UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

PRODUCTO TRENZADO DE GRUPOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

P R E S E N T A :

ALUMNO :
JUAN FLORES TORRES

DIRECTORA DE TESIS:
DRA. DIANA AVELLA ALAMINOS

CIUDAD UNIVERSITARIA, CD. MX., 2017

1. Datos del alumno

Flores Torres Juan

56 869448

Universidad Nacional Autónoma de México

Facultad de Ciencias

Matemáticas

305308805

2. Datos del tutor

Dra.

Diana Avella Alaminos

3. Datos del sinodal 1

Dr.

José Ríos Montes

3. Datos del sinodal 2

Dr.

Juan Morales Rodriguez

3. Datos del sinodal 3

Dr.

Alejandro Alvarado García

3. Datos del sinodal 4

M. en C.

José Cruz García Zagal

7. Datos del trabajo escrito

Producto Trenzado de Grupos

65 p

2017

Índice general

Introducción

Durante el curso de Álgebra Moderna 1 de la Facultad de Ciencias se introduce la operación entre grupos de producto directo y se estudian algunas de sus propiedades, en esta tesis retomamos esos conceptos del producto directo para poder estudiar las herramientas teóricas necesarias para construir el producto trenzado de grupos.

Durante el desarrollo de esta tesis encontramos una aplicación constante del producto trenzado al estudio de grupos finitos y específicamente en grupos de permutaciones. El objetivo principal de esta tesis es revisar la teoría relacionada con el producto trenzado de grupos y estudiar las herramientas teóricas necesarias para poder definirlo, con tal de generar un tratado básico en el cual se pueda apoyar quien esté interesado en aprender este tema.

En el capítulo 1 de preliminares revisamos muchos de los conceptos estudiados en la materia de Álgebra Moderna 1, con tal de señalar cuáles son las bases necesarias para poder empezar a estudiar el producto trenzado de grupos, estudiamos las propiedades de divisibilidad de los números enteros, el concepto de grupo y subgrupo, probamos el teorema de Lagrange, estudiamos los morfismos de grupos así como los teoremas de isomorfismo, el grupo cociente, algunos resultados básicos de acciones de grupos para poder probar el Teorema de Cauchy. Finalmente definimos el concepto de unidad en un anillo.

En el capítulo 2 definimos el grupo de automorfismos de un grupo cualquiera y el grupo de automorfismos internos, posteriormente verfificamos que es un subgrupo normal del grupo de automorfismos, finalmente definimos qué es un subgrupo característico y estudiamos algunas de sus propiedades importantes.

En la primera parte del capítulo 3 definimos el producto directo externo de grupos junto con algunos resultados ya conocidos de éste, en la segunda parte estudiamos el producto directo interno y verficamos que son conceptos equivalentes. Al final de este capítulo revisamos algunos resultados de productos directos de grupos cíclicos.

El capítulo 4 de producto semidirecto tiene una estructura similar a la del producto directo, en la primera parte estudiamos el producto semidirecto interno y luego señalamos las diferencias con el producto directo interno, en la segunda parte estudiamos el producto semidirecto externo y señalamos que un producto semidirecto interno induce un producto semidirecto externo y viceversa. Finalmente revisamos algunos resultados importantes del producto semidirecto.

En el capítulo 5 construimos el producto trenzado de grupos, que es un caso particular del producto semidirecto. Para definir un producto trenzado de grupos necesitamos tener un producto de copias de un grupo N, es decir $\prod N$ y un grupo H con los cuales hacemos un producto semidirecto de $\prod N$ con H. Tras haber construido el producto trenzado verificamos que podemos encajar un producto trenzado en un grupo de permutaciones y diremos a qué subgrupo de permutaciones es ismorfo ese prodcuto trenzado. Después definimos producto trenzado regular y damos un ejemplo de un producto trenzado importante, el Lampligther Group. Finalmente demostramos el teorema de Kaloujnine y utilizando este encontramos una

forma de calcular el p-subgrupo de Sylow de cualquier S_m.

A lo largo del trabajo incluimos las demostraciones de los resultados principales, de manera detallada y buscamos incluir ejemplos suficientes para entender mejor los conceptos a estudiar.

Capítulo 1

Preliminares

1.1. Números Enteros y Divisibilidad

En esta primera sección estudiaremos algunos conceptos útiles de divisibilidad en el conjunto $\mathbb{Z}$ con la operación de suma y producto. Empezaremos enunciando la propiedad de existencia del cociente y resto cuya prueba puede revisarse en [7].

Proposición 1.1. *Dados $m, n \in \mathbb{Z}$ existen enteros q y r, únicos, tales que*

$$n = mq + r,\ 0 \leq q < |m|.$$

Definición 1.2. *Sean $n, m \in \mathbb{Z}$ decimos que n divide a m si $n = mk$ para algún $k \in \mathbb{Z}$.*

Observación 1.3. *En términos de la proposición 1.1 es fácil darnos cuenta que n divide a m si y sólo si $r = 0$.*

Definición 1.4. *Un entero n es múltiplo de un entero m si m divide a n. Y al conjunto de los múltiplos de m lo denotamos $(m) = \{n \in \mathbb{Z} | n = mk, k \in \mathbb{Z}\}$*

Observación 1.5. *Para $n, m \in \mathbb{Z}$ es fácil verificar que las siguientes propiedades son equivalentes.*

1. *n es múltiplo de m.*
2. *m divide a n.*
3. *$n \in (m)$.*
4. *$(n) \subseteq (m)$.*

Observación 1.6. *Dados $n, m \in \mathbb{Z}$ es fácil darse cuenta que $(n) = (m)$ si y sólo si $m = n$ ó $m = -n$. Y si $n > 0$ entonces n es el menor entero positivo en (n).*

Proposición 1.7. *Para cualquier entero n se cumple que*

1. *$0 \in (n)$.*
2. *Si $a, b \in (n)$, entonces $a + b \in (n)$.*
3. *Si $z \in \mathbb{Z}$ y $a \in (n)$, entonces $az \in (n)$.*

Demostración. 1.- $0 = n0$ para cualquier $n \in \mathbb{Z}$. 2.- Si $a, b \in (n)$ entonces $a = nk$ y $b = nk'$ para algunas $k, k' \in \mathbb{Z}$ entonces $a + b = n(k + k') \in (n)$. 3.- Si $a \in (n)$ entonces $a = nk$ para alguna $k \in \mathbb{Z}$ y $az = nkz \in (n)$.

□

De la proposición anterior podemos concluir que $(n) \neq \emptyset$ pues $0 \in (n)$.

Definición 1.8. *Sea $I \subset \mathbb{Z}$ decimos que I es un ideal de $\mathbb{Z}$ si cumple que:*

1.- $0 \in I$.

2.- Si $a, b \in I$, entonces $a + b \in I$.

3.- Si $z \in \mathbb{Z}$ y $a \in I$, entonces $az \in I$.

Ejemplo 1.9. *Paca cualquier $m \in \mathbb{Z}$ tenemos que (m) es un ideal de $\mathbb{Z}$, como ya verificamos en la proposición 1.7*

Proposición 1.10. *Sea I un ideal de $\mathbb{Z}$. Existe un único entero $m \geq 0$ tal que $I = (m)$. Además, si $I \neq \{0\}$ entonces m es el menor entero positivo en I.*

Demostración. Si $I = \{0\}$, entonces $I = (0)$. Supongamos que $I \neq \{0\}$, notemos que si $0 \neq a \in I$ entonces $-1a = a \in I$ esto implica que hay enteros positivos en I, utilizando el principio del buen orden, consideramos m el menor de los enteros positivos en I, veamos que $(m) = I$. Como $m \in I$ entonces evidentemente $(m) \subset I$ por la condición 3 de la definición de ideal. Sea $a \in I$ por la Proposición 1.1 entonces $a = mq + r$ con $q, r \in \mathbb{Z}$ y $0 \leq r < m$ y por lo tanto $r = a - mq \in I$ pues $a, mq \in I$ y r es positivo pero como m es el menor entero positivo en I entonces $r = 0$ y por lo tanto $a \in (m)$ y $I = (m)$ ó $I = \{0\}$. □

Definición 1.11. *Dados 2 números enteros $n, m \in \mathbb{Z}$ distintos de cero, un máximo común divisor de n y m es un entero d que cumple que:*

1. *d divide a n y a m.*
2. *Si c es un entero tal que c divide a n y a m entonces c divide a d.*

Notación 1.12. *A un máximo comun divisor d de 2 enteros $n, m \in \mathbb{Z}$ lo denotamos $d = (n, m)$*

Observación 1.13. *Si tenemos d y d' dos máximos comunes dvisores de dos enteros n y m entonces $d = d'$ ó $d = -d'$, pues por la condición 2 de máximo común divisor d divide a d' y d' divide a d, lo cual implica que $d' = dk$ y $d = d'k'$, entonces $d' = d'k'k$. Así $kk' = 1$ y por lo tanto $1 = k = k'$ ó $-1 = k = k'$ de donde se concluye que $d = d'$ ó $d = -d'$. De aqui en adelante el máximo comun divisor de dos números enteros, sera el número entero mayor que cero que cumpla con las condiciones 1 y 2 de la Definición 1.11.*

Teorema 1.14. *Para dos enteros cualesquiera $n, m \in \mathbb{Z}$ se tiene que:*

1. *Existe el máximo común divisor de m y n.*
2. *Existen $s, t \in \mathbb{Z}$ tales que $d = sn + tm$.*

Demostración. Para $n, m \in \mathbb{Z}$ definimos el conjunto $S(n,m) = \{sn + tm | s, t \in \mathbb{Z}\}$ es fácil verificar que $S(n,m)$ es un ideal de $\mathbb{Z}$, por lo tanto existe un entero $d \in S(n,m)$, tal que $d \geq 0$ y que $S(n,m) = (d)$, lo cual implica que existen enteros $k, k' \in \mathbb{Z}$ tales que $d = kn + k'm$. Afirmamos que $d = (n,m)$, pues como $n, m \in S(n,m) = (d)$ entonces se tiene que d divide a n y a m y si c es un entero que divide a n y m entonces divide a $kn + k'm$ y por lo tanto divide a d. Con lo cual concluimos que $d = (n,m)$.

□

Definición 1.15. *Sean $n, m \in \mathbb{Z}$ decimos que m y n son primos relativos si $(m,n) = 1$.*

Notemos que con el teorema 1.14 podemos concluir que si n y m son primos relativos entonces existen $s, t \in \mathbb{Z}$ tales que $1 = sn + tm$.

Definición 1.16. *Sean $a, b \in \mathbb{Z}$ decimos que a y b son congruentes módulo n si n divide a $a - b$, y escribimos $a \equiv b \ mod \ n$.*

Definición 1.17. *Sea $p \in \mathbb{Z}$ tal que $p > 1$ decimos que p es un número primo si los únicos enteros positivos que lo dividen son 1 y p.*

Para terminar esta sección introduciremos el concepto de congruencia de números enteros y enunciaremos el teorema fundamental de la aritmética del cual omitiremos la prueba pues no es la finalidad de este trabajo profundizar en esta área, el lector interesado puede consultar en [8].

Teorema 1.18. ***Teorema Fundamental de la Aritmética.*** *Para cualquier $n \in \mathbb{Z}$ tal que $n > 1$, n puede escribirse de manera única, salvo el orden, como un producto de números primos.*

1.2. Grupos y Subgrupos

Definición 1.19. *Sea G un conjunto distinto del vacío con una operación $\circledast$ definida en él, decimos que G es un grupo si cumple:*

1. *$\forall a, b \in G$ se cumple que $a \circledast b \in G$ (cerradura).*
2. *$\forall a, b, c \in G$ se cumple que $a \circledast (b \circledast c) = (a \circledast b) \circledast c$ (asociatividad).*
3. *$\exists e \in G$ tal que $\forall a \in G$ se cumple que $a \circledast e = a = e \circledast a$ (existencia del neutro).*
4. *$\forall a \in G \ \exists b \in G$ tal que $a \circledast b = e = b \circledast a$ (existencia del inverso).*

Notación 1.20. *A lo largo de esta tesis cuando trabajemos con un grupo en abstracto y su operación utilizaremos siempre la notación multiplicativa y le llamaremos producto aunque no tenga nada que ver con el producto de números reales. Por ejemplo, si tenemos elementos $a, b, c \in G$ entonces podemos escribir $a(bc) = (ab)c$.*

Ahora revisemos algunos ejemplos de grupos.

Ejemplo 1.21. *$\mathbb{Z}$ el conjunto de números enteros con la operación de suma es un grupo.*

Ejemplo 1.22. *Sea n un entero positivo definimos $n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$, este conjunto con la operación de suma resulta ser un grupo.*

Ejemplo 1.23. *El conjunto de los números racionales* $\mathbb{Q} = \{a/b | a, b \in \mathbb{Z},\ b \neq 0\}$ *es un grupo con la operación de suma de números racionales y si consideramos* $\mathbb{Q} - \{0\}$ *éste resulta ser un grupo con la operación de producto de números racionales.*

Ejemplo 1.24. *El conjunto de los números reales* $\mathbb{R}$ *es un grupo con la operación de suma y* $\mathbb{R} - \{0\}$ *también lo es con la operación de producto de números reales.*

Ejemplo 1.25. *El conjunto de los números complejos* $\mathbb{C} = \{a + ib | i^2 = -1 \text{ y } a, b \in \mathbb{R}\}$ *es un grupo con la operación de suma y* $\mathbb{C} - \{0\}$ *también lo es con la operación de producto de números complejos.*

Definición 1.26. *Un grupo* G *es finito si consta de un número finito de elementos, el número de elementos se llama orden de* G *y se denota por* $|G|$.

Ejemplo 1.27. *Sea* $\mathbb{K} = \{1, a, b, ab\}$ *donde* $a^2 = 1 = b^2$ *y* $ab = ba$, $\mathbb{K}$ *tiene estructura de grupo y cada elemento es su propio inverso. Este grupo es conocido como el grupo de Klein.*

A lo largo de este trabajo encontraremos muchos ejemplos de grupos finitos que irán surgiendo conforme avancemos.

Definición 1.28. *Un grupo* G *se dice que es abeliano si* $\forall a, b \in G$ *se cumple que* $ab = ba$, *en este caso decimos que los elementos* a *y* b *conmutan.*

Fácilmente nos podemos dar cuenta de que todos los ejemplos que hemos mencionado hasta el momento son de grupos abelianos, así que veamos un ejemplo de un grupo que no sea abeliano.

Ejemplo 1.29. *Sea* A *un conjunto y consideramos el conjunto de todas las funciones biyectivas de* A *en s mismo con la operación de composición. Más adelante se verifica que este conjunto tiene estructura de grupo, pero en general no es un grupo abeliano pues la composición de funciones no siempre es conmutativa.*

Lema 1.30. *Si* G *es un grupo, se cumplen las siguientes propiedades.*

1. El elemento neutro es único.

2. Para cualquier $a \in G$, a^{-1} *es único.*

Para cualquier $a \in G$ $(a^{-1})^{-1} = a$. *Al elemento neutro lo denotaremos por* $1 = e$ *y si* $a \in G$ *entonces al inverso de* a *lo denotaremos por* a^{-1}, *de tal manera que* $aa^{-1} = 1$.

4. Si $a, b \in G$ *entonces* $(ab)^{-1} = b^{-1}a^{-1}$.

5. Si $a, b, c \in G$ *y* $ab = ac$ *entonces* $b = c$.

Definición 1.31. *Sea* H *un subconjunto no vacío de un grupo* G. *Decimos que* H *es un subgrupo de* G *si* H *es un grupo con las operaciones de* G *restringidas a* H.

Notación 1.32. *Cada que tengamos que* H *es subgrupo de* G *lo denotaremos así* $H \leq G$.

El siguiente lema nos dará una manera rápida de saber cuándo un subconjunto de un grupo es un subgrupo.

Lema 1.33. *Sea* G *un grupo y* A *un subconjunto de* G, A *es un subgrupo de* G *si es cerrado bajo la operación de* G *y dado* $a \in A$ *entonces* $a^{-1} \in A$

Observación 1.34. *El Lema 1.33 nos permite concluir que el neutro de* G *pertenece a* H *pues si tenemos* $a \in H$ *entonces* $1 = aa^{-1} \in H$.

A continuación revisaremos algunos ejemplos de subgrupos.

Ejemplo 1.35. *Anteriormente mencionamos los ejemplos $\mathbb{Z}$ y $n\mathbb{Z}$, notemos que $n\mathbb{Z} \subseteq \mathbb{Z}$ y dados $nk, nk' \in n\mathbb{Z}$ con $k, k' \in \mathbb{Z}$ se cumple que $nk + nk' = n(k + k')$ lo cual muestra que $n\mathbb{Z}$ es cerrado bajo la operación de $\mathbb{Z}$ y si $nk \in n\mathbb{Z}$ con $k \in \mathbb{Z}$ entonces $-nk \in n\mathbb{Z}$ con lo cual verificamos que $n\mathbb{Z} \leq \mathbb{Z}$*

Ejemplo 1.36. *Consideremos $z \in \mathbb{C} - \{0\}$ tenemos que $z = a + ib$ para $a, b \in \mathbb{R}$ definimos $|z| = a^2 + b^2$ y lo llamamos la norma de z. Ahora consideremos el siguiente conjunto, $\mathbb{S}_1 = \{z \in \mathbb{C} || z| = 1\}$, como ya vimos anteriormente $\mathbb{C} - \{0\}$ es un grupo con la operación de producto y es fácil verificar que $\mathbb{S}_1 \leq \mathbb{C}$.*

Ejemplo 1.37. *Cualquier grupo G tiene 2 subgrupos inmediatos que son G y $\{1\}$ a éstos se les llama subgrupos triviales de G.*

Ejemplo 1.38. *Sea G un grupo y $a \in G$, consideramos el subconjunto A de G, $A = \{a^i | i \in \mathbb{Z}\}$, A es un subgrupo de G y a este subgrupo lo llamamos el subgrupo cíclico de G generado por a y lo denotamos $\langle a \rangle$.*

Ejemplo 1.39. *Sea G un grupo y $a \in G$, definimos el subconjunto de G,*

$$C(a) = \{g \in G | ga = ag\}$$

formado por todos los elementos de G que conmutan con a, éste resulta ser un subgrupo de G y se le llama el centralizador de a en G.

Ejemplo 1.40. *Si tenemos un grupo G definimos el centro de G como*

$$Z(G) = \{g \in G | gx = xg \ \forall x \in G\}$$

$Z(G)$ es un subgrupo de G, si G es abeliano entonces $Z(G) = G$.

Ejemplo 1.41. *Los grupos $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ cunplen la siguiente relación $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$ con la operación de suma de número reales.*

1.3. Teorema de Lagrange

El teorema de Lagrange es un resultado muy importante en el estudio de grupos finitos, para llegar a él recordemos algunas propiedades de relaciones de equivalencia.

Definición 1.42. *Una relación $\sim$ en un conjunto A es una relación de equivalencia si satisface:*

1. *$\forall a \in A \ a \sim a$. Reflexividad*
2. *$\forall a, b \in A$, si $a \sim b$ entonces $b \sim a$. Simetría.*
3. *$\forall a, b, c \in A$ si $a \sim b$ y $b \sim c$ entonces $a \sim c$. Transitividad.*

Ejemplo 1.43. *Sean, $a, b \in \mathbb{Z}$. Definimos la relación $a \sim b$ si $n/(b - a)$ para $n \in \mathbb{Z}$ fijo. Ésta es una relación de equivalencia en $\mathbb{Z}$, ya que $\forall a \in \mathbb{Z}$, $a - a = 0$ y $n/0$ entonces $a \sim a$, ahora $\forall a, b \in \mathbb{Z}$ si $n/(a - b)$ esto implica que $a - b = nk$ y entonces $b - a = -nk$ lo cual implica que $n/(b - a)$ por lo tanto tenemos que si $a \sim b$ entonces $b \sim a$, por último $\forall a, b, c \in \mathbb{Z}$ si tenemos que $a \sim b$ y $b \sim c$ entonces $nk = a - b$ y $nk' = b - c$ sumando ambas expresiones tenemos*

$(k+k')n = a-c$ y por lo tanto $n/(a-c)$ y entonces $a \sim c$ y por lo tanto tenemos que $\sim$ como está definida anteriormente es una relación de equivalencia. En términos de la definición 1.16, tenemos que la congruencia de números enteros módulo n es una relación de equivalencia.

Ejemplo 1.44. *Sea G cualquier grupo y $H \leq G$, si tenemos $a, b \in G$ decimos que $a \sim b$ si $ab^{-1} \in H$, ésta es una relación de equivalencia, es reflexiva pues si tenemos $a \in G$ entonces $aa^1 = 1 \in H$ y por lo tanto $a \sim a$, es simétrica ya que si $a, b \in G$ y $a \sim b$ entonces $ab^{-1} \in H$ y como H es un subgrupo de G entonces $(ab^{-1})^{-1} \in H$ pero $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$ y por lo tanto $b \sim a$, por último es transitiva pues para $a, b, c \in G$ supongamos que $a \sim b$ y $b \sim c$ esto implica que $ab^{-1} \in H$ y $bc^{-1} \in H$ consideramos el producto $ab^{-1}bc^{-1} = ac^{-1}$ y por la cerradura de H entonces $ac^{-1} \in H$ y por lo tanto $a \sim c$. Por lo tanto $\sim$ es una relación de equivalencia.*

Definición 1.45. *Si $\sim$ es una relación de equivalencia en A entonces se define la clase de $a \in A$ como*

$$[a] = \{b \in A | b \sim a\}$$

.

Ejemplo 1.46. *Revisemos las clases de equivalencia del Ejemplo 1.44, consideremos $a, b \in G$ y $a \sim b$ esto implica que $ab^{-1} \in H$ es decir $ab^{-1} = h$, con $h \in H$, entonces $a = hb$. Ahora si $a = kb$ con $k \in H$ entonces $ab^{-1} = k$ y esto implica que $a \sim b$. Con esto concluimos que $a \sim b$ si y sólo si $a \in [b] = \{hb | h \in H\}$ en este caso a la clase de equivalencia de $[b]$ la denotamos Hb y la llamamos clase lateral derecha de H en G (mediante un razonamiento análogo podemos definir la clase lateral izquierda bH).*

Teorema 1.47. *Si $\sim$ es una relación de equivalencia en A entonces $A = \cup_{a \in A}[a]$ y además si $a, b \in A$ son tales que $[a] \neq [b]$, entonces $[a] \cap [b] = \emptyset$*

Demostración. Verifiquemos primero que $A = \cup_{a \in A}[a]$. Es claro que $\cup_{a \in A}[a] \subset A$ pues cada clase de equivalencia esta formada por elementos de A y $\forall a \in A$ se cumple que $a \in [a]$ por lo tanto $A \subset \cup_{a \in A}[a]$ y $A = \cup_{a \in A}[a]$.

Ahora supongamos que $[a] \neq [b]$ y que $[a] \cap [b] \neq \emptyset$ y tomamos $x \in [a] \cap [b]$ esto implica que $x \sim a$ y que $x \sim b$ y por transitividad $a \sim b$, ahora cualquier elemento $x' \in [a]$ cumple que $x' \sim a$ y por transitividad $x' \sim b$ y por lo tanto $x' \in [b]$ lo cual implica que $[a] \subset [b]$, mediante un razonamiento análogo concluimos que $[b] \subset [a]$ y por lo tanto $[a] = [b]$ lo cual contradice la hipótesis de que $[a] \neq [b]$. Por lo tanto si $[a] \neq [b]$ entonces $[a] \cap [b] = \emptyset$ y en caso de que la intersección no sea vacía entonces $[a] = [b]$.

□

Definición 1.48. *Una partición del conjunto A es una familia $\mathbb{P}$ de subconjuntos no vacíos de A, disjuntos dos a dos, cuya unión es A. Es decir, $\mathbb{P} = \{A_i | i \in I\}$, donde se cumple que para cada $i \in I$, $A_i \subseteq A$ y $A_i \neq \Phi$, siempre que $A_i \cap A_j \neq \Phi$, entonces $A_i = A_j$ y $\cup A_i = A$.*

Notemos que por el Teorema 1.47 cualquier relación de equivalencia definida en un conjunto A, induce una partición del conjunto A.

Lema 1.49. *Sea G un grupo finito y $H \leq G$ si $b \in G$ consideramos su clase de equivalencia $[b] = Hb$, entonces $|H| = |Hb|$.*

Demostración. Definimos una función $f : H \longrightarrow Hb$ como $f(h) = hb$, f es inyectiva pues si $f(h) = f(h')$ entonces $hb = h'b$ y $hbb^{-1} = h'bb^{-1}$ por lo que $h1 = h'1$ y entonces $h = h'$, es suprayectiva pues si $x \in Hb$ entonces $x = h''b$ para alguna $h'' \in H$ y se cumple que $f(h'') = h''b$. Por lo tanto f es biyectiva y $|H| = |Hb|$.

□

Teorema 1.50. ***Lagrange****. Si G es un subgrupo finito y H es un subgrupo de G entonces el orden de H divide al orden de G.*

Demostración. Sea $\{H_i\}_{i=1}^n$ la familia que consta de todas las clases laterales distintas, sabemos por el Teorema 1.47 que $\cup_{i=1}^n H_i = G$ y como para cada $i \neq j$ se cumple que $H_i \cap H_j = \Phi$ entonces $|G| = \sum_{i=1}^n H_i$, ahora si $|H| = k$ entonces por el Lema 1.49 se concluye que

$$|G| = n|H| = nk$$

lo cual prueba el teorema.

□

Notación 1.51. *Cuando tengamos G un grupo finito y $H \leq G$ al número de clases laterales de H en G o sea $|G|/|H|$ lo denotamos $[G : H]$ y le llamamos el índice de H en G.*

Definición 1.52. *Sea G un grupo finito y $g \in G$ definimos n el orden de g como el mínimo entero positivo para el cual $g^n = 1$ y lo denotamos $o(g) = n$.*

Observación 1.53. *Notemos que si tenemos un grupo finito G y un elemento $g, \in G$ entonces $|\langle g \rangle| = o(g)$.*

Teorema 1.54. *Sea G un grupo finito y $g \in G$ entonces se cumplen las siguientes condiciones:*

1. *El orden de $o(g)$ divide a $|G|$.*
2. *Si $|G| = n$ entonces $g^n = 1$.*

Demostración.

1. Por la Observación 1.53 es cierto que $o(g) = |\langle g \rangle|$ y por el teorema de Lagrange $|\langle g \rangle|$ divide a $|G|$ y por lo tanto $o(g)$ divide a $|G|$.
2. Calculemos $g^{|G|} = g^{o(g)k} = (g^{o(g)})^k = 1^k = 1$.

□

1.4. Grupos Cíclicos

En el Ejemplo 1.38 vimos que para cada grupo G y $g \in G$ podemos construir $\langle g \rangle$ el subgrupo cíclico generado por g. Ahora definiremos lo que es un grupo cíclico.

Definición 1.55. *Si tenemos un grupo G y $a \in G$ que cumple $G = \{a^n | n \in \mathbb{Z}\}$, decimos que G es un grupo cíclico generado por a.*

Proposición 1.56. *Sea G un grupo cíclico, entonces G es abeliano.*

Demostración. Sean $g_1, g_2 \in G$ como G es cíclico entonces está generado por un elemento a y se cumple que $g_1 = a^n$, $g_2 = a^m$ para algunas $n, m \in \mathbb{Z}$, consideramos el producto

$$g_1 g_2 = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = g_2 g_1$$

con lo cual podemos concluir que G es abeliano.

□

Proposición 1.57. *Sea G un grupo cíclico y $H \leq G$ entonces H es un grupo cíclico.*

Demostración. Si H es el grupo trivial entonces está generado por el elemento neutro, ahora supongamos que $H \neq \{1\}$. Sea a un generador de G, consideremos cualquier elemento en H que es de la forma a^n para alguna $n \in \mathbb{Z}$, por el principio del buen orden, sea m el mínimo entero positivo para el cual a^m pertenece a H, al dividir n entre m obtenemos $n = mk + r$ para algunas $k, r \in \mathbb{Z}$ y $0 \leq r < m$ y podemos escribir

$$a^n = a^{mk+r} = a^{mk} a^r = (a^m)^k a^r$$

de esto se sigue que $a^n (a^m)^{-k} = a^r$, notemos que tanto a^n como $(a^m)^{-k}$ son elementos de H, esto podemos concluir que $a^r \in H$, sabemos que $r < m$ por ser r el residuo de la división y m es el menor entero positivo para el cual $a^m \in H$ esto implica que $r = 0$ y por lo tanto $a^n = (a^m)^{-k}$, lo cual implica que cualquier elemento de H se puede escribir como una potencia de a^m por lo tanto a^m es el generador de H. Lo cual prueba que H es un subgrupo cíclico.

□

Proposición 1.58. *Sea G un grupo finito cuyo orden es un número primo, entonces G es un grupo cíclico.*

Demostración. Sea $g \in G$ tal que $g \neq 1$ y consideremos el subgrupo cícico $\langle g \rangle$, por el teorema de Lagrange $|\langle g \rangle|$ divide a $|G|$ pero como $|G|$ es primo esto implica que $|\langle g \rangle| = 1$ ó $|\langle g \rangle| = |G|$ como $g \neq 1$ entonces $|\langle g \rangle| = |G|$ y por lo tanto $\langle g \rangle = G$ de donde se concluye que G es un grupo cíclico. □

1.5. Conjuntos Generadores

En el caso de los grupos cíclicos teníamos que un grupo G era cíclico si estaba generado por un elemento a, en esta sección, estudiaremos los grupos que están generados por más de un elemento.

Proposición 1.59. *Sea G un grupo, I un conjunto de indices no vacío y $\{H_i | H_i \leq G \ \forall i \in I\}$ una familia de subgrupos de G, entonces $\cap_{i \in I} H_i \leq G$.*

Demostración. Sean $a, b \in \cap_{i \in I} H_i$, entonces $ab \in H_i$ para cada $i \in I$ pues cada H_i es subgrupo de G, por lo tanto $\cap_{i \in I} H_i$ es cerrado bajo la operación de G, ahora si $g \in \cap_{i \in I} H_i$ entonces $g \in H_i$ y $g^{-1} \in \cap_{i \in I} H_i$, $\forall i \in I$ para cada $i \in I$ entonces $g^{-1} \in \cap_{i \in I} H_i$. Por lo tanto $\cap_{i \in I} H_i \leq G$.

□

Definición 1.60. *Sea G un grupo y $\{a_i \in G | i \in I\}$, al subgrupo H de G más pequeño que contiene al conjunto $\{a_i \in G | i \in I\}$ lo llamamos el subgrupo generado por $\{a_i \in G | i \in I\}$. Si $G = H$ decimos que $\{a_i \in G | i \in I\}$ genera a G y todos los a_i son los generadores de G si $\{a_i \in G | i \in I\}$ es finito decimos que G es finitamente generado.*

Notación 1.61. *Cuando hablemos del subgrupo de G generado por un conjunto A lo denotamos por $\langle A\rangle$.*

Ejemplo 1.62. *El grupo $\mathbb{K}$ del ejemplo 1.27 está generado por los $\{a, b\}$ pues el subgrupo de $\mathbb{K}$ más pequeño que contiene a $\{a, b\}$ es $\mathbb{K}$ mismo.*

Teorema 1.63. *Sea G un grupo y $A = \{a_i \in G | i \in I\} \subset G$ entonces los elementos de $\langle A\rangle$ son productos finitos de potencias enteras de elementos de A, es decir $\prod_{s\in S} p_s^n$ donde S es un conjunto finito, $n \in \mathbb{Z}$ y $p_s \in A$ para cualquier $s \in S$.*

Demostración. Sea S un conjunto finito y K el conjunto de todos los productos finitos de potencias enteras de elementos de A, entonces se cumple que $K \subset \langle A\rangle$, ahora verifiquemos que, $K \leq G$.

Sean $l, k \in K$ y notemos que lk es un producto de potencias enteras de elementos de A por lo que K es cerrado y si $k \in K$, k es un producto finito de potencias enteras de elementos de A y k^{-1} es el producto de esos mismos elementos en orden contrario donde las potencias tienen signo contrario, por lo que $k^{-1} \in K$ por ser un producto finito de potencias de elementos de A, por lo tanto $K \leq G$ y como $\langle A\rangle$ es el subgrupo de G más pequeño que contiene a A esto implica que $K = \langle A\rangle$. Lo cual prueba el teorema.

□

Observación 1.64. *El teorema anterior tiene una interpretación muy útil, cuando trabajemos con elementos de $\langle A\rangle$ para algún conjunto A, cada uno de estos elementos se puede intepretar como una palabra formada por elementos de A, donde cada palabra representa un producto finito de elementos de A. Por ejemplo la palabra "hola" será el producto de los elementos $h, o, l, a \in A$. Y también podemos expresar estas palabras como producto finito de potencias enteras de elementos de A, por ejemplo $holaa = h^1o^1l^1a^2$.*

1.6. Morfismos y Subgrupos Normales

Definición 1.65. *Sean G y G' dos grupos y $\varphi : G \longrightarrow G'$ una función, decimos que φ es un morfismo de grupos si $\forall a, b \in G$ $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall g, h \in G$.*

Ejemplo 1.66. *Dados dos grupos G y G' siempre existe el morfismo trivial $\tau : G \longrightarrow G'$ dado por $\tau(g) = 1$, y es morfismo de grupos pues $\tau(gh) = 1 = 1 \cdot 1 = \tau(g)\tau(h)$.*

Ejemplo 1.67. *Sea G un grupo abeliano, definimos la función $\varphi : G \longrightarrow G$, como $\varphi(g) = g^2$, este es un morfismo de grupos pues $\varphi(ab) = (ab)^2 = (ab)(ab) = (ab)(ba) = ab^2a = a^2b^2 = \varphi(a)\varphi(b)$.*

Ejemplo 1.68. *Sea $r \in \mathbb{Z}$ y $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ definida como $\varphi(z) = rz$, φ es un morfismo de grupos pues $\varphi(z + s) = rz + rs = \varphi(z) + \varphi(s)$ para cualesquiera $z, s \in S$ lo cual verifica que φ es morfismo de grupos.*

Definición 1.69. *Sean $f : G \longrightarrow G'$ una función entre grupos, $H \leq G$ y $K \leq G'$, definimos $f(H) = \{f(h)|h \in H\}$ y $f^{-1}(K) = \{g \in G|f(g) \in K\}$. Los llamamos imagen de H bajo f e imagen inversa de K bajo f respectivamente.*

Teorema 1.70. *Sean G y G' grupos con $\varphi : G \longrightarrow G'$ un morfismo, entonces se cumplen las siguientes propiedades:*

1.- Si $1 \in G$ *entonces* $\varphi(1) = 1$

2.- Si $a \in G$ *entonces* $\varphi(a^{-1}) = \varphi(a)^{-1}$

3.- Si $H \leq G$ *entonces* $\varphi(H) \leq G'$

4.- Si $K \leq G'$ *entonces* $\varphi^{-1}(K) \leq G$

Demostración.

1.- Sean $1, a \in G$ entonces $\varphi(a) = \varphi(a1) = \varphi(a)\varphi(1)$ y esto implica que $\varphi(1) = 1$.

2.- Sea $a \in G$ entonces tenemos que $\varphi(1) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$ y por el inciso anterior $1 = \varphi(a)\varphi(a^{-1})$ por lo tanto $\varphi(a^{-1}) = \varphi(a)^{-1}$.

3.- Sean $a, b \in \varphi(H)$ entonces $a = \varphi(x)$ y $b = \varphi(y)$ para algunos $x, y \in H$ caculando

$$ab = \varphi(x)\varphi(y) = \varphi(xy)$$

por lo que concluimos que $ab \in \varphi(H)$. Ahora como $a \in \varphi(H)$ entonces $a^{-1} = \varphi(x)^{-1} = \varphi(x^{-1})$ lo cual implica que $a^{-1} \in \varphi(H)$ pues $x^{-1} \in G$ por lo tanto $\varphi(H) \leq G'$.

4.- Sean $a, b \in \varphi^{-1}(K)$ entonces $\varphi(a), \varphi(b) \in K$ y como K es subgrupo de G' tenemos que $\varphi(ab) = \varphi(a)\varphi(b) \in K$ y por lo tanto $ab \in \varphi^{-1}(K)$ por lo tanto $\varphi^{-1}(K)$ es cerrado. Ahora si $a \in \varphi^{-1}(K)$, se tiene que $\varphi(a) \in K$, de donde $\varphi(a^{-1}) = \varphi(a)^{-1} \in K$, por lo cual $a^{-1} \in \varphi^{-1}(K)$. Lo cual concluye la demostración.

□

Definición 1.71. *Sea* $\phi : G \longrightarrow G'$ *un morfismo de grupos, llamamos Kernel de* ϕ *al grupo* $\phi^{-1}\{1\} = \{g \in G | \phi(g) = 1\}$. *Y lo denotamos* $Ker(\phi)$.

Definición 1.72. *Sea* $f : G \longrightarrow G'$ *un morfismo de grupos, decimos que* f *es un monomorfismo de grupos si* f *es un morfismo de grupos y una función inyectiva.*

A continuación revisaremos un resultado que nos dará un criterio para verificar cuándo un morfismo de grupos es monomorfismo.

Teorema 1.73. *Sea* $\nu : G \longrightarrow G'$ *un morfismo de grupos entonces* ν *es un monomorfismo de grupos si y sólo si* $Ker(\nu) = \{1\}$.

Demostración. Supongamos que ν es monomorfismo y consideremos $k \in Ker(\nu)$, esto implica que $\nu(k) = 1$, sabemos por el Teorema 1.70 que $\nu(1) = 1$ lo cual implica que $\nu(k) = \nu(1)$ y como ν es inyectiva entonces $1 = k$ y por lo tanto $Ker(\nu) = \{1\}$.

Ahora supongamos que $Ker(\nu) = \{1\}$ y supongamos que $\nu(a) = \nu(b)$ entonces tenemos que $\nu(a)\nu(b)^{-1} = 1$ y por el Teorema 1.70 se cuple que $\nu(a)\nu(b^{-1}) = 1$ y como ν es morfismo de grupos se tiene que $\nu(ab^{-1}) = 1$ lo cual implica que $ab^{-1} \in Ker(\nu)$ por lo tanto $ab^{-1} = 1$ con lo cual se concluye que $a = b$ lo cual verifica que ν es monomorfismo de grupos.

□

Definición 1.74. *Sea* $f : G \longrightarrow G'$ *un morfismo de grupos, decimos que* f *es un epimorfismo de grupos si* f *es un morfismo de grupos y una función suprayectiva.*

Definición 1.75. *Sea* $f : G \longrightarrow G'$ *un morfismo de grupos, decimos que* f *es un isomorfismo de grupos si* f *es monomorfismo y epimorfismo de grupos.*

Definición 1.76. *Sea H un subgrupo de un grupo G, decimos que H es un subgrupo normal de G si $gH = Hg$ para cualquier $g \in G$.*

Notación 1.77. *Si tenemos N un subgrupo normal de G, lo denotamos $N \lhd G$.*

Observación 1.78. *Si H es un subgrupo normal entonces $gH = Hg$ para toda $g \in G$ esto implica que si $h \in H$ entonces $gh = h'g$ para alguna $h' \in H$, es decir $ghg^{-1} \in H$ para cualquier $g \in G$. Inversamente, si para cualesquiera $g \in G$, $h \in H$ se tiene que $ghg^{-1} \in H$, entonces $ghg^{-1} = h'$ para alguna $h' \in H$ y $gh = h'g$ de donde se sigue que $gH = Hg$ y por lo tanto H es un subgrupo normal.*

Ejemplo 1.79. *Si tenemos un grupo G abeliano entonces cualquier subgrupo de G es un subgrupo normal. Pues si consideramos $H \leq G$ y tomamos $g \in G$ y $h \in H$ entonces $ghg^{-1} = hgg^{-1} = h$, lo cual implica que H es subgrupo normal.*

Ejemplo 1.80. *En cualquier grupo G el centro $Z(G)$ es un subgrupo normal y se verifica de la misma forma que el ejemplo anterior.*

Corolario 1.81. *Sea $f : G \longrightarrow G'$ un morfismo de grupos, entonces $Ker(f)$ es un subgrupo normal de G.*

Demostración. Sea $x \in Ker(f)$ y $g \in G$, calculamos $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)1f(g)^{-1} = 1$ por lo tanto $gxg^{-1} \in Ker(f)$ y por lo tanto $Ker(f)$ es un subgrupo normal de G.

□

1.7. Grupo Cociente

Teorema 1.82. *Sea G un grupo y $H \lhd G$ definimos $G/H = \{aH | a \in G\}$ el conjunto de clases laterales izquierdas de H en G, entonces G/H es un grupo con la operación $aHbH = abH$.*

Demostración. Verifiquemos que el producto en G/H está bien definido, si tenemos $aH = a'H$ y $bH = b'H$ para $a, a', b, b' \in G$ entonces tenemos que $a = a'h$ y que $b = b'n$ para algunas $h, n \in H$ por la definicion de clase lateral izquierda, entonces calculamos

$$ab = a'hb'n = a'b'(b'^{-1}hb')n$$

notemos que $b'^{-1}hb' \in H$ pues H es normal en G, entonces $k = b'^{-1}hb'n \in H$ por lo que $ab = a'b'k$ con $k \in H$, lo cual implica que $ab \in a'b'H$ y por lo tanto $abH = a'b'H$. Con esto se concluye que

$$aHbH = abH = a'b'H = a'Hb'H$$

lo cual implica que la operación entre clases no depende de los representantes que se utilicen para cada clase, es decir la operación está bien definida.

El conjunto G/H cumple las 4 propiedades de la Definición 1.19 pues las hereda directamente de la estructura de grupo de G.

□

Observación 1.83. *Este grupo tiene como elemento neutro $1H$ pues para cualquier otra clase aH tenemos que $1HaH = 1aH = aH$, a este elemento lo representamos como H. Y para cualquier $h \in H$ se cumple que $hH = H$ con lo cual tenemos que para cualquier $h \in H$, hH representa al elemento neutro del grupo G/H.*

Ejemplo 1.84. *Consideremos los grupos* $2\mathbb{Z}$ *y* $\mathbb{Z}$ *es fácil verificar que* $2\mathbb{Z} \leq \mathbb{Z}$ *y como* $\mathbb{Z}$ *es abeliano entonces* $2\mathbb{Z} \lhd \mathbb{Z}$ *veamos cómo son los elementos del grupo cociente* $\mathbb{Z}/2\mathbb{Z}$*, si* $z \in \mathbb{Z}/2\mathbb{Z}$ *entonces* $z = t + 2\mathbb{Z}$ *para algún* $t \in \mathbb{Z}$*, notemos que si* t *es un número par entonces por la observación 1.83 entonces* $t + 2\mathbb{Z} = 2\mathbb{Z}$ *y si* $s, t \in \mathbb{Z}$ *son impares entonces* $s + 2\mathbb{Z} = t + 2\mathbb{Z}$ *lo cual nos deja a* $\mathbb{Z}/2\mathbb{Z}$ *sólo con 2 elementos* $2\mathbb{Z}$ *y* $s + 2\mathbb{Z}$ *donde* s *es un número entero impar.*

Observación 1.85. *Como vimos en la proposición anterior, el grupo* $\mathbb{Z}/2\mathbb{Z}$ *tiene únicamente 2 elementos, a este grupo se le conoce como* $\mathbb{Z}_2$ *y también se interpeta cómo* $\mathbb{Z}_2 = \{0, 1\}$ *donde* $0 + 0 = 0$*,* $0 + 1 = 1$*,* $1 + 0 = 1$ *y* $1 + 1 = 0$ *a ésta suma se le conoce como suma módulo* 2 *y corresponde con la suma entre las* 2 *clases laterlales en* $\mathbb{Z}/2\mathbb{Z}$*. De igual manera el grupo* $\mathbb{Z}/3\mathbb{Z}$ *se interpreta como* $\mathbb{Z}_3 = \{0, 1, 2\}$ *donde* $0 + 0 = 0$*,* $0 + 1 = 1$*,* $0 + 2 = 2$*,* $1 + 0 = 1$*,* $1 + 1 = 2$*,* $1 + 2 = 0$*,* $2 + 0 = 2$*,* $2 + 1 = 0$ *y* $2 + 2 = 1$ *a esta suma se le conoce cómo suma módulo* 3 *y corresponde con la suma entre las* 3 *clases laterales en* $\mathbb{Z}/3\mathbb{Z}$*. El concepto se generaliza para* $\mathbb{Z}/n\mathbb{Z}$ *donde este grupo se interpreta cómo* $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ *con la operación de suma modulo* n *que también corresponde con la suma entre las* n *clases laterales,* $\mathbb{Z}_n$ *es un grupo cíclico de orden* n*.*

Ejemplo 1.86. *Consideremos los grupos* $\mathbb{Q}$ *y* $\mathbb{Z}$*, como* $\mathbb{Q}$ *es abeliano entonces* $\mathbb{Z} \lhd \mathbb{Q}$*, veamos cómo son los elementos de* $\mathbb{Q}/\mathbb{Z}$*, sea* $q \in \mathbb{Q}/\mathbb{Z}$ *entonces* $q = r + \mathbb{Z}$ *con* $r \in \mathbb{Q}$*, ahora como* r *es un número racional entonces es de la forma* $r = a/b$ *donde* $a, b \in \mathbb{Z}$*, entonces tendríamos que* $q = a/b + \mathbb{Z}$ *si calculamos la suma de* q *consigo mismo* $|b|$ *veces entonces tendríamos*

$$|b|q = (|b|a)/b + \mathbb{Z}$$

y si $b < 0$ *entonces tenemos*

$$-bq = -ba/b + \mathbb{Q} = -a + \mathbb{Z} = \mathbb{Z}$$

ahora si $b > 0$ *etonces tenemos*

$$bq = ba/b + \mathbb{Q} = a + \mathbb{Z} = \mathbb{Z}$$

con lo cual concluimos que cualquier elemento de $\mathbb{Q}/\mathbb{Z}$ *tiene orden finito.*

Teorema 1.87. *Sea* $H \lhd G$ *entonces existe un morfismo* $\psi : G \longrightarrow G/H$*, tal que* $Ker(\psi) = N$*.*

Demostración. Definimos $\psi : G \longrightarrow G/H$, $\psi(g) = gH$, para toda $g \in G$, $Ker(\psi) = H$ pues si $\psi(g) = H$ esto implica que $gH = 1H$ y que $g = 1h$ lo cual implica que si $\psi(g) = H$ entonces $g \in H$ por lo tanto $Ker(\psi) \subseteq H$, ahora tomemos $h \in H$ y aplicamos $\psi(h) = hH$, claramente se cumple que $h = 1h$ lo cual implica que $h \in 1H$ por lo tanto $hH = 1H = H$ y $H \subseteq Ker(\psi)$, con lo cual concluimos que $Ker(\psi) = H$.

□

Teorema 1.88. *Si* G *es un grupo finito y* $H \lhd G$ *entonces* $|G/H| = |G|/|H|$

Demostración. Supongamos que $|G/H| = k$ entonces k es el número de clases laterales derechas y por lo visto en la demostración del teorema de Lagrange $k = |G|/|H|$, lo cual implica que $|G/H| = |G|/|H|$. □

1.8. Teoremas de Isomorfismo y Teorema de la Correspondencia

Teorema 1.89. ***Primer Teorema de Isomorfismo****. Sea $f : G \longrightarrow G'$ un epimorfismo de grupos, entonces $G/Ker(f) \cong G'$.*

Demostración. Definimos $\tau : G/ker(f) \longrightarrow G'$ como $\tau(gKer(f)) = f(g)$, para toda $g \in G$, verfiquemos que τ está bien definida.

Sea $hKer(f) = h'Ker(f)$ esto implica que $h = h'k$ para $k \in Ker(f)$ si calculamos $\tau(hKer(f)) = f(h) = f(h'k) = f(h')f(k) = f(h') = \tau(h'Ker(f))$ pues $k \in Ker(f)$. Ahora verifiquemos que τ es un isomorfismo.

τ es suprayectiva pues f lo es, dado $x \in G'$ se cumple que $x = f(h)$ para alguna $h \in G$ por lo que $\tau(hKer(f)) = f(h) = x$. Y si $\tau(hKer(f)) = \tau(h'ker(f))$ entonces $f(h) = f(h')$ y se cumple que $1 = f(h)^{-1}f(h') = f(h^{-1}h')$ y por lo tanto $h^{-1}h' \in Ker(f)$ lo cual implica que $hKer(f) = h'Ker(f)$ por lo que concluimos que es inyectiva. Por último verifiquemos que es un morfismo de grupos. Calculamos

$$\tau(aKer(f)bKer(f)) = \tau(abKer(f)) = f(ab) = f(a)f(b) = \tau(aKer(f))\tau(bKer(f))$$

por lo tanto $G/Ker(f) \cong G'$.

□

Teorema 1.90. ***Segundo Teorema de Isomorfismo****. Sea G un grupo y $N, H \leq G$ donde $N \lhd G$. Entonces $HN/N \cong H/(H \cap N)$. Con $HN = \{hn | h \in H,\ n \in N\}$.*

Demostración. Debido a que $N \lhd G$ es fácil verificar que HN es un subgrupo de G y como N es subgrupo normal de G entonces también lo es de HN. Consideremos $\gamma : G \longrightarrow G/N$ como $(g) = gN$. Ahora $\gamma[H] \leq G/N$, si restringimos γ al grupo H obtenemos un morfismo de grupos de H en $\gamma[H]$, y el kernel de esta restricción será $H \cap N$ y por el primer teorema de isomorfismo tenemos que $\gamma[H] \cong H/(H \cap N)$.

Ahora consideremos la restricción de γ a HN, esta restricción resulta ser un morfismo de HN en $\gamma[H]$ pues $\gamma(n)$ es la identidad N de G/N para cualquier $n \in N$. El kernel de esta restricción a HN es N y por el primer teorema de isomorfismo $HN/N \cong \gamma[H]$. Lo cual implica que $HN/N \cong H/(H \cap N)$.

□

Teorema 1.91. ***Tercer Teorema de Isomorfismo****. Sea $f : G \longrightarrow G$ un epimorfismo de grupos, si $N' \lhd G'$ y $N = f^{-1}(N')$ entonces $G/N \cong G'/N'$ y de forma equivalente $G/N \cong (G/Ker(f))/(N/Ker(f))$.*

Demostración. Definimos $\psi : G \longrightarrow G'/N'$ como $\psi(a) = f(a)N'$, como f es suprayectiva es claro que ψ lo es también, además ψ es un morfismo de grupos pues

$$\psi(ab) = f(ab)N' = f(a)f(b)N' = f(a)N'f(b)N' = \psi(a)\psi(b).$$

Ahora verifiquemos que $N = Ker(\psi)$. Si $m \in Ker(\psi)$ entonces $\psi(m) = f(m)N' = N'$ lo cual implica que $f(m) \in N'$ y entonces $m \in N$ por lo tanto $Ker(\psi) \subseteq N$, tomemos ahora un elemento $n \in N$ y calculemos $\psi(n) = f(n)N'$ y por definición de N tenemos que $f(n)$ pertenece a N' y por lo tanto $\psi(n) = f(n)N' = N'$ y entonces $n \in Ker(\psi)$ lo cual verifica que $N = Ker(\psi)$.

Entonces tenemos que ψ es un epimorfismo de G en G'/N' con kernel N, aplicando el primer teorema de isomorfismo tenemos que $G/N \cong G'/N'$. Y finalmente aplicando el primer y segundo teorema de isomorfismo tenemos que, $G' \cong G/ker(f)$, $N' \cong N/Ker(f)$, lo cual muestra que $G/N \cong (G/Ker(f))/(N/Ker(f))$.

□

Teorema 1.92. ***Teorema de la correspondencia****. Si N es un subgrupo normal de G, entonces existe una biyección entre la familia de subgrupos de G/N y los subgrupos $H \subseteq G$ tales que $N \subseteq H$. La correspondencia es*

$$N \subseteq H \longrightarrow H/N \subseteq G/N.$$

Demostración. Sea H un subgrupo de G tal que $N \subseteq H$. Supongamos ahora que aN, bN son dos elementos de H/N, entonces $a, b \in H$ y $ab \in H$ por lo que $abN \in H/N$. Finalmente, si $aN \in H/N$ entonces $a \in H$ y $a^{-1} \in H$ por lo que $a^{-1}N \in H/N$.

Mostraremos ahora que la correspondencia anterior es inyectiva. En efecto, si H, H' son dos subgrupos de G tales que $N \subseteq H$ y $N \subseteq H'$ y satisfacen que $H/N = H'/N$, probaremos que $H = H'$. Para esto, observemos que si $h \in H$, entonces $hN \in H/N = H'/N$, por lo que $hN \in H'/N$ y así $hN = \tilde{h}N$ con $\tilde{h} \in H'$. Se sigue que $h = h1 = hn$ para algun $n \in N$; y como $N \subseteq H'$, entonces $\tilde{h}n \in H'$ y por lo tanto $h \in H'$. Hemos mostrado que $H \subseteq H'$. En forma similar se muestra que $H' \subseteq H$.

Ahora mostraremos que la correspondencia anterior es suprayectiva. En efecto, si tenemos $\mathbb{H} \leq G/N$ y definimos el conjunto $H = \{h \in H | hN \in \mathbb{H}\}$. Entonces H es un subgrupo de G, ya que:

1) $1 \in H$ pues $1H \in \mathbb{H}$.

2) Si $a, b \in H$, entonces $aN, bN \in \mathbb{H}$ y así $(aN)(bN) = (ab)N \in \mathbb{H}$ por lo que $ab \in H$.

3) Si $a \in H$. entonces $aN \in \mathbb{H}$ y así $(aN)^{-1} = a^{-1}N \in \mathbb{H}$ por lo que $a^{-1} \in H$.

$H \subseteq N$, ya que si $a \in N = N = 1N \in \mathbb{H}$ por lo que $a^{-1} \in H$ y $\mathbb{H} = H/N$ ya que:

1) Si $aN \in \mathbb{H}$, entonces $a \in H$ por definición de H y así $aN \in H/N$.

2) Si $hN \in H/N$ esto implica que $h \in H$, entonces $hN \in \mathbb{H}$ por definición de H.

□

1.9. Grupos de Permutaciones

Definición 1.93. *Sea A un conjunto distinto del vacío, decimos que σ es una permutación de A si es una función biyectiva de A en sí mismo.*

Teorema 1.94. *Sea A un conjunto distinto del vacío y sea S_A el conjunto de todas las permutaciones de A entonces S_A es un grupo con la operación de composición de permutaciones.*

Demostración. Tenemos que S_A es cerrado pues la composición de 2 funciones biyectivas es una función biyectiva, es asociativo pues la composición de funciones es asociativa, el elemento neutro de S_A es la funcion identidad y como estamos trabajando con funciones biyectivas cada función tiene inverso. Con lo cual concluimos que S_A tiene estructura de grupo.

□

Definición 1.95. *Sea $A = \{1, 2, 3, ..., n\}$, al grupo de permutaciones de A lo llamamos S_n el grupo simétrico de grado n.*

Observación 1.96. *Notemos que $|S_n| = n!$, pues para una permutación $\sigma \in S_n$, dado $1 \in S_n$ σ tiene n opciones para mandar al 1 y para el 2 tiene $n-1$ opciones pues no puede pasar que $\sigma(1) = \sigma(2)$ porque σ es inyectiva, procediendo de manera análoga concluimos que σ tiene $n-2$ posibilidades para mandar a 3. Si continuamos con el procedimiento llegaremos a que σ tiene sólo una opcion para mandar a n por lo tanto hay $n(n-1)(n-2)\cdots 1$ opciones para σ y por lo tanto $|S_n| = n!$.*

Observación 1.97. *Si G y G' son grupos y ϕ un monomorfismo de G en G' entonces G es ismomorfo a $\phi[G]$, pues si definimos $\varphi : G \longrightarrow \phi[G]$ como $\varphi(g) = \phi(g)$, φ es evidentemente un monomorfismo pues ϕ lo es, tambien φ es un epimorfismo porque está restringido a la imagen de ϕ y por lo tanto $G \cong \phi[G]$.*

Teorema 1.98. ***Cayley**. Cualquier grupo G es isomorfo a un grupo de permutaciones.*

Demostración. Si logramos construir un monomorfismo entre G y S_G, por la observación 1.97, tendríamos que G es isomorfo a un subgrupo de S_G. Entonces construyamos dicho monomorfismo.

Para $x \in G$ definimos $\lambda_x : G \longrightarrow G$ donde $\lambda_x(g) = xg$, esta función λ_x es biyectiva pues para cualquier $c \in G$ $\lambda_x(x^{-1}c) = c$ lo cual verfica es suprayectiva, y si $\lambda_x(a) = \lambda_x(b)$ entonces $ax = bx$ lo cual implica que $a = b$, así es inyectiva. Por lo tanto para cada $x \in G$ se cumple que $\lambda_x \in S_G$. Ahora definimos $\theta : G \longrightarrow S_G$ como $\theta(x) = \lambda_x$, verifiquemos que $\theta(x)$ es un morfismo de grupos. Calculamos

$$\begin{aligned}
(\theta(x)\theta(y))(g) &= \theta(x)((\theta(y)(g))) \\
&= \theta(x)(\lambda_y(g)) \\
&= \theta(x)(yg) \\
&= \lambda_x(yg) \\
&= xyg \\
&= \lambda_{xy}(g) \\
&= \theta(xy)(g) \ \forall g \in G
\end{aligned}$$

Así, $\theta(x)\theta(y) = \theta(xy)$, y θ es un morfismo de grupos. Ahora sólo falta verificar que $Ker(\theta) = \{1\}$, si tenemos $\theta(x) = Id_G$ entonces esto implica que $xg = g$ para cualquier $g \in G$ lo cual implica que $x = 1$, entonces θ es un monomorfismo de grupos y por lo tanto $G \cong \theta[G] \leq S_G$.

□

1.10. Acciones de Grupos en Conjuntos

Definición 1.99. *Sean G un grupo y X un conjunto no vacío. Una acción izquierda de G en X es una función $\alpha : G \times X \longrightarrow X$ donde $\alpha((g,x)) = g \bullet x$, la cual satisface:*

1.- $1 \bullet x = x$ *para* $1 \in G$, $x \in X$.

2.- $(g_1 g_2) \bullet x = g_1 \bullet (g_2 \bullet x)$ *para* $g_1, g_2 \in G$ *y* $x \in X$.

Ejemplo 1.100. *Sea X un conjunto no vacío y consideremos el grupo simétrico S_X, este actúa naturalmente en X con la acción $\alpha : S_X \times X \longrightarrow X$, dada por $\alpha(\sigma, x) = \sigma \bullet x = \sigma(x)$*

Ejemplo 1.101. *Cualquier grupo G define una acción en sí mismo, $\alpha : G \times G \longrightarrow G$, dada por $\alpha(g_1, g_2) = g_1 \bullet g_2 = g_1 g_2$. De igual forma si $H \leq G$ entonces de manera similar al caso anterior definimos la acción $\beta : H \times G \longrightarrow G$ como $\beta(h, g) = h \bullet g = hg$.*

Notación 1.102. *Cada que tengamos una acción izquierda de un grupo G en un conjunto X, diremos que X es un G-conjunto. Y para denotar $g \bullet x$ para una acción en abstracto nuevamente utilizaremos la notación multiplicativa es decir gx ó $g(x)$.*

Observación 1.103. *Si tenemos $x, y \in X$ y $g \in G$ tales que $gx = y$ entonces $x = g^{-1}y$ pues $x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$.*

Proposición 1.104. *Sean G un grupo y X un G-conjunto. Entonces, las siguientes condiciones se satisfacen.*

1. *Una acción izquierda $\alpha : G \times X \longrightarrow X$ induce un morfismo de grupos $\varphi_\alpha : G \longrightarrow S_X$ dado por $\varphi_\alpha(g)(x) = gx$ para cualquier $g \in G$ y para cualquier $x \in X$.*

2. *Un morfismo de grupos $\varphi : G \longrightarrow S_X$ induce una accion izquierda $\alpha_\varphi : G \times X \longrightarrow X$, dada por $gx = \varphi(g)(x)$, para todo $g \in G$ y para todo $x \in X$.*

Demostración. 1. Primero verifiquemos que $\varphi_\alpha(g)$ es una función biyectiva para todo $g \in G$, calculamos

$$\begin{aligned}(\varphi_\alpha(g) \circ \varphi_\alpha(g^{-1}))(x) &= \varphi_\alpha(g)(\varphi_\alpha(g^{-1})(x)) \\ &= \varphi_\alpha(g)(g^{-1}x) \\ &= g(g^{-1})x \\ &= (gg^{-1})x = x \ \forall x \in X\end{aligned}$$

con lo cual concluimos que $\varphi_\alpha(g)$ es una función biyectiva pues tiene inversa.

Ahora verifiquemos que φ_α es un morfismo de grupos. Para $g, h \in G$ calculamos

$$\begin{aligned}\varphi_\alpha(gh)(x) &= (gh)x \\ &= g(hx) \\ &= \varphi_\alpha(g)(hx) \\ &= \varphi_\alpha(g)(\varphi_\alpha(h)(x)) \\ &= (\varphi_\alpha(g) \circ \varphi_\alpha(h))(x)\end{aligned}$$

lo cual verifica que $\varphi_\alpha(gh)(x) = (\varphi_\alpha(g) \circ \varphi_\alpha(h))(x)$ y entonces φ_α es un morfismo de grupos.

2. Para $1 \in G$ y $x \in X$ calculamos $1x = \varphi(1)(x) = Id_G(x) = x$ lo cual verifica la condición 1 de la definición de acción, ahora para $g_1, g_2 \in G$ y $x \in X$ calculamos

$$\begin{aligned}(g_1g_2)x &= \varphi(g_1g_2)(x)\\ &= (\varphi(g_1)\varphi(g_2))(x)\\ &= \varphi(g_1)(\varphi(g_2(x)))\\ &= \varphi(g_1)(g_2x)\\ &= g_1(g_2x)\end{aligned}$$

lo cual verifica la condición 2 de la definición de acción.

□

A continuación definiremos algunos conceptos importantes en la teoría de grupos que involucran acciones de grupos en conjuntos.

Definición 1.105. *Sea X un G-conjunto.*

1. *La G-órbita de $x \in X$ en X se define como*

$$O_G(x) = \{gx | g \in G\}.$$

2. *El estabilizador de $x \in X$ en G es el conjunto*

$$G(x) = \{g \in G | gx = x\}.$$

3. *El estabilizador de X en G es el conjunto*

$$G(X) = \cap_{x \in X} G(x) = \{g \in G | gx = x \ \forall x \in X\}.$$

Observación 1.106. *Dado un X un G-conjunto, las G-órbitas forman una partición del conjunto X dado que $1x = x$ entonces $X = \cup_{x \in X} O_G(x)$ y si $O_G(x) \cap O_G(y) \neq \Phi$ entonces $g_1x = g_2y$ para algunos $g_1, g_2 \in G$ pero esto implica que $x = g_1^{-1}(g_2y) = (g_1^{-1}g_2)y$ lo cual implica que $x \in O_G(y)$ y análogamente concluimos que $y \in O_G(x)$ lo cual implica que $O_G(x) = O_G(y)$.*

Observación 1.107. *El estabilizador $G(x)$ de $x \in X$ es un subgrupo de G, pues es distinto del vacío porque $1 \in G(x)$ y si consideramos $a, b \in G(x)$ entonces $(ab)x = a(bx) = ax = x$ con lo que concluimos que $G(x)$ es cerrado, ahora si $a \in G(x)$ entonces $ax = x$ y por la observación 1.103 entonces $x = a^{-1}x$ por lo que $a^{-1} \in G(x)$. Así $G(x) \leq G$.*

Teorema 1.108. *Sea G un grupo finito y X un G-conjunto y sea $x \in X$, entonces $|O_G(x)| = [G : G(x)]$, es decir $|O_G(x)|$ divide a $|G|$.*

Demostración. Sea $S = \{gG(x) | g \in G\}$, y notemos que para cada $x_1 \in O_G(x)$ existe $g_1 \in G$ tal que $g_1x = x_1$ definimos la siguiente función $\psi : O_G(x) \longrightarrow S$, dada por $\psi(x_1) = g_1G(x)$ verifiquemos que ψ está bien definida.

Supongamos que $g_1x = x_1$ y que $g_1'x = x_1$ entonces $g_1x = g_1'x$ y $g_1^{-1}(g_1x) = g_1^{-1}(g_1'x)$, entonces $x = (g_1^{-1}g_1')x$ lo cual implica que $g_1^{-1}g_1' \in G(x)$ y $g_1' \in g_1G(x)$ y por lo tanto $g_1G(x) = g_1'G(x)$. Con lo cual concluimos que ψ está bien definida.

Ahora verificaremos que ψ es una función biyectiva, primero veamos que es inyectiva, supongamos que $\psi(x_1) = \psi(x_2)$ entonces $g_1, g_2 \in G$ tales que $x_1 = g_1x$ y $x_2 = g_2x$. Entonces $g_2 \in g_1G(x)$ lo cual implica que $g1G(x) = a2G(x)$, con $g \in G(x)$, finalmente tenemos que

$$x_2 = g_2x = (g_1g)x = g_1(gx) = g_1x = x_1$$

con lo cual concluimos que ψ es inyectiva.

Veamos ahora que cualquier elemento de S se puede ver de la forma $\psi(x_i)$ para algún $x_i \in X$, consideremos un elemento arbitrario de S, digamos $g_1G(x)$ entonces g_ix es un elemento de X, digamos x_i, es decir, $g_ix = x_i$ con lo cual tenemos que $g_iG(x) = \psi(x_i)$. Por lo tanto ψ es biyectiva y $|O_G(x)| = |S| = [G : G(x)]$ y $|O_G(x)|$ divide a $|G|$.

□

Definición 1.109. *Sea X un G-conjunto. Decimos que la acción de G en X es fiel si cada que $gx = x$ para toda $x \in X$ entonces $g = 1$.*

Observación 1.110. *Notemos que si la acción es fiel y $gx = hx$ para cualquier $x \in X$, esto implica que $g = h$.*

1.11. Teorema de Cauchy

Sea X un G-conjunto finito y llamemos r al número de órbitas distintas y consideremos el conjunto $\{x_1, ..., x_r\}$ donde cada x_i es un elemento en una órbita distinta. Como las órbitas forman una partición del conjunto X tenemos que

$$|X| = |O_G(x_1)| + |O_G(x_2)| + ... + |O_G(x_r)|$$

existen algunas órbitas que constan de un solo elemento y a la unión de todas estas órbitas la denotaremos de la siguiente forma $X_G = \{x \in X | gx = x \ \forall g \in G\}$ suponiendo que X_G tiene s elementos, digamos $x_1, x_2, ...x_s$, entonces tendríamos la siguiente ecuación

$$|X| = |X_G| + |O_G(x_{s+1})| + ... + |O_G(x_r)|. \tag{1.1}$$

Teorema 1.111. *Sea G un grupo de orden p^n con p un número primo y X un G-conjunto finito entonces $|X| \equiv |X_G|$ mod p.*

Demostración. Por la ecuación 1.1 y el Teorema 1.108 tenemos que $|O_G(x_i)|$ divide a $|G|$ para $s+1 \leq i \leq r$ y de nuevo por la ecuación 1.108 $|X| - |X_G|$ es divisible por p lo cual implica que $|X| \equiv |X_G|$ *mod* p.

□

Definición 1.112. *Sea G un grupo y p un número primo, decimos que G es un p-grupo si para cualquier $g \in G$ se tiene que $o(g) = p^n$ con $n \in \mathbb{N}$. Y un subgrupo de un grupo G es un p-subgrupo de G si este subgrupo es a su vez un p-grupo.*

Teorema 1.113. ***Cauchy***. *Sea p un número primo y G un grupo finito tal que p divide a $|G|$, entonces G tiene un elemento de orden p. Y por lo tanto un subgrupo de orden p.*

Demostración. Sea $X = \{(g_1, ..., g_p) | g_i \in G, g_1 g_2 ... g_p = 1\}$, dados $g_1, ..., g_{p-1}$ elementos de G el elemento g_p que completa el producto queda compleatamente determinado por $g_p = (g_1 ... g_{p-1})^{-1}$ lo cual muestra que $|X| = |G|^{p-1}$ y como p divide a $|G|$ entonces p divide a $|X|$.

Consideremos $\sigma \in S_p$ dada por $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 4$,...,$\sigma(p) = 1$ y hacemos actuar a σ sobre X de la forma $\sigma((g_1, ..., g_p)) = (g_{\sigma(1)}, ..., g_{\sigma(p)}) = (g_2, ..., g_1)$, notemos que $(g_2, ..., g_1) \in X$ pues si $g_1 ... g_p = 1$ entonces $g_1 = (g_2 ... g_p)^{-1}$ y por lo tanto $g_2 ... g_p g_1 = g_2 ... g_p (g_2 ... g_p)^{-1} = 1$, entonces $\sigma(x) \in X$ para cualquier $x \in X$. Ahora consideremos $\langle \sigma \rangle \leq S_p$ y $\langle \sigma \rangle$ actúa sobre X iterando σ sobre los elementos de X.

Es claro que $o(\sigma) = p$, aplicando el Teorema 1.111 obtenemos que $|X| \equiv |X_{\langle \sigma \rangle}|$ *mod* p pero sabemos que p divide a $|X|$ entonces p divide a $|X_{\langle \sigma \rangle}|$.

Ahora si $(g_1, ..., g_p)$ es fijado por σ y cualquier elemento de $\langle \sigma \rangle$ esto implica que

$$x_1 = x_2 = ... = x_p$$

y como p divide a $|X_{\langle \sigma \rangle}|$ esto implica que $X_{\langle \sigma \rangle}$ tiene al menos p elementos y por lo tanto existe un elemento $a \in G$ tal que $a \neq 1$ y $a^p = 1$ lo cual prueba el teorema.

□

Corolario 1.114. *Sea G un grupo finito, entonces G es un p-grupo si y sólo si $|G|$ es una potencia de p.*

Demostración. Supongamos que G es un p-grupo y supongamos que $|G|$ no es una potencia de p, entonces $|G|$ es divisible por algún primo $q \neq p$, entonces por el teorema de Cauchy existe un elemento de orden q lo cual contradice la hipótesis de que G es p grupo. Por lo tanto $|G|$ es una potencia de p.

Si $|G|$ es una potencia de p, entonces el orden de cualquier elemento de G es una potencia de p pues el orden de cualquier elemento divide a $|G|$. Por lo tanto G es un p-grupo.

□

Para terminar esta sección definiremos el concepto de p-subgrupo de Sylow.

Definición 1.115. *Sea G un grupo finito, decimos que P es un p-subgrupo de Sylow si es un p-subgrupo maximal de G, es decir no existe otro p-subgrupo de G que lo contenga.*

1.12. Anillos

Definición 1.116. *Se dice que un conjunto no vacío R es un anillo, si tiene 2 operaciones $\circledast$ y $\odot$ tales que cumplen las siguientes propiedades*

1. *$\forall a, b \in R$ se cumple que $a \circledast b \in R$.*
2. *$\forall a, b \in R$ se cumple que $a \circledast b = b \circledast a$.*
3. *$\forall a, b, c \in R$ se cumple que $a \circledast (b \circledast c) = (a \circledast b) \circledast c$.*

4. $\exists e \in R$ *tal que* $\forall a \in R$ *se cumple que* $a \circledast e = a = e \circledast a$.

5. $\forall a \in R\ \exists b \in R$ *tal que* $a \circledast b = e = b \circledast a$.

6. $\forall a, b \in R$ *se cumple que* $a \odot b \in R$.

7. $\forall a, b, c \in R$ *se cumple que* $a \odot (b \odot c) = (a \odot b) \odot c$.

8. $\forall a, b, c \in R$ *se cumple que* $a \odot (b \circledast c) = (a \odot b) \circledast (a \odot c)$ *y* $(b \circledast c) \odot a = (b \odot a) \circledast (c \odot a)$.

Notación 1.117. *Cuando se esté trabajando con un anillo en abstracto se utilizará la notación aditiva para la operación de las primeras 5 propiedades de la definición de anillo es decir* $a \circledast b = a + b$ *y se utilizará la notación multiplicativa para la otra operación es decir* $a \odot b = ab$.

Ejemplo 1.118. *El conjunto* $\mathbb{Z}$ *resulta ser un anillo con las operaciones de suma y producto.*

Ejemplo 1.119. *El conjunto* $\mathbb{Z}_n$ *para cualquier* n *entero mayor a cero resulta ser un anillo con las operaciones de suma y producto módulo* n.

Ejemplo 1.120. *Sea* G *un grupo abeliano, a cualquier morfismo de* G *en sí mismo lo llamamos endomorfismo de* G *y al conjunto de todos los endomorfismos de* G *lo denotamos* $End(G)$. *Este conjunto resulta ser un anillo con la operación de suma definida de la siguiente forma para* $\phi, \varphi \in End(G)$ *tenemos que* $(\phi + \varphi)(a) = \phi(a) + \varphi(a)$ *y el producto lo definimos como la composición de los endomorfismos de* G *es decir* $(\phi\varphi)(a) = \phi(\varphi(a))$

Definición 1.121. *Sea* R *un anillo, si* $\exists\ 1 \in R$ *tal que* $1r = r = r1$ *para todo* $r \in R$, *decimos que* R *es un anillo con unidad.*

Definición 1.122. *Sea* R *un anillo con unidad, se dice que un elemento* $u \in R$ *es una unidad si existe un elemento* $v \in R$ *tal que* $uv = vu = 1$.

Observación 1.123. *El conjunto de todas las unidades de un anillo con unidad, forman un grupo con la multiplicación del anillo, a este conjunto lo denotamos* R^*.

Capítulo 2

Automorfismos

Definición 2.1. *Sea G un grupo, un automorfismo de G es un isomorfismo de G en sí mismo. Al conjunto de isomorfismos de G lo denotamos $Aut(G)$.*

Proposición 2.2. *Sea G un grupo, entonces $Aut(G)$ es también un grupo con la composición.*

Demostración. Sean $\alpha, \beta \in Aut(G)$. Probaremos primero que $\alpha \circ \beta \in Aut(G)$, como α y β son automorfismos ambos son homomorfismos biyectivos y sabemos que la composición de funciones biyectivas es una función biyectiva y la composición de morfismos es un morfismo, por lo tanto $\alpha \circ \beta \in Aut(G)$. Ahora, como la composición de funciones es asociativa tenemos que $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$, para todos $\alpha, \beta, \gamma \in Aut(G)$; por otro lado sabemos que $\alpha \circ Id = Id \circ \alpha$ para todo $\alpha \in Aut(G)$ donde Id es el morfismo identidad, por lo que existe un elemento neutro en $Aut(G)$. Finalmente, para todo $\alpha \in Aut(G)$, dado que α es una función biyectiva, es invertible y su inverso es un isomorfismo, así existe $\alpha^{-1} \in Aut(G)$ de manera que $\alpha \circ \alpha^{-1} = Id = \alpha^{-1} \circ \alpha$ y con esto concluimos que para cada elemento existe el inverso. Por lo tanto $Aut(G)$ tiene estructura de grupo con la composición. □

2.1. Automorfismos Internos

Una manera de construir automorfismos es mediante la conjugación.

Proposición 2.3. *Sea G un grupo. Para cada $g \in G$ definimos la función $\varphi : G \to G$ como $\varphi_g(x) = gxg^{-1}$ para toda $x \in G$. Tenemos que φ_g es un automorfismo de G.*

Demostración. Dada $g \in G$ verifiquemos $\varphi_g \in Aut(G)$. Veamos primero que es un morfismo, sean $a, b \in G$ calculemos

$$\varphi_g(ab) = gabg^{-1} = ga(1)bg^{-1} = ga(g^{-1}g)bg^{-1} = (gag^{-1})(gbg^{-1}) = \varphi_g(a)\varphi_g(b)$$

por lo tanto φ_g es un morfismo de G en sí mismo. Ahora si $\varphi_g(x) = 1$ tenemos que $gxg^{-1} = 1$ y entonces $gx = 1g$, o bien $gx = g$ por lo que $1 = x$, en conclusión si $\varphi_g(x) = 1$ entonces $x = 1$ por lo tanto $Ker(\varphi_g) = \{1\}$ y φ_g es un monomorfismo. Veamos por último que φ_g es suprayectiva, dado $p \in G$, consideremos el elemento $g^{-1}pg$ y calculemos

$$\varphi_g(g^{-1}pg) = g(g^{-1}pg)g^{-1} = 1p1 = p$$

por lo tanto tenemos que φ_g es un epimorfismo y $\varphi_g \in Aut(G)$. □

A todos los automorfismos de la forma φ_g los llamaremos automorfismos internos de G.

Notación 2.4. *Dado un grupo G, $Inn(G) = \{\varphi_g | g \in G\}$ es como denotaremos al conjunto de automorfismos internos de G.*

Observación 2.5. *Notemos que $Inn(G) \neq \emptyset$, ya que $G \neq \emptyset$.*

Veamos ahora algunas propiedades de los automorfismos internos:

Proposición 2.6. *Sea G un grupo.*

1. *$\varphi_g\varphi_h = \varphi_{gh}$, para todos $g, h \in G$.*
2. *$(\varphi_g)^{-1} = \varphi_{g^{-1}}$, para todo $g \in G$.*

Demostración. 1. Sean $g, h, x \in G$. Calculando tenemos que:

$$\varphi_g\varphi_h(x) = \varphi_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \varphi_{gh}.$$

Así, $\varphi_g\varphi_h = \varphi_{gh}$.

2. Ahora, dados $g, x \in G$ tenemos, usando el inciso anterior, que:

$$(\varphi_g\varphi_{g^{-1}})(x) = x = \varphi_{gg^{-1}}(x) = \varphi_1(x) = 1x1^{-1} = x$$

de donde concluimos que $\varphi_g\varphi_{g^{-1}} = Id$ y así $(\varphi_g)^{-1} = \varphi_{g^{-1}}$.

□

La Observación 2.5 junto con la proposición anterior nos dice que los automorfismos internos forman un subconjunto no vacío de $Aut(G)$ cerrado bajo la composición y bajo inversos, en otras palabras tenemos que:

Teorema 2.7. *Los automorfismos internos de un grupo G forman un subgrupo de los automorfismos de G, es decir, $Inn(G) \leq Aut(G)$.*

Consideremos ahora la función $In : G \to Aut(G)$, dada por $In(g) = \varphi_g$ para todo $g \in G$; In es un morfismo pues $In(gh) = \varphi_{gh} = \varphi_g\varphi_h = In(g)In(h)$ por el primer inciso de la Proposición 2.6. Por construcción la imagen de In es $Inn(G)$ y el kernel de In es el centro de G dado por:

$$Z(G) = \{g \in G | gx = xg \ \forall x \in G\}$$

ya que $g \in G$ es tal que $In(g) = Id$ si y sólo si $gxg^{-1} = x$ para todo $x \in G$, lo cual ocurre si y sólo si $gx = xg$ para todo $x \in G$, y por lo tanto si y sólo si $g \in Z(G)$. Recordemos que el hecho de que G sea abeliano es equivalente a que $Z(G) = G$ y en este caso $Inn(G)$ es el subgrupo trivial.

Otra propiedad importante de los automorfismos internos es la siguiente:

Teorema 2.8. *Los automorfismos internos de un grupo G forman un subgrupo normal de los automorfismos de G, es decir, $Inn(G) \lhd Aut(G)$.*

Demostración. Sean $\sigma \in Aut(G)$ y $\varphi_g \in Inn(G)$ con $g \in G$. Dado $p \in G$ calculamos

$$\begin{aligned}(\sigma\varphi_g\sigma^{-1})(p) &= \sigma(\varphi_g(\sigma^{-1}(p))) = \sigma(g(\sigma^{-1}(p))g^{-1}) = \sigma(g)\sigma(\sigma^{-1}(p))\sigma(g^{-1}) \\ &= \sigma(g)(p)\sigma(g^{-1}) = \varphi_{\sigma(g)}(p)\end{aligned}$$

entonces $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)} \in Inn(G)$ y por lo tanto $Inn(G) \lhd Aut(G)$. □

Ejemplo 2.9. *Sea G un grupo cíclico $G = \langle x \rangle$. Analicemos cómo son en este caso los automorfismos de G.*

Si G es infinito sabemos que $G \cong \mathbb{Z}$. En este caso sea $\varphi \in Aut(G)$, afirmamos que $\varphi(x)$ también genera a G pues si $g \in G$ existe $g_1 \in G$ tal que $\varphi(g_1) = g$ pero $g_1 = x^n$ para alguna $n \in \mathbb{N}$ y entonces $g = \varphi(g_1) = \varphi(x^n) = \varphi(x)^n$, por lo tanto $\varphi(x)$ también genera a G. Sabemos además que los únicos generadores de G son x y x^{-1}, así que $\varphi(x) = x$ o $\varphi(x) = x^{-1}$. Si $\varphi(x) = x$ entonces $\varphi(x^n) = \varphi(x)^n = x^n$ para todo $n \in \mathbb{Z}$. Por otro lado si $\varphi(x) = x^{-1}$ entonces $\varphi(x^n) = \varphi(x)^n = (x^{-1})^n = (x^n)^{-1}$. Esto significa que todo $\varphi \in Aut(G)$ fija a cualquier elemento o manda a todo elemento a su inverso y esto implica que $Aut(G)$ tiene sólo 2 elementos; así $Aut(G) \cong \mathbb{Z}_2$.

Ahora, si G es finito sabemos que $G \cong \mathbb{Z}_n$ para algún $n \in \mathbb{N}$. Dado φ un automorfismo de G, como es un epimorfismo tenemos que $\varphi(x) = x^m$ para algún $0 \leq m < n$, de aquí se sigue que φ manda a cualquier elemento de G en su emésima potencia pues $\varphi(x^t) = \varphi(x)^t = (x^m)^t = (x^t)^m$ para todo $t \in \mathbb{Z}$. Además, como x es de orden n cada $m \in \mathbb{Z}$ con $0 \leq m < n$ da lugar a automorfismos diferentes. Concluimos entonces que en este caso G tiene exactamente n automorfismos que elevan a la m a cualquier elemento de G con $0 \leq m < n$.

La siguiente proposición describe como son los grupos de automorfismos de grupos ciclicos de orden finito.

Proposición 2.10. *Sea $G = \langle x \rangle \cong \mathbb{Z}_n$, $n \in \mathbb{N}$, y para cualquier $0 \leq m < n$, sea σ_m el endomorfismo de G tal que $\sigma_m(x) = x^m$, entonces $Aut(G)$ consiste en todos los σ_m, $0 < m < n$ y $(m, n) = 1$. Además $Aut(G)$ es abeliano y es isomorfo al grupo $(\mathbb{Z}/n\mathbb{Z})^*$ de las unidades del anillo $\mathbb{Z}/n\mathbb{Z}$.*

Demostración. La función σ_0 tiene como imagen $\{1\}$ esto implica que no es un automorfismo de G, ahora consideremos σ_m con $1 \leq m < n$, si $(n, m) = 1$, existen enteros a y b tales que $am + bn = 1$.

Sea $g \in G$, verificaremos que σ_m es epimorfismo, calculamos

$$\sigma_m(g^a) = g^{am} = g^{1-bn} = g(g^n)^{-b} = g, \ \forall \ g \in G$$

por lo tanto σ_m es un epimorfismo.

Entonces σ_m es también monomorfismo pues si $\sigma_m(x^{n_1}) = \sigma_m(x^{n_2})$, entonces $(x^{n_1})^m = (x^{n_2})^m$, $(x^m)^{n_1} = (x^m)^{n_2}$ esto implica que $x^{mn_1 - mn_2} = 1$ entonces $mn_1 \equiv mn_2 \ mod \ n$ y como $(m, n) = 1$ esto implica que $n_1 \equiv n_2 \ mod \ n$ y de esto podemos concluir que $x^{n_1} = x^{n_2}$, por lo tanto σ_m es un monomorfismo y $\sigma_m \in Aut(G)$ (como G es finito habría bastado probar suprayectividad o inyectividad).

Ahora, si $\phi \in Aut(G)$, $\phi(x) = x^m$ para alguna $0 < m < n$, por lo que $\phi = \sigma_m$. Dado que es un automorfismo, en particular es suprayectivo, así $x = \sigma_m(x^a)$ con $a \in \mathbb{Z}$, entonces $x = x^{am}$, $1 = x^{-1}x^{am}$ y $1 = x^{am-1}$ esto implica que $am - 1 = bn$ para alguna $b \in \mathbb{Z}$ y de aquí concluimos que $(m, n) = 1$ con lo que ya tenemos la primera afirmación.

Ahora si $1 \leq m_1, m_2 < n$ tenemos que $\sigma_{m_1}\sigma_{m_2} = \sigma_t = \sigma_{m_2}\sigma_{m_1}$ donde $1 \leq t < n$ y $m_1 m_2 \equiv t \ mod \ n$, entonces $Aut(G)$ es abeliano.

Recordemos que $(\mathbb{Z}/n\mathbb{Z})^* = \{m + n\mathbb{Z} | 1 \leq m < n,\ (m,n) = 1\}$, definimos $h : Aut(G) \to (\mathbb{Z}/n\mathbb{Z})^*$ donde $h(\sigma_m) = m + n\mathbb{Z}$ verifiquemos que h es morfismo de grupos, calculamos $h(\sigma_{m_1}\sigma_{m_2}) = h(\sigma_t)$ donde $1 \leq t < n$ y $m_1 m_2 \equiv t \, mod \, n$, entonces $h(\sigma_t) = t + n\mathbb{Z} = m_1 m_2 + n\mathbb{Z} = (m_1 + n\mathbb{Z})(m_2 + n\mathbb{Z}) = (h(\sigma_m))(h(\sigma_{m_2}))$ por lo tanto h es un morfismo de grupos.

Ahora si $h(\sigma_m) = 1 + n\mathbb{Z}$ entonces $m = 1 + nk$ para alguna $k \in \mathbb{Z}$ así

$$\sigma_m(x) = x^m = x^{1+nk} = x^1 x^{nk} = x(1)$$

y como $G = \langle x \rangle$ esto implica que σ_m es la función identidad, entonces $ker(h) = \{id_G\}$ por lo tanto h es monomorfismo.

Por último sea $k + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*$ entonces $(k,n) = 1$ por lo tanto $\exists\ \sigma_k \in Aut(G)$ tal que $h(\sigma_k) = k + n\mathbb{Z}$ y así h es un epimorfismo, concluimos que $Aut(G) \cong (\mathbb{Z}/n\mathbb{Z})^*$. □

2.2. Subgrupos Característicos

Para terminar este capítulo estudiaremos el concepto de subgrupo característico y algunas de sus propiedades más importantes.

Definición 2.11. *Sean $\varphi \in Aut(G)$ y $H \leq G$ decimos que φ fija a H si $\varphi(H) = H$.*

Notemos que si φ fija a H la restricción de φ a H es un automorfismo de H.

Definición 2.12. *Sea $L < Aut(G)$ decimos que $H \leq G$ es fijado por L si H es fijado por $\varphi,\ \forall \varphi \in L$.*

Observación 2.13. *Con esta terminología podemos ver que H es normal en G si y sólo si H es fijado por $Inn(G)$.*

Esto motiva la siguiente definición.

Definición 2.14. *Decimos que H es un subgrupo característico de G si H es fijado por $Aut(G)$.*

Ejemplo 2.15. *El centro $Z(G)$ es siempre un subgrupo característico en G pues si $x \in Z(G)$ y $\varphi \in Aut(G)$ $\varphi(x)y = \varphi(x\varphi^{-1}(y)) = \varphi(\varphi^{-1}(y)x) = y\varphi(x)$ $\forall y \in G$ por lo tanto $\varphi(x) \in Z(G)$ $\forall x \in Z(G),\ \forall \varphi \in Aut(G)$ y entonces $Z(G)$ es subgrupo característico en G.*

Es claro que si N es un subgrupo característico entonces es un subgrupo normal de G, pues si N es característico en G quiere decir que N es fijado por $Aut(G)$ y en particular es fijado por $Inn(G)$.

Ejemplo 2.16. *Consideremos $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(1,0),(0,1),(1,1)\}$ el grupo de Klein y sea $\tau : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ tal que*

$$\begin{aligned} \tau((0,1)) &= (1,0) \\ \tau((1,0)) &= (0,1) \\ \tau((0,0)) &= (0,0) \\ \tau((1,1)) &= (1,1) \end{aligned}$$

Por construcción tenemos que τ es una función bieyctiva y es fácil verificar que

$$\tau \in Aut(\mathbb{Z}_2 \times \mathbb{Z}_2),$$

ahora consideremos el subgrupo normal $N = \{(0,0),(1,0)\}$ *y calculemos* $\tau(N) = \{(0,0),(0,1)\}$, *esto implica que* τ *no fija a* N *por lo tanto no todos los subgrupos normales son característicos.*

El siguiente lema nos dice que ser característico es una propiedad transitiva.

Lema 2.17. *Si* K *es característico de* H *y* H *es un subgrupo característico de* G *entonces* K *es un subgrupo característico de* G.

Demostración. Si $\varphi \in Aut(G)$, entonces la restricción de φ a H es un elemento de $Aut(H)$ pues H es característico en G, y la restricción de φ a K es un elemento de $Aut(K)$ pues K es característico en H. Así $\forall\ \varphi \in Aut(G)$ φ fija a K y por lo tanto K es característico en G. □

Definición 2.18. *Sean* $x, y \in G$, *el conmutador de* x, y *se define como* $[x,y] = xyx^{-1}y^{-1}$ *y el subgrupo* G' *como* $G' = \langle\{[x,y] | x, y \in G\}\rangle$ *y lo llamamos el conmutador de* G.

Claramente G es abeliano si y sólo si $G' = \{1\}$ pues si G es abeliano entonces $xyx^{-1}y^{-1} = xx^{-1}yy^{-1} = 1(1)$ y esto implica que G' es $\{1\}$. Y si $G' = \{1\}$ entonces $xyx^{-1}y^{-1} = 1\ \forall x, y \in G$, de aquí tenemos que $xyx^{-1} = y$ o bien $xy = yx$ por lo tanto G es abeliano.

También es claro que si $H \leq G$, entonces $H' \leq G'$. Notemos que $\forall\ x, y \in G$ tenemos que $[x,y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y,x]$. Recordemos cómo son los elementos en el subgrupo generado por un conjunto:

Proposición 2.19. *Sea* G *un grupo y* $X \subseteq G$, *entonces* $\langle X\rangle$ *consiste de la identidad y todos los productos de la forma*
$x_1^{\varepsilon_1}...x_r^{\varepsilon_r}$, *donde* $r \in \mathbb{N}$, $x_i \in X$ *y* $\varepsilon_i = \pm 1\ \forall i$.

Con esta proposición podemos concluir que si $g \in G'$ entonces g es de la forma

$$g = [x_1, y_1]^{\varepsilon_1}...[x_r, y_r]^{\varepsilon_r}$$

es decir es un producto finito de conmutadores de elementos de G.

Lema 2.20. *Sea* G *un grupo, entonces* G' *es un subgrupo característico en* G.

Demostración. Sea $\varphi \in Aut(G)$. Tenemos que $\varphi([x,y]) = [\varphi(x), \varphi(y)]$ para cualquier $x, y \in G$, pues $\varphi([x,y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x^{-1})\varphi(y^{-1}) = [\varphi(x), \varphi(y)]$. Si $g \in G'$ entonces como vimos g es un producto de conmutadores y lo mismo se cumple para $\varphi(g)$ por lo mencionado al principio de la prueba. Asi $\varphi(g) \in G'$, esto implica que $\varphi(G') \leq G'$ análogamente tenemos que $\varphi^{-1}(G') \leq G'$ y entonces $\varphi(\varphi^{-1}(G')) \leq \varphi(G')$, es decir $G' \leq \phi(G')$. Por lo tanto $\varphi(G') = G'$. Por lo tanto G' es característico en G. □

Proposición 2.21. *Sea* G *un grupo y sea* $N \lhd G$. *Entonces* G/N *es abeliano si y sólo si* $G' \leq N$.

Demostración. Para cualesquiera $x, y \in G$, tenemos que $[xG', yG'] = [x,y]G' = G'$, pues $[xG', yG'] = xG'yG'x^{-1}G'y^{-1}G' = xyx^{-1}y^{-1}G' = [x,y]G' = G'$, entonces el conmutador de G/G' es trivial y por lo tanto G/G' es abeliano. Sea $N \lhd G$, si $G' \leq N$ por el tercer teorema de isomorfismo $G/N \cong (G/G')/(N/G')$ un cociente del grupo abeliano G/G' y por lo tanto G/N es abeliano. Ahora si G/N es abeliano entonces, para cualesquiera $x, y \in G$ tenemos que $(xN)(yN) = (yN)(xN)$ y esto implica que $xyN = yxN$ entonces $xy(yx)^{-1}N = N$ y por lo tanto $xy(x^{-1}y^{-1})N = N$, lo cual indica que $[x,y] \in N$ de donde obtenemos que $G' \leq N$.

□

Capítulo 3

Producto Directo

En este capítulo estudiaremos el producto directo externo de grupos y el producto directo interno de grupos, nos daremos cuenta que son conceptos equivalentes y estudiaremos algunas de sus propiedades mas importantes.

3.1. Producto Directo Externo

Definición 3.1. *Sea $\{G_i\}_{i=1}^n$ una familia de grupos. Consideremos el producto cartesiano $G_1 \times ... \times G_n$ y definimos una operación binaria como $(g_1, ..., g_n)(g_1', ..., g_n') = (g_1g_1', ..., g_ng_n')$, llamamos a $G_1 \times ... \times G_n$ con esta operación el producto directo externo de $G_1, ..., G_n$.*

Observación 3.2. *Si tenemos G un producto directo externo entonces:*

1. *Esta operación le da al producto cartesiano estructura de grupo, el elemento neutro es $(1, ..., 1)$ y el inverso de un elemento $(g_1, ..., g_n)$ es $(g_1^{-1}, ..., g_n^{-1})$.*

2. *Notemos que no importa en qué orden aparezca cada G_i pues si cambiamos el orden de los factores es fácil darnos cuenta que obtenemos un grupo isomorfo.*

A continuación definiremos los conceptos de inclusión y proyección, éstos nos servirán para estudiar algunas propiedades del producto directo.

Definición 3.3. *Consideremos $\{G_i\}_{i=1}^n$ una familia de grupos y G su producto directo externo.*

1. *Definimos la inclusión natural para cada i.*

$$inc_i : G_i \longrightarrow G$$

donde

$$inc_i(g_i) = (inc_i(g_i)_1, ..., inc_i(g_i)_i, ..., inc_i(g_i)_n),$$

para los cuales

$$inc_i(g_i)_j = \begin{cases} g_i \ si \ i = j \\ 1 \ si \ i \neq j \end{cases}$$

entonces quedaría de la siguiente forma

$$inc_i(g_i) = (1, ..., g_i, ..., 1).$$

2. *Definimos ahora la proyección natural*

$$proy_i : G \longrightarrow G_i$$

donde

$$proy_i((g_1, ..., g_i, ..., g_n)) = g_i.$$

Notación 3.4. *Al subgrupo de G imagen de inc_i lo denotamos*

$$G_i^* = inc_i(G_i)$$

Observación 3.5. *Dada una familia de grupos $\{G_i\}_{i=1}^n$ y G su producto directo externo. Es fácil darnos cuenta que para cada i la inclusión natural $inc_i : G_i \longrightarrow G$ es un monomorfismo de grupos y la proyección natural $proy_i : G \longrightarrow G_i$ es un epimorfismo de grupos. Esto implica que cada grupo G_i se puede ver como un subgrupo de G, pues*

$$G_i \cong G_i^* = inc_i(G_i) \leq G.$$

Entonces tenemos la familia $\{G_i^*\}_{i=1}^n$ de subgrupos en G.

Definición 3.6. *Sea $\{H_i\}_{i=1}^n$ una familia de subgrupos de un grupo G. El producto de dicha familia es el conjunto*

$$\prod_{i=1}^{n} H_i = H_1H_2...H_n = \{x \in G | x = h_1h_2...h_n | h_i \in H_i \ \forall i\}.$$

Para cada i consideramos el producto $H_{j\neq i} = H_1H_2...H_{i-1}\overline{H}_iH_{i+1}...H_n$, donde $\overline{H}_i = \{1\}$.

La siguiente proposición estudia el comportamiento de los subgrupos $inc_i(G_i) = G_i^*$ y motiva la definición de producto directo interno.

Proposición 3.7. *Si tenemos $\{G_i\}_{i=1}^n$ una familia de grupos y G su producto directo externo, entonces la familia $\{G_i^*\}_{i=1}^n$ de subgrupos de G tiene las siguientes propiedades.*

1. *Para cualquier i, se cumple que $G_i^* \trianglelefteq G$.*
2. *Para cualquier i, se cumple que $G_i^* \cap (\prod_{i\neq j} G_j^*) = \{1\}$.*
3. *$G = \prod_{i=1}^n G_i^*$.*

Demostración. 1. Sin pérdida de generalidad podemos suponer que $i = 1$. Si $x \in G_1^*$ y $g \in G$. Conjugamos

$$gxg^{-1} = (g_1, ..., g_n)(x_1, 1, ..., 1)(g_1^{-1}, g_2^{-1}, ..., g_n^{-1}) = (g_1xg_1^{-1}, 1, ..., 1),$$

es decir

$$gxg^{-1} = inc_1(gxg^{-1}) \in G_1^*,$$

obteniendo finalmente que $G_1^* \trianglelefteq G$.

2. Sin pérdida de generalidad podemos suponer que $i = 1$. Como

$$G_1^* = inc_1(G_1) = G_1 \times 1_{G_2} \times ... \times 1_{G_n},$$

entonces

$$\prod_{j\neq 1} G_j^* = 1_{G_1}inc_2(G_2)...inc_n(G_n) = 1_{G_1} \times G_2 \times ... \times G_n.$$

con esto concluimos que $G_1^* \cap (\prod_{j\neq 1})G_j^* = \{1\}$.

3. Sea $x \in G_1 \times ... \times G_n$ entonces $x = (g_1, ..., g_n) = (g_1, 1, ..., 1)...(1, ..., 1, g_n)$ de donde concluimos que $inc_1(G_1)...inc_n(G_n) = G_1 \times ... \times G_n$ y finalmente

$$\prod_{i=1}^{n} G_i^* = inc_1(G_1)...inc_n(G_n) = G_1 \times ... \times G_n = G.$$

□

3.2. Producto Directo Interno

A partir de la Proposición 3.7 podemos darnos cuenta que cualquier producto directo externo $G = G_1 \times ... \times G_n$, se puede descomponer en un producto $\prod_{i=1}^{n} G_i^*$ de subgrupos normales de G. Esto motiva la siguiente definición.

Definición 3.8. *Sea $\{H_i\}_{i=1}^n$ una familia de subgrupos normales de un grupo G. Se dice que G es el producto directo interno de $\{H_i\}_{i=1}^n$, si*

$$G = \prod_{i=1}^{n} H_i \ y \ H_i \cap (\prod_{i \neq j}^{n} H_j) = \{1\}, \forall \ i.$$

Observación 3.9. *Con base en la Definición 3.8 y la Proposición 3.7 tenemos que cualquier producto directo externo $G_1 \times ... \times G_n$ es el producto directo interno de la familia $\{G_i^*\}$ de subgrupos normales de G.*

Lema 3.10. *Si tenemos $\{H_i\}_{i=1}^n$ una familia de subgrupos normales de un grupo G, tal que $H_i \cap (\prod_{i \neq j}^{n} H_j) = \{1\}$, $\forall i$. Entonces si $i \neq j$, se tiene que $xy = yx$, $\forall x \in H_i$, $\forall y \in H_j$.*

Demostración. Sean $x \in H_i$ y $y \in H_j$ con $i \neq j$, consideremos el conmutador como en la Definición 2.18, ahora calculamos

$$[x, y] = xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in H_j$$

esta pertenencia se debe a que H_j es normal y análogamente

$$[x, y] = xyx^{-1}y^{-1} = x(yxy^{-1}) \in H_i.$$

Por lo tanto

$$[x, y] \in H_i \cap H_j \subseteq H_i \cap (\prod_{k \neq i} H_k) = \{1\}$$

y entonces $xy = yx$.

□

Teorema 3.11. *Sea $\{H_i\}_{i=1}^n$ una familia de subgrupos normales de un grupo G. Entonces las siguientes condiciones son equivalentes.*

1. *G es el producto directo interno de $\{H_i\}_{i=1}^n$.*
2. *Cada $g \in G$ se escribe de una única manera como el producto $g = h_1...h_n$, con $h_i \in H_i$.*
3. *$\sigma : \times_{i=1}^{n} H_i \longrightarrow G$, definida como $\sigma(h_1, ..., h_n) = h_1...h_n$, es un isomorfismo de grupos.*

Demostración. $1 \Rightarrow 2$
Dado que por hipótesis G es el producto directo interno de $\{H_i\}_{i=1}^n$ sabemos que cada $g \in G$ se escribe como un poducto $h_1...h_n$, falta ver que esta expresión es única. Para $i \neq j$, por el Lema 3.10 $xy = yx \ \forall \ x \in H_i, \ \forall \ y \in H_j$. Como $G = \prod_{i=1}^n H_i$, entonces $g = h_1...h_n$, con $h_i \in H_i$. Supongamos que

$$h_1...h_n = g = t_1...t_n \ donde \ h_i, t_i \in H_i \ \forall i.$$

Como los elementos de diferentes H_i conmutan

$$t_i^{-1}h_i = \prod_{j \neq i} t_j h_j^{-1}.$$

Así $t_i^{-1}h_i \in H_i \cap (\prod_{i \neq j}^n H_j) = \{1\}$, por lo que $t_i = h_i \ \forall i$.

$2 \Rightarrow 3$

Por el Lema 3.10 si probamos que

$$H_i \cap (\prod_{i \neq j}^{n} H_j) = \{1\}, \ \forall i \ entonces \ xy = yx \ \forall x \in H_i, \ y \in H_j.$$

Consideremos $g \in H_i \cap (\prod_{i \neq j}^n H_j)$, entonces $g = h_i = \prod_{i \neq j} h_j$ por lo que

$$1..,1h_i1..,1 = g = h_1...h_{i-1}h_{i+1}...h_n$$

y como la descomposición de g es única tenemos que $g = h_i = 1$. Entonces

$$xy = yx \ \forall x \in H_i, \ \forall \ y \in H_j.$$

Ahora verIfiquemos que σ es un morfismo de grupos:
Sean h, $h' \in \times_{i=1}^n H_i$ $h = (h_i, ..., h_n)$ y $h' = (h'_1, ..., h_n)$, calculamos

$$\sigma(hh') = \sigma(h_1h'_1, ..., h_nh'_n) = \prod_{i=1}^{n} h_ih'_i = \prod_{i=1}^{n} h_i \prod_{i=1}^{n} h'_i = \sigma(h)\sigma(h')$$

esto se cumple por la conmutatividad del producto entre elementos que pertenecen a distintos H_i. Obteniendo que σ es un morfismo de grupos.

Ahora supongamos que $\sigma(h) = \sigma(h')$ para $h = (h_1, ..., h_n)$ y $h' = (h'_1, ..., h'_n)$ esto implica que $h_1...h_n = h'_1...h'_n$ y por la unicidad de la expresión tenemos que $h_i = h'_i \ \forall \ i$ y por lo tanto $h = h'$ obteniendo que σ es monomorfismo de grupos.

Sea $g \in G$ como g tiene una descomposición Única $g = h_1...h_n$ entonces podemos considerar $h = (h_1, ..., h_n)$ y evidentemente $\sigma(h) = h_1...h_n = g$ por lo tanto σ es un epimorfismo, concluyendo finalmente que σ es un isomorfismo de grupos.

$3 \Rightarrow 1$

Para cada i se cumple que,

$$\sigma(H_i^*) = \sigma(inc_i(H_i)) = H_i.$$

Como σ es un isomorfismo de grupos, por la Proposición 3.7 tenemos que

$$G = \sigma(\times_{i=1}^{n} H_i) = \sigma(\prod_{i=1}^{n} H_i^*) = \prod_{i=1}^{n} \sigma(H_i^*) = \prod_{i=1}^{n} H_i.$$

y finalmente

$$H_i \cap (\prod_{j \neq i} H_j) = \sigma(H_i^*) \cap (\prod_{j \neq i} \sigma(H_j^*)) = \sigma(H_i^* \cap (\prod_{j \neq i} H_j^*)) = \{1\}$$

terminando la demostración del teorema. □

Observación 3.12. *De acuerdo con el Teorema 3.11 podemos concluir que el producto directo externo y el producto directo interno son conceptos equivalentes, a partir de esta observación sólo nos referiremos a estos 2 conceptos como producto directo y utilizaremos ambas notaciones para referirnos a él.*

A continuación revisaremos 2 ejemplos de cómo un producto directo externo induce un interno y al revés.

Ejemplo 3.13. *Sea $G = \mathbb{Z} \times \mathbb{Z}$, el producto directo externo de $\mathbb{Z}$ consigo mismo, ahora consideremos*

$$H_1 = \{0\} \times \mathbb{Z} \text{ y } H_2 = \mathbb{Z} \times \{0\}$$

es fácil verificar que G es producto directo interno de H_1 y H_2 y además

$$H_1 \cong \mathbb{Z} \text{ y } H_2 \cong \mathbb{Z}.$$

Ejemplo 3.14. *Consideremos el grupo $\mathbb{C}$ de números complejos con la operación de suma. Definimos*

$$i\mathbb{R} = \{z \in \mathbb{C} | Re(z) = 0\}$$

es fácil darnos cuenta que $\mathbb{C}$ es producto directo interno de $\mathbb{R}$ y $i\mathbb{R}$ y la correspondencia que manda a cada complejo $a + bi$ en (a, bi) es un isomorfismo de $\mathbb{C}$ en $\mathbb{R} \times i\mathbb{R}$. Por otro lado, $i\mathbb{R} \cong \mathbb{R}$, así entonces $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$.

3.3. Propiedades Generales del Producto Directo

Ahora presentaremos algunos resultados útiles de productos directos.

Proposición 3.15. *Sean $\{H_i\}_{i=n}^{n}$ y $\{G_i\}_{i=1}^{n}$ familias de grupos, $H = \prod_{i=1}^{n} H_i$ y $G = \prod_{i=1}^{n} G_i$. Si para cada i, se tiene que $H_i \trianglelefteq G_i$, entonces $H \trianglelefteq G$ y además $G/H \cong \prod_{i=1}^{n} G_i/H_i$.*

Demostración. Consideremos la función

$$\varphi : G \longrightarrow \prod_{i=1}^{n} G_i/H_i, \ \varphi((g_1, ..., g_n)) = (g_1H_1, ..., g_nH_n)$$

verfiquemos que φ es un epimorfismo de grupos, calculando

$$\begin{aligned} \varphi((g_1', ..., g_n')(g_1, ..., g_n)) &= \varphi((g_1'g_1, ..., g_n'g_n)) = (g_1'g_1H_1, ..., g_n'g_nH_n) \\ &= (g_1'H_1, ..., g_n'H_n)(g_1H_1, ..., g_nH_n) = \varphi(g_1', ..., g_n')\varphi(g_1, ..., g_n) \end{aligned}$$

entonces tenemos que φ es un morfismo de grupos. Ahora para cada

$$(g_1H_1, ..., g_nH_n) \in \prod_{i=1}^{n} G_i/H_i \ \exists \ (g_1, ..., g_n) \ tal \ que \ \varphi(g_1, ..., g_n) = (g_1H_1, ..., g_nH_n)$$

por lo tanto φ es un epimorfismo. Finalmente $\varphi(g_1, ..., g_n) = (H_1, ..., H_n)$ si y sólo si $g_i \in H_i \ \forall i$ por lo tanto $Ker\varphi = H$ y por el primer teorema de isomorfismo $G/H \cong \prod_{i=1}^{n} G_i/H_i$ y $H \trianglelefteq G$. □

Proposición 3.16. *Sea G un grupo con subgrupos normales H y K tales que $G = HK$ entonces $G/(H \cap K) \cong H/(H \cap K) \times K/(H \cap K)$.*

Demostración. Sabemos que $L = H \cap K$ es normal en G por ser intersección de grupos normales en G. Ahora por el teorema de la correspondencia tenemos que H/L y K/L son subgrupos normales de G/L, y claramente $(H/L) \cap (K/L) = \{1\}$ pues si $hL = kL$, con $h \in H, \ k \in K$, $h^{-1}k \in L = H \cap K$ entonces $h^{-1}k = \overline{h}$, para algún $\overline{h}$, así $k = h\overline{h} \in H$ y como además $k \in K$ $k \in H \cap K$.

Entonces sólo nos queda mostrar que $G/L = (H/L)(K/L)$. Sea $g \in G$ entonces $g = hk$ para algunas $h \in H$ y $k \in K$ pues $G = HK$ y entonces $gL = hkL = hLkL$ y éste es un elemento de $(H/L)(K/L)$ como se requiere, por lo tanto $G/L = (H/L)(K/L)$ donde éste es un producto directo interno. □

Proposición 3.17. *Sea $n \in \mathbb{N}$ y $n = p_1^{a_1}...p_r^{a_r}$ donde los p_i son primos distintos y a_i son enteros positivos, entonces tenemos que $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \times ... \times \mathbb{Z}_{p_r^{a_r}}$.*

Demostración. Sea $P_i = \langle x_i \rangle \cong \mathbb{Z}_{p_i^{a_i}}$ para cada $1 \leq i \leq r$ podemos ver fácilmente que el orden de $(x_1, ..., x_r) \in P_i \times ... \times P_r$ es $p_1^{a_1}...p_r^{a_r} = n$ y por lo tanto $P_1 \times ... \times P_r \cong \mathbb{Z}_n$. □

Ejemplo 3.18. *El producto de grupos cíclicos no es necesariamente un grupo cíclico. Sea $\mathbb{Z}_3 \times \mathbb{Z}_3$ es fácil verificar que cualquier elemento no trivial en $\mathbb{Z}_3 \times \mathbb{Z}_3$ tiene orden 3 esto implica que no es isomormo a $\mathbb{Z}_9$. De la Proposicion 3.17 se obtiene el siguiente corolario que nos da condiciones para que el producto de 2 grupos cíclcos sea un grupo cíclico.*

Corolario 3.19. *Si $(a, b) = 1$ entonces $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$.*

Lema 3.20. *Sea G un grupo finito con elementos $h, k \in G$, tales que $(o(h), o(k)) = 1$ y $hk = kh$. Entonces $\langle h \rangle \times \langle k \rangle \cong \langle hk \rangle$.*

Demostración. Por el corolario anterior tenemos que

$$\langle h \rangle \times \langle k \rangle \cong \mathbb{Z}_{o(h)} \times \mathbb{Z}_{o(k)} \cong \mathbb{Z}_{o(h)o(k)} \cong \mathbb{Z}_{o(hk)} \cong \langle hk \rangle$$

□

Proposición 3.21. *Supongamos que un grupo finito G es el producto directo de sus subgrupos H y K donde $(|H|, |K|) = 1$. Entonces cualquier subgrupo L de G es el producto directo interno de $L \cap H, L \cap K$.*

Demostración. Tenemos que $G = HK$ y $(|H|, |K|) = 1$. Sea $L \leq G$ observemos que $L \cap H \trianglelefteq L$, $L \cap K \trianglelefteq L$ y $(L \cap H) \cap (L \cap K) = 1$ pues H y K son normales en G y $H \cap K = 1$.

Ahora cualquier elemento $g \in L$ se puede escribir como $g = hk$ para algunas $h \in H$ y $k \in K$ y para mostrar que $L = (L \cap H)(L \cap K)$ es suficiente ver que $h, k \in L$, ahora como h y k conmutan entre sí en G por las propiedades del producto directo interno y sus órdenes son primos relativos pues $(|H|, |K|) = 1$, utilizando el lema 3.20 obtenemos que

$$\langle h \rangle \times \langle k \rangle \cong \langle hk \rangle \cong \langle g \rangle$$

en particular $\langle hk \rangle$ y $\langle h \rangle \langle k \rangle$ tienen el mismo orden. Así

$$\langle hk \rangle \leq \langle h \rangle \langle k \rangle$$

con ambos del mismo orden por lo cual

$$\langle hk \rangle = \langle h \rangle \langle k \rangle.$$

Finalmente $h, k \in \langle h \rangle \langle k \rangle = \langle hk \rangle =\leq L$ de donde $h, k \in L$ como se buscaba. Por lo tanto L es producto directo de $L \cap H$ y $L \cap K$. □

Ahora enunciaremos un corolario de la Proposición 3.21, la prueba de este corolario se hace por induccíon.

Corolario 3.22. *Supongamos que un grupo finito G es el producto directo de sus subgrupos $H_1, ..., H_n$ donde los órdenes $|H_i|$ son 2 a 2 primos relativos. Entonces cualquier subgrupo L de G es el producto directo interno de $L \cap H_1, ..., L \cap H_n$.*

Capítulo 4

Producto Semidirecto

En este capítulo estudiaremos el producto semidirecto interno y algunas de sus propiedades más importantes, después utilizando la teoría estudiada en el capítulo de automorfismos construiremos el producto semidirecto externo y veremos cuando estos 2 productos coinciden.

4.1. Producto Semidirecto Interno

Definición 4.1. *Sea G un grupo que tiene un subgrupo H y un subgrupo normal N tal que $G = NH$ y $N \cap H = 1$ decimos que G es el producto semidirecto interno de N por H y lo escribimos $G = N \rtimes H$.*

Notemos que en el producto directo interno todos los factores tienen que ser subgrupos normales del producto, en este caso sólo tenemos 2 factores y sólo uno debe ser subgrupo normal.

Observación 4.2. *Si tenemos $G = N \rtimes H$, entonces por el segundo teorema de isomorfismo $H = H/(N \cap H) \cong (NH)/N = G/N$ y si G es finito entonces $|G| = |N||G : N| = |N||H|$.*

En el capítulo anterior vimos que cada elemento en un producto directo tiene una única expresión como producto de factores en los subgrupos, en el caso del producto semidirecto interno tenemos una proposición análoga.

Proposición 4.3. *Sea $G = N \rtimes H$, $\forall\ x \in G$, x tiene una única expresión $x = nh$ con $n \in N$ y $h \in H$.*

Demostración. Sea $x \in G$ por definición de producto semidirecto interno $G = NH$ lo cual implica que $x = n_1h_1$ para algunos $n_1 \in N$ y $h_1 \in H$. Ahora supongamos que $n_1h_1 = n_2h_2$ con $n_2 \in N$ y $h_2 \in H$, entonces

$$n_2^{-1}n_1 = h_2h_1^{-1} \in N \cap H = 1$$

forzando a que $h_1 = h_2$ y $n_1 = n_2$. □

Observación 4.4. *Sea $G = N \rtimes H$, $h \in H$ y $\varphi_h \in Inn(G)$, notemos que*

1. *Como $N \trianglelefteq G$, se sigue que $\varphi_h(N) = N$, $\forall\ h \in H$*
2. *$\varphi_h \in Aut(N)$ (Proposición 2.3)*
3. *$\varphi_h \circ \varphi_{h'} = \varphi_{hh'}$ (Proposición 2.6)*

Definición 4.5. *Sea $G = N \rtimes H$ definimos $\varphi : H \longrightarrow Aut(N)$, donde $\varphi(h) = \varphi_h$.*

Observación 4.6. *Es fácil verificar que $\varphi : H \longrightarrow Aut(N)$, $\varphi(h) = \varphi_h$ es un morfismo de grupos, a este morfismo lo llamamos el morfismo conjugación del producto semidirecto $N \rtimes H$.*

Corolario 4.7. *Sea $G = N \rtimes H$, $n \in H$ y φ el morfismo conjugación. Entonces*

$$n_1h_1n_2h_2 = n_1\varphi(h_1)(n_2)h_1h_2$$

para cualesquiera $n_1, n_2 \in N$ y $h_1, h_2 \in H$

Demostración. Calculamos

$$n_1\varphi(h_1)(n_2)h_1h_2 = n_1h_1n_2h_1^{-1}h_1h_2 = n_1h_1n_2h_2$$

□

Observación 4.8. *Gracias al corolario anterior podemos concluir que las operaciones en $N \rtimes H$ pueden ser expresadas en términos de las operaciones de N, H y el morfismo φ.*

Proposición 4.9. *Sea $G = N \rtimes H$ si $\varphi : H \longrightarrow Aut(N)$ es trivial, entonces $H \trianglelefteq G$ y $G = N \times H$. Y a la inversa si $\forall n \in N$ y $\forall h \in H$ se cumple que $nh = hn$ entonces el morfismo conjugación φ es trivial.*

Demostración. Como $\varphi : H \longrightarrow Aut(N)$ es trivial entonces $\varphi(h) = \varphi_h = Id_N$ $\forall h \in H$ esto implica que $\varphi(h)(n) = hnh^{-1} = n$ lo cual implica que h y n conmutan para toda n y h se sigue que si tenemos $ghg^{-1} = n_1h_1h(n_1h_1)^{-1} = n_1h_1hh_1^{-1}n_1^{-1} = n_1n_1^{-1}h_1hh_1^{-1} = h_1hh_1^{-1} \in H$ por lo tanto $H \trianglelefteq G$ y como $G = NH$ y $N \cap H = \{1\}$ entonces $G = N \times H$.

Ahora suponemos que $nh = hn$ $\forall n \in N$ y $\forall h \in H$ entonces $n = hnh^{-1} = \varphi_h(n)$ con esto concluimos que $\varphi_h = Id_N$ $\forall h \in H$ por lo tanto φ es trivial.

□

Observación 4.10. *Si $\varphi : H \longrightarrow Aut(N)$ no es trivial, entonces G sería no abeliano ya que para algunos $h \in H$ y $n \in N$ $hnh^{-1} = \varphi(h)(n) \neq n$ y en este caso n y h no conmutan. En términos de la proposición anterior podemos ver que el producto directo es un caso particular del producto semidirecto. Con los resultados anteriores hemos reunido la suficiente información para definir el producto semidirecto de 2 grupos cualesquiera.*

4.2. Producto Semidirecto Externo

Definición 4.11. *Sean N y H grupos y sea φ un morfismo de H en $Aut(N)$, definimos una operación binaria en $N \times H$ por $(n_1, h_1)(n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1h_2)$. Llamamos a este conjunto el producto semidirecto externo de N por H correspondiente a φ, y lo denotamos $N \rtimes_\varphi H = G$.*

Observación 4.12. *$G = N \rtimes_\varphi H$ tiene estructura de grupo donde el elemento identidad es $(1, 1)$ y el inverso de (n, h) es $(\varphi(h^{-1})(n^{-1}), h^{-1})$ pues*

$$\begin{aligned}(n, h)(\varphi(h^{-1})(n^{-1}), h^{-1}) &= (n(\varphi(h)(\varphi(h^{-1})(n^{-1})), hh^{-1}) \\ &= (nId_N(n^{-1}), 1) \\ &= (nn^{-1}, 1) = (1, 1).\end{aligned}$$

Notemos que cuando φ es trivial el inverso de (n,h) es (n^{-1},h^{-1}) y $(n_1,h_1)(n_2,h_2) = (n_1\varphi(h_1)(n_2),h_1h_2) = (n_1n_2,h_1h_2)$ de donde se sigue que el producto directo y el semidirecto externo coinciden sólo cuando φ es trivial.

Observación 4.13. *Si tenemos el producto semidirecto externo $N \rtimes_\varphi H$ y $H_1 \leq H$, consideramos el morfismo $\varphi|_{H_1} : H_1 \longrightarrow Aut(N)$ la restricción de φ a H_1. Entonces tendríamos un producto semidirecto $N \rtimes_{\varphi|_{H_1}} H_1$ donde $N \rtimes_{\varphi|_{H_1}} H_1 \leq N \rtimes_\varphi H$, pues es claro que $N \rtimes_{\varphi|_{H_1}} H_1$ es cerrado y para cada $(n,h_1) \in N \rtimes_{\varphi|_{H_1}} H_1$ tenemos que $(\varphi(h^{-1})(n^{-1}),h^{-1}) \in N \rtimes_{\varphi|_{H_1}} H_1$ pues $H_1 \leq H$. Entonces teniendo un producto semidirecto $N \rtimes_\varphi H$ podemos construir mas productos semidirectos a partir de subgrupos de H.*

Proposición 4.14. *Sean N_1, N_2, H_1 y H_2 grupos tales que $N_1 \cong N_2$ y $H_1 \cong H_2$ y $\varphi : H_1 \longrightarrow Aut(N_1)$ un morfismo de grupos, entonces $N_1 \rtimes_\varphi H_1 \cong N_2 \rtimes_{\widetilde{\varphi}} H_2$ para algún morfismo $\widetilde{\varphi} : H_2 \longrightarrow Aut(N_2)$.*

Demostración. Verifiquemos primero que $Aut(N_1) \cong Aut(N_2)$. Como $N_1 \cong N_2$ y $H_1 \cong H_2$, existen $f : N_1 \longrightarrow N_2$ y $g : H_1 \longrightarrow H_2$ isomorfismos. Sea $\Xi : Aut(N_2) \longrightarrow Aut(N_1)$ donde si $\sigma \in Aut(N_2)$ entonces $\Xi(\sigma) = f^{-1}\sigma f$, observemos que efectivamente $f^{-1}\sigma f \in Aut(N_1)$ pues f y σ son isomorfismos. Es fácil darnos cuenta que Ξ es un isomorfismo de grupos ya que la función que manda cada $\gamma \in Aut(N_1)$ en $f\gamma f^{-1}$ es su inversa. A partir de esto podemos definir $\widetilde{\varphi} : H_2 \longrightarrow Aut(N_2)$ como $\widetilde{\varphi}(h_2) = (\Xi^{-1} \circ \varphi \circ g^{-1})(h_2)$.

Ahora veamos que $N_1 \rtimes_\varphi H_1 \cong N_2 \rtimes_{\widetilde{\varphi}} H_2$. Sea $(n,h) \in N_1 \rtimes_\varphi H_1$ definimos

$$\Upsilon : N_1 \rtimes_\varphi H_1 \longrightarrow N_2 \rtimes_{\widetilde{\varphi}} H_2$$

Como $\Upsilon((n,h)) = (f(n),g(h))$, verifiquemos que Υ es un morfismo de grupos, calculemos

$$\begin{aligned}\Upsilon((n,h)(n',h')) &= \Upsilon(n\varphi(h)(n'),hh') \\ &= (f((n)\varphi(h)(n')),g(hh')) \\ &= (f(n)f(\varphi(h)(n')),g(h)g(h'))\end{aligned}$$

Por otro lado calculamos

$$\begin{aligned}\Upsilon((n,h))\Upsilon((n',h')) &= ((f(n),g(h))(f(n'),g(h')) \\ &= (f(n)\widetilde{\varphi}(g(h))f(n'),g(h)g(h')) \\ &= (f(n)(\Xi^{-1} \circ \varphi \circ g^{-1})(g(h))(f(n')),g(h)g(h')) \\ &= (f(n)(\Xi^{-1} \circ \varphi)(h)(f(n')),g(h)g(h')) \\ &= (f(n)(\Xi^{-1}(\varphi(h))(f(n')),g(h)g(h')) \\ &= (f(n)((f\varphi(h)f^{-1})(f(n')),g(h)g(h')) \\ &= (f(n)f(\varphi(h)(n')),g(h)g(h'))\end{aligned}$$

Por lo tanto $\Upsilon((n,h)(n',h')) = \Upsilon((n,h))\Upsilon((n',h'))$ y Υes un morfismo de grupos, como Υ está definido a partir de los isomorfismos f y g entonces es fácil concluir que Υ es un isomorfismo de grupos. Y por lo tanto $N_1 \rtimes_\varphi H_1 \cong N_2 \rtimes_{\widetilde{\varphi}} H_2$

□

Cuando estudiamos el producto directo externo vimos que para cada factor G_i del producto tenemos un G_i^* subgrupo del producto tal que $G_i \cong G_i^*$ y que el producto directo externo es igual al producto directo interno de todos los G_i^*. Para el producto semidirecto tenemos una propiedad análoga, la cual empezaremos a estudiar con la siguiente definición.

Definición 4.15. *Dado $G = N \rtimes_\varphi H$. Definimos la inclusión de N en G como*

$$inc : N \longrightarrow N \rtimes_\varphi H,\ inc(n) = (n, 1)$$

Observación 4.16. *Notemos que la inclusión de N es morfismo de grupos pues*

$$\begin{aligned} inc(n_1)inc(n_2) &= (n_1, 1)(n_2, 1) \\ &= (n_1\varphi(1)(n_2), 1) \\ &= (n_1(n_2), 1) \\ &= inc(n_1n_2). \end{aligned}$$

Notación 4.17. *Al subgrupo imagen $inc(N)$ lo llamamos N^* y además se cumple que*

$$N^* = inc(N) = N \times \{1\}$$

Ahora definiremos la inclusión de H.

Definición 4.18. *Dado $G = N \rtimes_\varphi H$. Definimos la inclusión de H en G como*

$$inc : H \longrightarrow N \rtimes_\varphi H,\ inc(h) = (1, h)$$

Observación 4.19. *Notemos que la inclusión de H es un morfismo de grupos pues*

$$inc(h_1)inc(h_2) = (1, h_1)(1, h_2) = (1\varphi(h_1)(1), h_1h_2) = (1(1), h_1h_2) = inc(h_1h_2)$$

Notación 4.20. *Al subgrupo imagen $inc(H)$ lo llamamos H^* y además se cumple que*

$$H^* = inc(H) = \{1\} \times H$$

La siguiente proposición nos dice que cada producto semidirecto externo induce un producto semidirecto interno.

Proposición 4.21. *Sea $G = N \rtimes_\varphi H$, los subgrupos $N^* = N \times \{1\}$ y $H^* = \{1\} \times H$ son isomorfos a N y H respectivamente, $N^* \trianglelefteq G$, $G = N^*H^*$ y $N^* \cap H^* = \{(1, 1)\}$.*

Demostración. Sean $(x, 1) \in N'$ y $(n, h) \in G$, calculando tenemos que

$$\begin{aligned} (n, h)(x, 1)(n, h)^{-1} &= (n\varphi(h)(x), h)(\varphi(h^{-1})(n^{-1}), h^{-1}) \\ &= (n\varphi(h)(x)\varphi(h)(\varphi(h^{-1})(n^{-1})), hh^{-1}) \\ &= (n\varphi(h)(x)n^{-1}, 1) \in N^*. \end{aligned}$$

Por lo tanto $N^* \trianglelefteq G$. Ahora si tenemos $(n, h) \in G$, entonces $(n, h) = (n\varphi(1)(1), h) = (n, 1)(1, h)$ para cualquier $(n, h) \in G$ y por lo tanto $G = N^*H^*$ y si $(n, h) \in N^* \cap H^*$ entonces $n = 1$ y $h = 1$ y por lo tanto $N^* \cap H^* = \{(1, 1)\}$. □

Observación 4.22. *De la proposición anterior podemos concluir que $G = N \rtimes_\varphi H$ es producto semidirecto interno de N^* por H^*. Esta estructura de grupo generalmente difiere de la de producto directo, pues en ésta los elementos de N^* y H^* no conmutan entre sí a menos que φ sea trivial, lo cual nos dice que $G = N \rtimes_\varphi H$ es abeliano sólo si φ es trivial.*

Observación 4.23. *Sea $G = N \rtimes H$, $g \in G$ y $\varphi(h) = \varphi_h \ \forall h \in H$, definimos $\kappa : N \rtimes H \longrightarrow N \rtimes_\varphi H$, $\kappa(g) = \kappa(nh) = (n, h)$ entonces:*

$$\begin{aligned}\kappa(n_1h_1)\kappa(n_2h_2) &= (n_1, h_1)(n_2, h_2)\\ &= (n_1\varphi(h_1)(n_2), h_1h_2)\end{aligned}$$

Por el Corolario 4.7 κ es un morfismo de grupos, y por la definición de κ es facil verificar que es un isomorfismo de grupos. En conclusión un producto semidirecto interno induce uno externo donde el φ correspondiente es un automorfismo interno.

4.3. Propiedades Generales del Producto Semidirecto

A continuación revisaremos algunas propiedades importantes del producto semidirecto.

Teorema 4.24. *Sea H un grupo cíclico y sea N un grupo cualquiera. Si φ y ψ son monomorfismos de H a $Aut(N)$ tales que $\varphi(H) = \psi(H)$, entonces $N \rtimes_\varphi H \cong N \rtimes_\psi H$.*

Demostración. Sea $H = \langle x\rangle$, como $\varphi(H) = \psi(H)$ veremos que $\varphi(x)$ y $\psi(x)$ generan el mismo subgrupo cíclico de $Aut(N)$. Como $\varphi(H) = \psi(H)$ entonces $\varphi(\langle x\rangle) = \psi(\langle x\rangle)$ y como $\varphi(\langle x\rangle) = \langle\varphi(x)\rangle$ y $\psi(\langle x\rangle) = \langle\psi(x)\rangle$ entonces $\langle\varphi(x)\rangle = \langle\psi(x)\rangle$ y así concluimos que generan el mismo subgrupo cíclico.

Notemos que

$$\psi(x) = (\varphi(x))^a = \varphi(x^a)$$

para alguna $a \in \mathbb{Z}$ y análogamente

$$\varphi(x) = (\psi(x))^b = \psi(x^b)$$

para alguna $b \in \mathbb{Z}$.

También notemos que para cualquier $h \in H$, como $h = x^m$ para alguna $m \in \mathbb{Z}$ se cumple que

$$\psi(h) = \psi(x^m) = (\psi(x))^m = \varphi(x^a)^m = \varphi(h^a)$$

y que

$$\varphi(h) = \varphi(x^m) = (\varphi(x))^m = (\psi(x^b))^m = \psi(m^b)$$

Ahora definimos $T : N \rtimes_\psi H \longrightarrow N \rtimes_\varphi H$ como $T(n, h) = (n, h^a)$. Entonces calculando

$$\begin{aligned}T((n_1, h_1)(n_2,h_2)) &= T((n_1\psi(h_1)(n_2), h_1h_2))\\ &= (n_1\psi(h_1)(n_2), (h_1h_2)^a)\\ &= (n_1\varphi(h_1^a)(n_2), h_1^ah_2^a)\\ &= (n_1, h_1^a)(n_2, h_2^a)\\ &= T(n_1, h_1)T(n_2, h_2).\end{aligned}$$

Lo que muestra que T es un morfismo de grupos. Análogamente podemos mostrar que $\lambda : N \rtimes_\varphi H \longrightarrow N \rtimes_\psi H$ definido por $\lambda(n, h) = (n, h^b)$ es un morfismo de grupos. Para terminar

es suficiente mostrar que T y λ son inversas. La función $T \circ \lambda$ manda $(n, h) \in N \rtimes_\varphi H$ a (n, h^{ab}). Pero $\varphi(x) = \psi(x)^b = (\varphi(x)^a)^b = \varphi(x^{ab})$ y φ es inyectiva entonces $x^{ab} = x$ y así $h^{ab} = h$ para cualquier $h \in H$. Entonces $T \circ \lambda$ es la función identidad en $N \rtimes_\varphi H$ y análogamente $\lambda \circ T$ es la identidad en $N \rtimes_\psi H$ como se busca. Por lo tanto $N \rtimes_\varphi H \cong N \rtimes_\psi H$.

□

Teorema 4.25. *Sean N y H grupos y sea $\psi : H \longrightarrow Aut(N)$ un morfismo y $f \in Aut(N)$. Si f' es el automorfismo interno de $Aut(N)$ inducido por f, es decir, $f' = f\varsigma f^{-1}$, con $\varsigma \in Aut(N)$ entonces $N \rtimes_{f'\circ\psi} H \cong N \rtimes_\psi H$.*

Demostración. Definimos $\theta : N \rtimes_\psi H \longrightarrow N \rtimes_{f'\circ\psi} H$ por $\theta(n, h) = (f(n), h)$ y tenemos lo siguiente:

$$\begin{aligned}
\theta((n_1, h_1)(n_2, h_2)) &= \theta(n_1\psi(h_1)(n_2), h_1h_2) \\
&= (f(n_1)f(\psi(h_1)(n_2)), h_1h_2) \\
&= (f(n_1)(f \circ \psi(h_1) \circ f^{-1} \circ f)(n_2), h_1h_2) \\
&= (f(n_1)(f' \circ \psi)(h_1)(f(n_2)), h_1h_2) \\
&= (f(n_1), h_1)(f(n_2), h_2) \\
&= \theta(n_1, h_1)\theta(n_2, h_2),
\end{aligned}$$

lo que muestra que θ es un morfismo de grupos pero el morfismo que manda $(n, h) \in N \rtimes_{f'\circ\psi} H$ a $(f^{-1}(n), h) \in N \rtimes_\psi H$ es inverso de θ y por lo tanto θ es isomorfismo.

□

Ejemplo 4.26. *Sea N un grupo, $G = N \times_\varphi Aut(N)$ es un producto semidirecto donde*

$$\varphi : Aut(N) \longrightarrow Aut(N)$$

es un morfismo de grupos y la operación en G esta dada por

$$(n, \sigma)(m, \tau) = (n\varphi(\sigma)(m), \sigma\tau)$$

donde $n, m \in N$ y $\sigma, \tau \in Aut(N)$, y el inverso de un elemento $(n, \sigma) \in G$ es el elemento $(\sigma^{-1}(\varphi^{-1}(n^{-1})), \sigma^{-1})$. Notemos que cuando φ es la función identidad G es un producto directo de N con $Aut(N)$.

Ejemplo 4.27. *Sea $N = \mathbb{Z}_n$ y sea $H = \mathbb{Z}_2$ con $\varphi : H \longrightarrow Aut(N)$ la función que manda el generador de H en el automorfismo que manda a cada elemento en su inverso. El grupo $N \rtimes_\varphi H$ es el grupo diédrico de orden $2n$.*

$N \rtimes_\varphi H$ tiene $2n$ elementos pues sus elementos son de la forma $(k, 0)$ y $(k, 1)$ donde $k \in \mathbb{Z}_n$ y de cada uno de estos hay n. Ahora veamos que es isomorfo a D_n, observando primero que los elementos $(1, 1)$ y $(1, 0)$, de orden 2 y n respectivamente, lo generan.

Veamos que cualquier elemento de $N \rtimes_\varphi H$ se puede expresar en términos de $(1, 1)$ y $(1, 0)$, si calculamos

$$\begin{aligned}
(1, 0)^2 &= (1, 0)(1, 0) = (1 + \varphi(0)(1), 0 + 0) = (1 + 1, 0) = (2, 0) \\
(1, 0)^3 &= (2, 0)(1, 0) = (2 + \varphi(0)(1), 0 + 0) = (2 + 1, 0) = (3, 0) \\
(1, 0)^4 &= (3, 0)(1, 0) = (3 + \varphi(0)(1), 0 + 0) = (3 + 1, 0) = (4, 0)
\end{aligned}$$

Entonces $(1,0)^k = (k,0)$. *Ahora calculemos*

$$\begin{aligned}(1,0)^{k-1}(1,1) &= (k-1,0)(1,1) = (k-1+\varphi(0)(1), 1+0)\\ &= (k-1+1,1)\\ &= (k,1)\end{aligned}$$

Entonces $N \rtimes_\varphi H$ *tiene 2 generadores* $(1,0)$ *y* $(1,1)$ *de orden* 2 *y* n *respectivamente sólo falta verificar que* $(1,1)(1,0)(1,1) = (1,0)^{-1}$. *Calculemos* $(1,1)(1,0)(1,1)$

$$\begin{aligned}(1,1)(1,0)(1,1) &= (1,1)(1+\varphi(0)(1), 0+1) = (1,1)(1+1,1)\\ &= (1,1)(2,1)\\ &= (1+\varphi(1)(2), 1+1) = (1+n-2,0)\\ &= (n-1,0)\end{aligned}$$

Y como $(1,0)(n-1,0) = (1+\varphi(0)(n-1), 0+0) = (1+n-1,0) = (0,0)$ *entonces* $(1,1)(1,0)(1,1) = (1,0)^{-1}$. *Por lo tanto* $N \rtimes_\varphi H \cong D_n$.

Capítulo 5

Producto Trenzado

En este capítulo construiremos y estudiaremos el producto trenzado de grupos, éste es un caso particular del producto semidirecto, donde uno de los factores es un producto directo de copias de un solo grupo. Comencemos con la siguiente proposición que nos ayudará a entender cómo funcionará nuestro nuevo producto.

5.1. Construcción del Producto Trenzado

Proposición 5.1. *Sean N y H grupos donde H actúa sobre un conjunto $\Omega \neq \emptyset$. Se cumplen las siguientes propiedades.*

1. *Si tenemos $\prod_{\omega\in\Omega} N_\omega$ (el producto directo de copias de N, tantas como elementos en Ω), la acción de H sobre Ω induce una acción de H en $\prod_{\omega\in\Omega} N_\omega$.*

2. *Para cada $h \in H$ definimos una función $f_h : \Pi_{w\in\Omega} N_\omega \longrightarrow \Pi_{\omega\in\Omega} N_\omega$, donde $f_h(n_\omega) = (n_{h\omega})$. Entonces $f_h \in Aut(\prod_{\omega\in\Omega} N_\omega)$.*

3. *La función $\Phi : H \longrightarrow Aut(\prod_{\omega\in\Omega} N_\omega)$, dada por $\Phi(h) = f_h$, es un morfismo de grupos.*

Demostración. 1. Si $h \in H$ y $(n_\omega) \in \prod_{\omega\in\Omega} N_\omega$, la acción se define como $h(n_\omega) = (n_{h\omega})$ donde $h\omega$ se obtiene usando la acción de H sobre Ω. Verifiquemos que efectivamente es una acción:

Sea $1 \in H$ y $(n_\omega) \in \prod_{\omega\in\Omega} N_\omega$, $1(n_\omega) = (n_{1\omega}) = (n_w)$ pues $1\omega = \omega\ \forall\omega \in \Omega$, porque H actúa en Ω. Ahora si $g, h \in H$ y $(n_\omega) \in \prod_{\omega\in\Omega} N_\omega$ calculando

$$g(h(n_\omega)) = g(n_{h\omega}) = (n_{g(h\omega)}) = (n_{(gh)\omega}) = (gh)(n_\omega).$$

Por lo tanto tenemos que H actúa sobre $\prod_{\omega\in\Omega} N_\omega$ a través de la acción de H sobre Ω.

2. Primero veamos que f_h es un morfismo de grupos, calculamos, $(n_\omega)(m_\omega) = (n_\omega m_\omega) = (t_\omega)$ y aplicamos f_h.
$$f_h((n_\omega)(m_\omega)) = f_h((n_\omega m_\omega)) = f_h(t_\omega) = (t_{h\omega})$$
y por otro lado

$$f_h(n_\omega)f_h(m_\omega) = (n_{h\omega})(m_{h\omega}) = (t_{h\omega})$$

por lo tanto f_h es un morfismo de grupos.

Ahora si $f_h(n_\omega) = (1)$ esto implica que $(n_{h\omega}) = (1)$, pero sabemos que

$$(n_\omega) = Id(n_\omega) = (f_{h^{-1}} \circ f_h)(n_\omega) = h^{-1}(h(n_\omega)) = h^{-1}(1) = (1),$$

es decir $n_\omega = 1$ para toda $\omega \in \Omega$ y por lo tanto f_h es monomorfismo de grupos. Sea $(n_\omega) \in \Pi_{\omega\in\Omega} N_\omega$ y $h, h^{-1} \in H$, calculamos

$$f_h(f_{h^{-1}}(n_\omega)) = (f_h \circ f_{h^{-1}})(n_\omega) = (hh^{-1})(n_\omega) = (n_{hh^{-1}w}) = (n_\omega)$$

por lo tanto f_h es un epimorfismo y así $f_h \in Aut(\prod_{\omega\in\Omega} N_\omega)$.

3. Calculando

$$\begin{aligned}\Phi(h_1h_2)(n_\omega) &= f_{h_1h_2}(n_\omega)\\ &= (n_{(h_1h_2)\omega})\\ &= (n_{h_1(h_2\omega)})\\ &= f_{h_1}(n_{h_2\omega})\\ &= f_{h_1}(f_{h_2}(n_\omega))\\ &= (f_{h_1} \circ f_{h_2})(n_\omega)\end{aligned}$$

para toda $(n_\omega) \in \prod_{\omega\in\Omega} N_\omega$, así $\Phi(h_1h_2) = f_{h_1} \circ f_{h_2} = \Phi(h_1) \circ \Phi(h_2)$ y con esto concluimos que Φ es un morfismo de grupos.

□

Esta proposición motiva de manera natural la siguiente definición.

Definición 5.2. *Al producto semidirecto externo $\prod_{\omega\in\Omega} N_\omega \rtimes_\Phi H$ lo llamamos el producto trenzado de N por H y lo escribimos de la forma $N \wr_\Omega H$.*

Ejemplo 5.3. *Sea $\mathbb{Z}_2$ y $\Omega = \{0,1\}$, tenemos que $\prod_{\omega\in\Omega}(\mathbb{Z}_2)_\omega = \mathbb{Z}_2 \times \mathbb{Z}_2$ y que $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{K}$ con $\mathbb{K}$ es el grupo de Klein, $\mathbb{K} = \{(0,0),(0,1),(1,0),(1,1)\}$, donde*

$$(0,1) + (0,1) = (1,0) + (1,0) = (0,0) \text{ y } (0,1) + (1,0) = (1,1) = (1,0) + (0,1).$$

$\mathbb{Z}_2$ actúa sobre Ω con la operación de suma de $\mathbb{Z}_2$ y $\mathbb{Z}_2$ actúa sobre $\mathbb{K} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ de la siguiente forma

$$\begin{aligned}0((0,0)) &= (0,0)\\ 0((1,0)) &= (1,0)\\ 0((0,1)) &= (0,1)\\ 0((1,1)) &= (1,1)\end{aligned}$$

y

$$\begin{aligned}1((0,0)) &= (0,0)\\ 1((1,0)) &= (0,1)\\ 1((0,1)) &= (1,0)\\ 1((1,1)) &= (1,1)\end{aligned}$$

De esta manera si $z \in \mathbb{Z}_2$, $\Phi(z) = \Phi(0) = Id_\mathbb{K}$ ó $\Phi(z) = \Phi(1)$ donde $\Phi(1)(k) = (1)(k)$ con $k \in \mathbb{K}$. Entonces $\mathbb{Z}_2 \wr_\Omega \mathbb{Z}_2 = \mathbb{K} \rtimes_\Phi \mathbb{Z}_2$, y sus elementos son:

$$\mathbb{Z}_2 \wr_\Omega \mathbb{Z}_2 = \{((1,0),0),\ ((1,0),1),\ ((0,1),0),\ ((0,1),1),\ ((1,1),0),\ ((1,1),1),\ ((0,0),0)\ ,((0,0),1)\}$$

De aquí vemos que $\mathbb{Z}_2 \wr_\Omega \mathbb{Z}_2$ *tiene 8 elementos, ahora veremos que* $\mathbb{Z}_2 \wr_\Omega \mathbb{Z}_2 \cong D_4$ *el grupo diédrico de orden 8. Recordemos que* D_4 *es el grupo formado por las simetrías del cuadrado y sabemos que está generado por 2 elementos, uno de orden 4 (rotación) y uno de orden 2 (reflexión) veamos que* $((0,1),0)$ *es de orden 2 y que* $((0,1),1)$ *es de orden 4. Calculamos.*

$$\begin{aligned}((0,1),0)^2 &= ((0,1),0)((0,1),0)\\ &= ((0,1)\Phi(0)((0,1)),0+0)\\ &= ((0,1)+(0,1),0)\\ &= ((0,0),0)\end{aligned}$$

$$\begin{aligned}((0,1),1)^2 &= ((0,1),1)((0,1),1)\\ &= ((0,1)\Phi(1)((0,1)),1+1)\\ &= ((0,1)+(1,0),0)\\ &= ((1,1),0)\end{aligned}$$

$$\begin{aligned}((0,1),1)^3 &= ((0,1),1)^2((0,1),1)\\ &= ((1,1),0)((0,1),1)\\ &= ((1,1)\Phi(0)((0,1)),0+1)\\ &= ((1,0),1)\end{aligned}$$

Finalmente

$$\begin{aligned}((0,1),1)^4 &= ((0,1),1)^3((0,1),1)\\ &= ((1,0),1)((0,1),1)\\ &= ((1,0)\Phi(1)((0,1)),1+1)\\ &= ((0,0),0)\end{aligned}$$

Con esto concluimos que $((0,1),0)$ *y* $((0,1),1)$ *son de orden 2 y 4 respectivamente. Hasta el momento con* $((0,1),0)$ *y* $((0,1),1)$ *hemos generado* $((1,1),0)$, $((1,0),1)$, $((0,0),0)$ *y* $((0,0),1)$ *con esto tenemos 6 de los 8 elementos de* D_4*, pongamos los demás en términos de* $((0,1),0)$ *y* $((0,1),1)$. *Calculamos*

$$\begin{aligned}((0,1),0)((0,1),1)^2 &= ((0,1),0)((1,1),0)\\ &= ((0,1)\Phi(0)((1,1)),0+0)\\ &= ((1,0),0)\end{aligned}$$

y por último

$$\begin{aligned}((0,1),0)((0,1),1)^3 &= ((0,1),0)((1,0),1)\\ &= ((0,1)\Phi(0)((1,0)),0+1)\\ &= ((1,1),1).\end{aligned}$$

Sólo falta verificar que los generadores $((0,1),0)$ *y* $((0,1),1)$ *cumplen la siguiente relación* $((0,1),0)((0,1),1) = ((0,1),1)^3((0,1),0)$*, calculamos*

$$\begin{aligned}((0,1),0)((0,1),1) &= ((0,1)\Phi(0)(0,1),0+1)\\ &= ((0,1)+(1,0),1) = ((0,0),1)\end{aligned}$$

y ahora

$$\begin{aligned}((0,1),1)^3((0,1),0) &= ((1,0),1)((0,1),0)\\ &= ((1,0)\Phi(1)(0,1),1+0)\\ &= ((1,0)+(1,0),1)\\ &= ((0,0),1)\end{aligned}$$

Con esto concluimos que $\mathbb{Z}_2 \wr_\Omega \mathbb{Z}_2 \cong D_4$.

Ejemplo 5.4. *Sea* Γ *la gráfica 5.1*[1] *consideremos* $h \in Aut(\Gamma)$[2]*, sabemos que* $h(\theta) = \theta \ \forall \ h \in Aut(\Gamma)$ *pues el grado*[3] *de los vértices se preserva bajo automorfismos y* θ *es el único vértice de grado 5. También si* $i \in \{\alpha, \beta, \gamma, \delta, \varepsilon\}$ *y* $h(i) = j$, $j \in \{\alpha, \beta, \gamma, \delta, \varepsilon\}$ *pues* $\alpha, \beta, \gamma, \delta, \varepsilon$ *son los únicos vértices que tienen grado 2, por último si* $h(i) = j$ *entonces* $h(a_i) = b_j$ *y* $h(b_i) = a_j$ *ó* $h(a_i) = a_j$ *y* $h(b_i) = b_j$ *con* $i, j \in \{\alpha, \beta, \gamma, \delta, \varepsilon\}$ *pues* h *preserva adyacencias por ser un automorfismo. Con esto vemos que, sabiendo cuáles son las imágenes de* a_i, b_i *con* $i \in \{\alpha, \beta, \gamma, \delta, \varepsilon\}$ *bajo* h*,* h *queda completamente determinado.*

Sabemos que S_5 *actúa sobre* Ω *de manera natural pues* Ω *es un conjunto de* 5 *elementos, en este ejemplo no tomaremos esta acción si no la acción inversa, para* $\sigma \in S_5$ *y* $i \in \Omega$, $\sigma(i) = \sigma^{-1}(i)$*. Considerando esta acción verificaremos que* $Aut(\Gamma) \cong S_2 \wr_\Omega S_5$.

En este ejemplo trabajaremos con el grupo $Aut(\Gamma)$ *con la operación* $\divideontimes$ *donde si* $\alpha, \beta \in Aut(\Gamma)$ *entonces* $\alpha \divideontimes \beta := \beta\alpha$ *donde* $\beta\alpha$ *es la composición de los automorfismos* β *y* α.

Definimos $\Phi : S_5 \longrightarrow Aut(S_2 \times S_2 \times S_2 \times S_2 \times S_2)$*, si tenemos* $\sigma \in S_5$ *y* $x_i \in S_2$, $i \in \Omega$, $\Phi(\sigma)((x_i)) = (x_{\sigma^{-1}(i)})$ *entonces,*

$$S_2 \wr_\Omega S_5 = (S_2 \times S_2 \times S_2 \times S_2 \times S_2) \rtimes_\Phi S_5$$

Ahora sean $p, q \in (S_2 \times S_2 \times S_2 \times S_2 \times S_2) \rtimes_\Phi S_5$, $p = ((p_i), \tau)$ *y* $q = ((q_i), \sigma)$*, con* $p_i, \ q_i \in S_2 \ \forall \ i \in \Omega$ *y* $\sigma, \ \tau \in S_5$.

Calculamos

$$pq = ((p_i), \tau)((q_i), \sigma) = ((p_i)\Phi(\tau)((q_i)), \tau\sigma) = ((p_i q_{\tau^{-1}(i)}), \tau\sigma)$$

Definimos $\Theta : S_2 \wr_\Omega S_5 \longrightarrow Aut(\Gamma)$*, donde* $q = ((q_i), \sigma) \in S_2 \wr_\Omega S_5$ *codifica el siguiente automorfismo* $\Theta(q)(a_i) = (q_i(a))_{\sigma^{-1}(i)}$, $\Theta(q)(b_i) = (q_i(b))_{\sigma^{-1}(i)}$, $\Theta(q)(i) = \sigma^{-1}(i)$ *y* $\Theta(q)(\theta) = \theta$.

Ahora probaremos que Θ *es morfismo de grupos calculando* $\Theta(qp)$ *y* $\Theta(p) \circ \Theta(q)$ *en* $a_i, \ b_i$ *pues ya vimos que las imágenes de éstos determinan cualquier automorfismo. Calculando*

[1]Una gráfica Γ es un conjunto V no vacío, sus elementos son llamados vértices, junto con una relación de adyacencia en V denotada $v \sim u$ que cumple con ser simétrica, es decir si para $u, v \in V$ se tiene que $v \sim u$ entonces $u \sim v$, también se cumple que no es reflexiva, es decir $u \nsim u$ para toda $u \in V$. Una gráfica se visualiza como un conjunto de puntos donde los puntos que estan relacionados se unen con una arista.

[2]Un automorfismo de una gráfica Γ con vértices V, es una función biyectiva $\varphi : V \longrightarrow V$ que preserva la relación de adyacencia, es decir para $v, u \in V$ entonces $v \sim u$ si y sólo si $\varphi(u) \sim \varphi(v)$. El conjunto de automorfismos de una gráfica tiene estructura de grupo con la operación de composición y lo denotamos $Aut(\Gamma)$.

[3]Para un vértice v el grado de este vértice es el número de vértices tales que $u \sim v$, ese número se preserva bajo automorfismos pues los automorfismos preservan adyacencia.

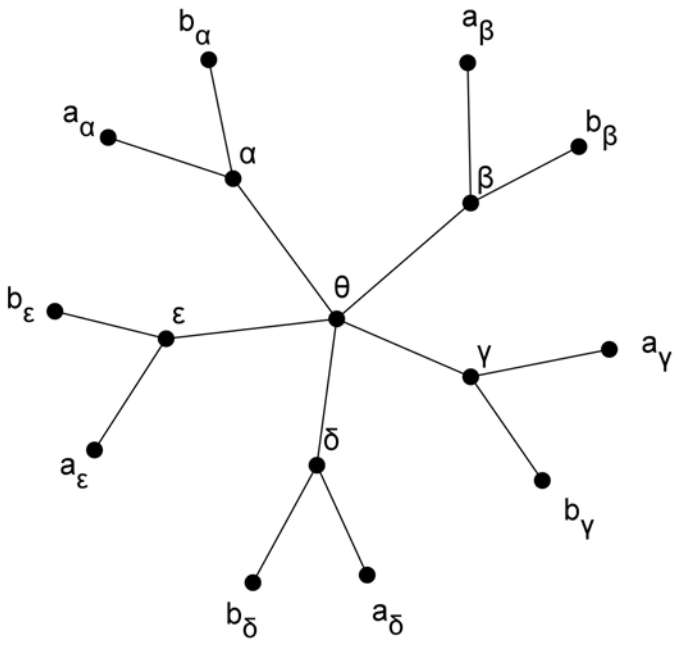

Figura 5.1: Γ

$$\Theta(pq)(a_i) = \Theta(((p_i q_{\tau^{-1}(i)}), \tau\sigma))(a_i) = (p_i q_{\tau^{-1}(i)}(a))_{(\tau\sigma)^{-1}(i)} = (p_i q_{\tau^{-1}(i)}(a))_{(\sigma^{-1}\tau^{-1})(i)}$$

y ahora

$$\Theta(p) \circledast \Theta(q)(a_i) = qp(a_i) = q(p_i(a)_{\tau^{-1}(i)}) = (q_{\tau^{-1}(i)} p_i(a))_{\sigma^{-1}(\tau^{-1}(i))}$$

Y como $p_i, q_{\tau^{-1}(i)} \in S_2$ *entonces conmutan y por lo tanto* $\Theta(pq)(a_i) = \Theta(p) \circledast \Theta(q)(a_i)$. *Análogamente para* b_i *concluimos que* $\Theta(pq)(b_i) = \Theta(p) \circledast \Theta(q)(b_i)$ *y se puede verificar fácilmente que* $\Theta(pq)(i) = \Theta(p) \circledast \Theta(q)(i)$ *y* $\Theta(pq)(\theta) = \Theta(p) \circledast \Theta(q)(\theta)$. *Por lo tanto* Θ *es un morfismo de grupos.*

Ahora verifiquemos que Θ *es un monomorfismo de grupos, supongamos que* $\Theta(q)(a_i) = a_i \ \forall i$ *esto implica que* $\Theta(q)(a_i) = (q_i(a))_{\sigma^{-1}(i)} = a_i \ \forall i$ *y por lo tanto* $q_i = 1 \ \forall i$ *y* $\sigma^{-1} = 1$ *lo cual implica que* $\sigma = 1$ *de donde se sigue que* $q = 1$ *y por lo tanto* Θ *es monomorfismo de grupos.*

Verifiquemos que Θ *es epimorfismo. Como* h *queda determinada a partir de las imágenes de cada pareja* a_i, b_i, *para cada* i *tenemos 2 opciones, la primera* $h : a_i \longrightarrow b_j$ *y* $h : b_i \longrightarrow a_j$ *en este caso* h *actúa sobre la pareja* a_i, b_i *como el elemento* $p_i \in S_2$ *con* $p_i \neq 1$. *Y en la segunda opcion tenemos.* $h : a_i \longrightarrow a_j$ *y* $h : b_i \longrightarrow b_j$ *aquí* h *actúa sobre la pareja* a_i, b_i *como* $p_i \in S_2$ *donde* $p_i = 1$. *Entonces a cada* $h \in Aut(\Gamma)$ *le podemos asociar* (p_i) *y* $\sigma \in S_5$ *tal que* $\sigma^{-1}(i) = j$ *correspondiendo cada* $h \in Aut(\Gamma)$ *a* $((p_i), \sigma) \in S_2 \wr_\Omega S_5$, *por lo tanto* Θ *es isomorfismo de grupos y* $Aut(\Gamma) \cong S_2 \wr_\Omega S_5$.

5.2. Versión de Permutación

Definición 5.5. *Sean D y Q grupos actuando fielmente en los conjuntos Λ y Ω respectivamente. Dados $d \in D$ y $\omega \in \Omega$ definimos una permutación $d^*_\omega : \Lambda \times \Omega \longrightarrow \Lambda \times \Omega$ como sigue. Para cada $(\lambda, \omega') \in \Lambda \times \Omega$*

$$d^*_\omega(\lambda, \omega') = \begin{cases} (d\lambda, \omega'), \ si\ \omega' = \omega \\ (\lambda, \omega'), \ si\ \omega' \neq \omega \end{cases}$$

Notación 5.6. *Al conjunto de todas las d^*_ω lo llamamos $D^*_\omega = \{d^*_\omega | d \in D\}$.*

Lema 5.7. *$D^*_\omega = \{d^*_\omega | d \in D\}$ es un grupo.*

Demostración. D^*_ω tiene elemento neutro, consideremos $1 \in D$ y $1^*_\omega \in D^*_\omega$ ahora calculemos

$$1^*_\omega d^*_\omega(\lambda, \omega') = \begin{cases} (1d\lambda, \omega') = (\lambda, \omega')\ si\ \omega' = \omega \\ (\lambda, \omega')\ si\ \omega' = \omega \end{cases}$$

Verificamos que $d^*_\omega d'^*_\omega = (dd')^*_\omega$ con $d, d' \in D$. Calculando

$(d^*_\omega d'^*_\omega)(\lambda, \omega')$

$$= \begin{cases} (d^*_\omega)(d'_\omega(\lambda, \omega')) = d^*_\omega(d'\lambda, \omega') = (d(d'\lambda), \omega') = ((dd')\lambda, \omega') = (dd')^*_\omega(\lambda, \omega'), \ si\ \omega' = \omega \\ (d^*_\omega)(d'_\omega(\lambda, \omega')) = d^*_\omega(\lambda, \omega') = (\lambda, \omega') = (dd')^*_\omega(\lambda, \omega'), \ si\ \omega' \neq \omega \end{cases}$$

Verifiquemos que los inversos de cada elemento están en D^*_ω, sea $d^*_\omega \in D^*_\omega = \{d^*_\omega | d \in D\}$

Entonces $(d^{-1})^*_\omega = (d^*_\omega)^{-1}$ pues

$$d^*_\omega(d^{-1})^*_\omega(\lambda, \omega) = \begin{cases} d^*_\omega(d^{-1})^*_\omega(\lambda, \omega) = (dd^{-1}\lambda, \omega') = (\lambda, \omega)\ si\ \omega = \omega' \\ d^*_\omega(d^{-1})^*_\omega(\lambda, \omega) = (\lambda, \omega)\ si\ \omega \neq \omega' \end{cases}$$

y es claro que $(d^{-1})^*_\omega \in D^*_\omega$.

Con esto podemos concluir que D^*_ω es un grupo y por lo tanto un subgrupo de $S_{\Lambda \times \Omega}$.

□

Definición 5.8. *Para cada $\omega \in \Omega$ definimos la función $h : D \longrightarrow D^*_\omega$ dada por $h(d) = d^*_\omega$*

Observación 5.9. *h es un isomorfismo de grupos. Notemos primero que h es un morfismo de grupos pues*

$$h(dd') = (dd')^*_\omega = (d^*_\omega)(d'^*_\omega) = h(d)h(d').$$

Donde la segunda igualad se debe al Lema 5.7, ahora si $h(d) = Id_{\Lambda \times \Omega}$, entonces $d^*_\omega(\lambda, \omega') = (\lambda, \omega')$ $\forall \omega' \in \Omega$, $\forall \lambda \in \Lambda$ y se sigue que $d\lambda = \lambda$, $\forall \lambda \in \Lambda$ y por lo tanto $d = 1$ ya que D actúa fielmente en Λ y así h es un monomorfismo. Por construcción h es un epimorfismo, por lo tanto h es un isomorfismo de grupos.

Con esto hemos visualizado a los elementos en D como permutaciones de $\Lambda \times \Omega$, hagamos ahora algo similar para los elementos de Q.

Definición 5.10. *Sea $q \in Q$ definimos una permutación q^* de $\Lambda \times \Omega$ como*

$$q^*(\lambda, \omega') = (\lambda, q\omega').$$

Y al conjunto de todas las permutaciones q^* lo denotamos $Q^* = \{q^* | q \in Q\}$.

Observación 5.11. *$Q^* = \{q^* | q \in Q\}$ es un subgrupo de $S_{\Lambda\times\Omega}$, pues si tenemos $q^*,\ q'^* \in Q^*$ calculamos $q^*q'^*(\lambda, \omega') = (\lambda, qq'\omega') = (qq')^*(\lambda, \omega')$ por lo tanto Q^* es cerrado y tiene neutro pues si $1 \in Q$ entonces $1^* \in D^*$ y $1^*(\lambda, \omega') = (\lambda, 1\omega') = (\lambda, \omega')$.*

Observación 5.12. *La función $g : Q \longrightarrow Q*$ dada por $g(q) = q^*$, g es un morfismo pues*

$$\begin{aligned} g(qq')(\lambda, \omega') &= (qq')^*(\lambda, \omega') \\ &= q^*(q'^*(\lambda, \omega')) \\ &= g(q)g(q')(\lambda, \omega'),\ \forall\lambda \in \Lambda,\ \forall\omega' \in \Omega. \end{aligned}$$

Y si $g(q) = Id_{\Lambda\times\Omega}$ entonces,

$$q^*(\lambda, \omega') = (\lambda, \omega')\ \forall\ (\lambda, \omega') \in \Lambda \times \Omega,$$

esto implica que $\omega' = q\omega'\ \forall\ \omega' \in \Omega$ por lo tanto $q = 1$ ya que Q actúa fielmente en Ω y g es un monomorfismo. Si $q^* \in Q^*$ entonces $g(q) = q^*$ por lo tanto g es un isomorfismo.

Veamos ahora que esta forma de ver a D y a Q como permutaciones de $\Lambda \times \Omega$ nos da, salvo isomorfía el producto trenzado de D y Q, que actúa sobre $\Lambda \times \Omega$.

Lema 5.13. *Sea $K^* =< \bigcup_{\omega\in\Omega} D^*_\omega >$, entonces $K^* = \prod_{\omega\in\Omega} D^*_\omega$, $\omega \in \Omega$.*

Demostración. Para $\omega' \neq \omega$ D^*_ω centraliza a $D^*_{\omega'}$ pues

$$(d^*_\omega d'^*_{\omega'})(\lambda, \omega'') = d^*_\omega(d'^*_{\omega'}(\lambda, \omega'')) = \begin{cases} (d\lambda, \omega''),\ si\ \omega = \omega'' \neq \omega' \\ (d'\lambda, \omega''),\ si\ \omega \neq \omega'' = \omega' \\ (\lambda, \omega''),\ si\ \ \omega \neq \omega'' \neq \omega' \end{cases}$$

no es posible el caso $\omega' = \omega' = \omega''$ pues por hipótesis $\omega \neq \omega'$, ahora calculemos $(d'^*_{\omega'} d^*_\omega)(\lambda, \omega'')$

$$(d'^*_{\omega'} d^*_\omega)(\lambda, \omega'') = \begin{cases} (d\lambda, \omega''),\ si\ \omega = \omega'' \neq \omega' \\ (d'\lambda, \omega''),\ si\ \omega \neq \omega'' = \omega' \\ (\lambda, \omega''),\ si\ \omega \neq \omega'' \neq \omega' \end{cases}$$

De nuevo no es posible el caso $\omega' = \omega' = \omega''$.

Con esto tenemos que $d^*_\omega d'^*_{\omega'} = d'^*_{\omega'} d^*_\omega$. Por lo tanto D^*_ω centraliza a $D^*_{\omega'}$ para $\omega \neq \omega'$, en particular $D^*_\omega \lhd K^*$, para cualquier $\omega \in \Omega$ y cualquier elemento $k \in K^*$ puede escribirse como $\prod_{\omega\in\Omega} d^*_\omega$ de donde obtenemos que $K^* = \prod_{\omega\in\Omega} D_\omega$.

Ahora sea $x \in D^*_\omega \cap \prod_{\omega'\neq\omega} D^*_{\omega'}$, y $(\lambda, \omega'') \in \Lambda \times \Omega$, entonces $d^*_\omega = x = \prod_{\omega\neq\omega'} d^*_{\omega'}$ y calculamos

$$d^*_\omega(\lambda, \omega'') = \begin{cases} (d\lambda, \omega'')\ si\ \omega'' = \omega \\ (\lambda, \omega'')\ si\ \omega'' \neq \omega \end{cases}$$

si $\omega = \omega''$ entonces.

$$d^*_\omega(\lambda,\omega'') = (d\lambda,\omega'') = \prod_{\omega\neq\omega'} d^*_{\omega'}(\lambda,\omega'') = (\lambda,\omega'')$$

pues $\omega \neq \omega'$ y así $(d\lambda,\omega'') = (\lambda,\omega'')$ lo cual implica que $d = 1$ y que d^*_ω es trivial. Ahora si $\omega \neq \omega''$ se sigue que

$$d^*_\omega(\lambda,\omega'') = (\lambda,\omega'')$$

Por lo tanto d^*_ω es trivial y $D^*_\omega \cap \prod_{\omega'\neq\omega} D^*_{\omega'} = \{1\}$ obteniendo por la definición 3.8 que K^* es el producto directo interno de todos los D^*_ω □

Teorema 5.14. ***Versión de Permutación****. Dados grupos D y Q, Ω un Q-conjunto finito y Λ un D-conjunto, entonces el producto trenzado $D \wr_\Omega Q \cong W$ donde $W = \langle Q^*, D^*_\omega | \omega \in \Omega\rangle \leq S_{\Lambda\times\Omega}$, y $\Lambda \times \Omega$ es un $(D \wr_\Omega Q)$-conjunto.*

Demostración. Por el Lema 5.13 tenemos que $K^* = \langle \bigcup_{\omega\in\Omega} D^*_\omega\rangle = \prod_{\omega\in\Omega} D^*_\omega$.

Verifiquemos ahora que $W = K^* \rtimes Q^*$, veamos primero que K^* es normal en W:

Si $q \in Q$ y $\omega \in \Omega$ entonces $q^* d^*_\omega (q^*)^{-1} = d^*_{q\omega}$ para cada $\omega \in \Omega$, pues calculando $q^* d^*_\omega (q^*)^{-1}$ tenemos

$$(q^* d_\omega (q^*)^{-1})(\lambda,\omega') = (q^* d_\omega)(\lambda, q^{-1}\omega')$$

y

$$(q^* d_\omega)(\lambda, q^{-1}\omega') = \begin{cases} q^*(d\lambda, q^{-1}\omega') = (d\lambda, q(q^{-1})\omega') = (d\lambda,\omega'),\ si\ q^{-1}\omega' = \omega \\ q^*(\lambda, q^{-1}\omega') = (\lambda, q(q^{-1}\omega') = (\lambda,\omega'),\ si\ q^{-1}\omega' \neq \omega \end{cases}$$

y calculando también $d^*_{q\omega}(\lambda,\omega')$

$$d^*_{q\omega}(\lambda,\omega') = \begin{cases} (d\lambda,\omega'),\ si\ \omega' = q\omega \\ (\lambda,\omega')\ si\ \omega' \neq q\omega \end{cases}$$

por lo tanto

$$q^* d^*_\omega (q^*)^{-1} = d^*_{q\omega} \tag{5.1}$$

y $K^* \lhd W$ entonces $D^*_\omega \lhd W$.

Ahora notemos que d^*_ω fija a la segunda entrada y como para $q^* \in Q^*$, $q^*(\lambda,\omega') = (\lambda, q\omega)$ y q^* fija la primera entrada, así cualquier $g \in K^* \cap Q^*$ fija cualquier (λ,ω) y entonces $g = Id$ por lo tanto $W = K^* \rtimes Q^*$ y W es un producto semidirecto interno de K^* por Q^*.

Ahora definimos $f : D \wr_\Omega Q \longrightarrow W$ dada como $f((d_\omega), q) = (d^*_\omega)q^*$ verificaremos que f es un isomorfismo. Veamos primero que es un morfismo.

Sean $((d_\omega), q)$ y $((d'_\omega), q') \in D \wr_\Omega Q$, calculamos

$$((d_\omega), q)((d'_\omega), q') = ((d_\omega)(d'_{q\omega}), qq')$$

y aplicamos

$$f(((d_\omega), q)((d'_\omega), q')) = f((d_\omega d'_{q\omega}), qq') = (d_\omega d'_{q\omega})^*(qq')^*$$

y como $q^* d^*_\omega = d^*_{q\omega} q^*$ por 5.1 entonces

$$f((d_\omega), q) f((d'_\omega), q') = (d^*_\omega) q^* (d'^*_\omega) q'^* = (d^*_\omega)(d'^*_{q\omega}) q^* q'^*$$

y como para cualesquiera $d_\omega, d'_{\omega'}$ se cumple que $d^*_\omega d'^*_{\omega'} = (d_\omega d'_{\omega'})^*$ y que $q^* q'^* = (qq')^*$ por las observaciones 5.9 y 5.11, entonces tenemos

$$f((d_\omega, q)(d'_\omega, q')) = f((d_\omega), q) f((d'_\omega), q')$$

por lo tanto f es morfismo. Ahora si $f((d_\omega, q)) = Id_\omega$ esto implica que

$$((d^*_\omega) q^*)(\lambda, \omega') = (d_{q^{-1}\omega}\lambda, q\omega') = (\lambda, \omega'),\ \forall(\lambda, \omega')$$

y por lo tanto $q = 1$ y $d_{q^{-1}\omega} = 1\ \forall \omega \in \Omega$ y de esto tenemos que f es monomorfismo.

Por último consideramos $(d^*_\omega) q^* \in W\ \exists\ (d_\omega) q \in D \wr_\Omega Q$, tal que $f(((d_\omega), q)) = (d^*_\omega) q^*$ por lo tanto$f$ es isomorfismo. □

Llamamos al subgrupo W de $S_{\Lambda\times\Omega}$ la versión de permutación de $D \wr_\Omega Q$.

Observación 5.15. *Notemos que debido a la " conmutatividad" obtenida a partir de la ecuación 5.1 podemos escribir cualquier elemento de W de la forma $(d^*_\omega) q^*$.*

Ejemplo 5.16. *Sea $D = \mathbb{Z}_2$, $Q = \mathbb{Z}_3$, $\Omega = \{0, 1, 2\}$ y $\Lambda = \{0, 1\}$ donde D y Q actúan sobre Ω y Λ respectivamente de manera natural. Entonces $D \wr_\Omega Q = \mathbb{Z}_2 \wr_{\mathbb{Z}_3} \mathbb{Z}_3$ y*

$$\mathbb{Z}_2 \wr_{\mathbb{Z}_3} \mathbb{Z}_3 = \{((z_0, z_1, z_2), g) | z_i \in \mathbb{Z}_2,\ g \in \mathbb{Z}_3\}.$$

La versión de permutación de $\mathbb{Z}_2 \wr_{\mathbb{Z}_3} \mathbb{Z}_3$ es

$$W = \langle \mathbb{Z}^*_3,\ (\mathbb{Z}^*_2)_i | i = 1,\ 2,\ 3\rangle$$

y W es subgrupo de $S_{\mathbb{Z}_2\times\mathbb{Z}_3}$. Ahora tomaremos un elemento en $\mathbb{Z}_2 \wr_{\mathbb{Z}_3} \mathbb{Z}_3$ y veremos como el elemento correspondiente en W mueve a una pareja en $\mathbb{Z}_2 \times \mathbb{Z}_3$. Sea

$$x = ((z_0, z_1, z_2), g) \in \mathbb{Z}_2 \wr_{\mathbb{Z}_3} \mathbb{Z}_3$$

con $((z_0, z_1, z_2), g) = ((0, 1, 0), 1)$ y el elemento correspondiente a x en W sería

$$((z^*_0, z^*_1, z^*_2), g^*) = ((0^*, 1^*, 0^*), 1^*)$$

ahora apliquemos x al elemento $(1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ entonces tenemos

$$((z^*_0, z^*_1, z^*_2), g^*)(1, 1) = (z_1(1), g(1)) = (1(1), 1(1)) = (1 + 1, 1 + 1) = (0, 2).$$

Definición 5.17. *Sean D y Q grupos y Ω un Q-conjunto finito y Λ un D-conjunto definimos*

$$D^*_\omega(\lambda) = \{d^*_\omega | d \in D(\lambda)\}$$

donde $D(\lambda)$ es el estabilizador de λ y

$$Q^*_\omega = \{q^* | q \in Q_\omega\}$$

donde Q_ω es el estabilizador de ω.

Siguiendo la notación anterior tenemos que.

Lema 5.18. *Sea $\omega \in \Omega$, entonces $D^*_\omega(\lambda)$ centraliza a $\langle \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle$.*

Demostración. Si $d^*_\omega \in D^*_\omega(\lambda)$ y $q^* \in Q^*_\omega$ entonces, dado que Q_ω estabiliza a ω, se tiene que

$$q^* d^*_\omega (q^{-1})^* = d^*_{q\omega} = d^*_\omega$$

y así

$$q^* d^*_\omega = d^*_\omega q^*$$

de aquí tenemos que d^*_ω conmuta con elementos de Q^*_ω.

Ahora veamos que d^*_ω conmuta con elementos de $\prod_{\omega' \neq \omega} D^*_{\omega'}$.

Sea $(d'^*_{\omega'}) \in \prod_{\omega' \neq \omega} D^*_{\omega'}$, supongamos que $\omega'' \neq \omega$ y calculamos

$$d^*_\omega (d'^*_{\omega'})(\lambda', \omega'') = (d'_{\omega''}\lambda', \omega'') = (d'^*_{\omega'}) d^*_\omega (\lambda', \omega'')$$

ahora supongamos que $\omega = \omega''$

$$d^*_\omega (d'^*_{\omega'})(\lambda', \omega'') = (d\lambda', \omega) = (d'^*_{\omega'}) d^*_\omega (\lambda', \omega'').$$

Y por lo tanto d^*_ω conmuta con los elementos de $\prod_{\omega' \neq \omega} D'_{\omega'}$ y con los de Q^*_ω por lo tanto $D^*_\omega(\lambda)$ centraliza a $\langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle$. □

Corolario 5.19. $D^*_\omega \trianglelefteq \langle D^*_\omega(\lambda), \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle$ *y* $\langle \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle \trianglelefteq \langle D^*_\omega(\lambda), \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle$.

Demostración. Por el Lema 5.18 cada elemento de $\langle D^*_\omega(\lambda), \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle$ se puede expresar de la forma $\widetilde{d^*}_\omega \prod_i P^*_i$ donde $\widetilde{d^*}_\omega \in D^*_\omega(\lambda)$ y cada P_i es elemento de $\prod_{\omega \neq \omega'} D^*_{\omega'}$ o de Q^*_ω, entonces conjugamos $\widetilde{d^*}_\omega$

$$\begin{aligned}(\widetilde{d^*}_\omega \prod_i P^*_i) d^*_\omega (\widetilde{d^*}_\omega \prod_i P^*_i)^{-1} &= \widetilde{d^*}_\omega \prod_i P^*_i d^*_\omega (\prod_i P^*_i)^{-1} (\widetilde{d^*}_\omega)^{-1} \\ &= \widetilde{d^*}_\omega d^*_\omega (\widetilde{d^*}_\omega)^{-1} \in D^*_\omega(\lambda)\end{aligned}$$

ya que d^*_ω conmuta con los elementos de $\prod_{\omega \neq \omega'} D^*_{\omega'}$ y de Q^*_ω. Por lo tanto

$$D^*_\omega(\lambda) \trianglelefteq \langle D^*_\omega(\lambda), \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle.$$

Siguiendo un procedimiento análogo podemos concluir que

$$\langle \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle \trianglelefteq \langle D^*_\omega(\lambda), \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle.$$

□

Teorema 5.20. *Sea* $(\lambda, \omega) \in \Lambda \times \Omega$, *entonces*

$$\langle D^*_\omega(\lambda), \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle \cong D^*_\omega(\lambda) \times \langle \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle$$

Demostración. Primero veamos que $D^*_\omega(\lambda) \cap \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle = \{1\}$.

Sea $f \in D^*_\omega(\lambda) \cap \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle$ y $(\lambda', \omega'') \in \Lambda \times \Omega$. Calculamos $f(\lambda', \omega'')$, por un lado

$$f(\lambda', \omega'') = d^*_\omega(\lambda', \omega'')$$

y por el otro

$$f(\lambda', \omega'') = \prod_{i \in I} P^*_i(\lambda', \omega'')$$

donde $d^*_\omega \in D^*_\omega(\lambda)$ y para toda i, $P^*_i \in \prod_{\omega' \neq \omega} D^*_{\omega'}$ ó $P^*_i \in Q^*_\omega$, definimos $S \subseteq I$ como

$$S = \{s \in I | P^*_s \in Q^*_\omega\}.$$

Considerando $\omega = \omega''$ tenemos que

$$d^*_\omega(\lambda', \omega'') = (d\lambda', \omega'') = \prod_{i \in I} P^*_i(\lambda', \omega'') = (\lambda', \prod_{s \in S} P^*_s \omega'').$$

Ya que aplicando $\prod_{i \in I} P^*_i$, λ' queda fija pues $P^*_i \in \prod_{\omega' \neq \omega} D_{\omega'}$ y en este caso $\omega'' = \omega \neq \omega'$ ó $P^*_i \in Q^*_\omega$. Tenemos así

$$(d\lambda', \omega'') = (\lambda', \prod_{s \in S} P^*_s \omega'')$$

donde $P^*_s \in Q^*_\omega$, entonces $d\lambda' = \lambda'$ por lo tanto $d = 1$ ya que D actúa fielmente y en consecuencia $d^*_\omega = Id$. Por lo tanto

$$D^*_\omega(\lambda) \cap \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle = \{1\}.$$

Y con el Corolario 5.19 obtenemos que

$$D^*_\omega(\lambda) \trianglelefteq \langle D^*_\omega(\lambda), \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle$$

$$y \ \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle \trianglelefteq \langle D^*_\omega(\lambda), \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle$$

Ahora como la intersección es trivial y ambos son normales en $\langle D^*_\omega(\lambda), \prod_{\omega \neq \omega'} D^*_{\omega'}, Q^*_\omega \rangle$ faltaría ver que $D^*_\omega(\lambda) \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle = \langle D^*_\omega(\lambda), \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle$ como producto interno de grupos.

Sea $\prod_{t \in T} P^*_t \in \langle D^*_\omega(\lambda), \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle$ donde T es finito y para cada t, $P^*_t \in D^*_\omega(\lambda)$ ó $P^*_t \in \prod_{\omega' \neq \omega} D^*_{\omega'}$ ó $P^*_t \in Q^*_\omega$ ahora definimos $R = \{r \in T | P^*_r \in D^*_\omega(\lambda)\}$ notemos que P^*_r con $r \in R$ conmuta con cualquier P_t con $t \in T$ porque $D^*_\omega(\lambda)$ centraliza a $\prod_{\omega' \neq \omega} D^*_\omega$ y a Q^*_ω por el Lema 5.18, por lo tanto $\prod_{t \in T} P^*_t = (\prod_{r \in R} P^*_r) \prod_{t \in T - R} P^*_t$ y así tenemos expresado cualquier elemento de $\langle D^*_\omega(\lambda), \prod_{\omega' \neq \omega} D^*_\omega, Q^*_\omega \rangle$ como producto de elementos de $D^*_\omega(\lambda)$ y de $\langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle$ y por lo tanto

$$\langle D^*_\omega(\lambda), \prod_{\omega' \neq \omega} D^*_\omega, Q^*_\omega \rangle \cong D^*_\omega(\lambda) \times \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle.$$

□

Teorema 5.21. *Sea $(\lambda,\omega)\in\Lambda\times\Omega$ y $W_{(\lambda,\omega)}$ el estabilizador de (λ,ω), entonces:*

1. $W_{(\lambda,\omega)}=\langle D^*_\omega(\lambda),\prod_{\omega'\neq\omega}D^*_{\omega'},Q^*_\omega\rangle$.
2. $W_{(\lambda,\omega)}=D(\lambda)\times(D\wr_{(\Omega-\{\omega\})}Q_\omega)\cong D^*_\omega(\lambda)\times\langle\prod_{\omega'\neq\omega}D^*_{\omega'},Q^*_\omega\rangle$.
3. $[W:W_{(\lambda,\omega)}]=[D:D(\lambda)][Q:Q_\omega]$.

Demostración. 1. Veamos que $W_{(\lambda,\omega)}=\langle D^*_\omega(\lambda),\prod_{\omega'\neq\omega}D^*_{\omega'},Q^*_\omega\rangle$.

Sea

$$\prod_{i\in I}P^*_i\in\langle D^*_\omega(\lambda),\prod_{\omega'\neq\omega}D^*_{\omega'},Q^*_\omega\rangle,$$

donde $P^*_i\in D^*_\omega(\lambda)$ ó $P^*_i\in\prod_{\omega'\neq\omega}D^*_{\omega'}$ ó $P^*_i\in Q^*_\omega$, para toda $i\in I$ ahora calculando

$$\prod_{i\in I}P^*_i(\lambda,\omega)=(\lambda,\omega)$$

pues cada $P^*_i(\lambda,\omega)=(\lambda,\omega)$ para toda $i\in I$ por lo tanto $\prod_{i\in I}P^*_i\in W_{(\lambda,\omega)}$ y

$$\langle D^*_\omega(\lambda),\prod_{\omega'\neq\omega}D^*_\omega,Q^*_\omega\rangle\subseteq W_{(\lambda,\omega)}.$$

Por la Observación 5.15 $\forall\ x\in W_{(\lambda,\omega)}$, $x=(d^*_\varpi)q^*$ con $\varpi\in\Omega$ y $q\in Q$, además

$$((d^*_\varpi)q^*)(\lambda,\omega)=(\prod_{\varpi\in\Omega}d^*_\varpi)(\lambda,q\omega)=d^*_{q\omega}(\lambda,q\omega)=(d\lambda,q\omega)$$

pero como $(d^*_\varpi)q^*\in W_{(\lambda,\omega)}$ entonces $(d\lambda,q\omega)=(\lambda,\omega)$ y de aquí tenemos que $q\in Q_\omega$ y $q^*\in Q^*_\omega$, también que $d\in D(\lambda)$ y $d^*_\varpi\in D^*_\omega(\lambda)$ y por lo tanto

$$(d^*_\varpi)q^*\in\langle D^*_\omega(\lambda),\prod_{\omega'\neq\omega}D^*_{\omega'},Q^*_\omega\rangle,$$

lo cual implica que

$$W(\lambda,\omega)=\langle D^*_\omega(\lambda),\prod_{\omega'\neq\omega}D_{\omega'},Q^*_\omega\rangle.$$

2. Notemos que Q_ω actúa sobre $\Omega-\{\omega\}$, por el Teorema 5.20 tenemos que

$$\langle D^*_\omega(\lambda),\prod_{\omega\neq\omega'}D^*_{\omega'},Q^*_\omega\rangle\cong D^*_\omega(\lambda)\times\langle\prod_{\omega\neq\omega'}D^*_{\omega'},Q^*_\omega\rangle$$

y así $W_{(\lambda,\omega)}\cong D^*_\omega(\lambda)\times\langle\prod_{\omega'\neq\omega}D^*_{\omega'},Q^*_\omega\rangle$

Ahora veamos que $D^*_\omega(\lambda)\cong D(\lambda)$.

Definimos $h:D^*_\omega(\lambda)\longrightarrow D(\lambda)$, $h(d^*_\omega)=d$, es fácil verificar por la Observación 5.9 que h es morfismo de grupos

$$h(d^*_\omega d'^*_\omega)=h((dd')^*_\omega)=dd'\ y\ h(d^*_\omega)h(d'^*_\omega)=dd'.$$

Por lo tanto h es un morfismo de grupos, ahora si $h(d^*_\omega) = 1$ entonces $d = 1$ y $d^*_\omega = Id$ y por último $\forall\ d \in D(\lambda)\ \exists\ d^*_\omega \in D^*_\omega(\lambda)$ tal que $h(d^*_\omega) = d$ por lo tanto $D^*_\omega(\lambda) \cong D(\lambda)$.

De manera similar podemos ver que $D^*_{\omega'} \cong D\ \forall\ \omega' \in \Omega - \{\omega\}$ y $Q^*_\omega \cong Q_\omega$, con lo cual podemos concluir que

$$\prod_{\omega' \neq \omega} D^*_{\omega'} \cong \prod_{\omega' \in \Omega - \{\omega\}} D_{\omega'}$$

y con la Proposición 4.14 concluimos que

$$\prod_{\omega' \neq \omega} D^*_{\omega'} \rtimes Q^*_\omega \cong \prod_{\omega' \in \Omega - \{\omega\}} D_{\omega'} \rtimes Q_\omega = D \wr_{\Omega - \{\omega\}} Q_\omega.$$

Ahora sólo nos falta demostrar que $\prod_{\omega' \neq \omega} D^*_{\omega'} \rtimes Q^*_\omega = \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle$. Primero verifiquemos $\prod_{\omega' \neq \omega} D^*_{\omega'} \lhd \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle$, para $q^* \in Q^*$ y $d^* \in \prod_{\omega' \neq \omega} D^*_{\omega'}$ sabemos por la ecuación 5.1 que $q^*(d^*_{\omega'})(q^{-1})^* = (d_{q\omega'})$, entonces

$$q^*(d_{\omega'}) = (d_{q\omega'})q^*.$$

Con esto notemos que si

$$\prod_{i \in I} m_i \in \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle$$

con $m_i \in \prod_{\omega' \neq \omega} D^*_{\omega'}$ o $m_i \in Q^*_\omega\ \forall\ i \in I$, $\prod_{i \in I} m_i$ puede verse como $\prod_{s \in S} m_s \prod_{t \in T} m_t$ ó $\prod_{t \in T} m_t \prod_{s \in S} m_s$ donde $m_t \in \prod_{\omega' \neq \omega} D^*_{\omega'}\ \forall t \in T \subset I$ y $m_s \in Q^*_\omega\ \forall s \in S \subset I$.

Entonces calculando

$$\begin{aligned} \textstyle\prod_{i \in I} m_i(d_{\omega'})(\prod_{i \in I} m_i)^{-1} &= \textstyle\prod_{s \in S} m_s \prod_{t \in T} m_t(d_{\omega'})(\prod_{s \in S} m_s \prod_{t \in T} m_t)^{-1} \\ &= \textstyle\prod_{s \in S} m_s((\prod_{t \in T} m_t)(d_{\omega'})(\prod_{t \in T} m_t)^{-1})(\prod_{s \in S} m_s)^{-1} \end{aligned}$$

como $m_t \in \prod_{\omega' \neq \omega} D^*_{\omega'}$ entonces

$$\overline{d}^*_{\omega'} = (\prod_{t \in T} m_t)(d_{\omega'})(\prod_{t \in T} m_t)^{-1} \in \prod_{\omega' \neq \omega} D^*_{\omega'}$$

y como $m_s \in Q^*_\omega$ entonces $\overline{q}^* = \prod_{s \in S} m_s \in Q^*_\omega$ y por lo tanto

$$\prod_{s \in S} m_s((\prod_{t \in T} m_t)(d_{\omega'})(\prod_{t \in T} m_t)^{-1})(\prod_{s \in S} m_s)^{-1} = \overline{q}^*(\overline{d}^*_{\omega'})(\overline{q}^{-1})^*$$

y finalmente

$$\prod_{i \in I} m_i(d_{\omega'})(\prod_{i \in I} m_i)^{-1} = (\overline{d}_{\overline{q}\omega'}).$$

Y por lo tanto $\prod_{\omega' \neq \omega} D^*_{\omega'} \lhd \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle$, fácilmente podemos verificar que

$$\prod_{\omega' \neq \omega} D^*_{\omega'} \cap Q^*_\omega = \{1\}$$

y si $g \in \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle$ entonces $g = (d^*_{\omega'})q^*$ con $d_{\omega'} \in \prod_{\omega' \neq \omega} D^*_{\omega'}$ y $q^* \in Q^*_\omega$, por la Observación 5.15.

Entonces $\langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle = \prod_{\omega' \neq \omega} D^*_{\omega'} \rtimes Q^*_\omega = D^*_{\omega'} \wr_{\Omega - \{\omega\}} Q^*_\omega$ y por lo tanto

$$D(\lambda) \times (D \wr_{\Omega - \{\omega\}} Q_\omega) \cong D^*(\lambda) \times \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle = W_{(\lambda,\omega)}.$$

3. Por 5.14 tenemos que $W \cong D \wr_\Omega Q$ y entonces $|W| = |D|^{|\Omega|}|Q|$ y por el inciso previo $W_{(\lambda,\omega)} \cong D^*(\lambda) \times \langle \prod_{\omega' \neq \omega} D^*_{\omega'}, Q^*_\omega \rangle$ y así $|W_{(\lambda,\omega)}| = |D(\lambda)||D|^{|\Omega|-1}|Q_\omega|$, con lo cual concluimos que

$$[W : W(\lambda,\omega)] = |D|^{|\Omega|}|Q|/|D(\lambda)||D|^{|\Omega|-1}|Q_\omega| = |D||Q|/|D(\lambda)||Q_\omega| = [D : D(\lambda)][Q : Q_\omega].$$

□

Teorema 5.22. *El producto trenzado es asociativo: Sean D, Q y T grupos con Ω un Q-conjunto finito Λ un D-conjunto finito y Δ un T-conjunto entonces $T \wr_{\Lambda\times\Omega} (D \wr_\Omega Q) \cong (T \wr_\Lambda D) \wr_\Omega Q$.*

Demostración. Veamos cómo son los generadores de la versión de permutación de $T \wr_{\Lambda\times\Omega} (D \wr_\Omega Q)$. Sea W_1 la versión de permutación de $D \wr_\Omega Q$ y como $W_1 \cong D \wr_\Omega Q$ entonces por la proposición 4.14 de producto semidirecto

$$T \wr_{\Lambda\times\Omega} W_1 \cong T \wr_{(\Lambda\times\Omega)} (D \wr_\Omega Q)$$

Y por lo tanto sus versiones de permutación son isomorfas y un subgrupo de $S_{\Delta\times\Lambda\times\Omega}$. Sea W la versión de permutación de $T \wr_{\Lambda\times\Omega} W_1$. Ahora por el Teorema 5.14 sabemos que W está generado por todos los $t^*_{(\lambda,\omega)}$ y todos los f^* con $t \in T$, $f \in W_1$ y $(\lambda,\omega) \in \Omega \times \Lambda$ donde si

$$(\delta', \lambda', \omega') \in \Delta \times \Lambda \times \Omega,\ t^*_{(\lambda,\omega)}(\delta', \lambda', \omega') = (t\delta', \lambda', \omega')\ si\ (\lambda', \omega') = (\lambda, \omega)$$

y lo deja fijo en otro caso y

$$f^*(\delta', \lambda', \omega') = (\delta', f(\lambda', \omega'))\ con\ f^* \in \langle Q^*, D^*_\omega : \omega \in \Omega \rangle.$$

De aquí vemos que $T \wr_{(\lambda,\omega)} W_1$ está generado por todos los $t^*_{(\omega,\lambda)}\ d^*_\omega$ y q^{**} donde

$$d^*_\omega(\delta', \lambda', \omega') = (\delta', d\lambda', \omega')\ si\ \omega' = \omega$$

y lo fija en cualquier otro caso. Y para $q^{**}(\delta', \lambda', \omega') = (\delta', \lambda', q\omega')$.

Ahora veamos cómo son los generadores de la versión de permutación de $(T \wr_\Lambda D) \wr_\Omega Q$, para concluir que son iguales a los de la versión de permutación de $T \wr_{\Lambda\times\Omega} (D \wr_\Omega Q)$. Llamamos Z_1 a la versión de permutación de $T \wr_\Lambda D$ y como $Z_1 \cong T \wr_\Lambda D$ entonces

$$(T \wr_\Lambda D) \wr_\Omega Q \cong Z_1 \wr_\Omega Q$$

Por lo tanto sus versiones de permutación son subgrupos isomorfos de $S_{\Delta\times\Lambda\times\Omega}$, llamemos Z a la versión de permutación de $Z_1 \wr_\Omega Q$, ahora $Z_1 \wr_\Omega Q$ está generado por todos los f'''^* y q^{**} con $f'' \in Z_1,\ q \in Q$ donde si $(\delta', \lambda', \omega') \in \Delta \times \Lambda \times \Omega$ entonces

$$f''^{*}_{\omega}(\delta', \lambda', \omega') = (f''(\delta, \lambda'), \omega) \text{ si } \omega = \omega'.$$

Y lo deja fijo en cualquier otro caso y $q^{**}(\delta', \lambda', \omega') = (\delta', \lambda', q\omega')$. Como

$$f''^{*} \in \langle D^*, T^*_\lambda; \lambda \in \Lambda \rangle$$

concluimos que Z está generado por todos los q^{**}, d^{**}_ω y $(t_\lambda)^*_\omega$ donde

$$(t_\lambda)^*_\omega(\delta', \lambda', \omega') = (t\delta', \lambda', \omega') \text{ si } \omega' = \omega \text{ y } \lambda' = \lambda.$$

Y lo fija en cualquier otro caso, de aquí tenemos que

$$(t^*_\lambda)_\omega = t^*_{(\lambda,\omega)} \text{ y } d^*_\omega(\delta', \lambda', \omega') = (\delta', d\lambda', \omega') \text{ si } \omega = \omega'.$$

Y lo fija en cualquier otro caso y por último $q^{**}(\delta', \lambda', \omega') = (\delta', \lambda', q\omega')$ entonces con esto concluimos que W y Z tienen los mismos generadores por lo tanto $W \cong Z$ y por lo tanto $T \wr_{\Lambda\times\Omega} (D \wr_\Omega Q) \cong (T \wr_\Lambda D) \wr_\Omega Q$.

□

5.3. Producto Trenzado Regular

Definición 5.23. *Sea $D \wr_\Omega Q$, con $\Omega = Q$, donde Q actúa sobre sí mismo de manera natural. A este caso particular de producto trenzado lo llamamos el producto trenzado regular y lo escribimos $D \wr_r Q$.*

Observación 5.24. *Por definición tenemos que $D \wr_r Q = \prod_{x\in Q} D_x \rtimes Q$ donde la acción de $q \in Q$ en $(d_x) \in \prod_{x\in Q} D_x$ manda a (d_x) en (d_{qx}). También notemos que $|D \wr_r Q| = |D|^{|Q|}|Q|$.*

Notemos que en el ejemplo 5.3 vimos el producto trenzado regular $\mathbb{Z}_2 \wr_{\mathbb{Z}_2} \mathbb{Z}_2$. Y vimos que tiene la propiedad de ser isomorfo a D_4 y también cumple que $|2|^{|2|}|2| = 8$.

Observación 5.25. *Notemos que en el caso del producto trenzado regular, no siempre se cumple la asociatividad, pues si tenemos T, D y Q grupos finitos, entonces*

$$|T \wr_r (D \wr_r Q)| = |T|^{|D\wr_r Q|}|D \wr_r Q|$$

y por otro lado

$$|(T \wr_r D) \wr_r Q| = |T \wr_r D|^{|D|}|D|$$

el orden de estos no siempre sera el mismo, pues si tomamos $T = \mathbb{Z}_2$, $D = \mathbb{Z}_3$ y $Q = \mathbb{Z}_2$ entonces

$$|\mathbb{Z}_2|^{|\mathbb{Z}_3\wr_r\mathbb{Z}_2|}|\mathbb{Z}_3 \wr_r \mathbb{Z}_2| = 4,718,592$$

y

$$|\mathbb{Z}_2 \wr_r \mathbb{Z}_3|^{|\mathbb{Z}_2|}|\mathbb{Z}_2| = 1,152$$

por lo tanto los grupos $T \wr_r (D \wr_r Q)$ y $(T \wr_r D) \wr_r Q$ no siempre serán iguales.

Este resultado podría parecer confuso, pues en el Teorema 5.22 verificamos la asociatividad del producto trenzado y ahora en el caso del producto trenzado regular acabamos de verificar lo contrario, la diferencia cae sobre el hecho de que cuando considero el producto $T \wr_{\Lambda\times\Omega} (D \wr_\Omega Q)$ el conjunto sobre el que actúa $(D \wr_\Omega Q)$ es $\Lambda \times \Omega$ y en el caso del producto trenzado regular es él mismo $(D \wr_\Omega Q)$ y estos 2 conjuntos no necesariamente tienen la misma cardinalidad.

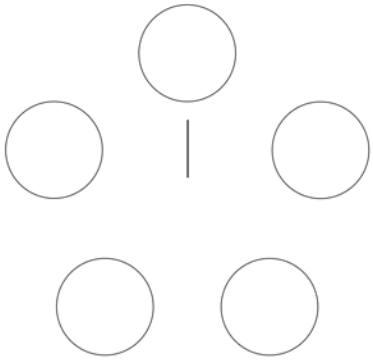

Figura 5.2: $((0,0,0,0,0),0)$

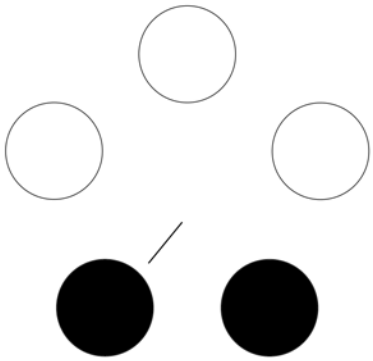

Figura 5.3: $((1,0,0,0,1),2)$

5.4. Lampligther Group

Este grupo lo estudiaremos en términos de operaciones en un arreglo circular de n lámparas en el cual tenemos 2 operaciones, rotar y prender (o apagar) cualquier lámpara.

Para poder visualizar cómo funcionan estas operaciones consideremos un arreglo circular de 5 lámparas. Nuestro arreglo tiene un estado inicial donde todas las lámparas están apagadas y las representaremos con círculos vacíos como en la figura 5.2.

Cualquier estado del arreglo se puede codificar con un "vector" que indica la posición de las lámparas, estos "vectores" serán los elementos de nuestro grupo y cada "vector" está en correspondencia biyectiva con cada estado de mi arreglo circular de 5 lamparas. Por ejemplo el de la figura 5.2 se representaría con $((0,0,0,0,0),0)$ donde los primeros 5 ceros indican que todas las lámparas están apagadas y el último indica que no ha habido rotación.

Por ejemplo el estado de la figura 5.3 se representa $((1,0,0,0,1),2)$ el número 2 indica que se rotó 2 veces en dirección contraria a las manecillas del reloj y sobre esa rotación la primera lámpara *(la primera lámpara es la que está señalada con un segmento de recta y la segunda es la que está a su izquiedra y así hasta llegar a la quinta lámpara)* y la quinta están prendidas como lo indican el primer y quinto número 1.

Por ejemplo si tenemos los elementos $((1,0,0,1,1),4)$ y $((1,0,0,0,1),3)$ los estados corres-

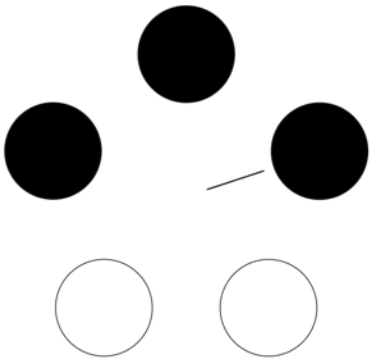

Figura 5.4: $((1,0,0,1,1),4)$

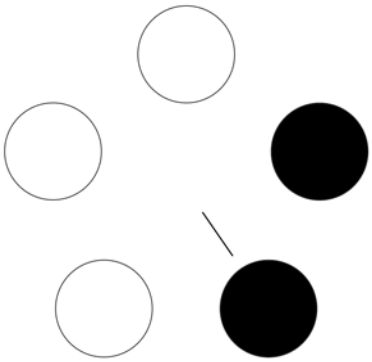

Figura 5.5: $((1,0,0,0,1),3)$

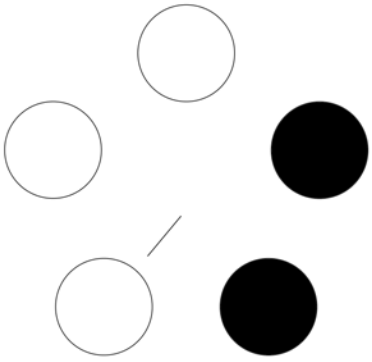

Figura 5.6: $((0,0,0,1,1),2)$

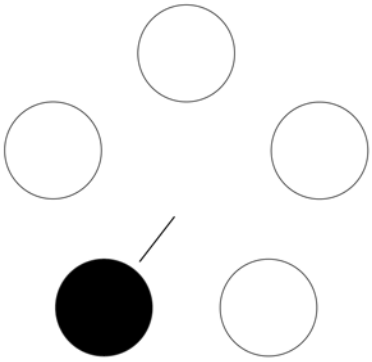

Figura 5.7: $((1,0,0,0,0),2)$

pondientes serían los de las figuras 5.4 y 5.5 respectivamente, ahora veamos cómo cambian los estados del arreglo de lámparas analizando la operación

$$((1,0,0,1,1),4)((1,0,0,0,1),3).$$

Visualicemos cómo sería aplicar el elemento $((1,0,0,1,1),4)$ al elemento $((1,0,0,0,1),3)$. Al estado de la figura 5.5 lo rotamos a la izquierda 4 veces sin mover de lugar las lámparas, sólo rotamos el punto inicial obteniendo momentaneamente el estado de la figura 5.6 el cual se representa $((0,0,0,1,1),2)$, después prendemos ó apagamos las lámparas que están en primer, cuarto y quinto lugar a partir del punto inicial en dirección a las manecillas del reloj como lo indica el elemento $((1,0,0,1,1),4)$, obteniendo finalmente el estado de la figura 5.7, el cual se representa de la forma $((1,0,0,0,0),2)$.

Algebraicamente obtendríamos lo siguiente

$$((1,0,0,1,1),4)((1,0,0,0,1),3) = ((1,0,0,0,0),2)$$

Esto nos dice que podemos interpretar estos elementos como si estuvieran en $\mathbb{Z}_2 \wr_r \mathbb{Z}_5$. Haciendo el cálculo obtenemos:

$$\begin{aligned} ((1,0,0,1,1),4)((1,0,0,0,1),3) &= ((1,0,0,1,1)(0,0,0,1,1),4+3) \\ &= ((1,0,0,0,0),4+3) \\ &= ((1,0,0,0,0),2) \end{aligned}$$

El producto trenzado de estos 2 grupos nos permite interpretar de manera formal el grupo formado por los estados del arreglo de lámparas. En el caso de tener n lámparas definimos el grupo de la siguiente forma.

Definición 5.26. *Sea $L_n = \mathbb{Z}_2 \wr_r \mathbb{Z}_n$ a este grupo se le conoce cómo **Lamplighter group**.*

5.5. Teorema de Kaloujnine

Lema 5.27. *Sea M un p-subgrupo de Sylow de S_m, entonces $|M| = p^{\mu(n)}$ donde*

$$\mu(n) = p^{n-1} + p^{n-2} + ... + p + 1$$

Demostración. Sean k y m enteros positivos tales que $k \leq m$ consideramos $t = [m/k]$ el mayor entero menor igual que m/k, entonces se cumple que $k, 2k, 3k, ..., tk \leq m$ y $(t+1)k > m$, notemos que t es el número de enteros positivos menores o iguales que m que son divisibles por k. Entonces es fácil darnos cuenta que $[m/k]$ es el número de factores de $m!$ que son divisibles por k.

Sea p un número primo, por nuestra observación anterior $[m/p]$ es el número de factores de $m!$ que son divisibles por p, análogamente $[m/p^2]$ es el número de factores de $m!$ que son divisibles por p^2 y así sucesivamente.

Consideremos los múltiplos de p que aparecen en la lista $1, 2, ..., m$ digamos

$$p^{k_1}m_1 < ... < p^{k_t}m_t$$

con $k_1, ..., k_t \in \mathbb{N}^+$ y $(p, m_i) = 1\ \forall i$ dado que los demás términos en $1, ..., m$ no son múltiplos de p se tiene que $m! = p^{k_1+...+k_t}s$ con $(p, s) = 1$, así la máxima potencia de p que divide a $m!$ es $p^{k_1+...+k_t}s$, es decir $\mu = k_1 + ... + k_t$ por otro lado los múltiplos de p en $1, ..., m$ son

$$p, 2p, ..., [m/p]p \tag{5.2}$$

los de p^2 son

$$p^2, 2p^2, ..., [m/p^2]p^2 \tag{5.3}$$

y así sucesivamente.

En el listado que sugieren 5.2 y 5.3 hay un total de $[m/p] + [m/p^2] + [m/p^3] + ...$ términos no necesariamente distintos, cada $p^{k_i}m_i$ contribuye a un múltiplo de p a saber $p(p^{k_i-1}m_i)$, un múltiplo de p^2, $p^2(p^{k_i-2}m_i)$, etcétera por lo cual $p^{k_i}m_i$ es contado k^i veces en el listado que sugieren 5.2 y 5.3. De aquí se concluye que

$$[m/p] + [m/p^2] + [m/p^3] + ... = k_1 + ... + k_t = \mu$$

En particular si $m = p^n$ entonces la potencia más grande de p que divide a $p!$ es

$$\mu(n) = p^{n-1} + p^{n-2} + ... + p + 1 \tag{5.4}$$

por lo tanto el orden de un p-subgrupo de Sylow de S_{p^n} es $p^{\mu(n)}$.

□

Observación 5.28. *Notemos que $p\mu(n) + 1 = \mu(n + 1)$, pues*

$$\begin{aligned} p\mu(n) + 1 = p(p^{n-1} + p^{n-2} + ... + p + 1) + 1 \quad &= (p^n + p^{n-1} + ... + p^2 + p) + 1 \\ &= p^n + p^{n-1} + ... + p^2 + p + 1 \\ &= \mu(n + 1) \end{aligned}$$

Teorema 5.29. ***Kaloujnine.*** *Si tenemos p un número primo, entonces un p-subgrupo de Sylow de S_{p^n} es el producto trenzado regular de n copias de $\mathbb{Z}_p$, $W_n = \mathbb{Z}_p \wr_r \mathbb{Z}_p \wr_r ... \wr_r \mathbb{Z}_p$ donde $W_{n+1} = W_n \wr_r \mathbb{Z}_p$*

Demostración. Esta prueba la haremos por inducción sobre n. Si $n = 1$ entonces $W_1 = \mathbb{Z}_p$ pues cualquier p-subgrupo de Sylow de orden S_p tiene orden p.

Ahora supongamos que $W_n = \mathbb{Z}_p \wr_r \mathbb{Z}_p \wr_r ...\mathbb{Z}_p$. Sea Λ un conjunto con p^n elementos y sea D un p-subgrupo de Sylow de S_Λ, notemos que Λ es un D-conjunto. Ahora consideremos $\Omega = \{0, 1, 2, ...p - 1\}$ y $Q =< q >$, donde Q es un grupo cíclico de orden p actuando en Ω de la forma $qi = i + 1\ mod p$. La versión de permutación $P \cong D \wr_r \mathbb{Z}_p$ es un subgrupo de $S_{\Lambda\times\Omega}$. Notemos que $|\Lambda \times \Omega| = p^{n+1}$ y sabemos por hipótesis de inducción que D es un producto trenzado regular de n copias de $\mathbb{Z}_p$ por lo tanto P es isomorfo al producto de $n+1$ copias de $\mathbb{Z}_p$.

Ahora verifiquemos que P es un p-subgrupo de Sylow, por el Lema 5.27 sólo necesitamos verificar que el orden de P es $p^{\mu(n+1)}$. Sabemos que $|D| = p^{\mu(n)}$ entonces

$$|P| = |D \wr_r \mathbb{Z}_p| = (p^{\mu(n)})^p p = p^{p\mu(n)+1}$$

y por la Observacion 5.28 concluimos que $|P| = p^{p\mu(n)+1} = p^{\mu(n+1)}$. □

El teorema de **Kaloujnine** nos da la posibilidad de calcular el p-subgrupo de Sylow de cuaqluier S_m. El siguiente corolario nos da un método para encontrarlo.

Corolario 5.30. *Sea S_m el grupo simétrico donde $m \in \mathbb{N}$, entonces existe un p-subgrupo de Sylow de S_m de orden p^N donde $N = a_1 + a_2\mu(2) + ... + a_t(t)$ con $0 \leq a_i \leq p-1$ y $\mu(i)$ como en la ecuación 5.4.*

Demostración. Expresamos a m en su base p como una suma de potencias de p de la siguiente manera

$$m = a_0 + a_1 p + a_2 p^2 + ... + a_t p^t$$

donde $0 \leq a_i \leq p-1$.

Consideremos el conjunto $X = \{1, 2, ..., m\}$ y dividimos este conjunto en a_0 subconjuntos de X de orden 1, a_1 subconjutos de orden p, a_2 subconjuntos de orden p^2 y así hasta a_t subconjuntos de orden p^t, para cada uno de esos subconjuntos consideramos el grupo S_{p^i} y con el teorema de **Kaloujnine** construimos un p-subgrupo de Sylow para cada S_{p^i}, como las permutaciones disjuntas conmutan entonces G, el producto directo de todos esos p-subgrupos de Sylow es un subgrupo de S_X de orden p^N donde $N = a_1 + a_2\mu(2) + ... + a_t(t)$ donde $\mu(i)$ es como en la ecuación 5.4.

Verifiquemos ahora que N es la máxima potencia de p que divide a $m!$ para concluir que G es p-subgrupo de Sylow.

Como

$$m = a_0 + a_1 p + a_2 p^2 + ... + a_t p^t$$

tenemos que $[m/p] = a_1 + a_2 p + a_3 p^2 + ... + a_t p^{t-1}$, $[m/p^2] = a_2 + a_3 p + a_4 p^2 + ... + a_t p^{t-2}$, $[m/p^3] = a_3 + a_4 p + ... + a_t p^{t-3}$ y así hasta $[m/p^t] = a_t$, entonces la suma de todos los $[m/p^i]$ cumple que

$$\begin{aligned} \textstyle\sum_{i=1}^{t}[m/p^i] &= a_1 + a_2(p+1) + a_3(p^2+p+1) + ... + a_t(p^{t-1} + p^{t-2} + ... + p + 1) \\ &= a_1 + a_2\mu(2) + ... + a_t\mu(t) = N \end{aligned}$$

Con esto verificamos que el producto directo G tiene el orden necesario para ser p-subgrupo de Sylow de S_m.

□

Ejemplo 5.31. *Utilicemos el Corolario 5.30 para calcular un 2-subgrupo de Sylow de S_6, escribimos*

$$6 = 0(2^0) + 1(2^1) + 1(2^2)$$

ahora $\mathbb{Z}_2$ es 2-subgrupo de Sylow de S_2 y $\mathbb{Z}_2 \wr_r \mathbb{Z}_2$ es 2-subgrupo de Sylow de S_4. Entonces un 2-subgrupo de Sylow de S_6 es $P = \mathbb{Z}_2 \times (\mathbb{Z}_2 \wr_r \mathbb{Z}_2)$ y como vimos en el Ejemplo 5.3

$$\mathbb{Z}_2 \wr_r \mathbb{Z}_2 \cong D_4$$

por lo que $P \cong \mathbb{Z}_2 \times D_4$.

Bibliografía

[1] Joseph J. Rotman *An Introduction to the Theory of Groups*, Fourth Edition, Springer, E.U., 1994.

[2] J.L Alperin, Rowen B. Bell *Groups and representations*, Springer, E.U., 1995.

[3] Diana Avella A., Octavio Mendoza H., Edith Corina Sáenz V. y María José Souto S. *Grupos I*, Segunda Edicion, Colección Papirhos Instituto de Matemáticas de la UNAM, México., 2014.

[4] Diana Avella A., Octavio Mendoza H., Edith Corina Sáenz V. y María José Souto S. *Grupos II*, Colección Papirhos Instituto de Matemáticas de la UNAM, México., 2016.

[5] I. N. Herstein, *Álgebra Abstracta*, Grupo Editorial Iberoamérica Edición S.A. de C.V. Original en inglés publicada por Macmillan Publishing Company, E.U., 1986.

[6] John B. Fraleigh, Victor J. Katz *A first course in abstract algebra*, Seventh Edition, Addison-Wesley Publishing Company, E.U., 2002.

[7] Francisco José González G., *Apuntes de Matemática Discreta. 10. Divisibilidad. Algoritmo de la División*, Universidad de Cádiz, España., 2004, http://www2.uca.es/matematicas/Docencia/ESI/1710003/Apuntes/Leccion10.pdf

[8] Francisco José González G., *Apuntes de Matemática Discreta. 11. Teorema Fundamental de la Aritmética*, Universidad de Cádiz, España., 2004, http://www2.uca.es/matematicas/Docencia/ESI/1710003/Apuntes/Leccion11.pdf

[9] Jaime Gutiérrez G. y Carlos Ruiz de Velasco y Bellas *Lecciones de Algebra*, Universidad de Cantabria. España 2002, http://personales.unican.es/ruizvc/algebra/divisibilidad1.pdf