Caracterización de grupos cuyos subgrupos tienen distinto cardinal

Andrés Yamith Villamizar Tarazona

Universidad Industrial de Santader
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
2018

Caracterización de grupos cuyos subgrupos tienen distinto cardinal

Andrés Yamith Villamizar Tarazona

Propuesta de trabajo de grado para optar al título de Matemático

Director

Héctor Edonis Pinedo Tapia
Doctor en Ciencias

Universidad Industrial de Santader
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
2018

AGRADECIMIENTOS

Quiero expresar mis más sinceros agradecimientos a esa persona que me apoyo en casi todas mis decisiones, esa persona que me vio avanzar a paso lento por este arduo camino y estuvo siempre ahí dándome animo, aquella que brindó sus mejores consejos sin esperar nada a cambio. Sin su ayuda no habría alcanzado este pequeño logro. A mi madre, Olga Tarazona le debo mucho más que este escrito. Te amo. Para tí está dedicada cada palabra de este trabajo.

También quiero agradecer al profesor Héctor Pinedo por toda la ayuda brindada, por compartir sus conocimientos dentro y fuera del aula, por motivarme a ser un mejor profesional y depositar su confianza en mi. El sentimiento de respeto y gratitud que experimento no se puede cuantificar en unas pocas líneas. Gracias por aceptar ser mi orientador. De igual manera quiero expresar mi gratitud a cada uno de los profesores que ayudaron en mi formación personal y profesional pues sin ellos me hubiese sido imposible haber culminado esta meta.

Finalmente quiero dar gracias a cada persona que de una u otra forma aportó para mi crecimiento personal y profesional durante mis años en la universidad, especialmente a mis amigos y mi tía Yoly Tarazona. De ustedes aprendí invaluables lecciones.

Índice general

RESUMEN

TÍTULO: CARACTERIZACIÓN DE GRUPOS CUYOS SUBGRUPOS TIENEN DISTINTO CARDINAL.[1]

AUTOR: ANDRÉS YAMITH VILLAMIZAR TARAZONA [2]

PALABRAS CLAVE: PROPIEDAD (D); GRUPO DE PRÜFER; GRUPO CÍCLICO FINITO; GRUPOS ABELIANOS.

DESCRIPCIÓN:

Dado un grupo cíclico finito G y un entero positivo d que divide al orden de G, entonces G tiene un único subgrupo de orden d ([13] p.1). Esta propiedad se generaliza para un grupo arbitrario diciendo que él tiene la ***Propiedad (D)*** *si distintos subgrupos de G tienen distinto cardinal.*

Este trabajo se enfoca en realizar un estudio detallado de la propiedad descrita anteriormente. Se quieren dar condiciones necesarias y suficientes para grupos G con este atributo. En el primer capítulo se retoman ciertos resultados básicos de teoría de conjuntos, teoría de números y teoría de grupos que son fundamentales para dar contexto al problema, y más que esto obtener herramientas útiles para llegar a una conclusión interesante.

En el segundo capítulo se aborda un poco la teoría de grupos abelianos con el ***Grupo de Prüfer*** *y sus principales características, que serán una pieza clave para el desarrollo de este trabajo. También se estudia la teoría de grupos finitos dando algunos resultados necesarios para introducir formalmente la Propiedad (D); luego de esto se demuestran los teoremas principales, que naturalmente están ligados a nuestra propiedad y finalmente damos una caracterización de todos los grupos que verifican la propiedad. En el tercer capítulo se profundiza un poco mas la Propiedad (D), estudiando y analizando ciertas proposiciones de manera unívoca y mostrando determinados contraejemplos.*

[1] Trabajo de grado

[2] Facultad de Ciencias. Escuela de Matemáticas. Director: Dr. Héctor Edonis Pinedo Tapia

ABSTRACT

TITLE: CHARACTERIZATION OF GROUPS WHOSE SUBGROUPS HAVE DIFFERENT CARDINAL.[3]

AUTHOR: ANDRES YAMITH VILLAMIZAR TARAZONA. [4]

KEYWORDS: PROPERTY (D); PRÜFER GROUP; FINITE CYCLIC GROUP; ABELIAN GROUPS.

DESCRIPTION:

Given a cyclic group G and a positive integer d, that divides the order of G, then G has a single subgroup of order d ([13] p.1). This property is generalized for an arbitrary group that has the ***Property (D)*** *if different subgroups of G have different cardinals.*

This work focuses on a detailed study of the property described above. With this attribute, necessary and sufficient conditions for groups want to be given. In the first chapter, the main sets of number theory and group theory are found, these ones are fundamental to the context of the problem, and more than that, useful tools are needed to arrive at a response.

In the second chapter, the theory of abelian groups is slightly discussed, with the ***Prüfer Group*** *and its main characteristics, which are a key element for the development of this work. The theory of finite groups is also studied, giving some necessary results to go directly to the Property (D); after this, the main theorems are evident, which are naturally linked to our property and, finally, all the groups that verify the property. In the third chapter, the Property (D) is deepened a little bit more, studying and analyzing certain propositions in a unique way and showing some counterexamples.*

[3]Bachelor Thesis

[4]Facultad de Ciencias. Escuela de Matemáticas. Director: Dr. Héctor Edonis Pinedo Tapia

INTRODUCCIÓN

Antes de la primera mitad del siglo XIX el álgebra se limitaba netamente en la solución de ecuaciones polinómicas. Por ese entonces era de gran interés para los matemáticos hallar fórmulas algebraicas que dieran solución a tales ecuaciones. Fue aquí cuando el problema de resolver la ecuación de quinto grado '*impulsó la transformación y evolución futura del álgebra*' [16]. Gracias a Abel y sus trabajos se pudo demostrar que los polinomios de grado igual a cinco no son resolubles por radicales [5], que a su vez sirvieron como base para las investigaciones de Galois quien más tarde generaliza este resultado. Es en este punto donde Évariste Galois habla por primera vez sobre grupos. Básicamente un grupo es un conjunto no vacío dotado de una operación binaria interna que es asociativa, modulativa e invertiva [2, pág. 10] . Lo anterior es una de las tantas versiones que tiene la definición moderna de grupo [3], la cual fue establecida en el año 1887 en manos del matemático alemán Ferdinand G. Frobenius [17]. Antes de esta fecha diferentes matemáticos intentaron dar una definición de grupo: Para Galois un grupo era lo que hoy en día se conoce como grupo de Galois [4], en 1845 Cauchy dio una definición, él consideraba sustituciones en n símbolos y definía sustituciones derivadas como todas aquellas que se obtienen como producto de las dadas y no importa el orden. Al conjunto obtenido lo llamó ***sistema conjugado de sustituciones***. El término grupo y sistema conjugado de sustituciones fueron sinónimos. En 1854 Cayley intentó dar una definición abstracta de grupo, la cual no trascendió posiblemente por el enfoque de las investigaciones matemáticas en aquella época [3]. En 1882 el matemático Heinrich Weber da una definición abstracta de grupo (la que coincide hoy día con la definición de grupo finito) [11]. Paralelamente a él y en el mismo año, el matemático Walther von Dyck da una definición abstracta de grupo en términos de generadores y relaciones.

La importancia de la teoría de grupos va más allá de las aplicaciones, y es que con el solo hecho de poder pensar, organizar y estructurar una idea, es razón suficiente para darle tal importancia. Para nadie es un secreto que la matemática está presente en nuestra vida cotidiana, pasando unas veces desapercibida y otras no tan implícita. En el caso particular de la teoría de grupos vemos una notable disposición en la cristalografía [6] pues son suficientes '*32 grupos para tratar los cristales de la naturaleza*' [2, pág. 54]. En el campo artístico, especificamente en la composición musical es un hecho que los pitagóri-

[5] Un polinomio es resoluble por radicales si sus raíces pueden ser halladas en términos de sus coeficientes mediante operaciones aritméticas, pudiendo incluir la radicación.

[6] Ciencia que estudia las estructuras cristalinas de la naturaleza.

cos han aportado matemáticamente en esta disciplina con la *afinación pitagórica*, pero ¿Son estos los únicos aportes matemáticos hechos a la teoría musical? Si consideramos los doce tonos musicales de la escala cromática $C, C\sharp, D, D\sharp, E, F, F\sharp, G, G\sharp, A, A\sharp, B$ ([1] p.88), podemos representarlos por el conjunto $\mathbb{Z}_{12}$ pues la escala cromática se comporta como clases de equivalencia en el sentido de que todos los múltiplos de una frecuencia son representados por la misma letra. Teniendo esta correspondencia podemos representar por ejemplo, acordes, con los cuales se pueden definir transposiciones e inversiones entre acordes. El conjunto de estas transposiciones e inversiones forman un grupo. Hemos de aclarar que aquí no termina el uso de la teoría de grupos en la música. Al lector interesado en profundizar sobre el tema se le invita a consultar [1]. Por otro lado hay campos del saber más afines a la matemática donde ésta teoría juega un papel más protagónico. Se podría pensar por ejemplo en la teoría de códigos, donde el método de decodificación para códigos formulado por el matemático David Slepian se basa en la utilización de clases laterales [12].

Este trabajo es motivado por la siguiente pregunta:

¿Cuáles grupos G tienen la propiedad de que distintos subgrupos de G tienen distinto cardinal?

En [13] se menciona que todos los grupos cíclicos finitos tienen esta particularidad. ¿Son éstos todos los grupos que satisfacen este atributo?

Capítulo 1

Preliminares

En este capítulo se disponen algunas definiciones y resultados elementales de la teoría de conjuntos, teoría de números y la teoría de grupos que son necesarios para el desarrollo y comprensión de los siguientes capítulos. Algunas proposiciones y teoremas serán demostrados a lo largo del capítulo dependiendo de la importancia y su uso a la hora de resolver nuestro problema. Cabe aclarar en este punto que los resultados no demostrados en ningún momento dejan de ser importantes para este trabajo. Las demostraciones restantes pueden ser consultadas en [5], [7] y [14] dependiendo de la sección que se esté analizando.

1.1. Conceptos básicos de la teoría de conjuntos

Definición 1.1.1. *Dado un conjunto A, diremos que A es un conjunto parcialmente ordenado si existe una relación binaria '$\leq$' sobre A que cumple las siguientes propiedades:*

i) Para cualquier $a \in A$, $a \leq a$ (propiedad reflexiva).

ii) Si $a, b \in A$ tales que $a \leq b$ y $b \leq a$, entonces $a = b$ (propiedad antisimétrica).

iii) Dados $a, b, c \in A$, si $a \leq b$ y $b \leq c$, entonces $a \leq c$ (propiedad transitiva).

Adicionalmente, si un conjunto parcialmente ordenado A satisface la condición de que para cualesquiera $a, b \in A$, $a \leq b$ o $b \leq a$, se dirá entonces que el conjunto esta ordenado totalmente o que el conjunto esta ordenado linealmente.

Ejemplo 1.1.1. [1]
Sea G un grupo y considere el conjunto $\mathcal{L}(G) = \{H \subseteq G : H \leq G\}$. Entonces $\mathcal{L}(G)$ es un conjunto parcialmente ordenado mediante la siguiente relación: Dados $H, K \in \mathcal{L}(G)$ se define $H \leq K \Leftrightarrow H \subseteq K$.

Observación 1.1.1. *Se le llamará **cadena** a todo subconjunto linealmente ordenado de un conjunto parcialmente ordenado.*

Teorema 1.1.1. ***Lema de Zorn***
Un conjunto parcialmente ordenado A con la propiedad de que toda cadena tiene una cota superior en A tiene al menos un elemento maximal.

Definición 1.1.2. *Diremos que dos conjuntos A y B son **equipotentes** si existe una función $f : A \to B$ biyectiva. Se escribirá $A \cong B$ si A es equipotente con B.*

Ejemplo 1.1.2. $\mathbb{N} \cong \mathbb{Z}$. *Para mostrar esto consideremos la función $f : \mathbb{N} \to \mathbb{Z}$ definida por:*

$$x \longmapsto f(x) = \begin{cases} \frac{x}{2} & si \quad x \quad es\ par \\ \\ \frac{1-x}{2} & si \quad x \quad es\ impar \end{cases}$$

Veamos que f es biyectiva. Primero mostremos que la función es sobreyectiva. Sea $y \in \mathbb{Z}$. Si $y = 0$ tome 1 y podremos verificar que $f(1) = \frac{1-1}{2} = 0$. Si $y > 0$ entonces considere $2y \in \mathbb{N}$. Finalmente, si $y < 0$ consideremos el elemento $-2y+1 \in \mathbb{N}$. Con esto hemos probado que la función es sobreyectiva. Veamos ahora que f es inyectiva. Para esto sean x_1, $x_2 \in \mathbb{N}$ tales que $f(x_1) = f(x_2)$ y probemos que $x_1 = x_2$. Supongamos que x_1 y x_2 son números pares, luego $\frac{x_1}{2} = f(x_1) = f(x_2) = \frac{x_2}{2}$. Se concluye que $x_1 = x_2$. Un procedimiento análogo, suponiendo que x_1 y x_2 son números impares, probaría que $x_1 = x_2$. Analicemos el caso en que x_1 es par y x_2 impar. Supongamos que $\frac{x_1}{2} = \frac{1-x_2}{2}$, de lo cual tenemos que $x_1 - 1 = -x_2$. Como x_1 es un número natural, $x_1 \geq 1$, de ello que $x_1 - 1 \geq 0$, es decír $-x_2 \geq 0$ y así $x_2 \leq 0$ lo cual es una contradicción pues $x_2 \in \mathbb{N}$. Se concluye que f es inyectiva. Así f es biyectiva.

Teorema 1.1.2. *Sean A, B, C y D conjuntos. Si $A \cong B$ y $C \cong D$, entonces $A \times C \cong B \times D$.*

[1] Para este ejemplo daremos un pequeño salto y consideraremos las definiciones *1.3.1* y *1.3.3* de la sección *1.3*.

Demostración. Como $A \cong B$ tenemos que existe $f : A \to B$ biyectiva. Análogamente se tiene que existe $g : C \to D$ biyectiva. Considere la función $f \times g : A \times C \to B \times D$ definida por $(f \times g)(a, b) = (f(a), g(b))$. Entonces $f \times g$ es biyectiva. En efecto, primero probaremos que la función es inyectiva. Si $(f \times g)(a, b) = (f \times g)(c, d)$, entonces $(f(a), g(b)) = (f(c), g(d))$; de ello que $f(a) = f(c)$ y $g(b) = g(d)$. Se concluye que $a = c$ y $b = d$. Así $(a, b) = (c, d)$ con lo cual la función es inyectiva. Veamos ahora que $f \times g$ es sobreyectiva. Sea $(a, b) \in B \times D$, de ello que $a \in B$ y $b \in D$. Como f es sobreyectiva, existe $c \in A$ talque $f(c) = a$. Análogamente existe $d \in C$ talque $g(d) = b$. Considere ahora $(c, d) \in A \times B$, luego $(f \times g)(c, d) = (f(c), g(d)) = (a, b)$. Con esto se tiene que la función es sobreyectiva. De lo anterior concluimos que $A \times C \cong B \times D$.

□

Queremos precisar la idea de conjunto finito e infinito. Para esto, dado n un entero positivo se denota $I_n := \{1, 2, \cdots, n\}$.

Definición 1.1.3. *Dado un conjunto A, diremos que A es finito si $A = \emptyset$ ó si existe $f : A \to I_n$ biyectiva, para algún $n \in \mathbb{N}$. En caso contrario se dirá que el conjunto es infinito.*

En el *Ejemplo 1.1.2* vimos que $\mathbb{N}$ es equipotente con $\mathbb{Z}$. Además de este hecho es bien común que utilicemos los números naturales para poder contar ciertos objetos o poder ***numerar*** una cierta cantidad de elementos de nuestra vida diaria. Es tan sutil el uso de estos números que pasa casi desapercibido para muchas personas. De suerte para nosotros que el gran matemático Georg Cantor pudo fijar su atención en este hecho y darle el mejor de los usos. A continuación daremos una definición que nos abrirá las puertas del ***paraíso que Cantor creó para nosotros***.

Definición 1.1.4. *Sea A un conjunto. Diremos que A es **numerable** si existe $f : A \to \mathbb{N}$ inyectiva, o equivalentemente si existe una función $g : \mathbb{N} \to A$ sobreyectiva ([14, pág. 144]).*

Ejemplo 1.1.3. *Citando nuevamente el Ejemplo 1.1.2 tenemos que $\mathbb{Z}$ es un conjunto numerable. Todos los conjuntos finitos son numerables, al igual que $2\mathbb{N}$ y el conjunto de números impares.*

Como observamos anteriormente los números enteros son equipotentes con $\mathbb{N}$. Enseguida mostramos un ingenioso método ideado por Cantor que prueba la numerabilidad de los números racionales. Básicamente lo que se busca es dar una lista ordenada

$0, k_1, k_2, k_3, \cdots$ de todos estos números. Empecemos tomando todos los racionales positivos y construyamos conjuntos A_i, donde $i \in \mathbb{N}$ y $n + m = i$, para todo $\frac{n}{m} \in A_i$. Por ejemplo: $A_2 = \{\frac{1}{1}\}$, $A_7 = \{\frac{1}{6}, \frac{2}{5}, \frac{3}{4}, \frac{4}{3}, \frac{5}{2}, \frac{6}{1}\}$, $A_9 = \{\frac{1}{8}, \frac{2}{7}, \frac{3}{6}, \frac{4}{5}, \frac{5}{4}, \frac{6}{3}, \frac{7}{2}, \frac{8}{1}\}$. Note que en cada A_i los elementos están ordenados de manera ascendente dependiendo del numerador de cada fracción. El siguiente paso será listar los elementos de cada A_i como sigue:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2} \cdots$$

Ahora borremos las fracciones equivalentes, por ejemplo $\frac{2}{2}, \frac{6}{3}$ etcétera. Con esto hemos dado una lista $r_1, r_2, r_3, \cdots$ de todos los números racionales positivos. Un proceso análogo pone en evidencia una lista $a_1, a_2, \cdots$ de números racionales negativos. Luego $0, r_1, a_1, r_2, a_2, r_3, \cdots$ es una enumeración de todos los números racionales. De esta última lista se deduce que $\mathbb{N} \cong \mathbb{Q}$. El lector interesado en los detalles puede consultar [14, pág. 141-142.].
El siguiente par de resultados caracterizan a los conjuntos infinitos.

Teorema 1.1.3. *[14, pág. 147] Un conjunto A es infinito si y solo si A tiene un subconjunto numerable.*

Teorema 1.1.4. *[14, pág. 148] Dado un conjunto A, entonces A es infinito si y solo si A es equipotente con un subconjunto propio de si mismo.*

Sean A y B conjuntos. Diremos que A y B tienen la misma cardinalidad si $A \cong B$ y escribiremos $|A| = |B|$. Lo anterior nos sugiere que pueden existir muchos conjuntos con igual cardinalidad. Enseguida definimos lo que es un número cardinal.

Definición 1.1.5. *Diremos que α es un número cardinal si existe un conjunto A tal que $|A| = \alpha$.*

Sean α, β números cardinales y A, B conjuntos tales que $|A| = \alpha$ y $|B| = \beta$. Se define el producto de cardinales como $\alpha\beta = |A \times B|$. Además, si los conjuntos A y B son disjuntos se define la suma de cardinales como $\alpha + \beta = |A \cup B|$. Veamos que el producto de cardinales está bien definido. Para esto considere conjuntos A, A', B y B' tales que $|A| = |A'|$ y $|B| = |B'|$. De ello que existan funciones biyectivas $f : A \to A'$ y $g : B \to B'$. Ahora consideremos la función $f \times g : A \times B \to A' \times B'$ definida por $(f \times g)(a, b) = (f(a), g(b))$. Entonces del *Teorema 1.1.2* se sigue que $f \times g$ es biyectiva. Se concluye que $|A \times B| = |A' \times B'|$.

De forma análoga se puede demostrar que $|A \cup B| = |A' \cup B'|$. En efecto. Sean conjuntos A, B, A', B' tales que $|A| = |A'|$, $|B| = |B'|$ y $A \cap B = \emptyset = A' \cap B'$. Como $|A| = |A'|$ y $|B| = |B'|$ entonces existen funciones $h : A \to A'$ y $g : B \to B'$ ambas biyecciones. Definimos una función f de $A \cup B$ a $A' \cup B'$ como sigue:

$$f(x) = \begin{cases} h(x) & \text{si} \quad x \in A \\ \\ g(x) & \text{si} \quad x \in B \end{cases}$$

Entonces f es biyectiva. Para ver esto tomemos un elemento $y \in A' \cup B'$. Deducimos que f es sobreyectiva, puesto que $y \in A'$ ó $y \in B'$. Veamos ahora que f es inyectiva. Tomemos dos elementos $x_1, x_2 \in A \cup B$ tales que $f(x_1) = f(x_2)$. Si $x_1, x_2 \in A$ entonces de h se sigue que $x_1 = x_2$. Pensando de forma análoga, si $x_1, x_2 \in B$ entonces de g se garantiza que $x_1 = x_2$. Pensemos por un momento si fuese posible que $x_1 \in A$ y $x_2 \in B$. De ello que $h(x_1) = g(x_2)$, es decir $h(x_1) \in B'$ y $h(x_1) \in A'$. Así $A' \cap B' \neq \emptyset$ lo cual no es posible. Por lo tanto f es biyectiva y se concluye que $|A \cup B| = |A' \cup B'|$.

Teorema 1.1.5. *[14, pág. 161-162] Sea α un número cardinal infinito, entonces:*

i) $\alpha\alpha = \alpha$.

ii) $\alpha + \alpha = \alpha$.

1.2. Definiciones y resultados básicos de la teoría de números

Teorema 1.2.1. *[5, pág. 17.] El Algoritmo de la División.*
Dados $a, b \in \mathbb{Z}$, con $b > 0$, existen enteros únicos q, r con $0 \leqslant r < b$ tales que $a = bq + r$.

Definición 1.2.1. *Sean $a, b \in \mathbb{Z}$. Diremos que **a divide a b** si existe un entero c tal que $b = ac$. En este orden de ideas se denotará $a \mid b$ si a divide a b. En caso contrario escribiremos $a \nmid b$.*

Enseguida enunciamos algunas propiedades relacionadas con la anterior definición.

Proposición 1.2.1. *Para enteros cualesquiera a, b, c se cumplen las siguientes afirmaciones:*

1) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

2) $a \mid b$ y $b \mid a$ si y solo si $a = \pm b$.

3) Si $a \mid b$ y $b \neq 0$, entonces $|a| \leq |b|$.

4) Si $a \mid b$ y $a \mid c$, entonces $a \mid bx + cy$ para cualquier $x, y \in \mathbb{Z}$.

Ahora, dados dos enteros no nulos a, b diremos que un entero d es divisor común de a y b si $d \mid a$ y $d \mid b$. Como el número de divisores comunes de a y b es finito, sería razonable preguntarse por el máximo de ellos. Formalmente se tiene lo siguiente:

Definición 1.2.2. *Sean a, b enteros con al menos uno de ellos diferente de cero. Se denomina el* ***máximo común divisor*** *de a y b al mayor entero que sea divisor común de ambos. El máximo común divisor de a y b será denotado por $mcd(a, b)$.*

Ejemplo 1.2.1. $mcd(6, 150) = 6$. $mcd(6, 155) = 1$

Cuando $mcd(a, b) = 1$ se dirá que los enteros a, b son *primos relativos.* Veamos algunos importantes resultados.

Teorema 1.2.2. *[5, pág. 21] Si $a, b \in \mathbb{Z}$ con alguno de ellos no nulo, entonces existen enteros x, y tales que:*

$$mcd(a, b) = ax + by.$$

Corolario 1.2.1. *[5, pág. 23] Dados $a, b \in \mathbb{Z}$, entonces a y b son primos relativos si y solo si existen enteros x, y tales que $1 = ax + by$.*

En la gran obra *Disquisitiones Arithmeticae* del prolífico matemático Carl Friedrich Gauss se daban los fundamentos de la teoría moderna de números. Es en este trabajo donde aparece por vez primera el concepto de *congruencia*, el cual definiremos a continuación. [2]

Definición 1.2.3. *Dado n un entero positivo fijo y $a, b \in \mathbb{Z}$, diremos que* ***a es congruente con b módulo n*** *si $n \mid a - b$. En ese caso escribiremos $a \equiv b (mod\ n)$.*

Teorema 1.2.3. *[5, pág. 79] Teorema Chino del Residuo*
Sean $n_1, n_2, \cdots, n_k$ enteros positivos primos relativos dos a dos y $a_1, a_2, \cdots, a_k$ enteros cualesquiera, entonces el sistema de congruencias lineales

[2] BURTON, D. (2007). *Elementary Number Theory, Sixth Edition.* New York: Mc Graw Hill. p 61

$$a_1 \equiv x(mod\ n_1)$$
$$a_2 \equiv x(mod\ n_2)$$
$$\vdots$$
$$a_k \equiv x(mod\ n_k)$$

Tiene solución única módulo $n_1 n_2 \cdots n_k$.

Terminamos esta sección dando una definición y un resultado que son considerados por algunos como la columna vertebral de la teoría de números.

Definición 1.2.4. *Un entero positivo* $p > 1$ *es dicho un número primo si* p *tiene únicamente dos divisores positivos:* 1 *y* p. *Si* p *tiene más de un divisor se dirá que el número es compuesto.*

Teorema 1.2.4. *[5, pág. 41] El Teorema Fundamental de la Aritmética*
Todo entero positivo $n > 1$ *puede ser expresado de forma única como producto de números primos. Es decír* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, *donde* $\alpha_i \in \mathbb{Z}^+$ *y cada* p_i *es un número primo.*

1.3. Algunos conceptos de la teoría de grupos

Definición 1.3.1. *Diremos que un grupo es un conjunto no vacío* G *dotado de una operación binaria interna '*$*$*', es decir una función* $* : G \times G \to G$; *talque:*

i) Todos los elementos de G *verifican la propiedad asociativa: Dados* $x, y, z \in G$ *se tiene que* $x * (y * z) = (x * y) * z$.

ii) Existe un elemento $e \in G$ *llamado neutro que verifica la ecuación* $e * x = x * e = x$, *para todo* $x \in G$.

iii) Todo elemento $x \in G$ *tiene asociado un* $y \in G$ *llamado inverso de* x; *esto es, dado* $x \in G$, *existe* $y \in G$ *talque* $x * y = y * x = e$.

Observación 1.3.1. *Dado un grupo* G *y un elemento* $x \in G$ *se tiene que el elemento neutro y el inverso de* x *son únicos; es decir, sí* e *y* e' *son neutros de* G *entonces* $e = e'$, *y si* $\bar{x}$ *y* y *son ambos inversos de* x *entonces* $\bar{x} = y$. *Además de esto el inverso de* x *será denotado por* x^{-1} *y cuando se esté trabajando de forma general se simplificara la*

notación del producto $a * b$ por ab. Asimismo diremos que G es un grupo finito si G tiene un número finito de elementos. Se pensará de manera análoga cuando se hable de un grupo infinito.

El siguiente ejemplo nos será de gran ayuda más adelante.

Ejemplo 1.3.1. *El siguiente conjunto es un grupo multiplicativo:*

$$Q_8 := \langle -1, i, j, k : (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle.$$

Dicho grupo se conoce como el ***grupo de los cuaterniones****. Notemos que $ij \neq ji$ pues por un lado $ij = k$, mientras que $ji = -k$. Los grupos que cumplen con la propiedad conmutativa tienen un nombre especial y se definen a continuación.*

Definición 1.3.2. *Dado un grupo G diremos que este es un* ***grupo abeliano*** [3] *si en G se verifica la propiedad conmutativa.*

Ejemplo 1.3.2. *Sea $n \in \mathbb{N}$, entonces $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ es un grupo abeliano donde la operación esta definida por: $\bar{x} + \bar{y} = \overline{x+y}$.*

Ahora tomemos un entero positivo m. El conjunto $S_m := \{\sigma : I_m \to I_m : \sigma \text{ es biyección}\}$ junto con la composición usual de funciones se conoce como **el grupo de permutaciones** sobre I_m. Denotaremos cada permutación $\sigma \in S_m$ como un arreglo ordenado $(a \ \ \sigma(a) \ \ \sigma(\sigma(a)) \cdots)$ donde $a \in I_m$, excepto la permutación *identidad* que se escribirá como Id_m. Por ejemplo, si $m = 3$, entonces $S_3 = \{Id_3, (23), (13), (12), (123), (132)\}$. Consideremos los subconjuntos $H_1 = \{(23), (13)\}$ y $H_2 = \{(23), Id_3\}$ de S_3. Note que H_2 tiene estructura de grupo a diferencia de H_1, pues $(23) \circ (13) = (123) \notin H_1$.
Como vimos anteriormente no todo subconjunto de un grupo tiene estructura de grupo. Esto sugiere la siguiente definición.

Definición 1.3.3. *Decimos que un subconjunto no vacío H de un grupo G es un subgrupo si H tiene estructura de grupo bajo la operación de G restringida a H. Escribiremos $H \leq G$ en caso de ser H un subgrupo de G.*

Observación 1.3.2. *Para cualquier grupo G se dirá que un subgrupo H es propio si $\{e\} \neq H \neq G$. En caso contrario diremos que H es un subgrupo trivial.*

Ejemplo 1.3.3. *Dado $H \leq G$ y $g \in G$ tenemos que $gHg^{-1} := \{ghg^{-1} : h \in H\}$ es un subgrupo de G. Dicho subgrupo se conoce como el conjugado de H por g.*

[3] Cabe resaltar que dicho nombre fue propuesto como una distinción al arduo trabajo del matemático noruego Niels Henrik Abel, quien aportó considerablemente al avance del álgebra.

El siguiente resultado da un método para saber cuando un subconjunto de un grupo es un subgrupo. Una prueba de este hecho puede ser consultada en [7, pág. 47].

Teorema 1.3.1. *Un subconjunto H de un grupo G es un subgrupo si y solo si $H \neq \emptyset$ y si para todo $x, y \in H$ se tiene que $xy^{-1} \in H$.*

El siguiente teorema es debido al matemático italiano J. L. Lagrange, el cual fue publicado en el año 1770. Vale la pena aclarar que la formulación original de aquel trabajo no estaba en términos de grupos.

Teorema 1.3.2. *(Teorema de Lagrange) Si H es un subgrupo de un grupo finito G, entonces el orden de H divide al orden de G.*

Ejemplo 1.3.4. *Consideremos el grupo $\mathbb{Z}_p$ donde p es un número primo y tomemos H un subgrupo propio de $\mathbb{Z}_p$, entonces por el Teorema de Lagrange se sigue que $|H| \mid p$ y por esto $|H| = 1$ o $|H| = p$. En cualquiera de los dos casos se llega a una contradicción pues H es un subgrupo propio. En general, dado un grupo finito G de orden un número primo tenemos que G no tiene subgrupos propios.*

Enseguida definimos un subgrupo de suma importancia para este trabajo pues es una pieza fundamental a la hora de caracterizar la *Propiedad (D)*.

Definición 1.3.4. *Sea G un grupo y a un elemento de G. Definimos el conjunto de las potencias enteras de a como sigue:*

$$\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$$

Entonces $\langle a \rangle \leq G$ y llamamos a este el ***subgrupo cíclico generado por a****. El elemento a se denomina un* ***generador*** *del subgrupo.*

Ejemplo 1.3.5. *Tomemos el grupo $\mathbb{Z}_8$. Entonces $\langle 3 \rangle = \{0, 3, 6, 1, 4, 7, 2, 5\} = \mathbb{Z}_8$, mientras que $\langle 2 \rangle = \{0, 2, 4, 6\}$.*

El ejemplo anterior nos dice que el generador de un subgrupo cíclico en ocasiones ***genera*** la totalidad del grupo. Cuando esto ocurra se dirá que el grupo es ***cíclico***. Exactamente se tiene la siguiente definición

Definición 1.3.5. *Sea G un grupo. Diremos que G es cíclico si existe $a \in G$ tal que $G = \langle a \rangle$.*

Ejemplo 1.3.6. *Dado $G = \mathbb{Z}_2 \times \mathbb{Z}_3$ considere el elemento $(1, 1)$. Entonces*

$$(0,0) = 6(1,1)$$
$$(0,1) = 4(1,1)$$
$$(0,2) = 2(1,1)$$
$$(1,0) = 3(1,1)$$
$$(1,1) = 1(1,1)$$
$$(1,2) = 5(1,1).$$

Por lo tanto se tiene que $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle$.

Ejemplo 1.3.7. *Sea* $G = \langle a \rangle$ *un grupo cíclico y* $H \leq G$. *Afirmamos que* H *también es cíclico. Como* $H \subseteq \langle a \rangle$ *se tiene que todo elemento de* H *es una potencia entera de* a. *Sea* m *el menor entero positivo talque* $a^m \in H$. *Veamos que* $H = \langle a^m \rangle$. *Es claro que* $\langle a^m \rangle \subseteq H$. *Ahora tomemos* $x \in H$, *de ello que exista* $k \in \mathbb{Z}$ *talque* $x = a^k$. *Por el algoritmo de la división existen enteros* q, r *tales que* $k = qm + r$, *donde* $0 \leqslant r < m$, *entonces* $x = a^k = a^{qm+r} = a^{qm}a^r$. *Se sigue que* $a^r = a^{k-qm} \in H$ *pero como* m *es el menor entero positivo tal que* $a^m \in H$ *y* $r < m$ *se tiene que* $r = 0$. *Así* $x = (a^m)^q \in \langle a^m \rangle$ *y con esto hemos probado que* $H = \langle a^m \rangle$.

El ejemplo anterior nos ha dado respuesta al siguiente resultado.

Proposición 1.3.1. *Todo subgrupo de un grupo cíclico es cíclico.*

Ejemplo 1.3.8. *Sea* $\mathbb{Q}$ *el grupo aditivo de números racionales, entonces* $\mathbb{Q}$ *no es un grupo cíclico. En efecto; supongamos que* $\mathbb{Q}$ *es un grupo cíclico, entonces existe* $\frac{a}{b} \in \mathbb{Q}$ *tal que* $\mathbb{Q} = \langle \frac{a}{b} \rangle$. *Ahora tomemos el elemento* $\frac{1}{p} \in \mathbb{Q}$, *donde* $p \in \mathbb{Z}^+$ *y* $mcd(p, b) = 1$. *Como* $\frac{1}{p} \in \mathbb{Q}$, *existe* $n \in \mathbb{Z}$ *tal que* $\frac{1}{p} = \frac{a}{b}(n)$ *o equivalentemente* $b = p(na)$. *De ello que* $p \mid b$ *lo cual es una contradicción pues* b *y* p *son primos relativos. Así* $\mathbb{Q}$ *no es cíclico.*

Proposición 1.3.2. *Un grupo* G *es cíclico si y solo si* G *no es unión de subgrupos propios.*

Demostración. Sea $G := \langle g \rangle$, para algún $g \in G$ y tomemos H un subgrupo propio de G. Note que $g \notin H$ pues en caso contrario $G = H$ y esto sería contradictorio. Ahora consideremos $\{H_i\}_{i \in I}$ la familia de subgrupos propios de G, se sigue que $g \notin \bigcup_{i \in I} H_i$ y con esto hemos probado que G no es unión de subgrupos propios.
Recíprocamente, sea $\{H_i\}_{i \in I}$ la familia de subgrupos propios de G. Como $G \neq \bigcup_{i \in I} H_i$, de ello que existe $g \in G$ talque $g \notin \bigcup_{i \in I} H_i$. Luego $\langle g \rangle$ no es un subgrupo propio de G. Concluimos que $G = \langle g \rangle$.

□

Definición 1.3.6. *Sea G un grupo y $a \in G$. Se define:*

1) *El orden de G como el número de elementos que tiene G. Escribiremos $|G|$ para denotar el orden de G.*

2) *El orden de a, simbolizado por $|a|$, como el menor entero positivo m tal que $a^m = e$ (en notación aditiva $ma = 0$). En ese caso escribiremos $|a| = m$. Si dicho entero no existe se dirá que el orden de a es infinito.*

Ejemplo 1.3.9. *Considere el grupo aditivo $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ y el elemento $(1, 1)$. Entonces $|G| = 4$ y $|(1, 1)| = 2$.*

Los siguientes resultados están particularmente ligados a los grupos cíclicos.

Teorema 1.3.3. *[10, pág. 73.] Sea G un grupo y $a \in G$. Si a tiene orden infinito, entonces $a^i = a^j$ si y sólo si $i = j$. Si a tiene orden finito, digamos m, entonces $a^i = a^j$ si y sólo si $i \equiv j (mod\ m)$.*

Proposición 1.3.3. *[10, pág. 74-75] Sea G un grupo y $k \in \mathbb{N}$. Entonces:*

1) *Para cualquier elemento a en G, $|a| = |\langle a \rangle|$.*

2) *$\langle a^k \rangle = \langle a^{mcd(n,k)} \rangle$, donde $|a| = n$.*

3) *Si $a^k = e$, entonces $|a| \mid k$.*

Definición 1.3.7. *Dado un grupo G y $H \leq G$ se define para algún elemento $a \in G$ la clase lateral izquierda de H en G como el conjunto*

$$aH := \{ah : h \in H\}.$$

Análogamente se define la clase lateral derecha de H como $Ha := \{ha : h \in H\}$.

Una clase lateral en general no tiene estructura de grupo. Por esto enunciaremos algunas propiedades inherentes a las clases laterales y daremos estructura de grupo al conjunto de todas ellas. Antes de hacer esto probaremos el siguiente lema:

Lema 1.3.1. *Si G es un grupo y $H \leq G$, entonces $G = \bigcup_{g \in G} gH$.*

Demostración. Probemos que $G = \bigcup_{g \in G} gH$. Es claro que $G \supseteq \bigcup_{g \in G} gH$. Veamos la otra contenencia. Sea $g \in G$, luego $g = ge \in gH$. De esto concluimos que $g \in \bigcup_{g \in G} gH$. □

Proposición 1.3.4. *[10, pág. 139.] Sean G un grupo, H un subgrupo de G y $a, b \in G$; entonces:*

1) $aH = H$ si y sólo si $a \in H$.

2) $aH = bH$ o $aH \cap bH = \varnothing$.

3) $aH = bH$ si y sólo si $ab^{-1} \in H$.

4) $aH = Ha$ si y sólo si $H = aHa^{-1}$.

5) $|aH| = |bH|$.

La primera propiedad nos dice cuando una clase lateral admite una estructura de grupo, 2) pone en evidencia que las clases laterales son iguales o disjuntas dos a dos. Las propiedades 3) y 4) nos caracterizan respectivamente la igualdad de clases laterales y cuando una clase lateral es indistinguible, en el sentido de que no se encuentra una diferencia relevante entre aH y Ha, mientras que 5) afirma que todas las clases laterales tienen igual cardinal.

Definición 1.3.8. *Si G es un grupo cualquiera y $H \leq G$ se define el número de clases laterales distintas dos a dos como el **índice** de H en G y será denotado por $[G : H]$.*

Observación 1.3.3. *De la definición anterior, si G fuera finito, se tendría por la prueba del Teorema de Lagrange que tal número es $\frac{|G|}{|H|}$ [7, pág. 89].*

A continuación se definirá un particular tipo de subgrupo que ha sido sumamente importante en el desarrollo del álgebra abstracta.

Definición 1.3.9. *Sea G un grupo y $N \leq G$. Decimos que N es un **subgrupo normal** en G si $N = gNg^{-1}$, para todo elemento $g \in G$. Se escribirá $N \trianglelefteq G$ si N es un subgrupo normal de G.*

Ejemplo 1.3.10. *Consideremos la función $f : \mathbb{C} \to \mathbb{R}$ definida por $f(x + iy) = x + y$. Entonces $N = \{z \in \mathbb{C} : f(z) = 0\}$ es un subgupo normal en $\mathbb{C}$.*

Definición 1.3.10. *Sea un grupo G y $N \trianglelefteq G$. El conjunto*

$$G/N := \{aN : a \in G\}.$$

*Dotado de la operación binaria definida por $(aN)(bN) = (ab)N$ es llamado el **grupo cociente de G por N.***

Ejemplo 1.3.11. $\mathbb{Q}/\mathbb{Z}$ *es el grupo cociente de* $\mathbb{Q}$ *por* $\mathbb{Z}$*, conocido como* ***el grupo de racionales módulo uno****.*

Definición 1.3.11. *Sean* G_1, G_2 *grupos y* $\varphi : G_1 \to G_2$ *una función. Diremos que* φ *es un* ***morfismo de grupos*** *si dados* $g_1, g_2 \in G_1, \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$*. A los morfismos de grupos se les suele llamar* ***homomorfismo de grupos.***

Ejemplo 1.3.12. *La función* $\pi : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ *definida por* $\pi(a) = \mathbb{Z} + a$ *es un homomorfismo de grupos. Dicha función recibe el nombre de* ***proyección natural de*** $\mathbb{Q}$ ***en*** $\mathbb{Q}/\mathbb{Z}$ *.*

Observación 1.3.4. *Dado un morfismo de grupos* $\varphi : G \to H$*, si* φ *es inyectiva diremos que* φ *es un monomorfismo. Análogamente, si* φ *es sobreyectiva o biyectiva diremos que el morfismo es un epimorfismo o un isomorfismo respectivamente.*

Ejemplo 1.3.13. *Consideremos la factorización del entero positivo* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *y definamos la siguiente función*

$$f_n : \mathbb{Z}_n \to \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \mathbb{Z}_{p_k^{\alpha_k}}$$
$$\bar{x} \longmapsto (\bar{x}, \bar{x}, \cdots, \bar{x})$$

Entonces f_n *está bien definida y del Teorema Chino de los Restos se sigue que esta función es un isomorfismo de grupos.*

Observación 1.3.5. *Cuando se tenga un isomorfismo de grupos* $\varphi : G \to K$ *diremos que* G ***es isomorfo a*** K *y lo denotaremos por* $G \simeq K$*. Además si* $K = G$ *entonces llamaremos al isomorfismo un* ***automorfismo*** *de* G*.*

Ejemplo 1.3.14. *Dado un grupo cíclico* $G = \langle a \rangle$ *de orden* n*, para algún* $a \in G$*. Afirmamos que* G *es isomorfo a* $\mathbb{Z}_n$*. Sabemos que* $G = \{a^0, a, a^2, \cdots, a^{n-1}\}$*, ahora consideremos la función* $f : G \to \mathbb{Z}_n$ *definida por* $f(a^i) = \bar{i}$*, con* $0 \leq i < n$*. Entonces del Teorema 1.3.3 tenemos que* f *está bien definida. Probemos ahora que* f *es un isomorfismo. Para ver que* f *es morfismo de grupos basta observar que* $f(a^{i+j}) = \overline{i+j} = \bar{i} + \bar{j} = f(a^i) + f(a^j)$*. Veamos ahora que la función es inyectiva. Sean* $a^i, a^j \in G$ *tales que* $f(a^i) = f(a^j)$*, luego* $\bar{i} = \bar{j}$*, es decír* $i \equiv j(\ mod\ n)$*. De ello que* $n \mid j - i$ *y por el Teorema 1.3.3* $a^i = a^j$*. Así* f *es inyectiva. Ahora, sea* $\bar{i} \in \mathbb{Z}_n$*, entonces consideremos* $a^i \in G$ *y así* $f(a^i) = \bar{i}$*. Concluimos que* f *es un isomorfismo y con esto hemos probado el siguiente resultado: Todo grupo cíclico finito de orden* n *es isomorfo a* $\mathbb{Z}_n$*, para cualquier* $n \in \mathbb{N}$*.*

Definición 1.3.12. *Sea $\Psi : G \to H$ un homomorfismo de grupos. Definimos el* ***Kernel*** *de Ψ como*

$$Ker(\Psi) := \{g \in G : \Psi(g) = e_H\}.$$

Donde e_H es la identidad de H. También definimos la ***Imagen*** *de Ψ como el conjunto de todas las imágenes de G bajo Ψ, esto es*

$$Im(\Psi) := \{h \in H : \Psi(g) = h, \text{para algún } g \in G\}.$$

Veamos unas cuantas propiedades básicas de los homomorfismos de grupos que serán utilizadas más adelante.

Proposición 1.3.5. *[10, pág. 202-204.] Sea $\phi : G \to H$ un homomorfismo de grupos, entonces*

i) $\phi(e_G) = e_H$, *donde e_G y e_H son las identidades de G y H respectivamente.*

ii) $Ker(\phi) \trianglelefteq G$ *y* $Im(\phi) \leq H$.

Terminamos esta sección enunciando algunos resultados importantes sobre isomorfismos de grupos. La demostración puede ser consultada en [12, pág. 44-45].

Teorema 1.3.4. *Sea $\varphi : G \to \overline{G}$ un morfismo de grupos, entonces:*

i) $G/ker(\varphi) \simeq Im(\varphi)$ *(Primer teorema de isomorfismo de grupos).*

ii) Si φ es un epimorfismo de grupos, entonces existe una biyección entre todos los subgrupos de G que contienen a $ker(\varphi)$ y todos los subgrupos de $\overline{G}$.

iii) Dado un grupo G y $N \trianglelefteq G$ de un grupo G se tiene que todo subgrupo de G/N es de la forma K/N, donde K es un subgrupo de G que contiene a N.

Capítulo 2

Planteamiento del problema

En este capítulo plantearemos formalmente el problema que motiva este trabajo, junto a su respectiva solución. Para lograrlo debemos previamente mostrar un poco de teoría adicional, esto con el objetivo de facilitar la solución a nuestro problema. Esta teoría sera dividida en dos secciones: grupos finitos y grupos abelianos. Habrán algunos teoremas y proposiciones exhibidos sin demostración alguna, ya que éstos no son los resultados principales del presente trabajo. Algunos de ellos son resultados clásicos o son bien conocidos y pueden encontrarse en cualquier libro de teoría de grupos. Se aconseja al lector interesado en una prueba consultar [12]. La última sección de este capítulo está dedicada netamente al estudio de la *Propiedad (D)* y por ende nuestro trabajo principal se encuentra allí.

2.1. Grupos finitos

Proposición 2.1.1. *Sea G un grupo cíclico finito, entonces para cualquier entero positivo d divisor de $|G|$, G tiene un único subgrupo de orden d.*

Demostración. Veamos primero que dicho subgrupo existe. Sea d un divisor positivo de $|G| = n$, de ello que exista $w \in \mathbb{Z}$ tal que $n = dw$, o equivalentemente $w = \frac{n}{d}$. Ahora, como G es cíclico, existe $g \in G$ tal que $G = \langle g \rangle$. Consideremos el elemento $g^w \in G$. Afirmamos que $|g^w| = d$. Para probar esto verifiquemos que d es el menor entero positivo que anula a g^w. Por un l tenemos que:

$$(g^w)^d = (g^{\frac{n}{d}})^d = g^n = e.$$

Ahora supongamos que existe $k \in \mathbb{Z}$ tal que $(g^w)^k = e$ y deduzcamos que $d \mid k$. Comencemos considerando las siguientes ecuaciones:

$$(g^w)^d = e, \tag{2.1}$$

$$(g^w)^k = e \tag{2.2}$$

De *(2.1) y (2.2)* tenemos que $(g^w)^d = (g^w)^k$, o equivalentemente $g^n = g^{wk}$. Se sigue del *Teorema 1.3.3* que $n \mid n-wk$, de ello que exista $j \in \mathbb{Z}$ tal que $n-wk = nj$. Como $n = dw$ entonces reemplazando se tiene que $dw - wk = (dw)j$ y despejando convenientemente se llega a que $d \mid k$. Luego $d \leq k$ y así hemos probado que d es el menor entero positivo que anula a g^w. Finalmente consideremos el subgrupo $\langle g^w \rangle$. De la *Proposición 1.3.3* se tiene que $\langle g^w \rangle$ es un subgrupo de orden d. Con esto hemos probado la existencia de dicho subgrupo. Veamos ahora que este subgrupo es único. Sean $H, K \leq G$ tal que $|H| = d = |K|$. Se sigue de la *Proposición 1.3.3* que $H = \langle g^{d_1} \rangle$ y $K = \langle g^{d_2} \rangle$, donde d_1 y d_2 dividen a $|G|$. Luego $\frac{n}{d_1} = |\langle g^{d_1} \rangle| = |H| = d = |K| = |\langle g^{d_2} \rangle| = \frac{n}{d_2}$. Así $d_1 = d_2$ y con esto $H = K$.

□

Gracias al sustancial legado que dejó Abel en Noruega, el matemático Ludwing Sylow pudo hacer sus respectivos aportes en esta rama de la matemática. Dichos resultados son conocidos como los ***teoremas de Sylow***. Antes de enunciarlos se tienen las siguientes definiciones.

Definición 2.1.1. *Diremos que dos subgrupos H, K de un grupo G son conjugados en G si existe $g \in G$ tal que $H = gKg^{-1}$.*

Definición 2.1.2. *Sea G un grupo finito y p un número primo que divide al orden de G. Si p^k es la mayor potencia de p que divide a $|G|$, entonces un subgrupo de orden p^k es llamado un* ***p-subgrupo de Sylow.***

Ejemplo 2.1.1. *Tengamos en cuenta al grupo $G = \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \mathbb{Z}_{p_k^{r_k}}$, donde $p_i \neq p_j, \forall i, j \in \{1, 2, \cdots, k\}$. Entonces $H = \{0\} \times \{0\} \times \cdots \times \mathbb{Z}_{p_i^{r_i}} \times \{0\} \times \cdots \times \{0\}$ es un p_i-subgrupo de Sylow de G.*

Ejemplo 2.1.2. *Pensemos en el grupo simétrico S_3. Este tiene tres 2-subgrupos de Sylow los cuales son $\langle (12) \rangle$, $\langle (23) \rangle$ y $\langle (13) \rangle$. También hay un 3-subgrupo de Sylow: $\langle (123) \rangle$. Observemos también que los 2-subgrupos son conjugados dos a dos, es decír:*

$$(13)\langle (12) \rangle (13)^{-1} = \langle (23) \rangle,\ (23)\langle (12) \rangle (23)^{-1} = \langle (13) \rangle,\ (12)\langle (23) \rangle (12)^{-1} = \langle (13) \rangle.$$

Teorema 2.1.1. *[12, pág. 94-95.]* ***Teoremas de Sylow:*** *Sea G un grupo finito y p un número primo que divide al orden de G, entonces:*

1) *Todo subgrupo cuyo orden es una potencia de p está contenido en algún p-subgrupo de Sylow.*

2) *Todos los p-subgrupos de Sylow son conjugados.*

3) *Sea n_p el número de p-subgrupos de Sylow de G, entonces $n_p \equiv 1 (mod\ p)$.*

Ahora consideremos un grupo finito G tal que él tiene un único subgrupo H de orden dado. Afirmamos que dicho subgrupo es normal en G. Para probar esto tomemos un elemento $g \in G$ y por el *Ejemplo 1.3.3* tenemos que $gHg^{-1} \leq G$, de donde $|H| = |gHg^{-1}|$ (basta tener en cuenta la biyección $\varphi : H \to gHg^{-1}$ definida por $\varphi(h) = ghg^{-1}$). Por hipótesis, como H es el único subgrupo de orden $|H|$, tenemos que $H = gHg^{-1}$. Con esto hemos probado el siguiente resultado:

Proposición 2.1.2. *Sea G un grupo finitio. Si H es el único subgrupo de orden $|H|$, entonces H es normal en G.*

El siguiente resultado caracteriza la normalidad de p-subgrupos de Sylow.

Proposición 2.1.3. *Dado un grupo finito G entonces para algún primo p, un p-subgrupo de Sylow es normal si y solo si es único.*

Demostración. Sea H un p-subgrupo de Sylow de G tal que $H \trianglelefteq G$ y supongamos que existe K p-subgrupo de Sylow de G tal que $K \trianglelefteq G$. Veamos que $H = K$. Como H y K son p-subgrupos de Sylow, por el *Teorema 2.1.1* tenemos que $K = gHg^{-1}$ para algún $g \in G$, luego $K = gHg^{-1} = H$ por ser H normal en G.
Recíprocamente, supongamos que H es el único p-subgrupo de Sylow de G. Por la *Proposición 2.1.2* tenemos que H es un subgrupo normal de G.

□

Proposición 2.1.4. *Asuma que G es un grupo finito tal que para todo primo p que divide a $|G|$, todo p-subgrupo de Sylow de G es normal. Entonces G es producto directo de sus p-subgrupos de Sylow.*

Antes de demostrar la proposición anterior es necesario recordar un par de resultados. Los detalles pueden ser consultados en [7, pág. 93-94].

Lema 2.1.1. *Sea G un grupo y H, K subgrupos de G, entonces:*

i) Sí H y K son subgrupos finitos, entonces $|HK| = \frac{|H||K|}{|H\cap K|}$.

ii) Si $H \trianglelefteq G$ o $K \trianglelefteq G$, entonces $HK \leq G$.

Demostración. Probemos el Lema anteriormente enunciado.

i) Dado $hk \in HK$ note que $hk \in hK$. Más aún, $hk \in \bigcup_{h\in H} hK$. Recíprocamente si $hk \in \bigcup_{h\in H} hK$, entonces $hk \in HK$. De ello que $HK = \bigcup_{h\in H} hK$.

Veamos cual es el número de clases laterales distintas. Sean $h_1, h_2 \in H$, luego:

$$h_1K = h_2K \Leftrightarrow h_1h_2^{-1} \in K \Leftrightarrow h_1h_2^{-1} \in H \cap K \Leftrightarrow h_1(H \cap K) = h_2(H \cap K)$$

Esto último nos dice que el número de clases laterales distintas de la forma hK es igual al número de clases laterales de la forma $h(H \cap K)$, para algún $h \in H$. Se sigue de la prueba del *Teorema de Lagrange* ([7, pág. 89]) que el número de clases laterales distintas de la forma $h(H \cap K)$ es $\frac{|H|}{|H\cap K|}$. Como cada clase lateral tiene $|K|$ elementos se concluye que $|HK| = |\bigcup_{h\in H} hK| = \frac{|H|}{|H\cap K|}|K|$.

ii) Supongamos sin pérdida de generalidad que $H \trianglelefteq G$. Por las propiedades de clases laterales tenemos que $gH = Hg$ para todo $g \in G$. En particular, si $g \in K$ entonces $KH = HK$. Dicho lo anterior procedamos a demostrar que $HK \leq G$. Sean $a, b \in HK$, entonces existen $h_1, h_2 \in H$ y $k_1, k_2 \in K$ tales que $a = h_1k_1$ y $b = h_2k_2$, luego $ab^{-1} = h_1(k_1k_2^{-1}h_2^{-1})$. Observemos que $k_1k_2^{-1}h_2^{-1} \in KH = HK$, luego existen $h_3, k_3 \in K$ tales que $k_1k_2^{-1}h_2^{-1} = h_3k_3$. Así $ab^{-1} = h_1h_3k_3 \in HK$. Concluimos por el *Teorema 1.3.1* que $HK \leq G$.

□

Proposición 2.1.5. *Dado un grupo G y dos subgrupos normales H, K en G. Si $H\cap K = \{e\}$ y $G = HK$, entonces $G \simeq H \times K$.*

Demostración. Antes que todo vamos a demostrar que todos los elementos de H conmutan con todos los elementos de K. Para esto sea $h \in H$ y $k \in K$. Como H es normal se sigue que $khk^{-1} \in H$, luego $(khk^{-1})h^{-1} \in H$. Análogamente concluimos que $k(hk^{-1}h^{-1}) \in K$. Por hipótesis $khk^{-1}h^{-1} = e$ y de esto deducimos que $kh = hk$. Considerando lo anterior veamos que $G \simeq H \times K$. Consideremos para nuestro caso la siguiente función

$$\begin{aligned} f : H \times K &\to G \\ (h,k) &\mapsto hk \end{aligned}$$

Veamos ahora que la función es un homomorfismo de grupos. Sean $(h_1,k_1),(h_2,k_2) \in H \times K$, luego

$$\begin{aligned} f((h_1,k_1)(h_2,k_2)) &= f(h_1h_2, k_1k_2) \\ &= (h_1h_2)(k_1k_2) \\ &= h_1(h_2k_1)k_2 \\ &= h_1(k_1h_2)k_2 \\ &= (h_1k_1)(h_2k_2) \\ &= f(h_1,k_1)f(h_2,k_2). \end{aligned}$$

Para verificar la inyectividad tomemos $(h_1,k_1),(h_2,k_2) \in H \times K$ tales que $f(h_1,k_1) = f(h_2,k_2)$, de ello que $h_1k_1 = h_2k_2$; luego $h_2^{-1}h_1 = k_2k_1^{-1}$. Note que $h_2^{-1}h_1 \in H \cap K$. Se sigue por hipótesis que $h_1 = h_2$. Análogamente se tiene que $k_1 = k_2$. Para finalizar la prueba tomemos $y \in G$. Por hipótesis existen $h \in H$ y $k \in K$ tales que $y = hk$. En ese sentido considere el elemento $(h,k) \in H \times K$ y así $f(h,k) = y$. Con esto hemos probado que f es un isomorfismo de grupos y concluimos que $G \simeq H \times K$.

□

La siguiente prueba es la correspondiente a la *Proposición 2.1.4*.

Demostración. Sea $n = |G| = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$. Ya que para todo $i \in I_k$ los p_i- subgrupos de Sylow son normales, por la *Proposición 2.1.3* ellos son únicos. Dicho esto, para cada $i \in I_k$, sea H_i el p_i- subgrupo de Sylow de G. Es claro que si $i \neq j$, entonces $H_i \cap H_j = \{e\}$. Por otro lado del *Lema 2.1.1* tenemos que $|H_1H_2| = |H_1||H_2|$. Más aún, note que $|H_1H_2H_3| = |H_1||H_2||H_3|$. Ahora supongamos que la propiedad se tiene para un entero k, es decír, $|H_1H_2\cdots H_k| = |H_1||H_2|\cdots|H_k|$ y probemos que esta propiedad se cumple para $k+1$. Antes de esto note que $H_1H_2\cdots H_kH_{k+1} = (H_1H_2\cdots H_k)H_{k+1}$. Entonces

$$\begin{aligned} |H_1H_2\cdots H_kH_{k+1}| &= |(H_1H_2\cdots H_k)H_{k+1}| \\ &= |H_1H_2\cdots H_k||H_{k+1}| \\ &= |H_1||H_2|\cdots|H_k||H_{k+1}|. \end{aligned}$$

Luego $|H_1H_2\cdots H_k| = |H_1||H_2|\cdots|H_k|$ para todo entero positivo k. Por otro lado, del *Lema 2.1.1* se garantiza que $H_1H_2\cdots H_k \leq G$ y por el razonamiento hecho anteriormente se concluye $H_1H_2\cdots H_k = G$. Finalmente, por la *Proposición 2.1.5* tenemos que $G \cong H_1 \times H_2 \times \cdots \times H_k$.

□

2.2. Grupos abelianos

A continuación se define un grupo que llama la atención por sus propiedades ya que él es un grupo infinito cuyos subgrupos son todos finitos, él no es cíclico pero cualquier subgrupo propio si lo es, ningún elemento allí tiene orden infinito y lo más importante, él es una pieza clave a la hora de clasificar a los grupos abelianos divisibles.

Definición 2.2.1. *Sea $p \in \mathbb{Z}$ un número primo, entonces el* ***grupo de Prüfer*** *de tipo p^∞, denotado por $\mathbb{Z}(p^\infty)$, es el subgrupo de $\mathbb{Q}/\mathbb{Z}$ definido por:*

$$\mathbb{Z}(p^\infty) := \{\tfrac{a}{p^n} + \mathbb{Z} : a \in \mathbb{Z}, n \in \mathbb{Z}^+\}.$$

Observación 2.2.1. *Dado p un número primo, el grupo de Prüfer también es conocido como el* ***grupo cuasi-cíclico*** *de tipo p^∞.*

Ejemplo 2.2.1. [1] *Tomemos $p = 2$ y consideremos el grupo $\mathbb{Z}(2^\infty)$. Ahora tomemos un elemento $\frac{a}{p^n} + \mathbb{Z}$. Por el Algoritmo de la División existen $q, r \in \mathbb{Z}$ tales que $a = p^nq + r$ con $0 \leq r < p^n$, entonces $\frac{a}{p^n} + \mathbb{Z} = \frac{p^nq+r}{p^n} + \mathbb{Z} = q + \frac{r}{p^n} + \mathbb{Z} = \frac{r}{p^n} + \mathbb{Z}$; entonces podemos escribir algunos elementos de $\mathbb{Z}(2^\infty)$ como: $0 + \mathbb{Z}$, $\frac{1}{2} + \mathbb{Z}$, $\frac{1}{4} + \mathbb{Z}$, $\frac{3}{4} + \mathbb{Z}$, $\frac{1}{8} + \mathbb{Z}$, $\frac{3}{8} + \mathbb{Z}$, $\frac{5}{8} + \mathbb{Z}$, $\frac{7}{8} + \mathbb{Z}$, $\cdots$.*

[1] FRÍAS, M. (1993). *Clasificación de grupos abelianos.* [En línea]. Trabajo de grado en Licenciatura en Matemáticas. Sonora: Universidad de Sonora. Departamento de Matemáticas. 87p. (Recuperado en 24 mayo 2017). Disponible en http://lic.mat.uson.mx/tesis/78TesisEduardoFrias.PDF p. 41.

Veamos algunos lemas ligados a este grupo que nos serán de gran ayuda más adelante.

Lema 2.2.1. *Sean $i, j \in \mathbb{Z}^+$ tales que $i \neq j$, entonces $\frac{1}{p^i} + \mathbb{Z} \neq \frac{1}{p^j} + \mathbb{Z}$.*

Demostración. Veamos que $\frac{1}{p^i}+\mathbb{Z} \neq \frac{1}{p^j}+\mathbb{Z}$. Por contradicción, supongamos que $\frac{1}{p^i}+\mathbb{Z} = \frac{1}{p^j} + \mathbb{Z}$. Por propiedades de clases laterales tenemos que $\frac{1}{p^i} - \frac{1}{p^j} \in \mathbb{Z}$, de lo cual se tiene que existe $k \in \mathbb{Z}$ tal que $\frac{1}{p^i} - \frac{1}{p^j} = k$, o equivalentemente $\frac{p^j - p^i}{p^i p^j} = k$. Concluimos que $p^i p^j \mid p^j - p^i$. Note además que $p^i \mid p^i p^j$ y por la *Proposición 1.2.1* tenemos que $p^i \mid p^j - p^i$. Nuevamente se sigue de la *Proposición 1.2.1* que $p^i \mid p^j$. Un razonamiento análogo mostraría que $p^j \mid p^i$, lo cual nos dice que $p^i = p^j$ y esto llevaría a que $i = j$, lo cual contradice nuestra hipótesis. Así $\frac{1}{p^i} + \mathbb{Z} \neq \frac{1}{p^j} + \mathbb{Z}$.

□

Lema 2.2.2. *Si p es un número primo y $x := \frac{a}{p^m} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$ es no nulo, entonces $\langle x \rangle = \langle \frac{1}{p^m} + \mathbb{Z} \rangle$.*

Demostración. Supongamos sin perdida de generalidad que a y p^m son primos relativos. Se sigue del *Corolario 1.2.1* que existen enteros c, d tales que

$$1 = ca + dp^m.$$

Afirmamos que $\langle x \rangle = \langle cx \rangle$. Primero notemos que

$$\begin{aligned} cx &= \frac{ca}{p^m} + \mathbb{Z} \\ &= \frac{1 - dp^m}{p^m} + \mathbb{Z} \\ &= \frac{1}{p^m} + \mathbb{Z}. \end{aligned}$$

Sea $y \in \langle x \rangle$, entonces existe $n \in \mathbb{Z}^+$ tal que $y = nx$. Luego

$$\begin{aligned} y = nx &= n(\frac{a}{p^m} + \mathbb{Z}) \\ &= an(\frac{1}{p^m} + \mathbb{Z}) \\ &= an(cx) \in \langle cx \rangle. \end{aligned}$$

Ahora sea $y := n(cx) \in \langle cx \rangle$, claramente $y \in \langle x \rangle$. Con esto damos por concluida la prueba.

□

Lema 2.2.3. *Dado un número primo p y $x := \frac{a}{p^m} + \mathbb{Z}$, $y := \frac{b}{p^n} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$, entonces $y \in \langle x \rangle$ si y sólo si $n \leq m$.*

Demostración. Primero supongamos que $y \in \langle x \rangle$ y mostremos que $n \leq m$. Por el *Teorema de Lagrange* tenemos que $|y| \mid |\langle x \rangle|$ y por el *Lema 2.2.2* $\langle x \rangle = \langle \frac{1}{p^m} + \mathbb{Z} \rangle$. Se sigue de lo anterior que $p^n \mid p^m$ (más adelante veremos que todo elemento de $\mathbb{Z}(p^\infty)$ tiene orden una potencia de p) y así $p^n \leq p^m$ con lo cual $n \leq m$. Recíprocamente, si $n \leq m$ entonces $\frac{b}{p^n} + \mathbb{Z} = \frac{bp^{m-n}}{p^m} + \mathbb{Z} \in \langle x \rangle$. Con esto hemos terminado la prueba. □

Probemos ahora otras propiedades del grupo $\mathbb{Z}(p^\infty)$.

Proposición 2.2.1. *Sea p un primo, entonces*

1) *$\mathbb{Z}(p^\infty)$ tiene orden infinito.*

2) *Todo elemento de $\mathbb{Z}(p^\infty)$ tiene orden finito.*

3) *Para todo $x, y \in \mathbb{Z}(p^\infty)$, se tiene que $\langle x \rangle \subseteq \langle y \rangle$ o $\langle y \rangle \subseteq \langle x \rangle$.*

4) *Todo subgrupo propio de $\mathbb{Z}(p^\infty)$ tiene orden finito.*

Demostración. Para probar 1) primero consideremos la función $f_p : \mathbb{Z}^+ \to \mathbb{Z}(p^\infty)$ definida por

$$f_p(i) = \tfrac{1}{p^i} + \mathbb{Z}.$$

Se sigue del *Lema 2.2.1* que f_p es inyectiva. Esto prueba que $\mathbb{Z}(p^\infty)$ tiene un subconjunto equipotente con $\mathbb{N}$ y por el *Teorema 1.1.3* se tiene que el grupo de Prüfer tiene orden infinito.

2) Sea $x := \frac{a}{p^m} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$ y supongamos sin pérdida de generalidad que a y p son primos relativos. Por un lado note que

$$p^m x = \tfrac{p^m a}{p^m} + \mathbb{Z} = 0 + \mathbb{Z}.$$

Ahora, supongamos que existe $y \in \mathbb{Z}^+$ tal que $yx = 0 + \mathbb{Z}$ y probemos que $p^m \mid y$. Como $p^m x = 0 + \mathbb{Z}$ y $yx = 0 + \mathbb{Z}$ entonces $p^m x = yx$; es decír $\frac{p^m a}{p^m} + \mathbb{Z} = \frac{ay}{p^m} + \mathbb{Z}$. De la *Proposición 1.3.4* se sigue que existe $k \in \mathbb{Z}$ tal que

$$\tfrac{ay}{p^m} - \tfrac{p^m a}{p^m} = k.$$

O equivalentemente $\frac{ay}{p^m} = k + a$, de donde se obtiene que $p^m \mid y$.

3) Dados $x := \frac{a}{p^m} + \mathbb{Z}, y := \frac{b}{p^n} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$ veamos que $\langle x \rangle \subseteq \langle y \rangle$ o $\langle y \rangle \subseteq \langle x \rangle$. Por el *Lema 2.2.2* tenemos que $\langle x \rangle = \langle \frac{1}{p^m} + \mathbb{Z} \rangle$ y $\langle y \rangle = \langle \frac{1}{p^n} + \mathbb{Z} \rangle$. Supongamos ahora que $m < n$, luego $\frac{1}{p^m} + \mathbb{Z} = \frac{p^{n-m}}{p^n} + \mathbb{Z} \in \langle y \rangle$. Así $\langle x \rangle \subseteq \langle y \rangle$. Si $n < m$ un procedimiento similar mostraría que $\langle y \rangle \subseteq \langle x \rangle$. Finalmente el resultado es claro si $m = n$.

4) Si H es un subgrupo propio de $\mathbb{Z}(p^\infty)$, veamos que H es finito. Para esto consideremos $x = \frac{a}{p^m} + \mathbb{Z} \in \mathbb{Z}(p^\infty) \backslash H$ y probemos que $H \subseteq \langle x \rangle$. Sea $y = \frac{b}{p^n} + \mathbb{Z} \in H$. Si $n \leq m$ se tiene del *Lema 2.2.3* que $y \in \langle x \rangle$. Si por el contrario $m < n$, nuevamente por el *Lema 2.2.3* tendríamos que $x \in \langle y \rangle \subseteq H$, luego $x \in H$ lo cual es contradictorio. De lo anterior se concluye que $H \subseteq \langle x \rangle$. Finalmente de la *Proposición 1.3.3* se tiene que $|\langle x \rangle|$ es finito, luego H es finito.

□

Observación 2.2.2. *Dado un subgrupo propio H de $\mathbb{Z}(p^\infty)$ se sigue de 4) de la proposición anterior y de la Proposición 1.3.1 que H es cíclico.*

Definición 2.2.2. *Sea p un número primo y G un grupo abeliano. Decimos que G es* ***p- divisible*** *si $G = pG := \{pg : g \in G\}$. Adicionalmente si lo anterior se cumple para todo entero positivo n, es decír si $nG := \{ng : g \in G\} = G$ entonces decimos que G es* ***divisible.***

Ejemplo 2.2.2. *[8, pág. 50] Dado un número primo p, $\mathbb{Z}(p^\infty)$ es divisible. Para ver esto tomemos un entero positivo $n > 1$ y probemos que $\mathbb{Z}(p^\infty) = n\mathbb{Z}(p^\infty)$. Por el Teorema Fundamental de la Aritmética $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, donde cada p_i es un número primo distinto y cada α_i es un entero mayor que uno, para todo $i \in \{1, 2, \cdots, k\}$. Por otro lado, sea $g = \frac{a}{p^m} + \mathbb{Z}$ con $mcd(a, p^m) = 1$. Si existe $i \in \{1, 2, \cdots, k\}$ tal que $p = p_i$, entonces consideremos el entero $\frac{n}{p}$. De esto se deduce que existen enteros c, d tales que $\frac{n}{p}c + dp^m = 1$, entonces*

$$\begin{aligned} g &= 1g \\ &= \left(\frac{n}{p}c + dp^m\right) g \\ &= n\left(c\frac{g}{p}\right) + d(p^m g) \\ &= n(cy). \end{aligned}$$

Donde $y = \frac{a}{p^{m+1}} + \mathbb{Z}$. *Si por el contrario* $p_i \neq p$, *para todo* $i \in \{1, 2, \cdots, k\}$, *entonces* $mcd(n, p^m) = 1$ *y un procedimiento análogo muestra que existe un entero* c *tal que* $g = n(cg)$. *Así hemos probado que* $\mathbb{Z}(p^\infty) \subseteq n\mathbb{Z}(p^\infty)$. *De forma rápida podemos comprobar que* $n\mathbb{Z}(p^\infty) \subseteq \mathbb{Z}(p^\infty)$. *Así* $\mathbb{Z}(p^\infty)$ *es divisible.*

Lema 2.2.4. *Si* G *es un grupo abeliano* p*-divisible, entonces* $p^nG = G$, *para todo* $n \in \mathbb{N}$.

Demostración. Utilicemos inducción para probar esto. Como G es p-divisible claramente $p^1G = G$. Ahora supongamos que $p^nG = G$ y veamos que $p^{n+1}G = G$. Por hipótesis de inducción $p^nG = G$, luego $p^{n+1}G = pG = G$. Así $p^{n+1}G = G$ y con esto damos por concluida la demostración.

□

Con el anterior lema es fácil ver que un grupo abeliano G es divisible si y solo si G es p-divisible para todo primo p. En efecto, si G es un grupo divisible, entonces claramente él es p- divisible para todo p. Recíprocamente, sea $n > 1$ un entero positivo. Por el *Teorema Fundamental de la Aritmética* $n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Como G es p- divisible para todo primo, en particular para cada p_i. Por otro lado, del *Lema 2.2.4* tenemos que $p_i^{\alpha_i}G = G$, para todo índice i. Luego

$$p_1^{\alpha_1}G = G \Rightarrow p_1^{\alpha_1}p_2^{\alpha_2}G = G \Rightarrow \cdots \Rightarrow p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k}G = G.$$

Así G es divisible.

Proposición 2.2.2. *Sea* G *un grupo abeliano, entonces* G *es divisible o existe* $K \trianglelefteq G$ *tal que* $G/K \simeq \mathbb{Z}_p$, *para algún primo* p.

Demostración. Supongamos que G es un grupo abeliano que no es divisible y mostremos la existencia de $K \trianglelefteq G$. Como G no es divisible tenemos que para algún número primo p, G no es p-divisible, de ello que $pG \subsetneq G$. Ahora dotemos a G/pG de estructura de espacio vectorial sobre $\mathbb{Z}_p$. Para esto consideremos la función

$$\begin{aligned} \bullet : \mathbb{Z}_p \times G/pG &\to G/pG \\ (\bar{x}, g + pG) &\longmapsto xg + pG \end{aligned}$$

Entonces $\bullet$ está bien definida. En efecto, supongamos que $(\bar{x}, g + pG) = (\bar{y}, h + pG)$, entonces $x \equiv y(mod\ \text{p})$ y $g - h \in pG$, de ello que $x(g - h) \in pG$, luego $x(g - h) = xg - xh = xg - yh \in pG$, es decir $xg + pG = yh + pG$.
Consideremos ahora una base $\beta = \{\beta_i\}_{i \in I}$ del espacio vectorial G/pG y $x \in G/pG$, luego $x = \sum_{i \in I}(\beta_i)(\alpha_i)$ donde $\alpha_i \in \mathbb{Z}_p$, para todo $i \in I$. Fijemos un índice $i_0 \in I$

y tomemos la función $\varphi_p : G/pG \to \mathbb{Z}_p$ definida por $\varphi_p(x) = \alpha_{i_0}$. Veamos primero que la función está bien definida. Sean $x, y \in G/pG$ tales que $x = y$ entonces x y y tienen la misma combinación lineal. De ello que $\varphi_p(x) = \varphi_p(y)$. Probemos ahora que la función es sobreyectiva. Para esto tomemos $\alpha \in \mathbb{Z}_p$ y consideremos cualquier vector $x \in G/pG$ tal que en la posición i_0 de su combinación lineal esta el escalar α; es decír, $x = \sum_{i\in I}(\beta_i)(\alpha_i)$ donde $\alpha_{i_0} = \alpha$. Entonces $\varphi_p(x) = \alpha$. Luego de esto consideremos la proyección

$$\pi : G \to G/pG.$$

entonces $\varphi_p \circ \pi : G \to \mathbb{Z}_p$ es un epimorfismo. Si K es el kernel de $\varphi_p \circ \pi$, del *Primer Teorema de Isomorfismo* se sigue que $G/K \simeq \mathbb{Z}_p$. Con esto damos por concluida la prueba.

□

Observación 2.2.3. *Como $\mathbb{Z}_p$ no tiene subgrupos propios, por el Teorema 1.3.4 tenemos que los únicos subgrupos de G que contienen a K son G y K, esto nos dice que K es el subgrupo más grande en el sentido que no existe otro subgrupo que lo contenga salvo G y él mismo.*

Ahora tomemos una familia de grupos abelianos $\{G_i\}_{i\in I}$ y consideremos el conjunto $\prod_{i\in I} G_i := \{(g_i)_{i\in I} : g_i \in G_i\}$. Dados $(g_i)_{i\in I}, (h_i)_{i\in I} \in \prod_{i\in I} G_i$, definimos la suma $(g_i)_{i\in I} + (h_i)_{i\in I} = (g_i + h_i)_{i\in I}$. Entonces esta suma da estructura de grupo a $\prod_{i\in I} G_i$. Antes de enunciar un importante teorema sobre grupos abelianos damos la siguiente definición. La prueba del resultado mencionado es omitida en este trabajo por las razones descritas al principio del capítulo.

Definición 2.2.3. *Dada una familia de grupos $\{G_i\}_{i\in I}$ se define la suma directa de los G_i como el subgrupo de $\prod_{i\in I} G_i$ definido y denotado por:*

$$\bigoplus_{i\in I} G_i := \{(g_i)_{i\in I} \in \prod_{i\in I} G_i : g_i \neq 0 \text{ para un número finito de índices}\}.$$

Teorema 2.2.1. *(Teorema de Estructura de Grupos Abelianos Divisibles) [13, pág. 6] Sea G un grupo abeliano. Entonces G es divisible si y solo si existe una familia de grupos abelianos $\{G_i\}_{i\in I}$ tal que:*

i) Para todo $i \in I$, $G_i = \mathbb{Q}$ o $G_i = \mathbb{Z}(p^\infty)$, para algún primo p.

ii) $G \simeq \bigoplus_{i\in I} G_i$.

Consideremos ahora un número primo p, entonces de la *Proposición 2.2.1* todo elemento de $\mathbb{Z}(p^\infty)$ tiene orden finito. En general los grupos donde todo elemento tiene orden finito son llamados de **torsión**. Siendo más precisos tenemos la siguiente definición

Definición 2.2.4. *Un grupo abeliano G es llamado **de torsión** si todo elemento de G tiene orden finito. Por el contrario, si ningún elemento diferente del neutro tiene orden finito se dirá que G es **libre de torsión**.*

Queremos recordar un par de resultados que serán necesarios en el siguiente capítulo. Para ello se introduce la siguiente definición.

Definición 2.2.5. *Dado un grupo abeliano G y un número primo p se define el **componente p-primario** G_p de G como el subgrupo de todos los elementos que tienen orden una potencia de p.*

La demostración del siguiente hecho puede ser consultada en [6, pág. 30-32]

Teorema 2.2.2. *Sean G y H grupos abelianos.*

i) Si G es de torsión, entonces G es suma directa de sus componentes p-primarios, esto es $G = \bigoplus_p G_p$.

ii) Si $G \simeq H$, entonces $G_p \simeq H_p$ para todo primo p.

Terminamos esta sección enunciando la siguiente proposición. Para ello debemos recordar el *Ejemplo 1.3.1*. Cabe aclarar que dicho resultado se sigue de la prueba de un teorema más general, el cual puede ser consultado en [15, pág. 143-144].

Proposición 2.2.3. *Suponga que G es un grupo no abeliano tal que todo subgrupo de G es normal, entonces existe un grupo abeliano de torsión P que no tiene elementos de orden 4 tal que $G \simeq Q_8 \times P$.*

2.3. Sobre la propiedad (D)

Ya en esta etapa del trabajo se han recolectado una considerable cantidad de conceptos previos que serán utilizados a lo largo de esta sección para obtener una caracterización de todos los **grupos cuyos subgrupos tienen distinto cardinal**. Es aquí donde se van a exhibir y estudiar los resultados principales de este trabajo, que corresponden a una publicación hecha por el matemático ***Greg Oman***, la cual puede ser consultada

en [13]. Estos resultados serán demostrados con el mayor detalle posible ya que es de nuestro interés dejar clara la esencia de la propiedad estudiada. Paralelamente a esto se darán algunas proposiciones relacionadas con dicha propiedad, con su respectiva demostración.

Definimos a continuación la propiedad que inspira este trabajo.

Definición 2.3.1. *Decimos que un grupo G satisface la* ***Propiedad (D)*** *si distintos subgrupos de G tienen distinto cardinal.*

Observación 2.3.1. *Siempre que se quiera verificar que un grupo G posee la* ***Propiedad (D)*** *basta examinar la siguiente implicación:*

$$\textit{Dados } H, K \leq G\textit{; si } H \neq K\textit{, entonces } |H| \neq |K|.$$

O equivalentemente

$$\textit{Si } |H| = |K|\textit{, entonces } H = K.$$

Ejemplo 2.3.1. *Consideremos el grupo cíclico $\mathbb{Z}_6$. Tomemos los subgrupos $\langle 2\rangle$, $\langle 3\rangle$ y $\langle 4\rangle$. Note que $\langle 2\rangle \neq \langle 3\rangle$, más aún $|\langle 2\rangle| \neq |\langle 3\rangle|$. Además de lo anterior se puede observar que $|\langle 2\rangle| = |\langle 4\rangle|$ y una rápida verificación nos revela que $\langle 2\rangle = \langle 4\rangle$. Note que los únicos subgrupos propios de $\mathbb{Z}_6$ son $\langle 2\rangle$ y $\langle 3\rangle$, por esto es suficiente considerar solo estos subgrupos. ([7, pág. 68])*

Ejemplo 2.3.2. *Sea $\mathbb{R}$ el grupo aditivo de los números reales y pensemos en $\mathbb{Q}$ y $\mathbb{Z}$ como subgrupos. Como se vio en el capítulo uno $\mathbb{Q} \cong \mathbb{N}$ y siguiendo esta idea puede demostrarse que $\mathbb{Q} \cong \mathbb{Z}$. De esto deducimos que $|\mathbb{Q}| = |\mathbb{Z}|$. Por otro lado es claro que $\mathbb{Q} \neq \mathbb{Z}$, luego $\mathbb{R}$ no satisface la Propiedad (D).*

Ejemplo 2.3.3. *Nuevamente tome el grupo de permutaciones S_3 y considere los mismos subgrupos del Ejemplo 2.1.2. Note lo siguiente: $|\langle(12)\rangle| = |\langle(13)\rangle| = |\langle(23)\rangle|$. Además de esto una rápida verificación nos garantiza que $\langle(12)\rangle \neq \langle(13)\rangle \neq \langle(23)\rangle$. Por lo tanto, S_3 no satisface la Propiedad (D).*

Como vimos en los ejemplos anteriores hay grupos que verifican la *Propiedad (D)* y otros que no. Adicionalmente a esto también se puede percibir que el único grupo que satisfacía la propiedad era cíclico. Estas observaciones proponen el siguiente resultado.

Teorema 2.3.1. *[13, pág. 2.]*
Sea G un grupo cíclico finito, entonces G goza de la Propiedad (D).

Demostración. Probemos que G satisface la *Propiedad (D)*. Por hipótesis, como G es cíclico existe $g \in G$ talque $G = \langle g \rangle$. Ahora supongamos que $|G| = n$ y sean H, K subgrupos de G tales que $|H| = |K|$. Veamos que $H = K$. Como H es un subgrupo de un grupo cíclico, de ello que exista g^k tal que $H = \langle g^k \rangle$, dónde $0 \leq k < n$. Análogamente tenemos que existe g^m tal que $K = \langle g^m \rangle$ y $0 \leq m < n$. Por 2) de la *Proposición 1.3.3* tenemos que $\langle g^k \rangle = \langle g^{d_1} \rangle$ y $\langle g^m \rangle = \langle g^{d_2} \rangle$, siendo $d_1 = mcd(n, k)$ y $d_2 = mcd(n, m)$. Se sigue de la prueba de la *Proposición 2.1.1* que $|H| = |\langle g^{d_1} \rangle| = \frac{n}{d_1} = |K| = |\langle g^{d_2} \rangle| = \frac{n}{d_2}$. Se concluye de esto que $d_1 = d_2$ y así $H = K$.

□

El anterior teorema es uno de los principales resultados que se quieren exhibir en este trabajo. El siguiente ejemplo muestra la importancia de que el grupo sea finito.

Ejemplo 2.3.4. *El grupo aditivo $\mathbb{Z}$ es cíclico. Ahora tome $\langle 2 \rangle$ y $\langle 4 \rangle$. Note que $|\langle 2 \rangle| = |\langle 4 \rangle|$, pero $\langle 2 \rangle \neq \langle 4 \rangle$.*

Nuestra intención es dar condiciones al grupo para que se pueda dar el recíproco del teorema anterior. Para ello damos una sencilla prueba de la siguiente proposición que será de ayuda para tal fin.

Proposición 2.3.1. *Sea G un grupo que satisface la Propiedad (D), entonces todo subgrupo de G es normal.*

Demostración. Para demostrar esto tomemos $g \in G$ y $H \leq G$. Por el *Ejemplo* 1,3,3 tenemos que $gHg^{-1} \leq G$. Además de esto si consideramos la función biyectiva $\varphi : H \to gHg^{-1}$ definida por $\varphi(h) = ghg^{-1}$ podemos concluir que $|H| = |gHg^{-1}|$. Como G satisface la *Propiedad (D)* se sigue que $H = gHg^{-1}$ y con esto hemos probado que $H \trianglelefteq G$.

□

Enseguida enunciamos y probamos nuestro segundo teorema principal.

Teorema 2.3.2. *[13, pág. 3.]*

Si G es un grupo finito que satisface la Propiedad (D), entonces G es cíclico.

Demostración. Consideremos un grupo finito G tal que $|G| = n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$, donde $n > 1$ que satisface la *Propiedad (D)*. Por la proposición anterior tenemos que todo subgrupo de G es normal; en particular todo p_i- subgrupo de Sylow de G es normal, donde $i \in I_k$. Si H_i es un p_i- subgrupo de Sylow, entonces de la *Proposición 2.1.3* se sigue que H_i es único, para cada $i \in I_k$. De la *Proposición 2.1.4* se sigue

que $G \simeq H_1 \times H_2 \times \cdots \times H_k$. Probemos ahora que cada H_i es cíclico. Por simplicidad tomemos H_1 y supongamos que él no es cíclico. Como H_1 no es cíclico, de la *Proposición 1.3.2* H_1 es unión de subgrupos propios; es decír, si $\{K_j\}_{j=1}^m$ es la familia de subgrupos propios de H_1, entonces $H_1 = \bigcup_{j=1}^m K_j$. Por otro lado, del *Teorema de Lagrange* se sigue que para todo $j \in I_m$, $|K_j| = p_i^r$, donde $1 \leq r \leq \alpha_1$. Como G tiene la *Propiedad (D)*, H_1 también satisface esta propiedad. De esto se sigue que para cada j, con $0 \leq j \leq \alpha_1$ H_1 tiene un único subgrupo de orden p_1^j. Ahora considere lo siguiente:

$$|H_1| = |\bigcup_{j=1}^m K_j| \leq 1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1 - 1} = \frac{p_1^{\alpha_1}-1}{P_1-1} < p_1^{\alpha_1} = |H_1|.$$

Esto claramente es una contradicción que se generó al asumir que H_1 no es cíclico. Un procedimiento análogo muestra que para cada $i \in I_k$, H_i es cíclico. Finalmente de la *Proposición 1.3.1*, *Ejemplo 1.3.14* y del *Teorema Chino de los Restos* se sigue que:

$$G \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \mathbb{Z}_{p_3^{\alpha_3}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} \simeq \mathbb{Z}_{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}} = \mathbb{Z}_{|G|}.$$

Luego G es cíclico.

□

Combinando el *Teorema 2.3.1* y el *Teorema 2.3.2* tenemos que

Un grupo finito G satisface la *Propiedad (D)* si y solo si G es cíclico.

Esto nos da una respuesta parcial a nuestra pregunta. Veamos ahora como se comporta el *Grupo de Prüfer* con la *Propiedad (D)*.

Teorema 2.3.3. *[13, pág. 5]*

Dado un número primo p entonces el grupo de Prüfer $\mathbb{Z}(p^\infty)$ goza de la Propiedad (D).

Demostración. Veamos que $\mathbb{Z}(p^\infty)$ satisface la *Propiedad (D)*. Sean H, K subgrupos de G de igual cardinalidad. Por la *Proposición 2.2.1* podemos suponer sin pérdida de generalidad que $H \subseteq K$. Por un lado, si K es finito, entonces como $|H| = |K|$ se deduce que $H = K$. Ahora, si K es infinito tenemos que $K = \mathbb{Z}(p^\infty)$ pues de no ser así tendríamos una contradicción. Nuevamente, como $|H| = |K|$ concluimos que $H = K = \mathbb{Z}(p^\infty)$.

□

El siguiente resultado da una primera caracterización de la *Propiedad (D)* para grupos abelianos.

Teorema 2.3.4. *[13, pág. 6]*

Sea G un grupo abeliano, entonces G satisface la Propiedad (D) si y solo si G es un grupo cíclico finito o $G = \mathbb{Z}(p^\infty)$, para algún número primo p.

Demostración. Primero supongamos que G es un grupo cíclico finito. Por el *Teorema 2.3.1* se tiene que G verifica la *Propiedad (D)*. Si $G = \mathbb{Z}(p^\infty)$ para algún primo p, entonces del *Teorema 2.3.3* se sigue que G goza de la *Propiedad (D)*.
Recíprocamente, sea G un grupo abeliano que satisface la *Propiedad (D)*. Si G es finito, por el *Teorema 2.3.2* se garantiza que él es cíclico. Supongamos ahora que G es infinito. Afirmamos que G es divisible, pues en caso de no serlo por la *Proposición 2.2.2* tenemos que existe un número primo p y $N \trianglelefteq G$ tal que $G/N \simeq \mathbb{Z}_p$. Además de esto note que N es un subgrupo infinito ya que de no ser así tendríamos que $G = \bigcup_{i=1}^{p}(N + g_i)$; es decír, un conjunto infinito es igual a una unión finita de conjuntos finitos. Del *Teorema 1.1.5* se sigue lo siguiente

$$\begin{aligned} |G| &= |(N + g_1) \cup (N + g_2) \cup \cdots \cup (N + g_p)| \\ &= |N + g_1| + |N + g_2| + \cdots + |N + g_p| \\ &= |N| + (|N| + \cdots |N|) \\ &= |N| \end{aligned}$$

y esto es contradictorio, pues por hipótesis G satisface la *Propiedad (D)*. De todo el trabajo hecho anteriormente se deduce que G es divisible. Por el *Teorema 2.2.1* tenemos que $G \simeq \bigoplus_{i\in I} G_i$, donde para cada $i \in I$, $G_i = \mathbb{Q}$ o $G_i = \mathbb{Z}(p^\infty)$, para algún primo p. veamos que $|I| = 1$. Si $|I| \neq 1$ entonces basta con borrar un sumando de $\bigoplus_{i\in I} G_i$ y obtendremos con esto un sugrupo propio H de G de igual cardinalidad que G y esto es contradictorio ya que G satisface la *Propiedad (D)*. Finalmente $G \simeq \mathbb{Q}$ o $G \simeq \mathbb{Z}(p^\infty)$. Note que $\mathbb{Q}$ no satisface la *Propiedad (D)*, luego $G \simeq \mathbb{Z}(p^\infty)$ y con esto damos por terminada nuestra prueba.

□

Retomando todo lo que se ha hecho hasta ahora tenemos dos teoremas principales sobre la *Propiedad (D)* que nos hablan sobre grupos finitos, un resultado que relaciona los grupos de Prüfer con la *Propiedad (D)* y una caracterización para grupos abelianos. El siguiente resultado nos brinda la pieza restante para dar la caracterización que se estaba buscando.

Teorema 2.3.5. *[13, pág. 7]*

Todo grupo con la Propiedad (D) es abeliano.

Demostración. Supongamos que G es un grupo no abeliano. De la *Proposición 2.3.1* se tiene que todo subgrupo de G es normal. Por la *Proposición 2.2.3* se tiene que existe un grupo de torsión P sin elementos de orden cuatro tal que $G \simeq Q_8 \times P$, donde Q_8 es el grupo del **Ejemplo 1.3.1**. Note que cualquier subgrupo de G también satisface la *Propiedad(D)*, en particular Q_8 pero esto no es posible pues $H_1 = \{1, -1, i, -i\}$, $H_2 = \{1, -1, j, -j\}$ y $H_3 = \{1, -1, k, -k\}$ son tres subgrupos de orden cuatro. Con esto hemos demostrado que cualquier grupo que satisfaga la *Propiedad (D)* es abeliano. □

Esta última serie de teoremas son la respuesta a la pregunta planteada en la introducción de este trabajo y nos dice que **un grupo que satisfaga la Propiedad (D) necesariamente debe ser un grupo cíclico finito o un grupo de Prüfer, para algún primo** p.

Capítulo 3

Posibles generalizaciones

Es natural preguntarse si la propiedad estudiada en este escrito puede generalizarse en algún sentido. El objetivo de este capítulo es ver porque la propiedad en estudio no puede generalizarse en el sentido que un grupo G que satisfaga cierta propiedad P no necesariamente verifica la *Propiedad (D)*.

Definición 3.0.1. *Sea G un grupo. Entonces:*

1) *Decimos que G goza de la propiedad (L) Si los subgrupos de G estan totalmente ordenados bajo la inclusión de conjuntos.*

2) *Se dice que G tiene la propiedad (C) si todo subgrupo de G es característico en G, donde un subgrupo H de G se dice que es característico en G si $\varphi[H] = H$ para todo automorfismo φ sobre G.*

3) *Llamamos a G un grupo que satisface la propiedad (N) si todo subgrupo de G es normal en G.*

Ejemplo 3.0.1. *Dado un número primo p, de la Proposición 2.2.1 se sigue que $\mathbb{Z}(p^\infty)$ satisface la Propiedad (L). Todo grupo que satisfaga la Propiedad (D) también tiene la Propiedad (N). Además $\mathbb{Z}(p^\infty)$ verifica la Propiedad (C).*

Observación 3.0.1. *El hecho de que $\mathbb{Z}(p^\infty)$ tenga la Propiedad (C) es debido a que distintos subgrupos de $\mathbb{Q}/\mathbb{Z}$ no son isomorfos. A continuación se esboza una rápida demostración de este hecho. Supongamos dos subgrupos H, K de $\mathbb{Q}/\mathbb{Z}$ tales que $H \simeq K$ y probemos que $H = K$. Para esto veamos primero que H es de torsión. Sea $g \in H \subseteq \mathbb{Q}/\mathbb{Z}$, de ello que exista $\frac{a}{b} \in \mathbb{Q}$, con $b \neq 0$ tal que $g = \frac{a}{b} + \mathbb{Z}$. Como en la demostración de la Proposición 2.2.1 se sigue que el orden de g es precisamente $|b|$ y con esto hemos*

probado que H es de torsión. Análogamente se tiene que K es un grupo de torsión. Por el Teorema 2.2.3 se tiene que $H = \bigoplus_p H_p$ y $K = \bigoplus_p K_p$, donde cada H_p y K_p son los componentes p-primarios de H y K respectivamente, para todo número primo p. Como $H \simeq K$, nuevamente, del Teorema 2.2.3 se garantiza que $H_p \simeq K_p$, para todo primo p. Por otro lado note que para todo número primo p, H_p y K_p son subgrupos de $\mathbb{Z}(p^\infty)$. Como $|H_p| = |K_p|$ entonces por la ***Propiedad (D)*** *concluimos que $H_p = K_p$, para todo p primo. De todo esto se garantiza que $H = K$.*

Proposición 3.0.1. *Sea G un grupo y considere las siguientes condiciones:*

1) G tiene la propiedad (L).

2) G tiene la propiedad (D).

3) G tiene la propiedad (C).

4) G tiene la propiedad (N).

entonces, $1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 4)$.

Demostración. Sea G un grupo.

$1) \Rightarrow 2)$ Veamos que G verifica la *Propiedad (D)*. Para ello probemos primero que todo subgrupo propio de G es finito. Sea $H \leq G$ y $x \in G \setminus H$. Por hipótesis $H \subseteq \langle x \rangle$ o $\langle x \rangle \subseteq H$. Es claro que $\langle x \rangle \nsubseteq H$. Además de esto note que $\langle x \rangle$ siempre es finito, pues de no ser así $\langle x \rangle \simeq \mathbb{Z}$ y esto sería contradictorio ya que $\mathbb{Z}$ no satisface la *Propiedad (L)*. De esto se sigue que H es finito. Por otro lado, sean $K, M \leq G$ tales que $|K| = |M|$. Sin pérdida de generalidad asumamos que $K \subseteq M$. Si M es un subgrupo propio, entonces él es finito y concluimos que $K = M$. Si M es trivial se verifica que $K = M = G$ o $K = M = \{e\}$. Así G goza de la *Propiedad (D)*.

$2) \Rightarrow 3)$ Asumamos que G es un grupo que tiene la *Propiedad (D)*. Si $\varphi : G \to G$ es un automorfismo y $H \leq G$, entonces $|H| = |\varphi(H)|$. Concluimos por hipótesis que $H = \varphi(H)$.

$3) \Rightarrow 4)$ Supongamos que G tiene la *Propiedad (C)*. Sea $H \leq G$ y $g \in G$. Consideremos ahora la función $\varphi : G \to G$ definida por $\varphi(x) = gxg^{-1}$. Entonces φ es un automorfismo. Por otro lado de la hipótesis se sigue $\varphi(H) = H$, de ello que $H = \varphi(H) = gHg^{-1}$. Así H es normal en G.

□

Veamos que el recíproco del anterior resultado no es cierto. Para ello considere el siguiente ejemplo.

Ejemplo 3.0.2. *Los siguientes grupos son claros contraejemplos.*

2) $\not\Rightarrow$ 1) $\mathbb{Z}_6$ *tiene la Propiedad (D) pero no satisface la Propiedad (L), pues no se tiene que* $\langle 2\rangle \subseteq \langle 3\rangle$ *o* $\langle 3\rangle \subseteq \langle 2\rangle$.

3) $\not\Rightarrow$ 2) *Sabemos que* $\mathbb{Q}/\mathbb{Z} = \bigoplus_p \mathbb{Z}(p^\infty)$ *([9] p.43). Tomemos* $G = \mathbb{Z}(2^\infty) \oplus \mathbb{Z}(3^\infty)$. *Note que* G *no satisface la Propiedad (D) pues de ser así, por el Teorema 2.3.4 existe un número primo* p *talque* $G = \mathbb{Z}(p^\infty)$ *y esto seria contradictorio. Por otro lado, de la Observación 3.0.1 tenemos que* G *verifica la Propiedad (C). En efecto, pues si se tiene un automorfismo* $\varphi : G \to G$ *y un subgrupo* H *de* G *tal que* $\varphi(H) \neq H$, *entonces* $\varphi(H) \simeq H$, *de lo cual concluimos que* $\varphi(H) = H$ *y esto contradice nuestra hipótesis.*

4) $\not\Rightarrow$ 3) *Sea* $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. *Note que* G *es abeliano y de esto* G *satisface la Propiedad (N). Una rápida verificación del subgrupo* $H = \mathbb{Z}_2 \times \{0\}$ *en el automorfismo* $\varphi : G \to G$ *definido por* $\varphi(x, y) = (y, x)$ *nos dice que* H *no es característico y con esto* G *no satisface la Propiedad (C) .*

Corolario 3.0.1. *Sea* G *un grupo infinito. Los siguientes enunciados son equivalentes:*

1) $G \simeq \mathbb{Z}(p^\infty)$, *para algún primo* p.

2) Los subgrupos de G *están linealmente ordenados bajo la inclusión de conjuntos.*

3) Distintos subgrupos de G *tienen distinto cardinal.*

Demostración. Dado un grupo un grupo infinito G, entonces

1) $\Rightarrow$ 2) Se sigue por 3) de la *Proposición 2.2.1.*

2) $\Rightarrow$ 3) Se garantiza por la *Proposición 3.0.1.*

3) $\Rightarrow$ 1) Utilizando el *Teorema 2.3.5* es inmediato.

□

Bibliografía

[1] AGUSTÍN-AQUINO, Octavio, *et al. Una Introducción a la Teoría de Grupos con Aplicaciones en la Teoría Matemática de la Música*. [En línea]. México: Sociedad Matemática Mexicana. 2009. (Recuperado el 8 marzo 2017). Disponible en http://www.pesmm.org.mx/Serie%20Textos_ archivos/T10.pdf

[2] ALMEIDA VELANDIA, Sandra Yaneth. *Grupos Cíclicos y Algunas Aplicaciones*. Trabajo de grado en Licenciatura en Matemáticas. Bucaramanga: Universidad Industrial de Santander. Facultad de ciencias. Escuela de Matemáticas, 2006. 67p.

[3] AZNAR, Enrique. *Historia del Concepto de Grupo*. [En línea]. (Recuperado en 13 febrero 2017). Disponible en http://www.ugr.es/∼ eaznar/concepto_ grupo.htm

[4] BARRERA MORA, Fernando. *Introducción a la Teoría de Grupos*. [En línea]. México: Sociedad Matemática Mexicana. (Recuperado en 3 marzo 2017). Disponible en http://www.pesmm.org.mx/Serie% 20Textos.htm

[5] BURTON, David. *Elementary Number Theory, Sixth Edition*. New York: Mc Graw Hill, 2007. 448p.

[6] CAÑAS PÉREZ, Andrés Sebastián. *Sobre Grupos Divisibles e Isomorfismos Relacionados*. Trabajo de grado en Matemáticas. Bucaramanga: Universidad Industrial de Santander. Facultad de ciencias. Escuela de Matemáticas, 2015. 53p.

[7] DUMMIT, David y FOOTE, Richard. *Abstract Algebra Third Edition*. USA: Jhon Wiley and Sons Inc, 2004. 932p.

[8] FRÍAS ARMENTA, Martín Eduardo. *Clasificación de grupos abelianos*. Trabajo de grado en Licenciatura en Matemáticas. Sonora: Universidad de Sonora. Departamento de Matemáticas, 1993. 87p.

[9] FUCHS, László. *Infinite Abelian Groups Volume I*. New York: Academic Press, 1970. p.43.

[10] GALLIAN, Joseph. *Contemporary Abstract Algebra Seventh Edition*. Belmont: Brooks/Cole, Cengage Learning, 2010. 646p.

[11] GAVIRIA LONDOÑO, Luz Marina. *De los Grupos y Cuerpos como "Herramientas" a "Objetos" Matemáticos*. Trabajo de grado en Licenciatura en Matemáticas. Santiago de Cali: Universidad del Valle. Instituto de Educación y Pedagogía, 2014. 116p.

[12] HUNGERFORD, Thomas. *Algebra*. New York: Springer-Verlag, 1974. 502p.

[13] OMAN, Greg. *Groups whose subgroups have distinct cardinalities*. En: Pi Mu Epsilon Journal, vol.14, no. 1, p.31-37.

[14] PINTER, Charles. *A Book of Set Theory*. New York: Dover Publications inc, 2014. 256p.

[15] ROBINSON, Derek. *A Course in the Theory of Groups, Second Edition*. New York: Springer, 2009. 499p.

[16] SANCHEZ FERNANDEZ, Carlos. y NORIEGA SANCHEZ, Teresita. *Abel el Romántico Nórdico*. Madrid: NIVOLA libros y ediciones, 2005. 224p.

[17] ZALDÍVAR, Felipe. *Introducción a la teoría de grupos*. México: Sociedad Matemática Mexicana, 2006. 255p.