Ejemplo 3.1.1. *Sea $G = \{1, 2, 3, 4, 5, 6, 7, 8\}$ y sea $(*)$ definido por la siguiente tabla de Cayley:*

$*$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	1	2	8	7	5	6
4	4	3	2	1	7	8	6	5
5	5	6	7	8	1	2	3	4
6	6	5	8	7	2	1	4	3
7	7	8	5	6	4	3	1	2
8	8	7	6	5	3	4	2	1

Sea $H = \{1, 2\}$. Nótese que $1H = 2H = \{1, 2\}$, $3H = 4H = \{3, 4\}$, $5H = 6H = \{5, 6\}$, $7H = 8H = \{7, 8\}$. El conjunto de clases laterales izquierdas módulo H forma una partición del conjunto G. Por lo tanto, $(G, *)$ tiene una descomposición de clases laterales izquierdas módulo H.

Teorema 3.1.1. *Sea $(G, *)$ un lazo y sea $H \leq G$. $(G, *)$ tiene una descomposición de clases laterales izquierdas (derechas) módulo H si y sólo si $(a * h)H = aH$ $(H(h * a) = Ha)$ para todo $a \in G$ y todo $h \in H$.*

Demostración.
Sea e el elemento identidad del lazo $(G, *)$ y sea P el conjunto de todas las clases laterales izquierdas módulo H.
($\Longrightarrow$) Si $(G, *)$ tiene una descomposición de clases laterales izquierdas módulo H entonces P es una partición de G, para $a \in G$ y $h \in H$ notamos que $a * h = (a * h) * e$ y así $a * h \in aH \cap (a * h)H$. Por lo tanto, $aH \in P$, $(a * h)H \in P$ y $(a * h)H \cap aH \neq \emptyset$. Como P es una partición de G, por **(4)** en la **Observación 3.1.1** vemos que $(a * h)H = aH$.

($\Longleftarrow$)Supongamos ahora que $(a * h)H = aH$ para todo $a \in G$ y todo $h \in H$. Es claro que $P \subseteq 2^G$ y para cada $g \in G$ notamos que $g = g * e \in gH$, así $G = \bigcup_{X \in P} X$. Además, si $X \in P$ entonces $X = gH$ para algún $g \in G$, se sigue que $g = g * e \in gH$, es decir, $X \neq \emptyset$. Finalmente, para aH y bH en P con $aH \cap bH \neq \emptyset$, debemos mostrar que $aH = bH$. Si $aH \cap bH \neq \emptyset$, hay $g \in aH \cap bH$, con esto, $g = a * x = b * y$ para algunos $x, y \in H$, por la suposición anterior se sigue que $aH = (a * x)H = (b * y)H = bH$. Por lo tanto, P es una partición de G.

Para completar la prueba solo necesitamos mostrar que $(G, *)$ tiene una descomposición de clases laterales derechas módulo H si y sólo si $H(h * a) = Ha$ para todo $h \in H$ y todo $a \in G$. Solo necesitamos modificar o imitar la primera parte de nuestra prueba. $\square$

Definición 3.1.3. *Sea $(G,*)$ un lazo finito y sea $H \leq G$. Un sublazo H de $(G,*)$ es de Lagrange si $|H|$ divide $|G|$.*

Definición 3.1.4. *Sea $(G,*)$ un lazo finito, $(G,*)$ satisface la propiedad débil de Lagrange si cada sublazo finito H de $(G,*)$ es de Lagrange.*

Definición 3.1.5. *Sea $(G,*)$ un lazo finito. $(G,*)$ satisface la propiedad fuerte de Lagrange si $(H,*)$ satisface la propiedad débil de Lagrange siempre que H sea un sublazo de $(G,*)$.*

Para que un lazo finito $(G,*)$ cumpla la propiedad fuerte de Lagrange, debe suceder que $|H|$ divide $|K|$ siempre que $H \leq K \leq G$. Encontraremos lazos finitos que satisfacen la propiedad débil de Lagrange sin satisfacer la propiedad fuerte de Lagrange. Consideremos el siguiente ejemplo: sea $(G,*)$ un lazo de orden 10, y sea $\{e\}, H, K$ los únicos sublazos de $(G,*)$. Además, sea $H \leq K \leq G$ y $|H| = 2, |K| = 5$. Dado que 1, 2, 5 dividen 10, $(G,*)$ tiene la propiedad débil de Lagrange. Pero $(K,*)$ no tiene la propiedad débil de Lagrange ($|H|$ no es divisor de $|K|$), por lo tanto $(G,*)$ no tiene la propiedad fuerte de Lagrange.

Teorema 3.1.2. *Sea $(G,*)$ un lazo finito y sea $H \leq G$. Si $(G,*)$ tiene una descomposición de clases laterales izquierdas (derechas) módulo H entonces H es de Lagrange.*

Demostración.
Sea $(G,*)$ un lazo finito, tal que tenga una descomposición de clases laterales izquierdas módulo H y sea P el conjunto de todos las clases laterales izquierdas módulo H. Dado que P es una partición de G, es claro que

$$|G| = \sum_{X \in P} |X|.$$

Pero ahora miremos los sumandos más de cerca. Sea $X \in P$ y note que $X = aH$ para algún $a \in G$. Sea α una aplicación dada por $\alpha(h) = a * h$ para todo $h \in H$. Dado que $(G,*)$ es un cuasigrupo se tiene que $\alpha : H \to aH$ es una biyección. Por lo tanto, $|H| = |X|$. Se sigue fácilmente que

$$|G| = \sum_{X \in P} |X| = m|H|$$

donde $m = |P|$. Así, $|H|$ divide $|G|$. Una modificación de este argumento produce la misma conclusión cuando G tiene una descomposición de clases laterales derechas módulo H. □

Teorema 3.1.3. *Sea $(G,*)$ un lazo finito y sea $H \leq G$. Si $(a*h)H = aH$ ($H(h*a) = Ha$) para todo $a \in G$ y todo $h \in H$ entonces H es de Lagrange.*

Demostración.
Por los **Teoremas 3.1.1** y **3.1.2** se tiene el resultado. □

Definición 3.1.6. *Sea $(G,*)$ un lazo y $H \leq G$, con $(G,*)$ teniendo descomposiciones de clases laterales izquierdas y derechas módulo H. H se llama un sublazo normal si*

$$xH = Hx, \quad (xH)y = x(Hy) \quad y \quad x(yH) = (xy)H.$$

Proposición 3.1.1. *El centro Z de un lazo $(G,*)$ es un sublazo normal de $(G,*)$.*

Demostración.
Verifiquemos si G tiene una descomposición en clases laterales módulo Z, sea $y \in xZ$, se sigue que $y = x*z = (x*z)*e \in (x*z)Z$, para algún $z \in Z$, con lo cual $xZ \subset (x*z)Z$. Ahora, si $y \in (x*z)Z$ entonces $y = (x*z)*z_1 = x*(z*z_1) \in xZ$, para algún $z_1 \in Z$ y por ser Z subgrupo conmutativo del núcleo de G, por tanto $(x*z)Z \subset xZ$. Las condiciones de normalidad se cumplen dado que Z es subgrupo conmutativo del núcleo de G (ver **Teorema 2.3.6**). □

Observación 3.1.2. *Por la definición de sublazo normal, un lazo $(G,*)$ tiene una descomposición en clases laterales módulo sus sublazos normales. De manera similar, un lazo $(G,*)$ tiene una descomposición en clases laterales módulo su núcleo N. Esto puede verse de la siguiente manera. Dado $x \in G$ y $n, n_1 \in N$, entonces $(x*n)*n_1 = x*(n*n_1)$, por lo tanto, $(x*n)N = xN$, de manera similar para el lado derecho.*

Lema 3.1.2. *Sea $(G,*)$ un lazo y sea $H \leq G$ generado por un elemento. Si G es potencia alternativo derecho (ver **Definición 2.2.6**) entonces G tiene una descomposición de clases laterales izquierdas módulo H.*

Demostración.
Por el **Teorema 3.1.1**, basta con mostrar que $(x * h)H = xH$ para todo $x \in G$ y $h \in H$. Como H es generado por un elemento, podemos asumir que $H = \langle t \rangle$ y debemos probar que $(x * t^n)H = xH$ para todo x, dado que $h = t^n$ para algún n entero. Procedamos por doble inclusión, sea $y \in (x * t^n)H$, se sigue que $y = (x * t^n) * t^m = x * t^{n+m} \in xH$, ya que t^{n+m} se sigue quedando en H. Ahora, si $y \in xH$ entonces $y = x * t^m = (x * t^n)t^{m-n} \in (x * t^n)H$, ya que t^{m-n} se sigue quedando en H. □

Proposición 3.1.2. *Si $(G,*)$ un lazo de Bol derecho entonces G tiene una descomposición de clases laterales izquierdas módulo $\langle a \rangle$ para todo $a \in G$.*

Demostración.
Por la **Proposición 2.2.2**, G es potencia alternativo derecho y por el **Lema 3.1.2** se tiene el resultado. □

Definición 3.1.7. *Sea $(G,*)$ un lazo, el conjunto generado por las traslaciones derechas $Mlt_\rho(G) = \langle R_x | x \in G \rangle$, se denomina grupo de multiplicación derecho de G.*

Al considerar la composición de aplicaciones como operación sobre $Mlt_\rho(G)$, éste toma estructura de grupo, ya que sus elementos son composiciones de traslaciones y de sus inversas, además son biyectivas (por ser G un lazo), su elemento identidad es R_e, donde e es elemento identidad de G, las demás propiedades de grupo se cumplen por las propiedades de la composición de aplicaciones y por ser biyectivas.

Definición 3.1.8. *Dados un lazo G y un sublazo $H \leq G$, el conjunto $Mlt_\rho(G,H) = \langle R_x | x \in H \rangle$ es el grupo de multiplicación derecho relativo de G respecto a H.*

Proposición 3.1.3. *Sean $(G,*)$ y $H \leq G$, tanto $Mlt_\rho(G)$ como $Mlt_\rho(G,H)$ actúan sobre G (ver **Definición 1.1.6**).*

Demostración.
Consideremos la función $f\colon Mlt_\rho(G) \times G \to G$, mediante la cual un par (g,x) es enviado a $g(x)$, recordemos que g es una composición de traslaciones derechas y de sus inversas.

1. Dado que la identidad en $Mlt_\rho(G)$ es R_e se tiene que $R_e(x) = x * e = x$ para todo $x \in G$.
2. Dados dos elementos cualesquiera g, h en $Mlt_\rho(G)$, se cumple que $g(h(x)) = (g \circ h)(x)$ (definición de composición) para todo $x \in G$.

Por lo tanto $Mlt_\rho(G)$ actúa sobre G. Análogamente se verifica que $Mlt_\rho(G,H)$ actúa sobre G. □

Dado que $Mlt_\rho(G)$ y $Mlt_\rho(G,H)$ actúan sobre G, estos dividen los elementos de G en órbitas. Sea $O_x(G,H)$ la órbita de un elemento $x \in G$ bajo $Mlt_\rho(G,H)$.

Lema 3.1.3. *Sean $(G,*)$ un lazo y $H \leq G$.*

(i) Si $|O_x(G,H)|$ es un múltiplo de $|H|$ para cada $x \in G$ entonces H es Lagrange en G.

(ii) Si $O_x(G,H)$ puede escribirse como una unión disjunta de clases laterales derechas de H para cada $x \in G$ entonces G tiene una descomposición (partición) de clases laterales izquierdas módulo H.

Demostración.
Ambas afirmaciones se deducen inmediatamente del hecho de que las órbitas forman una partición de G. □

Observación 3.1.3. *Recordemos de teoría de conjuntos lo siguiente:*

1. *Dado un conjunto X y F una familia de subconjuntos no vacíos de X, se dice que F es un recubrimiento de X o que X está cubierto por F si y sólo si $X = \bigcup_{A \in F} A$.*
2. *F es una partición de X si y sólo si es un recubrimiento de X y cada par de sus miembros son mutuamente disjuntos.*

Con la observación anterior se verifica que, dado un lazo G, $H \leq G$, $F_i = \{xH | x \in G\}$ y $F_d = \{Hx | x \in G\}$, si G tiene una descomposición de clases laterales izquierdas (derechas) módulo H entonces G está cubierto por F_i (F_d).

3.2. Índice de un sublazo.

Si un lazo tiene una descomposición en clases laterales izquierdas módulo un sublazo entonces podemos definir un índice izquierdo del sublazo en el lazo.

Definición 3.2.1. *Sea $(G, *)$ un lazo y $H \leq G$, con G teniendo una descomposición en clases laterales izquierdas módulo H. Sea X una transversal izquierda de H en G (ver **Definición 1.3.5**). El índice izquierdo de H en G es la cardinalidad de X, denotada por $[G : H]_l = n$, donde n es finito o infinito (nótese que esta es una definición bien establecida desde que las clases laterales forman una partición).*

Lema 3.2.1. *Sea $(G, *)$ un lazo, K y H sublazos de G. Si G tiene descomposiciones en clases laterales izquierdas módulo H y K entonces G tiene una descomposición en clases laterales izquierdas módulo $H \cap K$ y si $xH \cap yK$ para $x, y \in G$ es no vacío entonces $xH \cap yK$ es una clase lateral izquierda de $H \cap K$ en G.*

Demostración.
Sea $x \in G$ y $t \in H \cap K$. Por el **Lema 3.1.1** y el **Teorema 3.1.1**, tenemos que

$$x(H \cap K) = xH \cap xK = (x * t)H \cap (x * t)K = (x * t)(H \cap K).$$

Por la **Teorema 3.1.1** se tiene que G tiene una descomposición en clases laterales izquierdas módulo $H \cap K$. Esto prueba la primera parte de nuestro lema.

Asumamos ahora que $xH \cap yK$ es no vacío y $z \in xH \cap yK$. Por el **Teorema 3.1.1**, se sigue que $zH = xH$ y $zK = yK$. Así, $zH \cap zK = xH \cap yK$. Por el **Lema 3.1.1**, obtenemos que $xH \cap yK = z(H \cap K)$. □

Proposición 3.2.1. *Sea $(G, *)$ un lazo y H y K sublazos de G con G teniendo descomposiciones en clases laterales izquierdas módulo H y K. Si H y K tienen índice izquierdo finito en G entonces $H \cap K$ tiene índice izquierdo finito en G. Específicamente*

$$[G : H \cap K]_l \leq [G : H]_l [G : K]_l.$$

Demostración.
A cada clase lateral $x(H \cap K)$ asignamos el par ordenado de clases laterales (xH, xK). Dado que por el **Teorema 3.1.1** tenemos $(x * h)H = xH$ y $(x * k)K = xK$ para todo $h \in H$, $k \in K$, esta asignación está bien definida. Debemos mostrar que la aplicación $x(H \cap K) \to (xH, xK)$ es inyectiva. Sea $(xH, xK) = (yH, yK)$ y supongamos $x = y * h = y * k$ para algún $h \in H$, $k \in K$. Por cancelación concluimos $h = k$. Por el **Teorema 3.1.1** y el **Lema 3.2.1** se sigue que $x(H \cap K) = (y * h)(H \cap K) = y(H \cap K)$. □

El siguiente corolario es el **Teorema de Poincaré** para lazos.

Corolario 3.2.1. *Sea G un lazo y $H_1, \ldots, H_n$ sublazos de G con G teniendo descomposiciones en clases laterales izquierdas módulos $H_1, \ldots, H_n$. Si $H_1, \ldots, H_n$ tienen cada uno índice izquierdo finito en G entonces $H_1 \cap \cdots \cap H_n$ tiene índice izquierdo finito en G.*

Dado un lazo G y un sublazo H, es claro que $G = \bigcup_{x \in G} xH$, por lo que G es la unión (no necesariamente disjunta) de clases laterales de H. Si G es la unión de una familia F de clases laterales de H, decimos que F es irredundante si $A \in F$ implica que A no está contenida en ninguna otra $B \in F$. Observamos que esto es un recubrimiento de G por complejos mínimos de G en el sentido de Steinberger [Ste73]. Esto lleva a una noción más débil de índice.

Definición 3.2.2. *Si G es la unión de una familia finita F de clases laterales izquierdas (derechas) irredundantes de H entonces el índice del recubrimiento izquierdo (derecho) de H en G se define como*

$$[G : H]_l^* = \min\{|F| : F \text{ un recubrimiento finito irredundante de } G \text{ por clases laterales izquierdas de } H\}.$$

Si G no tiene un recubrimiento por una familia finita F de clases laterales izquierdas irredundantes de H, entonces decimos que $[G : H]_l^*$ es infinito. De manera similar, definimos el *índice de recubrimiento derecho* y lo denotamos por $[G : H]_r^*$.

Capítulo 4

Recubrimientos finitos y n-recubrimientos para lazos.

En el capítulo anterior se estudiaron las descomposiciones de un lazo por medio de clases laterales módulo un sublazo, al final se dio un tipo particular de recubrimiento, tomando esto en cuenta, el presente capítulo se centra en dar una definición más amplia de un recubrimiento y de manera más general un n-recubrimiento así como algunas de sus propiedades. Se presenta el **Teorema de Neumann para lazos** como resultado principal de este trabajo, el cual nos asegura que dado un lazo con un recubrimiento por clases laterales, podemos excluir ciertas clases laterales con ciertas características de dicha unión y las restantes seguir formando un recubrimiento para el lazo, finalmente mostramos algunos ejemplos que nos permiten visualizar el uso de los resultados expuestos.

4.1. n-recubrimientos para lazos.

Definición 4.1.1. *Un lazo G tiene un n-recubrimiento si existen sublazos H_i con $i \in \Omega$ un conjunto de índices, tal que para cada $\{x_1, \ldots, x_n\} \subseteq G$ existe un $i \in \Omega$ con $\{x_1, \ldots, x_n\} \subseteq H_i$. Un 1-recubrimiento de un lazo se llama un recubrimiento si todos los sublazos son propios(son distintos de G). Un n-recubrimiento es finito si Ω es finito.*

Nos interesan los n-recubrimientos por subgrupos, ya que conducen a ciertas condiciones de asociatividad. Esto es el contenido del siguiente teorema.

Teorema 4.1.1. *Sea G un lazo:*

(i) G tiene un 1-recubrimiento por subgrupos si y sólo si es potencia-asociativo;

(ii) G tiene un 2-recubrimiento por subgrupos si y sólo si es disasociativo;

(iii) G tiene un 3-recubrimiento por subgrupos si y sólo si es un grupo.

Demostración.
Para demostrar (i), observamos que si G tiene un 1-recubrimiento por subgrupos entonces G tiene un recubrimiento por sus subgrupos cíclicos, ya que para cada $x \in G$, existe un subgrupo H de G tal que $x \in H$, por ser H cerrado, todas las potencias de x también se quedan en H, con lo cual $\langle x \rangle$ es subgrupo de H, por lo tanto, G es potencia-asociativo. Ahora, si G es potencia-asociativo, tiene un 1-recubrimiento por sus subgrupos cíclicos.

Ahora, si G tiene un 2-recubrimiento por subgrupos entonces, dado $a, b \in G$, existe un subgrupo H de G con $a, b \in H$, se sigue que $\langle a, b \rangle$ es el sublazo más pequeño que contiene a a y b y además es subgrupo de H, por tanto G es disasociativo. Inversamente, si G es disasociativo entonces $\langle a, b \rangle$ es un grupo para todo $a, b \in G$. Por lo tanto, G tiene un 2-recubrimiento. Así se demuestra (ii).

Finalmente para (iii), sea G un lazo con un 3-recubrimiento por subgrupos, entonces, dado $a, b, c \in G$, existe un subgrupo H de G con $a, b, c \in H$. Por lo tanto, $\langle a, b, c \rangle$ es un grupo, por lo que G es asociativo.

Ahora si G es un grupo entonces claramente G tiene un 3-recubrimiento por subgrupos de G. $\square$

Ahora nos enfocamos en los recubrimientos finitos y n-recubrimientos finitos de lazos. Recordemos que un lazo tiene un recubrimiento finito si es la unión de un número finito de sublazos propios, y de manera similar, un lazo tiene un n-recubrimiento finito si el recubrimiento finito es un n-recubrimiento. Primero, mostramos que el análogo del resultado de que un grupo nunca es la unión de dos subgrupos propios se traslada directamente no solo a los lazos sino incluso a los cuasigrupos.

Teorema 4.1.2. *Un cuasigrupo nunca es la unión de dos subcuasigrupos propios.*

Demostración.
Supongamos que $G = A \cup B$, donde $(G, *)$ es un cuasigrupo y A y B son subcuasigrupos propios. Si $X = A - (A \cap B)$ y $Y = B - (A \cap B)$, entonces X y Y son no vacíos. Sea $a \in X$ y $b \in Y$, entonces $ab \in G$. Sin pérdida de generalidad, podemos suponer que $a * b \in A$, es decir, $a * b = a' \in A$. Dado que A es un cuasigrupo, existe un único $x \in A$ tal que $a * x = a'$. Por cancelación, $b = x$, por lo tanto $b \in A$, lo que es una contradicción. $\square$

Definición 4.1.2. *Un elemento a de un lazo G se llama diasociativo si para cualquier $x \in G$ se tiene que $\langle x, a\rangle$ es un grupo.*

Proposición 4.1.1. *Dado un lazo G con un recubrimiento finito por subgrupos H_i, $i = 1, \ldots, n$, de índices izquierdos finitos, de manera que si G tiene una descomposición en clases laterales izquierdas módulo H_i para todo i entonces G es potencia-asociativo con un subgrupo H de índice lateral izquierdo finito en G y todo elemento de H es diasociativo.*

Demostración.
Por (i) del **Teorema 4.1.1**, G es potencia-asociativo. Sea $H = H_1 \cap \cdots \cap H_n$, por el **Corolario 3.2.1** se tiene que H tiene índice izquierdo finito en G. Sea $a \in H$ y $x \in G$, existe un i tal que $x \in H_i$. Por lo tanto $\langle x, a\rangle$ es un grupo, ya que $a \in H_i$. $\square$

Nuestro próximo ejemplo muestra que un lazo que satisface las condiciones de la **Proposición 4.1.1** no es necesariamente un grupo.

Ejemplo 4.1.1. *Sea $L = H \times G$, donde H es un lazo potencia-alternativo no asociativo finito y G es un grupo. Se verifica que $L = \bigcup_{x \in H} H_x$, donde $H_x = \langle x\rangle \times G$, es un recubrimiento finito de L, y L tiene una descomposición en clases laterales izquierdas módulo H_x para cada x. Además, L/H tiene una descomposición en clases laterales izquierdas módulo cualquier subgrupo cíclico, ya que es un lazo potencia-alternativo.*

Proposición 4.1.2. *Dado un lazo G con un 2-recubrimiento finito por subgrupos H_i, $i = 1, \ldots, n$, de índices izquierdos finitos, si G tiene una descomposición en clases laterales izquierdas módulo H_i para todo i entonces G es un lazo diasociativo y el $N(G)$ es un subgrupo de índice finito en G.*

Demostración.
Por (ii) del **Teorema 4.1.1**, G es diasociativo. Sea $H = H_1 \cap \cdots \cap H_n$. El **Corolario 3.2.1** implica que H tiene índice izquierdo finito en G. Sea $a \in H$ y $x, y \in G$, se tiene que existe un i tal que $x, y \in H_i$. Como $a \in H_i$, se deduce que $\langle x, y, a\rangle$ es un grupo. Por lo tanto, $a \in N(G)$, es decir, $H \subseteq N(G)$. Con lo cual $N(G)$ tiene índice izquierdo finito en G y, por lo tanto, $N(G)$ tiene índice finito en G. $\square$

Al igual que en el **Ejemplo 4.1.1**, proporcionamos aquí un ejemplo de un lazo que satisface los supuestos de la **Proposición 4.1.2** y que no es un grupo.

Ejemplo 4.1.2. *Sea $L = H \times G$, donde H es un lazo de Moufang finito no asociativo (los lazos de Moufang son diasositivos, ver Capítulo 4 en [Pfl90]) con todos sus elementos de orden impar y G es un grupo. Se cumple que $L = \bigcup_{\{x,y\} \subseteq H} H_{\{x,y\}}$, donde $H_{\{x,y\}} = \langle x, y\rangle \times G$, es un 2-recubrimiento finito de L, y L tiene una descomposición en clases laterales módulo $H_{\{x,y\}}$ para todo $x, y \in L$.*

En el caso de que tengamos un 2-recubrimiento finito por subgrupos de lazos, garantizamos una imagen homomorfa finita, como el siguiente corolario lo indica.

Corolario 4.1.1. *Dado un lazo $(G,*)$ con un 2-recubrimiento finito por subgrupos abelianos H_i, $i = 1,\ldots,n$, con índices izquierdos finitos, tal que G tiene una descomposición de clases laterales izquierdas módulo H_i para todo i, se tiene que $Z(G)$ tiene índice lateral finito en G como un subgrupo normal de L.*

Demostración.
Sea $H = H_1 \cap \cdots \cap H_n$. Por la **Proposición 4.1.2**, tenemos que $[G : H]_l$ y $[G : N(G)]$ son finitos. Para $x \in G$, existe un i tal que $x \in H_i$. Como $H \subseteq H_i$ y H_i es un subgrupo abeliano, tenemos $a * x = x * a$ para todo $a \in H$ y para todo $x \in G$. Luego $H \subseteq Z(G)$. Se deduce que $Z(G)$ tiene un índice finito en G. □

Tomar en cuenta que si se elige el lazo H como en el **Ejemplo 4.1.2**, pero conmutativo y G como un grupo abeliano, nos proporciona un lazo que no es un grupo y satisface las suposiciones del corolario anterior. Como se puede ver en la siguiente proposición, un núcleo normal de índice finito en un lazo potencia alternativo garantiza la existencia de un recubrimiento finito por subgrupos.

Proposición 4.1.3. *Si $(G,*)$ es un lazo potencia alternativo con $N(G)$ un subgrupo normal de índice finito en G y $G/N(G)$ no cíclico, entonces G tiene un recubrimiento finito por subgrupos H_i de índice finito tales que G tiene una descomposición en clases laterales módulo H_i para todo i.*

Demostración.
Como $N(G)$ es un subgrupo normal de G, el cociente $G/N(G)$ está definido. Sea $N(G) = N$ y sea $H = \langle g, N\rangle$ para algún $g \in G$. Observamos que H es un subgrupo de G y cualquier $h \in H$ se puede escribir como $h = g^j * n$, donde j es un entero y $n \in N$. Vamos a demostrar que G tiene una descomposición en clases laterales módulo H. Por el **Teorema 3.1.1**, basta con demostrar que $(x*h)H = xH$ y $H(h*x) = Hx$ para todos $h \in H$ y para todo $x \in G$. Sean $h, h_1 \in H$ con $h = g^j * n$, $n \in N$, se sigue que

$$(x * h) * h_1 = (x * (g^j * n)) * h_1 = ((x * g^j) * n) * h_1 = (x * g^j) * (n * h_1).$$

Dado que $n * h_1 \in H$, tenemos $n * h_1 = g^i * n'$ para algún $n' \in N$. Por lo tanto,

$$(x * g^j)(n * h_1) = (x * g^j)(g^i * n') = (x * g^{i+j}) * n = x * (g^{i+j} * n) = x * h_2,$$

donde $h_2 \in H$. Se deduce que G tiene una descomposición en clases laterales izquierda módulo H. La prueba para la descomposición en clases laterales derecha es similar.
Sea $X = \{x_1,\ldots,x_n\}$ una transversal izquierda de $N(G)$. Consideremos $H_i = \langle x_i, N(G)\rangle$. Se sigue de lo anterior que H_i es un subgrupo de G y G tiene una descomposición en clases laterales módulo H_i. Obviamente, $G = \bigcup_{i=1}^{n} H_i$, por lo que G tiene un recubrimiento. Como $G/N(G)$ no es cíclico y $[G : H_i] < [G : N(G)]$, cada H_i es un subgrupo propio de G de índice finito. □

Corolario 4.1.2. *Si G es un lazo diasociativo con $N(G)$ un subgrupo normal de índice lateral finito en G, y $L/N(G)$ no es cíclico entonces G tiene un recubrimiento finito por subgrupos H_i de índice finito tal que G tiene una descomposición en clases laterales con respecto a H_i para todo i. Además, si $Z(G)$ tiene índice finito en G entonces G es la unión de un número finito de subgrupos abelianos, cada uno con índice finito en G.*

4.2. Lema de Neumann para Lazos

En esta sección se demuestra un análogo del lema de Neumann, pero ahora para lazos. Para ello, necesitamos fortalecer nuestras condiciones sobre las descomposiciones en clases laterales módulo un sublazo, tal como se presenta en la siguiente definición.

Definición 4.2.1. *Un lazo $(G,*)$ tiene una fuerte descomposición en clases laterales izquierdas (derechas) módulo H, donde H es un sublazo de G, si $y(aH) = (y * a)H$ para todo $y, a \in G$. Si G tiene fuertes descomposiciones en clases laterales izquierdas y derechas módulo H entonces decimos que G tiene una fuerte descomposición en clases laterales módulo H.*

Proposición 4.2.1. *Sea $(G,*)$ un lazo y H, K sublazos de G. Si G tiene una fuerte descomposición en clases laterales módulo H y K entonces tiene una fuerte descomposición en clases laterales módulo $H \cap K$.*

Demostración.
Vamos a probar que G tiene una fuerte descomposición en clases laterales izquierdas, es decir que $x(y(H \cap K)) = (x * y)(H \cap K)$ para todo x, y en G. Para una fuerte descomposición en clases laterales derechas la prueba es análoga.

Sea $z \in x(y(H \cap K))$, se sigue que $z = x(y * a)$ con $a \in H$ y $a \in K$, con esto, $z \in x(yH) = (x * y)H$ y $z \in x(yK) = (x * y)K$ por tanto $z \in (x * y)H \cap (x * y)K = (x * y)(H \cap K)$ por el **Lema 3.1.1**.
Ahora, si $z \in (x*y)(H \cap K)$ entonces $z = (x*y)a$, con $a \in H$ y $a \in K$, con lo cual $z \in (x*y)H = x(yH)$ y $z \in (x*y)K = x(yK)$, así $z = x*(y*h)$ y $z = x*(y*k)$, para algunos $h \in H, k \in K$, por cancelación a la izquierda $h = k$, por lo tanto $z \in x(y(H \cap K))$. □

Corolario 4.2.1. *Sea $(G, *)$ un lazo y H_i, con $i = 1, ..., n$ sublazos de G. Si G tiene una fuerte descomposición en clases laterales módulo H_i para todo $i = 1$ entonces tiene una fuerte descomposición en clases laterales módulo $\bigcap_{i=1}^{n} H_i$.*

Demostración.
Consecuencia directa de la **Proposición 4.2.1**

Lema 4.2.1. *Sea G un lazo y H un sublazo de G. Se tiene que G tiene una fuerte descomposición en clases laterales izquierdas módulo H si y sólo si tiene una descomposición en clases laterales izquierdas módulo H y dado que $\{a_iH\}$ es una descomposición en clases laterales de G módulo H, se verifica que $\{y(a_iH)\}$ también lo es para cualquier $y \in G$.*

Demostración.
Supongamos que $(G, *)$ tiene una fuerte descomposición en clases laterales izquierdas módulo H. Por la **Proposición 3.1.1** y la **Definición 4.2.1**, es claro que G tiene una descomposición en clases laterales izquierdas módulo H. Dado que $y(a_iH) = (y * a_i)H$, observamos que $y(a_iH)$ es una clase lateral de H. Supongamos que $y(a_iH) = y(a_jH)$, se tiene que $y*a_i = y*(a_j*h)$, así que $a_i = a_j*h$ y con esto $a_iH = (a_j * h)H = a_jH$ con lo cual $j = i$. Por lo tanto, si $G = \bigcup_{i \in I} a_iH$ entonces $G = yG = \bigcup_{i \in I}(y * a_i)H$.
Ahora, supongamos que G tiene una descomposición en clases laterales izquierdas módulo H y asumamos que $\{a_iH\}$ es una descomposición en clases laterales izquierdas de G módulo H, implicando que $\{y(a_iH)\}$ también lo es para cualquier $y \in G$. Así, para cada $y, a \in G$, $y(aH)$ es una clase lateral izquierda de H, también lo es $(y * a)H$, pero $y * a \in y(aH) \cap (y * a)H$. Por lo tanto, dado que G tiene un módulo de descomposición lateral izquierda H, $y(aH) = (y * a)H$ y con esto G tiene un fuerte descomposición en clases laterales izquierdas módulo H. □

Como se observa en la demostración del **Lema 4.2.1**, $\{y(a_iH)\}$ es una partición de G si $\{a_iH\}$ es una descomposición en clases laterales izquierdas de G módulo H. Sin embargo, $\{y(a_iH)\}$ no es necesariamente una descomposición en clases laterales.

Lema 4.2.2. *Sean $(G, *)$ un lazo y K, H sublazos de G con $K \leq H$, con G teniendo descomposiciones en clases laterales izquierdas módulo K y H. Si $[G : K]_l$ es finito entonces H tiene una descomposición en clases laterales izquierdas módulo K y $[H : K]_l$ es finito.*

Demostración.
Por hipótesis tenemos que $G = \coprod_{i=1}^{n} a_iK$, donde $\coprod$ denota una unión disjunta. Intersectando con H y distribuyendo obtenemos que

$$H = G \cap H = \left(\coprod_{i=1}^{n} a_iK \right) \cap H = \coprod_{i=1}^{n} (a_iK \cap H).$$

Vamos a demostrar que $a_iK \cap H$ no es vacío si y sólo si $a_i \in H$. Supongamos que $a_i \in H$, se sigue que $a_iK \subseteq H$ y $a_iK \cap H = a_iK$. Inversamente, si $a_iK \cap H$ no es vacío entonces existe $h \in a_iK \cap H$, con lo cual $h \in H$ y $h \in a_iK$, por tanto, existe $k \in K$ tal que $h = a_i * k$. Dado que H es un sublazo de G, existe un único $x \in H$ tal que $x * k = h$. Por cancelación obtenemos $x = a_i$, por lo que $a_i \in H$. Consideremos ahora la transversal $\{a_1, \ldots, a_m, a_{m+1}, \ldots, a_n\}$ tal que $a_iK \cap H$ no es vacío para $i \leq m$ y vacío para $i > m$. Por el **Lema 3.2.1** y lo anterior se sigue que

$$H = \coprod_{i=1}^{m} (a_iK \cap H) = \coprod_{i=1}^{m} a_iK,$$

con $a_i \in H$. Con esto, concluimos que H tiene una descomposición en clases laterales izquierdas módulo K y que $[H : K]_l$ es finito. $\square$

Antes de iniciar nuestra teorema principal, notemos que el **Lema 3.2.1** y **4.2.2** se aplican para una fuerte descomposición en clases laterales.

Teorema 4.2.1. ***(Lema de Neumann para lazos)****. Sea $(G, *)$ un lazo con $G = \bigcup_{i=1}^{n} g_i H_i$, donde $H_1, \ldots, H_n$ son (no necesariamente distintos) sublazos de G tales que G tiene una fuerte descomposición en clases laterales izquierdas módulo H_i para $i = 1, ..., n$. Se tiene que, si uno de los sublazos en esta unión tiene un índice infinito, es decir, el correspondiente $[G : H_i]_l$ es infinito, este sublazo puede omitirse de la unión y los sublazos restantes aún forman un recubrimiento para el lazo.*

Demostración.
Primero mostramos que al menos uno de los sublazos H_i tiene índice izquierdo finito en G. Sea $G = \bigcup_{i=1}^{n} g_i H_i$ y supongamos que r de los $H_1, \ldots, H_n$ son distintos. Procedamos por inducción en r.
Si $r = 1$ entonces G es una unión de un número finito de clases laterales del sublazo H_1 y $[G : H_1]_l$ es finito. Ahora, sea $r > 1$ y supongamos que $r - 1$ sublazos son distintos, se tiene que al menos uno tiene índice finito en G.
Supongamos que los H_i están etiquetados de tal manera que $H_{m+1} = \cdots = H_n$, con $m < n$ y H_n es distinto de cada uno de $H_1, \ldots, H_m$, y donde exactamente $r - 1$ de los primeros m sublazos son distintos, por lo que $r - 1 \leq m$. Luego, tenemos

$$G = \left(\bigcup_{i=1}^{m} g_i H_i \right) \cup \left(\bigcup_{i=m+1}^{n} g_i H_n \right).$$

Si $G = \bigcup_{i=m+1}^{n} g_i H_n$ entonces $[G : H_n]_l$ es finito y los sublazos $H_1, \ldots, H_m$ pueden ser omitidos. De lo contrario, existe un $x \in G$ tal que

$$x \in \bigcup_{i=1}^{m} g_i H_i, \quad \text{pero} \quad x \notin \bigcup_{i=m+1}^{n} g_i H_n.$$

Demostraremos que

$$xH_n \subseteq \bigcup_{i=1}^{m} g_i H_i. \tag{4.1}$$

Por contradicción, supongamos que existe un $h \in H_n$ tal que $x*h \notin \bigcup_{i=1}^{m} g_i H_i$. Así, $x*h \in \bigcup_{i=m+1}^{n} g_i H_n$, y usando la **Proposición 3.1.1**, obtenemos $xH_n = g_j H_n$ para algún j con $m + 1 \leq j \leq n$. Concluimos que $x \in \bigcup_{i=m+1}^{n} g_i H_i$, lo cual es una contradicción.

Sea u_j la solución única de $u_j * x = g_j$, de modo que $u_j(xH_n) = (u_j * x)H_n = g_j H_n$. La multiplicación por la izquierda de (4,1) por u_j lleva a

$$g_j H_n \subseteq u_j \left(\bigcup_{i=1}^{m} g_i H_i \right) = \bigcup_{i=1}^{m} (u_j * g_i) H_i = \bigcup_{i=1}^{m} c_{ij} H_i,$$

donde $c_{ij} = u_j * g_i$. Concluimos que

$$\bigcup_{j=m+1}^{n} g_j H_n \subseteq \bigcup_{j=m+1}^{n} \bigcup_{i=1}^{m} c_{ij} H_i.$$

Por lo tanto,

$$G = \left(\bigcup_{i=1}^{m} g_i H_i \right) \cup \left(\bigcup_{j=m+1}^{n} \bigcup_{i=1}^{m} c_{ij} H_i \right).$$

Así que G es una unión de un número finito de clases laterales de $H_1, \ldots, H_m$ de las cuales sólo $r - 1$ son distintas según nuestra suposición, y por inducción en r, al menos uno de los H_i tiene índice izquierdo

finito en G.

Consideremos $G = \bigcup_{i=1}^{n} g_i H_i$ y supongamos que $H_1, \ldots, H_m$ tienen índice izquierdo infinito en G, y que $H_{m+1}, \ldots, H_n$ tienen índice izquierdo finito en G. Según lo anterior, sabemos que $m < n$ y obtenemos

$$G = \left(\bigcup_{i=1}^{m} g_i H_i \right) \cup \left(\bigcup_{j=m+1}^{n} g_j H_j \right).$$

Sea $I = H_{m+1} \cap \cdots \cap H_n$. Dado que $[G : H_j]_l < \infty$ para $m+1 \leq j \leq n$, se deduce por la **Corolario 3.2.1** que $[G : I]_l$ es finito. Como $I \subseteq H_j$ para $m+1 \leq j \leq n$, el **Lema 4.2.2** implica que $[H_j : I]_l = n_j < \infty$ y que H_j tiene una fuerte descomposición en clases laterales izquierdas módulo I. Sea $\{a_{jk}\}, a_{jk} \in H_j, 1 \leq k \leq n_j$ un conjunto de representantes de las clases laterales de H_j módulo I. Definiendo $b_{jk} = g_j a_{jk}$, vemos que

$$g_j H_j = \bigcup_{k=1}^{n_j} g_j(a_{jk} I) = \bigcup_{k=1}^{n_j} (g_j * a_{jk}) I = \bigcup_{k=1}^{n_j} b_{jk} I.$$

Concluimos que

$$G = \left(\bigcup_{i=1}^{m} g_i H_i \right) \cup \left(\bigcup_{j=m+1}^{n} \bigcup_{k=1}^{n_j} b_{jk} I \right). \tag{4.2}$$

Ahora, si $G = \bigcup_{j=m+1}^{n} \bigcup_{k=1}^{n_j} b_{jk} I$, entonces $G = \bigcup_{j=m+1}^{n} g_j H_j$, y todos los sublazos de índice izquierdo infinito han sido omitidos. De lo contrario, existe $x \in G$ tal que

$$x \in \bigcup_{i=1}^{m} g_i H_i \quad \text{y} \quad x \notin \bigcup_{j=m+1}^{n} \bigcup_{k=1}^{n_j} b_{jk} I.$$

De igual forma que antes, demostraremos que

$$xI \subseteq \bigcup_{i=1}^{m} g_i H_i. \tag{4.3}$$

Nuevamente, por contradicción, supongamos que existe $h \in I$ con $xh \notin \bigcup_{i=1}^{m} g_i H_i$. Por lo tanto,

$$xh \in \bigcup_{j=m+1}^{n} g_j H_j.$$

De ahí, $xh \in g_{j'} H_{j'}$ para algún j', con $m+1 \leq j' \leq n$. Como $I \subseteq H_{j'}$, se sigue que

$$xH_{j'} = g_{j'} H_{j'} \quad \text{y} \quad x \in \bigcup_{j=m+1}^{n} g_j H_j,$$

lo cual es una contradicción. Esto prueba $(4{,}3)$.
Sea w_{jk} la única solución de $w_{jk} x = b_{jk}$, y sea $d_{ijk} = w_{jk} g_i$. La multiplicación por la izquierda de $(4{,}1)$ por w_{jk} junto con el **Colorario 4.2.1** lleva a

$$w_{jk}(xI) = (w_{jk} x) I = b_{jk} I \subseteq \bigcup_{i=1}^{m} w_{jk}(g_i H_i) = \bigcup_{i=1}^{m} d_{ijk} H_i.$$

Por lo tanto,

$$\bigcup_{j=m+1}^{n} \bigcup_{k=1}^{n_j} b_{jk} I \subseteq \bigcup_{j=m+1}^{n} \bigcup_{k=1}^{n_j} \bigcup_{i=1}^{m} d_{ijk} H_i.$$

Esto, junto con (4,2), da

$$G = \left(\bigcup_{i=1}^{m} g_i H_i \right) \cup \left(\bigcup_{j=m+1}^{n} \bigcup_{k=1}^{n_j} \bigcup_{i=1}^{m} d_{ijk} H_i \right).$$

Pero esto implicaría que al menos uno de los $H_1, \ldots, H_m$ tiene índice izquierdo finito en G, lo que contradice nuestra suposición de que $H_1, \ldots, H_m$ tienen índice izquierdo infinito en G. Así, $G = \bigcup_{j=m+1}^{n} g_j H_j$, como se quería demostrar. □

Ahora el **Teorema 4.2.1** junto con las **Proposiciones 4.1.1, 4.1.2** y el **Corolario 4.1.1**, respectivamente, conducen a los siguientes tres corolarios:

Corolario 4.2.2. *Dado un lazo G con un recubrimiento finito por subgrupos H_i, $i = 1, \ldots, n$, tal que G tiene una fuerte descomposición por clases laterales izquierdas módulo H_i para todo i, se tiene que G es un lazo potencia asociativo con un subgrupo H de índice izquierdo finito en G y cada elemento de H es diasociativo.*

Corolario 4.2.3. *Dado un lazo G con una 2-recubrimiento finito por subgrupos H_i, $i = 1, \ldots, n$, tal que G tiene una fuerte descomposición por clases laterales izquierdas módulo H_i para todo i, se cumple que G es un lazo disasociativo y Nuc(G) es un subgrupo de índice finito en G.*

Corolario 4.2.4. *Dado un lazo G con una 2-recubrimiento finito por subgrupos abelianos H_i, $i = 1, \ldots, n$, si G tiene una fuerte descomposición por clases laterales izquierdas módulo H_i para todo i entonces $Z(G)$ es de índice finito en G.*

A continuación presentamos 2 ejemplos en los cuales se muestra que existen lazos que satisfacen las suposiciones del **Teorema 4.2.1**, los **Corolarios 4.2.2** y **4.2.3**, pero que no son necesariamente grupos. Un lazo en el cual todos su sublazos son normales se denomina **Lazo Hamiltoniano**. Dado un lazo G, este tiene una fuerte descomposición en clases laterales izquierdas módulo cada subgrupo normal (ver **Definición 3.1.6**), los lazos Hamiltonianos tienen una fuerte descomposición por clases laterales izquierdas. Norton en [Nor52] muestra la existencia de lazos finitos potencia asociativos así como lazos Hamiltonianos diasociativos que no son grupos.

Ejemplo 4.2.1. *Sea $L = H \times G$, donde H es un lazo finito, no asociativo, potencia asociativo, Hamiltoniano y G es un grupo, entonces $L = \bigcup_{x \in H} H_x$, donde $H_x = \langle x \rangle \times G$, es un recubrimiento finito de L, y L tiene una fuerte descomposición por clases laterales izquierdas módulo H_x para todo x.*

Ejemplo 4.2.2. *Sea $G = H \times G$, donde H es un lazo finito, no asociativo, diasociativo, Hamiltoniano y G es un grupo, entonces $L = \bigcup_{\{x,y\} \subseteq H} H_{\{x,y\}}$, donde $H_{\{x,y\}} = \langle x, y \rangle \times G$, es un 2-recubrimiento finito de L, y L tiene una fuerte descomposición por clases laterales izquierdas módulo $H_{\{x,y\}}$ para todo $\{x, y\}$.*

Norton en [Nor52] demuestra que todo lazo Hamiltoniano, diasociativo y conmutativo es un grupo abeliano. Por lo tanto, una construcción similar a las de los **Ejemplos 4.2.1** y **4.2.2** no conduce a un lazo no-asociativo que satisfaga las suposiciones del **Corolario 4.2.4**.

4.3. Ejemplos.

Ejemplo 4.3.1. *Consideremos el conjunto generado por los elementos de la base de los octoniones $\mathbb{O} = \langle \{1, e_i\} \rangle$, con $i = 1, ..., 7$, este forma un lazo de Moufang no asociativo (ver [Bae01]), como se menciona en el **Ejemplo 4.1.2**, este es diasociativo y por tanto potencia asociativo.*
La tabla de Cayley viene dada de la siguiente manera.

$*$	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_4	$-e_3$	e_5	$-e_2$	$-e_7$	e_6
e_2	e_2	$-e_4$	-1	e_1	e_6	e_7	$-e_5$	$-e_3$
e_3	e_3	e_3	$-e_1$	-1	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	-1	e_1	e_2	e_3
e_5	e_5	e_2	$-e_7$	e_6	$-e_1$	-1	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	-1	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	-1

Se verifica que para cada e_i su generado es $\langle e_i\rangle = \{1, e_i, -1, -e_i\}$, para $i = 1, ..., 7$. Con esto es claro que

$$\mathbb{O} = \bigcup_{i=1}^{7} \langle e_i\rangle$$

*como lo asegura el **Teorema 4.1.1**.*

Ese mismo teorema nos asegura que existe un 2-recubrimiento finito por sublazos generados por dos elementos, es decir si consideramos $A = \{\langle e_i, e_j\rangle | i = 1, ..., 7, j = 1, ..., 7, i \neq j\}$

$$\mathbb{O} = \bigcup_{B\in A} B$$

Notar que, aunque los sublazos generados por uno o dos elementos si forman un recubrimiento finito y 2-recubrimiento finito respectivamente, en ninguno de los casos estos no forman una partición de $\mathbb{O}$.

Ejemplo 4.3.2. *De manera similar al ejemplo anterior, consideremos el conjunto de los sedeniones $\mathbb{S}$ (ver [KM00]) y tomemos su base $E_{16} = \{e_i | i = 0, 1, ..., 15\}$. Sea $\mathbb{S}_L = \{\pm e_i | i = 0, 1, ..., 15\}$ el **Lazo Sedenión** (ver [RS05]), donde $e_0 = 1$, es el elemento identidad, $\mathbb{S}_L$ resulta ser un lazo potencia asociativo, con lo cual, podríamos hacer una construcción de un recubrimiento finito usando el **Teorema 4.1.1**, pero en esta ocasión, usaremos otros sublazos para construir dicho recubrimiento. Consideremos la tabla con los siguientes sublazos dada en [RS05])*

A_1	$\{e_0, e_1, e_2, e_3, e_4, e_5, e_6, e_7, -e_0, -e_1, -e_2, -e_3, -e_4, -e_5, -e_6, -e_7\}$
A_2	$\{e_0, e_1, e_2, e_3, e_8, e_9, e_{10}, e_{11}, -e_0, -e_1, -e_2, -e_3, -e_8, -e_9, -e_{10}, -e_{11}\}$
A_3	$\{e_0, e_1, e_4, e_5, e_8, e_9, e_{12}, e_{13}, -e_0, -e_1, -e_4, -e_5, -e_8, -e_9, -e_{12}, -e_{13}\}$
A_4	$\{e_0, e_1, e_6, e_7, e_8, e_9, e_{14}, e_{15}, -e_0, -e_1, -e_6, -e_7, -e_8, -e_9, -e_{14}, -e_{15}\}$
A_5	$\{e_0, e_2, e_4, e_6, e_8, e_{10}, e_{12}, e_{14}, -e_0, -e_2, -e_4, -e_6, -e_8, -e_{10}, -e_{12}, -e_{14}\}$
A_6	$\{e_0, e_2, e_5, e_7, e_8, e_{10}, e_{13}, e_{15}, -e_0, -e_2, -e_5, -e_7, -e_8, -e_{10}, -e_{13}, -e_{15}\}$
A_7	$\{e_0, e_3, e_4, e_7, e_8, e_{11}, e_{12}, e_{15}, -e_0, -e_3, -e_4, -e_7, -e_8, -e_{11}, -e_{12}, -e_{15}\}$
A_8	$\{e_0, e_3, e_5, e_6, e_8, e_{11}, e_{13}, e_{14}, -e_0, -e_3, -e_5, -e_6, -e_8, -e_{11}, -e_{13}, -e_{14}\}$

Notar que cada sublazo A_i con $i = 1, ..., 8$ es isomorfo a $\mathbb{O}$ (lazo de los octoniones), con sus elementos en términos de los generadores e_i del lazo de los sedeniones. Es claro con esto que,

$$\mathbb{S}_L = \bigcup_{i=1}^{8} A_i.$$

Para los siguientes ejemplos, consideremos el siguiente teorema mostrado en [Che74] y [Bri22].

Teorema 4.3.1. *Si $(L, *)$ es un lazo de Moufang no asociativo para el cual todo conjunto mínimo de generadores contiene un elemento de orden 2 entonces existe un grupo no abeliano G, y un elemento x de orden 2 en L, tal que cada elemento de L puede expresarse de manera única en la forma $g \cdot x^\alpha$, donde $g \in G$, $\alpha = 0, 1$, y el producto de dos elementos de L está dado por*

$$(g_1 \cdot x^\delta) * (g_2 \cdot x^\epsilon) = (g_1^\nu g_2^\mu) \cdot x^{\delta+\epsilon}$$

donde $\nu = (-1)^\epsilon$ y $\mu = (-1)^{\epsilon+\delta}$.

Recíprocamente, dado cualquier grupo no abeliano G, el lazo L construido como se indicó anteriormente es un lazo de Moufang no asociativo.

Observación 4.3.1. *Notamos que si $\alpha = 1$, entonces el orden de cada elemento $g \cdot x$ es 2, ya que $(g \cdot x) * (g \cdot x) = (g^{-1}g)x^2 = e$.*

Ejemplo 4.3.3. *Consideremos con grupo simétrico de orden 3, $S_3 = \{\sigma_i\}$ con $i = 0, 1, ..., 5$, donde σ_0 es el elemento identidad.*

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

La operación es la composición de funciones y la tabla de Cayley viene dada de la siguiente manera:

$\cdot$	e	σ_1	σ_2	σ_3	σ_4	σ_5
e	e	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	e	σ_4	σ_5	σ_3	σ_2
σ_2	σ_2	σ_5	e	σ_4	σ_1	σ_3
σ_3	σ_3	σ_4	σ_5	e	σ_2	σ_1
σ_4	σ_4	σ_3	σ_1	σ_2	σ_5	e
σ_5	σ_5	σ_2	σ_3	σ_1	e	σ_4

Notamos que S_3 no es abeliano y tampoco cíclico ya que la cantidad mínima de generadores es 2. Un conjunto generador mínimo es $\{\sigma_1, \sigma_4\}$, además σ_i y σ_j tienen orden 2 y 3 respectivamente, para $i = 1, 2, 3$ y $j = 4, 5$.
*Verificamos que cumple los requisitos del **Teorema 4.3.1**, para construir el lazo L de dicho teorema, consideremos $x \in L$ tal que este tiene orden 2. Así los elementos de L son de la forma $g \cdot x^\alpha$, con $g \in G$ y $\alpha = 0, 1$.*

$$L = \{\sigma_0 \cdot x^0, \sigma_1 \cdot x^0, \sigma_2 \cdot x^0, \sigma_3 \cdot x^0, \sigma_4 \cdot x^0, \sigma_5 \cdot x^0, \sigma_0 \cdot x, \sigma_1 \cdot x, \sigma_2 \cdot x, \sigma_3 \cdot x, \sigma_4 \cdot x, \sigma_5 \cdot x\},$$

donde $\sigma_i \cdot x^0 = \sigma_i$ para todo $i = 0, 1, ..., 5$. Los elementos se operan de la siguiente manera

$$(g_1 \cdot x^\delta) * (g_2 \cdot x^\epsilon) = (g_1^\nu g_2^\mu) \cdot x^{\delta+\epsilon}.$$

*Por la **Observación 4.3.1**, se tiene que el orden de $\sigma_i \cdot x$ es 2, para todo $i = 0, 1, ..., 5$. Así los elementos de orden 2 en L son $\{\sigma_1, \sigma_2, \sigma_3, \sigma_i \cdot x\}$, con $i = 0, 1, ..., 5$ y los de orden 3 son $\{\sigma_4, \sigma_5\}$ Ahora, L construido de esta forma es un lazo de Moufang y por el **Teorema 4.1.1** aseguramos que existen 1-recubrimientos y 2-recubrimientos por subgrupos.*
Consideremos algunos sublazos de L generados por dos elementos(grupos)

- $\langle \sigma_4, \sigma_3 \cdot x \rangle = \{\sigma_0, \sigma_4, \sigma_5, \sigma_1 \cdot x, \sigma_2 \cdot x, \sigma_3 \cdot x\} \cong S_3$
- $\langle \sigma_4, \sigma_4 \cdot x \rangle = \{\sigma_0, \sigma_4, \sigma_5, x, \sigma_4 \cdot x, \sigma_5 \cdot x\} \cong S_3$
- $\langle \sigma_1, \sigma_2 \rangle = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\} = S_3$
- $\langle e, \sigma_1 \cdot x \rangle = \{\sigma_0, \sigma_1 \cdot x\}$

Por lo tanto, si $X = \{\langle \sigma_4, \sigma_3 \cdot x \rangle, \langle \sigma_4, \sigma_4 \cdot x \rangle, \langle \sigma_1, \sigma_2 \rangle\}$ entonces $L = \bigcup_{A \in X} A \longrightarrow \{S_3, S_3, S_3\}$.

Ejemplo 4.3.4. *Consideremos el conjunto de las traslaciones y reflexiones de un triángulo, el grupo diédrico $D_3 = \{e, r, r^2, s, sr, sr^2\}$, su tabla de Cayley esta dada de la siguiente manera*

$*$	e	r	r^2	s	sr	sr^2
e	e	r	r^2	s	sr	sr^2
r	r	r^2	e	sr	sr^2	s
r^2	r^2	e	r	sr^2	s	sr
s	s	sr	sr^2	e	r	r^2
sr	sr	sr^2	s	r	r^2	e
sr^2	sr^2	s	sr	r^2	e	r

D_3 es no abeliano y no es cíclico ya que la cantidad mínima de generadores es 2. Un conjunto generador mínimo es $\{r, s\}$, además s, r tienen orden 2 y 3 respectivamente.
*Verificamos que cumple los requisitos del **Teorema 4.3.1**, para construir el lazo L, consideremos $x \in L$ tal que este tiene orden 2. Así los elementos en L son de la forma $g \cdot x^{\alpha}$, con $g \in G$ y $\alpha = 0, 1$. Con esto, consideremos que $g \cdot x^0 = g$ y $e \cdot x = x$, para todo $g \in G$ y por tanto*

$$L = \{e, r, r^2, s, sr, sr^2, x, r \cdot x, r^2 \cdot x, s \cdot x, sr \cdot x, sr^2 \cdot x\}.$$

Al igual que en el ejemplo anterior, los elementos se operan de la siguiente manera

$$(g_1 \cdot x^{\delta}) * (g_2 \cdot x^{\epsilon}) = (g_1^{\nu} g_2^{\mu}) \cdot x^{\delta + \epsilon}.$$

*Nuevamente por la **Observación 4.3.1**, se tiene que el orden de $g \cdot x$ es 2, para todo $i = 0, 1, ..., 5$ y $g \in D_3$. Así, los elementos r, r^2 en L tienen orden 3, sr, sr^2 tienen orden 6 y el resto de elementos tienen orden 2. Ahora, L construido de esta manera es un lazo de Moufang y por el **Teorema 4.1.1** aseguramos que existen 1-recubrimientos y 2-recubrimientos por sublazos, que además son asociativos.*

Consideremos algunos sublazos de L generados por dos elementos(grupos).

- $\langle r, x \rangle = \{e, r, r^2, x, r \cdot x, r^2 \cdot x\}$
- $\langle s, x \rangle = \{e, s, sr, sr^2, x, s \cdot x, sr \cdot x, sr^2 \cdot x\}$
- $\langle r, r \cdot x \rangle = \{e, r, r^2, r \cdot x, r^2 \cdot x, x\}$

Nuevamente vemos que

$$L = \langle r, x \rangle \cup \langle s, x \rangle.$$

En general, dado cualquier grupo no abeliano con las condiciones del **Teorema 4.3.1**, podemos construir un lazo de Moufang, con lo cual garantizamos que existen tanto 1-recubrimientos como 2-recubrimientos finitos por sublazos que en este caso también son grupos.

Bibliografía

[Bae01] John C. Baez. "The Octonions". En: *Bull. Amer. Math. Soc. 30* (2001), págs. 145-205.

[Bri22] Riley Britten. *Power graphs of Moufang loops*. 2022. URL: https://arxiv.org/pdf/2204.07165v3.

[Che74] Orin Chein. "Moufang Loops of small order. I". En: *Transactions of the American Mathematical Society* 188.2 (1974). URL: https://www.ams.org/journals/tran/1974-188-00/S0002-9947-1974-0330336-3/S0002-9947-1974-0330336-3.pdf.

[Con07] Keith Conrad. *DIHEDRAL GROUPS*. 2007. URL: https://api.semanticscholar.org/CorpusID:19763796.

[HAL97] H. Bell, A. Klein y L.C. Kappe. "An analogue for rings of a group problem of P. Erdös and B.H. Neumann". En: *Acta Math. Hungar. 77* (1997), págs. 57-67.

[KM00] K. Imaeda y M. Imaeda. "Sedenions: algebra and analysis". En: *Appl. Math. Comput. 115 (200)* 115.2-3 (2000), págs. 77-88. ISSN: 0096-3003.

[LJJ01] L.C. Kappe,An, J.C. Lennox y J. Wiegold. "An analogue for semigroups of a group problem of P. Erdös and B.H. Neumann". En: *Bull. Austral. Math. Soc. 63* (2001), págs. 59-66.

[MAA70] M. Bruckheimer, A. C. Bryan y A. Muir. "Groups Which are the Union of Three Subgroups". En: *The American Mathematical Monthly* (1970).

[MKP11] Michael Kinyon, Kyle Pula y Petr Vojtěchovský. *Incidence Properties of Cosets in Loops*. Accessed: 16-Dec-2011. 2011. arXiv: 1108.3656v3 [math.CO].

[MP03] Moreno Frías, María Ángeles y Pardo Espino, Enrique. *Teoría de Grupos*. Servicio de Publicaciones de la Universidad de Cádiz, 2003. ISBN: 84-7786-807-7. URL: http://hdl.handle.net/10498/26928.

[Neu54a] B.H. Neumann. "Groups covered by finitely many cosets". En: *Publ. Math. Debrecen 3* (1954), págs. 227-242.

[Neu54b] B.H. Neumann. "Groups covered by permutable subsets". En: *J. London Math. Soc. 29* (1954), págs. 236-248.

[Nor52] D.A. Norton. "Hamiltonian Loops". En: *Proc. Amer. Math. Soc. 3* (1952), págs. 56-65.

[Pfl90] Hala O. Pflugfelder. *Cuasigroups and Loops: Introduction*. Heldermann Verlag Berlin, 1990.

[Rag12] K. N. Raghavan. *Group Actions on Sets*. 2012. URL: https://www.imsc.res.in/~knr/past/14alg/1207mysore_public.pdf.

[RS05] Raoul E. Cawagas y Sheree Ann G. Gutierrez. "The Subloop Structure of the Cayley-Dickson Sedenion Loop". En: *MATIMYAS MATEMATIKA, Journal of the Mathematical Society of the Philippines* 28.1-3 (2005), págs. 10-20. ISSN: 0115-6926.

[Rob65] D.A. Robinson. *Bol Loops*. 1965. URL: https://www.ams.org/journals/tran/1966-123-02/S0002-9947-1966-0194545-4/S0002-9947-1966-0194545-4.pdf.

[Ste73] M. Steinberger. "On multiplicative properties of families of complexes of certain loops". En: *Canad. J. Math. 25* (1973), págs. 1066-1077.

[TL05] Tuval Foguel y Luise-Charlotte Kappe. "On loops covered by subloops". En: *Expositiones Mathematicae* (2005).