CUADERNOS DE ÁLGEBRA

No. 1

Grupos

Oswaldo Lezama

Departamento de Matemáticas
Facultad de Ciencias
Universidad Nacional de Colombia
Sede de Bogotá

30 de junio de 2014

Cuaderno dedicado a Justo Pastor, mi padre.

Contenido

Prólogo

La colección *Cuadernos de álgebra* consta de 10 publicaciones sobre los principales temas de esta rama de las matemáticas, y pretende servir de material para preparar los exámenes de admisión y de candidatura de los programas colombianos de doctorado en matemáticas. Los primeros cinco cuadernos cubren el material básico de los cursos de estructuras algebraicas y álgebra lineal de los programas de maestría; los cinco cuadernos siguientes contienen algunos de los principales temas de los exámenes de candidatura, a saber: anillos y módulos; categorías; álgebra homológica; álgebra no conmutativa; álgebra conmutativa y geometría algebraica. Cada cuaderno es fruto de las clases dictadas por el autor en la Universidad Nacional de Colombia en los últimos 25 años, y están basados en las fuentes bibliográficas consignadas en cada uno de ellos, como también en el libro *Anillos, Módulos y Categorías*, publicado por la Facultad de Ciencias de la Universidad Nacional de Colombia, y cuya edición está totalmente agotada (véase [8]). Un material similar, pero mucho más completo que el presentado en estas diez publicaciones, es el excelente libro de Serge Lang, *Algebra*, cuya tercera edición revisada ha sido publicada por Springer en el 2004 (véase [7]). Posiblemente el valor de los *Cuadernos de álgebra* sea su presentación ordenada y didáctica, así como la inclusión de muchas pruebas omitidas en la literatura y suficientes ejemplos que ilustran la teoría. Los cuadernos son:

1. **Grupos**
2. Anillos
3. Módulos
4. Álgebra lineal
5. Cuerpos
6. Anillos y módulos
7. Categorías
8. Álgebra homológica
9. Álgebra no conmutativa
10. Álgebra conmutativa y geometría algebraica

Los cuadernos están dividido en capítulos, los cuales a su vez se dividen en secciones. Para cada capítulo se añade al final una lista de ejercicios que debería ser complementada por los lectores con las amplias listas de problemas que inluyen las principales monografías relacionadas con el respectivo tema.

Cuaderno de grupos. La teoría de grupos, como todas las ramas del álgebra contemporánea, estudia ciertos objetos matemáticos llamados grupos, así como las relaciones entre estos objetos, llamadas homomorfismos. Podríamos justificar el es-

tudio de la teoría de los grupos diciendo que los conjuntos son para la matemática como los grupos son para el álgebra.

En el primer capítulo daremos la definición axiomática de la estructura abstracta de grupo y veremos algunos conjuntos estructurados como grupos. Se estudiará la noción de subgrupo y se demostrará un teorema de gran imortancia dentro de la teoría de grupos finitos como es el teorema de Lagrange. Quizá los grupos abelianos más importantes son los llamados grupos cíclicos, ya que los grupos abelianos finitamente generados son expresables a través de sumas directas de grupos cíclicos.

En el segundo capítulo mostraremos las propiedades básicas de los grupos cíclicos. El objetivo central del capítulo 3 es mostrar la estrecha relación que guardan los conceptos de subgrupo normal y homomorfismo de grupos. Será demostrado que, salvo isomorfismo, hay tantos subgrupos normales en un grupo G como imágenes homomorfas tiene este último.

El concepto de homomorfismo e isomorfismo, así com o los teoremas correspondientes, son el objeto del capítulo 4. Por medios de estos teoreams se pueden caracterizar las imágenes homomorfas de un grupo, y son herramienta clave para la clasificación de grupos, en particular, para la clasificación de grupos finitos. Los homomorfismos biyectivos de un grupo G en si mismo se conocen como los automorfismos de G. Estas funciones conforman un grupo que tiene información importante relativa sobre grupo G y serán estudiados en el quinto capítulo.

En el capítulo 6 estudiaremos con algún detalle al grupo simétrico S_n. Destacaremos en S_n el subgrupo alternante A_n y describiremos el grupo dihédrico de grado n, D_n por medio de permutaciones. El objetivo del capítulo 7 es presentar la construcción del grupo producto cartesiano y la suma directa externa para una familia dada de grupos. Como fundamento teórico para la demostración de los teoremas de Sylow, en el capítulo 8 serán tratadas las acciones de grupos sobre conjuntos. Para los grupos cíclicos finitos es válido el recíproco del teorema de Lagrange (véase el segundo capítulo), es decir, si G un grupo cíclico finito de orden n y m divide a n entonces G contiene exactamente un subgrupo de orden m. En el noveno capítulo se mostrará que la afirmación anterior es válida para cuando m es potencia de un primo. Este resultado es uno de los famosos teoremas de Sylow.

El objetivo del capítulo 10 es describir para un entero positivo n dado todos los grupos abelianos de orden n (salvo isomorfismo). Se incluirá tambien en este capítulo una tabla con la lista de todos los grupos de orden ‘15. Por último, una de las más importantes generalizaciones de la noción de conmutatividad es la solubilidad, de la cual nos ocupamos en el capítulo 11.

El material presentado en está complementado con una gran variedad de ejemplos que ilustran las definiciones y propiedades estudiadas a lo largo del texto. Estos ejemplos constituyen parte muy importante de la teoría básica de grupos introducida en el presente cuaderno.

El autor desea expresar su agradecimiento a Milton Armando Reyes Villamil, discípulo y amigo, por la digitalización del material del presente cuaderno.

Oswaldo Lezama
Departamento de Matemáticas
Universidad Nacional de Colombia
Bogotá, Colombia
jolezamas@unal.edu.co

Capítulo 1

Grupos y subgrupos

La teoría de grupos estudia ciertos objetos matemáticos llamados grupos, así como las relaciones entre ellos, los homomorfismos. Podríamos justificar el estudio de la teoría de los grupos diciendo que los conjuntos son para la matemática como los grupos son para el álgebra. En este primer capítulo presentamos la definición axiomática de la estructura abstracta de grupo y veremos algunos ejemplos notables. Se estudiará la noción de subgrupo y se demostrará un teorema de gran importancia dentro de la teoría de grupos finitos como es el teorema de Lagrange sobre clases laterales.

1.1. Operaciones binarias y estructuras algebraicas elementales

En esta sección definimos el concepto de operación entre elementos de un conjunto, noción que hemos utilizado tácitamente en todas nuestras matemáticas elementales. Se dará además una definición precisa de las propiedades más comunes de las que gozan estas operaciones. Esto permitirá introducir posteriormente la estructura de grupo.

Definición 1.1.1. *Sea G un conjunto no vacío. Una* ***operación binaria interna*** *(ley de composición interna) en G es una función $\triangle : G \times G \to G$ del producto cartesiano de G con G en G.*

Así pues, a cada par ordenado (x, y) de elementos de G se le asigna un único elemento de G. La imagen del par (x, y) mediante la función $\triangle$ se denota por $x \triangle y$. Se dice también que $x \triangle y$ es el resultado de operar x con y (en ese orden).

Ejemplo 1.1.2. La adición de números naturales es una ley de composición:

$$\begin{aligned} + : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (a, b) &\mapsto a + b. \end{aligned}$$

Ejemplo 1.1.3. En $\mathbb{N}$ podemos definir una función $\triangle$ por

$$\begin{aligned} \triangle : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (a, b) &\mapsto \text{mín}(a, b). \end{aligned}$$

$\triangle$ es una operación binaria interna en $\mathbb{N}$. Por ejemplo, $3\triangle 4{=}3$, $5\triangle 2{=}2$, y $3\triangle 3{=}3$.

Ejemplo 1.1.4. Sea X un conjunto no vacío y sea $\boldsymbol{P(X)}$ el conjunto de todos los subconjuntos de X. La intersección de conjuntos define una operación binaria interna en $P(X)$:

$$\begin{aligned} \cap : P(X) \times P(X) &\to P(X) \\ (A, B) &\mapsto A \cap B. \end{aligned}$$

Ejemplo 1.1.5. En el conjunto de los números naturales $\mathbb{N}$ definimos la función:

$$\begin{aligned} * : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ a * b &\mapsto (a \triangle b) + 2, \end{aligned}$$

donde la operación $\triangle$ es como en el ejemplo 1.1.3. Así pues,

$$\begin{aligned} 5 * 3 = (5\triangle 3) + 2 = 3 + 2 = 5, \\ 4 * 4 = (4\triangle 4) + 2 = 4 + 2 = 6. \end{aligned}$$

Ejemplo 1.1.6. La función $\nabla : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, definida por $a\nabla b = (ab) \div 2$, no define en $\mathbb{Z}$ una operación binaria interna.

Dado un conjunto G con una operación binaria interna Δ y dados 3 elementos a,b y c del conjunto G, podemos preguntarnos las maneras de operar estos tres elementos en ese orden e investigar si los resultados de estas formas de operar coinciden. Así pues, en el ejemplo 1.1.2 sean 2,5, $7 \in \mathbb{N}$. Entonces,

$$2 + 5 = 7,\ 7 + 7 = 14,\ 5 + 7 = 12,\ 2 + 12 = 14.$$

Es decir, $(2 + 5) + 7 = 2 + (5 + 7)$, donde los paréntesis indican la secuencia en que se han efectuado las operaciones. Es bien conocido que para la adición de números naturales esta propiedad es válida, es decir, cualesquiera que sean $a, b, c \in \mathbb{N}$, se cumple $(a + b) + c = a + (b + c)$. Nótese sin embargo que en el ejemplo 1.1.5 sobre $\mathbb{N}$ se definió la operación $*$ la cual no cumple esta propiedad:

$$(3 * 5) * 7 = 5 * 7 = 7,\ 3 * (5 * 7) = 3 * 7 = 5.$$

Esto permite clasificar las operaciones binarias de acuerdo con esta condición.

Definición 1.1.7. *Sea $*$ una operación binaria definida sobre un conjunto G. Se dice que la operación $*$ tiene la propiedad* ***asociativa****, o que * es una operación asociativa, si para cualesquiera elementos a,b,c de G se cumple la igualdad*

$$a * (b * c) = (a * b) * c.$$

De esta definición surge una pregunta inmediata: en el caso que sean dados $4, 5$, ó n elementos (en un orden determinado), ¿la secuencia en que se efectuen las operaciones influye en el resultado? Se puede probar por inducción sobre n que si la operación es asociativa, es decir, si para el caso de 3 elementos se tiene la propiedad exigida, entonces la misma propiedad tendrá lugar para cualesquiera n elementos dados . Así pues, si se dan n elementos $a_1, \ldots, a_n$ del conjunto G y suponiendo que la operación $*$ de G es asociativa, los paréntesis que indican la secuencia de como se realizan las operaciones en la expresión $a_1 * \cdots * a_n$ pueden ser colocados donde se quiera y el resultado no varía.

Proposición 1.1.8. *Sea G un conjunto donde se ha definido una operación binaria asociativa $*$. Para $a \in G$, sea*

$$a^1 := a,\ a^n := a^{n-1} * a, \quad n \geq 2.$$

Entonces, para cualesquiera naturales m y n se tienen las identidades

$$a^n * a^m = a^{n+m},\ (a^n)^m = a^{nm}.$$

Demostración. La prueba se realiza por inducción y se deja como ejercicio al lector. □

Definición 1.1.9. *Un* ***semigrupo*** *es un conjunto G dotado de una operación binaria interna asociativa $*$, y se denota por $(G, *)$. Se dice también que sobre G se tiene una estructura de semigrupo.*

Ejemplo 1.1.10. $(\mathbb{N}, +)$ es un semigrupo.

Ejemplo 1.1.11. Sea X un conjunto no vacío cualquiera y sea $\boldsymbol{Aplc(X)}$ el conjunto de aplicaciones (funciones) de X en si mismo. Por teoría elemental de conjuntos sabemos que la operación composición de funciones $\circ$ es una operación binaria interna en $Aplc(X)$, y además es asociativa. Así pues, $(Aplc(X), \circ)$ es un semigrupo.

El ejemplo anterior ilustra que no toda operación binaria $*$ definida sobre un conjunto G satisface $a * b = b * a$ para todos los elementos a y b de G.

Definición 1.1.12. *Sea $*$ una operación binaria definida sobre un conjunto G. Se dice que la operación $*$ es **conmutativa** si para cualesquiera elementos a y b de G se tiene que:*

$$a * b = b * a.$$

Mediante inducción es fácil probar la siguiente propiedad.

Proposición 1.1.13. *Sea $(G, *)$ un semigrupo conmutativo, es decir, la operación $*$ es asociativa y conmutativa. Entonces, para cualequiera $a, b \in G$ y cualquier natural n se tiene que:*

$$(a * b)^n = a^n * b^n.$$

Demostración. Ejercicio para el lector. □

Existen conjuntos con operaciones binarias internas donde se destacan elementos especiales.

Definición 1.1.14. *Sea G un conjunto en el cual se ha definido una operación binaria $*$. Se dice que el elemento e de G es una **identidad** de G con respecto a la operación $*$ si para cualquier elemento de G se tiene que:*

$$e * a = a = a * e.$$

Ejemplo 1.1.15. En el semigrupo $(\mathbb{Z}, +)$, donde $\mathbb{Z}$ es el conjunto de números enteros y $+$ es la adición habitual, 0 es una identidad.

Surge la siguiente pregunta: ¿en un conjunto G con una operación binaria $*$ pueden existir varias identidades?

Proposición 1.1.16. *En un conjunto G con una operación binaria $*$ solo puede existir un elemento identidad respecto de $*$.*

Demostración. Sean e, e' dos identidades, entonces $e * e' = e = e'$. □

Nótese que para diferentes operaciones, las identidades no necesariamente coinciden, como tampoco cada operación debe tener un elemento identidad. Por ejemplo, 0 es la identidad del semigrupo $(\mathbb{Z}, +)$, 1 es la identidad de $(\mathbb{Z}, \cdot)$ y $(\mathbb{N}, +)$ no tiene identidad.

Definición 1.1.17. *Un **monoide** es un semigrupo que posee elemento identidad.*

Definición 1.1.18. *Sea G un conjunto dotado de una operación binaria interna $*$ la cual posee un elemento identidad e, se dice que $u \in G$ es **invertible** si existe $u' \in G$ tal que $u' * u = e = u * u'$. El elemento u' se denomina el **inverso** de u respecto de la operación $*$.*

En la definición anterior no se exige que cada elemento de G sea invertible. Sin embargo, de esta definición se desprende lo siguiente.

Proposición 1.1.19. *Sea G un monoide.*

(i) *Si $u \in G$ es invertible entonces su inverso u' es único.*

(ii) *Sean x', u' los inversos de x y u respectivamente. Entonces, $x * u$ es invertible y además*

$$(x * u)' = u' * x' \ , \ (x')' = x.$$

Demostración. Notemos que $(u' * x') * (x * u) = 1 = (x * u) * (u' * x')$. De igual manera, puesto que $x' * x = 1 = x * x'$, entonces $(x')' = x$. □

1.2. Grupos

En la sección anterior fueron estudiadas algunas propiedades que pueda tener una operación binaria definida en un conjunto. Así pues, se dijo que cuando la operación binaria $*$ definida sobre el conjunto G es asociativa se obtiene sobre el conjunto G una estructura de semigrupo. Al poseer la operación $*$ más propiedades, la estructura se hace más rica y las posibilidades de operar en G se hacen mayores. Un ejemplo de tal situación lo constituyen los llamados grupos, los cuales pasamos a definir.

Definición 1.2.1. *Sea G un conjunto no vacío y $*$ una operación binaria definida en G. Se dice que G es un **grupo** respecto de $*$, o también que $*$ da a G una estructura de grupo, si $*$ cumple las siguientes propiedades:*

(i) *$*$ es asociativa.*

(ii) *En G existe un elemento identidad e respecto de $*$.*

(iii) *Cada elemento de G es invertible.*

Denotaremos un grupo por $(G, *)$, pero cuando no haya ambiguedad sobre la operación $*$, escribiremos simplemente G.

Definición 1.2.2. *Un grupo $(G, *)$ es **conmutativo**, también denominado **abeliano**, si la operación $*$ es conmutativa.*

Ejemplo 1.2.3. Los siguientes conjuntos numéricos, donde las operaciones indicadas son las habituales, constituyen grupos conmutativos:

$$(\mathbb{Z}, +, 0), (\mathbb{Q}, +, 0), (\mathbb{R}, +, 0), (\mathbb{C}, +, 0).$$

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ denotan los conjuntos de números enteros, racionales, reales y complejos, respectivamente.

Ejemplo 1.2.4. Los siguientes ejemplos no conforman grupos:

$(\mathbb{Z}, \cdot, 1)$: sólo hay dos elementos invertibles: 1 y -1,
$(\mathbb{Q}, \cdot, 1)$: el cero no es invertible,
$(\mathbb{R}, \cdot, 1)$: el cero no es invertible,
$(\mathbb{C}, \cdot, 1)$: el cero no es invertible.

Ejemplo 1.2.5. ***El grupo de elementos invertibles de un semigrupo***: sea $(G, ., 1)$ un monoide con identidad 1. Entonces, el conjunto de elementos de G que son invertibles no es vacío y, respecto de la misma operación, constituye un grupo, el cual se acostumbra a denotar por G^*: $G^* \neq \emptyset$ ya que $1 \in G^*$; sean $x, y \in G^*$, entonces $xy \in G^*$ ya que $xyy'x' = 1, y'x'xy = 1$. Puesto que la operación que actúa sobre los elementos de G^* es la misma que la de G, entonces la propiedad asociativa también se cumple para G^*. $1 \in G^*$ es la identidad. Por último, de acuerdo con la definición de G^*, cada uno de sus elementos es invertible y su inverso está en G^*.

Notemos por ejemplo que $(\mathbb{Z}, ., 1)$ es un semigrupo conmutativo con elemento identidad 1 y

$$\mathbb{Z}^* = \{1,- 1\}.$$

De igual manera,

$$(\mathbb{Q}^*, \cdot, 1); (\mathbb{R}^*, \cdot, 1); (\mathbb{C}^*, \cdot, 1)$$

son grupos conmutativos, con

$$\mathbb{Q}^* = \mathbb{Q} \backslash \{0\}, \mathbb{R}^* = \mathbb{R} \backslash \{0\}, \mathbb{C}^* = \mathbb{C} \backslash \{0\}.$$

De la proposición 1.1.19 y de la definición de grupo se obtienen de manera inmediata las siguientes conclusiones.

Proposición 1.2.6. *Sea $(G, \cdot, 1)$ un grupo. Entonces,*

(i) *El elemento identidad 1 del grupo G es único.*

(ii) *Cada elemento x de G tiene un único inverso, el cual se denota por x^{-1}.*

(iii) *Se cumple la* ***ley cancelativa****, es decir, para cualesquiera elementos $x, y, z \in G$ se tiene que*

$$x \cdot z = y \cdot z \Leftrightarrow x = y$$
$$z \cdot x = z \cdot y \Leftrightarrow x = y.$$

(iv) *Sean a, b elementos cualesquiera de G, entonces las ecuaciones lineales $a \cdot x = b$ y $z \cdot a = b$ tienen solución única en G.*

Demostración. Ejercicio para el lector. □

La proposición que demostraremos a continuación indica que los axiomas que definen un grupo pueden ser debilitados.

Proposición 1.2.7. *Sea $(G, *)$ un semigrupo. Entonces, G es un grupo si, y sólo si, $*$ tiene las siguientes propiedades:*

(i) *Existe un elemento identidad a la izquierada $e \in G$ tal que $e*x = x$, para cada $x \in G$.*

(ii) *Para cada $x \in G$ existe $x' \in G$ tal que $x' * x = e$.*

Demostración. $\Rightarrow$) Las condiciones (i) y (ii) se cumplen trivialmente ya que G es un grupo.

$\Leftarrow$) Sea $(G, *)$ un semigrupo en el cual se cumplen las condiciones (i) y (ii). Demostremos que el inverso x' de x a la izquierda es también a la derecha, es decir,

$$x * x' = e.$$

Sea $x * x' = y \in G$, entonces

$$y * y = x * x' * x * x' = x * (x' * x) * x' = x * (e * x') = x * x' = y.$$

Ahora, por (ii), existe $y' \in G$ tal que $y' * y = e$. Así pues, de $y * y = y$ se deduce que

$$(y' * y) * y = y' * y, \text{ luego } e * y = e, \text{ es decir, } y = e, \text{ de donde, } x * x' = e.$$

Finalmente, probemos que $x * e = x$:

$$x * e = x * (x' * x) = (x * x') * x = e * x = x.$$

□

Observación 1.2.8. (i) Según la proposición anterior, si se da un semigrupo G, es suficiente encontrar en G un elemento identidad a la izquierda e y encontrar para cada $x \in G$ un inverso a la izquierda x' para concluir que G es un grupo.

(ii) La proposición anterior es válida para el caso derecho.

(iii) No es siempre cierto que si en un semigrupo $(G, *)$ tiene lugar la propiedad (i) por la derecha y la propiedad (ii) por la izquierda el sistema sea un grupo. Por ejemplo, sea G un conjunto no vacío cualquiera y sea $*$ definida por $a * b = a$. $*$ es claramente asociativa. Además, cualquier elemento x_0 de G es identidad a la derecha: $a * x_0 = a$. También, dado $a \in G$, a tiene inverso a la izquierda respecto del elemento x_0 : $x_0 * a = x_0$. Sin embargo, $(G, *)$ no es un grupo en el caso que G tenga al menos tres elementos distintos a, b, c. En efecto, si G fuera un grupo se tendría la ley cancelativa:

$$a * b = a,$$
$$a * c = a,$$
$$a * b = a * c \Rightarrow b = c.$$

Analogamente, si tiene lugar la propiedad (i) a la izquierda y la propiedad (ii) a la derecha, el sistema $(G, *)$ no es necesariamente un grupo.

Presentamos a continuación algunos ejemplos notables de grupos.

Ejemplo 1.2.9. El grupo de elementos invertibles del semigrupo $Aplc(X)$, denotado por $\boldsymbol{S(X)}$, está constituido por las funciones $f : X \to X$ tales que existe $g : X \to X$ para la cual $f \circ g = i_X = g \circ f$. En otras palabras, $f \in S(X)$ si, y sólo si, f es una función biyectiva. $S(X)$ es pues el grupo de todas las funciones biyectivas definidas de X en X. En el caso en que X sea un conjunto finito de $n \geq 1$ elementos, $S(X)$ se denota por S_n. Este grupo será estudiado en detalle en el capítulo 6. Para el caso $n = 3$, los elementos de S_3 son:

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ \downarrow & \downarrow & \downarrow \\ x_1 & x_2 & x_3 \end{pmatrix}, \begin{pmatrix} x_1 & x_2 & x_3 \\ \downarrow & \downarrow & \downarrow \\ x_1 & x_3 & x_2 \end{pmatrix}, \begin{pmatrix} x_1 & x_2 & x_3 \\ \downarrow & \downarrow & \downarrow \\ x_3 & x_2 & x_1 \end{pmatrix}$$
$$\begin{pmatrix} x_1 & x_2 & x_3 \\ \downarrow & \downarrow & \downarrow \\ x_2 & x_1 & x_3 \end{pmatrix}, \begin{pmatrix} x_1 & x_2 & x_3 \\ \downarrow & \downarrow & \downarrow \\ x_2 & x_3 & x_1 \end{pmatrix}, \begin{pmatrix} x_1 & x_2 & x_3 \\ \downarrow & \downarrow & \downarrow \\ x_3 & x_1 & x_2 \end{pmatrix}$$

Notemos que este grupo no es conmutativo.

Ejemplo 1.2.10. Sea X un conjunto no vacío y sea $(G, .)$ un grupo con elemento identidad 1. Sea $\boldsymbol{Aplc(X,G)}$ el conjunto de funciones de X en G. Se define en este conjunto la siguiente operación:

$$\begin{aligned} fg : X &\to G \\ x &\to (fg)(x) = f(x) \cdot g(x), \end{aligned}$$

donde f, g son elementos de $Aplc(X, G)$ y $x \in X$. Esta operación convierte a $Aplc(X, G)$ en un grupo. Nótese que el elemento identidad es la función i que asigna a cada elemento x de X el elemento identidad 1 de G. El inverso de la función f es una función f^{-1} tal que $f^{-1}(x) = f(x)^{-1}$, para cada $x \in X$. Un caso particular de esta construcción es cuando $X = \mathbb{N}$ y $G = (\mathbb{R}, +)$, en este caso $Aplc(\mathbb{N}, \mathbb{R})$ es el ***grupo de sucesiones reales***.

Ejemplo 1.2.11. Del álgebra lineal tenemos el siguiente ejemplo: sea $\boldsymbol{M_{n\times m}}(\mathbb{R})$ el conjunto de matrices rectangulares de n filas y m columnas con la operación habitual de adición definida sobre las entradas de las matrices. Esta operación convierte a $M_{n\times m}(\mathbb{R})$ en un grupo conmutativo, en el cual el elemento identidad es la matriz

nula y el inverso aditivo de una matriz $F := [f_{ij}]$ es la matriz cuyas entradas son los elementos opuestos a las entradas de la matriz F, es decir, $-F := [-f_{ij}]$. El grupo de matrices cuadradas de tamaño $n \times n$ se denota por $M_n(\mathbb{R})$.

Ejemplo 1.2.12. En álgebra elemental se consideran los ***polinomios*** $a_0 + a_1x + \cdots + a_nx^n$ con coeficientes reales; la colección de todos estos polinomios (n no es fijo) se denota por $\mathbb{R}[x]$, y constituye un grupo respecto de la adición mediante reducción de términos semejantes. El polinomio nulo es el elemento identidad y el inverso aditivo de un polinomio se obtiene cambiandole el signo a cada uno de sus coeficientes.

1.3. Subgrupos

Dado un grupo $(G, \cdot, 1)$ y un subconjunto no vacío S de G, es intresante conocer si bajo la misma operación binaria S tiene también estructura de grupo. Lo primero que deberá cumplirse es que el producto $x \cdot y$ de dos elementos del conjunto S debe permanecer también en S.

Definición 1.3.1. *Sean $(G, \cdot, 1)$ un grupo y $S \neq \emptyset$ un subconjunto G. Se dice que S es un **subgrupo** de G si S bajo la operación $\cdot$ tiene estructura de grupo. En tal caso se escribe $S \leq G$.*

De acuerdo con esta definición tendríamos que verificar cuatro condiciones para garantizar que un subconjunto $\emptyset \neq S \subseteq G$ constituye un subgrupo:

(i) Si $x, y \in S$, entonces $x \cdot y \in S$.

(ii) La operación $\cdot$ es asociativa en S.

(iii) En S hay elemento identidad con respecto a la operación $\cdot$

(iv) Cada elemento x de S tiene un inverso x^{-1} en S respecto de la operación $\cdot$ y del elemento identidad encontrado en (iii).

Sin embargo, como lo muestra la siguiente proposición, sólo hay que comprobar el cumplimiento de dos condiciones.

Proposición 1.3.2. *Sea $(G, \cdot, 1)$ un grupo y $\emptyset \neq S \subseteq G$. S es un subgrupo de G respecto de la operación $\cdot$ si, y sólo si, se cumplen las siguientes condiciones:*

(i) *Si $a, b \in S$ entonces $a \cdot b \in S$.*

(ii) *Si $a \in S$ entonces $a^{-1} \in S$.*

Demostración. $\Rightarrow$): si S es un subgrupo de G, entonces S bajo la operación $\cdot$ es un grupo. Por tanto, $\cdot$ es una operación binaria en S, con lo cual se garantiza la condición (i). Puesto que $S \neq \emptyset$, sea $a \in S$; sabemos entonces que las ecuaciones $a \cdot x = a$ y $x \cdot a = a$ tienen soluciones únicas en el grupo S, pero estas condiciones pueden ser consideradas en el grupo G, por tanto, 1, que es la solución de ellas en G, debe ser también la solución en S, es decir, $1 \in S$. Ahora, las ecuaciones $a \cdot x = 1$ y $x \cdot a = 1$ también tienen soluciones únicas tanto en S como en G. Esto indica que $a^{-1} \in S$ y la condición (ii) está demostrada.

$\Leftarrow$): la condición (i) indica que $\cdot$ define en S una operación binaria interna. La asociatividad de $\cdot$ en S es evidente ya que se cumple para todos los elementos de G, en particular, para los elementos de S. Sea $a \in S$ ($S \neq \emptyset$). Entonces, según (ii), $a^{-1} \in S$, y según (i), $a \cdot a^{-1} = 1 = a^{-1} \cdot a \in S$. □

Ejemplo 1.3.3. ***Subgrupos triviales***. Todo grupo $(G, \cdot, 1)$ tiene al menos dos subgrupos, llamados sus subgrupos triviales:

$$1 := \{1\},\ G := (G, \cdot, 1).$$

Ejemplo 1.3.4. $(\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0) \leq (\mathbb{R}, +, 0) \leq (\mathbb{C}, +, 0)$.

Esta cadena de subgrupos induce la siguiente propiedad evidente.

Proposición 1.3.5. *Sean $(G, \cdot, 1)$ un grupo, $(H, \cdot, 1)$ un subgrupo de G y $(K, \cdot, 1)$ un subgrupo de H, entonces $(K, \cdot, 1)$ es un subgrupo de $(G, \cdot, 1)$.*

Demostración. Evidente a partir de la proposición 1.3.2. □

Ejemplo 1.3.6. $(\mathbb{Z}^*, \cdot, 1) \leq\ (\mathbb{Q}^*, \cdot, 1) \leq (\mathbb{R}^*, \cdot, 1) \leq (\mathbb{C}^*, \cdot, 1)$.

Ejemplo 1.3.7. Sea X un conjunto no vacío y sea $S(X)$ el grupo de permutaciones de X respecto de la operación de composición de funciones. Sea x_0 un elemento fijo de X. Sea $C := \{f \in S(X) \mid f(x_0) = x_0\}$ el conjunto de funciones que dejan fijo el punto x_0. Entonces, $C \leq S(X) : C \neq \emptyset$ ya que $i_X \in C$. Sean $f, g \in C$, entonces $(f \circ g)(x_0) = f\,[g(x_0)] = f(x_0) = x_0$, así pues $f \circ g \in C$. Ahora, sea $f \in C; f^{-1}(x_0) = f^{-1}\,[f(x_0)] = (f^{-1} \circ f)(x_0) = i_X(x_0) = x_0$, por tanto $f^{-1} \in C$.

Como caso particular, sea $S(X) = S_3$ y sea C el conjunto de permutaciones que dejan fijo el punto 3, entonces

$$C = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

Ejemplo 1.3.8. Para un semigrupo con notación multiplicativa fueron definidas las potencias enteras positivas (véase la proposición 1.1.8). Pretendemos ahora extender estas potencias a todos los enteros y presentar la correspondiente notación para el caso de los grupos aditivos. Sea G un grupo, entonces

Notación multiplicativa	***Notación aditiva***
$(G, \cdot, 1)$	$(G, +, 0)$
$a^1 =: a$	$1 \cdot a =: a$
$a^n =: a^{n-1} \cdot a, n \in \mathbb{Z}^+$	$n \cdot a =: (n-1) \cdot a + a, n \in \mathbb{Z}^+$
$a^0 =: 1$	$0 \cdot a =: 0$
$a^{-n} =: (a^{-1})^n, n \in \mathbb{Z}^+$	$(-n) \cdot a =: n \cdot (-a), n \in \mathbb{Z}^+.$

Teniendo en cuenta esta definición, es posible demostrar por inducción matemática las siguientes relaciones en cualquier grupo:

Notación multiplicativa	Notación aditiva
$(a^n)^m = a^{nm}$	$m \cdot (n \cdot a) = (mn) \cdot a$
$a^n \cdot a^m = a^{n+m}$	$(n \cdot a) + (m \cdot a) = (n+m) \cdot a$
$(a^n)^{-1} = a^{-n}$	$-(n \cdot a) = (-n) \cdot a$

para cualesquiera $m, n \in \mathbb{Z}$.

Sea $(G, \cdot, 1)$ un grupo y sea a un elemento cualquiera de G. Simbolizamos por $\langle a \rangle$ el conjunto de todos los elementos de G que son potencias enteras de a :

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, \ldots\} = \{a^n \mid n \in \mathbb{Z}\}.$$

Nótese que $\langle a \rangle$ es un subgrupo de G: claramente $\langle a \rangle$ es no vacío ya que $a \in \langle a \rangle$, y además

$$\text{Si } x = a^n \in \langle a \rangle, y = a^m \in \langle a \rangle, \text{ entonces } xy = a^{n+m} \in \langle a \rangle.$$
$$\text{Si } x = a^n \in \langle a \rangle \text{ entonces } x^{-1} = (a^n)^{-1} = (a^{-n}) \in \langle a \rangle.$$

$\langle a \rangle$ se denomina el ***subgrupo cíclico*** de G generado por el elemento a. En notación aditiva tenemos que el subgrupo cíclico generado por a es :

$$\langle a \rangle = \{\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots\} = \{n \cdot a \mid n \in \mathbb{Z}\}.$$

Definición 1.3.9. *Sea G un grupo, se dice que G es **cíclico** si existe un elemento $a \in G$ tal que el subgrupo cíclico generado por a coincide con todo el grupo G, es decir, $G = \langle a \rangle$.*

Ejemplo 1.3.10. ***El grupo*** $\mathbb{Z}$. $(\mathbb{Z}+, 0)$ es un grupo cíclico y todos sus subgrupos son cíclicos. Sea $H \leq \mathbb{Z}$, si $H = \{0\}$ es el subgrupo trivial nulo, entonces claramente $\langle 0 \rangle = \{0\}$ y H es cíclico. Supóngase que $H \neq \{0\}$. Entonces existe $k \neq 0$, k entero, $k \in H$. Si $k \in \mathbb{Z}^-$, entonces $-k \in \mathbb{Z}^+$ y $-k \in H$. Así pues, el conjunto

$$H^+ := \{x \in H \mid x \in \mathbb{Z}^+\} \neq \emptyset.$$

Ya que $(\mathbb{Z}^+, \leq)$ es bien ordenado, existe un entero positivo mínimo n en H. Queremos probar que H coincide con el subgrupo cíclico generado por n, es decir, $H = \langle n \rangle$. En efecto, sea $p \in H$. Existen enteros q, r tales que $p = q \cdot n + r$, $0 \leq r < n$, entonces $r = p + [-(q \cdot n)]$. Si $q \in \mathbb{Z}^+$, entonces $r = p + q \cdot (-n)$. Como $-n$ y $p \in H$, entonces $r \in H$. Por la escogencia de $n, r = 0$ y así $p = q \cdot n \in \langle n \rangle$. Si $q \in \mathbb{Z}^-$, entonces $-q \in \mathbb{Z}^+$ y $r = p + [(-q) \cdot n]$. Como $p, n \in H$, entonces $r \in H$ y nuevamente $r = 0$, con lo cual $p = q \cdot n \in \langle n \rangle$. Si $q = 0$ entonces $p = r \in H$, luego $r = 0$ y entonces $p = 0 \in \langle n \rangle$. En los tres casos hemos probado que $H \leq \langle n \rangle$. Puesto que $n \in H$, la otra inclusión es obvia. Se ha demostrado que cada subgrupo H de $\mathbb{Z}$ es cíclico y generado por el menor entero positivo n contenido en H. Además, $\langle n \rangle = \langle -n \rangle$. Así pues, los subgrupos de $\mathbb{Z}$ son: $\langle n \rangle, n \geq 0$.

Observación 1.3.11. En adelante omitiremos en la teoría general de grupos con notación mutltiplicativa el punto para representar la operación correspondiente, así pues, escribiremos xy en lugar de $x \cdot y$ para denotar el producto de los elementos x, y.

1.4. Generación de subgrupos

Dado un subconjunto X de un grupo G se desea establecer si existe un subgrupo H en G, distinto de G, que contenga a X. En caso de que podamos determinar una colección de tales subgrupos, conviene preguntar cuál es el subgrupo más pequeño de G que contiene X. Antes de responder a estas preguntas aclaremos primero la expresión "subgrupo más pequeño".

Proposición 1.4.1. *Sea G un grupo. En el conjunto de todos los subgrupos de G la relación "ser subgrupo de" determina un orden parcial.*

Demostración. Evidente. □

Como en cualquier conjunto parcialmente ordenado, podemos hablar de subgrupo maximal y subgrupo minimal.

Definición 1.4.2. *Sean $(G, \cdot, 1)$ un grupo y $H \neq G$ un subgrupo de G.*

(i) *Se dice que que H es un **subgrupo maximal** de G, si para cada subgrupo K de G se tiene*

$$H \leq K \Leftrightarrow (K = H \text{ ó } K = G).$$

(ii) *Se dice que $H \neq \{1\}$ es un **subgrupo minimal** de G, si para cada subgrupo K de G se tiene*

$$K \leq H \Leftrightarrow (K = H \text{ ó } K = \{1\}).$$

Ejemplo 1.4.3. Los subgrupos maximales del grupo $(\mathbb{Z}, +, 0)$ son de la forma $\langle p \rangle$, donde p es primo. Además, $(\mathbb{Z}, +, 0)$ no posee subgrupos minimales.

Queremos responder ahora las preguntas planteadas al principio de la sección.

Proposición 1.4.4. *Sean G un grupo, $\{H_i\}_{i \in I}$ una familia de subgrupos de G y X un subconjunto cualquiera de G. Entonces,*

(i) *La intersección $\bigcap_{i \in I} H_i$ es un subgrupo de G.*

(ii) *Existe en G un subgrupo, denotado por $\langle X \rangle$, que contiene a X y es el más pequeño subgrupo de G con dicha propiedad.*

(iii) *$\langle X \rangle$ coincide con la intersección de la familia de todos los subgrupos de G que contienen a X.*

(iv) $\langle \emptyset \rangle = 1$.

Demostración. Evidente. □

La proposición anterior no permite de una manera concreta determinar los elementos del subgrupo $\langle X \rangle$, ya que sería necesario determinar todos los subgrupos de G que contienen X y luego efectuar la intersección. Se tiene en cambio el siguiente resultado.

Proposición 1.4.5. *Sean $(G, \cdot, 1)$ un grupo y $X \neq \emptyset$ un subconjunto de G. Entonces,*

$$\langle X \rangle = \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \mid x_i \in X,\ \varepsilon_i = \pm 1, n \geq 1\}.$$

Demostración. Sea S el conjunto de la derecha de la igualdad anterior. Entonces, S es un subgrupo de G: sean $x = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$, $y = y_1^{\theta_1} \cdots y_m^{\theta_m}$ dos elementos de S, entonces $xy = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} y_1^{\theta_1} \cdots y_m^{\theta_m}$ tiene la forma de los elementos del conjunto S. Es claro que el inverso de un elemento de S tiene la forma de los elementos de S. Además, S contiene al conjunto X: en efecto, para cada elemento x de X se tiene que $x = x^1 \in S$. De lo anterior se obtiene que $\langle X \rangle \leq S$.

De otra parte,

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H$$

entonces, cada H que contiene a X contiene a todos los productos de elementos de X e inversos de elementos de X, así pues, cada H que contiene a X contiene también a S, luego $S \leq \langle X \rangle$. □

Corolario 1.4.6. *Sean $(G, \cdot, 1)$ un grupo abeliano y $\emptyset \neq X \subseteq G$. Entonces,*

$$\langle X\rangle = \left\{x_1^{k_1}\cdots x_n^{k_n} \mid k_i \in \mathbb{Z}, x_i \in X,\ n \geq 1\right\}.$$

En notación aditiva, $\langle X\rangle = \{k_1 \cdot x_1 + \cdots + k_n \cdot x_n \mid k_i \in \mathbb{Z}, x_i \in X,\ n \geq 1\}$.

Demostración. Como G es abeliano, para cada elemento $x = x_1^{\varepsilon_1}\cdots x_n^{\varepsilon_n} \in \langle X\rangle$ podemos agrupar las potencias de elementos iguales. □

Definición 1.4.7. *Sea G un grupo y sea X un subconjunto de G. $\langle X\rangle$ se denomina el* ***subgrupo generado por*** *X y a X se le llama un* ***conjunto de generadores*** *de $\langle X\rangle$. Si X es finito y $\langle X\rangle = G$ se dice que G es un* ***grupo finitamente generado****.*

Ejemplo 1.4.8. Todo grupo cíclico G con generador a es un grupo finitamente generado con conjunto generador $\{a\}$:

$$G = \langle\{a\}\rangle = \langle a\rangle = \left\{a^k \mid k \in \mathbb{Z}\right\}.$$

Nótese por ejemplo que

$$\mathbb{Z} = \langle\{1\}\rangle = \langle 1\rangle = \{k \cdot 1 \mid k \in \mathbb{Z}\}.$$

Ejemplo 1.4.9. Sea $(\mathbb{Q}, +, 0)$ el grupo aditivo de los números racionales, entonces

$$\mathbb{Q} = \left\langle \tfrac{1}{n} \mid n \in \mathbb{N}\right\rangle.$$

En efecto, sea r un racional. Si r es positivo entonces podemos considerar que r es de la forma $r = \frac{p}{q}$, con $p, q \in \mathbb{N}$, luego $r = p \cdot \left(\frac{1}{q}\right)$. Si $r = 0$ entonces $r = \frac{0}{1} = 0 \cdot \left(\frac{1}{1}\right)$. Si r es negativo entonces podemos suponer que r es de la forma $r = \frac{-p}{q}$, con $p, q \in \mathbb{N}$ luego $r = (-p) \cdot \left(\frac{1}{q}\right)$.

Ejemplo 1.4.10. Sea $(\mathbb{Q}^*, \cdot, 1)$ el grupo multiplicativo de los números racionales no nulos, entonces

$$\mathbb{Q}^* = \langle -1, 2, 3, 5, 7, \dots\rangle = \langle x \in \mathbb{Q} \mid x = -1 \ \text{ ó } \ x \ \text{ es primo positivo}\rangle.$$

En efecto, sea r un racional no nulo. Si r es positivo entonces r es de la forma $\frac{p}{q}$ con $p, q \in \mathbb{N}$. p y q se pueden descomponer en factores primos,

$$p = p_1^{\alpha_1}\cdots p_r^{\alpha_r}\ ,\ q = q_1^{\beta_1}\cdots q_s^{\beta s}, \text{ con } \alpha_1, \dots, \alpha_r,\ \beta_1, \dots, \beta_s \in \mathbb{N} \cup \{0\},$$
$$\frac{p}{q} = pq^{-1} = (p_1^{\alpha_1}\cdots p_r^{\alpha_r})\ \left(q_1^{-\beta_1}\cdots q_s^{-\beta s}\right).$$

Si r es negativo podemos suponer que r es de la forma $-\frac{p}{q}$ con $p, q \in \mathbb{N}$, entonces

$$r = -\tfrac{p}{q} = (-1)\tfrac{p}{q} = (-1)pq^{-1} = (-1)p_1^{\alpha_1}\cdots p_r^{\alpha_r}\ q_1^{-\beta_1}\cdots q_s^{-\beta_s}.$$

Proposición 1.4.11. *Sea G un grupo y H un subconjunto no vacío de G. Entonces*

(i) $H \leq G \Leftrightarrow \langle H\rangle = H$.

(ii) $X \subseteq Y \subseteq G \Rightarrow \langle X\rangle \leq \langle Y\rangle$.

(iii) $\langle X\rangle \cup \langle Y\rangle \subseteq \langle X \cup Y\rangle$.

Demostración. (i) es evidente.

(ii) $\langle Y\rangle$ es un subgrupo de G que contiene a $Y \supseteq X$, por tanto, $\langle X\rangle \leq \langle Y\rangle$.

(iii) $\langle X \cup Y\rangle \supseteq X \cup Y \supseteq X$, luego $\langle X \cup Y\rangle \geq \langle X\rangle$. Análogamente, $\langle X \cup Y\rangle \geq \langle Y\rangle$, de donde $\langle X\rangle \cup \langle Y\rangle \subseteq \langle X \cup Y\rangle$ (en general, la unión de subgrupos no es un subgrupo). □

Proposición 1.4.12. *Sea G un grupo finitamente generado y sea H un subgrupo propio de G. Entonces, existe un subgrupo maximal de G que contiene a H.*

Demostración. Sea $\{x_1, \ldots, x_n\}$ un sistema finito de generadores de G. Sea $\Phi := \{K \mid H \leq K \lneq G\}$. Notemos que $\Phi \neq \emptyset$ ya que $H \in \Phi$. $(\Phi, \leq)$ es un conjunto parcialmente ordenado. Sea Φ_0 una cadena de Φ. Sea $H' := \bigcup K$, la unión de los subgrupos K de esta cadena. Nótese que $H \leq H' \leq G$. En efecto, Sean $x, y \in H'$, entonces existen K_x,$K_y \in \Phi_0$ tales que $x \in K_x$, $y \in K_y$. Como Φ_0 es totalmente ordenado, entonces podemos suponer que $K_x \leq K_y$ y entonces $x, y \in K_y$, luego $xy \in K_y$, con lo cual $xy \in H'$. Además, $x^{-1} \in K_x \subseteq H'$. Ahora, como $H \leq K$ para cada $K \in \Phi_0$, entonces $H \leq H'$.

Observemos que $H' \neq G$. En efecto, si $H' = G = \langle x_1, \ldots, x_n\rangle$, entonces $x_1 \in K_{x_1}, \ldots, x_n \in K_{x_n}$, con $K_{x_i} \in \Phi_0$. Existe entonces K_{x_j} tal que $x_1, \ldots, x_n \in K_{x_j}$, luego $G \leq K_{x_j}$, es decir, $K_{x_j} = G$, lo cual es contradictorio. Así pues, $H' \neq G$. H' es cota superior para Φ_0 en Φ. De acuerdo con el Lema de Zorn, Φ tiene elemento maximal H_0 el cual es obviamente subgrupo maximal de G. □

1.5. Teorema de Lagrange

Sea G un grupo con un número finito de elementos y sea H un subgrupo de G. Resulta interesante preguntar qué relación guardan la cantidad de elementos de H y la cantidad de elementos de G. En esta sección mostraremos que el número de elementos de H divide al número de elementos del grupo dado G.

Proposición 1.5.1. *Sea G un grupo y sea H un subgrupo de G. La relación en G definida por*

$$a \equiv b \Leftrightarrow ab^{-1} \in H, \quad a, b \in G \tag{1.5.1}$$

es de equivalencia.

Demostración. Si dos elementos a y b de G están relacionados mediante (1.5.1) se dice que a ***es congruente con*** b ***módulo*** H.

Reflexiva: sea $a \in G$ entonces $a \equiv a$ ya que $aa^{-1} = 1 \in H$.

Simétrica: sean $a, b \in G$ tales que $a \equiv b$. Entonces, $ab^{-1} \in H$, pero como $H \leq G$ tenemos que $(ab^{-1})^{-1} = ba^{-1} \in H$, o sea que $b \equiv a$.

Transitiva: sean a, b, c elementos de G tales que $a \equiv b$ y $b \equiv c$. Entonces $ab^{-1} \in H$ y $bc^{-1} \in H$. De ahí que resulta que $(ab^{-1})(bc^{-1}) \in H$, es decir, $ac^{-1} \in H$, y por tanto, $a \equiv c$. Esto completa la demostración de la proposición. □

Observación 1.5.2. Si el grupo G tiene notación aditiva entonces la relacion $\equiv$ se define como $a \equiv b \Leftrightarrow a - b \in H$.

Es conocido que cualquier relación de equivalencia $\equiv$ definida sobre un conjunto G determina una partición de dicho conjunto en clases de equivalencia disyuntas entre si, y la reunión de las cuales da G. Así pues, para el caso que estamos tratando, sea a un elemento cualquiera del grupo G, la clase de eqivalencia a la cual pertenece el elemento a será denotada por $[a]$ y está constituída por todos los elementos x de G con los cuales a está relacionado mediante la relación $\equiv$, es decir,

$$[a] = \{x \in G \mid a \equiv x\} = \{x \in G \mid ax^{-1} \in H\}.$$

Como dijimos arriba, la reunión de las clases determinadas por la relación $\equiv$ es todo el grupo G: $\bigcup_{a \in G}[a] = G$.

Proposición 1.5.3. *Sean G un grupo, $H \leq G$ y $\equiv$ la relación de equivalencia definida en (1.5.1). Sea a un elemento cualquiera de G. Entonces, $[a] = Ha := \{xa \mid x \in H\}$. En particular, $[1] = H$.*

Demostración. Sea $z \in [a]$, entonces $a \equiv z$. Por ser $\equiv$ una relacion simétrica tenemos que $z \equiv a$, y por eso, $za^{-1} = x$, con $x \in H$, luego $z = xa \in Ha$. Hemos probado que $[a] \subseteq Ha$. Sea $z = xa$ un elemento de Ha, con $x \in H$, entonces $za^{-1} = x \in H$, o sea $z \equiv a$, de donde $a \equiv z$, es decir, $z \in [a]$. □

Definición 1.5.4. *Sean G un grupo, $H \leq G$ y $a \in G$. El conjunto Ha se llama la* ***clase lateral derecha*** *del elemento a módulo H .*

La proposición anterior muestra que la clase del elemento identidad 1 del grupo G coincide con el subgrupo H. Luego $[1]$ y H tienen la misma cantidad de elementos. A continuación probaremos que todas las clases tienen la cardinalidad de H, y por ende, todas las clases de equivalencia tienen la misma cantidad de elementos.

Proposición 1.5.5. *Sean G un grupo, H un subgrupo de G y $\equiv$ la relación de equivalencia definida en (1.5.1). Entonces, todas las clases de equivalencia determinadas por $\equiv$ tienen el mismo cardinal que el subgrupo H.*

Demostración. Sea a un elemento cualquiera de G. Entonces $[a] = Ha$ y la función $f : Ha \to H$, $f(xa) = x$, $x \in H$, es biyectiva. En efecto, claramente f es sobreyectiva. Supóngase que $f(xa) = f(ya)$, entonces $x = y$ y así $xa = xy$, con lo cual f es inyectiva. □

Estamos ya en condiciones de demostrar el teorema de Lagrange para grupos finitos. Si G es un grupo, $|G|$ denota el ***cardinal*** de G.

Teorema 1.5.6 (Teorema de Lagrange). *Sea G un grupo finito y sea H un subgrupo cualquiera de G. Entonces, $|H| \mid |G|$.*

Demostración. Puesto que G es finito entonces H determina un número finito de clases de equivalencia en G . Sea k el número de clases de equivalencia definidas; como estas clases son disyuntas, y además todas tienen $|H|$ elementos, entonces $|H| + \cdots + |H| = |G|$, es decir, $k|H| = |G|$, así $|H| \mid |G|$. □

Definición 1.5.7. *Sean G un grupo y H un subgrupo de G. El cardinal del conjunto de clases de equivalencia determinado por H mediante la relación definida en (1.5.1) se llama el **índice** del subgrupo H en el grupo G, y se simboliza por $|G : H|$.*

Cuando G es finito se tiene que

$$|G : H| = \frac{|G|}{|H|}. \tag{1.5.2}$$

Ejemplo 1.5.8. (i) Sea $G = S_3$ y sea $H = \{1, f\}$, donde

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

Calculemos $\mid G : H \mid$ y además determinemos el conjunto de clases laterales de H. Por el Teorema de Lagrange, $\mid G : H \mid = \frac{|G|}{|H|} = \frac{6}{2} = 3$, $H1 = H = \{1, f\}$, $Hh = \{h, fh\} = \{h, k\}$, $Hf = \{f, f^2\} = \{1, f\}$, $Hk = \{k, fk\} = \{k, h\}$, $Hg = \{g, fg\} = \{g, m\}$, $Hm = \{m, fm\} = \{m, g\}$. Nótese que $H1 = Hf = H$, $Hg = Hm$ y $Hh = Hk$, es decir, se tienen 3 clases de equivalencia tal como lo había pronosticado el Teorema de Lagrange. Obsérvese que una clase de equivalencia, o en otras palabras, una clase lateral derecha no es general un subgrupo del grupo dado.

(ii) $\mid \mathbb{Z} : \langle n \rangle \mid = n$, para $n \geq 1$ y $\mid \mathbb{Z} : \langle 0 \rangle \mid = \aleph_0$.

1.6. Ejercicios

1. Demuestre por inducción las proposiciones 1.1.8 y 1.1.13.

2. Sea G un conjunto dotado de una operación binaria interna $*$, se dice que un elemento $e \in$ G es:

   (i) ***Identidad a la izquierda*** de $*$ si $e * a = a$, cualquiera que sea $a \in G$.

   (ii) ***Identidad a la derecha*** de $*$ si $a * e = a$, cualquiera que sea $a \in G$.

   Sean e_1 y e_2 elementos de G tales que e_1 es identidad a la izquierda de $*$ y e_2 es identidad a la derecha de $*$, pruebe que $e_1 = e_2$.

3. Compruebe que en

   (i) $(\mathbb{N}, *)$, donde $a * b := a$, todo elemento de $\mathbb{N}$ es identidad a la derecha, pero no existe identidad a la izquierda.

   (ii) $(\mathbb{N}, *)$, donde $x * y :=$ máximo común divisor de x e y, no hay elementos identidad.

   (iii) $(\mathbb{N}, *)$, donde $a * b :=$ mínimo común múltiplo de a y b, 1 es el elemento identidad.

   (iv) $(\mathbb{Z}, *)$ donde $a * b := a - b$, 0 es identidad a la derecha pero no posee identidad a la izquierda.

4. Sea G un conjunto dotado de una operación binaria interna $*$ asociativa, la cual posee elemento identidad e. Sea $a \in G$, se dice que

   (i) a posee un ***inverso a la izquierda*** (respecto de e) si existe $b \in G$ tal que $b * a = e$.

   (ii) a posee un ***inverso a la derecha*** (respecto de e) si existe $c \in G$ tal que $a * c = e$.

   Demuestre que si a posee un inverso a la izquierda b y un inverso a la derecha c, entonces $b = c$.

5. Demuestre la proposición 1.2.6.

6. Sean $(A, *)$ y (B, Δ) conjuntos con operaciones binarias internas. Una función $f : A \to B$ se denomina un ***homomorfismo*** si f respeta las operaciones de los conjuntos A y B, es decir,

$$f(a_1 * a_2) = f(a_1)\Delta f(a_2)$$

   para cualesquiera elementos a_1, a_2 de A. Además, si A y B poseen elementos identidad e y k respectivamente, entonces f debe cumplir la propiedad adicional $f(e) = k$. Sea f un homomorfismo de A en B. Pruebe por inducción que $f(a^n) = f(a)^n$ para todo $a \in A$ y todo $n \in N$. Pruebe además que si a es invertible en A, entones $f(a)$ es invertible en B, y $f(a^{-1}) = f(a)^{-1}$.

7. Sea $f : (A, *, e) \to (B, \Delta, k)$ un homomorfismo de A en B, donde e y k son los respectivos elementos identidad. Se definen los siguientes objetos:

   (i) El conjunto de imágenes de la función f se llama ***imagen*** del homomorfismo f y se simboliza por $Im(f)$, así pues, $Im(f) := \{f(x) \,|\, x \in A\}$.

   (ii) El conjunto de elementos de A cuya imagen es el elemento identidad k se llama el ***núcleo*** del homomorfismo f y se denota por $\ker(f)$ (de la palabra alemana *kernel*). Así pues, $\ker(f) := \{x \in A | f(x) = k\}$.

   (iii) Se dice que f es un ***sobreyectivo*** si la función f es sobreyectiva, es decir, $Im(f) = B$.

   (iv) Se dice que el homomorfismo f es ***inyectivo*** si la función f es inyectiva, es decir, para cualesquiera elementos x, y en A, la igualdad $f(x) = f(y)$ implica $x = y$.

   (v) Se dice que f es un ***isomorfismo*** si f es sobreyectivo e inyectivo.

   (vi) Si los conjuntos A y B coinciden y las operaciones $*$, y, Δ también, entonces un isomorfismo f en este caso se denomina ***automorfismo*** de A.

   Sea X un conjunto y sea $P(X)$ su conjunto de partes. Sea $f : (P(X), \cup) \to (P(X), \cap)$ la función que a cada subconjunto V de X le asigna su complemento: $f(V) = X - V$. Determine las identidades en $(P(X), \cup)$ y $(P(X), \cap)$ y demuestre que f es un isomorfismo ($\cup$ representa la unión de conujuntos y $\cap$ la intersección).

8. Sea A un conjunto dotado de una operación binaria interna $*$. Supóngase que en A ha sido definida una relación de equivalencia $\equiv$. Se dice que la relación $\equiv$ es ***compatible*** con la operación $*$ si para cualesquiera $a_1, b_1, a_2, b_2 \in A$, $a_1 \equiv b_1$ y $a_2 \equiv b_2$, implica $a_1 * a_2 \equiv b_1 * b_2$. Denotemos para $\overline{A}$ el conjunto $A/\equiv$ de clases de equivalencia $[a], a \in A$. Se desea definir en $\overline{A}$ una operación binaria inducida por $*$ y $\equiv$: sean [a] y [b] elementos de A entonces definimos

$$[a]\overline{*}[b] = [a * \ b]. \tag{1.6.1}$$

   (i) Demuestre que (1.6.1) está bien definida, es decir, demuestre que para otros representantes a_1 y b_1 de las clases $[a]$ y $[b]$, respectivamente, se cumple que $[a_1]\overline{*}[b_1] = [a]\overline{*}[b]$.

   (ii) La función $j : (A, *) \to (\overline{A}, \overline{*})$ que asigna a cada elemento a de A su clase $[a]$ es un homomorfismo sobreyectivo.

9. Sea $f : j : (A, *) \to (B, \Delta)$ un homomorfismo sobreyectivo. Definimos en A la relación $\equiv$ como sigue:

$$a_1 \equiv a_2 \Leftrightarrow f(a_1) = f(a_2), \text{ para cualesquiera } a_1, a_2 \text{ en } A.$$

(i) Demuestre que $\equiv$ es una relación de equivalencia.

(ii) Demuestre que $\equiv$ es compatible con $*$, es decir, si $a_1 \equiv a_2$ y $b_1 \equiv b_2$, entonces $a_1 * b_1 \equiv a_2 * b_2$.

(iii) Sean $\overline{A}, \overline{*}$ definidos como en el ejercicio anterior. Entonces, demuestre que $\overline{f} : (\overline{A}, \overline{*}) \to (B, \Delta)$ definido por $\overline{f}([a]) := f(a)$ es un isomorfismo (como toda función definida sobre un conjunto cociente, es importante probar como primer paso que $\overline{f}$ está bien definida, es decir que si $a_1 \equiv a_2$, entonces $\overline{f}([a_1]) = \overline{f}([a_2])$).

10. Sea $(G, \cdot)$ un semigrupo finito en el cual se cumplen las leyes cancelativas, es decir, para cualesquiera elementos $a, b, c \in G$ se tiene que

$$ac = bc \Leftrightarrow a = b,$$
$$ca = cb \Leftrightarrow a = b.$$

Demuestre que $(G, \cdot)$ es un grupo.

11. Demuestre que si $(G, \cdot)$ es un semigrupo en el cual las ecuaciones $ax = b,\ xa = b$ son solubles para cualesquiera elementos $a, b \in G$, entonces $(G, \cdot)$ es un grupo.

12. Demuestre que el conjunto $G := \{(a, b) \mid a, b \in \mathbb{R}, a \neq 0\}$ con la operación

$$(a, b)\,(c, d) := (ac, ad + b)$$

es un grupo. ¿G es conmutativo?

13. Sea G un grupo tal que $(ab)^2 = a^2b^2$ para cualesquiera elementos $a, b \in G$. Pruebe que G es conmutativo.

14. Pruebe que todo grupo finito de tamaño $n \leq 5$ es conmutativo.

15. Sea $\mathbb{R} \setminus \{0\}$ el conjunto de reales no nulos con la operación $\circ$ definida por

$$a \circ b := |a|\, b.$$

Pruebe que $\circ$ es asociativa, que existe elemento identidad al lado izquierdo y que cada elemento tiene inverso al lado derecho respecto de la identidad de la izquierda. ¿Es G un grupo ?

16. Cada una de las siguientes tablas definen operaciones binarias internas de las cuales se saben que son asociativas. Compruebe que ellas definen grupos:

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$V = \{e, a, b, c\}$

$.$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

¿Es $\mathbb{Z}_4$ un grupo conmutativo? ¿Es V un grupo conmutativo? Es $\{0, 2\}$ un subgrupo de $\mathbb{Z}_4$? ¿Es $\{e, c\} \leq V$? ¿Es $\{0, 3\}$ un subgrupo de $\mathbb{Z}_4$? ¿Es $\{e, a, b\} \leq V$?

17. Sea H un subconjunto finito no vacío de un grupo $(G, \cdot, 1)$ y sea H cerrado respecto a la operación, es decir, $a, b \in H$ implica $ab \in H$. Demuestre que H es un subgrupo de G.

18. Sea G un grupo y a un elemento de G. Se define $N_G(a) := \{x \in G \mid xa = ax\}$. $N_G(a)$ se llama el ***normalizador*** de a en G. Demuestre que $N_G(a) \leq G$.

19. Sea $(G, \cdot, 1)$ un grupo abeliano. Pruebe que el conjunto $H := \{x \in G \mid x^2 = 1\}$ es un subgrupo de G.

20. Sea $M_n(\mathbb{R})$ el grupo de matrices reales de tamaño $n \times n$, $n \geq 1$, con respecto a la adición, y sea D el conjunto de matrices de $M_n(\mathbb{R})$ que son diagonales, es decir,

$$D := \left\{ \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{bmatrix} \mid d_1, \ldots, d_n \in \mathbb{R} \right\}.$$

Demuestre que $D \leq M_n(\mathbb{R})$.

21. Sea $GL_n(\mathbb{R})$ el ***grupo lineal general de orden*** n sobre los números reales, es decir, $GL_n(\mathbb{R}) := M_n(\mathbb{R})^*$ es el grupo de elementos invertibles del semigrupo multiplicativo $(M_n(\mathbb{R}), \cdot)$. Entonces,

(i) Sea $SL_n(\mathbb{R})$ el subconjunto de $GL_n(\mathbb{R})$ constituido por las matrices de determinante 1, es decir,

$$SL_n(\mathbb{R}) := \{F \in GL_n(\mathbb{R}) \mid \det(F) = 1\}.$$

Demuestre que $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$. $SL_n(\mathbb{R})$ se denomina el ***grupo especial de orden*** n sobre $\mathbb{R}$.

(ii) Sea

$$D_n(\mathbb{R}) := \left\{ \operatorname{diag}(d_1, \ldots, d_n) := \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{bmatrix} \in M_n(\mathbb{R}) \mid d_1 \cdots d_n \neq 0 \right\}.$$

Demuestre que $D_n(\mathbb{R}) \leq GL_n(\mathbb{R})$. $D_n(\mathbb{R})$ se conoce como el ***grupo de matrices diagonales de orden*** n sobre $\mathbb{R}$.

(iii) Sea

$$T_n(\mathbb{R}) := \left\{ \begin{bmatrix} f_{11} & \cdots & f_{1n} \\ & \ddots & \vdots \\ 0 & & f_{nn} \end{bmatrix} \in M_n(\mathbb{R}) \mid f_{11} \cdots f_{nn} \neq 0, f_{ij} = 0 \,\text{si}\, i > j \right\}.$$

Demuestre que $T_n(\mathbb{R}) \leq GL_n(\mathbb{R})$. $T_n(\mathbb{R})$ se denomina el grupo de ***matrices triangulares superiores de orden*** n sobre $\mathbb{R}$.

(iv) Sea

$$UT_n(\mathbb{R}) := \{F \in T_n(\mathbb{R}) \mid f_{ii} = 1, 1 \leq i \leq n\}.$$

Demuestre que $UT_n(\mathbb{R}) \leq T_n(\mathbb{R}) \cap SL_n(\mathbb{R})$. $UT_n(\mathbb{R})$ se denomina el ***grupo de matrices unitriangulares superiores de orden*** n sobre $\mathbb{R}$.

(iv) Para $1 \leq m \leq n$ sea $UT_n^m(\mathbb{R})$ el conjunto de matrices unitriangulares $F = [f_{ij}] \in UT_n(\mathbb{R})$ tales que $f_{ij} = 0$ para $i < j < i + m$, es decir, las primeras $m - 1$ diagonales consecutivas por encima de la diagonal principal de F son nulas. Demuestre que $UT_n^m(\mathbb{R}) \leq UT_n(\mathbb{R})$, y además

$$UT_n(\mathbb{R}) = UT_n^1(\mathbb{R}) \supseteq UT_n^2(\mathbb{R}) \supseteq \cdots \supseteq UT_n^n(\mathbb{R}) = \{E\}.$$

22. En el grupo $GL_n(\mathbb{R})$ se tienen tres tipos de ***matrices elementales***:

(i) ***Matrices propiamente elementales o transvecciones***: $T_{ij}(a) := E + aE_{ij}$, $i \neq j$, $a \in \mathbb{R}$, donde E es la ***matriz idéntica*** y $E_{ij} \in M_n(\mathbb{R})$ es la ***matriz canónica*** que tiene todas sus entradas nulas, salvo la entrada (i, j) que es 1. Nótese que $T_{ij}(a) \in SL_n(\mathbb{R})$.

(ii) ***Matrices diagonales***: $D_i(d) := \operatorname{diag}(1, \ldots, d, \ldots, 1) \in D_n(\mathbb{R})$, $0 \neq d \in \mathbb{R}$, $1 \leq i \leq n$.

(iii) ***Permutaciones***: $P_{ij} = E - E_{ii} - E_{jj} + E_{ij} + E_{ji}$.

Demuestre que:

(i) $GL_n(\mathbb{R})$ se puede generar por matrices elementales. Mejor aún, demuestre que

$$GL_n(\mathbb{R}) = \langle T_{ij}(a), D_n(d) | 1 \leq i, j \leq n, i \neq j, a \in \mathbb{R}, 0 \neq d \in \mathbb{R} \rangle.$$

(ii) $SL_n(\mathbb{R}) = \langle T_{ij}(a) | 1 \leq i, j \leq n, i \neq j, a \in \mathbb{R} \rangle$.

(iii) $D_n(\mathbb{R}) = \langle D_i(d_i) | 0 \neq d_i \in \mathbb{R}, 1 \leq i \leq n \rangle$.

(iv) $T_n(\mathbb{R}) = \langle T_{ij}(a), D_i(d_i) | j > i, a \in \mathbb{R}, 0 \neq d_i, 1 \leq i, j \leq n \rangle$.

(iv) $UT_n(\mathbb{R}) = \langle T_{ij}(a) | j > i, a \in \mathbb{R}, 1 \leq i, j \leq n \rangle$.

(v) $UT_n^m(\mathbb{R}) = \langle T_{ij}(a) | j - i \geq m, a \in \mathbb{R}, 1 \leq i, j \leq n \rangle$.

Capítulo 2

Grupos cíclicos

Una rama destacada dentro de la teoría de grupos la constituyen los llamados grupos abelianos. Quizá los grupos abelianos más importantes son los llamados grupos cíclicos, ya que los grupos abelianos finitamente generados son expresables a través de sumas directas de grupos cíclicos. En este capítulo vamos a mostrar las propiedades básicas de los grupos cíclicos finitos. Se establecerá la relación que guardan los conceptos de periodo de un elemento y orden. Para grupos cíclicos finitos son demostradas algunas proposiciones relacionadas con el orden de sus subgrupos y el número de generadores de dichos grupos. Al final del capítulo hemos incluido una serie de ejercicios donde se estudian algunas aplicaciones de los grupos cíclicos a teoría elemental de números.

2.1. Definición

Sea G un grupo cualquiera y sea a un elemento arbitrario de G. El conjunto de todas las potencias enteras a^n, $n \in \mathbb{Z}$, del elemento a constituye un subgrupo de G llamado el subgrupo cíclico de G generado por el elemento a. Como vimos en el capítulo anterior, cuando el grupo G sea aditivo, na, $n \in \mathbb{Z}$, representa los múltiplos enteros del elemento a.

Definición 2.1.1. *Sea G un grupo y sea a un elemento cualquiera de G. El conjunto*

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{\dots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, \dots\}$$

es un subgrupo del grupo G, llamado el ***subgrupo cíclico*** *de G generado por el elemento a. Si G es un grupo con notación aditiva escribiremos*

$$\langle a \rangle = \{na \mid n \in \mathbb{Z}\} = \{\dots, -3a, -2a, , -a, 0, a, 2a, 3a, \dots\}.$$

Es posible que el subgrupo generado por algún elemento a del grupo G coincida con todo el grupo: $\langle a \rangle = G$; esta situación se presenta por ejemplo con el entero 1

en el grupo aditivo de los números enteros. Los grupos para los cuales se tiene este tipo de situación reciben un nombre especial.

Definición 2.1.2. *Sea G un grupo cualquiera. Se dice que G es* ***cíclico*** *si G coincide con uno de sus subgrupos cíclicos; es decir, si existe un elemento a en G tal que $\langle a\rangle = G$. En este caso se dice que a es un* ***generador*** *del grupo cíclico G.*

Ejemplo 2.1.3. (i) $\mathbb{Z}$ es un grupo cíclico y todos sus subgrupos son cíclicos.

(ii) El grupo de raíces complejas de grado n de la unidad, $n \geq 1$, es cíclico: denotemos por U_n las soluciones complejas de la ecuación $x^n = 1$, es decir,

$$U_n := \{z \in \mathbb{C} \mid z^n = 1\};$$

afirmamos que U_n es un subgrupo de $\langle \mathbb{C}*, \cdot, 1\rangle$: en efecto, $U_n \neq \emptyset$ ya que $1^n = 1$ y por lo tanto $1 \in U_n$. Sean z_1 y z_2 elementos de U_n, entonces $(z_1 z_2)^n = {z_1}^n {z_2}^n$ por ser $\langle \mathbb{C}^*, \cdot, 1\rangle$ un grupo abeliano, luego $(z_1 z_2)^n = 1$ y así $z_1 z_2 \in U_n$. Sea ahora $z \in U_n$, entonces $(z^{-1})^n = z^{-n} = (z^n)^{-1} = 1^{-1} = 1$, es decir, $z^{-1} \in U_n$ y nuestra afirmación está probada.

Sea z un elemento de U_n. Al escribir z en la forma polar $z = r\,(\cos\theta + i \sin\ \theta)$, donde $r = |\ z|$ es la norma de z, y teniendo en cuenta que la norma de un producto de complejos es el producto de las normas, concluimos que $|\ z^n| = |\ z|^n = r^n = |1| = 1$. Puesto que la norma es un real no negativo entonces $r = 1$ y z tiene la forma polar $z = \cos\theta + i \sin\theta$. Podemos utilizar el teorema de D'Moivre para determinar la cantidad de elementos de U_n y para demostrar que este subgrupo es cíclico: $z^n = \cos n\theta + i \sin n\theta = 1 = 1 + i0$, entonces $\cos n\theta = 1$ y $\sin n\theta = 0$, así $n\theta = 2k\pi$, $k = 0, 1, 2, \ldots$. Despejando θ obtenemos que $\theta = \frac{2k\pi}{n}$, $k = 0, 1, 2, \ldots$. Sin embargo, por la periodicidad de las funciones cos y sin es suficiente considerar los valores de k hasta $n - 1$: $\theta = \frac{2k\pi}{n}$, $k = 0, 1, 2, \ldots, n - 1$. De tal manera que si $z \in U_n$ entonces z es de la forma $z = \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}$, con $k = 0, 1, \ldots, n - 1$. Utilizando la forma exponencial de z podemos demostrar que los complejos $\cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}$, con $k = 0, 1, \ldots, n - 1$ son diferentes: si $\cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n} = \cos\frac{2k'\pi}{n} + i \sin\frac{2k'\pi}{n}$ entonces $e^{i\frac{2k\pi}{n}} = e^{i\frac{2k'\pi}{n}}$ así, $i\frac{2k\pi}{n} = i\frac{2k'\pi}{n}$ y por tanto $k = k'$.

De tal manera que $U_n = \left\{e^{i\frac{2k\pi}{n}} = \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n} \mid k = 0, 1, \ldots, n - 1\right\}$ consta de n elementos exactamente (nótese que $\mathbb{C}^*$ es un grupo infinito que posee grupos finitos no triviales: U_n , $n > 1$). Utilizando nuevamente el teorema de D'Moivre comprobemos que U_n es cíclico y generado por $z_1 = e^{i\frac{2\pi}{n}} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$. Sea $z = e^{i\frac{2k\pi}{n}}$ un elemento cualquiera de U_n, entonces z es la k-ésima potencia de z_1 : $(z_1)^k = \left(e^{i\frac{2\pi}{n}}\right)^k = e^{i\frac{2k\pi}{n}} = z$. Así que, $U_n \leq \langle\ z_1\rangle \subseteq U_n$ entonces $U_n = \langle z_1\rangle$, $|U_n| = n$.

2.2. Orden y periodo de un elemento

Consideremos nuevamente un grupo cualquiera G y $\langle a\rangle$ el subgrupo cíclico generado por el elemento a de G. Vale la pena preguntar sobre la cantidad de elementos del subgrupo $\langle a\rangle$. Descartemos en primer lugar el caso trivial $a = 1$; en este caso $\langle 1\rangle = \{1\}$ y es un subgrupo de un sólo elemento. Sea pues $a \neq 1$ (en notación aditiva $a \neq 0$)

Caso infinito. Si para cada par de enteros diferentes m y n, $m \neq n$, $a^m \neq a^n$ entonces lógicamente $\langle a\rangle$ contiene una cantidad infinita de elementos y por tanto el subgrupo cíclico $\langle a\rangle$ es infinito. La condición que $a^m \neq a^n$ para cada par de enteros diferentes $m \neq n$ es equivalente a la condición $a^n \neq 1$ para todo entero $n > 0$. En efecto, si existe $n > 0$ tal que $a^n = 1$ entonces $a^{n+1} = a = a^1$. Recíprocamente, supóngase que hay enteros $m \neq n$ tales que $a^m = a^n$. Supóngase por ejemplo que $m > n$, entonces $a^m.a^{-n} = a^n.a^{-n}$ entonces $a^{m-n} = 1$, donde $m - n > 0$.

Definición 2.2.1. *Sea $\langle G, \cdot, 1\rangle$ un grupo y sea $a \neq 1$ un elemento cualquiera de G. Se dice que a es de **periodo infinito** si para cada entero positivo $n > 0$, $a^n \neq 1$.*

En notación aditiva tendremos que $0 \neq a \in \langle G, +, 0\rangle$ es de periodo infinito si $na \neq 0$ para todo $n > 0$.

Caso finito. Sea G nuevamente un grupo y $\langle a\rangle$ el subgrupo cíclico generado por a. Supóngase que existen enteros $m \neq n$ tales que $a^m = a^n$. Sea $m > n$, entonces $a^{m-n} = 1$ con $m - n > 0$. Considérese entonces el conjunto $A := \{k \in \mathbb{Z}^+ \mid a^k = 1\}$, entonces por ser $\langle \mathbb{Z}^+, \leq \rangle$ un conjunto bien ordenado A tiene primer elemento n, es decir, n es el menor entero positivo tal que $a^n = 1$.

Definición 2.2.2. *Sea $\langle G, \cdot, 1\rangle$ un grupo y sea a un elemento cualquiera de G. Se dice que a es de **periodo finito** si existe $k > 0$ tal que $a^k = 1$. El menor entero positivo $n > 0$ tal que $a^n = 1$ se llama el **periodo** del elemento a. En notación aditiva tendremos que $a \in \langle G, +, 0\rangle$ es de periodo finito n si n es el menor entero positivo tal que $n.a = 0$.*

Podemos ahora responder a nuestra pregunta sobre el número de elementos del subgrupo cíclico generado por a.

Proposición 2.2.3. *Sea G un grupo y sea a un elemento cualquiera de G. Entonces*

(i) *El subgrupo cíclico $\langle a\rangle$ generado por a es infinito si, y sólo si, a es un elemento de periodo infinito.*

(ii) *El subgrupo cíclico $\langle a\rangle$ generado por a es finito si, y sólo si, a es un elemento de periodo finito. Además, si n es el periodo del elemento a entonces el orden $|\langle a\rangle|$ del subgrupo generado por el elemento a es exactamente n, se denomina el **orden** del elemento a y se simboliza por $|a|$. Si a es de periodo infinito diremos que a es un elemento de orden infinito y escribiremos $|a| = \infty$*

Demostración. (i) $\Rightarrow$) : supóngase que a no es un elemento de periodo infinito. Entonces existe un entero $k > 0$ tal que $a^k = 1$. Esto quiere decir que a es de periodo finito. Sea n el periodo del elemento a. Afirmamos que entonces $\langle a \rangle$ contiene exactamente n elementos diferentes: $\langle a \rangle = \{1, a, a^2, a^3, \ldots, a^{n-1}\}$. Probemos inicialmente que los elementos 1, a, a^2, $a^3, \ldots,$ a^{n-1} son diferentes. Si $a^i = a^j$ con $i \neq j$ e $1 \leq i, j \leq n-1$, entonces, suponiendo por ejemplo $i > j$ tendremos que $a^{i-j} = 1$ con $0 < i - j < n$, pero esto contradice el hecho de ser n el periodo de a. Sea ahora $k \in \mathbb{Z}$ y a^k un elemento cualquiera de $\langle a \rangle$. Por el algoritmo de la división tenemos que $k = ng + r$ con $0 \leq r < n$. Entonces $a^k = a^{ng}\, a^r = (a^n)^g\, a^r = 1.a^r = a^r$, así pues a^k coincide con una de las potencias $a^0 = 1, a, \ldots, a^{n-1}$. Esto prueba entonces que $\langle a \rangle$ es finito. Nótese que cuando a es de periodo finito n entonces $n =$ periodo de a $= |\langle a \rangle| =$ orden del subgrupo cíclico generado por $a = |a| =$ orden del elemento a.

$\Leftarrow$): si a es de periodo infinito entonces $a \neq 1$ para todo $n > 0$. Como vimos antes, esto implica que $a^m \neq a^n$ para cada par de enteros diferentes m y n. Entonces lógicamente $\langle a \rangle$ es infinito.

(ii) $\Rightarrow$): supóngase que a no es de periodo finito. Entonces a es de periodo infinito y, como acabamos de ver en (i), $\langle a \rangle$ es un subgrupo infinito.

$\Leftarrow$): si a es de periodo finito n entonces como se demostró anteriormente $\langle a \rangle$ contiene n elementos. □

Corolario 2.2.4. (i) *Sea G un grupo grupo finito. Entonces $|a| \mid |G|$.*

(ii) *Sea a un elemento de periodo finito n del grupo G (G no necesariamente finito). Supóngase que $a^k = 1$, con $k \in \mathbb{Z}$. Entonces, $n \mid k$. Recíprocamente, si k es un entero tal que $n \mid k$, entonces $a^k = 1$.*

(iii) *Sea G un grupo finito. Entonces, $a^{|G|} = 1$.*

Demostración. (i) Si G es un grupo finito entonces $\langle a \rangle$ es también finito. Como $|\langle a \rangle| = |a|$ entonces por el teorema de Lagrange $|a| \mid |G|$.

(ii) Por el algoritmo de la división, $k = ng + r$, con $0 \leq r < n$. Entonces $a^k = 1 = (a^n)^g\ a^r = a^r$. Por ser n el periodo de a entonces $r = 0$, y así, $n \mid k$. Recíprocamente, si $k = ns$, entonces $a^k = (a^n)^s = 1$.

(iii) Se desprende de (i) y (ii). □

Definición 2.2.5. *Se dice que G es un **grupo sin torsión** si cada elemento $a \neq 1$ tiene periodo (orden) infinito. Si cada elemento a de G es de periodo finito, se dice que G es un grupo **periódico**. Finalmente, se dice que G es un **grupo mixto** si G contiene elementos $a \neq 1$ tanto de periodo infinito como de periodo finito.*

2.3. Ejemplos

Ejemplo 2.3.1. ***Grupo sin torsión***. Notemos en primer lugar que todo grupo sin torsión debe ser infinito. Sea p un número primo. El conjunto de números racionales

$$\mathbb{Q}_p = \left\{ \frac{m}{p^n} \in \mathbb{Q} \mid m, n \in Z \right\}$$

bajo la adición es un grupo abeliano sin torsión, y se denomina el grupo de los p-cocientes racionales: por ser $\mathbb{Q}_p \subset Q$ y por ser la operación definida en $\mathbb{Q}_p$ la inducida por la adición en $\mathbb{Q}$ entonces es suficiente probar que $Q_p \leq Q$ y que Q_p es un grupo sin torsión:

$$\frac{m_1}{p^{n_1}} + \frac{m_2}{p^{n_2}} = \frac{m_1.p^{n_2} + m_2.p^{n_1}}{p^{n_1+n_2}} \in \mathbb{Q}_p,$$
$$-\frac{m}{p^n} = \frac{-m}{p^n} \in \mathbb{Q}_p$$

Sea $\frac{m}{p^n} \in \mathbb{Q}_p$, supóngase que existe $k > 0$ tal que $k\left(\frac{m}{p^n}\right) = 0$, es decir, $\frac{km}{p^n} = 0$, entonces $km = 0$, así $m = 0$. Luego, $\frac{m}{p^n} = 0$.

Ejemplo 2.3.2. ***Grupo infinito periódico***. Observemos en primer lugar que cada grupo finito es necesariamente periódico. Sin embargo, como lo muestra este ejemplo, la recíproca de la afirmación anterior no es correcta. Sea p un número primo. El conjunto de números complejos

$$\mathbb{C}_{p^\infty} := \left\{ z \in \mathbb{C} \mid z^{p^n} = 1, \text{ para algún } \ n = 0, 1, 2, \dots \right\}$$

bajo la multiplicación es un grupo abeliano infinito donde cada elemento diferente de 1 tiene periodo finito. Nótese pues que $\mathbb{C}_{p^\infty}$ consta de las raíces complejas de las ecuaciones $x^{p^n} = 1$, con $n = 0, 1, 2, \dots$. El grupo $\mathbb{C}_{p^\infty}$ se denomina ***grupo semicíclico*** del tipo p^∞.

Para probar que $\mathbb{C}_{p^\infty}$ es un grupo es suficiente probar que $\mathbb{C}_{p^\infty}$ es un subgrupo de $\mathbb{C}^*$: sean z_1 y $z_2 \in \mathbb{C}_{p^\infty}$, entonces existen n_1 y n_2 tales que $z_1^{p^{n_1}} = 1$ y $z_2^{p^{n_2}} = 1$. Si $n := n_1 + n_2$, entonces $z_1^{p^n} = 1$ y $z_2^{p^n} = 1$, luego $(z_1 z_2)^{p^n} = 1$, es decir, $z_1 z_2 \in \mathbb{C}_{p^\infty}$.

Sea $z \in \mathbb{C}_{p^\infty}$, entonces existe $n \geq 1$ tal que $z^{p^n} = 1$. Esto quiere decir que $z \in U_{p^n}$ y como $U_{p^n} \leq \mathbb{C}^*$ entonces $z^{-1} \in U_{p^n}$, es decir, $(z^{-1})^{p^n} = 1$ y así $z^{-1} \in \mathbb{C}_{p^\infty}$. Notemos que para cada $n \geq 1, U_{p^n} \leq \mathbb{C}_{p^\infty}$, y por la misma definición de $\mathbb{C}_{p^\infty}$, cada elemento z de $\mathbb{C}_{p^\infty}$ tiene periodo finito. Nótese que para cada $n \geq 1$ $U_{p^n} \leq U_{p^{n+1}}$. Denotando por $\mathbb{C}_{p^n}$ el grupo U_{p^n} obtenemos la cadena de subgrupos de $\mathbb{C}_{p^\infty}$:

$$\mathbb{C}_{p^\infty} = \bigcup_{k \geq 0} \mathbb{C}_{p^k}$$
$$\{1\} = \mathbb{C}_{p^0} \leq \mathbb{C}_p \leq \mathbb{C}_{p^2} \leq \mathbb{C}_{p^3} \leq \cdots \leq \mathbb{C}_{p^n} \leq \mathbb{C}_{p^{n+1}} \leq \cdots$$

Ejemplo 2.3.3. ***Grupo mixto***. El grupo multiplicativo de los números complejos es mixto ya que hay elementos, como por ejemplo los enteros diferentes de 1, que son de periodo infinito y complejos como $z_1 = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$, $n \neq 1$, que son de periodo finito.

2.4. Propiedades

Las siguientes afirmaciones son válidas para grupos cíclicos cualesquiera. Especialmente importante es la afirmación (iv).

Proposición 2.4.1. (i) *Todo grupo cíclico es abeliano.*

(ii) *Cada subgrupo de un grupo cíclico es cíclico.*

(iii) *Si* $\langle G, \cdot, 1\rangle$ *es un grupo cíclico infinito entonces cada subgrupo de* G *diferente de* $\{1\}$ *es también infinito.*

(iv) *Sea* $G \neq \{1\}$ *un grupo. Entonces,* G *es un grupo cíclico finito de orden primo si, y sólo si,* G *no tiene subgrupos diferentes de los triviales.*

Demostración. (i) Esta propiedad se deduce de la regla de exponentes $a^m a^n = a^{m+n}$ válida en todo grupo.

(ii) Sea $G = \langle a\rangle$ un grupo cíclico generado por el elemento a; sea H un subgrupo de G. Si $H = \{1\}$ entonces el es claramente cíclico con generador 1. Sea $H \neq \{1\}$, entonces existe un $k \neq 0$ tal que $a^k \in H$. Esto indica que H contiene potencias enteras positivas del elemento a. Por el principio de buena ordenación del conjunto $\mathbb{Z}^+$ escogemos el menor entero positivo s tal que $a^s \in H$. Afirmamos que $H = \langle a^s\rangle$. Claramente $\langle a^s\rangle \subseteq H$. Sea $x \in H \subseteq G$, entonces existe $m \in \mathbb{Z}$ tal que $x = a^m$. Utilizando el algoritmo de la división encontramos enteros g, r tales que $m = gs + r$, con $0 \leq r < s$, de donde $a^m = (a^s)^g a^r$ por lo que $a^r = a^{m-sg} \in H$. Por la elección de s concluimos que $r = 0$ y así $x = (a^s)^g \in \langle a^s\rangle$.

(iii) Sea $H \neq \{1\}$ un subgrupo del grupo cíclico infinito $\langle a\rangle = G$. Según (ii) existe $s > 0$ tal que $H = \langle a^s\rangle$. Si H es finito entonces eso quiere decir que el orden de a^s es finito con lo cual a es de periodo finito y así $\langle a\rangle$ es finito, lo cual contradice la hipótesis. Esto indica que H debe ser infinito.

(iv) $\Rightarrow$): sea G un grupo finito de orden primo $p : |G| = p$. Sea $H \leq G$, entonces $|H| \mid |G|$ de modo que $|H| = 1$ ó $|H| = p$, por lo tanto $H = \{1\}$ ó $H = G$.

$\Leftarrow$): sea $b \neq 1$, $b \in G$. El subgrupo cíclico $\langle b\rangle$ generado por b es entonces diferente de $\{1\}$. Por lo tanto $\langle b\rangle = G$, lo cual quiere decir que G es cíclico. Probemos ahora que G es finito. Consideremos el subgrupo cíclico generado por b^2. Por la condición de la hipótesis $\langle b^2\rangle = \{1\}$ ó $\langle b^2\rangle = G = \langle b\rangle$. En el primer caso tendremos que $b^2 = 1$ con lo cual b es de periodo 1 ó 2. No puede ser de periodo 1 ya que $b \neq 1$. Por lo tanto b es de periodo 2 y así $\langle b\rangle = \{1, b\}$, de donde se tiene que G es finito y su orden es el primo 2. Supóngase que $\langle b^2\rangle = G = \langle b\rangle$. Existe entonces $k \in \mathbb{Z}$ tal que $b = (b^2)^k$, es decir, $b^{2k-1} = 1$ con lo cual b es de período finito y $\langle b\rangle$ es finito; es decir G es finito. Resta sólo probar que el orden de G es un numero primo. Sea $p = |G|$ el orden del grupo G y sea $k \in \mathbb{Z}^+$ tal que $k \mid p$. Consideremos el subgrupo cíclico generado por b^k. Si $\langle b^k\rangle = \{1\}$ entonces $b^k = 1$ y k es un múltiplo del periodo p,

por lo que $k = p$. Supóngase ahora que $\langle b^k \rangle = G = \langle b \rangle$ entonces existe $t \in \mathbb{Z}$ tal que $\left(b^k\right)^t = b$, así $b^{kt-1} = 1$ entonces $p \mid kt - 1$, es decir que existe $s \in \mathbb{Z}$ tal que $kt - 1 = ps$, pero $k \mid p$ entonces existe $k' \in \mathbb{Z}$ tal que $p = kk'$; luego $kt - 1 = kk's$; así $k(t - k's) = 1$ entonces $k = 1$. Esto prueba que los únicos divisores de p son p y 1, y de esta forma se tiene que p es primo. □

2.5. Generadores

Teorema 2.5.1. (i) *Sea G un grupo cíclico finito de orden n con generador a. Entonces, $x \in G$ es generador de $G \Leftrightarrow x = a^r$, donde $m.c.d.(n, r) = 1$.*

(ii) *Sea G un grupo cíclico con generador a y sea $H \neq \{1\}$ un subgrupo de G. Entonces $H = \langle a^s \rangle$, donde s es el menor entero positivo tal que $a^s \in H$. Además, si G es de orden finito n entonces $|H| = \frac{n}{d}$, $d = m.c.d.(n, s)$.*

(iii) *Sea G un grupo cíclico de orden finito n y sea $t \in \mathbb{Z}^+$ tal que $t \mid n$. Entonces G contiene exactamente un subgrupo de orden t.*

Demostración. (i) $\Rightarrow$): sea x un generador de $G = \langle a \rangle$. Entonces existe un $r \in \mathbb{Z}$ tal que $x = a^r$ y $\langle x \rangle = \langle a^r \rangle = \langle a \rangle$. De aquí obtenemos que $a \in \langle a^r \rangle$, es decir, existe $k \in \mathbb{Z}$ tal que $a = (a^r)^k$ entonces $a^{rk-1} = 1$, así $n \mid rk - 1$ es decir $rk - 1 = sn$, con $s \in \mathbb{Z}$; de lo cual $rk - sn = 1$, así r y n son primos relativos y $m.c.d.(r, n) = 1$.

$\Leftarrow$): sea $r \in \mathbb{Z}$ tal que $m.c.d.(n, r) = 1$. Lógicamente, $\langle a^r \rangle \subseteq G$. Sea $x \in G$, entonces existe $k \in \mathbb{Z}$ tal que $x = a^k$. Como $m.c.d.(n, r) = 1$ existen $t, v \in \mathbb{Z}$ tales que $1 = nt + rv$, así $k = ntk + rvk$; luego $x = a^k = a^{ntk}a^{rvk} = a^{rvk} = (a^r)^{vk} \in \langle a^r \rangle$.

(ii) La primera parte de esta afirmación fue demostrada en el punto (ii) de la proposición 2.4.1.

Para la segunda parte, el orden de H es el orden de a^s. Sea $m := |a^s|$, entonces $(a^s)^m = 1$, es decir, $a^{sm} = 1$, luego $n \mid sm$, por lo tanto $\frac{n}{d} \mid m$, con $d := m.c.d.(n, s)$. De otra parte, $(a^s)^{\frac{n}{d}} = (a^n)^{\frac{s}{d}} = 1$ entonces $m \mid \frac{n}{d}$. Por lo tanto, $\frac{n}{d} \mid m$ y $m \mid \frac{n}{d}$ con lo cual $m = \frac{n}{d}$.

(iii) Existencia: como $t \mid n$ entonces $n = ts$, con $s \in \mathbb{Z}$, así $|\langle a^s \rangle| = t$. En efecto, $(a^s)^t = 1$, entonces $|a^s| \mid t$. Si $|a^s| := t_0$ y $t_0 < t$ entonces $a^{st_0} = 1$ y $st_0 < n$, lo cual es una contradicción.

Unicidad: sea H un subgrupo de G de orden t. Sea $n = ts$ y sea k el menor entero positivo tal que $a^k \in H$. Por (ii) sabemos que $H = \langle a^k \rangle$ y $t = |H| = \frac{n}{d}$, donde $d = m.c.d.(n, k)$; entonces $n = td = ts$ de modo que $s = d$, así $s \mid k$, es decir, $k = sw$ con $w \in \mathbb{Z}$. Luego, $a^k = (a^s)^w$ y por tanto $H \subseteq \langle a^s \rangle$, pero $|H| = |\langle a^s \rangle| = t$ entonces $H = \langle a^s \rangle$. □

Ejemplo 2.5.2. ***Los enteros módulo*** n. Sea $n \geq 2$ un entero, entonces el conjunto $\mathbb{Z}_n$ conformado por todos los enteros $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{n-1}\}$ conforman un grupo

cíclico respecto de la siguiente adición: $\overline{r}+\overline{s}:=\overline{t}$, donde t es el resíduo de dividir $r+s$ entre t. Nótese que el generador de $\mathbb{Z}_n$ es $\overline{1}$. El grupo $\mathbb{Z}_n$ lo consideraremos nuevamente en el capítulo 3. Por ahora digamos algo más respecto a su definición. También podríamos haberlo definido usando las ideas previas al teorema de Lagrange, es decir, se vió que en $\mathbb{Z}$ se puede definir la relación de equivalencia $\equiv$ respecto del subgrupo $\langle n\rangle$ en la forma $a\equiv b$ si, y sólo si, $a-b\in\langle n\rangle$. Esta relación divide a $\mathbb{Z}$ en n clases de equivalencia de la forma $[a]=\{x\in\mathbb{Z}\,|\,a-x\in\langle n\rangle\}=\langle n\rangle+a$. Las clases en este caso se denotan mejor en la forma $[a]=\overline{a}$, y la suma de clases se hace como se dijo arriba. Nótese que las clase distintas son exactamente $\{\overline{0},\overline{1},\overline{2},\overline{3},\ldots,\overline{n-1}\}$. Qeremos ahora calcular todos los subgrupos de $\mathbb{Z}_{24}$ y todos sus generadores.

Si $H\leq\mathbb{Z}_{24}$ entonces $|H|\mid 24$ de modo que $|H|\in\{1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 12,\ 24\}$

Para $|H|=1$ tenemos $H=\{\overline{0}\}$ y para $|H|=24$ tenemos $H=\mathbb{Z}_{24}$.

Para cada $r=\ 2,\ 3,4,6,8,12$ sabemos que $\mathbb{Z}_{24}$ contiene solamente un subgrupo de orden r. Ahora, cada subgrupo H es cíclico y de la forma $H=\langle s.\overline{1}\rangle=\langle\ \overline{s}\ \rangle$, donde $|H|=r=\frac{24}{d}$, con $d=m.c.d.(24,s)$. Obtenemos pues:

$\frac{24}{d}=2$, entonces $d=12=s$; $\langle\overline{12}\rangle=\{\overline{0},\ \overline{12}\}$
$\frac{24}{d}=3$, entonces $d=8=s$; $\langle\overline{8}\rangle=\{\overline{0},\ \overline{8},\ \overline{16}\}$
$\frac{24}{d}=4$, entonces $d=6=s$; $\langle\overline{6}\rangle=\{\overline{0},\ \overline{6},\ \overline{12},\ \overline{18}\}$
$\frac{24}{d}=6$, entonces $d=4=s$; $\langle\overline{4}\rangle=\{\overline{0},\ \overline{4},\ \overline{8},\ \overline{12},\ \overline{16},\ \overline{20}\}$
$\frac{24}{d}=8$, entonces $d=3=s$; $\langle\overline{3}\rangle=\{\overline{0},\ \overline{3},\ \overline{6},\ \overline{9},\ \overline{12},\ \overline{15},\ \overline{18},\ \overline{21}\}$
$\frac{24}{d}=12$, entonces $d=2=s$; $\langle\overline{2}\rangle=\{\overline{0},\ \overline{2},\ \overline{4},\ \overline{6},\ \overline{8},\ \overline{10},\ \overline{12},\ \overline{14},\ \overline{16},\ \overline{18},\ \overline{20},\ \overline{22}\}$.

Los generadores de $\mathbb{Z}_{24}$ son de la forma $\overline{1}=\overline{s}$, con $m.c.d.(s,24)=1$. Entonces $s=1,5,7,11,13,17,19,23$.

2.6. Ejercicios

1. Sea G un grupo y sean a,b elementos de G tales que:

   (i) $\langle a\rangle\cap\langle b\rangle=\{1\}$

   (ii) ab=ba

   (iii) $|a|=m,\quad |b|=n$

   Demuestre que $|ab|=m.c.m.\,(|a|\,,|b|)$.

2. Sea G un grupo y sean a,b elementos de G tales que:

   (i) ab=ba

   (ii) $|a|=n,\quad |b|=m$

   (iii) $m.c.d.(n,m)=1$

Demuestre que $|ab| = nm$. Además, $\langle a, b\rangle = \langle ab\rangle$.

3. Sea G un grupo y sean a, b elementos de G. Demuestre que:

   (i) $|a| = |a^{-1}|$

   (ii) $|xax^{-1}| = |a|$, para todo $x \in G$.

   (iii) $|ab| = |ba|$

   (iv) Sea $|a| = n$. Pruebe que $a^i = a^j \Leftrightarrow n \mid i - j$.

4. Sea $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{n-1}\}$ el conjunto de los enteros módulo n. En $\mathbb{Z}_n$ definimos la multiplicación mediante la regla $\overline{r}.\overline{s} := \overline{rs}$. Demuestre que $\langle \mathbb{Z}_n, \cdot\rangle$ es un semigrupo conmutativo con elemento identidad $\overline{1}$ (compruebe inicialmente que la operación $\cdot$ en $\mathbb{Z}_m$ está bien definida). Construya la tabla para $n = 8$. Es $\langle \mathbb{Z}_8, \cdot\rangle$ un grupo?

5. Sea $\mathbb{Z}_n$ el conjunto de los enteros módulo n. Sea $\mathbb{Z}_n^*$ el grupo multiplicativo del semigrupo $\langle \mathbb{Z}_n, \cdot\rangle$ del ejercicio anterior. Demostrar que: $[r] \in Z_n^* \Leftrightarrow m.c.d.(r, n) = 1$.

6. La función $\varphi : \mathbb{N} \to \mathbb{N}$ del conjunto de los números naturales que asigna a cada natural m el número de enteros positivos menores que m y que son primos relativos con él. Por ejemplo, $\varphi(6) = 2$, $\varphi(10) = 4$. La función φ es denominada ***función de Euler***. Según el ejercicio anterior, $\mathbb{Z}_m^*$ tiene $\varphi(m)$ elementos. Utilice estas observaciones para demostrar los siguientes teoremas:

   (i) **Teorema de Euler**: sean a, m enteros, $m > 0$ y $m.c.d.(a, m) = 1$. Entonces $a^{\varphi(m)} \equiv 1$ (módulo m), es decir, $m \mid a^{\varphi(m)} - 1$.

   (ii) **Teorema de Fermat**: si p es primo entonces $a^p \equiv a$ (módulo p), para todo $a \in \mathbb{Z}$.

7. Sea G un grupo cíclico de orden 60. ¿Cuántos generadores tiene G ?

8. Determine el subgrupo cíclico de $\langle \mathbb{Z}_{42}, +\rangle$ generado por $\overline{30}$.

9. Demuestre que $\frac{(1+i)}{\sqrt{2}}$ es un elemento de periodo finito de $\mathbb{C}^*$.

10. Sean p y q primos diferentes. Calcule el número de generadores del grupo cíclico $\langle \mathbb{Z}_{pq}, +\rangle$.

11. Determine todos los subgrupos de $\mathbb{Z}_{36}$ y todos sus generadores.

12. Determine todos los subgrupos de $\mathbb{C}_{36}$ y todos sus generadores.

13. Demuestre que los subgrupos de $\mathbb{C}_{p^\infty}$ son: $1 = \mathbb{C}_{p^0} < \mathbb{C}_{p^1} < \mathbb{C}_{p^2} < \cdots < \mathbb{C}_{p^n} < \cdots$.

Demostración. Sea H un subgrupo propio de $\mathbb{C}_p\infty$. Si para cada $k \geq 0$, $\mathbb{C}_{p^k} \leq H$, entonces $H = \mathbb{C}_{p^\infty}$, pero este caso está descartado. Entonces existe un $k \geq 0$ tal que $\mathbb{C}_{p^k}$ no está incluido en H. Escojamos el menor k tal que $\mathbb{C}_{p^{k-1}} \leq H$ pero $\mathbb{C}_{p^k}$ no está incluido en H. k no puede ser 0 ya que $\mathbb{C}_{p^0} \leq H$. Por lo tanto $k \geq 1$. La idea es entonces demostrar que $H = \mathbb{C}_{p^{k-1}}$. Si esto es así entonces el n buscado es $n = k - 1$.

Sabemos que $\mathbb{C}_{p^{k-1}} \leq H$ y supongamos que la inclusión es estricta, es decir, existe $z \in H$ pero $z \notin \mathbb{C}_{p^{k-1}}$. Como $z \in \mathbb{C}_{p^\infty}$ existe un $m \geq 1$ mínimo tal que $z \in \mathbb{C}_{p^m}$ pero $z \notin \mathbb{C}_{p^{m-1}}$. Nótese que $m \geq k$ porque de lo contario $z \in \mathbb{C}_{p^{k-1}}$. Se tiene que $\mathbb{C}_{p^k} \leq C_{p^m}$. Sea $\mathbb{C}_{p^m} =< z_1 >$, entonces $z = z_1^a$, donde $0 \leq a \leq p^m - 1$, nótese que p no divide al entero a. En efecto, si $p|a$, entonces $a = pb$ y en consecuencia $z^{p^{m-1}} = z_1^{ap^{m-1}} = z_1^{bp^m} = 1$, pero esto indica que $z \in \mathbb{C}_{p^{m-1}}$, lo cual es falso. Se tiene entonces que a y p^m son primos realtivos, es decir, $1 = ua + vp^m$, donde u, v son enteros. De aquí resulta que $z_1 = (z_1^a)^u(z_1^{p^m})^v = z^u$. Esto implica que $\mathbb{C}_{p^m} \leq< z >\leq H$ y de aquí se tendría que $\mathbb{C}_{p^k} \leq H$, lo cual es falso. En conclusión, $H = \mathbb{C}_{p^{k-1}}$. □

Capítulo 3

Subgrupos normales y homomorfismos

El objetivo central de este capítulo es mostrar la estrecha relación que guardan los conceptos de subgrupo normal y homomorfismo de grupos. Será demostrado que, salvo isomorfismo, hay tantos subgrupos normales en un grupo G como imágenes homomorfas tiene este último. El concepto de grupos isomorfos permite, entre otras cosas, clasificar los grupos cíclicos: los infintos que son isomorfos a $\langle \mathbb{Z}, + \rangle$, y los finitos de orden n que son isomorfos a $\langle \mathbb{Z}_n, + \rangle$. Dentro de los ejercicios hemos incluído un grupo muy importante como es el grupo óctico correspondiente a las 8 simetrías del cuadrado.

3.1. Subgrupos normales

En el capítulo 1 se construyó el grupo de enteros módulo $n, \mathbb{Z}_n$, por medio de 4 objetos, a saber: el grupo $\mathbb{Z}$, el subgrupo $\langle n \rangle$ de múltiplos de n, la relación de equivalencia en $\mathbb{Z}$ definida como $a \equiv b$ si, y sólo si,, $a - b \in \langle n \rangle$ y la operación de adición entre clases de equivalencia determinadas por esta relación: $\overline{a} + \overline{b} = \overline{a + b}$, $a, b \in \mathbb{Z}$

Vale la pena preguntarnos si, dado un grupo G y H un subgrupo cualquiera de G, podemos repetir la construcción mencionada anteriormente con ayuda de la relación de equivalencia en G utilizada para la demostración del teorema de Lagrange: $a \equiv b \Leftrightarrow ab^{-1} \in H$. Puesto que las clases de equivalencia están determinadas por el subgrupo H, será lógico preguntarnos que condición debe satisfacer H para que podamos dar al conjunto de clases de equivalencia una estructura de grupo. Antes de responder a estas preguntas recordemos cierta terminología ya introducida antes por nosotros.

Definición 3.1.1. *Sea G un grupo y sean A y B subconjuntos no vacíos de G.*

Se denomina ***producto de los conjuntos*** A *y* B *(en ese orden) al conjunto de productos de la forma* ab*, donde* $a \in A$ *y* $b \in B$*, y se denota por* AB*. En otras palabras,* $AB := \{ab \mid a \in A, b \in B\}$*.*

Proposición 3.1.2. *Sea* G *un grupo y sea* H *un subgrupo de* G*. Entonces las siguientes condiciones son equivalentes:*

(i) $\forall x \in G, \forall h \in H : x^{-1}hx \in H$

(ii) $\forall x \in G : x^{-1}Hx = H$

(iii) $\forall x \in G : xH = Hx$

(iv) $\forall x, y \in G : xHyH = xyH$

Demostración. (i) $\Rightarrow$ (ii): evidentemente $x^{-1}Hx \leq H$. Sea ahora $h \in H$. Entonces $h = x^{-1}(xhx^{-1})x$; según (i), $xhx^{-1} \in H$; así pues, $H \leq x^{-1}Hx$.

(ii)$\Rightarrow$ (iii): sea $h \in H$, entonces $xhx^{-1} \in H \Rightarrow xhx^{-1} = h_0 \in H \Rightarrow xh = h_0x \in Hx; \Rightarrow xH \leq Hx$. Análogamente, $Hx \leq xH$.

(iii)$\Rightarrow$ (iv): sean $h_1, h_2 \in H :\Rightarrow xh_1\ yh_2 = xyh_1'h_2$, donde $h_1' \in H; \Rightarrow xHyH \leq xyH$. Ahora, si $h \in H$ se obtiene que $xyh = x,1yh \in xHyH$, es decir, $xyH \leq xHyH$.

(iv)$\Rightarrow$ (i): sea $x \in G$, $h \in H \Rightarrow x^{-1}hx \in x^{-1}HxH \Rightarrow x^{-1}hx \in x^{-1}xH = H$. Esto completa la prueba de la proposición. □

Definición 3.1.3. *Sea* G *un grupo y* $H \leq G$*. Se dice que* H *es un* ***subgrupo normal*** *de* G*, lo cual denotamos por* $H \trianglelefteq G$*, si* H *cumple una de las condiciones de la proposicion anterior.*

Definición 3.1.4. *Sea* $G \neq \{1\}$ *un grupo. Entonces* G *posee al menos dos subgrupos normales, llamados los* ***subgrupos normales triviales****:* $\{1\}$*,* G*. Si* G *no posee otros subgrupos normales fuera de los triviales se dice que* G *es un* ***grupo simple****.*

3.2. Grupo cociente

Sea G un grupo y $H \trianglelefteq G$. En G se tiene la relacion

$$a \equiv b \Leftrightarrow ab^{-1} \in H$$

Como ya fue demostrado en el capítulo 1, $\equiv$ es una relacion de equivalencia la cual determina una partición del grupo G en clases de equivalencia, llamadas también ***clases laterales derechas***:

$$[a] = Ha$$

Nótese que la relación $\equiv$ es igual a la relacion $\equiv'$ definida por $a \equiv' b \Leftrightarrow a^{-1}b \in H$. En tal caso $[a] = aH$. Pero como $H \trianglelefteq G$ entonces las clases laterales derechas e izquierdas de a coinciden.

Podemos definir un producto entre clases de equivalencia, así como se hizo en $\mathbb{Z}_n$, y dar al conjunto de clases estructura de grupo.

Proposición 3.2.1. *Sea $\langle G, \cdot, 1\rangle$ un grupo y sea $H \trianglelefteq G$. Sea $\equiv'$ la relación de equivalencia de G definida por:*

$$a \equiv' b \Leftrightarrow a^{-1}b \in H$$
$$(\textit{equivalentemente, } \ a \equiv b \Leftrightarrow ab^{-1} \in H)$$

Sea G/H el conjunto de clases de equivalencia (de clases laterales derechas o izquierdas) determinadas por la relacion $\equiv$. Entonces definiendo el producto de clases de G/H por:

$$aH \ bH := abH, \ \ \forall a, b \in G$$
$$(\bar{a} \ \bar{b} := \overline{ab})$$

*G/H adquiere estructura de grupo. G/H se denomina el **grupo cociente** de G por H.*

La clase con representante a será denotada simplemente por $\overline{a}$ o aH en el caso multiplicativo; en notación aditiva $\bar{a} = a + H$.

Proposición 3.2.2. *Sea G un grupo y $H \trianglelefteq G$. Entonces,*

(i) *Si G es abeliano, entonces G/H es también abeliano.*

(ii) *Si G es cíclico con generador a, entonces G/H es cíclico con generador $\overline{a}$*

(iii) *Si G es finito, entonces $|G : H| = |G/H| = \frac{|G|}{|H|}$*

(iv) $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$

(v) *Sea $K \leq G$ y $H \trianglelefteq G$ tal que $H \leq K$. Entonces, $H \trianglelefteq K$.*

(vi) *Sea $H \leq G$ tal que $|G : H| = 2$, entonces $H \trianglelefteq G$.*

(vii) *La relación de normalidad no es en general transitiva.*

Demostración. Las cinco primeras afirmaciones son casi evidentes. Veamos la prueba de (vi): G queda dividido en sólo dos clases laterales izquierdas: $G = H \bigcup (G - H)$. Sea $x \in G, \ h \in H$; consideremos las siguientes cuatro posibilidades:

a) $x^{-1}h \in H, \ x^{-1} \in H \Rightarrow x^{-1}hx \in H$

b) $x^{-1}h \in H, \ x^{-1} \notin H$, imposible

c) $x^{-1}h \notin H, \ x^{-1} \in H$, imposible

d) $x^{-1}h \notin H, \ x^{-1} \notin H \Rightarrow \ x^{-1}h \equiv x^{-1} \Rightarrow x^{-1}hx \in H \Rightarrow H \trianglelefteq G.$

(vii) Esto se ilustra en el siguiente ejemplo. □

Ejemplo 3.2.3. Consideremos un cuadrado cuyos vértices se numeran sucesivamente en sentido contrario al movimiento de las manecillas del reloj con los números 1, 2, 3, 4, comenzando en el extremo inferior izquierdo, y consideremos el conjunto D_4 de las 8 simetrías de un cuadrado: cuatro rotaciones en sentido contrario al movimiento de las manecillas del reloj a través de los ángulos: $\frac{2\pi k}{4}$, $k = 0, 1, 2, 3$:

Cuatro reflexiones a través de cuatro ejes de simetría: $X, Y, \overline{13}, \overline{24}$. Este conjunto de 8 movimientos posee estructura de grupo bajo la operación de composición de movimientos. Nótese que cada movimiento permuta los vértices 1, 2, 3, 4; por lo tanto el grupo D_4 puede ser mirado como subgrupo de S_4: la rotación a través del ángulo $\theta = \frac{\pi}{2}$, $k = 1$, corresponde a la permutación:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 2\ 3\ 4)$$

Observe que las otras tres rotaciones corresponden a potencias de f : f^2, f^3, $f^4 = 1$ = rotación de cero grados.

La reflexión a través del eje $\overline{13}$ corresponde a la permutación:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2\ 4),\ g^2 = 1$$

Las otras tres reflexiones corresponden a productos de f y g :

Reflexión a través del eje Y:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = fg$$

Reflexión a través del eje X:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = f^3 g$$

Reflexión a través del eje $\overline{24}$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = f^2 g$$

Como dijimos anteriormente, $D_4 = \{1, f, f^2, f^3, fg, f^2g, f^3g, g\}$ es un subgrupo conocido como grupo dihédrico de grado 4. Nótese que $H = \{1, g\} \leq K = \{1, g, f^2, f^2g\}$. Además, $K \trianglelefteq D_4$ ya que $|D_4 : K| = 2$, $H \trianglelefteq K$ ya que $|K : H| = 2$ pero H no es subgrupo normal de D_4 : $f^3 g \left(f^3\right)^{-1} = f^3 gf = f^2 g \notin H$.

3.3. Homomorfismo de grupos

En esta sección se presenta el concepto de homomorfismo de grupos así como también algunas de las propiedades fundamentales de estas funciones. Al final, con ayuda del concepto de isomorfismo, se hace una clasificación de los grupos cíclicos.

Definición 3.3.1. *Sean $\langle G, \cdot\rangle$ y $\langle F, \cdot\rangle$ dos grupos. Una función $\varphi : G \to F$ tal que $\varphi(ab) = \varphi(a)\ \varphi(b), \forall a, b \in G$ se denomina un* ***homomorfismo*** *del grupo G en el grupo F.*

Si ambos grupos tienen notación aditiva, entonces la condición anterior se escribe como $\varphi(a + b) = \varphi(a) + \varphi(b)$. Veamos algunos ejemplos:

(i) Sea $G = \mathbb{R}$ el grupo aditivo de los números reales, y sea $F = \mathbb{R}^*$ el grupo multiplicativo de los números reales no nulos. La función $f : \mathbb{R} \to \mathbb{R}^*$ definida por $f(x) =: e^x$ es un homomorfismo de $\mathbb{R}$ en $\mathbb{R}^*$.

(ii) ***Homomorfismo trivial***: sea $\langle G, \cdot, 1\rangle$ un grupo multiplicativo y sea $\langle F, +, \circ\rangle$ un grupo con notación aditiva. La función de G en F definida por $f : G \to F$, $f(x) = 0$ es un homomorfismo, Además la función $g : F \to G$ es definida por $g(x) = 1$ es también un homomorfismo; lo podemos denominar homomorfismo unitario.

(iii) ***Homomorfismo idéntico***: sea $\langle G, \cdot\rangle$ un grupo. La función $\imath : G \to G$ de G en si mismo definida por $i_G(x) := x$ es un homomorfismo.

Definición 3.3.2. *Sea $\varphi : G \to F$ un homomorfismo de grupos.*

(i) *Sea 1 el elemento identidad del grupo F. El conjunto de elementos de G cuya imagen es el elemento identidad 1 de F se denomina el* ***núcleo*** *de φ y se denota por* $\ker(\varphi)$*:*

$$\ker(\varphi) := \{g \in G \mid \varphi(g) = 1\}.$$

(i) *Sea $A \subseteq G$. El conjunto de las imágenes de los elementos del conjunto A se denomina* ***imagen*** *del conjunto A mediante φ y se denota por $\varphi(A)$:*

$$\varphi(A) := \{\varphi(a) \mid a \in A\}.$$

En particular el conjunto $\varphi(G)$ se denomina la imagen del homomorfismo φ y se simboliza también por $Im(\varphi)$.

(iii) *Sea $B \subseteq F$. El conjunto de elementos de G cuyas imágenes pertenencen al conjunto B se denomina* ***imagen inversa*** *de B mediante φ,*

$$\varphi^{-1}(B) := \{g \in G \mid \varphi(g) \in B\}.$$

(iv) *Se dice que φ es un* ***homomorfismo inyectivo*** *si φ es una función inyectiva, es decir, para cualesquiera elementos $x, y \in G$ se cumple*

$$\varphi(x) = \varphi(y) \Leftrightarrow x = y.$$

(v) *Se deice que φ es un* ***homomorfismo sobreyectivo*** *si $Im(\varphi) = F$.*

(vi) *Se dice que un grupo F es una* ***imagen homomorfa*** *de un grupo G si existe un homomorfismo sobreyectivo de G en F.*

(vii) *Se dice que φ es un* ***isomorfismo*** *o también que G y F son grupos isomorfos, lo cual se dentoa por $G \cong F$, si φ es inyectivo y sobreyectivo.*

Proposición 3.3.3. *Sea $\varphi : G \to F$ un homomorfismo, entonces:*

(i) $\varphi(1) = 1$.

(ii) $\varphi(x^{-1}) = \varphi(x)^{-1}$, *para cada $x \in G$.*

(iii) $\ker(\varphi) \trianglelefteq G$.

(iv) *La imagen de un subgrupo de G mediante φ es un subgrupo de F:*

$$H \leq G \Rightarrow \varphi(H) \leq F.$$

(v) *La imagen inversa de un subgrupo de F mediante φ es un subgrupo de G:*

$$K \leq F \Rightarrow \varphi^{-1}(K) \leq G.$$

(vi) *La imagen de un subgrupo normal de G mediante φ es un subgrupo normal de la imagen de φ:*

$$H \trianglelefteq G \Rightarrow \varphi(H) \trianglelefteq \mathrm{Im}(\varphi).$$

(vii) *La imagen inversa de un subgrupo normal de F mediante φ es un subgrupo normal de G:*

$$K \trianglelefteq F \Rightarrow \varphi^{-1}(K) \trianglelefteq G.$$

(viii) φ *es inyectivo* $\Leftrightarrow \ker(\varphi) = \{1\}$.

(ix) *Sea* $H \trianglelefteq G$. *La función* $j : G \to G/H$ *definida por* $j(x) =: \bar{x} = xH$ *es un homomorfismo sobreyectivo.* j *se denomina el* ***homomorfismo canónico****.*

(x) φ *es un isomorfismo si, y sólo si,, existe una función* $\theta : F \to G$ *tal que*

$$\theta\varphi = i_G, \varphi\ \theta = i_F.$$

Además, θ *es también un homomorfismo.* θ *se denomina el* ***homomorfismo inverso*** *de* φ *y se denota por* φ^{-1}*.*

(xi) *Sea* $\alpha : F \to M$ *un homomorfismo. Entonces la función compuesta* $\alpha\varphi : G \to M$ *es un homomorfismo.*

Demostración. Todas las pruebas se reducen a aplicar directamente las definiciones anteriores. □

Teorema 3.3.4. *Sea* G *un grupo cíclico. Entonces,*

(i) *Si* G *es infinito, entonces* $G \cong \mathbb{Z}$*.*

(ii) *Si es finito de orden* n*, entonces* $G \cong \mathbb{Z}_n$*.*

Demostración. Es un ejercicio sencillo que se deja al lector. □

3.4. Ejercicios

1. Demuestre que en un grupo abeliano todos sus subgrupos son normales.

2. Sea G un grupo y A un subconjunto no vacío de G. Sea $x \in G$ el conjunto:

$$A^x := x^{-1}Ax = \{x^{-1}ax \,|\, a \in A\}.$$

se denomina el ***conjugado*** de A por x. Demuestre que el conjugado de un subgrupo de G mediante cualquier elemento x de G es también un subgrupo de G. Demuestre que si $A \subseteq G$, entonces $\forall x \in G$, $Card(x^{-1}Ax) = Card(A)$.

3. Sea G un grupo, H un subgrupo de G y A un subconjunto no vacío de G. Demuestre que

$$N_H(A) := \{x \in H \,|\, A^x = A\} \text{ y } C_H(A) := \{x \in H \,|\, xs = sx, \forall s \in A\}$$

son subgrupos de H ($N_H(A)$ se llama el ***normalizador*** de A en H y $C_H(A)$ se llama el ***centralizador*** de A en H). Compruebe además que $C_H(A) \trianglelefteq N_H(A)$.

4. Sea G un grupo y $K \leq G$. Con las definiciones del ejercicio anterior, $N_G(K)$ se denomina el normalizador de K en G y $C_G(K)$ se denomina el centralizador de K. El centralizador de G se denota por $Z(G)$ y se llama el ***centro*** del grupo G. Demuestre que

   a) $K \trianglelefteq N_G(K)$ y $Z(G)$ es un grupo abeliano.

   b) $K \trianglelefteq G \Leftrightarrow G = N_G(K)$.

   c) Sea $H \leq G$ tal que $K \trianglelefteq H$. Entonces $H \subseteq N_G(K)$.

5. Sea G un grupo, $H \leq G$, $A \neq \emptyset$, $A \subseteq G$. Denotemos por F a la familia de subconjuntos de G constituidos por los conjugados de A con elementos de H, es decir $F := \{A^x \mid x \in H\}$. Demuestre que $Card(F) = |H : N_H(A)|$.

6. Sea G un grupo y sea X un conjunto no vacío. Demuestre que $Z[Apl(X, G)] = Aplc(X, Z(G))$.

7. Demuestre que la intersección de dos subgrupos normales es un subgrupo normal. Generalice este resultado a una familia no vacía cualquiera de subgrupos normales.

8. Sea G un grupo y $H \trianglelefteq G$. Demuestre que las relaciones de equivalencia $\equiv_1$ y $\equiv_2$ definidas por $a \equiv_1 b \Leftrightarrow ab^{-1} \in H$ y $a \equiv_2 b \Leftrightarrow a^{-1}b \in H$ son iguales, es decir, $\forall a, b \in G$, $a \equiv_1 b \Leftrightarrow a \equiv_2 b$.

Capítulo 4

Teoremas de estructura

El concepto de homomorfismo e isomorfismo, así como los teoremas correspondientes, son el objeto del presente capítulo. Por medios de estos teoremas se pueden caracterizar las imágenes homomorfas de un grupo, y son herramienta clave para la clasificación de grupos, en particular, para la clasificación de grupos finitos.

4.1. Teorema fundamental de homomorfismo

Se mostrará en esta sección que un grupo G tiene tantas imágenes homomorfas como grupos cocientes por subgrupos normales, este es precisamente el contenido del teorema fundamental de homomorfismo.

Teorema 4.1.1 (Teorema fundamental de homomorfismo). *Sea G un grupo cualquiera. Entonces hay tantas imágenes homomorfas de G como subgrupos normales tiene G (o lo que es lo mismo, como grupos cocientes de G). Más exactamente, si G' es una imagen homomorfa de G entonces existe un subgrupo normal H de G tal que $G' \cong G/H$. H es precisamente el núcleo del homomorfismo $G \to G'$. Recíprocamente, dado un subgrupo normal H de G, G/H es una imagen homomorfa de G. El homomorfismo sobreyectivo requerido es el homomorfismo canónico $j : G \to G/H$.*

Demostración. Sea G' una imagen homomorfa de G con homomorfismo sobreyectivo $h : G \to G'$; sea $\ker(h)$ el núcleo de h y sea $j : G \to G/kerh$ el homomorfismo canónico de G sobre el grupo cociente $G/\ker(h)$. Se define la función

$$\overline{h} : G/\ker h \to G'$$

mediante $\bar{h}(\bar{x}) := h(x)$, donde $\bar{x} = x \ker h$ es la clase de equivalencia (clase lateral izquierda) determinada por el elemento x. $\bar{h}$ está bien definida, $\bar{h}$ es sobre y $\bar{h}$ es inyectiva. Además, $\bar{h}$ es un homomorfismo de grupos. Finalmente, ya se ha visto que la función canónica j es un homomorfismo sobre de G en G/H. □

Corolario 4.1.2. *Sea $h : G \to G'$ un homomorfismo de grupos. Entonces $Im(h) \cong G/\ker h$.*

Ejemplo 4.1.3. (i) Determinemos todas las imágenes homomorfas del grupo aditivo de los números enteros $\langle \mathbb{Z}, + \rangle$: según el teorema fundamental de homomorfismo las imágenes homomorfas de $\langle \mathbb{Z}, + \rangle$ son los subgrupos cociente de $\mathbb{Z}$ por sus subgrupos normales. De esta manera debemos determinar todos los subgrupos normales H de $\mathbb{Z}$ y construir los grupos cociente G/H. Como $\langle \mathbb{Z}, + \rangle$ es un grupo abeliano entonces cada uno de sus subgrupos es normal. Así pues, las imágenes homomorfas de $\mathbb{Z}$ son de la forma $\mathbb{Z}/\langle n \rangle$ con $n \geq 0$, es decir las imágenes de $\langle \mathbb{Z}, + \rangle$ son $\mathbb{Z}_n$ con $n \geq 0$.

(ii) Sea $(\mathbb{R}, +, 0)$ el grupo de los números reales bajo la adición y sea $(U, \cdot, 1)$ el grupo multiplicativo de los complejos de módulo 1: $U = \{z \in \mathbb{C} \mid |z| = 1\}$. Nótese que $U = \{\cos\theta + i \sin\theta \mid \theta \in \mathbb{R}\} = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$. La función $\varphi : \mathbb{R} \to U$ definida por $\varphi(\theta) = e^{i\theta}$ es un homomorfismo: en efecto, $\varphi(\theta_1 + \theta_2) = e^{i(\theta_1+\theta_2)} = e^{i\theta_1} \cdot e^{i\theta_2}$. φ es obviamente un homomorfismo sobreyectivo ya que cada complejo tiene determinado al menos un argumento θ. Según el teorema fundamental de homomorfismo $U \cong \mathbb{R}/\ker(\varphi)$; $\ker(\varphi) = \{\theta \in \mathbb{R} \mid \cos\theta + i \sin\theta = 1\} \Rightarrow$ si $\theta \in \ker(\varphi) \Rightarrow \sin\theta = 0 \Rightarrow \theta = 2k\pi$, $k \in \mathbb{Z}$. Recíprocamente, cada real de forma $\theta = 2k\pi$, $k \in \mathbb{Z}$ es un elemento de $\ker(\varphi) \Rightarrow N(\varphi) = \langle 2\pi \rangle$, grupo generado por $2\pi \Rightarrow U \cong \mathbb{R}/\langle 2\pi \rangle$.

(iii) Imágenes homomorfas de S_3 : determinamos en primer lugar los subgrupos de S_3. Puesto que $|S_3| = 6$ entonces S_3 sólo puede tener grupos de orden $1, 2, 3$ y 6:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \ , \qquad g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix}$$

$$S_3 = \{1, f, f^2, g, fg, f^2g\} \ ; \ f^2 = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}, \ fg = \begin{pmatrix} 1 & 2 \end{pmatrix}, \ f^2g = \begin{pmatrix} 1 & 3 \end{pmatrix}$$

$$1 = \{1\} \text{ es el único subgrupo de orden 1}$$

Los subgrupos de orden 2 son cíclicos y por lo tanto generados por los elementos de orden 2:

$$\langle g \rangle, \langle fg \rangle, \ \langle f^2g \rangle \text{ son los subgrupos de orden 2}$$

Los subgrupos de orden 3 son necesariamente cíclicos y son generados por elementos de orden 3 :

$$\langle f \rangle \text{ es el único subgrupo de orden 3}$$

$$S_3 \text{ es el único subgrupo de orden 6}$$

1 y S_3 son normales. Puesto que $|S_3 : \langle f \rangle| = 2$ entonces $\langle f \rangle \trianglelefteq S_3$.

Para la determinación de subgrupos normales de orden 2 no sobra construir la tabla del grupo S_3 :

$\circ$	1	f	f^2	g	fg	f^2g
1	1	f	f^2	g	fg	f^2g
f	f	f^2	1	fg	f^2g	g
f^2	f^2	1	f	f^2g	g	fg
g	g	f^2g	fg	1	f^2	f
fg	fg	g	f^2g	f	1	f^2
f^2g	f^2g	fg	g	f^2	f	1

$\langle g\rangle$ no es subgrupo normal de S_3 ya que $fgf^{-1} = fgf^2 = f^2g \notin \langle g\rangle$; $\langle fg\rangle$ no es subgrupo normal de S_3 ya que $f^2fg\,(f^2)^{-1} = f^2fgf = gf = f^2g \notin \langle fg\rangle$; $\langle f^2g\rangle$ no es subgrupo normal de S_3 ya que $ff^2gf^{-1} = gf^2 = fg \notin \langle f^2g\rangle$.

S_3 no tiene subgrupos normales de orden 2

1, $\langle f\rangle$, S_3 son los subgrupos normales de S_3

De aquí obtenemos que las imágenes homomorfas de S_3 (salvo isomorfismo) son $S_3/1 = S_3$, $S_3/\langle f\rangle \cong \mathbb{Z}_2$ ya que $|S_3/\langle f\rangle| = \frac{6}{3} = 2$; $S_3/S_3 \cong \mathbb{Z}_1$ (grupo unitario).

4.2. Teorema de factorización

Definición 4.2.1. *Sea $\alpha : G_1 \to G_2$ un homomorfismo de grupos. Se dice que el homomorfismo α se puede **factorizar** a través del homomorfismo $j : G_1 \to G_3$ (o también, a través del grupo G_3) si existe un homomorfismo $\theta : G_3 \to G_2$ tal que $\theta j = \alpha$.*

Teorema 4.2.2. *Sea $\alpha : G \to G'$ un homomorfismo de grupos y sea H un subgrupo normal de G. Entonces α se puede factorizar de una manera única a través de G/H si, y sólo si,, $H \subseteq \ker\alpha$.*

Demostración. $\Rightarrow$): sea $H \trianglelefteq G$ tal que α se puede factorizar a través de G/H. Esto quiere decir que existe un homomorfismo $\theta : G/H \to G'$ tal que $\theta j = \alpha$. Sea $x \in H \Rightarrow \theta j(x) = \alpha(x) \Rightarrow \theta(j(x)) = \theta(\bar{x}) = \theta(\bar{1}) = 1 = \alpha(x) \Rightarrow x \in \ker(\alpha) \Rightarrow H \subseteq \ker(\alpha)$.

$\Leftarrow$) Supóngase que $H \trianglelefteq G$ tal que $H \subseteq \ker(\alpha)$. Definimos

$$\theta : G/H \to G' \ \theta(\bar{x}) := \alpha(x), \ \ \bar{x} = xH, \ \ x \in G \ .$$

θ está bien definida : $\bar{x} = \bar{y} \Rightarrow x^{-1}y \in H \Rightarrow x^{-1}y \in \ker(\alpha) \Rightarrow \alpha(x^{-1}y) = 1 \Rightarrow \alpha(x)^{-1}\alpha(y) = 1 \Rightarrow \alpha(x) = \alpha(y) \Rightarrow \theta(\bar{x}) = \theta(\bar{y})$.

θ es homomorfismo : $\theta(\bar{x}\cdot\bar{y}) = \theta(\overline{xy}) = \alpha(xy) = \alpha(x)\alpha(y) = \theta(\bar{x})\theta(\bar{y})$.

$\theta j(x) = \theta(\bar{x}) = \alpha(x)$, para todo $x \in G; \Rightarrow \theta j = \alpha$.

θ es única : sea $\beta : G/H \to G'$ un homomorfismo tal que $\beta j = \alpha; \Rightarrow \beta j(x) = \beta(\bar{x}) = \alpha(x) = \theta(\bar{x}); \Rightarrow \beta = \theta$. $\square$

Corolario 4.2.3. (i) *El homomorfismo θ del teorema anterior es inyectivo $\Leftrightarrow$ $H = \ker(\alpha)$. Además, θ es sobreyectivo $\Leftrightarrow$ α es sobreyectivo.*

(ii) *Cada homomorfismo sobreyectivo $G \xrightarrow{\alpha} G'$ se puede factorizar de manera única a través del grupo cociente $G/\ker(\alpha)$. Además, en este caso θ es un isomorfismo.*

Demostración. (i) Supóngase que θ es un homomorfismo inyectivo y sea $x \in \ker(\alpha)$. Entonces $\alpha(x) = 1 = \theta(\bar{x}); \Rightarrow \bar{x} = \bar{1} \Rightarrow x \in H; \Rightarrow \ker(\alpha) \subseteq H; \Rightarrow H = \ker(\alpha)$. Recíprocamente, sea $\bar{x} \in \ker(\theta) \Rightarrow \theta(\bar{x}) = \alpha(x) = 1 \Rightarrow x \in \ker(\alpha) \Rightarrow x \in H \Rightarrow \bar{x} = \bar{1}$.

Puesto que $\alpha = \theta \circ j$, entonces como θ sobreyectivo, α lo es ya que j es el homomorfismo canónico.

Supóngase ahora que α es sobreyectivo, y sea $y \in G'$. Entonces, existe $x \in G$ tal que $\alpha(x) = y \Rightarrow \theta(\bar{x}) = \alpha(x) = y$, es decir, θ es sobreyectivo.

(ii) Es consecuencia directa del teorema. □

Las afirmaciones siguientes evidencian la utilidad del teorema de factorización.

Corolario 4.2.4. *Sea $\alpha : G \to K$ un homomorfismo sobreyectivo de grupos y sea $H \trianglelefteq G$. Entonces α induce el homomorfismo sobreyectivo*

$$\alpha' : G/H \to K/\alpha(H)$$

definido por $\alpha'(\bar{x}) := \overline{\alpha(x)}$, donde $\bar{x} = xH$ y $\overline{\alpha(x)} := \alpha(x)\alpha(H)$. Además, α' es inyectivo (y por lo tanto un isomorfismo) si, y sólo si,, $\ker(\alpha) \subseteq H$.

Corolario 4.2.5. *Sea $\alpha : G \to K$ un homomorfismo de grupos y sea H un subgrupo normal de K. Entonces α induce el homomorfismo inyectivo*

$$\alpha' : G/\alpha^{-1}(H) \to K/H$$

definido por $\alpha'(\tilde{x}) := \overline{\alpha(x)}$, $\tilde{x} = x\alpha^{-1}(H)$, $\overline{\alpha(x)} := \alpha(x)H$. Además, si α es sobreyectivo, entonces α' es un isomorfismo.

Corolario 4.2.6. *Sea G un grupo y sean H y K subgrupos normales de G tales que $H \subseteq K$. Entonces se tiene el homomorfismo sobreyectivo*

$$\theta : G/H \to G/K$$

definido por $\theta(\bar{x}) := \tilde{x}$, donde $\bar{x} := xH$ y $\tilde{x} := xK$.

4.3. Teorema de correspondencia

Sea G un grupo y H un subgrupo normal de G. Consideremos el grupo cociente G/H y el homomorfismo canónico $j : G \to G/H$. Sea X un subconjunto de G que contiene H, $H \subseteq X \subseteq G$. Según vimos, la imagen de X mediante j es

$$j(X) = \{j(x) \mid x \in X\} = \{\bar{x} \mid x \in X\}$$

Denotamos este conjunto por X/H. Sea ahora K un subgrupo de G que contiene H, $H \leq K \leq G$. Entonces

$$j(K) = \{j(x) \mid x \in K\} = \{\bar{x} \mid x \in K\} = K/H$$

Además, como $H \trianglelefteq K$ podemos construir el grupo cociente de K por H, K/H, y por tanto, la notación K/H para $j(K)$ es adecuada. Podemos ahora demostrar el siguiente teorema.

Teorema 4.3.1 (Teorema de correspondencia). *Sea G un grupo y sea H un subgrupo normal de G. Sea $L(G, H)$ la familia de subgrupos de G que contienen H*

$$L(G, H) := \{K \leq G | \, H \subseteq K\},$$

Sea $L(G/H)$ la familia de subgrupos de G/H. Entonces existe una correspondencia biyectiva entre $L(G, H)$ y $L(G/H)$

$$\varphi : L(G, H) \to L(G/H)$$
$$\varphi(K) := j(K) = K/H = \{\bar{x} \in G/H \, | \, x \in K\}$$

Además, si N es un subgrupo normal de G que contiene a H, entonces $\varphi(N) \trianglelefteq G/H$. Por último, si A y B son elementos de $L(G, H)$ tales que $A \leq B$, en otras palabras, si $H \leq A \leq B \leq G$, entonces $\varphi(A) \leq \varphi(B)$ y además $|B : A| = |\varphi(B) : \varphi(A)|$.

Demostración. Nótese en primer lugar que $\varphi(K)$ es realmente un subgrupo de G/H ya que j es un homomorfismo.

φ es una función inyectiva: supóngase que $\varphi(K_1) = \varphi(K_2) \Rightarrow K_1/H = K_2/H$. Sea $x \in K_1 \Rightarrow \bar{x} \in K_1/H \Rightarrow \bar{x} \in K_2/H \Rightarrow \bar{x} = \bar{y}$ para algún $y \in K_2 \Rightarrow x^{-1}y \in H \subseteq K_2 \Rightarrow x \in K_2$. En total $K_1 \subseteq K_2$. Análogamente se prueba que $K_2 \subseteq K_1$ y así $K_1 = K_2$ con lo cual φ es $1 - 1$.

φ es una función sobreyectiva: sea M un subgrupo de G/H, como hemos visto $j^{-1}(M)$ es un subgrupo de G. Veamos en primer lugar que $H \leq j^{-1}(M)$: sea $x \in H \Rightarrow j(x) = \bar{x} = \bar{0} \in M$. Así pues, $j^{-1}(M)$ es un elemento de $L(G, H)$. Finalmente, notemos que $j\left[j^{-1}(M)\right] = M$ por ser j una función sobre. Esto completa la prueba de que φ es una función sobre.

Si N es un subgrupo normal de G que contiene H, entonces según vimos la imagen de cada subgrupo normal mediante un homomorfismo es nuevamente un subgrupo normal en la imagen. Por tanto, $\varphi(N) = j(N) \trianglelefteq G/H$.

Sea ρ la relación de equivalencia inducida en B por el subgrupo A:

$$x, y \in B : x\rho y \Leftrightarrow xy^{-1} \in A.$$

Denotemos por $[x]$ la clase de equivalencia correspondiente al elemento $x \in B$ mediante la relación ρ. Sea θ la relación de equivalencia inducida en B/H por el subgrupo A/H:

$$\bar{x}, \bar{y} \in B/H : \bar{x}\theta\bar{y} \Leftrightarrow \bar{x}\ \bar{y}^{-1} \in A/H.$$

($\bar{x} = Hx$, $x \in B$). Denotemos por $[\bar{x}]$ la clase de equivalencia determinada por el elemento $\bar{x}$ de B/H mediante la relación θ.

Sean $C_1 = B/\rho$ y $C_2 = (B/H)/\theta$ los respectivos conjuntos cocientes. Se quiere probar que $Card(C_1) = Card(C_2)$: Definimos

$$F : C_1 \rightarrow C_2$$
$$F([x]) := [\overline{x}]$$

F está bien definida: $[x] = [y] \Rightarrow xy^{-1} \in A \Rightarrow \overline{xy^{-1}} \in A/H \Rightarrow \overline{x}\ \overline{y}^{\,-1} \in A/H \Rightarrow [\overline{x}] = [\overline{y}] \Rightarrow F([x]) = F([y])$.

F es inyectiva: $F([x]) = F([y]) \Rightarrow [\overline{x}] = [\overline{y}] \Rightarrow \overline{x}\ \overline{y}^{\,-1} \in A/H \Rightarrow xy^{-1} \in A \Rightarrow [x] = [y]$ F es obviamente sobreyectiva. □

4.4. Teoremas de isomorfismo

El primer teorema fundamental de isomorfismo combinado con el teorema de correspondencia permite determinar las imágenes homomorfas de $\mathbb{Z}_n$, $n \geq 2$.

Teorema 4.4.1 (Primer teorema fundamental de isomorfismo). *Sea G un grupo y sean H y K subgrupos normales de G tales que $H \leq K$. Entonces $K/H \trianglelefteq G/H$ y se tiene el isomorfismo*

$$(G/H)/(K/H) \cong G/K.$$

Demostración. Podemos aplicar el teorema de factorización y el teorema fundamental de homomorfismo para demostrar este importante teorema: en efecto el homomorfismo canónico $j : G \rightarrow G/K$ se puede factorizar a través del homomorfismo $j_1 : G \rightarrow G/H$ debido a que $H \subseteq K = \ker(j)$ Denotamos los elementos de G/H mediante $\bar{x} := xH$ y los de G/K por $\tilde{x} := xK$, entonces $\theta : G/H \rightarrow G/K$ está definido por $\theta(\bar{x}) := \tilde{x}$; puesto que j es sobreyectivo, entonces θ también lo es, y según el teorema fundamental de homomorfismo $(G/K) \cong (G/H)/\ker(\theta)$ pero $\ker(\theta) = \{\bar{x} \in G/H \mid \tilde{x} = \tilde{0}\} = \{\bar{x} \in G/H \mid x \in K\} = K/H$. Así pues, $(G/H)/(K/H) \cong G/K$. □

Teorema 4.4.2 (Segundo teorema fundamental de isomorfismo). *Sean G un grupo, $H \leq G$ y $K \trianglelefteq G$. Entonces,*

$$HK/K \cong H/H \cap K.$$

Demostración. En primer lugar $HK = KH$: sea $hk \in HK \Rightarrow hk = (hkh^{-1})h \in KH$ ya que $K \trianglelefteq G$; así pues, $HK \subseteq KH$. Sea ahora $kh \in KH$; entonces $kh = h(h^{-1}kh) \in HK \Rightarrow KH \subseteq HK$ y en consecuencia $HK = KH$. Esto garantiza que HK es un subgrupo de G. Como $K \trianglelefteq G$ entonces $K \trianglelefteq HK$ y tiene sentido el grupo factor HK/K. Definimos la función

$$\begin{aligned} f : H &\to HK/K \\ h &\mapsto hK \end{aligned}$$

Probemos que f es un homomorfismo sobreyectivo con núcleo $\ker(f) = H \cap K$: $f(h_1h_2) = (h_1h_2)K = h_1Kh_2K = f(h_1)f(h_2)$. Sea $x \in HK/K$. Entonces x es de la forma $x = hkK = hK = f(h)$. Esto prueba que f es sobre. Sea $x \in \ker(f) \Rightarrow f(x) = xK = 1K \Rightarrow x \in K \Rightarrow x \in H \cap K \Rightarrow \ker(f) = H \cap K$ y el teorema está demostrado. □

Ejemplo 4.4.3. (i) Calculemos las imágenes homomorfas de $\mathbb{Z}_n$, $n \geq 0$. Para $n = 0$, $\mathbb{Z}_0 = \mathbb{Z}$, según vimos, en este caso las imágenes homomorfas son de la forma $\mathbb{Z}_n$, $n \geq 0$. Sea $n = 1$, $\mathbb{Z}_1 = 0$, grupo con un solo elemento. Por tanto, las únicas imágenes homomorfas de $\mathbb{Z}_1$ son los grupos unitarios. Sea $n \geq 2$, $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$. Las imágenes homomorfas de $\mathbb{Z}_n$ según el teorema fundamental de homomorfismo son de la forma $\mathbb{Z}_n/H$ donde H es subgrupo normal de $\mathbb{Z}_n$. Como $\mathbb{Z}_n$ es un grupo abeliano entonces todos sus subgrupos son normales. Según el teorema de correspondencia los subgrupos de $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ son de la forma $K/\langle n\rangle$ donde K es un subgrupo de $\mathbb{Z}$ que contiene al subgrupo $\langle n\rangle$. Los subgrupos de $\mathbb{Z}$ son de la forma $\langle m\rangle$. Así pues, los subgrupos de $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ son de la forma $\langle m\rangle / \langle n\rangle$ donde $\langle m\rangle \supseteq \langle n\rangle$. Nótese que si $\langle n\rangle \subseteq \langle m\rangle$ entonces $n = km$, $k \in \mathbb{Z}$, $\Rightarrow m|n$. Recíprocamente, si $m|n \Rightarrow \langle n\rangle \subseteq \langle m\rangle$. En conclusión los subgrupos de $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ son de la forma $\langle m\rangle / \langle n\rangle$ con $m|n$. Por tanto las imágenes homomorfas de $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ son de la forma $\mathbb{Z}/\langle n\rangle / \langle m\rangle / \langle n\rangle \cong \mathbb{Z}/\langle m\rangle = \mathbb{Z}_m$. Así pues, las imágenes homomorfas de $\mathbb{Z}_n$ son los subgrupos $\mathbb{Z}_m$ con $m|n$. Por ejemplo, las imágenes homomorfas de $\mathbb{Z}_{12}$ son : $\mathbb{Z}_1 = 0$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_{12}$.

(ii) Sea G un grupo no unitario y sea $H \trianglelefteq G$. Se dice que H es un subgrupo ***normal maximal*** de G si se cumple que

$$H \leq K \text{ y } K \trianglelefteq G \Leftrightarrow K = H \text{ o } K = G,$$

en otras palabras, los únicos subgrupos normales de G que contienen H son G y H. Sea $\langle G, \cdot, 1\rangle$ un grupo simple, es decir, G es no trivial y los únicos subgrupos normales de G son los triviales: $\{1\}$ y G. Probemos que $H \trianglelefteq G$ es maximal si, y sólo si, G/H es simple: sea W un subgrupo normal de G/H, según el teorema de correspondencia existe en G un subgrupo normal K que contiene H. Por ser H normal maximal $K = H$ o $K = G$, es decir $W = K/H = H/H$ o $W = G/H$, es

decir, los únicos subgrupos normales de G/H son los triviales. Sea ahora $K \leq G$, $K \trianglelefteq G$, $H \leq K$. Entonces según el teorema de correspondencia $K/H \trianglelefteq G/H$; como este último es simple entonces $K/H = \{1\}$ o $K/H = G/H \Rightarrow K/H = H/H$ o $K/H = G/H \Rightarrow K = H$ o $K = G$ con lo cual H es maximal normal.

(iii) Calculemos las imágenes homomóficas del ***grupo de Klein***

$$V = \{1, a, b, ab\}, a^2 = 1, b^2 = 1, ab = ba.$$

V es un grupo de orden 4. Por tanto, sus subgrupos son de órdenes 1,2,4. Subgrupo de orden 1 : $H_1 = \{1\}$. Los subgrupos de orden 2 son necesariamente cíclicos: $H_2 = \langle a \rangle = \{1, a\}$, $K_2 = \langle b \rangle = \{1, b\}$, $L_2 = \langle ab \rangle = \{1, ab\}$. Así pues, los subgrupos de orden 2 son $H_2 = \langle a \rangle$, $K_2 = \langle b \rangle$, $L_2 = \langle ab \rangle$. Hay un único subgrupo de orden 4: V. De lo anterior obtenemos que todos los subgrupos de V son normales. Así, las imágenes homomorfas de V son : $V/H_1 \cong V$, $V/H_2 \cong V/K_2 \cong V/L_2 \cong \mathbb{Z}_2$, $V/V = 1$.

(iv) Notemos que V es un grupo abeliano de orden 4 al igual que $\mathbb{Z}_4$. Sin embargo, V no es isomorfo a $\mathbb{Z}_4$ ya que este último es cíclico. Tenemos pues dos grupos distintos de orden 4. Nos preguntamos si existen otros grupos de orden 4 diferentes (no isomorfos) a $\mathbb{Z}_4$ y V. La respuesta es no: como V es de orden 4, V es necesariamente abeliano. En efecto, probemos que si G es un grupo de orden ≤ 5 entonces G es abeliano: $|G| = 1 \Rightarrow G$ es un grupo unitario y por ende abeliano

$|G| = 2 \Rightarrow G$ es un grupo cíclico $\Rightarrow G \cong \mathbb{Z}_2 \Rightarrow G$ es abeliano

$|G| = 3 \Rightarrow G$ es un grupo cíclico $\Rightarrow G \cong \mathbb{Z}_3 \Rightarrow G$ es abeliano

$|G| = 4$, si G es cíclico $\Rightarrow G \cong \mathbb{Z}_4 \Rightarrow G$ es abeliano

$|G| = 5 \Rightarrow G$ es un grupo cíclico $\Rightarrow G \cong \mathbb{Z}_5 \Rightarrow G$ es abeliano.

Volvemos al caso $|G| = 4$ y G no es cíclico. Entonces cada elemento de G es de orden 1 o 2 (no hay elementos de orden 4 ya que de lo contrario G sería cíclico). De esto concluimos que $G = \{1, a, b, ab\}$, $a^2 = 1$, $b^2 = 1$, $ab = ba$, es decir, G es el grupo de Klein.

(v) Determinemos la imágenes homomorfas de D_4 : recordemos que $D_4 = \{1, f, f^2$ $f^3, g, fg, f^2g, f^3g\}$. La tabla de D_4 ayuda a determinar los subgrupos de D_4 (véase el capítulo 3). 1 es el único subgrupo de orden 1. Los subgrupos de orden 2 son los determinados por las permutaciones de orden 2:

$$\langle g \rangle, \langle f^2 \rangle, \langle fg \rangle, \langle f^2g \rangle, \langle f^3g \rangle \text{ son los subgrupos de orden 2.}$$

Los subgrupos de orden 4 son de dos tipos: unos isomorfos a $\mathbb{Z}_4$ y otros isomorfos al grupo de Klein, V: elementos de orden 4 : f, f^3. Pero $\langle f \rangle = \langle f^3 \rangle \cong \mathbb{Z}_4$. Subgrupos isomorfos a $V = \{1, a, b, ab\}$, $a^2 = 1$, $b^2 = 1$, $ab = ba$. a puede tomar los valores f^2, g, fg, f^2g, f^3g; lo mismo ocurre para b. Se presentan entonces $\frac{5 \cdot 4}{2} = 10$ combinaciones posibles :

1) $a = f^2$, $b = g \rightarrow K_4 = \{1, f^2, g, f^2g\}$

2) $a = f^2$, $b = fg \rightarrow H_4 = \{1, f^2, fg, f^3g\}$

3) $a = f^2,\ b = f^2g \to K_4$
4) $a = f^2,\ b = f^3g \to H_4$
5) $a = g,\ b = fg \to$ Descartado ya que $g(fg) \neq (fg)g$
6) $a = g,\ b = f^2g \to K_4$
7) $a = g,\ b = f^3g \to$Descartado ya que $g(f^3g) \neq (f^3g)g$
8) $a = fg,\ b = f^2g \to$ Descartado ya que $(fg)(f^2g) \neq (f^2g)(fg)$
9) $a = fg,\ b = f^3g \to H_4$
10) $a = f^2g,\ b = f^3g \to$ Descartado ya que $(f^2g)(f^3g) \neq (f^3g)(f^2g)$
Subgrupos de orden 4: Isomorfos a $\mathbb{Z}_4$: $\langle f\rangle$, isomorfos a V : K_4, H_4.
Único subgrupo de orden 8 : D_4
En resumen se obtiene lo siguiente: $\langle f\rangle \cong \mathbb{Z}_4$
$K_4 \cong H_4 \cong V$
$\langle g\rangle \cong \langle f^2g\rangle \cong \langle f^2\rangle \cong \langle f^3g\rangle \cong \langle fg\rangle \cong \mathbb{Z}_2$
De otra parte, 1 y D_4 son automáticamente subgrupos normales de D_4.
Además, K_4, H_4 y $\langle f\rangle$ son también normales ya que su índice en D_4 es 2.
$\langle g\rangle$ no es subgrupo normal de D_4 ya que $f^{-1}gf = f^3gf = f^2g \notin \langle g\rangle$
$\langle fg\rangle$ no es subgrupo normal de D_4 ya que $g^{-1}(fg)g = f^3g \notin \langle fg\rangle$
$\langle f^2g\rangle$ no es subgrupo normal de D_4 ya que $f^{-1}(f^2g)f = g \notin \langle f^2g\rangle$
$\langle f^3g\rangle$ no es subgrupo normal de D_4 ya que $f^{-1}(f^3g)f = fg \notin \langle f^3g\rangle$
$\langle f^2\rangle \trianglelefteq D_4$ ya que $f^{-1}f^2f = f^2$; $(f^2)^{-1}f^2f^2 = f^2$; $(f^3)^{-1}f^2f^3 = f^2$; $g^{-1}f^2g = f^2$; $(fg)^{-1}f^2(fg) = f^2$; $(f^2g)^{-1}f^2(f^2g) = f^2$; $(f^3g)^{-1}f^2(f^3g) = f^2$.
Subgrupos normales de D_4 : 1, D_4, $\langle f^2\rangle$, $\langle f\rangle$, K_4, H_4
Las imágenes homomorfas de D_4 (salvo isomorfismo) son :
$D_4/1 = D_4$; $D_4/\langle f\rangle = \mathbb{Z}_2$; $D_4/K_4 \cong D_4/H_4 \cong \mathbb{Z}_2$; $D_4/D_4 = 1$.
Para $\langle f^2\rangle$ se tiene que $D_4/\langle f^2\rangle \cong \mathbb{Z}_4$ o $D_4/\langle f^2\rangle \cong V$.
La primera posibilidad es descartada ya que en $D_4/\langle f^2\rangle$ no hay elementos de orden 4: en efecto, en D_4 todos los elementos salvo 1, f^2, f^3 son de orden 2.
Además, para estos últimos se tiene que $|\bar{1}| = 1, \left|\bar{f}\right| = 2, \left|\overline{f^3}\right| = 2$. Por tanto, $D_4/\langle f^2\rangle \cong V$, esta es la otra imagen homomorfa de D_4.

(vi) Calculemos las imágenes homomorfas del grupo de los ***cuaterniones de Hamilton*** Q_8: el grupo Q_8 es de orden 8 y puede ser definido por las siguientes relaciones:

$$Q_8 = \langle a, b \mid a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1}\rangle,$$
$$Q_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

La tabla para Q_8 viene dada por

$\circ$	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	1	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	1
a^2b	a^2b	ab	b	a^3b	1	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	1	a^3	a^2

$ba = a^{-1}b = a^3b$; $ba^2 = (ba)a = (a^3b)a = a^3(ba) = a^3(a^3b) = a^2b$; etc

Subgrupos de Q_8 : los subgrupos de Q_8 tienen orden 1, 2, 4, 8 :

Subgrupo de orden 1 : 1

Subgrupo de orden 8 : Q_8

Subgrupos de orden 2 : cíclicos y están generados por los elementos de orden 2 : $\langle a^2\rangle$ es el único subgrupo de orden 2

Subgrupos de orden 4 :

cíclicos : $\langle a\rangle = \langle a^3\rangle$; $\langle b\rangle = \langle a^2b\rangle$, $\langle ab\rangle = \langle a^3b\rangle$

No cíclicos : son de la forma $V = \{1, x, y, xy\}$, donde $x^2 = y^2 = 1$, $xy = yx$. Pero en Q_8 sólo hay un elemento de orden 2. Por tanto, Q_8 no tiene subgrupos de orden 4 no cíclicos.

Subgrupos normales :

Los subgrupos normales 1 y Q_8 son normales. Los subgrupos de orden 4 $\langle a\rangle$, $\langle b\rangle, \langle ab\rangle$ son también normales por ser de índice 2.

$\langle a^2\rangle = \{a^2, 1\} : 1a^21^{-1} = a^2; aa^2a^{-1} = aa^2a^3 = a^2; a^2a^2a^2 = a^2; a^3a^2(a^3)^{-1} = a^3a^2a = a^2; ba^2b^{-1} = a^2;\ aba^2(ab)^{-1} = a^2; a^2ba^2(a^2b)^{-1}) = a^2; a^3ba^2(a^3b)^{-1} = a^2; \Rightarrow \langle a^2\rangle \trianglelefteq Q_8$. Así pues, en Q_8 todos sus subgrupos son normales.

Imágenes homomorfas :

$Q_8/1 \cong Q_8$; $Q_8/\langle a\rangle \cong Q_8/\langle b\rangle \cong Q_8/\langle ab\rangle \cong \mathbb{Z}_2$; $Q_8/Q_8 \cong \mathbb{Z}_1$; $Q_8/\langle a^2\rangle \cong V$ ya que en $Q_8/\langle a^2\rangle$ no hay elementos de orden 4 :

$|\bar{1}| = 1$, $|\overline{a}| = 2 : \overline{a}^{\,2} = \overline{a^2} = \bar{1}$.

$\left|\overline{a^2}\right| = 1$, $\left|\overline{a^3}\right| = 2 : (\overline{a^3})^{\,2} = \overline{a^6} = \overline{a^2} = \bar{1}$,

$\left|\overline{b}\right| = 2 : \overline{b}^{\,2} = \overline{b^2} = \overline{a^2} = \bar{1}$

$\left|\overline{ab}\right| = 2 : \overline{ab}^{\,2} = \overline{(ab)^2} = \overline{a^2} = \bar{1}$; $\left|\overline{a^2b}\right| = 2 : (\overline{a^2b})^{\,2} = \overline{(a^2b)^2} = \bar{1}$;

$\left|\overline{a^3b}\right| = 2 : (\overline{a^3b})^{\,2} = \overline{(a^3b)^2} = \overline{a^2} = \bar{1}$.

Matricialmente Q_8 se puede interpretar como

$Q_8 = \langle A, B\rangle$,

$$A = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},\ B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix},$$

$i \in C, i^2 = -1,\ \ A^4 = E, B^2 = A^2, BAB^{-1} = A^{-1}$.

Nótese que Q_8 y D_4 no son isomorfos, ya que en Q_8 hay 6 elementos diferentes de orden 4 : $a, a^3, b, a^2b,\ ab, a^3b$, en cambio en D_4 sólo hay 2 : f, f^3. Otra forma de explicar esto es que en Q_8 todos sus sugrupos son normales, en cambio en D_4 el subgrupo $\langle g \rangle$ no es normal.

Centro de Q_8: $a \notin Z(Q_8)$ ya que $ab \neq ba \Rightarrow \langle a \rangle \neq Z(Q_8); b \notin Z(Q_8) \Rightarrow Z(Q_8) \neq \langle b \rangle$; $ab \notin Z(Q_8)$ ya que $(ab)a \neq a(ab) \Rightarrow Z(Q_8) \neq \langle ab \rangle$. Según lo anterior $Z(Q_8) \neq Q_8$. Nótese que, $Z(Q_8) = \langle a^2 \rangle \cong \mathbb{Z}_2$.

4.5. Ejercicios

1. Calcule las imágenes homomorfas del grupo $GL_2(\mathbb{R})$.
2. ¿Cuántos homomorfismos no triviales hay de D_4 en $\mathbb{Z}_p$?, donde p es primo.
3. ¿ Cuántos homomorfismos no triviales hay de Q_8 en $\mathbb{Z}_p$?, donde p es primo.

Capítulo 5

Automorfismos

Los homomorfismos biyectivos de un grupo G en si mismo se conocen como los automorfismos de G. Estas funciones conforman un grupo que tiene información importante relativa al grupo G.

5.1. Automorfismos interiores

Estudiamos en esta sección la relación entre los automorfismos de un grupo, sus automorfismos interiores y su centro. Recordemos que si G es un grupo, su centro simbolizado por $Z(G)$ y es un subgrupo normal de G el cual está definido por

$$Z(G) = \{x \in G \mid xa = ax \text{ para cada } a \in G\}.$$

Notemos que G es abeliano si, y sólo si,, $G = Z(G)$.

Antes de demostrar el primer resultado importante de esta lección definamos los automorfismos y en particular los automorfismos interiores de un grupo.

Definición 5.1.1. *Sea $(G, \ . \ , 1)$ un grupo, un **automorfismo** de G es un homomorfismo biyectivo de G en si mismo. Sea $x \in G$; la función definida por*

$$f_x : G :\to G$$

$$a \longmapsto x^{-1}ax$$

*es un automorfismo de G y se denomina **automorfismo interior** de G determinado por x.*

Teorema 5.1.2. *Sea $(G, \ . \ , 1)$ un grupo, $Aut(G)$ su colección de automorfismos y sea $Int\,(G)$ el conjunto de automorfismos interiores de G. Entonces,*

(i) *$Aut(G)$ es un subgrupo del grupo $S(G)$ de funciones biyectivas de G en G.*

(ii) $Int\,(G) \trianglelefteq Aut\,(G)$.

Demostración. (i) La primera afirmación es evidente.

(ii) $Int\,(G) \leq Aut\,(G)$: $Int\,(G) \neq \emptyset$ ya que $i_G = f_1 \in Int\,(G)$. Sean $x, y \in G$. Entonces $f_x \circ f_y = f_{yx}$, $f_x^{-1} = f_{x^{-1}}$.

$Int\,(G) \trianglelefteq Aut\,(G)$: sea $x \in G$, $h : G \to G$ un automorfismo cualquiera de G. Entonces para cada $a \in G$,

$$h^{-1}f_x h(a) = h^{-1}(f_x(h(a))) = h^{-1}(x^{-1}h(a)x) = h^{-1}(x^{-1})ah^{-1}(x) =$$
$$(h^{-1}(x))^{-1}ah^{-1}(x) = f_{h^{-1}(x)}(a), \text{ es decir, } h^{-1}f_x h = f_{h^{-1}(x)} \in Int\,(G).$$

□

Teorema 5.1.3. *Sea G un grupo cualquiera. Entonces*

$$G/Z\,(G) \cong Int\,(G).$$

Demostración. Consideremos la función

$$\varphi : G \to Int\,(G)$$
$$x \mapsto f_{x^{-1}}$$

φ es un homomorfismo: $\varphi(xy) = f_{(xy)^{-1}} = f_{y^{-1}x^{-1}} = f_{x^{-1}} \circ f_{y^{-1}} = \varphi(x) \circ \varphi(y)$. φ es evidentemente sobre. Por último, veamos que $\ker(\varphi) = Z\,(G)$: sea $x \in \ker(\varphi) \Rightarrow f_{x^{-1}} = i_G \Rightarrow xax^{-1} = a$ para cada $a \in G \Rightarrow x \in Z\,(G)$, y recíprocamente si $x \in Z\,(G)$ entonces $x \in \ker(\varphi)$. Por el teorema fundamental de homomorfismo se tiene que $G/Z\,(G) \cong Int\,(G)$. □

Corolario 5.1.4. *G es abeliano $\Leftrightarrow Int\,(G) = \{i_G\}$.*

5.2. Teorema de Cayley

La importancia del teorema de Cayley radica en parte en que determina la cota superior $\binom{n!}{n}$ para el número de grupos finitos no isomorfos de orden n.

Teorema 5.2.1. *Sea G un grupo y sea $S\,(G)$ el grupo de permutaciones del conjunto G. Entonces G es isomorfo a un subgrupo de $S\,(G)$.*

Demostración. Considérese la función

$$\Psi : G \to S(G)$$

definida por $\Psi(x) := \varrho_x$, $\varrho_x : G \to G$, $\varrho_x(a) := xa$. $\varrho_x \in S(G)$ para cada $x \in G$: $\varrho_x(a) = \varrho_x(b) \Rightarrow xa = xb$, es decir, ϱ_x es $1-1$; sea $y \in G$ entonces $y = \varrho_x(x^{-1}y)$. Ψ es un homomorfismo: $\Psi(xy) = \varrho_{xy}$, $\varrho_{xy}(a) = xya = \varrho_x(\varrho_y(a)) \Rightarrow \varrho_{xy} = \varrho_x \cdot \varrho_y = \Psi(x)\Psi(y)$. Ψ es inyectiva : $\Psi(x) = \Psi(y) \Rightarrow x1 = y1 \Rightarrow x = y$. □

Corolario 5.2.2. *Sea $n \geq 1$. Existen a lo sumo $\binom{n!}{n}$ grupos no isomórficos de orden n.*

Demostración. Sea G un grupo finito de orden n. Entonces G es isomorfo a un subgrupo de S_n. Pero S_n tiene un número finito de subgrupos de orden n, este número es menor que $\binom{n!}{n}$. Nótese que el problema de determinar todos los grupos no isomorfos de orden n se reduciría a determinar todos los subgrupos no isomorfos de S_n con n elementos. □

5.3. Ejemplos

Ejemplo 5.3.1. Automorfismos de grupos cíclicos: (i) Grupo cíclico infinito $\mathbb{Z}$: sea $f \in Aut(\mathbb{Z})$. Como f es un automorfismo, la imagen de cada generador de $\mathbb{Z}$ es nuevamente un generador de $\mathbb{Z}$, más generalmente, si G es un grupo cíclico con generador a y $f \in Aut\,(G)$ entonces $f\,(a)$ es un generador de G. En efecto, dado $x \in G$ existe $y \in G$ tal que $x = f(y) \Rightarrow x = f(a^t) = f(a)^t$.

Puesto que $\mathbb{Z}$ tiene sólo dos generadores entonces se presentan dos posibilidades para f, $f(1) = 1$ ó $f(1) = -1$,

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\quad f \quad} & \mathbb{Z} \\ 1 & \longrightarrow & 1 \\ k & \longrightarrow & k \end{array} \qquad\qquad \begin{array}{ccc} \mathbb{Z} & \xrightarrow{\quad f \quad} & \mathbb{Z} \\ 1 & \longrightarrow & -1 \\ k & \longrightarrow & \text{-}k \end{array}$$

Luego, $\Rightarrow Aut(\mathbb{Z}) \cong \mathbb{Z}_2$.

(ii) Grupo cíclico finito de orden n, $\mathbb{Z}_n$: recordemos que el grupo $\mathbb{Z}_n$ se obtuvo a partir de $\mathbb{Z}$ por medio de una relación de equivalencia

$$a \equiv b \Leftrightarrow m|(a-b), \qquad a, b \in \mathbb{Z}.$$

En otras palabras $\mathbb{Z}_n$ es el grupo cociente $\mathbb{Z}/\langle n\rangle$. En $\mathbb{Z}_n$ se puede definir un producto y convertirlo así en un semigrupo multiplicativo:

$$\overline{r}\ \overline{s} = \overline{rs} \qquad \text{para} \qquad 0 \leq r, s < n.$$

Es sencillo verificar que el producto está correctamente definido. Además, este producto es asociativo con elemento neutro $\overline{1}$, luego se tiene el monoide $\left(\mathbb{Z}_n, ., \overline{1}\right)$. Asociado a todo monoide se tiene su grupo de elementos invertibles $\mathbf{Z}_n^*$. Nótese que

$$\mathbb{Z}_n^* = \{\overline{r}|\,(r,n) = 1, 1 \leq r < n\}$$

En efecto,

$$\overline{r} \in \mathbb{Z}_n^* \Leftrightarrow \exists \overline{s} \in \mathbb{Z}_n \text{ tal que } \overline{r}\ \overline{s} = \overline{1} \Leftrightarrow \overline{rs} = \overline{1} \Leftrightarrow n|\,(rs-1) \Leftrightarrow rs - 1 = nk \text{ con } k \in \mathbb{Z} \Leftrightarrow (r,n) = 1.$$

Con la observación anterior queremos probar que $Aut(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.

Sea $h : \mathbb{Z}_n \to \mathbb{Z}_n$ un automorfismo de $\mathbb{Z}_n$. Como $\overline{1}$ genera a $\mathbb{Z}_n$ entonces $h(\overline{1})$ es un generador de $\mathbb{Z}_n$. Así pues, tenemos tantos automorfismos como generadores tiene $\mathbb{Z}_n$. Pero nótese que $\overline{r}$ genera $\mathbb{Z}_n$ si, y sólo si,, $(r, n) = 1$. Podemos entonces definir

$$\begin{array}{rccc} \theta : & Aut\left(\mathbb{Z}_n\right) & \to & \mathbb{Z}_n^* \\ & h & \longmapsto & \theta\left(h\right) = \overline{r} \end{array}$$

donde $\overline{r} = h\left(\overline{1}\right)$.

θ es un homomorfismo: sean f y h automorfismos de $\mathbb{Z}_n$ tales que $f\left(\overline{1}\right) = \overline{r}$, $h\left(\overline{1}\right) = \overline{s}$. Nótese que $\theta\left(h \circ f\right) = \left(h \circ f\right)\left(\overline{1}\right) = h\left(f\left(\overline{1}\right)\right) = h\left(\overline{r}\right) = h\left(r\overline{1}\right) = rh\left(\overline{1}\right)$ $= r\overline{s} = rs\overline{1} = \overline{rs} = \overline{sr} = \overline{sr} = \theta\left(h\right) \circ \theta\left(f\right)$.

θ es inyectiva: sea $h \in Aut\left(\mathbb{Z}_n\right)$ con $\theta\left(h\right) = \overline{1} \Rightarrow h\left(\overline{1}\right) = \overline{1} \Rightarrow h\left(\overline{r}\right) = \overline{r}$ pra cada $0 \leq r < n \Rightarrow h = i_{\mathbb{Z}_n}$.

θ es sobre: sea $\overline{r} \in \mathbb{Z}_n^*$ y sea h definido por $h\left(\overline{s}\right) := \overline{sr}$. Nótese que $h\left(\overline{1}\right) = \overline{r}$ y además $h \in Aut\left(\mathbb{Z}_n\right)$, con lo cual $\theta\left(h\right) = \overline{r}$.

Ejemplo 5.3.2. El grupo de automorfismos de un grupo finito es finito:

Sea G un grupo de orden n. Nótese que $Aut\left(G\right) \leq S\left(G\right) \cong S_n \Rightarrow \left|Aut\left(G\right)\right| \mid \left|S_n\right| = n!$. Más exactamente, $\left|Aut\left(G\right)\right| \mid (n-1)!$ ya que para cada $f \in Aut\left(G\right), f\left(1\right) = 1$.

Ejemplo 5.3.3. El grupo de automorfismos de un grupo conmutativo puede ser no conmutativo: Consideremos el grupo de Klein: $V = \left\{1, a, b, ab\right\}, a^2 = 1, b^2 = 1, ab = ba$. Según el ejemplo anterior $\left|Aut\left(V\right)\right| = 1, 2, 3, 6$.

Fácilmente se comprueba que las siguientes funciones son automorfismos de V y además diferentes:

$$\begin{array}{rr} i_G : \left(\begin{smallmatrix} 1 & a & b & ab \\ 1 & a & b & ab \end{smallmatrix}\right), & f = \left(\begin{smallmatrix} 1 & a & b & ab \\ 1 & b & ab & a \end{smallmatrix}\right) \\ g : \left(\begin{smallmatrix} 1 & a & b & ab \\ 1 & a & ab & b \end{smallmatrix}\right), & f^2 = \left(\begin{smallmatrix} 1 & a & b & ab \\ 1 & ab & a & b \end{smallmatrix}\right) \\ fg = \left(\begin{smallmatrix} 1 & a & b & ab \\ 1 & b & a & ab \end{smallmatrix}\right), & f^2 g = \left(\begin{smallmatrix} 1 & a & b & ab \\ 1 & ab & b & a \end{smallmatrix}\right). \end{array}$$

Entonces, $Aut\left(V\right) \cong S_3$.

Ejemplo 5.3.4. Dos grupos no isomorfos pueden tener grupos de automorfismos isomorfos: $Aut\left(\mathbb{Z}_3\right) \cong \mathbb{Z}_2 \cong Aut\left(\mathbb{Z}\right)$.

Ejemplo 5.3.5. $Aut\left(D_4\right)$: en el capítulo 6 estudiaremos los automorfismos del grupo dihédrico D_n. Según se verá allá $\left|D_4\right| = 4\varphi\left(4\right) = 8$; $Int\left(D_4\right) \cong V$ y además $Aut\left(D_4\right) \cong D_4$. Explícitamente los automorfismos de D_4 son:

$$
\begin{array}{rccc}
T_{1,0}: & D_4 & \to & D_4 \\
 & f^\alpha g^\beta & \to & f^\alpha (f^0 g)^\beta = f^\alpha g^\beta \\
 & T_{1,0} = i_{D_4} & & \\
T_{1,1}: & D_4 & \to & D_4 \\
 & f^\alpha g^\beta & \to & f^\alpha (fg)^\beta \\
T_{1,1} = & \begin{pmatrix} 1 & f & f^2 & f^3 & g & fg & f^2g & f^3g \\ 1 & f & f^2 & f^3 & fg & f^2g & f^3g & g \end{pmatrix} & & \\
T_{1,2}: & D_4 & \to & D_4 \\
 & f^\alpha g^\beta & \to & f^\alpha (f^2 g)^\beta \\
T_{1,2} = & \begin{pmatrix} 1 & f & f^2 & f^3 & g & fg & f^2g & f^3g \\ 1 & f & f^2 & f^3 & f^2g & f^3g & g & fg \end{pmatrix} & & \\
T_{1,3}: & D_4 & \to & D_4 \\
 & f^\alpha g^\beta & \to & f^\alpha (f^3 g)^\beta \\
T_{1,3} = & \begin{pmatrix} 1 & f & f^2 & f^3 & g & fg & f^2g & f^3g \\ 1 & f & f^2 & f^3 & f^3y & g & fg & f^2g \end{pmatrix} & & \\
T_{3,0}: & D_4 & \to & D_4 \\
 & f^\alpha g^\beta & \to & (f^3)^\alpha (f^0 g)^\beta \\
T_{3,0} = & \begin{pmatrix} 1 & f & f^2 & f^3 & g & fg & f^2g & f^3g \\ 1 & f^3 & f^2 & f & g & f^3g & f^2g & fg \end{pmatrix} & & \\
T_{3,1}: & D_4 & \to & D_4 \\
 & f^\alpha g^\beta & \to & (f^3)^\alpha (fg)^\beta \\
T_{3,1} = & \begin{pmatrix} 1 & f & f^2 & f^3 & g & fg & f^2g & f^3g \\ 1 & f^3 & f^2 & f & fg & g & f^3g & f^2g \end{pmatrix} & & \\
T_{3,2}: & D_4 & \to & D_4 \\
 & f^\alpha g^\beta & \to & (f^3)^\alpha (f^2 g)^\beta \\
T_{3,2} = & \begin{pmatrix} 1 & f & f^2 & f^3 & g & fg & f^2g & f^3g \\ 1 & f^3 & f^2 & f & f^2g & fg & g & f^3g \end{pmatrix} & & \\
T_{3,3}: & D_4 & \to & D_4 \\
 & f^\alpha g^\beta & \to & (f^3)^\alpha (f^3 g)^\beta \\
T_{3,3} = & \begin{pmatrix} 1 & f & f^2 & f^3 & g & fg & f^2g & f^3g \\ 1 & f^3 & f^2 & f & f^3g & f^2g & fg & g \end{pmatrix} & &
\end{array}
$$

Ejemplo 5.3.6. $Aut(\mathbb{Q})$: sea $f \in Aut(\mathbb{Q})$ y sea $\frac{p_o}{q_o} = f(1), (p_o, q_o) = 1$. Entonces $f(p/q) = pf(1/q) \Rightarrow qf(p/q) = pf(1) \Rightarrow f(p/q) = \frac{p}{q} f(1)$. Lo anterior permite establecer la función

$$
\begin{array}{rccc}
\tau: & Aut(\mathbb{Q}) & \to & \mathbb{Q}^* \\
 & f & \to & f(1).
\end{array}
$$

$f(1) \neq 0$ ya que f es $1-1$. τ es un homomorfismo de grupos:

$\tau(f \circ g) = (f \circ g)(1) = f[g(1)] = f\left(\frac{p_1}{q_1}\right)$, donde $g(1) = \frac{p_1}{q_1}$. Sea $f(1) = \frac{p_o}{q_o}$, entonces $f\left(\frac{p_1}{q_1}\right) = \frac{p_1}{q_1} f(1) \Rightarrow \tau(f \circ g) = \tau(f)\tau(g)$.

τ es $1-1$: $f(1) = g(1) \Rightarrow f(p/q) = \frac{p}{q} f(1) = \frac{p}{q} g(1) = g\left(\frac{p}{q}\right) \Rightarrow f = g$.

τ es sobre: sea $\dfrac{p_o}{q_o} \neq 0$ un racional. Definimos

$$\begin{array}{rccc} f: & \mathbb{Q} & \to & \mathbb{Q} \\ & \dfrac{p}{q} & \to & \dfrac{p}{q}\dfrac{p_o}{q_o}. \end{array}$$

Nótese que $f(1) = \dfrac{p_o}{q_o}$, es decir, $\tau(f) = \dfrac{p_o}{q_o}$. Veamos que $f \in Aut(\mathbb{Q})$:

$$\begin{aligned} f\left(\frac{p}{q} + \frac{r}{s}\right) &= f\left(\frac{ps+qr}{qs}\right) = \left(\frac{ps+qr}{qs}\right)\frac{p_o}{q_o} \\ &= \frac{p}{q}\frac{p_o}{q_o} + \frac{r}{s}\frac{p_o}{q_o} = f\left(\frac{p}{q}\right) + f\left(\frac{r}{s}\right); \end{aligned}$$

si $f\left(\dfrac{p}{q}\right) = 0$ entonces $\dfrac{p}{q}\dfrac{p_o}{q_o} = 0 \Rightarrow p = 0 \Rightarrow \dfrac{p}{q} = 0$.

Sea $\dfrac{r}{s} \in \mathbb{Q}$; entonces $f\left(\dfrac{r}{s}\dfrac{q_o}{p_o}\right) = \dfrac{r}{s}$, es decir, f es sobre $\Rightarrow Aut\,(\mathbb{Q}) \cong \mathbb{Q}^*$.

5.4. Ejercicios

1. Calcule $Aut\,(S_3)$.

2. Calcule $Aut\,(Q_8)$.

   Solución. Sea $F : Q_8 \to Q_8$ un automorfismo de Q_8. Puesto que en $Q_8 = \langle a, b \mid a^4 = 1, b^2 = a^2, ba = a^{-1}b\rangle$ el único elemento de orden 2 es a^2, entonces $F(a^2) = a^2$, además, $F(1) = 1$, luego F realmente permuta los 6 elementos restantes, a saber: $a, a^3, b, ab, a^2b, a^3b$. Esto parece mostrar una relación de $Aut(Q_8)$ con el grupo de permutaciones S_4. En realidad se verá que $Aut\,(Q_8) \cong S_4$. Cada F viene determinado por su acción sobre los generadores a, b. Puesto que tanto a como b son de orden 4, entonces $F(a) = a, a^3, b, ab, a^2b, a^3b$ y $F(b) = a, a^3, b, ab, a^2b, a^3b$. Esto genera 36 posibilidades, de las cuales sólo 24 corresponden a funciones biyectivas:

$F(a) = a$	$F(b) = a$	Descartada ya que F debe ser biyectiva
$F(a) = a$	$F(b) = a^3$	Descartada ya que entonces $F(a^3) = a^3$
$F_1(a) = a$	$F_1(b) = b$	$\Rightarrow F_1(a^3) = a^3, F_1(ab) = ab, F_1(a^2b) = a^2b, F_1(a^3b) = a^3b$
$F_2(a) = a$	$F_2(b) = ab$	$\Rightarrow F_2(a^3) = a^3, F_2(ab) = a^2b, F_2(a^2b) = a^3b, F_2(a^3b) = b$
$F_3(a) = a$	$F_3(b) = a^2b$	$\Rightarrow F_3(a^3) = a^3, F_3(ab) = a^3b, F_3(a^2b) = b, F_3(a^3b) = ab$
$F_4(a) = a$	$F_4(b) = a^3b$	$\Rightarrow F_4(a^3) = a^3, F_4(ab) = b, F_4(a^2b) = ab, F_4(a^3b) = a^2b$
$F(a) = a^3$	$F(b) = a$	Descartada ya que $F(a^3) = a$
$F(a) = a^3$	$F(b) = a^3$	Descartada ya que F debe ser biyectiva
$F_5(a) = a^3$	$F_5(b) = b$	$\Rightarrow F(a^3) = a, F_5(ab) = a^3b, F_5(a^2b) = a^2b, F_5(a^3b) = ab$
$F_6(a) = a^3$	$F_6(b) = ab$	$\Rightarrow F_6(a^3) = a, F_6(ab) = b, F_6(a^2b) = a^3b, F_6(a^3b) = a^2b$
$F_7(a) = a^3$	$F_7(b) = a^2b$	$\Rightarrow F_7(a^3) = a, F_7(ab) = ab, F_7(a^2b) = b, F_7(a^3b) = a^3b$
$F_8(a) = a^3$	$F_8(b) = a^3b$	$\Rightarrow F_8(a^3) = a, F_8(ab) = a^2b, F_8(a^2b) = ab, F_8(a^3b) = b$
$F_9(a) = b$	$F_9(b) = a$	$\Rightarrow F_9(a^3) = a^2b, F_9(ab) = a^3b, F_9(a^2b) = a^3, F_9(a^3b) = ab$
$F_{10}(a) = b$	$F_{10}(b) = a^3$	$\Rightarrow F_{10}(a^3) = a^2b, F_{10}(ab) = ab, F_{10}(a^2b) = a, F_{10}(a^3b) = a^3b$
$F(a) = b$	$F(b) = b$	Descartada ya que F debe ser biyectiva
$F_{11}(a) = b$	$F_{11}(b) = ab$	$\Rightarrow F_{11}(a^3) = a^2b, F_{11}(ab) = a, F_{11}(a^2b) = a^3b, F_{11}(a^3b) = a^3$
$F(a) = b$	$F(b) = a^2b$	Descartada ya que $F(ba) = 1 = F(a^3b) = F(1)$
$F_{12}(a) = b$	$F_{12}(b) = a^3b$	$\Rightarrow F_{12}(a^3) = a^2b, F_{12}(ab) = a^3, F_{12}(a^2b) = ab, F_{12}(a^3b) = a$

$F_{13}(a) = ab$	$F_{13}(b) = a$	$\Rightarrow F_{13}(a^3) = a^3b, F_{13}(ab) = b, F_{13}(a^2b) = a^3, F_{13}(a^3b) = a^2b$
$F_{14}(a) = ab$	$F_{14}(b) = a^3$	$\Rightarrow F_{14}(a^3) = a^3b, F_{14}(ab) = a^2b, F_{14}(a^2b) = a, F_{14}(a^3b) = b$
$F_{15}(a) = ab$	$F_{15}(b) = b$	$\Rightarrow F_{15}(a^3) = a^3b, F_{15}(ab) = a^3, F_{15}(a^2b) = a^2b, F_{15}(a^3b) = a$
$F(a) = ab$	$F(b) = ab$	Descartada ya que F es biyectiva
$F_{16}(a) = ab$	$F_{16}(b) = a^2b$	$\Rightarrow F_{16}(a^3) = a^3b, F_{16}(ab) = a, F_{16}(a^2b) = b, F_{16}(a^3b) = a^3$
$F(a) = ab$	$F(b) = a^3b$	Descartada ya que $F(ba) = 1 = F(a^3b) = F(1)$
$F_{17}(a) = a^2b$	$F_{17}(b) = a$	$\Rightarrow F_{17}(a^3) = b, F_{17}(ab) = ab, F_{17}(a^2b) = a^3, F_{17}(a^3b) = a^3b$
$F_{18}(a) = a^2b$	$F_{18}(b) = a^3$	$\Rightarrow F_{18}(a^3) = b, F_{18}(ab) = a^3b, F_{18}(a^2b) = a, F_{18}(a^3b) = ab$
$F(a) = a^2b$	$F(b) = b$	Descartada ya que $F(ab) = 1 = F(1)$
$F_{19}(a) = a^2b$	$F_{19}(b) = ab$	$\Rightarrow F_{19}(a^3) = b, F_{19}(ab) = a^3, F_{19}(a^2b) = a^3b, F_{19}(a^3b) = a$
$F(a) = a^2b$	$F(b) = a^2b$	Descartada ya que F es biyectiva
$F_{20}(a) = a^2b$	$F_{20}(b) = a^3b$	$\Rightarrow F_{20}(a^3) = b, F_{20}(ab) = a, F_{20}(a^2b) = ab, F_{20}(a^3b) = a^3$
$F_{21}(a) = a^3b$	$F_{21}(b) = a$	$\Rightarrow F_{21}(a^3) = ab, F_{21}(ab) = a^2b, F_{21}(a^2b) = a^3, F_{21}(a^3b) = b$
$F_{22}(a) = a^3b$	$F_{22}(b) = a^3$	$\Rightarrow F_{22}(a^3) = ab, F_{22}(ab) = b, F_{22}(a^2b) = a, F_{22}(a^3b) = a^2b$
$F_{23}(a) = a^3b$	$F_{23}(b) = b$	$\Rightarrow F_{23}(a^3) = ab, F_{23}(ab) = a, F_{23}(a^2b) = a^2b, F_{23}(a^3b) = a^3$
$F(a) = a^3b$	$F(b) = ab$	Descartada ya que $F(ba) = 1 = F(a^3b) = F(1)$
$F_{24}(a) = a^3b$	$F_{24}(b) = a^2b$	$\Rightarrow F_{24}(a^3) = ab, F_{24}(ab) = a^3, F_{24}(a^2b) = b, F_{24}(a^3b) = a$
$F(a) = a^3b$	$F(b) = a^3b$	Descartada ya que F es biyectiva

Ahora sólo falta demostrar que estas 24 funciones biyectivas son homomorfismos, es decir, son los únicos automorfismos en $Aut(Q_8)$. Tendríamos pues que las 24 permutaciones de los 6 elementos $a, a^3, b, ab, a^2b, a^3b$ corresponden a los automorfismos de Q_8, quedando probado de esta manera que $Aut\,(Q_8) \cong S_4$.

Sólo revisamos la función F_{24}, las otras 22 se revisan de manera similar (nótese que la función F_1 corresponde a la idéntica). Cada elemento de Q_8 es de la forma a^rb^s, donde $0 \leq r \leq 3, 0 \leq s \leq 1$. Se debe entonces demostrar que $F_{24}(a^rb^sa^pb^q) = F_{24}(a^rb^s)F_{24}(a^pb^q)$. Consideremos dos casos:

(i) $s = 0$. Entonces, $F_{24}(a^rb^sa^pb^q) = F_{24}(a^ra^pb^q) = F_{24}(a^{r+p}b^q)$. Si $q = 0$, entonces $F_{24}(a^rb^sa^pb^q) = F_{24}(a^{r+p})$. Debemos entonces considerar 16 posibilidades, pero en vista de la simetría de la situación, basta tener en cuenta sólo los siguientes 10 casos:

$r = 0, p = 0 \Rightarrow F_{24}(a^rb^sa^pb^q) = 1, F_{24}(a^rb^s)F_{24}(a^pb^q) = 1$

$r = 0, p = 1 \Rightarrow F_{24}(a^rb^sa^pb^q) = a^3b, F_{24}(a^rb^s)F_{24}(a^pb^q) = a^3b$

$r = 0, p = 2 \Rightarrow F_{24}(a^rb^sa^pb^q) = a^2, F_{24}(a^rb^s)F_{24}(a^pb^q) = a^2$

$r = 0, p = 3 \Rightarrow F_{24}(a^rb^sa^pb^q) = ab, F_{24}(a^rb^s)F_{24}(a^pb^q) = ab$

$r = 1, p = 1 \Rightarrow F_{24}(a^rb^sa^pb^q) = a^2, F_{24}(a^rb^s)F_{24}(a^pb^q) = aa = a^2$

$r = 1, p = 2 \Rightarrow F_{24}(a^rb^sa^pb^q) = ab, F_{24}(a^rb^s)F_{24}(a^pb^q) = a^3ba^2 = ab$

$r = 1, p = 3 \Rightarrow F_{24}(a^rb^sa^pb^q) = 1, F_{24}(a^rb^s)F_{24}(a^pb^q) = a^3bab = 1$

$r = 2, p = 2 \Rightarrow F_{24}(a^rb^sa^pb^q) = 1, F_{24}(a^rb^s)F_{24}(a^pb^q) = a^2a^2 = 1$

$r = 2, p = 3 \Rightarrow F_{24}(a^rb^sa^pb^q) = a^3b, F_{24}(a^rb^s)F_{24}(a^pb^q) = a^2ab = a^3b$

$r = 3, p = 3 \Rightarrow F_{24}(a^rb^sa^pb^q) = a^2, F_{24}(a^rb^s)F_{24}(a^pb^q) = abab = a^2.$

Para $q = 1$ entonces $F_{24}(a^rb^sa^pb^q) = F_{24}(a^{r+p}b)$, se presentan entonces 16 posibilidades:

$r = 0, p = 0 \Rightarrow F_{24}(a^rb^sa^pb^q) = a^2b, F_{24}(a^rb^s)F_{24}(a^pb^q) = a^2b$

$r = 0, p = 1 \Rightarrow F_{24}(a^r b^s a^p b^q) = a^3, F_{24}(a^r b^s) F_{24}(a^p b^q) = a^3$

$r = 0, p = 2 \Rightarrow F_{24}(a^r b^s a^p b^q) = b, F_{24}(a^r b^s) F_{24}(a^p b^q) = b$

$r = 0, p = 3 \Rightarrow F_{24}(a^r b^s a^p b^q) = a, F_{24}(a^r b^s) F_{24}(a^p b^q) = a$

$r = 1, p = 0 \Rightarrow F_{24}(a^r b^s a^p b^q) = a^3, F_{24}(a^r b^s) F_{24}(a^p b^q) = a^3 b a^2 b = a^3$

$r = 1, p = 1 \Rightarrow F_{24}(a^r b^s a^p b^q) = b, F_{24}(a^r b^s) F_{24}(a^p b^q) = a^3 b a^3 = b$

$r = 1, p = 2 \Rightarrow F_{24}(a^r b^s a^p b^q) = a, F_{24}(a^r b^s) F_{24}(a^p b^q) = a^3 b b = a$

$r = 1, p = 3 \Rightarrow F_{24}(a^r b^s a^p b^q) = a^2 b, F_{24}(a^r b^s) F_{24}(a^p b^q) = a^3 b a = a^2 b$

$r = 2, p = 0 \Rightarrow F_{24}(a^r b^s a^p b^q) = b, F_{24}(a^r b^s) F_{24}(a^p b^q) = a^2 a^2 b = b$

$r = 2, p = 1 \Rightarrow F_{24}(a^r b^s a^p b^q) = a, F_{24}(a^r b^s) F_{24}(a^p b^q) = a^2 a^3 = a$

$r = 2, p = 2 \Rightarrow F_{24}(a^r b^s a^p b^q) = a^2 b, F_{24}(a^r b^s) F_{24}(a^p b^q) = a^2 b$

$r = 2, p = 3 \Rightarrow F_{24}(a^r b^s a^p b^q) = a^3, F_{24}(a^r b^s) F_{24}(a^p b^q) = a^2 a = a^3$

$r = 3, p = 0 \Rightarrow F_{24}(a^r b^s a^p b^q) = a, F_{24}(a^r b^s) F_{24}(a^p b^q) = a b a^2 b = a$

$r = 3, p = 1 \Rightarrow F_{24}(a^r b^s a^p b^q) = a^2 b, F_{24}(a^r b^s) F_{24}(a^p b^q) = a b a^3 = a^2 b$

$r = 3, p = 2 \Rightarrow F_{24}(a^r b^s a^p b^q) = a^3, F_{24}(a^r b^s) F_{24}(a^p b^q) = a b b = a^3$

$r = 3, p = 3 \Rightarrow F_{24}(a^r b^s a^p b^q) = b, F_{24}(a^r b^s) F_{24}(a^p b^q) = a b a = b.$

(ii) $s = 1$. Entonces, $F_{24}(a^r b^s a^p b^q) = F_{24}(a^{r+3p} b^{q+1})$. Al igual que en el caso (i) se debe considerar por separado cuando $q = 0$ y cuando $q = 1$. Revisemos en calidad de ilustración el caso $r = 3, p = 3, q = 1$: $F_{24}(a^r b^s a^p b^q) = F_{24}(a^{12} b^2) = F_{24}(a^2) = a^2, F_{24}(a^r b^s) F_{24}(a^p b^q) = aa = a^2$.

Capítulo 6

Grupos de permutaciones

En el capítulo anterior se probó que cada grupo G es isomorfo a un subgrupo del grupo de permutaciones $S(G)$. Cuando $G = \{x_1, \ldots, x_n\}$ es finito, el grupo de permutaciones se acostumbra a denotar S_n. En este caso los elementos $x_1, \ldots, x_n$ pueden ser reemplazados por los naturales $1, \ldots, n$. Así pues, S_n es el grupo de todas las funciones biyectivas del conjunto $I_n := \{1, 2, \ldots, n\}$.

En este capítulo estudiaremos con algún detalle al grupo S_n, denominado ***grupo simétrico de grado*** n. Destacamos en S_n algunos subgrupos importantes: el grupo alternante A_n y el grupo dihédrico de grado n, D_n.

6.1. Ciclos

Definición 6.1.1. *Sea f un elemento de S_n. Se dice que f es un* ***ciclo de longitud*** *m, $(1 \leq m \leq n)$, si existen $a_1, a_2, \ldots, a_m$ elementos diferentes de I_n tales que*

1. $f(a_1) = a_2, f(a_2) = a_3, \ldots, f(a_{m-1}) = a_m, f(a_m) = a_1,$
2. $f(x) = x$ *para* $x \notin \{a_1, \ldots, a_m\}$.

Se denota a f por

$$f = (a_1 a_2 \cdots a_m) = (a_2 a_3 \cdots a_m a_1) = (a_3 a_4 \cdots a_m a_1 a_2) = \cdots = (a_m a_1 a_2 \cdots a_{m-1})$$

Nótese que un ciclo de longitud 1 es la idéntica de I_n.

Sean $f = (a_1 \ldots a_m)$ y $g = (b_1 \ldots b_r)$ dos ciclos de S_n. Se dice que f y g son dos ***ciclos disyuntos*** si $\{a_1, a_2, \ldots, a_m\} \cap \{b_1, b_2, \ldots, br\} = \emptyset$. Nótese que las siguientes permutaciones f y g de S_7 son ciclos disyuntos:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 4 & 5 & 6 & 7 \end{pmatrix} = (123)$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 5 & 7 & 4 & 6 \end{pmatrix} = (4576)$$

Proposición 6.1.2. *En S_n el producto de ciclos disjuntos conmuta.*

Demostración. Sean $f = (a_1 \cdots a_m)$ y $g = (b_1 \cdots b_r)$ dos ciclos disyuntos de S_n. Sean $A := \{a_1, \ldots, a_m\}$ y $B := \{b_1, \ldots, b_r\}$. Sean $A_1 := I_n - A$ y $B_1 := I_n - B$. Dado $x \in I_n$ existen tres posibilidades

(i) $x \in A$: entonces $f(x) \in A, f(x) \notin B \Rightarrow g(f(x)) = f(x)$; $g(x) = x \Rightarrow f(g(x)) = f(x) \Rightarrow fg(x) = gf(x)$.

(ii) $x \in B$: es análogo al anterior.

(iii) $x \notin A$ y $x \notin B \Rightarrow f(x) = x, g(x) = x \Rightarrow fg(x) = x = gf(x)$.

De (i), (ii) y (iii) se desprende que $fg = gf$. □

La importancia de la anterior proposición se pone de manifiesto en el siguiente teorema.

Teorema 6.1.3. (i) *Sea $f = (a_1 \cdots a_m)$ un ciclo de longitud m de S_n. Entonces*

$$|f| = m.$$

(ii) *Sea $f = f_1 \cdots f_t$ una permutación de S_n, donde $f_1, \ldots, f_t$ son ciclos disyuntos de longitudes $m_1, \ldots, m_t$, respectivamente. Entonces*

$$|f| = m.c.m.(m_1, \ldots, m_t)$$

Demostración. (i) Probemos en primer lugar que $f^m = 1$: si $x \notin \{a_1, \ldots, a_m\} \Rightarrow f(x) = x \Rightarrow f^m(x) = x$. Sea $a_j \in \{a_1, \ldots, a_m\}, 1 \leq j \leq m$, f se puede expresar también como $f = (a_j a_{j+1} \cdots a_m a_1 a_2 \cdots a_{j-1}) \Rightarrow f(a_j) = a_{j+1} \Rightarrow f^2(a_j) = a_{j+2} \Rightarrow \cdots \Rightarrow f^{m-1}(a_j) = a_{j-1} \Rightarrow f^m(a_j) = a_j$; es decir, f^m actua también como la idéntica sobre los elementos de $\{a_1, \ldots, a_m\}$.

El orden de f es el menor entero positivo k tal que $f^k = 1$. Supóngase que existe $1 \leq k < m$ tal que $f^k = 1$. Por lo tanto, $f(a_1) = a_2, f^2(a_1) = a_3, \ldots, f^{k-1}(a_1) = a_k, f^k(a_1) = a_1 = f(a_k) = a_{k+1}$, pero esto es una contradicción ya que los elementos del ciclo f son diferentes. Lo anterior prueba que $|f| = m$.

(ii) La demostración se efectua por inducción sobre t.

$t = 1$: la afirmación es consecuencia de (i).

$t = 2$: $f = f_1 f_2$, donde f_1 y f_2 son ciclos disyuntos de longitudes m_1 y m_2 respectivamente. Según la proposición 6.1.2, $f_1 f_2 = f_2 f_1$. Además, $\langle f_1 \rangle \cap \langle f_2 \rangle = 1$. En efecto, sea $g \neq 1$ tal que $g = f_1^s = f_2^r$ con $1 \leq s < m_1$ y $1 \leq r < m_2$. Sea $f_1 = (a_1 \cdots a_m)$. Puesto que $g \neq 1$ existe $x \in I_n$ tal que $g(x) \neq x$. Necesariamente $x \in \{a_1, \ldots, a_m\}$. Sea pues $x = a_j \Rightarrow f_1^s(a_j) \neq a_j$ pero $f_2^r(a_j) = a_j$, contradicción.

Así pues, $\langle f_1 \rangle \cap \langle f_2 \rangle = 1$, $f_1 f_2 = f_2 f_1 \Rightarrow |f_1 f_2| = m.c.m.(m_1, m_2)$.

Supongamos que la afirmación es cierta para t: sea $f = f_1 f_2 \cdots f_t f_{t+1}$, donde $f_1, f_2, \ldots, f_t, f_{t+1}$ son ciclos disyuntos dos a dos y de longitudes $m_1, m_2, \ldots, m_{t+1}$, respectivamente. Sea $f' := f_1 f_2 \cdots f_t$. Entonces, $f = f' f_{t+1}$. Nótese que $\langle f' \rangle \cap \langle f_{t+1} \rangle = 1$. Además, $f' f_{t+1} = f_{t+1} f'$; entonces

$$\begin{aligned} |f| = m.c.m.(|f'|, m_{t+1}) &= m.c.m.(m.c.m.(m_1, \ldots, m_t), m_{t+1}) \\ &= m.c.m.(m_1, \ldots, m_{t+1}). \end{aligned}$$

□

Teorema 6.1.4. *Cada permutación f de S_n es representable como producto de ciclos disyuntos dos a dos. Tal representación es única salvo el orden y la inclusión de ciclos de longitud* 1.

Demostración. La existencia se realiza por induccion sobre n.

$n = 1$: S_1 sólo posee un elemento, el cual es un ciclo de longitud 1.

Supóngase que la afirmación es válida para toda permutación de un conjunto de m elementos con $m < n$. Sea $f \in S_n$. Si f es un ciclo entonces no hay nada que probar. Sea f una permutación que no es un ciclo. Esto en particular implica que $f \neq 1$. Existe entonces $a_1 \in I_n$ tal que $f(a_1) \neq a_1$. Cosideremos la sucesión $f(a_1), f^2(a_1), f^3(a_1), \ldots$. En esta sucesión se tiene un número finito de elementos diferentes de I_n debido a que para cada k ≥ 1, $f^k(a_1) \in I_n$ y I_n es finito. Por lo tanto existen r y p enteros positivos diferentes (por ejemplo $r > p$) tales que

$$f^p(a_1) = f^r(a_1), \text{ luego } f^{r-p}(a_1) = a_1.$$

Sea $A := \{r \in \mathbb{N} \mid f^r(a_1) = a_1\}$. Según lo dicho anteriormente, $A \neq \emptyset$. Como $A \subset \mathbb{N}$ y $\mathbb{N}$ es bien ordenado A posee entonces primer elemento k, es decir, k es el menor entero positivo tal que $f^k(a_1) = a_1$. Los elementos $f(a_1), f^2(a_1), \ldots, f^{k-1}(a_1), f^k(a_1) = a_1$ son diferentes, ya que en caso contrario existiría un $s < k$ tal que $f^s(a_1) = a_1$. La permutación f determina así el k-ciclo $g = (a_1 a_2 \cdots a_k)$, donde

$$a_2 = f(a_1), a_3 = f(a_2) = f^2(a_1), \ldots, a_k = f(a_{k-1}) = f^{k-1}(a_1), a_1 = f(a_k) = f^k(a_1).$$

Consideremos la permutación $f_1 \in S_n$ definida por $f_1(a_i) = a_i$, $1 \leq i \leq k$, $f_1(x) = f(x)$, $x \in I_n - \{a_1, \ldots, a_k\}$. Nótese que $f = f_1 g$. En efecto, si $x \in \{a_1, \ldots, a_k\}$ entonces sea $x = a_j$ para algún $1 \leq j \leq k$. Si $j < k$ entonces

$$g(x) = g(a_j) = a_{j+1} \Rightarrow f_1 g(x) = f_1(a_{j+1}) = a_{j+1} = f(a_j) = f(x). \text{ Si } j = k \text{ entonces}$$
$$g(x) = g(a_k) = a_1 \Rightarrow f_1 g(x) = f_1(a_1) = a_1 = f(a_k) = f(x).$$

Ahora, si $x \notin \{a_1, \ldots, a_k\}$ entonces $g(x) = x$, luego $f_1 g(x) = f_1(x) = f(x)$.

Puesto que f_1 fija los elementos $a_1, \ldots, a_k$ entonces f_1 puede considerarse como una permutación del conjunto $I_n - \{a_1, \ldots, a_k\}$. Por la hipótesis de induccion f_1 es producto de ciclos disyuntos conformados por los elementos de $I_n - \{a_1, \ldots, a_k\}$. En

total f es producto de ciclos disyuntos conformados por los elementos de I_n. Esto completa la prueba de la primera afirmación del teorema.

Probemos ahora la unicidad de la descomposición: sean

$$\begin{aligned} f &= (a_{11}a_{12}\cdots a_{1k_1})(a_{21}a_{22}\cdots a_{2k_2})\cdots(a_{r1}a_{r2}\cdots a_{rk_r}) \\ &= (b_{11}b_{12}\cdots b_{1m_1})(b_{21}b_{22}\cdots b_{2m_2})\cdots(b_{s1}b_{s2}\cdots b_{sm_s}) \end{aligned}$$

dos descomposiciones de f en producto de ciclos disyuntos. Nótese que $1 \leq r \leq n, 1 \leq s \leq n$. Estamos considerando que los elementos de I_n que permanezcan fijos bajo f conforman ciclos de longitud 1, es decir,

$$1 \leq k_i \leq n, 1 \leq i \leq r;\ 1 \leq m_j \leq n, 1 \leq i \leq s.$$

En otras palabras, estamos considerando que

$$\begin{aligned} I_n &= \{a_{11}, a_{12}, \ldots, a_{1k_1}; \ldots; a_{r1}, a_{r2}, \ldots, a_{rk_r}\} \\ &= \{b_{11}, b_{12}, \ldots, b_{1m_1}; \ldots; b_{s1}, b_{s2}, \ldots, b_{sm_s}\}. \end{aligned}$$

El elemento a_{11} debe aparecer en alguno de los ciclos de la segunda descomposición. Por la conmutatividad de los factores podemos asumir que $a_{11} \in \{b_{11}, b_{12}, \ldots, b_{1m_1}\}$. Reordenando el ciclo $(b_{11}b_{12}\cdots b_{1m_1})$ podemos considerar sin pérdida de generalidad que $a_{11} = b_{11}$. Según el teorema 6.1.3, k_1 es el menor entero positivo tal que $f^{k_1}(a_{11}) = a_{11}$. Se obtiene pues que $k_1 = m_1$ y además

$$\begin{gathered} f(b_{11}) = b_{12} = f(a_{11}) = a_{12};\ f(b_{12}) = b_{13} = f(a_{12}) = a_{13};\ \ldots; \\ f(b_{1m_1-1}) = b_{1m_1} = f(a_{1k_1-1}) = a_{1k_1};\ f(b_{1m_1}) = b_{11} = f(a_{1k_1}) = a_{11}, \end{gathered}$$

es decir, $(a_{11}a_{12}\cdots a_{1k_1}) = (b_{11}b_{12}\cdots b_{1m_1})$. El mismo análisis podemos aplicar a $a_{21}, a_{31}\ldots, a_{r1}$ demostrando que $r \leq s$ y la igualdad de ciclos. En forma similar $s \leq r$, lo cual concluye la prueba del teorema. □

Ejemplo 6.1.5.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 3 & 1 & 7 & 6 & 9 & 8 & 4 \end{pmatrix} \Rightarrow$$

$f = (125794)(3)(6) = (125794)$;

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 1 & 2 & 5 & 8 & 7 & 9 \end{pmatrix} \Rightarrow$$

$g = (134)(265)(78)(9) = (265)(134)(78) = (78)(134)(265) = (134)(78)(265) = (78)(265)(134) = (265)(78)(134)$.

6.2. El grupo alternante A_n

Definición 6.2.1. *Para $n \geq 2$, los ciclos de longitud 2 de S_n se conocen como* ***transposiciones****.*

Teorema 6.2.2. *Cada permutación de S_n es representable como un producto finito de transposiciones.*

Demostración. Puesto que cada permutacion es representable como un producto de ciclos disyuntos entonces es suficiente demostrar el teorema para cada ciclo. Sea $f = (a_1 a_2 \cdots a_m)$ un m-ciclo. Si $m = 1$ entonces $f = 1$ y $f = (a_1 a_2)(a_1 a_2)$. Sea pues $m \neq 1$. Nótese que $(a_1 a_2 \cdots a_m) = (a_m a_1)(a_{m-1} a_1) \cdots (a_2 a_1)$. □

Observación 6.2.3. (i) A diferencia del teorema 6.1.4, la representación de una permutación en producto de transposiciones no es única:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix} = (12435) = (51)(31)(41)(21) = (12)(52)(32)(42).$$

(ii) Según el teorema anterior, cada permutación f de S_n es representable como un número finito r de transposiciones; además se vió que dicha representación no es única. De tal manera que podría presentarse la posibilidad de que en una descomposición r sea par y en otra r sea impar. Sin embargo, la siguiente proposición muestra que tal situación es imposible.

Proposición 6.2.4. *Sea f una permutación de S_n la cual tiene dos descomposiciones en producto de r y s transposiciones. Entonces, r es par si, y sólo si,, s es par.*

Demostración. Sea f una permutación de S_n la cual tiene dos descomposiciones en producto de transposiciones $f = f_1 \cdots f_r = f'_1 \cdots f'_s$ $r \geq 1, s \geq 1$. Consideremos el natural $p = \Pi_{j>i}(j - i)$, $i, j \in I_n$ (por ejemplo para $n = 4$ se tiene que $p = (4-3)(4-2)(4-1)(3-2)(3-1)(2-1) = 12$). Sea f una permutación cualquiera de S_n. Definamos la acción de f sobre p como $pf = \Pi_{j>i}(f(j) - f(i))$.

Nótese que pf es un entero (no necesariamente positivo como p); los factores $(f(j) - f(i))$ que conforman pf son diferencias de elementos de I_n y además $|pf| = p$. En efecto, demostraremos que si $f = f_1 \cdots f_r$, donde cada f_i, $1 \leq i \leq r$, es una transposición, entonces

$$pf = (-1)^r p.$$

(a) Sea $f = (ab)$ una transposición con $a > b$. Los factores $(j - i)$ de p en los cuales no intervienen ni a ni b no cambian al aplicar f. Consideremos pues aquellos factores donde aparezcan a o b o ambos. Se presentan entonces las siguientes posibilidades.

(i) Factores donde aparece a pero no b:

$$(n-a),((n-1)-a),((n-2)-a)\cdots((a+1)-a),$$
$$(a-(a-1)),(a-(a-2))\cdots(a-(b+1)),(a-(b-1))\cdots(a-1).$$

Al aplicar f a los factores de la primera fila obtenemos

$$(n-b),((n-1)-b)\cdots((a+1)-b)$$

y no hay cambios de signo. Al aplicar f a los factores de la seguda fila obtenemos

$$(b-(a-1)),(b-(a-2))\cdots(b-(b+1))(b-(b-1))\cdots(b-1)$$

y hay $a-b-1$ cambios de signo.

(ii) Los factores donde aparece b pero no a :

$$(n-b),((n-1)-b)\cdots((a+1)-b)$$
$$((a-1)-b),((a-2)-b)\cdots((b+1)-b)$$
$$(b-(b-1))\cdots(b-1).$$

Aplicando f a los factores anteriores obtenemos

$$(n-a),((n-1)-a)\cdots((a+1)-a)$$
$$((a-1)-a),((a-2)-a)\cdots((b+1)-a)$$
$$(a-(b-1))\cdots(a-1).$$

se presenta en este caso $a-b-1$ cambios de signo.

(iii) Factor donde aparece a y b: $(a-b)$

Al aplicar f obtenemos $(b-a)$ y hay un cambio de signo.

En total al aplicar f a p se efectuan $2(a-b-1)+1$ cambios de signos y así pf tiene signo menos.

Nótese que los factores de (i) mediante f se convierten en los factores de (ii) con algunos signos cambiados, y a su vez los de (ii) en los de (i) con algunos signos cambiados. De lo anterior se desprende que

$$pf=-p, f=(ab), a>b.$$

(b) Si $f=f_1\cdots f_r$ es un producto de r transposiciones, entonces

$$pf=(pf_1)f_2\cdots f_r=(-1)^r p.$$

(c) $pf=(-1)^r p=(-1)^s p$, entonces $(-1)^r=(-1)^s \Leftrightarrow r$ y s son pares o r y s son impares. □

Según la proposición anterior se pueden distinguir aquellas permutaciones que son producto de un número par de transposiciones.

Teorema 6.2.5. *Sea $n \geq 2$ y $A_n := \{f \in S_n \mid f$ es producto de un número par de transposiciones$\}$. Entonces, $A_n \trianglelefteq S_n$ y se denomina el* ***grupo alternante*** *o grupo de permutaciones pares. Además, $|A_n| = \frac{n!}{2}$.*

Demostración. Claramente $A_n \neq \emptyset$. Además, según la proposición anterior el producto de dos permutaciones pares es par y la inversa de una permutación par es también par, con lo cual $A_n \leq S_n$.

Probemos ahora que A_n es normal en S_n. Consideremos la función signo

$$sgn : S_n \to \mathbb{Z}^*$$

$$sgn(f) := \begin{cases} 1, \text{ si } f \text{ es par} \\ -1, \text{ si } f \text{ es impar} \end{cases}$$

sgn es un homomorfismo: sean $f, g \in S_n$. Entonces se presentan las siguientes posibilidades:

f y g pares: entonces fg es par y así

$$sgn(fg) = 1 = sgn(f)sgn(g) = (1)(1)$$

f es par y g es impar: entonces fg es impar y así

$$sgn(fg) = -1 = sgn(f)sgn(g) = 1(-1).$$

f es impar y g es par: análogo al anterior.

f y g impares: entonces fg es par y así

$$sgn(fg) = 1 = sgn(f)sgn(g) = (-1)(-1).$$

sgn es una función sobre:

$$sgn(1) = 1, \quad sgn(ab) = -1;\ a, b \in I_n, a \neq b.$$

Según el teorema fundamental de homomorfismo

$$\mathbb{Z}^* \simeq S_n/\ker(sgn),$$

pero $\ker(sgn) = A_n$, así pues, $\mathbb{Z}^* \simeq S_n/A_n; \Rightarrow |S_n : A_n| = 2 \Rightarrow A_n \trianglelefteq S_n$. Nótese además que $|A_n| = \frac{n!}{2}$. □

6.3. Sistemas de generadores

Ya hemos visto que el subconjunto de todos los ciclos y también el conjunto de todas las transposiciones constituyen sistemas de generadores para S_n. Queremos ahora mostrar otros sistemas más reducidos de generadores.

Proposición 6.3.1. (i) $S_n = \langle (12), (123\cdots n)\rangle$

(ii) $S_n = \langle (12), (13), \ldots, (1n)\rangle$.

Demostración. Es suficiente demostrar la primera afirmación, ya que

$$(123\cdots n) = (1n)\cdots(13)(12).$$

Sea f una permutación de S_n. Entonces f es producto de ciclos disyuntos; basta pues probar que cada ciclo está en el generado por (12) y $(123\cdots n)$. Sea $(a_1a_2\cdots a_m)$ un m-ciclo de S_n. Entonces $(a_1a_2\cdots a_m) = (a_1a_m)\cdots(a_1a_2)$. Nótese que cada transposición (ab) se puede escribir como

$$(ab) = (1a)(1b)(1a).$$

Probemos entonces que para cada a, $(1a) \in \langle (12), (123\cdots n)\rangle$:

$$\begin{aligned} &a = 1 : (1a) = 1 = (12)(12)\\ &a = 2 : (1a) = (12)\\ &a = 3 : (13) = (21345\cdots n)(12)(21345\cdots n)^{-1}. \end{aligned}$$

Pero nótese que

$$(21345\cdots n) = (12)(123\cdots n)(12);$$

por tanto

$$\begin{aligned} (13) &= (21345\cdots n)(12)(12)(123\cdots n)^{-1}(12),\\ (13) &= (12)(123\cdots n)(12)(123\cdots n)^{-1}(12). \end{aligned}$$

En general, $(1a)$, con $a \geq 3$, se puede expresar como

$$\begin{aligned} (1a) = (2, 3, \ldots, a-2, a-1, 1, a, a+1, a+2, \ldots, n)(1, a-1)(2, 3, \ldots, a-2,\\ a-1, 1, a, a+1, a+2, \ldots, n)^{-1}. \end{aligned}$$

Por inducción suponemos que $(1b) \in \langle (12), (123\cdots n)\rangle$, con $b < a$; entonces resta probar que $(2, 3\ldots, a-2, a-1, 1, a, a+1, a+2\ldots n)$ está en el mencionado subgrupo.

$$\begin{aligned} (2, 3, \ldots, a-2, a-1, 1, a, a+1, a+2, \ldots, n) =\\ (1, a-1)(1, a-2)\cdots(13)(12)(123\cdots n)(12)(13)\cdots(1, a-2)(1, a-1). \end{aligned}$$

Según la hipótesis inductiva $(1, a-1), (1, a-2), \ldots, (13), (12) \in \langle (12), (123\cdots n)\rangle$. Esto completa la demostración de la proposición. □

Proposición 6.3.2. *Para $n \geq 3$, A_n coincide con con el subgrupo generado por los 3-ciclos.*

Demostración. Sea f una permutación par. Podemos agrupar las transposiciones de f de dos en dos y probar que cada pareja así constituida es producto de 3-ciclos.

Sean pues (a_1a_2) y (b_1b_2) dos transposiciones cualesquiera. Consideremos dos casos posibles:

(i) $\{a_1, a_2\} \cap \{b_1, b_2\} = \emptyset$:

$$\begin{aligned}(a_1a_2)(b_1b_2) &= (b_1b_2)(a_1b_1)(a_1b_1)(a_1a_2)\\ &= (b_1b_2)(b_1a_1)(a_1a_2b_1)\\ &= (b_1a_1b_2)(a_1a_2b_1)\end{aligned}$$

ya que $(a_1b_1) = (b_1a_1)$.

(ii) $\{a_1, a_2\} \cap \{b_1, b_2\} \neq \emptyset$: si $\{a_1, a_2\} = \{b_1, b_2\}$, entonces $(a_1a_2) = (b_1b_2)$ y $(a_1a_2)(b_1b_2) = 1 = (abc)(abc)(abc)$; hemos utilizado el hecho de que $n \geq 3$.

(iii) Si $a_1 = b_1$ pero $a_2 \neq b_2$ entonces

$$(a_1a_2)(b_1b_2) = (a_1a_2)(a_1b_2) = (a_1b_2a_2).$$

Si $a_1 = b_2$ pero $a_2 \neq b_1$ entonces se obtiene un 3-ciclo como en el caso anterior.

□

Proposición 6.3.3 (Teorema de Jordan). *Sea f una permutación cuaquiera de S_n. Entonces para cada ciclo $(a_1a_2\cdots a_m)$ se tiene que*

$$f^{-1}(a_1a_2\cdots a_m)f = (f(a_1)f(a_2)\cdots f(a_m)).$$

Demostración. Puesto que cada permutación es producto de transposiciones, es suficiente suponer que f es una pernutación $(\alpha\beta)$. Consideremos dos casos posibles:

(i) $\{\alpha, \beta\} \cap \{a_1, a_2, \ldots, a_m\} = \emptyset$:

$$\begin{aligned}(\alpha\beta)(a_1a_2\cdots a_m)(\alpha\beta) &= (a_1a_2\cdots a_m)(\alpha\beta)(\alpha\beta) = (a_1a_2\cdots a_m)\\ &= (f(a_1)f(a_2)\cdots f(a_m))\end{aligned}$$

ya que $f(a_i) = a_i$ para $1 \leq i \leq m$.

(ii) $\{\alpha, \beta\} \cap \{a_1, a_2, \ldots, a_m\} \neq \emptyset$: se presentan entonces dos situaciones:

(a) $\alpha \in \{a_1, a_2, \ldots, a_m\}, \beta \notin \{a_1, a_2, \ldots, a_m\}$: sea $\alpha = a_j, 1 \leq j \leq m$. Entonces

$$\begin{aligned}(\alpha\beta)(a_1\cdots a_{j-1}a_ja_{j+1}\cdots a_m)(\alpha\beta) &= (a_1\cdots a_{j-1}\beta a_{j+1}\cdots a_m)\\ &= (f(a_1)\cdots f(a_{j-1})f(a_j)f(a_{j+1})\cdots f(a_m))\end{aligned}$$

(b) $\alpha, \beta \in \{a_1, a_2, \ldots, a_m\}$: sea $\alpha = a_j$, $\beta = a_s$, $s \neq j$, $s < m$, $j < m$. Entonces

$$(\alpha\beta)(a_1\cdots a_j\cdots a_s\cdots a_m)(\alpha\beta) = (a_1\cdots a_{j-1}a_s\cdots a_{s-1}a_j\cdots a_m) = \\ (f(a_1)\cdots f(a_{j-1})f(a_j)\cdots f(a_{s-1})f(a_s)\cdots f(a_m)).$$

Por último, si por ejemplo $j = m \Rightarrow \alpha = a_m$ y entonces

$$\begin{aligned}(\alpha\beta)(a_1\cdots a_{s-1}a_s\cdots a_m)(\alpha\beta) &= (a_1\cdots a_{s-1}a_m a_{s+1}\cdots a_s) \\ &= (f(a_1)f(a_2)\cdots f(a_s)\cdots f(a_m)).\end{aligned}$$

□

6.4. El grupo dihédrico D_n, $n \geq 3$

Consideremos un polígono regular de $n \geq 3$ lados. Como ilustración consideremos un pentágono y un hexágono: por simetrías de un polígono regular de n lados se entienden el siguiente conjunto de movimientos de dicho polígono.

(i) n rotaciones en sentido contrario al movimiento de las manecillas del reloj a través de los ángulos $\frac{2\pi k}{n}$, $k = 0, 1, 2, \ldots, n-1$.

(ii) n reflexiones correspondientes a los n ejes de simetría.

Para el caso en que n sea par los ejes de simetría son: (a) $\frac{n}{2}$ líneas obtenidas uniendo el centro O del polígono con cada uno de sus vértices $1, 2, \ldots, n$. (b) $\frac{n}{2}$ líneas obtenidas uniendo el centro O con los puntos medios de los n lados del polígono. Para el caso en que n es impar las n reflexiones corresponden a los n ejes de simetría obtenidos uniendo el centro O del polígono con sus vértices.

Este conjunto de $2n$ movimientos constituye un grupo bajo la operación de composición de movimientos, y se denomina el ***grupo dihédrico de grado*** n el cual se denota por D_n.

El grupo dihédrico D_n como subgrupo de S_n: sea R_1 la rotación a través del ángulo $\theta := \frac{2\pi}{n}$. Esta rotación corresponde a la permutación de los vértices dada por

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix} = (123\cdots n).$$

Si denotamos la rotación a través del ángulo $\frac{2\pi k}{n}$ por R_k, $k = 0, 1, 2, \ldots, n$, entonces a R_k corresponde f^k. Nótese que R_1 es un elemento de D_n de orden n: $R_1^n = R_0$, $f^n = 1$.

Sea R_1' es la reflexión a través del eje de simetría que pasa por el vértice 1. Esta reflexión corresponde a la permutación de los vértices dada por

$$g = \begin{pmatrix} 1 & 2 & 3 & \cdots & k & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & n-k+2 & \cdots & 3 & 2 \end{pmatrix}$$

Nótese que R_1' tiene orden 2: $(R_1')^2 = R_0$, $g^2 = 1$. Por último, nótese que fg es de orden 2, de donde $(fg)^2 = 1$, luego

$$gfg = f^{-1}.$$

Generadores y relaciones del grupo dihédrico: consideremos la rotación y reflexión anteriores las cuales podemos identificar con las permutaciones f y g , respectivamente. Desde luego que $\langle f, g\rangle \leq D_n$. Si probamos que $|\langle f, g\rangle| = 2n$ entonces tendríamos que

$$D_n = \langle f, g\rangle, \text{ con } f^n = 1, g^2 = 1, gfg = f^{-1}. \tag{6.4.1}$$

Sea $x \in \langle f, g\rangle$, entonces x tiene la forma

$$x = f^{k_1} g^{l_1} f^{k_2} g^{l_2} \cdots f^{k_m} g^{l_m},\ k_i, l_i \in \mathbb{Z},\ 1 \leq i \leq m.$$

Puesto que f es un elemento de orden n y g un elemento de orden 2 podemos considerar que

$$x = f^{k_1} g^{l_1} f^{k_2} g^{l_2} \cdots f^{k_m} g^{l_m}, \text{ con } 0 \leq k_i \leq n-1,\ 0 \leq l_i \leq 1,\ 1 \leq i \leq m.$$

Como $gf = f^{-1}g$, entonces cada elemento $x \in \langle f, g\rangle$ tiene la forma $x = f^k g^l$, con $0 \leq k \leq n-1$, $0 \leq l \leq 1$. Resultan $2n$ elementos. Comprobemos que ellos son diferentes. Sean $0 \leq k, r \leq n-1$ y $0 \leq l, s \leq 1$ tales que $f^k g^l = f^r g^s \Rightarrow f^{r-k} = g^{s-l} \in \langle f\rangle \cap \langle g\rangle = 1$ (de lo contrario $g = f^k$, con $1 \leq k \leq n-1$, luego $gf = f^{k+1} = f^{-1}g$, y de esta forma $f^{k+2} = g = f^k$, es decir, $f^2 = 1$, lo cual es falso). En consecuencia, $n|(r-k)$. Siendo r y k con las condiciones dadas sólo puede tenerse que $r = k$, y de esto resulta también que $l = s$.

De lo anterior obtenemos que

$$D_n = \{1, f, f^2, \ldots, f^{n-1}, g, fg, \ldots, f^{n-1}g\}. \tag{6.4.2}$$

De otra parte, sea G un grupo generado por los elementos a y b tales que

$$\begin{aligned} a^n &= 1 \text{ es decir, } a \text{ es de orden } n, \\ b^2 &= 1 \text{ es decir, } b \text{ es de orden } 2, \\ bab &= a^{-1}. \end{aligned}$$

Entonces es posible repetir la prueba realizada anteriormente para comprobar que G tiene $2n$ elementos diferentes a saber

$$G = \{1, a, a^2, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\}.$$

La función $\varphi : G \to D_n$, definida por $\varphi(a^k b^l) = f^k g^l$, $0 \leq k \leq n-1$, $0 \leq l \leq 1$ es un isomorfismo de grupos.

Representación matricial del grupo dihédrico: consideremos en $GL_2(\mathbb{R})$ las matrices

$$A := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

$$B := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

con $\theta := \frac{2\pi}{n}$. Nótese que A es de orden n y B es de orden 2. Además,

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix},$$

es decir $BAB = A^{-1}$. Esto indica que $\langle A, B\rangle$ es isomorfo al grupo dihédrico. La matriz A representa la rotación del sistema de coordenadas xy a través de de un ángulo $\theta = \frac{2\pi}{n}$; la matriz B representa una reflexión de dicho sistema .

Regla de multiplicación en el grupo dihédrico: nótese que en D_n se tiene la siguiente regla de multiplicación:

$$(f^k g^m)(f^{k'} g^{m'}) = \begin{cases} f^{k+k'} g^{m+m'}, \text{ si } m = 0 \\ f^{k-k'} g^{m+m'}, \text{ si } m = 1. \end{cases}$$

Ejemplo 6.4.1. Algunos subgrupos de D_n. A partir de los generadores y las relaciones que definen D_n podemos presentar inmediatamente los siguientes subgrupos: de orden 1 el trivial $1 := \{1\}$; de orde $2n$ el trivial D_n; de orden n tenemos al menos a $\langle f\rangle$ (como se observó, en D_4, este no es el único subgrupo de orden 4). Puesto que $\langle f\rangle$ es cíclico entonces por cada divisor de n tendremos al menos un subgrupo de orden k.

Los subgrupos de orden 2 son:

$$\langle f^{\frac{n}{2}}\rangle \text{ si n es par}; \langle g\rangle, \langle fg\rangle, \langle f^2 g\rangle, \ldots, \langle f^{n-1} g\rangle.$$

Ejemplo 6.4.2. *Centro de* D_n. Para todo $0 \leq k \leq n-1$, $f^k g \notin Z(D_n)$: en efecto, $(\ f^k g)f = f^{k-1}g, f(\ f^k g) = f^{k+1}g$. Si fuese $f^{k-1}g = f^{k+1}g$ entonces $f^2 = 1$; pero $n \geq 3$ y $f^n = 1$. De lo anterior obtenemos que $Z(D_n)$ contiene solamente rotaciones: Sea $f^k \in Z(D_n)$ con $0 \leq k \leq n-1$. Entonces $f^k g = g f^k \Rightarrow f^k g = f^{-k} g \Rightarrow f^{2k} = 1 \Rightarrow n|2k$. Cuando n es impar $\Rightarrow k = 0 \Rightarrow Z(D_n) = 1$. Sea $n = 2m$ par. Como $2m|2k$ entonces existe $\lambda \geq 1$ tal que $2k = 2m\lambda \Rightarrow k = m\lambda$. Si fuese $\lambda \geq 2 \Rightarrow m\lambda \geq 2m = n \Rightarrow k \geq n$ contradicción; por lo tanto $\lambda = 1 \Rightarrow k = n/2$. De lo anterior obtenemos que si $x \in Z(D_n)$ entonces x es de la forma $x = f^{\frac{n}{2}}$. Veamos que realmente en este caso par $f^{\frac{n}{2}} \in Z(D_n)$:

$$f f^{\frac{n}{2}} = f^{\frac{n}{2}} f, \quad g f^{\frac{n}{2}} = f^{-\frac{n}{2}} g = f^{\frac{n}{2}} g.$$

Obtenemos que $f^{\frac{n}{2}}$ conmuta con cada elemento de $\langle f, g\rangle = D_n$, es decir, $f^{\frac{n}{2}} \in Z(D_n)$. De lo dicho obtenemos que

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

6.5. Subgrupos normales del grupo D_n, $n \geq 3$

Sea $N \trianglelefteq D_n$. Consideremos los siguientes casos posibles:

(i) n es impar y N no contiene reflexiones: en este caso $N \leq \langle f\rangle$ y existe entonces un divisor positivo k de n tal que $N = \langle f^k\rangle$. Veamos que cada subgrupo de este tipo es efectivamente normal en D_n:

$$(f^\alpha g^\beta)^{-1}(f^k)^j(f^\alpha g^\beta) = \begin{cases} f^{-kj} & si\ \beta = 1 \\ f^{kj} & si\ \beta = 0 \end{cases}$$

(ii) n es impar y en N hay al menos una reflexión: sea $f^k g$ en N, donde k es fijo y cumple $0 \leq k \leq n-1$. Sea $0 \leq r \leq n-1$, entonces $(f^r)^{-1}(f^k g)(f^r) \in N$, luego $f^{k-2r}g \in N$. Tomando $r = k$ se tiene que $f^{-k}g \in N$ y entonces $f^{-2k} \in N$. Tomemos ahora $r = k+1$, entonces $f^{k-2(k+1)}g = f^{-k-2}g \in N$ y entonces $f^k g f^{-k-2}g = f^{2k+2} \in N$. De aquí resulta entonces que $f^2 \in N$. Como n es impar, $\langle f\rangle = \langle f^2\rangle \subseteq N$, es decir, $f \in N$. Finalmente, $f^{-k} \in N$ y entonces $g \in N$. Esto garantiza que $N = D_n$.

(iii) n es par y N no contiene reflexiones: razonando como en el caso impar se obtiene que existe entonces un divisor positivo k de n tal que $N = \langle f^k\rangle$.

(iv) n es par y en N hay al menos una reflexión: sea $n = 2t$ y sea $f^k g$ en N, donde k es fijo y cumple $0 \leq k \leq n-1$. Al igual que en el caso impar podemos concluir que $f^2 \in N$. Consideremos dos casos posibles: (a) $g \in N$: entonces el siguiente conjunto de n elementos distintos está incluido en N: $\{f^{2r}g^l \,|\, 0 \leq r \leq \frac{n}{2} - 1,\ 0 \leq l \leq 1\}$. Si N posee al menos un elemento adicional, entonces $|N| \geq n+1$ y esto implica que $|N| = 2n$. En efecto, $|N|$ divide a $2n$ y entonces $2n = |N|a$; si $a \geq 2$ entonces $|N|a \geq 2|N|$, luego $2n \geq 2n+2$, lo cual es falso. Así pues, si N no posee al menos un elemento adicional, entonces N es exactamente el subgrupo

$$N = \{f^{2r}g^l \,|\, 0 \leq r \leq \frac{n}{2} - 1,\ 0 \leq l \leq 1\} =< f^2, g > \cong D_{\frac{n}{2}}$$

En caso contrario, N coincide con D_n.

(b) $g \notin N$: veamos que entonces necesariamente $fg \in N$. En efecto, k debe ser impar, ya que de lo contrario $k = 2u$ y entonces $(f^2)^{-u} = f^{-k} \in N$,

con lo cual $f^{-k}f^k g = g \in N$, lo cual es falso. Así pues, $k = 2w+1$ y esto implica que $f^{-2w}f^k g = fg \in N$. Nótese que entonces N contiene al conjunto $\{f^{2k} \,|\, 0 \leq k \leq \frac{n}{2}-1\}$ y también al conjunto $\{f^{2k+1}g \,|\, 0 \leq k \leq \frac{n}{2}-1\}$, la reunión de los cuales tiene n elementos. Como se vió anteriormente, si N posee al menos un elemento adicional, entonces $N = D_n$, en caso contrario N es exactamente la reunión de estos dos conjuntos. Pero notemos que la reunión de estos dos conjuntos es $\langle f^2, fg\rangle$

En conclusión, los subgrupos normales de D_n se caracterizan de la siguiente manera: sea $N \trianglelefteq D_n$, si n es impar, entonces $N = D_n$ ó $N = \langle f^k\rangle$ con $k|n$; si n es par, entonces $N = D_n$ ó $N = \langle f^k\rangle$ con $k|n$ ó $N = \langle f^2, g\rangle \cong D_{\frac{n}{2}}$ ó $N = \langle f^2, fg\rangle \cong D_{\frac{n}{2}}$.

6.6. Ejercicios

1. Calcule $Z(S_n)$ y $Z(A_n)$.

   Solución. $n = 2 \Rightarrow S_2 \cong \mathbb{Z}_2 \Rightarrow Z(S_2) = S_2$; $Z(A_2) = A_2$.

   $n \geq 3$: si $n = 3 \Rightarrow A_3 \cong \mathbb{Z}_3 \Rightarrow Z(A_3) = A_3$. Sea π un elemento cualquiera de S_n, $\pi \neq 1$. Entonces π es producto de ciclos disjuntos:

   $$\pi = (ij\cdots)(\cdots)\cdots, \text{ donde } i \neq j.$$

   Como $n \geq 3$ existe $k \neq i$, $k \neq j$; consideremos la trasposición (jk). Nótese que $\pi(jk) \neq (jk)\pi$. En efecto, $\pi(jk)i = j$; $(jk)\pi i = k$. Por lo tanto, para cada $\pi \neq 1$ en S_n, $n \geq 3$, existe un elemento con el cual π no conmuta $\Rightarrow$ $Z(S_n) = 1, n \geq 3$.

   Sea ahora $n \geq 4$ y sea $\pi = (ij\cdots)(\cdots)\cdots$ un elemento de A_n diferente de 1. Sea $\ell \neq i$, $\ell \neq j$, $\ell \neq k$ y k escogido como antes. Entonces $(jk\ell) \in A_n$ y además $\pi(jk\ell) \neq (jkl)\pi$. En efecto, $\pi(jkl)i = j \neq k = (jk\ell)\pi i$; $\Rightarrow$ para cada $\pi \neq 1$ en A_n, $n \geq 4$, existe un elemento con el cual π no conmuta $\Rightarrow Z(A_n) = 1, n \geq 4$.

2. Demuestre que $Int(D_n) = \begin{cases} D_n, & \text{si } n \text{ es impar,} \\ D_{\frac{n}{2}}, & \text{si } n \text{ es par.} \end{cases}$

3. ¿Cuántos subgrupos normales tiene D_{21}?

4. ¿Cuántos subgrupos normales tiene D_{12}?

Capítulo 7

Productos y sumas directas

El objetivo de este capítulo es presentar la construcción del grupo producto cartesiano y su suma directa externa para una familia dada de grupos. Mostraremos cómo se definen el producto y la suma directa externa en el caso de una familia infinita. Se da además la definición de suma directa interna de una familia finita de subgrupos de un grupo dado, mostrando la relación que ésta guarda con el producto cartesiano. Las construcciones presentadas aquí servirán como base teórica para iniciar en el capítulo 10 el estudio de los grupos abelianos finitos.

7.1. Definición

Sea $\{G_1, \ldots, G_n\}$ una colección finita de grupos (tomados con notación multiplicativa) y sea

$$\prod_{i=1}^{n} G_i := G_i \times \cdots \times G_n := \{(x_i, \ldots, x_n) \mid x_i \in G_i, 1 \leq i \leq n\}$$

el producto cartesiano conjuntista de la familia dada. Se pretende definir en $\prod_{i=1}^{n} G_i$ una operación binaria bajo la cual $\prod_{i=1}^{n} G_i$ tenga estructura de grupo.

Proposición 7.1.1. *Sea $\{G_1 \ldots G_n\}$ una familia finita de grupos y sea $\prod_{i=1}^{n} G_i$ el producto cartesiano de los conjuntos $G_i, 1 \leq i \leq n$. El producto de n-plas definido por*

$$(x_1, \ldots, x_n)\,(x'_1, \ldots, x'_n) := (x_1 x'_1, \ldots, x_n x'_n)$$

*da a $\prod_{i=1}^{n} G_i$ una estructura de grupo. La pareja $(\prod_{i=1}^{n} G_i, .)$ así constituida se denomina **producto cartesiano** de la familia $\{G_1, \ldots, G_n\}$.*

Demostración. En efecto, la asociatividad del producto de n-plas se desprende de las respectivas propiedades asociativas de los productos definidos en los grupos $G_i, 1 \leq i \leq n$. Denotando por 1 el elemento neutro del grupo G_i, entonces la n-pla $1 :=$

$(1,\ldots,1)$ es el elemento neutro del producto cartesiano. Además, si x_i^{-1} denota el inverso de x_i en G_i entonces el inverso de la n-pla $x = (x_1,\ldots,x_n)$ es $x^{-1} = (x_1^{-1},\ldots,x_n^{-1})$. □

Observación 7.1.2. Si los grupos $G_i, 1 \leq i \leq n$, presentan notación aditiva, entonces la operación entre n-plas se denota por

$$(x_1,\ldots,x_n) + (x_1',\ldots,x_n') = (x_1 + x_1',\ldots,x_n + x_n')$$

En este caso el neutro y los opuestos toman la forma

$$0 := (0,\ldots,0),\ -(x_1,\ldots,x_n) = (-x_1,\ldots,-x_n) = -x$$

Ejemplo 7.1.3. (i) Sean $G_1 = \mathbb{Z}_2$ y $G_2 = \mathbb{Z}_3$. Entonces los elementos de $\mathbb{Z}_2 \times \mathbb{Z}_3$ son

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}.$$

Nótese que $|\mathbb{Z}_2 \times \mathbb{Z}_3| = 6 = 2.3 = |\mathbb{Z}_2|\,.\,|\mathbb{Z}_3|$. Más aún, $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$: $\mathbb{Z}_2 \times \mathbb{Z}_3$ es un grupo cíclico con generador $(1,1)$: $1\,(1,1) = (1,1)\,, 2\,(1,1) = (0,2)\ 3\,(1,1) = (1,0)\,, 4\,(1,1) = (0,1)\ 5\,(1,1) = (1,2)\,, 6\,(1,1) = (0,0)\,.$

(ii) Sean $G_1 = G_2 = \mathbb{Z}_2$. Entonces los elementos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ son

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

Obsérvese que $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$ pero $\mathbb{Z}_2 \times \mathbb{Z}_2$ no es isomorfo a $\mathbb{Z}_4$:

$|(0,0)| = 1, \quad |(0,1)| = |(1,0)| = |(1,1)| = 2 \Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ no es cíclico, $\Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ no es isomorfo con $\mathbb{Z}_4$, luego $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$.

Algunas propiedades del producto cartesiano se presentan a continuación.

Proposición 7.1.4. *Sea $\{G_i\}_{i=1}^n$ una familia de grupos arbitrarios. Entonces:*

(i) $G_1 \times G_2 \cong G_2 \times G_1$.

(ii) $G_1 \times \cdots \times G_n \cong G_{\pi(1)} \times \cdots \times G_{\pi(n)}$, *para cada* $\pi \in S_n$.

(iii) $G_1 \times G_2 \times G_3 \cong G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3$.

(iv) *El producto cartesiano tiene la propiedad asociativa generalizada.*

(v) $G_1 \times \cdots \times G_n$ *es abeliano* $\Leftrightarrow$ *para cada* $i, 1 \leq i \leq n$, G_i *es abeliano.*

Demostración. Todas las afirmaciones se obitenen en forma inmediata de la definición de producto cartesiano. □

Proposición 7.1.5. *Sea $\{G_i\}_{i=1}^n$ una familia de grupos finitos. Entonces:*

$$|G_1 \times \cdots \times G_n| = |G_1| \cdots |G_n|.$$

Además,

(i) *Sea* $\{G_i\}_{i=1}^n$ *una familia finita de grupos arbitrarios y sea* $x = (x_1, \ldots, x_n) \in \prod_{i=1}^n G_i$ *tal que* x_i *es de orden finito para cada* $1 \leq i \leq n$, *entonces* $|x| = m.c.m. \{|x_i|\}_{i=1}^n$.

(ii) *Si* m *y* n *son enteros positivos primos relativos, entonces* $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

(iii) *Sean* $m_1, \ldots, m_k$ *enteros positivos tales que* $(m_i, m_j) = 1$ *para* $i \neq j$, $1 \leq i, j \leq n$. *Entonces*

$$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k} \cong \mathbb{Z}_{m_1 \cdots m_k}$$

(iv) *Sea* $n = p_1^{m_1} \cdots p_k^{m_k}$ *la descomposición del entero* n *en factores primos. Entonces*

$$\mathbb{Z}_{p_1^{m_1}} \times \cdots \times \mathbb{Z}_{p_k^{m_k}} \cong \mathbb{Z}_n.$$

Demostración. Basta encontrar dos elementos a, b en $\mathbb{Z}_m \times \mathbb{Z}_n$ tales que su órdenes $|a| = m$ y $|b| = n$ sean primos entre si, porque entonces ab es de orden mn y $\mathbb{Z}_m \times \mathbb{Z}_n$ resulta cíclico de orden mn, es decir, $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. Nótese que $a = (1, 0)$ y $b = (0, 1)$ son los elementos buscados. La parte (iii) de esta proposición se prueba usando lo que acabamos de ver en forma recurrente, y la parte (iv) es un caso particular de (iii). □

Notemos que para cada $1 \leq i \leq n$, G_i se sumerge de manera natural en el producto $G_1 \times \cdots \times G_n$, y por lo tanto puede ser considerado como un subgrupo de éste.

Proposición 7.1.6. *Sea* $\{G_i\}_{i=1}^n$ *una familia finita de grupos. Entonces:*

(i) $G_i \trianglelefteq G_1 \times \cdots \times G_n$, *para cada* $1 \leq i \leq n$.

(ii) $(G_1 \times \cdots \times G_n) \,/\, G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$.

Demostración. Esto es un sencillo ejercicio para el lector. □

7.2. Producto cartesiano: caso infinito

Sea $\{G_i\}_{i\in I}$ una familia cualquiera de grupos. Sea $\prod_{i\in I} G_i$ el ***producto cartesiano*** de los conjuntos de la familia dada, es decir,

$$\prod_{i\in I} G_i := \{x : I \to \bigcup_{i\in I} G_i \mid x(i) \in G_i\}.$$

Definimos en $\prod_{i\in I} G_i$ el producto de manera análoga a como se hizo en el caso finito. Sea $x_i := x(i)$, luego $x = (x_i)_{i\in I}$ y entonces

$$xy = (x_i)(y_i) := (x_i y_i).$$

Nótese que este producto da a $\prod_{i\in I} G_i$ una estructura de grupo, cuyo elemento neutro es $1 := (e_i)$, donde $e_i = 1 \in G_i$, para cada $i \in I$. El inverso de $x = (x_i)$ es entonces $x^{-1} = (x_i^{-1})$. Cuando $I = I_n = \{1, 2 \dots n\}$ entonces esta definición de producto $\prod_{i\in I} G_i$ coincide con la definición de producto cartesiano dada en la sección anterior.

Las ***proyecciones canónicas*** del producto se definen por

$$\pi_j : \prod G_i \to G_j, \quad \pi_j[(x_i)] := x_j.$$

El producto cartesiano junto con sus proyecciones está caracterizado por la siguiente propiedad universal.

Teorema 7.2.1. *Sean $\{G_i\}_{i\in I}$ una familia de grupos, $\prod_{i\in I} G_i$ su producto cartesiano y $\{\pi_j : \prod_{i\in I} G_i \to G_j\}_{j\in I}$ las proyecciones canónicas. Entonces,*

(i) *Para cada grupo G con homomorfismos $\{p_j : G \to G_j\}_{j\in I}$ existe un único homomorfismo α de G en $\prod_{i\in I} G_i$ tal que para cada $j \in I$ se tiene que $\pi_j\alpha = p_j$.*

(ii) *Cualquier otro grupo H con homomorfismos $\{H \xrightarrow{\pi'_j} G_j\}_{j\in I}$ que tenga la propiedad (i) es isomorfo al producto cartesiano.*

Demostración. (i) α se define por $\alpha(y) := (p_j(y))$ con $y \in G$; claramente α es un homomorfismo de grupos y satisface $\pi_j\alpha = p_j$ para cada $j \in I$. Sea θ otro homomorfismo de G en el producto que cumple estas mismas igualdades; sea $\theta(y) := (x_i)_{i\in I}$. Entonces, $\pi_j\theta(y) = x_j = p_j(y)$, para cada $j \in I$, luego $\theta(y) = (x_j) = \alpha(y)$.

(ii) Puesto que tanto H como el producto tienen la propiedad (i), entonces para cada $j \in I$ resulta $\pi_j(\alpha\beta) = \pi_j$, $\pi'_j(\beta\alpha) = \pi'_j$, con $\beta : \Pi G_i \to H$ un homomorfismo. En vista de la unicidad, $i_H = \beta\alpha$ y $\alpha\beta = i_{\Pi G_i}$. Esto muestra que H y ΠG_i son isomorfos. □

7.3. Suma directa externa

Sea $\{G_i\}_{i\in I}$ una familia de grupos y sea $\prod_{i\in I} G_i$ su grupo producto. Se denomina ***soporte*** de $x = (x_i)$ al subconjunto I_x de I de elementos i tales que $x_i \neq 1$. Definimos el conjunto

$$\bigoplus_{i\in I} G_i := \{x = (x_i) \in \prod G_i \mid x \text{ es de soporte finito}\}.$$

$\bigoplus_{i\in I} G_i$ es un subgrupo del producto y se denomina ***suma directa externa*** de la familia dada. En efecto, $1 \in \bigoplus_{i\in I} G_i$, con lo cual la suma directa externa no es vacía. Sean $x,\ z \in \bigoplus_{i\in I} G_i$ con soportes I_x, I_z. Entonces, $x_i z_i = 1$ para cada $i \in I - (I_x \cup I_z)$. Esto indica que sólo para los elementos de un cierto subconjunto finito $I_y \subseteq I_x \cup I_z$ se tiene que $x_i z_i \neq 1$. Por lo tanto, si $y = (y_i)$ es el producto de x y z entonces $y \in \bigoplus_{i\in I} G_i$. Es claro que si $x \in \bigoplus_{i\in I} G_i$ entonces $x^{-1} \in \bigoplus_{i\in I} G_i$.

Asociadas a la suma directa externa de una familia de grupos están las siguientes ***inyecciones canónicas***:

$$\mu_j : G_j \to \bigoplus_{i\in I} G_i,$$
$$\mu_j(a) := x := (x_i), \text{ donde } x_j := \left\{ \begin{array}{ll} a, & i = j \\ 1, & i \neq j \end{array} \right\}$$

Evidentemente estas funciones son homomorfismos inyectivos.

Para la clase de los grupos abelianos, la suma directa externa con sus inyecciones canónicas está caracterizada por la siguiente propiedad universal.

Teorema 7.3.1. *Sea $\{G_i\}_{i\in I}$ una familia de grupos abelianos, y sea $\bigoplus_{i\in I} G_i$ su suma directa externa y sean $\{\mu_j : G_j \to \bigoplus_{i\in I} G_i\}$ sus inyecciones canónicas. Entonces,*

(i) *Para cada grupo abeliano G con homomorfismos $\{t_j : G_j \to \bigoplus_{i\in I} G_i\}_{j\in I}$ existe un único homomorfismo $\alpha : \bigoplus_{i\in I} G_i \to G$ tal que para cada $j \in I$ se tiene que $\alpha\mu_j = t_j$.*

(ii) *Cualquier otro grupo abeliano H con homomorfismos $\{\mu'_j : G_j \to H\}_{j\in I}$ que tenga la propiedad (i) es isomorfo a la suma directa externa.*

Demostración. (i) Definimos α por

$$\alpha(x) := \left\{ \begin{array}{ll} \prod_{j\in I_x} t_j(x_j), & si\ x \neq 1 \\ 1 \quad , & si\ x = 1 \end{array} \right\}$$

α es un homomorfismo: si $x = 1$ o $y = 1$ entonces evidentemente $\alpha(xy) = \alpha(x)\alpha(y)$. Supóngase pues que $x \neq 1$ y $y \neq 1$. Sea $z = (z_i) = xy$. Si $z = 1$, entonces $y = x^{-1}$ y asi $y_i = x_i^{-1}$ para cada $i \in I$, con lo cual $\alpha(z) = 1 = \prod_{j\in I_x} t_j(x_j) \prod_{j\in I_y} t_j(y_j) = \alpha(x)\alpha(y)$. Sea entonces $z \neq 1$. Ya que $I_z \subseteq I_x \cup I_y$ se tiene que

$$\alpha(z) = \prod_{j\in I_z} t_j(z_j) = \prod_{j\in I_x\cup I_y} t_j(z_j) = \prod_{j\in I_x\cup I_y} t_j(x_j y_j) =$$
$$\prod_{j\in I_x\cup I_y} t_j(x_j) \prod_{j\in I_x\cup I_y} t_j(y_j) = \prod_{j\in I_x} t_j(x_j) \prod_{j\in I_y} t_j(y_j) = \alpha(x)\alpha(y).$$

Probemos ahora la unicidad de α : sea θ otro homomorfismo de $\bigoplus_{i\in I} G_i$ en G tal que $\theta \circ \mu_j = t_j$ para cada $j \in I$. Sea x un elemento cualquiera de $\bigoplus_{i\in I} G_i$. Si $x = 1$ entonces necesariamente $\alpha(1) = \theta(1) = 1$. Considérese pues que $x \neq 1$. Entonces

$\alpha(x) = \prod_{j\in I_x} t_j(x_j) = \prod_{j\in I_x} \theta\mu_j(x_j) = \theta\left[\prod_{j\in I_x} \mu_j(x_j)\right] = \theta(x)$, ya que $x = \prod_{j\in I_x} \mu_j(x_j)$.

(ii) La prueba es como en el caso del producto y la dejamos al lector. □

Observación 7.3.2. Nótese que cuando $I = I_n := \{1, 2, \ldots, n\}$ es un conjunto finito, entonces el producto cartesiano $G_1 \times \cdots \times G_n$ y la suma directa externa $\bigoplus_{i=1}^n G_i$ de grupos abelianos coinciden y entonces se usa también la siguiente notación: $G_1 \times \cdots \times G_n = G_1 \oplus \cdots \oplus G_n$.

7.4. Suma directa interna

Sea G un grupo y sean H, K subgrupos de G. Se ha visto que el conjunto $HK = \{hk \mid h \in H,\ k \in K\}$ es un subgrupo de G si, y sólo si, $HK = KH$. Es posible que para dos subgrupos H y K de G el producto HK coincida con G. En efecto, considérese el grupo $D_4 = \{1, f, f^2, f^3, g, fg, f^2g, f^3g\}$, $f^4 = 1, g^2 = 1$, y $gfg = f^{-1}$. Sean $K = \{1,\ f^2,\ g,\ f^2g\}$ y $H = \{1,\ f^2,\ fg,\ f^3g\}$. Nótese que $KH = HK = D_4$. De aquí en particular se desprende que cada elemento de D_4 puede escribirse como producto de un elemento de K y otro de H. Por ejemplo: $f = g(f^3g)$, $g \in K$, $f^3g \in H$. Sin embargo esta representación de f no es única: $f = (f^2g)(fg)$, $f^2g \in K$, $fg \in H$. Esta no unicidad se debe al hecho que $H \cap K \neq 1$.

La suma directa interna de subgrupos de un grupo puede ser definida para el caso infinito. Nosotros consideramos sólo el caso de una colección finita de subgrupos.

Proposición 7.4.1. *Sean $H_1 \ldots H_n$ subgrupos normales de G. Entonces*

$$\langle \textstyle\bigcup_{i=1}^n H_i\rangle = H_1 \cdots H_n := \{h_1 \cdots h_n \mid h_i \in H_i,\ \ 1 \leq i \leq n\}.$$

Además, $H_1 \cdots H_n \trianglelefteq G$ y para cada $\pi \in S_n$, $H_1 \cdots H_n = H_{\pi(1)} \cdots H_{\pi(n)}$.

Demostración. Inducción sobre n : $n = 1 : \langle H_1\rangle = H_1$.

$n = 2$: evidentemente $H_1H_2 \subseteq \langle H_1 \cup H_2\rangle$. Sea $x \in \langle H_1 \cup H_2\rangle$; $\Rightarrow x = x_1^{\epsilon_1} \cdots x_t^{\varepsilon_t}$, donde $x_i \in H_1 \cup H_2$, $\varepsilon_i = \pm 1$, $1 \leq i \leq t$. Se desea ahora reordenar los elementos $x_1^{\epsilon_1} \ldots x_t^{\epsilon_t}$, de tal manera que aparezcan a la izquierda sólo elementos de H_1 y a la derecha sólo elementos de H_2. Sea i el menor índice ($1 \leq i \leq t$) tal que $x_i^{\varepsilon_i} \in H_2$ y $x_{i+1}^{\epsilon_{i+1}} \in H_1$. Si $i = t$ entonces $x \in H_1H_2$. Sea pues $i \neq t$, entonces

$$x = x_1^{\epsilon_1} \cdots x_i^{\epsilon_i} x_{i+1}^{\varepsilon_{i+1}} \cdots x_t^{\epsilon_t} = x_1^{\epsilon_1} \cdots x_i^{\epsilon_i} x_{i+1}^{\epsilon_{i+1}} (x_i^{\epsilon_i})^{-1} x_i^{\epsilon_i} x_{i+2}^{\epsilon_{i+2}} \cdots x_t^{\epsilon_t}$$

Como $H_1 \trianglelefteq G$ entonces $x_i^{\epsilon_i} x_{i+1}^{\epsilon_{i+1}} (x_i^{\epsilon_i})^{-1} \in H_1$. Si $x_{i+2}^{\epsilon_{i+2}} \dots x_t^{\epsilon_t}$ están todos en H_2, entonces tendremos que $x = x_1' x_2'$, con $x_1' := x_1^{\epsilon_1} \cdots x_i^{\epsilon_i} x_{i+1}^{\epsilon_{i+1}} (x_i^{\epsilon_i})^{-1} \in H_1$ y $x_2' := x_i^{\epsilon_i} x_{i+2}^{\epsilon_{i+2}} \cdots x_t^{\epsilon_t} \in H_2$. En caso contrario repetimos lo anterior máximo hasta t. De esto obtenemos que $\langle H_1 \cup H_2 \rangle \subseteq H_1 H_2$.

Supóngase que $\langle H_1 \cup \cdots \cup H_{n-1} \rangle = H_1 \cdots H_{n-1}$. Nótese que $\langle H_1 \cup \cdots \cup H_n \rangle = \langle K \cup H_n \rangle$, con $K = \langle H_1 \cup \cdots \cup H_{n-1} \rangle$, además, $K \trianglelefteq G$ ya que $gH_1 \cdots H_{n-1} g^{-1} = gH_1 g^{-1} gH_2 g^{-1} g \cdots gH_{n-1} g^{-1} = H_1 \cdots H_{n-1}$.

De acuerdo con el paso $n = 2$ y con la hipótesis de inducción, $\langle H_1 \cup \cdots \cup H_n \rangle = K H_n = H_1 \cdots H_{n-1} H_n$.

La normalidad se acaba de probar; la última afirmación de la proposición es evidente ya que $\bigcup_{i=1}^n H_i = \bigcup_{i=1}^n H_{\pi(i)}$. □

Teorema 7.4.2. *Sean G un grupo y $H_1, \dots, H_n$ subgrupos normales de G. Las siguientes condiciones son equivalentes:*

(i) *Para cada $1 \leq j \leq n$, $H_j \cap (H_1 \dots H_{j-1} H_{j+1} \dots H_n) = 1$.*

(ii) *Cada elemento x de $H_1 \cdots H_n$ tiene una representación única en la forma:*

$$x = h_1 \cdots h_n, \quad h_i \in H_i, \quad 1 \leq i \leq n.$$

Demostración. (i) ⇒ (ii): sea $x \in H_1 \cdots H_n$. Por hipótesis x tiene una representación en la forma

$$x = h_1 \cdots h_n,\ h_i \in H_i, 1 \leq i \leq n.$$

Sean $h_i' \in H_i$, $1 \leq i \leq n$, tales que

$$\begin{aligned} x = h_1 \cdots h_n = h_1' \cdots h_n' &\Rightarrow (h_1'^{-1} h_1) h_2 \cdots h_n = h_2' \cdots h_n' \\ &\Rightarrow h_1'^{-1} h_1 = (h_2' \cdots h_n')(h_2 \cdots h_n)^{-1} \in H_2 \cdots H_n \Rightarrow \\ &h_1'^{-1} h_1 = 1 \Rightarrow h_1' = h_1 \Rightarrow h_2 h_3 \cdots h_n = h_2' h_3' \cdots h_n'. \end{aligned}$$

Procediendo de manera análoga encontramos que $h_i = h_i'$ para cada $1 \leq i \leq n$.

(ii) ⇒ (i): sea $x \in H_j$, j fijo. Supóngase que $x \in H_1 \cdots H_{j-1} H_{j+1} \cdots H_n$, entonces existen $x_1 \in H_1, \dots, x_{j-1} \in H_{j-1}$, $x_{j+1} \in H_{j+1}, \dots, x_n \in H_n$ tales que $x = x_1 \cdots x_{j-1} 1 x_{j+1} \cdots x_n$. El elemento x se puede representar también como $x = 1 \cdots 1 x 1 \cdots 1$, luego $x_1 = 1, \dots, x_{j-1} = 1, x = 1, \dots, x_n = 1$, de donde $H_j \cap (H_1 \cdots H_{j-1} H_{j+1} \dots H_n) = 1$. □

Definición 7.4.3. *Se dice que el grupo G es **suma directa interna** de los subgrupos normales $H_1, \dots, H_n$ si:*

(i) $G = H_1 \cdots H_n$

(ii) *Se cumple una cualquiera de las condiciones del teorema anterior.*

Dicha relación entre G y los subgrupos $H_1, \ldots, H_n$ se denota por $G = \sum_{i=1}^{n} \oplus H_i = H_1 \oplus \cdots \oplus H_n$.

Proposición 7.4.4. *Sea $\{G_i\}_{i=1}^n$ una colección finita de grupos, y sea $G = G_1 \times \cdots \times G_n$ su producto cartesiano. Sea*

$$G_i' := \mu_i(G_i) = \{(1, \ldots, x, \ldots, 1) \mid x \in G_i\}$$

la imagen de G_i mediante la inyección canonica μ_i. Entonces, G es suma directa interna de los subgrupos G_i',

$$G = G_1' \oplus \cdots \oplus G_n'.$$

Además $G_i' \cong G_i$, $1 \leq i \leq n$.

Demostración. Claramente $G_i' \trianglelefteq G$ para cada $1 \leq i \leq n$. Además, cada elemento $x = (x_1, \ldots, x_n)$ de G tiene la representación única

$$x = (x_1, 1, \ldots, 1) \cdots (1, \ldots, 1, x_n).$$

Por ser μ_i inyectivo se tiene que $G_i' \cong G_i$. □

Ejemplo 7.4.5. (i) Sea $M_2(\mathbb{R})$ el grupo aditivo de las matrices cuadradas reales de orden 2. Sean

$$M_{11} := \begin{pmatrix} \mathbb{R} & 0 \\ 0 & 0 \end{pmatrix} = \{A = (a_{ij}) \mid a_{ij} = 0 \text{ para } i \neq 1 \text{ y } j \neq 1.\},$$
$$M_{12} := \begin{pmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{pmatrix}, \quad M_{21} := \begin{pmatrix} 0 & 0 \\ \mathbb{R} & 0 \end{pmatrix}, \quad M_{22} := \begin{pmatrix} 0 & 0 \\ 0 & \mathbb{R} \end{pmatrix}.$$

Entonces, $M_2(\mathbb{R}) = M_{11} \oplus M_{12} \oplus M_{21} \oplus M_{22}$.

(ii) Sea $\mathbb{C}$ el grupo aditivo de los números complejos, y sean $\mathbb{R}$ y $i\mathbb{R}$ los subgrupos de números reales e imaginarios, respectivamente. Entonces $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$.

(iii) Sea $V = \{1, a, b, ab\}$, $a^2 = 1 = b^2$, $ab = ba$ el grupo de Klein; V es suma directa de los subgrupos $\langle a \rangle$ y $\langle b \rangle$ ya que ambos son normales en V y además $\langle a \rangle \cap \langle b \rangle = 1$; luego, $V = \langle a \rangle \oplus \langle b \rangle$.

(iv) Cada grupo G se puede descomponer trivialmente en suma directa interna: $G = G \oplus 1$. Hay grupos para los cuales esta es la única descomposición posible. Consideremos el grupo dihédrico de grado 4, D_4 :

Los subgrupos normales de D_4 son $1, D_4, \langle f \rangle, \langle f^2 \rangle$, $K_4 = \{1, f^2, g, f^2 g\}$, $H_4 = \{1, f^2, fg, f^3 g\}$. Si D_4 es suma directa de dos de sus subgrupos normales entonces se presentan las siguientes posibilidades:

$$G = 1 \oplus D_4,\ \langle f \rangle \oplus \langle f^2 \rangle, \quad \langle f^2 \rangle \oplus K_4,\ \langle f^2 \rangle \oplus H_4.$$

Sólo la primera posibilidad tiene lugar ya que $\langle f\rangle \cap \langle f^2\rangle \neq 1$, $\langle f^2\rangle \cap K_4 \neq 1$, $\langle f^2\rangle \cap H_4 \neq 1$.

(v) Nótese que si un grupo G no se puede descomponer en suma directa de dos subgrupos no triviales entonces no se puede descomponer en suma directa de 3 o más subgrupos no triviales.

(vi) Sea $G = G_1 \times G_2 \times \cdots \times G_n$ y sea $A_i \trianglelefteq G_i$, $1 \leq i \leq n$. Entonces $A := A_1 \times \cdots \times A_n \trianglelefteq G$: sea $x = (x_1 \dots x_n) \in G$ y sea $a = (a_1 \dots a_n) \in A$. Entonces

$$x^{-1}ax = (x_1^{-1}a_1x_1, \cdots ., x_n^{-1}a_nx_n) \in A.$$

El resultado anterior podemos generalizarlo: sea $G = \prod_{i\in I} G_i$, y sea $A_i \trianglelefteq G_i$, $i \in I$. Si $A := \prod_{i\in I} A_i$, entonces $A \trianglelefteq G$.

7.5. Ejercicios

1. Pruebe que S_3 sólo tiene la descomposición trivial $S_3 = 1 \oplus S_3$.

2. Sea $G := G_1 \times \cdots \times G_n$. Demuestre que $Z(G) = Z(G_1) \times \cdots \times Z(G_n)$. Extienda este resultado a una familia cualquiera de grupos, es decir, pruebe que $Z(\prod_{i\in I} G_i) = \prod_{i\in I} Z(G_i)$.

3. Sea $G := G_1 \times \cdots \times G_n$ y sean $H_i \leq G_i$, $1 \leq i \leq n$. Sea $H := H_1 \times \cdots \times H_n$. Demuestre que

$$N_G(H) = N_{G_1}(H_1) \times \cdots \times N_{G_n}(H_n).$$

   Extienda este resultado a una familia cualquiera de grupos.

4. Sean G y H grupos finitos cuyos órdenes son primos relativos. Pruebe que $Aut(G \times H) \cong Aut(G) \times Aut(H)$.

5. ¿ Es cierto que la única descomposición de Q_8 es la trivial: $Q_8 = 1 \oplus Q_8$?

6. Calcule $Aut(D_n)$ y demuestre que $|Aut(D_n)| = \phi(n)n$, para $n \geq 3$, ϕ denota la ***función de Euler*** que calcula los enteros positivos menores que n y primos relativos con él.

   Solución. $D_n = \{1, f, f^2, \dots, f^{n-1}, g, fg, f^2g, \dots, f^{n-1}g\}$, y además $f^n = 1$, $g^2 = 1$, $gf = f^{-1}g = f^{n-1}g$.

   Sean

$$\mathcal{A} := \langle f\rangle,\ \mathcal{B} := \{g, fg, f^2g, \dots, f^{n-1}g\},$$

$$F := \{\mu \in Aut(D_n) \mid \mu(f) = f\} \text{ y } G := \{\mu \in Aut(D_n) \mid \mu(g) = g\}.$$

La solución implica realizar varios pasos.

a) En primer lugar nótese que F y G son subgrupos de $Aut(D_n)$.

b) Si $\mu \in Aut(D_n)$, entonces, $\mu(\mathcal{A}) = \mathcal{A}$ y $\mu(\mathcal{B}) = \mathcal{B}$: puesto que todo elemento de $\mathcal{B}$ es de orden 2 y el orden de $\mu(f)$ es n, entonces $\mu(f)$ es un generador de $\mathcal{A}$, es decir, $\mu(\mathcal{A}) = \mathcal{A}$. Como μ es inyectivo, entonces $\mu(\mathcal{B}) = \mathcal{B}$.

c) F es un subgrupo normal de $Aut(D_n)$: sea $\mu \in Aut(D_n)$ y $\phi \in F$. Entonces, $\mu(\mathcal{A}) = \mathcal{A}$ y $\phi|_{\mathcal{A}} = i_{\mathcal{A}}$. Para f se tiene que $\mu \circ \phi \circ \mu^{-1}(f) = \mu \circ \phi(\mu^{-1}(f)) = \mu(\mu^{-1}(f)) = f$, es decir, $\mu \circ \phi \circ \mu^{-1} \in F$.

d) Es claro que $F \cap G = \{i_{D_n}\}$.

e) Como $F \trianglelefteq Aut\ D_n$, entonces $FG \leq Aut\ D_n$. Además, $|FG| = |F|\,|G|$. En efecto, ya que $F \cap G = \{i_{D_n}\}$, cada elemento de FG se puede representar en forma única en la forma xy, con $x \in F$ y $y \in G$. El número de tales elementos es claramente $|F|\,|G|$.

f) $|G| = \varphi(n)$: sea J el conjunto de generadores de $\mathcal{A}$, sabemos entonces que $|J| = \varphi(n)$. Vamos a probar que $|J| = |G|$. Sea $\mu \in G$, entonces $\mu(f)$ debe ser un generador de $\mathcal{A}$, es decir, $\mu(f) \in J$. Así pues, definimos

$$\begin{aligned} G &\to J \\ \mu &\mapsto \mu(f) \end{aligned}$$

Si $\mu_1(f) = \mu_2(f)$ entonces $\mu_1 = \mu_2$ ya que $\mu_1(g) = g = \mu_2(g)$. Veamos finalmente que la asignación que estamos haciendo es sobre: sea k primo relativo con n y menor que n, de tal forma que $f^k \in J$. Definimos la función μ por $\mu(f^r g^s) := f^{kr} g^s$, con $0 \leq r \leq n-1$, $s = 0, 1$. Veamos que μ es un automorfismo. En efecto, primero veamos que μ es un homomorfismo: $\mu(f^r g^s f^p g^q) = \mu(f^{r+p} g^q)$ si $s = 0$, y en este caso $\mu(f^{r+p} g^q) = f^{kr+kp} g^q = f^{kr} g^s f^{kp} g^q$ es decir, $\mu(f^r g^s f^p g^q) = \mu(f^r g^s)\mu(f^p g^q)$. Para $s = 1$ se tiene que

$$\mu(f^r g^s f^p g^q) = \mu(f^{r-p} g^{s+q}) = f^{kr} f^{-kp} g^s g^q = f^{kr} g^s f^{kp} g^q,$$

es decir, $\mu(f^r g^s f^p g^q) = \mu(f^r g^s)\mu(f^p g^q)$. Teniendo en cuenta que $\langle f \rangle \cap \langle g \rangle = 1$, entonces μ es claramente inyectiva y por lo tanto biyectiva. Entonces μ es la preimagen buscada ya que $\mu(f) = f^k$ y $\mu \in G$ por ser $\mu(g) = g$.

g) $|F| = n$. Sea $\mu \in F$, según la parte b) $\mu(g)$ debe ser un elemento de $\mathcal{B}$, digamos, $\mu(g) = f^k g$, con $0 \leq k \leq n-1$. Así pues cada elemento $\mu \in F$ determina un único elemento $f^k g \in \mathcal{B}$, es decir, definimos

$$\begin{aligned} F &\to \mathcal{B} \\ \mu &\mapsto \mu(g) \end{aligned}$$

Si $\mu_1(g) = \mu_2(g)$ entonces $\mu_1 = \mu_2$ ya que $\mu_1(f) = f = \mu_2(f)$. Veamos finalmente que la asiganción que estamos haciendo es sobre: sea $f^k g \in \mathcal{B}$, con $0 \leq k \leq n-1$, definimos la función μ por $\mu(f^r g^s) := f^{r+ks} g^s$, con $0 \leq r \leq n-1$, $s = 0, 1$. μ es un automorfismo: primero veamos que μ es un homomorfismo, $\mu(f^r g^s f^p g^q) = \mu(f^{r+p} g^q)$ si $s = 0$, y en este caso $\mu(f^{r+p} g^q) = f^{r+p+kq} g^q = f^{r+ks} g^s f^{p+kq} g^q$, es decir, $\mu(f^r g^s f^p g^q) = \mu(f^r g^s)\mu(f^p g^q)$. Cuando $s = 1$, se tiene que $\mu(f^r g^s f^p g^q) = \mu(f^{r-p} g^{s+q})$. Consideremos los dos casos posibles, $q = 0$: entonces

$$\begin{gathered} \mu(f^r g^s f^p g^q) = f^{r-p+ks} g^s = f^{r+ks} f^{-p} g^s = \\ = f^{r+ks} g^s f^p = f^{r+ks} g^s f^{p+kq} g^q = \mu(f^r g^s)\mu(f^p g^q). \end{gathered}$$

Si $q = 1$, entonces $\mu(f^r g^s f^p g^q) = \mu(f^{r-p}) = f^{r-p}$, por el otro lado, $\mu(f^r g^s)\mu(f^p g^q) = f^{r+k} g f^{p+k} g = f^{r+k-p-k} = f^{r-p}$. Al igual que el punto f), $\langle f \rangle \cap \langle g \rangle = 1$, luego μ es claramente inyectiva y por lo tanto biyectiva. Entonces μ es la preimagen buscada ya que $\mu(g) = f^k g$ y $\mu \in F$ debido a que $\mu(f^r) = f^r$, para cada $0 \leq r \leq n-1$.

h) Se tiene que $|FG| = |F|\,|G| = n\varphi(n)$. De otra parte, si $\mu \in Aut(D_n)$, entonces por b) $\mu(f)$ debe ser un generador de $\mathcal{A}$ y $\mu(g) \in \mathcal{B}$, esto hace que $|Aut(D_n)| \leq \varphi(n)n$. Como se probó en e), FG es un sugrupo de $Aut(D_n)$ y en consecuencia $FG = Aut(D_n)$ y $|Aut(D_n)| = \varphi(n)n$.

Si G fuera subgrupo normal de $Aut(D_n)$ entonces $Aut(D_n)$ sería suma directa interna de F y G. Pero G no es un subgrupo normal de $Aut(D_n)$: en efecto, según f) y g) las siguientes funciones son elementos de G y F, respectivamente: $\phi(f) = f^k$, $\phi(g) = g$, $\theta(f) = f$, $\theta(g) = fg$, donde k es primo relativo con n y distinto de 1. Esta última condición se da ya que $n \geq 3$. Entonces, $\theta\phi\theta^{-1}(g) = \theta\phi(f^{n-1} g) = \theta(f^{-k} g) = f^{-k+1} g$. Es decir, $\theta\phi\theta^{-1} \notin G$, con lo cual G no es un subgrupo normal de $Aut(D_n)$.

Entonces, ¿qué es $Aut(D_n)$ respecto de F y G?

i) Sean G_1 y G_2 grupos y μ un homomorfismo de G_2 en $Aut(G_1)$; en el conjunto $G_1 \times G_2$ definimos la operación $\times_\mu$, así: $(a, b) \times_\mu (c, d) = (a\mu(b)(c), bd)$. Entonces, $G_1 \times G_2$ con esta operación es un grupo y recibe el nombre de ***producto semidirecto*** de G_1 y G_2 con respecto a μ. Para el producto corriente de grupos en calidad de μ se toma el homomorfismo trivial que asigna a cada elemento de G_2 el automorfismo idéntico.

j) Sea G un grupo con M y N subgrupos de G tal que M es normal en G. Si $M \cap N = \{1\}$ y $MN = G$, G es isomorfo al producto semidirecto de M y N mediante el homomorfismo $\mu : N \to Aut(M)$ dado por: $\mu(n)(m) = nmn^{-1}$. En efecto, como $G = MN$, entonces todo elemento $g \in G$ se puede escribir en la forma $g = mn$, $m \in M$, $n \in N$ y de manera única ya que $M \cap N = \{1\}$. Definimos $f : G \to M \times_\mu N$, de la siguiente manera: $f(g) := f(mn) = (m, n)$; f está bien definida y es obviamente biyectiva. Veamos que f es un homomorfismo: sea $g_1 = m_1n_1$, $g_2 = m_2n_2$ elementos de G, entonces $g_1g_2 = (m_1n_1)(m_2n_2) = m_1(n_1m_2n_1^{-1})n_1n_2 = m_1\mu(n_1)(m_2)n_1n_2$, donde $m_1\mu(n_1)m_2 \in M$ y $n_1n_2 \in N$. Así pues, $f(g_1g_2) = f(m_1\mu(n_1)(m_2)n_1n_2) = (m_1\mu(n_1)(m_2), n_1n_2) = (m_1, n_1) \times_\mu (m_2, n_2) = f(g_1) \times_\mu f(g_2)$.

k) De los puntos anteriores tenemos que $Aut(D_n) \cong F \times_\mu G$, mediante el homomorfismo $\mu : G \to Aut(F)$ dado por $\mu(y)(x) = y \circ x \circ y^{-1}$.

l) Una última observación. De manera más sencilla se define la ***suma semidirecta interna*** de dos subgrupos de un grupo de la siguiente forma: sea G un grupo y M, N subgrupos de G. Se dice que G es suma semidirecta interna de M y N (en ese orden) si: M es normal en G, $M \cap N = \{1\}$ y $G = MN$. Uno podría entonces obviar los pasos i), j) y k) y decir simplemente que $Aut(D_n)$ es la suma semidirecta interna de F y G.

Capítulo 8

G-conjuntos

Como fundamento teórico para la demostración de los teoremas de Sylow aparece el concepto de acción de un grupo sobre un conjunto. Esta noción tiene bastante analogía con el de operación binaria externa y será tratada en el presente capítulo. Se estudiará en particular la acción de conjugación. Además, serán definidos los grupos transitivos del grupo simétrico S_n. De vital importancia para la demostración de los teoremas de Sylow es la ecuación de clases, la cual estableceremos en este capítulo. Un tratamiento completo de los G-conjuntos nos llevará a la teoría de los espacios vectoriales y módulos sobre anillos. Nosotros nos limitaremos a utilizar los G-conjuntos como lenguaje y herramienta para comprender mejor la teoría de Sylow.

8.1. Acción de grupos sobre conjuntos

En esta sección se establece la equivalencia entre los conceptos de representación de un grupo en un grupo de permutaciones y el concepto de acción de un grupo sobre un conjunto.

Definición 8.1.1. *Sean X un conjunto y $(G, ., 1)$ un grupo. Se dice que el grupo G actua sobre el conjunto X, si existe una función*

$$\phi : G \times X \to X \ , \ \phi(g, x) := gx$$

tal que

(i) $\phi(gh, x) = (gh)x = g(hx) = \phi(g, \phi(h, x))$

(ii) $\phi(1, x) = 1x = x$,

para cualesquiera elementos g, h de G y cualquier elemento x de X.

Se dice también que X es un G-***conjunto*** o que X tiene a G como grupo de operadores.

Estrechamente relacionado con el concepto de G-conjunto aparece el concepto de representación de un grupo.

Definición 8.1.2. *Sea X un conjunto no vacío, $S(X)$ el grupo de permutaciones de X y sea $(G, ., 1)$ un grupo. Por* ***representación*** *de G en $S(X)$ se entiende cualquier homomorfismo*

$$\Phi : G \to S(X).$$

Proposición 8.1.3. *Sea $(G, ., 1)$ un grupo y sea X un conjunto no vacío arbitrario. Entonces, cada representación de G en $S(X)$ determina una acción de G sobre X, es decir, convierte a X en un $G-$conjunto. Recíprocamente, cada estructura de $G-$conjunto sobre X determina una representación de G en $S(X)$.*

Demostración. Sea $\Phi : G \to S(X)$ una representación de G en $S(X)$. Definamos la función

$$\begin{aligned} \phi : G \times X &\to X \\ (g, x) &\longmapsto \phi(gx) =: \Phi_g(x), \end{aligned}$$

donde Φ_g denota la imagen de g mediante el homomorfismo Φ.

Se debe probar que para cualesquiera elementos $g, h \in G$ y cualquier elemento $x \in X$, $(gh)x = g(hx)$ y $1x = x$, donde 1 es el elemento identidad del grupo G.

$$\begin{aligned} (gh)x = \Phi_{gh}(x) &= \Phi(gh)(x) = (\Phi(g) \circ \Phi(h))(x) \\ &= (\Phi_g \circ \Phi_h)(x) = \Phi_g[\Phi_h(x)] = \Phi_g(hx) \\ &= g(hx). \\ 1x = \Phi_1(x) &= I_{S(X)}(x) = x. \end{aligned}$$

Sea ahora $\phi : G \times X \to X$ una función que define una estructura de $G-$conjunto sobre X. Denotemos la imagen de la pareja (g, x) mediante ϕ por gx. La función

$$\Phi : G \to S(X)$$

definida por $\Phi(g) = \Phi_g$, donde $\Phi_g(x) := gx$, $\forall x \in X$, es un homomorfismo. En efecto,

$$\begin{aligned} \Phi(gh) = \Phi_{gh},\ \Phi_{gh}(x) = (gh)x = g(hx) = g(\Phi_h(x)) = \Phi_g[\Phi_h(x)] \\ = (\Phi_g \circ \Phi_h)(x); \Rightarrow \Phi_{gh} = \Phi_g \circ \Phi_h, \text{es decir, } \Phi(gh) = \Phi(g) \circ \Phi(h). \end{aligned}$$

□

Definición 8.1.4. *Sea $\phi : G \times X \to X, \phi(g,x) = gx$, una acción del grupo G sobre el conjunto X y sea $\Phi : G \to S(X),\ \Phi(g) = \Phi_g,\ \Phi_g(x) = gx$, la representación de G en $S(X)$ asociada a ϕ. Se denomina* ***núcleo*** *de la acción ϕ y se denota por* $\ker(\phi)$ *al núcleo del homomorfismo Φ:*

$$\ker(\phi) =: \ker(\Phi) = \{g \in G \,|\, gx = x, \forall x \in X\}.$$

Se dice que G actua ***efectivamente*** *sobre X si* $\ker(\phi) = 1$, *es decir, $gx = x, \forall x \in X$ si, y sólo si, $g = 1$.*

Directamente de la definición de acción de un grupo sobre un conjunto se desprenden las siguientes propiedades.

Proposición 8.1.5. *Sea X un $G-$conjunto. Entonces,*

(i) *$X^k = X \times \cdots \times X$ es un $G-$conjunto.*

(ii) *2^X es un $G-$conjunto, donde 2^X denota el conjunto de partes del conjunto X.*

(iii) *Sea $Y \subseteq X$ y sea $C(Y) := \{Z \subseteq X \,|\, Card(Z) = Card(Y)\}$. Entonces $C(Y)$ es un $G-$conjunto.*

Demostración. Ejercicio para el lector. □

8.2. Órbitas y subgrupos estacionarios

Proposición 8.2.1. *Supóngase que G actua sobre el conjunto X. En X se define la relacion $\sim$ por*

$$x \sim y \Leftrightarrow \exists g \in G : gx = y.$$

*$\sim$ es de equivalencia en X. La clase de equivalencia del elemento x se denota por $G(x)$ y se llama la $G-$**órbita** determinada por x. Para cada $x \in X$*

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

Al $Card(G(x))$ se le denomina la ***longitud*** *de la $G-$órbita determinada por x.*

Demostración. Ejercicio para el lector. □

Proposición 8.2.2. *Sea X un $G-$conjunto y sea x un elemento de X. Se denomina* ***subgrupo estacionario*** *del punto x en G y se denota por G_x al subgrupo de elementos de G que dejan fijo x*

$$G_x =: \{g \in G : gx = x\}$$

Además, $Card(G(x)) = |G : G_x|$.

Demostración. Sean $g, h \in G_x$. Entonces $gx = x,\ hx = x$, luego $hgx = hx = x$, es decir, $hg \in G_x$; $g^{-1}x = g^{-1}(gx) = x$, con lo cual $g^{-1} \in G_x$. Denotemos por A el conjunto de clases laterales izquierdas determinadas por el subgrupo estacionario G_x en G. La correspondencia

$$\Phi : G(x) \to A,$$

definida por $\Phi(gx) = gG_x$ es una biyección. En efecto, $\Phi(gx) = \Phi(hx) \Rightarrow gG_x = hG_x \ \Rightarrow g^{-1}h \in G_x \Rightarrow g^{-1}hx = x \ \Rightarrow gx = hx$; Φ es evidentemente sobre. □

Corolario 8.2.3. *Sea X un $G-$conjunto, con G un grupo finito. Entonces, la longitud de cualquier $G-$órbita divide al orden de G, $|G(x)|\,||G|$.*

Demostración. Consecuencia directa de la proposición anterior y del teorema de Lagrange. □

Proposición 8.2.4. *Sea G un grupo que actua sobre el conjunto X.*

(i) *Si x, y están en la misma órbita entonces sus grupos estacionarios son conjugados:*

$$y = gx \ \Rightarrow G_y = gG_xg^{-1}$$

(ii) *Si G es un grupo finito y $X = X_1 \cup \cdots \cup X_r$ es la partición de X en un número finito de r órbitas con representantes $x_1, \cdots, x_r$, entonces*

$$|X| = \sum_{i=1}^{r} |G : G_{x_i}| \ \ (\textbf{\textit{Ecuación de clases}}).$$

Demostración. (i) $h \in G_y \Leftrightarrow hy = y \Leftrightarrow hgx = gx \Leftrightarrow g^{-1}hgx = x \Leftrightarrow g^{-1}hg \in G_x \Leftrightarrow h \in gG_xg^{-1}$

(ii) La segunda afirmación de la proposición es debido a que G es finito. En efecto, si G es finito entonces para cada $x \in X$, G_x es también finito, con lo cual $|G : G_x|$ es finito y así cada $G(x_i) = X_i$ es finito. Como $X_1 \cup \cdots \cup X_r$ es una partición de X entonces la ecuación de clases se cumple. □

Algunos de los conceptos estudiados anteriormente como centro, centralizador, normalizador, etc., pueden ser vistos como consecuencia de acciones de grupos sobre conjuntos.

Ejemplo 8.2.5. ***Acción de conjugación.*** Sea G un grupo cualquiera y consideremos la acción de G sobre si mismo, es decir, con $X = G$, definida por:

$$\begin{gathered} \phi : G \times G \to G \\ (g, x) \longmapsto gxg^{-1} \end{gathered}$$

Notemos que el núcleo de ϕ es el centro del grupo G:

$$\begin{aligned}\ker(\phi) &= \{g \in G \,|\, gxg^{-1} = x,\ \forall x \in G\} \\ &= \{g \in G \,|\, gx = xg,\ \forall x \in G\} = Z(G).\end{aligned}$$

Sea x un elemento cualquiera de G. La órbita $G(x)$ del elemento x, en este caso denotada por x^G, se denomina la clase de ***elementos conjugados*** con x:

$$x^G = \{gxg^{-1} \,|\, g \in G\}.$$

Nótese que G ha sido particionado en clases conjugadas. Decir que dos elementos $x, y \in G$ son conjugados significa que están en una misma clase (de equivalencia) conjugada, es decir, existe $g \in G$ tal que $y = gxg^{-1}$. Sea x un elemento cualquiera de G. El subgrupo estacionario de x se denomina en este caso el ***centralizador*** de x en G:

$$C_G(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}.$$

Según la proposición 8.1.5, la acción de conjugación puede ser extendida a los subconjuntos del grupo G. Sean A, B subconjuntos de G. Decimos que A y B son conjugados si existe $g \in G$ tal que $B = gAg^{-1}$. Notemos que cuando A es un subgrupo de G entonces gAg^{-1} es también un subgrupo de G, es decir, la acción de conjugación a subconjuntos de G puede ser restringida a subgrupos de G. En este caso, dado un subgrupo H de G la órbita de H, H^G, está constituida por los subgrupos de G que son conjugados con H:

$$H^G = \{gHg^{-1} : g \in G\}.$$

Además, el subgrupo estacionario en este caso coincide con el ***normalizador*** de H en G:

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

Nótese que $Card(H^G) = |G : N_G(H)|$, es decir, el número de subgrupos conjugados de un subgrupo H de G es igual al índice de su normalizador en G.

Ejemplo 8.2.6. Generalización del Teorema de Cayley. Sea G un grupo y H un subgrupo cualquiera de G. Denotemos por G/H el conjunto de clases laterales izquierdas determinadas por H en G. La aplicación definida por

$$\begin{aligned}\phi : G \times G/H &\to G/H \\ (x,\ gH) &\longmapsto xgH,\end{aligned}$$

determina una acción de G en G/H. Notemos en primer lugar que ϕ es una función: sean $gH = hH \Rightarrow g^{-1}h \in H \Rightarrow g^{-1}x^{-1}xh \in H \Rightarrow xgH = xhH$. Además, $(1, gh) \to 1gH = gH$, y también, $(xy) \cdot (gH) = (xy)gH = x(yg)H = x \cdot (y \cdot (gH))$.

Determinemos el núcleo de ϕ:

$$\begin{aligned}\ker(\phi) &= \{x \in G \,|\, xgH = gH,\ \forall g \in G\} \\ &= \{x \in G \,|\, g^{-1}xgH = H,\ \forall g \in G\};\end{aligned}$$

de aquí obtenemos que

$$x \in \ker(\phi) \Leftrightarrow g^{-1}xg \in H,\ \forall g \in G \Leftrightarrow x \in gHg^{-1},\ \forall g \in G,$$

es decir,

$$\ker(\phi) = \bigcap_{g\in G} gHg^{-1} = \text{Intersección de los subgrupos de } G \text{ conjugados con } H.$$

Demostremos que

$\bigcap_{g\in G} gHg^{-1}$ es el subgrupo normal más grande de G que está contenido en H

En efecto, sea

$$x \in \bigcap_{g\in G} gHg^{-1}$$

Se desea probar que para cada elemento $w \in G$

$$wxw^{-1} \in \bigcap_{g\in G} gHg^{-1},$$

es decir, que $\forall g \in G,\ wxw^{-1} \in gHg^{-1}$. Sea g un elemento cualquiera de G, entonces: $x \in w^{-1}gHg^{-1}w = (w^{-1}g)H(w^{-1}g)^{-1} \Rightarrow x = w^{-1}ghg^{-1}w,$ con $h \in H, \Rightarrow wxw^{-1} = ghg^{-1}, \Rightarrow wxw^{-1} \in gHg^{-1}$. Claramente,

$$\bigcap_{g\in G} gHg^{-1} \subseteq 1H1^{-1} = H.$$

Sea $K \trianglelefteq G,\ K \leq H \ \Rightarrow$ para cada $g \in G, K = gKg^{-1} \subseteq gHg^{-1} \ \Rightarrow K \subseteq \bigcap_{g\in G} gHg^{-1}$.

La acción ϕ determina desde luego una representación del grupo G en $S(G/H)$:

$$\begin{gathered}\Phi : G \to S(G/H) \\ \Phi(x) \longmapsto \Phi_x \\ \Phi_x : G/H \to G/H \\ gH \longmapsto xgH.\end{gathered}$$

Tomando $H = \{1\}$ la función Φ es precisamente el isomorfismo del teorema de Cayley. Nótese que cuando $H \neq \{1\}$ y $\ker(\phi) = \ker(\Phi) = \{1\}$, G no es tan "pequeño" con respecto a $S(G/H)$ como en el teorema de Cayley.

De este segundo ejemplo se obtiene el siguiente resultado:

Proposición 8.2.7. *Sea G un grupo finito y sea $H \leq G$ un subgrupo de G tal que $|G|$ no divide a $|G : H|!$. Entonces, H contiene un subgrupo normal no trivial de G. En consecuencia, G no es simple.*

Demostración. Supóngase que el único subgrupo normal de G contenido en H es $\{1\}$. Esto indica que

$$\ker(\phi) = \bigcap_{g \in G} gHg^{-1} = \ker(\Phi) = \{1\}.$$

Por lo tanto Φ es $1-1$ y así G es isomorfo a un subgrupo de $S(G/H)$. De aquí se obtiene que $|G|$ divide a $|G : H|!$. □

8.3. Grupos transitivos

Se dice que el grupo G actua ***transitivamente*** sobre X si G determina en X solamente una órbita, es decir, para cada par de elementos $i, j \in X$ existe $g \in G$ tal que $gi = j$. Más generalmente, se dice que G actua $k-$ transitivamente sobre X o también que G es un grupo $k-$***transitivo*** sobre X, si para cualesquiera subconjuntos ordenados de k elementos de X $\{x_1, \ldots, x_k\}$, $\{y_1, \ldots, y_k\}$ existe $g \in G$ tal que $gx_i = y_i,\ i = 1, 2, \ldots, k$. Esto equivale a decir que G actua transitivamente sobre el conjunto $X^{[k]}$ de subconjuntos ordenados de X de k elementos.

Proposición 8.3.1. *Si G actua $k-$transitivamente sobre X, donde $k \leq |X|$, entonces G actua $s-$transitivamente sobre X para cada $s \leq k$.*

Demostración. Si $s = k$ entonces no hay nada que probar. Sea $s < k$ y $\{x_1, \ldots, x_s\}$ y $\{y_1, \ldots, y_s\}$ subconjuntos ordenados de X de s elementos. Sean $\{x_{s+1}, \ldots, x_k\} \subseteq X \backslash \{x_1, \ldots, x_s\}$ y $\{y_{s+1}, \ldots, y_k\} \subseteq X \backslash \{y_1, \ldots, y_s\}$. Consideremos los conjuntos ordenados $\{x_1, \ldots, x_s, x_{s+1}, \ldots, x_k\}$ y $\{y_1, \ldots, y_s, y_{s+1}, \ldots, y_k\}$. Como G es $k-$transitivo entonces existe $g \in G$ tal que $gx_i = y_i,\ i = 1, \ldots, s, s+1, \ldots, k$; es decir, G es $s-$transitivo. □

Proposición 8.3.2. (i) *S_n actua $n-$transitivamente sobre $I_n = \{1, 2, \cdots, n\}$.*

(ii) *A_n actua $(n-2)-$transitivamente sobre I_n.*

Demostración. (i) Sean $\{x_1, \ldots, x_n\}$ y $\{y_1, \ldots, y_n\}$ dos ordenaciones de I_n. Sean $\sigma, \rho \in S_n$ definidas por $\sigma(i) = x_i$ y $\rho(i) = y_i$. Entonces $\rho(\sigma^{-1}(x_i)) = y_i\ \forall i = 1, \ldots, n$.

(ii) Sean $\{x_1, \ldots, x_{n-2}\}$ y $\{y_1, \ldots, y_{n-2}\}$ subconjuntos ordenados de I_n. Como S_n es $n-$transitivo, entonces S_n es $(n-2)-$transitivo, es decir, existe $\sigma \in S_n$ tal que $\sigma(x_i) = y_i\ \forall i = 1, \ldots, n-2$.

Si σ es par, entonces no hay nada que probar. Supóngase que σ es impar. Sean $z_1, z_2 \in I_n \backslash \{y_1, \ldots, y_{n-2}\}$. Entonces $\Theta = (z_1 z_2)\sigma$ es par y además $\Theta(x_i) = y_i \ \ \forall i = 1, \ldots, n-2$. □

Proposición 8.3.3. *Sea $G \leq S_n$ y $I_n = \{1, 2, \cdots, n\}$. Supóngase que G actua transitivamente sobre I_n. Sea $N(g)$ el conjunto de puntos de I_n que quedan fijos bajo g, $g \in G$. Entonces,*

(i)
$$\sum_{g \in G} |N(g)| = |G|.$$

(ii) *Si G es $2-$transitivo sobre I_n entonces*
$$\sum_{g \in G} |N(g)|^2 = 2|G|.$$

Demostración. (i) Simbolicemos por G_1 el subgrupo estacionario del punto $1 \in I_n$. Sea i un elemento cualquiera de I_n, como G actua transitivamente, entonces existe $g_i \in G$ tal que $g_i(1) = i$. Se determinan así n elementos (los cuales no podemos asegurar por ahora que sean diferentes) $g_1 = i_{I_n}, \ldots, g_n$ de S_n. Considérese el conjunto cociente G/G_1 de clases laterales izquierdas determinadas por G_1 (recordemos que las clases se definen por medio de la relacion de equivalencia $g \equiv h \pmod{G_1} \Leftrightarrow g^{-1}h \in G_1$). Demostremos que

$$G = \textstyle\bigcup_{i=1}^{n} g_i G_1$$

(siendo así, podemos afirmar que los n elementos $g_1, \ldots, g_n$ son diferentes). Sea g un elemento cualquiera de G. Sea $i \in I_n$ la imagen de 1 mediante g: $g(1) = i$. Entonces

$$g(1) = i = g_i(1) \Rightarrow g_i^{-1} g(1) = 1 \Rightarrow g_i^{-1} g(1) \in G_1 \Rightarrow g \in g_i G_1$$
$$\Rightarrow G \subseteq \bigcup_{i=1}^{n} g_i G_1. \text{ Obviamente } \bigcup_{i=1}^{n} g_i G_1 \subseteq G.$$

Supóngase que para dos elementos $i, j \in I_n$ se tiene

$$g_i G_1 \cap g_j G_1 \neq \emptyset \Rightarrow g_i h = g_j g \text{ con } h, g \in G_1 \ \Rightarrow h(1) = 1 = g(1) \Rightarrow$$
$$g_i h(1) = g_i(1) = i, \ \ g_j g(1) = g_j(1) = j, \Rightarrow i = j \Rightarrow g_i G_1 = g_j G_1.$$

Esto completa la prueba de la igualdad (8.3.3).

Sea $N(g)$ el conjunto de puntos de I_n que permanecen fijos bajo g; sea $\{g\} \times N(g)$ el producto cartesiano del conjunto unitario $\{g\}$ y el conjunto $N(g)$. Nótese que para $g \neq h$, $\{g\} \times N(g) \cap \{h\} \times N(h) = \emptyset$. Es posible además que $N(g) = \emptyset$.

Sea G_j el subgrupo estacionario del punto $j \in I_n$. Considérese el producto cartesiano $G_j \times \{j\}$; como antes, para $i \neq j$ se tiene que $G_j \times \{j\} \cap G_i \times \{i\} = \emptyset$. Evidentemente

$$Card\left[(\bigcup_{g\in G})_{\emptyset}\{g\} \times N(g)\right] = Card\left[(\bigcup_{i=1}^{n})_{\emptyset} G_j \times \{j\}\right];$$

$$Card\left[(\bigcup_{i=1}^{n})_{\emptyset}\{g\} \times N(g)\right] = \sum_{g\in G} Card(\{g\} \times N(g)) =$$

$$\sum_{g\in G} |N(g)| = \sum_{j=1}^{n} Card(G_j \times \{j\}) = \sum_{j=1}^{n} |G_j|.$$

Teniendo en cuenta que $g_j(1) = j \Rightarrow g_j^{-1} G_j g_j = G_1$ (proposición 8.2.4) entonces, para cada $j \in I_n$, $|G_j| = |G_1|$. Ya que todas las clases laterales $G_1, g_2G_1, \ldots, g_nG_1$ tienen el mismo cardinal, y además utilizando (8.3.3) resulta

$$\sum_{g\in G} |N(g)| = \sum_{j=1}^{n} |G_j| = \sum_{j=1}^{n} n|G_1| = |G_1| + \cdots + |G_1| = |G_1| + |g_2G_1| + \cdots + |g_nG_1| = |G|,$$

(ii) Supóngase que el grupo G es 2−transitivo sobre I_n. Esto implica que G_1 es un grupo transitivo sobre $\hat{I}_n = I_n \backslash \{1\}$.

En efecto, sean $x, y \in \hat{I}_n$. Entonces existe $\sigma \in G$ tal que $\sigma\{x, 1\} = \{y, 1\}$, es decir, $\sigma(x) = y$ y $\sigma(1) = 1$; esto indica que $\sigma \in G_1$. (Obsérvese que G_1 determina en I_n solo dos órbitas $\{1\}$ y $\hat{I}_n$). Sea $\hat{N}(g)$ el conjunto de puntos de $\hat{I}_n$ que quedan fijos bajo $g \in G_1$. Según la parte i) de esta proposición obtenemos que

$$\sum_{g\in G_1} |\hat{N}(g)| = |G_1| \;\Rightarrow \sum_{g\in G_1} |N(g)| = \sum_{g\in G_1} (1 + |\hat{N}(g)|),$$

la última igualdad se debe a que cada $g \in G_1$, deja fijo un punto mas en I_n, el 1.

De esto obtenemos que

$$\sum_{g\in G_1} |N(g)| = \sum_{g\in G_1} 1 + \sum_{g\in G_1} |\hat{N}(g)| = |G_1| + |G_1| = 2|G_1|.$$

Analogamente, para cada $j \in I_n$ obtenemos que

$$\sum_{g\in G_j} |N(g)| = 2|G_j| = 2|G_1|,$$

Por lo tanto

$$\sum_{j=1}^{n} \sum_{g\in G_j} |N(g)| = 2n|G_1| = 2|G|.$$

Pero

$$\sum_{j=1}^{n} \sum_{g \in G_j} |N(g)| = \sum_{g \in G} |N(g)|^2.$$

□

8.4. Ejercicios

1. Demuestre la proposición 8.2.1.

Capítulo 9

Teoremas de Sylow

De fundamental importancia para el estudio de los grupos finitos son los teoremas probados por el matemático noruego Ludwig Sylow. Es conocido que para los grupos cíclicos finitos es válido el recíproco del teorema de Lagrange, es decir, si G un grupo cíclico finito de orden n y m divide a n entonces G contiene exactamente un subgrupo de orden m. En este capítulo se mostrará que la afirmación anterior es válida para grupos finitos cualesquiera pero con m una potencia de un primo. Además, la unicidad se da salvo conjugación. Los resultados de este capítulo ayudarán a describir en el próximo los grupos abelianos finitos.

9.1. p-grupos

En el capítulo 2 se definieron los principales conceptos relacionados con la parte finita de un grupo. Además, se tienen las siguientes definiciones.

(i) ***Periodo*** (***exponente***) de un grupo periódico: supóngase que el conjunto de los periodos de los elementos de un grupo periódico es acotado superiormente. Entonces el mínimo comun múltiplo de estos períodos se denomina periodo del grupo periódico G.

(ii) ***Parte periódica de un grupo abeliano***: sea G un grupo abeliano. El conjunto de elementos de G de periodo finito constituyen un subgrupo de G llamado ***subgrupo de torsión*** de G o parte periódica de G.

(iii) p***-grupos***: sea G un grupo (finito o infinito). Si cada elemento de G tiene periodo potencia del primo p, se dice que G es un $p-grupo$.

(iv) p***-subgrupo***: se dice que $H \leq G$ es un $p-subgrupo$ de G , si H es un $p-grupo$.

(v) ***Grupos primarios***: un grupo G se dice que es primario, si G es un $p-grupo$ para algún primo p. En otras palabras, la coleccion de los grupos primarios es la reunión de los $p-grupos$, donde p recorre los primos positivos.

(vi) ***Subgrupo de Sylow***: sea G un grupo. Supóngase que G contiene $p-$ *subgrupos*. Un $p-$ *subgrupo* H se denomina $p-$ *subgrupo* de Sylow de G si H es maximal entre los $p-$ *subgrupos* de G.

Ejemplo 9.1.1. Sea $(G,\cdot,1)$ un grupo abeliano y sea P el conjunto de elementos de G de periodo finito. $P\neq\emptyset$ ya que $1\in P$; sean $x,y\in P$, entonces existen $n,m\in Z^+$ tales que $x^n=1$, $y^m=1$. Sea $k=m.c.m.\ \{n,m\}\Rightarrow (x.\ y)^k=x^k.y^k=1\Rightarrow x.y\in P$; si $x\in P$ entonces claramente $x^{-1}\in P\Rightarrow P\leq G$.

Ejemplo 9.1.2. $(\mathbb{Z}_{p^n},+,0)$, con $n\geq 1$, es un p-grupo finito, $\mathbb{C}_{p^\infty}$ es un p-grupo infinito.

Ejemplo 9.1.3. Ejemplos de p-subgrupos en un grupo no abeliano: sea $GL_n(\mathbb{R})$ el grupo multiplicativo formado por las matrices reales invertibles. Podemos definir conjuntos de matrices sobre otros grupos que tienen, al igual que sobre $\mathbb{R}$, un producto. Sea $M_3(\mathbb{Z}_n)=\{A=[a_{ij}]\,|\,a_{ij}\in\mathbb{Z}_n\}$ se definen en $M_3(\mathbb{Z}_n)$ dos operaciones:

Adición: $A=[a_{ij}]$, $B=[b_{ij}]\in M_3(\mathbb{Z}_n)$ tal que $A+B=[a_{ij}+b_{ij}]$.

Multiplicación: $AB=C=[c_{ij}]$, donde $c_{ij}:=\sum_{k=1}^{3}a_{ik}b_{kj}$.

Se puede comprobar fácilmente que $(M_3(\mathbb{Z}_n),+,0)$, donde 0 es la matriz nula, es un grupo abeliano, y que $(M_3(\mathbb{Z}_n),\cdot,E)$, con E la matriz idéntica, es un monoide. Tomemos en particular $n=p$ primo y sea $GL_3(\mathbb{Z}_p)$ un grupo multiplicativo del monoide $M_3(\mathbb{Z}_n)$. Destacamos en $GL_3(\mathbb{Z}_p)$ el subconjunto $UT_3(\mathbb{Z}_p)$ definido por:

$$UT_3(,\mathbb{Z}_p):=\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\,|\,a,b,c\in\mathbb{Z}_p\right\};$$

$$UT_3(\mathbb{Z}_p)\leq GL_3(\mathbb{Z}_p)\text{: } UT_3(\mathbb{Z}_p)\neq\emptyset \text{ ya que } E\in UT_3(\mathbb{Z}_p);$$

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}^{-1}=\begin{pmatrix}1&-a&ac-b\\0&1&-c\\0&0&1\end{pmatrix},$$

por último, el producto de dos matrices de $UT_3(\mathbb{Z}_p)$ es nuevamente una matriz de este conjunto.

Nótese que $|UT_3(\mathbb{Z}_p)|=p^3$ con lo cual $UT_3(\mathbb{Z}_p)$ es un p-subgrupo de $GL_3(\mathbb{Z}_p)$, el cual no es abeliano:

$$\begin{pmatrix}1&1&1\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&1\\0&1&1\\0&0&1\end{pmatrix}\neq\begin{pmatrix}1&0&1\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}1&1&1\\0&1&0\\0&0&1\end{pmatrix}.$$

Ejemplo 9.1.4. Algunos ejemplos de grupos primarios son $\mathbb{C}_{p^\infty},\mathbb{Z}_{p^n},UT(3,\mathbb{Z}_p)$.

Ejemplo 9.1.5. Subgrupos de Sylow de $\mathbb{Z}_{72}$: 2-subgrupos: $\mathbb{Z}_1,\mathbb{Z}_2,\ \mathbb{Z}_4,\ \mathbb{Z}_8$; 2-subgrupo de Sylow : $\mathbb{Z}_8$. 3-subgrupos: $\mathbb{Z}_1,\mathbb{Z}_3,\ \mathbb{Z}_9$; 3-subgrupo de Sylow : $\mathbb{Z}_9$.

Proposición 9.1.6. *Sea G un grupo de orden p^n, con p primo y $n \geq 1$. Entonces, $Z\ (G) \neq 1$.*

Demostración. Sea G un grupo finito cualquiera y sean $x_1^G, \ldots, x_r^G$, las clases de equivalencia determinadas por la acción de conjugación :

$$G = \cup_{i=1}^{r} x_i^G, \quad x_i \in G.$$

Se tienen clases de un solo elemento (por ejemplo 1^G). Podemos reordenar los índices y suponer que las primeras q clases constan de un sólo elemento. Se afirma que $Z(G)$ $=\{x_1, \ldots, x_q\}$. En efecto, si $x \in Z(G) \ \Rightarrow gxg^{-1} = x$ para cada $g \in G \Rightarrow \ x^G = \{x\}$ $\Rightarrow \ x \in \{x_1, \ldots, x_q\}$. El recíproco es evidente.

La ecuación numérica de clases toma la forma

$$|G| = |\ Z(G)| \ + \sum_{i=q+1}^{r} |\ G : C_G(x_i)|$$

Si $\ q = r$ entonces G es abeliano y así $Z(G) = G \neq 1$. Sea pues $q < r$. Nótese que $\ |G : C_G(x_i)|\, |p^n \Rightarrow p^{n_i} = |G : C_G(x_i)|$ con $1 \leq n_i < n$, $q+1 \leq i \leq r \Rightarrow p||Z(G)|$ luego $Z(G) \neq 1$. □

Corolario 9.1.7. *Todo grupo de orden $\ p^2$ es abeliano.*

Demostración. El $Z(G)$ es de orden $1, p, p^2$. Según la proposición anterior $Z(G) \neq 1$. Supongamos que $|Z(G)| = p$. Entonces, $\ |G/Z(G)| = p \Rightarrow G/Z(G) = \langle \overline{a} \rangle, \ a \in G$. Lógicamente $\ a \notin Z(G)$, además, $Z(G) \subset C_G(a)$. Ya que $\ a \notin Z(G) \Rightarrow |C_G(a)| >$ $p \Rightarrow |C_G(a)| = p^2 \Rightarrow C_G(a) = G \Rightarrow a \in Z(G)$, lo cual es contradictorio. Luego, $|Z(G)| = p^2 \Rightarrow G$ es abeliano. □

Proposición 9.1.8. *Sean G un grupo y $P, Q \leq G$ tales que:*

(i) *P es un p-subgrupo de G.*

(ii) *P y Q son conjugados, es decir, existe $x \in G$ tal que $Q = xPx^{-1}$.*

(iii) *P normaliza Q, es decir, para cada $p \in P$, $pQp^{-1} = Q$.*

Entonces PQ es un p-subgrupo de G.

Demostración. $PQ \leq G$: sea $\ pq \in PQ \ \Rightarrow \ pqp^{-1} \in Q \ \Rightarrow pq \in QP \ \Rightarrow PQ \subseteq QP$. Análogamente, $QP \subseteq PQ$ y así $PQ = QP$.

$Q \trianglelefteq PQ$: sean $q \in Q$, $pq_0 \in PQ \ \ \Rightarrow pq_0q(pq_0)^{-1} = pq_0qq_0^{-1}p^{-1} \in Q$.

Por el teorema fundamental de isomorfismo $PQ/Q \cong P/(P \cap Q)$. Nótese que $P/(P \cap Q)$ es un p-grupo (más generalmente, si G es un p-grupo y $N \trianglelefteq G$ entonces G/N es un p-grupo : $x \in G \Rightarrow |x| = p^\alpha, \ \alpha \geq 0$; $(\overline{x})^{p^\alpha} = \overline{x^{p^\alpha}} = \overline{1} \Rightarrow |\overline{x}| \ | \, p^\alpha)$. Q es un p-grupo ya que los elementos de Q tienen el mismo orden que los elementos de P.

PQ es un p-grupo: más generalmente, si G/N es un p-grupo y N es un p-subgrupo de G, entonces G es un p-grupo : $x \in G \Rightarrow |\overline{x}| = p^{\alpha}$, con $\alpha \geq 0; \Rightarrow (\overline{x})^{p^{\alpha}} = \overline{1} \Rightarrow x^{p^{\alpha}} \in N \Rightarrow (x^{p^{\alpha}})^{p^{\beta}} = 1$ con $\beta \geq 0 \Rightarrow x^{p^{\alpha+\beta}} = 1 \Rightarrow |x| \mid p^{\alpha+\beta}$, esto completa la prueba de la afirmación. □

Proposición 9.1.9. *Sean G un grupo y H un p-subgrupo de G. Entonces, xHx^{-1} es un p-subgrupo de G para cada $x \in G$.*

Demostración. Fue probada en la demostración anterior. □

9.2. Preliminares

El siguiente ejemplo ilustra que el recíproco del teorema de Lagrange no es en general válido.

Ejemplo 9.2.1. En A_5 no hay subgrupos de orden 30, aunque $30 \mid |A_5| = 60$. Si existiera $H \leq A_5$ tal que $|H| = 30 \Rightarrow H \trianglelefteq A_5$. Pero probaremos que para cada $n \geq 5$, A_n es simple.

Proposición 9.2.2. *Para cada $n \geq 5$, A_n es simple.*

Demostración. Sea $H \trianglelefteq A_n$ y $H \neq 1$. Sea $\tau \neq 1$, $\tau \in H$. Puesto que cada permutación es producto de ciclos disyuntos entonces τ tiene alguna de las siguientes formas:

(a) En la descomposición de τ hay al menos un ciclo de longitud ≥ 4, $\tau = (\alpha_1\alpha_2\alpha_3\alpha_4\cdots)\cdots$

(b) Si en τ todos los ciclos son de longitud ≤ 3 entonces se presentan dos posibilidades :

(b1) τ es exactamente un ciclo de longitud 3 , $\tau = (\alpha_1\alpha_2\alpha_3)$.

(b2) En τ hay un ciclo de longitud 3 y otros ciclos de longitud ≤ 3 , $\tau = (\alpha_1\alpha_2\alpha_3)(\alpha_4, \alpha_5\cdots)\cdots$

(c) En τ todas los ciclos son de longitud ≤ 2, es decir, τ es producto de transposiciones (al menos 2 ya que $H \leq A_n$), $\tau = \cdots(\ \alpha_3\ \alpha_4)(\ \alpha_1\ \alpha_2)$ (si para cada $\tau \in H$ no se presenta ninguna de estas 4 formas entonces $H = 1$).

Demostraremos que la existencia en H de un elemento $\tau \neq 1$ implica la existencia en H de al menos un ciclo de longitud 3. Estudiaremos las 4 formas posibles.

(a) $\tau = (\alpha_1\alpha_2\alpha_3\alpha_4\cdots)\cdots \in H$; sea $\theta = (\alpha_1\alpha_2\alpha_3)$. Como $\theta = (\alpha_1\alpha_2)(\alpha_1\alpha_3)\cdots \in A_n$ y $H \trianglelefteq A_n$ entonces $(\theta\tau\theta^{-1})\tau^{-1} \in H$, es decir,

$(\alpha_1\alpha_2\alpha_3)(\alpha_1\alpha_2\alpha_3\alpha_4\cdots)\cdots(\alpha_3\alpha_2\alpha_1)\cdots(\cdots\alpha_4\alpha_3\alpha_2\alpha_1) = (\alpha_1\alpha_2\alpha_4) \in H$

(b1) No hay nada que probar.

(b2) $\tau = \cdots(\alpha_4\alpha_5\cdots)(\alpha_1\alpha_2\alpha_3) \in H$. Sea $\theta = (\alpha_1\alpha_2\alpha_4) \in A_n \Rightarrow \theta\tau\theta^{-1}\tau^{-1} = (\alpha_1\alpha_2\alpha_5\alpha_3\alpha_4) \in H$. Según (a), esto implica que H contiene un ciclo de longitud 3.

(c) $\tau = \cdots(\ \alpha_3\ \alpha_4)(\ \alpha_1\ \alpha_2) \in H;\ \ \theta = (\alpha_1\alpha_2\alpha_3) \in A_n\ \Rightarrow \theta\tau\theta^{-1}\tau^{-1} = (\alpha_2\alpha_4)(\alpha_1\ \alpha_3) \in H$. Puesto que $n \geq 5$ entonces $(\alpha_1\alpha_2\alpha_5\alpha_3\alpha_4) = (\alpha_1\alpha_4)(\alpha_1\alpha_3)(\alpha_1\alpha_5)(\alpha_1\alpha_2) \in A_{n,}$ de aquí resulta: $(\alpha_1\alpha_2\alpha_5\alpha_3\alpha_4)(\alpha_2\alpha_4)(\alpha_1\alpha_3)(\alpha_1\alpha_2\alpha_5\alpha_3\alpha_4)^{-1} = (\alpha_1\alpha_5)(\alpha_2\alpha_4) \in H$. Hagamos ahora el producto de estas permutaciones $(\alpha_1\alpha_5)(\alpha_4\alpha_2)(\alpha_2\alpha_4)(\alpha_1\alpha_3) = (\alpha_1\alpha_3\alpha_5) \in H$.

Queremos mostrar ahora que la contenencia en H de un ciclo de longitud 3 implica la inclusión en H de todos los 3-ciclos, con lo cual $H = A_n$. Sea pues $(\alpha_1\alpha_2\alpha_3)$ un ciclo de H. Sea $(\beta_1\beta_2\beta_3)$ un 3-ciclo cualquiera de A_n. Puesto que $n \geq 5$ entonces A_n es 3-transitivo; existe entonces $\sigma \in A_n$ tal que $\sigma(\beta_i) = \alpha_i$, $i = 1, 2, 3$. Entonces $\sigma^{-1}(\alpha_1\alpha_2\alpha_3)\sigma = (\beta_1\beta_2\beta_3) \in H$. □

Antes de probar los tres teoremas de Sylow consideremos algunos hechos elementales de la teoría de números.

Proposición 9.2.3. *Sea X un conjunto de n elementos. Entonces el número de subconjuntos diferentes de k elementos de X , $0 \leq k \leq n$, es*

$$\left(\begin{array}{c} n \\ k \end{array}\right) = \frac{n!}{(n-k)!k!}\ .$$

Demostración. Por inducción sobre n.

$n = 1$: valores de k; $k = 0$, $\left(\begin{array}{c} 1 \\ 0 \end{array}\right) = 1$; $k = 1$ $\left(\begin{array}{c} 1 \\ 1 \end{array}\right) = 1$.

Supongamos que la afirmación es cierta para conjuntos de n elementos: $X = \{x_1, x_2, \ldots, x_n\}$. Agregamos a X un nuevo elemento x_{n+1} y vemos cuántos subconjuntos de k elementos, $0 \leq k \leq n$, tiene $X' := X \cup \{x_{n+1}\}$.

Podemos considerar que la colección de subconjuntos de X' de k elementos está conformada por aquellos subconjuntos donde x_{n+1} no aparece y aquellos que contienen a x_{n+1}. Del primer tipo de subconjuntos tenemos de acuerdo a la hipótesis inductiva $\binom{n}{k}$.

Los subconjuntos del segundo tipo podemos obtenerlos de la siguiente manera. En cada uno de los $\binom{n}{k}$ subconjuntos de k elementos donde no aparece x_{n+1} podemos suprimir un elemento y en su lugar colocar x_{n+1}. Puesto que cada conjunto tiene k elementos podemos hacer con cada uno k sustituciones; en total obtenemos $k\binom{n}{k}$ conjuntos donde aparece x_{n+1}. Sin embargo, en este proceso cada conjunto aparece $n+1-k$ veces repetido (en efecto consideremos el conjunto de k elementos $\{\ x_{i_1}, \cdots, x_{i_k}\} \subset X$, quitamos por ejemplo x_{i_1} y obtenemos $\{\ x_{n+1},\ x_{i_2}, \cdots x_{i_k}\}$. El número de conjuntos iguales en este es $n-1+k$ obteniendo al cambiar x_{i_1} por los $n-k+1$ elementos restantes de $X - \{\ x_{i_1}, \cdots, x_{i_k}\}$).

Por lo tanto el número de conjuntos diferentes de k elementos donde figura x_{n+1} es $\frac{k\binom{n}{k}}{n-k+1}$. Como conclusión obtenemos que el número de conjuntos de k elementos

de X' es :

$$\binom{n}{k} + \left(\frac{k\ \binom{n}{k}}{n\ -\ k\ +1}\right) = \binom{n}{k}\left[1 + \frac{k}{n\ -\ k\ +1}\right] = \binom{n\ +1}{k}.$$

Hemos probado que el número de subconjuntos de k elementos con $0 \leq k \leq n$, de un conjunto de $n+1$ elementos es $\binom{n\ +1}{k}$.

El caso $k = n+1$ es evidentemente pues $\binom{n\ +1}{n\ +1} = 1$. □

La siguiente afirmación es clave en la demostración de los teoremas de Sylow.

Proposición 9.2.4. *Sean p primo, $m \in \mathbb{Z}^+, m.c.d.(p,m) = 1$, $r \geq 0$, $0 \leq k \leq n$. Entonces, la mayor potencia de p que divide a $\binom{p^r m}{p^k}$ es $p^{r\ -k}$.*

Demostración. Notese en primer lugar que

$$\binom{p^r m}{p^k} = \frac{p^{r\ -k}\ m(\ p^r\ m\ -\ 1)\cdots(\ p^r\ m\ -(\ p^k - 1))}{12\cdots(p^k\ -1)}$$

Consideremos el racional $\frac{p^r m\ -\ i}{i}$, con $1 \leq i \leq p^k - 1 < p^k$. Si p^j es una potencia de p que divide a i, entonces

$i = p^j\lambda < p^k \Rightarrow j < k \leq r \Rightarrow p^r m - i = p^{r-\ j+\ j}m - p^j\lambda = p^j(p^{r-j}m - \lambda) \Rightarrow p^j | p^r m - i$, es decir, p^j es también una potencia que divide a $p^r m - i$.

Sea ahora p^j una potencia de p que divide a $p^r m - i$, entonces $p^r m - i = p^j\lambda \Rightarrow p^r m - p^j\lambda = i \Rightarrow j \leq r$ de lo contrario, $p^r m - p^{j-r+r}\lambda = i \Rightarrow p^r(m - p^{j-r}\lambda) = i \Rightarrow i \geq p^r \geq p^k$, lo cual es falso.

Por lo tanto, $p^{r+\ j-\ j}mp^j\lambda = i \Rightarrow p^j(p^{r-j}m - \lambda) = i \Rightarrow p^j | i$.

En conclusión, como $(m,p) = 1$, entonces el racional $\frac{m(p^r m-1)\cdots(p^r m-(p^k-1))}{1,2\cdots(p^k\ -1)}$ es libre de potencias de p.

Resta ver que $p^{r-k} \mid \binom{p^r m}{p^k}$. Sea $c = \binom{p^r m}{p^k}$ y $\frac{m(p^r m-1)\cdots(p^r m-p^{k+1})}{1,2\cdots(p^k\ -1)} = \frac{a}{b}$, donde esta última fracción ya está libre de factores p en su numerador y denominador. Entonces $c = p^{r-k}\frac{a}{b}$, luego $cb = p^{r-k}a$, es decir, $p^{r-k} \mid c$. Nótese que p^{r-k+1} no divide a $\binom{p^r m}{p^k}$, ya que de lo contario $\frac{a}{b}p^{r-k} = p^{r-k+1}\lambda$ y entonces $\frac{a}{b} = p\lambda$, lo cual ya probamos no se tiene. □

9.3. Teoremas

Teorema 9.3.1 (Teoremas de Sylow). *Sea G un grupo finito y sea p un número primo que divide al orden de G. Entonces:*

(i) *Existencia: para cada potencia p^α que divide al orden de G, existe en G un subgrupo de orden p^α. Además, si $p^{\alpha+1}$ divide también a $|\ G|$ entonces cada*

subgrupo de orden p^α está incluido en un subgrupo de orden $p^{\alpha+1}$. En particular, los p-subgrupos de Sylow de G existen y son los subgrupos de G de orden p^r, donde p^r es la máxima potencia de p que divide al orden de G.

(ii) *Conjugación: todos los p-subgrupos de Sylow son conjugados en G.*

(iii) *Cantidad: la cantidad de los p-subgrupos de Sylow de G es congruente con* 1 *modulo p y divide al orden del grupo G.*

Demostración. (i) *Existencia*: sea n el orden del grupo G y sea p^r la máxima potencia de p que divide a n. Sea pues $n := p^r m$, donde $m.c.d.(p, m) = 1$. Consideremos el conjunto M de todos los subconjuntos de G que contiene p^α elementos. Puesto que G actua sobre si mismo de la manera trivial

$$G \times G \to G,\ (g, x) \to gx,$$

se induce entonces una acción de G sobre M. Demostraremos en primer lugar que la acción de G sobre M determina una órbita de s elementos $\{M_1 \dots M_s\}$ tal que $p^{r\,-\,\alpha\,+\,1}$ no divide a s: sabemos que $card(M) = \binom{p^r m}{p^\alpha}$; si la longitud de cada una de las órbitas determinadas en M por el grupo G es divisible por $p^{r\,-\,\alpha\,+\,1}$, entonces $p^{r\,-\,\alpha\,+\,1}$ divide a $card(M)$ debido a la ecuación de clases, pero esto no es posible según la proposición 9.2.4.

Sea G_1 el sugrupo estacionario de M_1. Queremos demostrar que G_1 es de orden p^α. Sea $|G_1| = t$. Entonces de acuerdo con el teorema de Lagrange $|G : G_1|\,|G_1| = |G|$, es decir, , $st = p^r m$. Sea p^w la mayor potencia de p que divide a s y p^v la mayor potencia de p que divide a t, es decir, $s = p^w a, t = p^v b$. Entonces la mayor potencia de p que divide a st, es decir a n , es p^{w+v}. Por lo tanto $w+v = r$. Pero como $p^{r\,-\alpha\,+1}$ no divide a s, entonces $w < r - \alpha + 1$, es decir, $w \leq r - \alpha$, de aquí obtenemos que $v = r - w \geq \alpha$ y por lo tanto $p^\alpha \mid p^v \mid t$. Así pues, $p^\alpha \mid t$ y con esto $t \geq p^\alpha$.

Sea ahora $x \in M_1$. Nótese que $G_1 x \subseteq M_1$. En efecto, sea $g \in G_1$. Entonces $gx \in gM_1 = M_1$, es decir $gx \in M_1$ y así obtenemos la inclusión mencionada. De esta inclusión obtenemos que $|G_1| = |G_1 x| \leq |M_1| = p^\alpha$, es decir, $t \leq p^\alpha$. De $t \geq p^\alpha$ y $t \leq p^\alpha$ obtenemos que $|G_1| = t = p^\alpha$.

Hemos probado pues que el grupo G contiene necesariamente un subgrupo de orden p^α; el subgrupo G_1.

Pasamos ahora a demostrar la segunda afirmación del primer teorema de Sylow.

Supóngase que $p^{\alpha\,+1}$ divide a $n = |G|$ y sea P un subgrupo de G de orden p^α. Consideremos la acción de conjugación sobre el conjunto S de subgrupos del G. Sea C la órbita del subgrupo P, es decir,

$$C = \{gPg^{-1} \mid g \in G\} = P^G.$$

Recordemos que $|C| = |G : N_G(P)|$, donde $N_G(P)$ es el normalizador de P en G (=grupo estacionario de P mediante la acción de conjugación). Nótese que

$$|C| = \frac{|G|}{|N_G(P)|} \Rightarrow |G| = |C||N_G(P)|.$$

Consideremos 2 posibilidades: si p no divide a $|C|$ entonces como $p^{\alpha+1} \mid |G|$ entonces necesariamente $p^{\alpha+1} \mid |N_G(P)|$. Nótese que entonces p divide al orden del grupo cociente $N_G(P)/P$. Según lo demostrado en la primera parte, $N_G(P)/P$ debe contener un subgrupo de orden p. Según el teorema de correspondencia dicho subgrupo es de la forma P^*/P, donde $P^* \leq G$. Por lo tanto, $|P^*/P| = \frac{|P^*|}{|P|} = \frac{|P^*|}{P^\alpha} = p \Rightarrow |P^*| = p^{\alpha+1}$ y entonces P^* es el subgrupo buscado.

Analicemos ahora la segunda posibilidad: $p \mid |C|$. Consideremos nuevamente el conjunto C de los subgrupos de G conjugados con P. El subgrupo P actua sobre C mediante la conjugación, es decir, si $gPg^{-1} \in C$ con $g \in G$, entonces $x(\, gPg^{-1})x^{-1} \in C$ para cada $x \in P$. Como es sabido la longitud de las órbitas determinadas mediante esta acción dividen al orden del grupo P, es decir, dichas longitudes son de la forma p^{α_i}, con $0 \leq \alpha_i \leq \alpha$.

Nótese que uno de los elementos de C es el subgrupo P, por lo tanto, la órbita por él determinada consta de un sólo elemento; el mismo subgrupo P. Sean $O_1 = \{P\}, O_2, \ldots, O_s$ las órbitas que determina la acción de P sobre C. Entonces según la ecuación de clases

$$|C| = 1 + |O_2| + \cdots + |O_s|.$$

Puesto que estamos suponiendo que $p \mid |C|$ y las longitudes de las orbitas $O_2 \ldots O_s$ son potencias de p entonces debe existir al menos otra órbita con un sólo elemento Q ; de lo contrario $p|1$, lo cual es falso. Q es por lo tanto un subgrupo conjugado con P tal que $xQx^{-1} = Q$ para cada $x \in p$; es decir, P normaliza Q.

Tenemos pues en G, P y Q subgrupos conjugados tales que P normaliza Q y P es un p-subgrupo de G. Según la proposición 9.1.8, PQ es un p-subgrupo de G. Como Q es conjugado con P existe $g \in G$ tal que $P = gQg^{-1}$. En la prueba de la proposición 9.1.8 se vió que Q es subgrupo normal de PQ, nótese que en realidad la contenencia es propia: si $Q = PQ \Rightarrow P \leq PQ = Q \Rightarrow P \leq Q$, pero $|P| = |Q| \Rightarrow P = Q$, lo cual es falso.

PQ/Q es un p-subgrupo no trivial $\Rightarrow p \mid |PQ/Q| \Rightarrow$ en PQ/Q hay un subgrupo Q^*/Q de orden $p \Rightarrow |Q^*| = p\,|Q| = p^{\alpha+1} \Rightarrow Q \leq Q^*$ donde $|Q^*| = p^{\alpha+1} \Rightarrow g^{-1}Pg = Q \leq Q^* \Rightarrow P \leq gQ^*g^{-1}$ y $|gQ^*g^{-1}| = p^{\alpha+1}$.

Para terminar la demostración del primer teorema de Sylow mostremos que los p-subgrupos de Sylow de G son los subgrupos de G de orden p^r, donde p^r es la máxima potencia de p que divide al orden de G.

Demostramos en primer lugar la siguiente afirmación consecuencia directa del primer teorema de Sylow.

Afirmación. Sea G un grupo finito y sea $H \leq G$, un p-subgrupo de G. Entonces $|H| = p^n$, $n \geq 0$.

En efecto, sea $H \neq \{1\}$, y sea $q \,|\, |H|$ donde q es un primo diferente de p. Entonces, H contiene un subgrupo de orden q, el cual es cíclico, es decir, H contiene un elemento de orden q. Pero esto contradice que H p-grupo. Por lo tanto, el único primo que divide el orden de H es p, por lo tanto $|H| = p^n$, $n \geq 0$.

Regresamos sobre los p-subgrupos de Sylow de G. Sea H un p-subgrupo de Sylow de G. Entonces, según la afirmación anterior $|H| = p^\alpha$, $0 \leq \alpha \leq r$. Si $\alpha \neq r$ entonces H está incluido en un grupo de orden $p^{\alpha+1}$. Pero esto contradice la condición de ser H maximal. Por lo tanto, $|H| = p^r$.

Sea ahora K un p-subgrupo de G de orden p^r donde p^r es la máxima potencia de p que divide al orden de G. Sea H un p-subgrupo de G que contiene a K; como vimos, $|H| = p^\alpha$, pero como p^r es la máxima potencia de p que divide a $|G|$ entonces $\alpha = r$ y así $H = K$, es decir, K es maximal y por lo tanto K es un p-subgrupo de Sylow de G. Hemos concluido la demostracion del primer teorema de Sylow.

(ii) *Conjugación*: sean nuevamente G a un grupo de orden n y sea p^r la máxima potencia de p que divide a n, $n = p^r m$, donde $m.c.d(p, m) = 1$. Sea P un p-subgrupo de Sylow de G, es decir, $|P| = p^r$. Consideremos nuevamente la acción de conjugación sobre el conjunto S de los subgrupos de G. Sea C la órbita del subgrupo P, es decir $C = \{gPg^{-1} \,|\, g \in G\} = P^G$, en otras palabras, C es el conjunto de todos los subgrupos de G conjugados con P.

Sea Q otro p-subgrupo de Sylow de G. Se desea probar que $Q \in C$. El subgrupo Q actua nuevamente con la acción de conjugación sobre C, dividiendo a C en órbitas. La longitud de cada órbita divide al orden de Q, $|Q| = p^r$. Por lo tanto la longitud de cada órbita es de la forma p^α con $0 \leq \alpha \leq r$. Nótese que $|C| = \frac{|G|}{|N_G(P)|}$ o también $|C|\,|N_G(P)| = |G| = p^r m$, como $P \leq N_G(P)$ entonces $|P| = p^r \mid |N_G(P)|$. Puesto que p^r es la máxima potencia de p que divide a $n = |G|$ entonces p no divide a $|C|$. Por lo dicho anteriormente, debe existir al menos una órbita de un sólo elemento P'. Esto implica que para cada $x \in Q$ se tiene que $xP'x^{-1} = P'$, es decir, Q normaliza P'. Además, como P' es conjugado con P, entonces P' es un p-subgrupo de Sylow. Tenemos pues que $Q/P' \cap Q$ es un p-grupo. Se tiene el isomorfismo

$$P'Q/P' \cong Q/P' \cap Q.$$

Puesto que P' es un p-grupo y $P'Q/P'$ también lo es, entonces $P'Q$ es un p-subgrupo de G. Nótese que $P' \leq P'Q$, $Q \leq P'Q$; como P' y Q son p-subgrupos de Sylow, entonces $P' = P'Q = Q$.

(iii) *Cantidad*: como P un p-subgrupo de Sylow de G todos los p-subgrupos de Sylow de G están en P^G, además cada subgrupo gPg^{-1} de P^G es un p-subgrupo de Sylow. La primera afirmación fue demostrada en 2) y la segunda se desprende de que $|gPg^{-1}| = |P|$. Por lo tanto el número de p-subgrupos de Sylow de G es igual al cardinal de P^G.

Puesto que $\left|P^G\right| |N_G(P)| = |G|$ entonces el número de p-subgrupos de Sylow de G divide el orden de G. P actua sobre P^G mediante la acción de conjugación determinado al menos una órbita de un solo elemento: $\{P\}$. Supóngase que P determina otra órbita de un solo elemento Q, $Q \neq P$. Entonces se tiene que P y Q con conjugados, P normaliza Q, P es un p-subgrupo. De aquí obtenemos que PQ es un p-subgrupo y además P es subgrupo propio de PQ. Esto contradice el hecho de que P es maximal. Por lo tanto, P determina sobre P^G sólo una órbita unitaria. Ya que las longitudes de las órbitas dividen a $p^r = |P|$ entonces $\left|P^G\right| \equiv 1 \pmod{\text{p}}$. □

9.4. Aplicaciones

Proposición 9.4.1. *Sea G un grupo finito y sea H un p-subgrupo de Sylow de G. Entonces, $H \trianglelefteq G \Leftrightarrow H$ es único.*

Demostración. $\Rightarrow$): sea K un p-subgrupo de Sylow $\Rightarrow K = xHx^{-1} = H \Rightarrow H$ es único.

$\Leftarrow$): sea $x \in G \Rightarrow |xHx^{-1}| = |H| \Rightarrow xHx^{-1}$ es p-subgrupo de Sylow $\Rightarrow xHx^{-1} = H$, entonces $H \trianglelefteq G$. □

Corolario 9.4.2. *Sea G un grupo finito y sea H el p-subgrupo de Sylow de G tal que $H \trianglelefteq G$. Entonces $H = \{x \in G \,|\, |x| \text{ es una potencia de } p\}$.*

Demostración. Sea $x \in H$, como H por definición es p-subgrupo entonces $|x|$ es una potencia de p. De otra parte, sea $x \in G$ tal que $|x| = p^\alpha \Rightarrow \langle x \rangle$ es un p-subgrupo de $G \Rightarrow \langle x \rangle$ está contenido en el único p-subgrupo de Sylow de G. □

La proposición anterior sirve para caracterizar todos los subgrupos de orden pq con $p > q$ y p, q primos

Proposición 9.4.3. *Sea G un grupo de orden pq con p y q primos y con $p > q$. Entonces:*

(i) *$G \cong \mathbb{Z}_{pq}$ ó*

(ii) *G es no abeliano y se tiene que $G = G_{pq} := \langle a, b \,|\, a^p = 1, b^q = 1, bab^{-1} = a^k$ con $k \not\equiv 1$ (mód p) y $k^q \equiv 1$ (mód p), $p \equiv 1$ (mód q) $\rangle$.*

Demostración. G contiene al menos un subgrupo de Sylow $H = \langle a \rangle$ de orden p y un sugrupo de Sylow $K = \langle b \rangle$ de orden q. Sean n_p y n_q el número de tales subgrupos de Sylow, como $p > q$ entonces $n_p = 1$. De aqui se afirma que $H \trianglelefteq G$. Para n_q se tienen entonces dos posibilidades, $n_q = 1$ ó $n_q = p$.

Caso 1. En G sólo hay un subgrupo de Sylow de orden q. Entonces $K \trianglelefteq G$ y $aba^{-1}b^{-1} \in H \cap K = 1$, luego $ab = ba \Rightarrow G \cong \mathbb{Z}_{pq}$.

Caso 2. En G hay p subgrupos de Sylow de orden q. Esto implica que $p \equiv 1(\text{mód } q)$. Veamos que esta situación es descrita por b). G no es abeliano, en caso contrario $n_q = 1$, como $H \trianglelefteq G$ existe $1 < k < p$ tal que $bab^{-1} = a^k$ y $k \not\equiv 1(p)$. Si fuese $k \equiv 1(p)$ entonces: $p|(k-1) \Rightarrow a^{k-1} = 1 \Rightarrow a^k = a \Rightarrow ab = ba \Rightarrow G \cong \mathbb{Z}_{pq}$ y G sería abeliano.

Nótese que escogiendo k entre 1 y p tal k es único. Obsérvese que $b^2ab^{-2} = a^{k^2}$. En efecto,$(a^k)^k = a^{k^2} = (bab^{-1})^k = ba^kb^{-1} = b(bab^{-1})b^{-1} = b^2ab^{-2}$.

Podemos generalizar esta relación por inducción y probar que

$$b^nab^{-n} = a^{k^n},\ n \geq 0 \tag{9.4.1}$$

Tomando en particular $n = q$ obtenemos que $a = a^{k^q} \Rightarrow p|(k^q - 1) \Rightarrow k^q \equiv 1(p)$.

Sea $W = \langle a, b\rangle \leq G$; y sea $x \in W$. Entonces $x = a^{r_1}b^{l_1} \cdots a^{r_m}b^{l_m}$, $0 \leq r_i \leq p-1$, $0 \leq l_i \leq q-1$, $0 \leq i \leq m$. Consideremos el producto b^la^r con $0 \leq l \leq q-1$, $0 \leq r \leq p-1$. De (9.4.1) se desprende que $b^na^rb^{-n} = a^{rk^n}$, $n \geq 0$, $r \geq 0$. De aquí obtenemos que $b^na^r = a^{rk^n}b^n$ de esta relación se obtiene que cada elemento $x \in G$ toma la forma $x = a^rb^l$ con $0 \leq r \leq p-1$, $0 \leq l \leq q-1$. Tales x tenemos máximo pq. Veamos que son exactamente pq. Sean $0 \leq r, s \leq p-1$ y $0 \leq l, m \leq q-1$ tales que $a^rb^l = a^sb^m \Rightarrow b^{m-l} = a^{r-s} \in \langle a\rangle \cap \langle b\rangle \Rightarrow \left|b^{m-l}\right| \mid p, \left|b^{m-l}\right| \mid q \Rightarrow b^{m-l} = 1$. Por la condición de m y l se tiene que $m = l$. Análogamente $r = s$.

Así pues, $|W| = pq$ con lo cual $G = W$. Hemos probado pues que G cumple todas las condiciones de b), por último notemos la regla de multiplicación en G_{pq} y escribamos sus elementos:

$$G_{pq} = \left\{1, a, a^2 \ldots a^{p-1}; b, b^2 \ldots b^{q-1}; ab, ab^2 \ldots ab^{q-1}; \cdots, a^{p-1}b \ldots a^{p-1}b^{q-1}\right\}$$

$$a^rb^la^sb^m = a^{r+sk^l}b^{l+m},\quad r, l, s, m \geq 0.$$

□

Proposición 9.4.4. *Sea p primo impar y G un grupo de orden $2p$. Entonces, $G \cong \mathbb{Z}_{2p}$ ó $G \cong D_p$.*

Demostración. Si G es abeliano entonces $G \cong \mathbb{Z}_{2p}$. En caso contrario existen $a, b \in G$ tales que $|a| = p$, $|b| = 2$, $bab^{-1} = a^k$ con $k \not\equiv 1(p), k^2 \equiv 1(p)$, $p \equiv 1(2)$, $2 \leq k \leq p-1$. Supóngase que $k \leq p-2$. Como $p|(k^2-1) \Rightarrow p|k+1$ ó $p|k-1$. Por la condición de k obtenemos una contradicción. Así, $k = p-1 \Rightarrow bab = a^{p-1} = a^{-1}$. Entonces, $G \cong D_p$. □

Corolario 9.4.5. *Los grupos de orden 6 son $\mathbb{Z}_6$ y $D_3 \cong S_3$.*

Demostración. Consecuencia directa de la proposición anterior. □

Proposición 9.4.6. *Los grupos no abelianos de orden 8 son D_4 y Q_8.*

Demostración. Sea G un grupo no abeliano de orden 8. Entonces en G debe existir al menos un elemento a de orden 4. En efecto, si todos los elementos $\neq 1$ tienen orden 2 entonces G es abeliano. G tampoco posee elementos de orden 8, ya que en caso contrario sería cíclico y por lo tanto abeliano.

Puesto que $|G : \langle a\rangle| = 2$ entonces $\langle a\rangle \trianglelefteq G$. Evidentemente existe al menos un elemento b en G tal que $b \notin \langle a\rangle$. Nótese que los elementos $1, a, a^2, a^3, b, ba, ba^2, ba^3$ son diferentes, con lo cual $G = \langle a, b\rangle$. Puesto que $|G : \langle a\rangle| = 2$ entonces $b^2 \in \langle a\rangle$. En efecto, como en $G/\langle a\rangle$ sólo hay dos clases entonces $\overline{b^2} \neq \overline{b}$ (de lo contrario, $\overline{b} = \overline{1}$ y así $b \in \langle a\rangle$).

Se presentan entonces las siguientes posibilidades: $b^2 = 1, a, a^2, a^3$;

$b^2 = a \Rightarrow b^8 = a^4 = 1 \Rightarrow |b| = 8$, falso.

$b^2 = a^3 \Rightarrow b^8 = a^{12} = 1 \Rightarrow |b| = 8$ falso.

Se tiene entonces que $b^2 = 1$ *ó* $b^2 = a^2$.

De otra parte como $\langle a\rangle \trianglelefteq G$ entonces $bab^{-1} = 1, a, a^2, a^3$.

$bab^{-1} = 1 \Rightarrow a = 1$, falso.

$bab^{-1} = a \Rightarrow ab = ba \Rightarrow G$ es abeliano, falso.

$bab^{-1} = a^2 \Rightarrow |bab^{-1}| = |a| = |a^2| = 4 = 2$, imposible.

En total, $bab^{-1} = a^3 = a^{-1}$.

Se tiene pues que G es un grupo generado por dos elementos a y b para los cuales $a^4 = 1$, $b^2 = 1$, $bab^{-1} = a^{-1}$ ó $a^4 = 1$, $b^2 = a^2$, $bab^{-1} = a^{-1}$. En el primer caso $G \cong D_4$ y en el segundo $G \cong Q_8$. □

Proposición 9.4.7. *Los grupos no abelianos de orden* 12 *son:* A_4, D_6 *y*

$$T := \langle a, b \,|\, a^6 = 1, b^2 = a^3, bab^{-1} = a^{-1}\rangle.$$

Demostración. Sea H un subgrupo de Sylow de G de orden 3: $H = \langle c\rangle$. Mediante el refinamiento del teorema de Cayley (véase el ejemplo 8.2.6) podemos definir un homomorfismo

$$\Phi : G \to S\,(G/H) \cong S_4$$

Nótese que $\ker(\Phi) \subseteq H$ ($\ker(\Phi)$ es el subgrupo normal más grande de G contenido en H) $\Rightarrow \ker(\Phi) = 1$ ó $\ker(\Phi) = H$. Si $\ker(\Phi) = 1 \Rightarrow G$ es isomorfo a un subgrupo de S_4 de orden 12. Pero se puede probar que si $n \geq 2$, $G \leq S_n$, $|G| = \frac{n!}{2} \Rightarrow G = A_n$ (véase el ejecicio 6 del presente capítulo).

Supóngase ahora que $\ker(\Phi) = H$, entonces H es normal en G y por lo tanto H es el único 3-subgrupo de Sylow. Entonces, en G sólo hay dos elementos de orden 3: c y c^2. Puesto que dos elementos conjugados tienen el mismo orden entonces $\left|c^G\right| = 1$ ó $2 \Rightarrow |C_G(c)| = 12$ ó 6. En cualquiera de los dos casos $C_G(c)$ contiene un elemento d de orden 2. Como $cd = dc$, sea pues $a := cd \Rightarrow |a| = 6 \Rightarrow \langle a\rangle \trianglelefteq G$ y $|G/\langle a\rangle| = 2$.

Sea $b \in G$ con $b \notin \langle a\rangle \Rightarrow b^2 \in \langle a\rangle$ (véase la prueba de la proposición 9.4.6) $\Rightarrow b^2 = 1, a, a^2, a^3, a^4, a^5$; también, $bab^{-1} \in \langle a\rangle \Rightarrow bab^{-1} = 1, a, a^2, a^3, a^4, a^5$.

$bab^{-1} = 1 \Rightarrow a = 1$, falso.

$bab^{-1} = a \Rightarrow ab = ba \Rightarrow \langle a, b\rangle$ es abeliano, pero este subgrupo tiene 12 elementos y coincide entonces con G, falso.

$bab^{-1} = a^2 \Rightarrow (bab^{-1})^3 = 1 \Rightarrow ba^3b^{-1} = 1 \Rightarrow a^3 = 1$, falso.

$bab^{-1} = a^3 \Rightarrow (bab^{-1})^2 = 1 \Rightarrow a^2 = 1$, falso.

$bab^{-1} = a^4 \Rightarrow (bab^{-1})^3 = 1 \Rightarrow a^3 = 1$, falso.

$bab^{-1} = a^5 = a^{-1} \Rightarrow bab^{-1} = a^{-1}$, esta es una entonces una condición necesaria en G.

$b^2 = 1$, esta es una posibilidad.

$b^2 = a \Rightarrow (b^2)^6 = 1 \Rightarrow b^{12} = 1 \Rightarrow |b| \mid 12$, luego

$|b| = 1 \Rightarrow b = 1$, falso.

$|b| = 2 \Rightarrow b^2 = 1 = a$, falso.

$|b| = 3 \Rightarrow b^2b = 1 \Rightarrow ab = 1 \Rightarrow b \in \langle a\rangle$, falso.

$|b| = 4 \Rightarrow b^4 = a^2 = 1$, falso.

$|b| = 6 \Rightarrow b^6 = a^3 = 1$, falso.

$\Rightarrow |b| = 12 \Rightarrow G$ es abeliano, falso.

$b^2 = a^2$: puesto que $bab^{-1} = a^{-1} \Rightarrow (bab^{-1})^2 = a^{-2} \Rightarrow ba^2b^{-1} = a^{-2} \Rightarrow bb^2b^{-1} = a^{-2} \Rightarrow b^2 = a^{-2} = a^2 \Rightarrow a^4 = 1$, falso.

$b^2 = a^3$, esta es una posibilidad.

$b^2 = a^4 : (bab^{-1})^4 = a^{-4} \Rightarrow ba^4b^{-1} = a^{-4} \Rightarrow bb^2b^{-1} = a^{-4} \Rightarrow b^2 = a^{-4} = a^4 \Rightarrow a^8 = 1 \Rightarrow 6|8$, imposible.

$b^2 = a^5 \Rightarrow (b^2)^6 = (a^5)^6 = 1 \Rightarrow b^{12} = 1 \Rightarrow |b| \mid 12$, luego

$|b| = 1 \Rightarrow b = 1$, falso.

$|b| = 2 \Rightarrow a^5 = 1$, falso

$|b| = 3 \Rightarrow a^{15} = 1 \Rightarrow 6|15$, falso.

$|b| = 4 \Rightarrow a^{10} = 1$, falso.

$|b| = 6 \Rightarrow a^{15} = 1$, falso.

$|b| = 12 \Rightarrow G$ es abeliano, falso.

Resumiendo los resultados anteriores obtenemos que si G es un grupo no abeliano de orden 12 entonces: G es A_4 o en G se tienen dos elementos a y b tales que $a^6 = 1, b^2 = 1, bab^{-1} = a^{-1}$, o en G hay dos elementos a , b tales que $a^6 = 1, b^2 = a^3, bab^{-1} = a^{-1}$.

Veamos que en los dos últimos casos $G = \langle a, b\rangle$. En ambas situaciones consideremos el conjunto

$$C := \left\{a^k b^m \mid 0 \leq k \leq 5, 0 \leq m \leq 1\right\}$$

y sean $0 \leq k_1, k_2 \leq 5, 0 \leq m_1, m_2 \leq 1$ tales que $a^{k_1}b^{m_1} = a^{k_2}b^{m_2} \Rightarrow a^{k_1-k_2} = b^{m_2-m_1}$. Supongamos que $m_2 \neq m_1$ y por ejemplo $m_2 > m_1 \Rightarrow a^{k_1-k_2} = b \in \langle a\rangle$, falso $\Rightarrow m_2 = m_1 \Rightarrow k_1 = k_2$.

Así pues, en A hay 12 elementos y en consecuencia $G = \langle a, b\rangle$. En total obtenemos que si G es un grupo no abeliano de orden 12, entonces G es alguno de los siguientes grupos:

$$A_4, D_6 = \left\langle a, b \mid a^6 = 1, b^2 = 1, bab^{-1} = a^{-1}\right\rangle, T = \left\langle a, b \mid a^6 = 1, b^2 = a^3, bab^{-1} = a^{-1}\right\rangle.$$

□

9.5. Ejercicios

1. Sea G un grupo formado por dos elementos x, y tales que

   (i) $x^p = 1$ (es decir x es de orden p)

   (ii) $y^q = 1$ (es decir y es de orden $q < p$)

   (iii) Existe $1 < k_0 < p$, $k_0 \not\equiv 1(p)$ tal que $yxy^{-1} = x^{k_0}$

   (iv) $k_0^q \equiv 1$ (p)

   (v) $p \equiv 1$ (q).

   Entonces, $G \cong G_{pq}$.

2. Demuestre que ningún grupo de orden pq es simple, donde p, q son primos.

3. Demuestre que todo grupo de orden 15 es cíclico.

4. Demuestre que todo grupo de orden 35 es cíclico.

5. Demuestre que todo grupo de orden 77 es cíclico.

6. Demuestre que si $n \geq 2$, $H \leq S_n$, $|H| = \frac{n!}{2} \Rightarrow H = A_n$ (véase la demostración de la proposición 9.2.2).

7. Demuestre que los grupos A_4, D_6 y T no son isomorfos.

   Demostración. Solución. En el capítulo 6 se demostró que $Z(D_6) = \mathbb{Z}_2$. En el capítulo 11 se calcula el centro del grupo alternante A_n a partir únicamente de la definición de centro y de la definición del grupo alternante, allí se muestra que $Z(A_n) = 1$ para $n \geq 4$. Esto ilustra que D_6 y A_4 no son isomorfos. De igual forma, en el Capítulo 11 se calcula el centro del grupo T a partir únicamente de su tabla y se establece que $Z(T) = \langle a^3\rangle \cong \mathbb{Z}_2$; de esto se deduce que A_n y T no son isomorfos. Finalmente, de la tabla de T se deduce que en este grupo b es un elemento de orden 4, en cambio D_6 no tiene elementos de este orden. Esto demuestra que T y D_6 no son isomorfos. □

8. Calcule todos los 3-subgrupos de Sylow del grupo T.
9. Calcule el grupo $Aut(T)$.
10. Calcule el grupo $Aut(G_{pq})$.

Capítulo 10

Grupos abelianos finitos

El objetivo central de este capítulo es describir para un entero positivo dado n todos los grupos abelianos de orden n (salvo isomorfismo). La descripción se hará en términos de p-grupos cíclicos, los cuales, como veremos, son indescomponibles. Se establecerá además un criterio para la unicidad de dicha descomposición.

10.1. p-grupos abelianos finitos

Comenzamos probando que todo grupo finito G de orden $n = p_1^{r_1} \cdots p_k^{r_k}$ es suma directa de sus subgrupos de Sylow si, y sólo si, estos son normales. En el caso de ser G abeliano esta condición se da automáticamente y podemos enunciar el siguiente teorema.

Teorema 10.1.1. *Sea G un grupo finito de orden n,*

$$|G| = n = p_1^{r_1} \cdots p_k^{r_k} \ ; \ p_1, \ldots, p_k \text{ primos diferentes y } r_1, \ldots, r_k \geq 1$$

Entonces, G es suma directa de sus subgrupos de Sylow si, y sólo si, estos son normales en G:

$$G = P_1 \oplus \cdots \oplus P_k, \tag{10.1.1}$$

donde P_i es el p_i-subgrupo de Sylow de G, $1 \leq i \leq k$. En particular, si G es abeliano, entonces G es suma directa interna de sus subgrupos de Sylow.

Demostración. $\Rightarrow$): si G es suma directa de sus subgrupos de Sylow, entonces por la definición de suma directa, cada sumando es necesariamente subgrupo normal de G.

$\Leftarrow$): para $1 \leq i \leq k$, sea P_i un p_i-subgrupo de Sylow de G tal que P_i es un subgrupo normal de G. Entonces P_i es único. Probaremos entonces que (10.1.1) se cumple. Veremos que cada elemento $x \in G$ tiene una representación única en la forma $x = x_1 \cdots x_k$, donde $x_i \in P_i$, $1 \leq i \leq k$.

(a) Por razones de orden de sus elementos, para $i \neq j$ se tiene que $P_i \cap P_j = 1$.

(b) A partir de (a) se obtiene que para $i \neq j$ los elementos de P_i conmutan con los de P_j.

(c) El neutro 1 de G tiene representación única: sean $x_i \in P_i$, $1 \leq i \leq k$ tales que $1 = x_1 \cdots x_k$. Sea $s_i = |x_i|$, entonces $s_i = p_i^{\alpha_i}$, $0 \leq \alpha_i \leq r_i$. Sea $s = s_1 \cdots s_{i-1} s_{i+1} \cdots s_k$, entonces $1^s = x_i^s$, luego $s_i | s$ y $p_i^{\alpha_i} | p_1^{\alpha_1} c \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k}$. Esto implica que $\alpha_i = 0$, luego $s_i = 1$, es decir, $x_i = 1$, para cada $1 \geq i \geq k$.

(d) Cada elemento $x \in G$ se puede representar en la forma única anunciada: sea $x \in G$ de orden r de tal forma que $r|n$ y $r = p_1^{s_1} \ldots p_k^{s_k}$, donde $0 \leq s_i \leq r_i$ con $1 \leq i \leq k$. Sea $u_i = \frac{r}{p_i^{s_i}}$, entonces $m.c.d.\{u_1, \ldots, u_k\} = 1$. Existen entonces enteros $t_1, \ldots, t_k$ tales que $1 = t_1 u_1 + \cdots + t_k u_k$, sea $x_i = x^{t_i u_i}$, $1 \geq i \geq k$. Nótese que $x_i^{p_i^{s_i}} = (x^{t_i u_i})^{p_i^{s_i}} = x^{t_i u_i p_i^{s_i}} = x^{t_i r} = 1$; luego $x_i \in P_i$. Nótese ahora que $x_1 \cdots x_k = x^{t_1 u_1} \ldots x^{t_k u_k} = x^{t_1 u_1 + \cdots + t_k u_k} = x^1 = x$. A partir de (b) y (c) se obtiene que esta representación es única. □

Corolario 10.1.2. *Sea $n = p_1^{r_1} \cdots p_k^{r_k}$. Entonces,*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}.$$

Demostración. Consecuencia inmediata del teorema anterior. □

El objetivo central en la descripción de los grupos abelianos finitos consiste en expresar G como suma directa de subgrupos de estructura simple y conocida, como por ejemplo a tráves de subgrupos cíclicos. Desde luego que sobre estos subgrupos habrá que colocar alguna restricción ya que de lo contrario la descomposición no sería única. Nótese por ejemplo que $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

Nuestro objetivo inmediato es estudiar los p-grupos abelianos finitos, es decir, los grupos abelianos cuyo orden es de la forma p^n, $n \geq 0$.

Proposición 10.1.3. *Si G es un grupo cíclico de orden p^n, entonces G no se puede descomponer en suma directa de subgrupos cíclicos de orden menor, es decir, G es irreducible.*

Demostración. Sabemos que $G \cong \mathbb{Z}_{p^n} \cong \mathbb{C}_{p^n}$. Probemos inicialmente que los únicos subgrupos de $\mathbb{C}_{p^n}$ son los subgrupos de la cadena

$$\{1\} = \mathbb{C}_{p^0} \subset \mathbb{C}_{p^1} \subset \mathbb{C}_{p^2} \subset \cdots \subset \mathbb{C}_{p^{n-1}} \subset C_{p^n}.$$

Sea $K \leq \mathbb{C}_{p^n} \Rightarrow |K| \mid p^n \Rightarrow |K| = p^\alpha, 0 \leq \alpha \leq n$; sea $x \,\epsilon\, K \Rightarrow x^{p^\alpha} = 1 \Rightarrow K \leq \mathbb{C}_{p^\alpha} \Rightarrow K = \mathbb{C}_{p^\alpha}$.

Ahora si existieran H, K en $\mathbb{C}_{p^n}$ tales que $\mathbb{C}_{p^n} = H \oplus K$ entonces $H = \mathbb{C}_{p^\alpha}$, $K = \mathbb{C}_{p^\beta}$, $H \cap K = \{1\}$. Para α y β dados se tiene que $\alpha \leq \beta$ o $\beta \leq \alpha$. En el primer caso $H \leq K$ y $H \cap K = H = \{1\} \Rightarrow \alpha = 0$ y $\beta = n$. En el segundo caso $K \leq H$, $H \cap K = K = \{1\} \Rightarrow \alpha = n$, $\beta = 0$. En total la única descomposición de $\mathbb{C}_{p^n}$ es la trivial: $\mathbb{C}_{p^n} = \{1\} \oplus \mathbb{C}_{p^n}$. □

Ejemplo 10.1.4. $\mathbb{Z}_4$ y $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ no son isomorfos; $\mathbb{Z}_9$ y $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ no son isomorfos.

Teorema 10.1.5. *Cada p-grupo abeliano finito G es suma directa de subgrupos cíclicos.*

Demostración. Sea G un p-grupo abeliano finito, entonces $|G| = p^n$, con $n \geq 0$. La prueba se realiza por inducción sobre n. Si $n = 0$ ó $n = 1$, entonces G es cíclico y no hay nada más que demostrar.

Sea $n \geq 2$. Suponemos que el teorema ya ha sido probado para grupos de orden p^α con $0 \leq \alpha < n$. Sea G de orden p^n. Si G es cíclico entonces según la proposición anterior la única descomposición de G es la trivial: $G = \{1\} \oplus G$.

Supóngase que G no es cíclico. Cada elemento a de G, $a \neq 1$, tiene orden de la forma $|a| = p^\beta$, $0 < \beta < n$. Escojamos un $a \neq 1$ que tenga orden maximal p^m (esto quiere decir que no existe y en G tal que $|y| = p^{m+1}$).

Consideremos el grupo cociente $\bar{G} = G/\langle a\rangle$. Puesto que $|\bar{G}| = \frac{p^n}{p^m} = p^{n-m}$ y $0 < n - m < n$ entonces según la hipótesis inductiva

$$\bar{G} = \bar{G}_1 \oplus \cdots \oplus \bar{G}_r$$

donde cada $\bar{G}_i$ es un subgrupo cíclico de $\bar{G}$ de orden $|\overline{G_i}| = p^{m_i}, 1 \leq m_i \leq n-m, 1 \leq i \leq r$; además

$$m_1 + m_2 + \cdots + m_r = n - m.$$

Sea $\bar{G}_i = \langle \bar{\delta}_i\rangle$, $\bar{\delta}_i = \delta_i\langle a\rangle$, $\delta_i \ \epsilon \ G$, $1 \leq i \leq r$. Sería lógico pensar que $G = \langle \delta_1\rangle \oplus \cdots \oplus \langle \delta_r\rangle \oplus \rangle a\rangle$. Sin embargo no es este el caso, pero con ayuda de los elementos $\delta_1, \ldots, \delta_r$ construiremos otros $a_1, \ldots, a_r$ y para ello probaremos que $G = \langle a_1\rangle \oplus \langle a_2\rangle \oplus \cdots \oplus \langle a_r\rangle \oplus \langle a\rangle$.

Nótese que para cada $1 \leq i \leq r$, $(\bar{\delta}_i)^{p^{m_i}} = \overline{(\delta_i^{p^{m_i}})} = \bar{1} \Rightarrow \delta_i^{p^{m_i}}\epsilon\langle a\rangle \Rightarrow \delta_i^{p^{m_i}} = a^{s_i}$ con $0 \leq s_i < p^m$. Sea $|b_i| = p^{\alpha_i}$ con $1 \leq \alpha_i \leq m$, entonces $(b_i^{p^{m_i}})^{p^{\alpha_i}} = (a^{s_i})^{p^{\alpha_i}}$, luego $1 = a^{s_i p^{\alpha_i}}$, entonces $p^m | s_i p^{\alpha_i}$ y existe entonces t_i tal que $s_i = t_i p^{m-\alpha_i}$. Definimos entonces

$$a_i =: \delta_i a^{-t_i}, \ \ 1 \leq i \leq r.$$

Nótese que para cada $1 \leq i \leq r$ $\bar{a}_i = \bar{\delta}_i$: en efecto, $\bar{a}_i = a_i\langle a\rangle = \delta_i\langle a\rangle = \bar{\delta}_i$ ya que $a_i\delta_i^{-1} = a^{-t_i}\epsilon\langle a\rangle$. De aquí obtenemos que $\langle \bar{a}_i\rangle = \langle \bar{\delta}_i\rangle = \bar{G}_i$, $1 \leq i \leq r$. Por lo tanto, $\bar{G} = \langle \bar{a}_i\rangle \oplus \cdots \oplus \langle \bar{a}_r\rangle$.

Sea x un elemento cualquiera de G. Entonces $\bar{x} = \bar{x}_1 \cdots \bar{x}_r$ donde $\bar{x}_i\epsilon\langle \overline{a_i}\rangle$, $1 \leq i \leq r$; $\Rightarrow \bar{x}_i = \bar{a_i}^{k_i}, 0 \leq k_i < p^{m_i}$, $\Rightarrow \bar{x}_i = \overline{a_i^{k_i}} \Rightarrow \bar{x} = \overline{a_1^{k_1} \cdots a_r^{k_r}} \Rightarrow x(a_1^{k_1} \cdots a_r^{k_r})^{-1} = a^k\epsilon\langle a\rangle \Rightarrow x = a_1^{k_1} \cdots a_r^{k_r} a^k$.

Se ha probado que cada elemento x de G se expresa como producto de elementos de $\langle a_1\rangle \cdots \langle a_r\rangle$ y $\langle a\rangle$. Queda por demostrar que la representación es única. Para esto es suficiente demostrar la unicidad de la representación del elemento identidad 1. Sea

$$1 = a_1^{k_1} \cdots a_r^{k_r} a^k \quad \text{con } 0 \leq k_i < p^{m_i},\ \ 0 \leq k < p^m.$$

Mediante el homomorfismo $G \to G\ /\langle a\rangle$ obtenemos $\bar{1} = \overline{a_1^{k_1}} \cdots \overline{a_r^{k_r}} \Rightarrow \overline{a_1^{k_1}} = \bar{1} \ldots \overline{a_r^{k_r}} = \bar{1}$ ya que $\overline{G} = \overline{G_1} \oplus \cdots \oplus \overline{G_r}$ y $\overline{a_i^{k_i}} \epsilon \overline{G_i}$, $1 \leq i \leq r \quad \Rightarrow a_i^{k_i} \epsilon < a >$, $1 \leq i \leq r \Rightarrow a_i^{k_i} = a^z$ con $0 \leq z < p^m$; $\Rightarrow \delta_i^{k_i} a^{-t_i k_i} = a^z \Rightarrow \delta_i^{k_i} = a^{z+t_i k_i} \Rightarrow \overline{\delta_i^{k_i}} = \overline{a^{z+t_i k_i}} = \bar{1} \Rightarrow (\overline{\delta_i})^{k_i} = \bar{1}$. Como $|\overline{\delta_i}| = p^{m_i}$ y $0 \leq k_i < p^{m_i} \Rightarrow k_i = 0$, $1 \leq i \leq r$ $\Rightarrow 1 = a^k$. Como $0 \leq k < p^m$ y $|a| = p^m \Rightarrow k = 0$. □

El teorema anterior ha probado que cada grupo abeliano finito de orden p^n se descompone en suma directa de subgrupos cíclicos

$$G = G_1 \oplus \cdots \oplus G_r,$$

donde $|G_i| = p^{m_i}$, $1 \leq m_i \leq n$, $1 \leq i \leq r$, $m_1 + \cdots + m_r = n$, $1 \leq r \leq n$ (Nótese que aquí se ha incluido el caso trivial en el que G es cíclico y $r = 1$).

Vale la pena entonces preguntar sobre la unicidad de la descomposición anterior.

Teorema 10.1.6. *Si el grupo abeliano finito G se descompone en dos formas en producto de subgrupos cíclicos*

$$G = G_1 \oplus \cdots \oplus G_r = H_1 \oplus \cdots \oplus H_s,$$

entonces $r = s$ y los órdenes $|G_i|$ coinciden con los órdenes $|H_j|$ después de una reordenación de índices.

Demostración. Este resultado se puede enunciar y probar de una manera más general usando teoría de módulos, omitimos sun demostración e invitamos al lector a consultar [9]. □

10.2. Sistemas de invariantes

Según el teorema 10.1.5 cada p-grupo abeliano finito G, $|G| = p^n$, determina un arreglo ordenado $(p^{m_1}, \ldots, p^{m_r})$ conformada por los órdenes de los subgrupos cíclicos de su descomposición:

$$G = G_1 \oplus \cdots \oplus G_r, |G_i| = p^{m_i},$$

La suma directa se puede reordenar de tal forma que $m_1 \geq m_2 \geq \cdots \geq m_r \geq 1$, $1 \leq r \leq n$ (se ha incluido el caso trivial cuando G es cíclico y $r = 1$). Según el teorema 10.1.6, la longuitud r del arreglo así como sus componentes $p^{m_1}, \ldots, p^{m_r}$, están determinadas unívocamente por el grupo G. Esta primera observación permite dar la siguiente definición.

Definición 10.2.1. *Sea G un $p-$ grupo abeliano finito, ($|G| = p^n$).*

(i) *Se dice que G es del tipo $(p^{m_1}, \ldots, p^{m_r})$ si G es suma directa de subgrupos cíclicos de órdenes p^{m_i}, $1 \leq i \leq r$, $m_1 \geq m_2 \geq \cdots \geq m_r$, $1 \leq r \leq n$, $m_1 + \cdots + m_r = n$; las componentes $p^{m_1}, \ldots, p^{m_r}$ se denominan* ***divisores elementales*** *del grupo G.*

(ii) *Sean A y B dos $p-$grupos abelianos finitos con el mismo sistema de divisores elementales $(p^{m_1}, \ldots, p^{m_r})$. Entonces $A = A_1 \times \cdots \times A_r$, $B = B_1 \times \cdots \times B_r$ con $A_i \cong \mathbb{Z}_{p^{m_i}} \cong B_i$. El sistema de isomorfismos φ_i induce el isomorfismo*

$$\varphi : A \to B$$
$$\varphi(a_1, \ldots, a_r) := (\varphi_1(a_1), \ldots, \varphi_r(a_r)).$$

Hemos probado entonces la siguiente proposición.

Proposición 10.2.2. *Con sus divisores elementales cada p-grupo abeliano finito queda determinado unívocamente salvo isomorfismo.*

Veamos en un ejemplo la ilustración de los resultados anteriores.

Ejemplo 10.2.3. Sea p un primo cualquiera y $n = 4$. Determinemos todos los posibles grupos abelianos de orden p^4.

Divisores elementales: (p^4), (p^3, p), (p^2, p^2), (p^2, p, p), (p, p, p, p). Salvo isomorfismo, únicamente se tienen los siguientes grupos distintos de orden p^4:

$$\mathbb{Z}_{p^4}, \quad \mathbb{Z}_{p^3} \oplus \mathbb{Z}_p, \quad \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}, \quad \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p, \quad \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p.$$

El ejemplo anterior permite la siguiente generalización:

Definición 10.2.4. *Sea n un entero positivo. Una sucesión de enteros positivos $(m_1, \ldots, m_r)$ con $m_1 \geq m_2 \geq \cdots \geq m_r \geq 1$ y $m_1 + \cdots + m_r = n$ se denomina una* ***partición*** *de n. Sea $p(n)$ el número de particiones de n.*

Ejemplo 10.2.5. $n = 4$: (4), $(3, 1)$, $(2, 2)$, $(2, 1, 1)$, $(1, 1, 1, 1) \Rightarrow p(4) = 5$.

Proposición 10.2.6. *Sea F la clase de todos los grupos abelianos no isomorfos de orden p^n, $n \geq 1$, y sea P el conjunto de todas las particiones de n. Existe una correspondencia biunívoca entre F y P, es decir, el número de grupos abelianos no isomorfos de orden p^n es finito e igual a $p(n)$.*

Demostración. Según hemos visto, cada elemento G de F determina unívocamente su tipo $(p^{m_1}, \ldots, p^{m_r})$ con $m_1 \geq m_2 \geq \cdots \geq m_r$ y $m_1 + \cdots + m_r = n$. Tenemos pues la función

$$h\colon F \to P$$
$$h(G) := (m_1, \ldots, m_r)$$

Cada partición $(m_1 \dots m_r)$ determina un único grupo (salvo isomorfismo) con sistema de divisores elementales $(p^{m_1}, \dots, p^{m_r})$. Así pues, h es $1-1$. Ahora, h es claramente sobre: $(m_1, \dots, m_r)$ determina $(p_1^{m_1}, \dots, p^{m_r})$, el cual una vez determina $\mathbb{Z}_{p^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{m_r}}$. □

Ejemplo 10.2.7. (i) Determinemos todos los subgrupos abelianos de orden 4 : $4 = 2^2 \Rightarrow\ p = 2$, $n = 2$, luego (4), (2, 2) y entonces $\mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong V$.

(ii) Calculemos todos los grupos abelianos de orden 9 : $9 = 3^2 \Rightarrow p = 3$, $n = 2$, con lo cual tenemos (9), $(3, 3) \Rightarrow \mathbb{Z}_9$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

(iii) Determinemos todos los grupos abelianos de orden 125 : $p = 5$, $n = 3 \Rightarrow$ (5^3), $(5^2, 5)$, $(5, 5, 5) \Rightarrow\ \mathbb{Z}_{125}$, $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$, $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$.

Definición 10.2.8. *Un grupo abeliano de orden p^n con sistema de divisores elementales $(p, \dots, p)$ (es decir, isomorfo a $\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$) se denomina* ***grupo abeliano elemental****.*

10.3. Grupos abelianos finitos

De los resultados de las secciones anteriores obtenemos las siguientes conclusiones.

Teorema 10.3.1. *Cada grupo abeliano finito es suma directa de p-subgrupos cíclicos. Dos descomposiciones difieren sólo en el orden de disposición de los sumandos.*

Demostración. Sea G un grupo abeliano finito de orden n

$$|G| = p_1^{n_1} \cdots p_k^{n_k},\ \ p_1 \dots p_k \ \text{ son primos diferentes.}$$

Entonces, según el teorema 10.1.1 G tiene una descomposicion única en suma directa de sus subgrupos de Sylow (sus componentes primarias),

$$G = P_1 \oplus \cdots \oplus P_k$$

Según el teorema 10.1.5 cada componente primaria P_i, $1 \le i \le k$, se descompone en suma directa de subgrupos cíclicos (componetes primarias cíclicas). Además, según el teorema 10.1.6 cada componente primaria P_i determina unívocamente el número y orden de sus subgrupos cíclicos:

$$P_1 = G_1^1 \oplus \cdots \oplus G_{t_1}^1, \quad P_2 = G_1^2 \oplus \cdots \oplus G_{t_2}^2, \quad \dots \quad , P_k = G_1^k \oplus \cdots \oplus G_{t_k}^k,$$

donde los G_j^i son p_i-subgrupos cíclicos. Entonces,

$$G = G_1^1 \oplus \cdots \oplus G_{t_1}^1 \oplus G_1^2 \oplus \cdots \oplus G_{t_2}^2 \oplus \cdots \oplus G_1^k \oplus \cdots \oplus G_{t_k}^k.$$

Si G tiene otra descomposicion en suma directa de subgrupos primarios cíclicos $G = H_1 \oplus H_2 \oplus \cdots \oplus H_\ell$, entonces podemos ordenar dichos sumandos de tal forma que colocamos todos los p_1-grupos a la izquierda, los p_2-grupos a la derecha a continuación y así sucesivamente. Según el primer teorema de Sylow en esta nueva descomposicion de G deben aparecer p_i- grupos para cada primo p_i, $1 \leq i \leq k$.

Además, según el segundo teorema de Sylow los p_i-sumandos conforman el p_i-subgrupo de Sylow de G. Luego según el teorema 10.1.6, los p_i sumandos de la nueva descomposicion deben ser tantos como t_i, $1 \leq i \leq k$, además los órdenes deben coincidir con los órdenes de $G_1^i, \ldots, G_{t_i}^i$. □

El teorema anterior describe de manera completa los grupos abelianos finitos en términos de grupos primarios cíclicos.

Corolario 10.3.2. *El número de grupos abelianos no isomorfos de orden*

$$n = p_1^{n_1} \cdots p_k^{n_k},\ p_1, \ldots, p_k \text{ primos diferentes}$$

es $p(n_1)p(n_2)\cdots p(n_k)$, *donde* $p(n_i)$ *es el número de particiones del entero positivo* n_i, $1 \leq i \leq k$.

Demostración. Consecuencia directa del teorema anterior y de la proposición 10.2.6. □

Proposición 10.3.3 (Recíproco del teorema de Lagrange para grupos abelianos finitos). *Sea* G *un grupo abeliano finito y sea* $m \in \mathbb{Z}^+$ *tal que* $m||G|$. *Entonces* G *contiene al menos un subgrupo de orden* m.

Demostración. Sea $|G| = n = p_1^{n_1} \cdots p_k^{n_k}$ y sea $m|n$, $m = p_1^{m_1} \cdots . \ p_k^{m_k}$ con $0 \leq m_i \leq n_i$, $1 \leq i \leq k$. Existen en G subgrupos $H_1, \ldots, H_k$ de órdenes $|H_i| = p_i^{m_i}$, $1 \leq i \leq k$. Como G es abeliano $H_1 \cdots H_k \leq G$. Veamos que $|H_1 \cdots H_k| = m$. Para ello probemos que $H_j \cap (H_1 \cdots H_{j-1} H_{j+1} \cdots H_k) = 1$, para cada $1 \leq j \leq k$.

Sea $x \in H_j \cap (H_1 \cdots H_{j-1} H_{j+1} \cdots H_k)$, entonces $|x| \mid p_j^{m_j}$ y $|x| \mid p_1^{m_1} \cdots p_{j-1}^{m_{j-1}} p_{j1}^{m_{j+1}} \cdots p_k^{m_k} \Rightarrow |x| \mid d$, donde $d = m.c.d.\ (p_j^{m_j}; p_1^{m_1} \cdots p_{j-1}^{m_{j-1}}\ p_{j+1}^{m_{j+1}} \cdots p_k^{m_k}) = 1 \Rightarrow |x| = 1 \Rightarrow x = 1$. □

Ejemplo 10.3.4. (i) Determinemos todos los grupos abelianos de orden 1440.

$1440 = 2^5 \times 5 \times 3^2$;
p(5): (5),(4,1),(3,2),(3,1,1),(2,2,1),(2,1,1,1),(1,1,1,1,1);
p(1)=(1);
p(2):(2),(1,1); ⇒
$\mathbb{Z}_{32} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_9; \mathbb{Z}_{32} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
$\mathbb{Z}_{16} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_9; \mathbb{Z}_{16} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
$\mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_9; \mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
$\mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_9; \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_9; \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_9; \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$,
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_9; \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
(ii)Veamos que $\mathbb{Z}_{72} \oplus \mathbb{Z}_{84} \cong \mathbb{Z}_{36} \oplus \mathbb{Z}_{168}$:
$\mathbb{Z}_{72} \oplus \mathbb{Z}_{84} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_9 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{36} \oplus \mathbb{Z}_{168}$
(iii) Son $\mathbb{Z}_{72} \oplus \mathbb{Z}_{12}$ y $\mathbb{Z}_{18} \oplus \mathbb{Z}_{48}$ isomórfos?
$\mathbb{Z}_{72} \oplus \mathbb{Z}_{12} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \quad \Rightarrow (2^3, 2^2, 3^2, 3^1)$;
$\mathbb{Z}_{18} \oplus \mathbb{Z}_{48} \cong \mathbb{Z}_9 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{16} \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{16} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \Rightarrow \ (2^4, 2^1, 3^2, 3^1)$.

Puesto que los sistemas de divisores elementales son distintos, entonces los grupos no son isomorfos.

10.4. Grupos de orden ≤ 15

Con la información obtenida en éste y el capítulo anterior podemos determinar (salvo isomorfismo) todos los grupos de oren ≤ 15.

n	**Abelianos**	**No abelianos**
1	1	
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4, V = \langle a, b \mid a^2 = 1 = b^2, ab = ba \rangle$	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6$	$D_3 = S_3$
7	$\mathbb{Z}_7$	
8	$\mathbb{Z}_8, \mathbb{Z}_4 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	D_4, Q_8
9	$\mathbb{Z}_9, \mathbb{Z}_3 \oplus \mathbb{Z}_3$	
10	$\mathbb{Z}_{10}$	D_5
11	$\mathbb{Z}_{11}$	
12	$\mathbb{Z}_{12}, \mathbb{Z}_6 \oplus \mathbb{Z}_2$	$A_4, D_6, T = \langle a, b \mid a^6 = 1, b^2 = a^3, bab^{-1} = a^{-1} \rangle$
13	$\mathbb{Z}_{13}$	
14	$\mathbb{Z}_{14}$	D_7
15	$\mathbb{Z}_{15}$	

10.5. Ejercicios

1. Determine todos los grupos abelianos de orden 1024.

2. Sean G, H grupos abelianos finitos tales que $G \times G \cong H \times H$. Demuestre que $G \cong H$.

3. Sean G, H grupos abelianos finitos tales que para cada entero positivo m ambos tienen el mismo número de elementos de orden m. Demuestre que $G \cong H$.

4. Sea G un grupo abeliano que tiene 8 elementos de orden 3, 18 elementos de orden 9 y el elemento identidad. Encuentre la descomposición de G como producto de grupos cíclicos.

Capítulo 11

Grupos solubles

En los capítulos anteriores hemos tratado con grupos abelianos y grupos finitos. Un grupo cualquiera no está obligado a pertenecer a alguna de estas clases, sin embargo, siempre se puede relacionar de alguna manera con ellas y estudiar por este camino el grupo. Una de las generalizaciones más importantes de la conmutatividad es la solubilidad, de la cual nos ocupamos en este capítulo. Es importante anotar que la solubilidad en grupos está estrechamente ligada con la solubilidad por radicales de las ecuaciones algebraicas (véase [10]). La solubilidad, será estudiada a través de los conmutadores y el conmutante de un grupo.

11.1. Centro de un grupo

Uno de los parámetros que indica el grado de conmutatividad de un grupo es la aproximación de él con su centro. A continuación repasaremos algunas nociones y propiedades introducidas en capítulos anteriores.

Proposición 11.1.1. *Sea G un grupo, H un subgrupo de G y A un subconjunto no vacío de G. Sean*

$$N_H(A) := \{x \in H | A^x := xAx^{-1} = A\},$$
$$C_H(A) := \{x \in H | a^x := xax^{-1} = a \text{ para cada } a \in A\}$$

el normalizador y centralizador de A en H, respectivamente. Entonces,

$$C_H(A) \trianglelefteq N_H(A) \leq H$$

Demostración. Nótese que $N_H(A) \neq \emptyset$ ya que $1 \in N_H(A)$. Sean $x, y \in N_H(A) \Rightarrow A^{xy} = (A^x)^y = A^y = A \Rightarrow xy \in N_H(A)$; además $A^{x^{-1}} = A$, es decir, $x^{-1} \in N_H(A)$. Esto indica que $N_H(A) \leq H$. De manera análoga se prueba que $C_H(A) \leq H$. Evidentemente $C_H(A) \leq N_H(A)$. Sean $a \in A$, $x \in N_H(A)$ y sea $y \in C_H(A) \Rightarrow xyx^{-1}a(xyx^{-1})^{-1} = xyx^{-1}axy^{-1}x^{-1} = xya_0y^{-1}x^{-1}$, donde $a_0 := x^{-1}ax \in A$; luego $xya_0y^{-1}x^{-1} = xa_0x^{-1} = a$, es decir, $xyx^{-1} \in C_H(A)$. □

Consideremos ahora el caso particular en el cual $H = G$ y $A = K$ es un subgrupo de G.

Proposición 11.1.2. *Sea G un grupo y $K \leq G$. Entonces*

(i) *$K \trianglelefteq N_G(K)$ y $N_G(K)$ es el subgrupo más grande de G en el cual K es normal.*

(ii) *$K \trianglelefteq G \Leftrightarrow N_G(K) = G$.*

Demostración. (i) La primera parte es consecuencia de la definición de normalizador.
(ii) Es una consecuencia directa de (i). □

Recordemos que so G es un grupo su centro se define como el centralizador de G en G y se denota por $Z(G)$, es decir,

$$Z(G) := \{x \in G | a^x = a \text{ para cada } a \in G\}.$$

Proposición 11.1.3. *Sea G un grupo. Entonces*

(i) *$Z(G)$ es un grupo abeliano.*

(ii) *$Z(G) \trianglelefteq G$.*

(iii) *G es abeliano $\Leftrightarrow G = Z(G)$.*

Demostración. Consecuencia directa de la definición de centro. □

11.2. Conmutante de un grupo

Además de centro, otro de los parámetros que permite establecer la "distancia"de un grupo a la conmutatividad es su conmutante. Definimos en esta lección el conmutante de dos subconjuntos cualesquiera de un grupo.

Definición 11.2.1. *Sea G un grupo cualquiera y sean a, b elementos de G. Se denomina **conmutador** de los elementos a y b al elemento $[a, b]$ de G definido por*

$$[a, b] := a^{-1}b^{-1}ab$$

*Se denomina **conmutante** de G o **subgrupo derivado** de G al subgrupo generado por los conmutadores y se denota por G' o también por $[G, G]$:*

$$G' = [G, G] := \langle [a, b] \mid a \in G, b \in G \rangle.$$

*Más generalmente, sean $L, M \subseteq G$ no vacíos. Se denomina **conmutante mutuo**, o sencillamente conmutante de L y M, al subgrupo*

$$[L, M] := \langle [a, b] \mid a \in L, b \in M \rangle.$$

Proposición 11.2.2. *Sea G un grupo y sean $L, M \trianglelefteq G$. Entonces $[L, M] \trianglelefteq G$. En particular, $G' \trianglelefteq G$.*

Demostración. Cada elemento z de $[L, M]$ es de la forma $z = z_1 \cdots z_k$, donde cada z_i, $1 \leq i \leq k$, es de la forma $[a, b]$ o $[a, b]^{-1}$ con $a \in L$, $b \in M$. Sea x un elemento cualquiera de G. Entonces $z^x = x^{-1}zx = z_1^x \cdots z_k^x$. Pero

$$[a, b]^x = [a^x, b^x] \text{ y } a^x \in L,\ b^x \in M$$
$$\left([a, b]^{-1}\right)^x = ([a, b]^x)^{-1} = [a^x, b^x]^{-1}.$$

Se obtiene entonces que $z^x \in [L, M]$, es decir, $[L, M] \trianglelefteq G$. □

Proposición 11.2.3. *Sea G un grupo. G es abeliano $\Leftrightarrow G' = 1$.*

Demostración. Evidente. □

Proposición 11.2.4. *Sea G un grupo. Si $G' \leq K \leq G$ entonces $K \trianglelefteq G$. Además, G/G' es un grupo abeliano y G' está contenido en cada subgrupo normal K de G tal que G/K sea abeliano. En particular, el máximo cardinal de G/K, con este último abeliano, es igual a $\mid G : G' \mid$.*

Demostración. Sea K tal que $G' \leq K \leq G$. Sea $x \in G$ y a un elemento cualquiera de K. Entonces $(x^{-1}ax)\, a^{-1} \in G' \underline{\trianglelefteq K \Rightarrow}\ x^{-1}ax \in K$, es decir, $K \trianglelefteq G$. Sean $x, y \in G$. Entonces, $\overline{x}^{\,-1}\, \overline{y}^{\,-1}\, \overline{xy} = \overline{x^{-1}y^{-1}xy} = \overline{1}$, es decir, $\overline{x}\,\overline{y} = \overline{y}\,\overline{x}$ y así G/G' es abeliano.

Sea ahora $K \trianglelefteq G$ tal que G/K es abeliano. Sea $z = z_1 \cdots z_k$ un elemento cualquiera de G'. Cada z_i es de la forma $[a, b] = a^{-1}b^{-1}ab$ o de la forma $[a, b]^{-1} = [b, a] = b^{-1}a^{-1}ab$, donde $a, b \in G$. Consideremos la clase de $a^{-1}b^{-1}ab$ en el cociente G/K: $\overline{a^{-1}b^{-1}ab} = \overline{a}^{\,-1}\overline{b}^{\,-1}\,\overline{a}\overline{b} = \overline{1}$, o sea que $\left(a^{-1}b^{-1}ab\right)^{-1} \in K$. De lo anterior se desprende que $z \in K$ y en total $G' \leq K$. Ademas, $\mid G \mid = \mid G : K \mid\mid K \mid \geq \mid G : K \mid\mid G' \mid \Rightarrow \mid G : G' \mid\mid G' \mid = \mid G \mid \geq \mid G : K \mid\mid G' \mid \Rightarrow \mid G : G' \mid \geq \mid G : K \mid$. □

Consideremos ahora algunas propiedades de los conmutadores y conmutantes.

Proposición 11.2.5. *Sea G un grupo tal que $G/Z(G)$ es cíclico. Entonces G es abeliano.*

Demostración. Sea x un elemento de G. Entonces, $\overline{x} = xZ(G) \in G/Z(G)$. Como este cociente es cíclico existe $a \in G$ tal que $\overline{x} = \overline{a}^{\,k}$ para algún $k \in \mathbb{Z} \Rightarrow x^{-1}a^k \in Z(G)$, es decir, existe $z \in Z(G)$ tal que $x^{-1}a^k = z \Rightarrow x = a^k z^{-1}$, es decir, x es de la forma $x = a^k\omega$, donde $\omega \in Z(G)$.

Sean x, y elementos cualesquiera de G. Entonces

$$[x, y] = x^{-1}y^{-1}xy = \left(a^{k_1}w_1\right)^{-1}\left(a^{k_2}w_2\right)^{-1} a^{k_1}w_1a^{k_2}w_2, \text{ donde } k_1, k_2 \in \mathbb{Z} \text{ y}$$
$$w_1w_2 \in Z(G);$$
$$\Rightarrow [x, y] = w_1^{-1}a^{-k_1}w_2^{-1}a^{-k_2}a^{k_1}w_1a^{k_2}w_2 = a^{-k_1-k_2+k_1+k_2} = 1,$$

es decir, x, y conmutan. Lo anterior implica que G es abeliano. □

Proposición 11.2.6. *Sea G un grupo de orden pq, donde p y q son primos diferentes, tal que $Z(G) \neq 1$. Entonces $G \cong \mathbb{Z}_{pq}$.*

Demostración. Puesto que $Z(G) \leq G$ entonces $\mid Z(G) \mid = p, q, pq$. Si $\mid Z(G) \mid = pq$ entonces es abeliano e isomorfo a $\mathbb{Z}_{pq}$. Si $\mid Z(G) \mid = p$ entonces $\mid G/Z(G) \mid = q$ y en consecuencia $G/Z(G)$ es cíclico. Según vimos G es abeliano y nuevamente $G \cong \mathbb{Z}_{pq}$. Análogamente, si $\mid Z(G) \mid = q$. □

Ejemplo 11.2.7. (i) $\mathbb{Z}' = 0$, $\mathbb{Z}'_n = 0$, $n \geq 1$; $\mathbb{Q}' = 0$, $\mathbb{R}' = 0$, $\mathbb{C}' = 0$, $\mathbb{Z}^{*'} = 1$, $\mathbb{Q}^{*'} = 1$, $\mathbb{R}^{*'} = 1$, $\mathbb{C}^{*'} = 1$, $\mathbb{C}'_{p\infty} = 1$, $\mathbb{Q}'_p = 0$.

(ii) $S'_n = A_n$: en efecto, para $n = 1, S'_1 = 1 = S_1 = A_1$. Para $n = 2, S'_2 = 1 = A_2$ ya que S_2 es abeliano. Veamos la prueba para $n \geq 3$.

Probemos en primer lugar que $A_n \subseteq S'_n$: puesto que A_n está generado por los ciclos de longitud 3 basta probar que cada ciclo (abc) de longitud 3 está en S'_n : Sean a, b, c diferentes, entonces

$$(abc) = [(ab), (ac)], \text{ en efecto}$$
$$[(ab), (ac)] = (ab)^{-1}(ac)^{-1}(ab)(ac) = (ab)(ac)(ab)(ac) = (abc).$$

$S'_n \subseteq A_n$: sean $\alpha, \beta \in S_n$. Entonces, $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$ es una permutacion par.

(iii) Calculemos ahora A'_n. Para $n = 1, A'_1 = 1$, para $n = 2, A'_2 = 1$, para $n = 3, A'_3 = 1$ ya que A_3 es abeliano.

Para $n = 4$ probemos que $A'_4 = \{1, (12)(34), (13)(24), (14)(23)\}$, es decir, $A'_4 \cong V$. Sea $L := \{1, (12)(34), (13)(24), (14)(23)\}$, veamos que$L \trianglelefteq A_n$: denotando por $a = (12)(34)$, $b = (13)(24)$, entonces $a^2 = 1 = b^2$, $ab = (14)(23) = ba$, esto prueba que el conjunto mencionado es realmente un subgrupo de A_n y además que es isomorfo al grupo de Klein.

Nótese que en L están todos los productos de dos transposiciones disyuntas. Sea $\pi \in S_n$ una permutación cualquiera de S_n y sea $(\alpha_1\alpha_2)(\beta_1\beta_2)$ uno cualquiera de tales productos. Entonces

$$\pi^{-1}(\alpha_1\alpha_2)(\beta_1\beta_2)\pi = \pi^{-1}(\alpha_1\alpha_2)\pi\pi^{-1}(\beta_1\beta_2)\pi$$
$$= (\pi(\alpha_1), \pi(\alpha_2))(\pi(\beta_1), \pi(\beta_2)) \in L;$$

lo anterior prueba que $L \trianglelefteq S_n$, en particular, $L \trianglelefteq A_n$.

$A'_4 \subseteq L$: teniendo en cuenta que A_n está generado por ciclos de longitud 3, $L \trianglelefteq A_n$ y por las fórmulas del ejercicio 4 de este capítulo, es suficiente probar que el conmutador de 2 tres-ciclos está en L. Sean i, j, k, l elementos diferentes de I_n (en particular, si $n = 4$). Entonces

$$[(ijk), (ijl)] = (ij)(kl) \in L$$
$$[(ijk), (ilj)] = (il)(jk) \in L.$$

Nótese que el conmutador $[(ijk),(lij)]$ coincide con el primero, $[(ijk),(jli)]$ también coincide con el primero.

$L \subseteq A_n^{'}$: las relaciones anteriores demuestran esta inclusión ya que además $(ik)(jl) = (il)(jk)(ij)(kl)$.

$n \geq 5 : A_n^{'} = A_n$, $n \geq 5$. En efecto, sean i, j, k, l, m elementos diferentes de I_n. Entonces $(ijk) = [(ikl),(ijm)]$ y esto prueba que $A_n \subseteq A_n^{'}$ y en consecuencia $A_n^{'} = A_n$.

Cerramos esta sección con otras propiedades de los conmutantes.

Proposición 11.2.8. *Sea G un grupo, $A, B \leq G$ y sea $H := \langle A, B\rangle$. Entonces*

(i) $[A,B], A[A,B], B[A,B] \trianglelefteq H$.

(ii) $A[A,B]B[A,B] = H$.

Demostración. (i) $[A,B] \trianglelefteq H$: sea $y \in [A,B]$ y sea $x \in H$. Queremos mostrar que $x^{-1}yx \in H$. Notemos que y es de la forma

$$y = [a_1,b_1]^{\varepsilon_1} \cdots [a_n,b_n]^{\varepsilon_n}, \tag{11.2.1}$$

donde $a_i \in A$, $b_i \in B$, $\varepsilon_i = \pm 1$, $1 \leq i \leq n$, x es de la forma

$$x = x_1^{\lambda_1} \cdots x_m^{\lambda_m}, x_i \in A \cup B, \lambda_i = \pm 1, 1 \leq i \leq m. \tag{11.2.2}$$

Basta entonces considerar los productos de la forma $x^{-1}[a,b]x$, $x^{-1}[a,b]^{-1}x$, con $a \in A, b \in B$ y $x \in A \cup B$.

$x \in A$: nótese que $x^{-1}[a,b]x = [ax,b][x,b]^{-1} \in [A,B]$ (véase el ejercicio 4).

$x^{-1}[a,b]^{-1}x = (x^{-1}[a,b]x)^{-1} \in [A,B]$

$x \in B$: $x^{-1}[a,b]x = x^{-1}[b,a]^{-1}x = (x^{-1}[b,a]x)^{-1}$

$= \left([bx,a][x,a]^{-1}\right)^{-1}$ (véase el ejercicio 4)

$= [x,a][bx,a]^{-1}$

$= [a,x]^{-1}[a,bx] \in [A,B]$.

Ahora, $x^{-1}[a,b]^{-1}x = (x^{-1}[a,b]x)^{-1} \in [A,B]$.

$A[A,B] \trianglelefteq H$: sean $y \in [A,B]$ un elemento como en (11.2.1) y sea $x \in H$ un elemento como en (11.2.2); sea además $a \in A$. Es suficiente entonces considerar solamente un producto de la forma

$$x^{-1}ayx, \text{ con } x \in A \cup B.$$

Pero $x^{-1}ayx = x^{-1}axx^{-1}yx$; según lo probado , $x^{-1}yx \in [A,B]$. Además, si $x \in A$ entonces $x^{-1}ax \in A$ y así $x^{-1}ayx \in A[A,B]$.

Si $x \in B$ entonces $x^{-1}ax = x^{-1}axa^{-1}a = [x,a^{-1}]a = [a^{-1},x]^{-1}a \in [A,B]A = A[A,B]$, y así $x^{-1}ayx \in A[A,B]$ (la última igualdad es consecuencia de que A normaliza $[A,B]$).

$B\,[A,B] \trianglelefteq H$: análogo al caso anterior pero considerando el producto $x^{-1}byx$ con $b \in B$, $y \in [A,B]$.

(ii) $A\,[A,B]\,B\,[A,B] = H$: según (i) $A\,[A,B]\,B\,[A,B] \leq H$. Puesto que $H = \langle A, B\rangle$ sea $x \in A$ o $x \in B$. Entonces $x = x \cdot 1 \cdot 1 \cdot 1 \in A\,[A,B]\,B\,[A,B]$ o $x = 1 \cdot 1 \cdot x \cdot 1 \in A\,[A,B]\,B\,[A,B]$. □

Proposición 11.2.9. *Sea $G = A \times B$, entonces $[G,G] = [A,A] \times [B,B]$. Este resultado se puede extender a un producto finito de grupos.*

Demostración. Sean $x := [a_1, b_1]$, $y := [a_2, b_2] \in G$. Se tiene entonces la identidad

$$[x, y] = ([a_1, a_2]\,, [b_1, b_2])$$

la cual inmediatamente da la inclusión de izquierda a derecha.

Para la otra inclusión observemos que cada elemento de $[A,A] \times [B,B]$ es de la forma $[c_1 \cdots c_m, d_1 \cdots d_l]$, donde c_i son conmutadores de A y d_j conmutadores de B. Se puede suponer sin pérdida de generalidad que $m = l$, y entonces se tiene $[c_1, d_1] \cdots [c_m, d_m]$ y resta aplicar otra vez la identidad de arriba. □

Ejemplo 11.2.10. Recordemos que $Q_8 = \langle a, b \mid a^4 = 1,\ b^2 = a^2,\ bab^{-1} = a^{-1}\rangle$. Calculemos $[Q_8, Q_8]$:

$b^{-1} = a^2 b, ba = a^3 b$

$\left[a^k b^i, a^r b^j\right] = (a^k b^i)^{-1}(a^r b^j)^{-1} a^k b^i a^r b^j$

$= b^{-i} a^{-k} b^{-j} a^{-r} a^k b^i a^r b^j = b^{-i} a^{-k} b^{-j} a^{k-r} b^i a^r b^j$

(a) $i = 0, j = 0 : a^{-k} a^{k-r} a^r = 1$.

(b) $i = 0, j = 1 : a^{-k} b^{-1} a^{k-r} a^r b = a^{-k} a^2 b a^k b$

$= a^{-k+2} a^{-k} b^2 = a^2 a^2 = 1$.

(c) $i = 1, j = 0 : b^{-1} a^{-k} a^{k-r} b a^r = a^2 b a^{-r} a^{3r} b = a^2 b a^{2r} b$

$= a^2 a^{6r} b^2 = a^2 a^{6r} a^2 = a^{6r} = (a^2)^{3r} \in \langle a^2\rangle$.

(d) $i = 1, j = 1 : b^{-1} a^{-k} b^{-1} a^{k-r} b a^r b = (a^2)^{9r+3k} \in \langle a^2\rangle \Rightarrow [Q_8, Q_8] = \langle a^2\rangle$ ya que tomando $r = 1$ en (c) tenemos que $a^2 \in [Q_8, Q_8]$.

11.3. Cadenas normales

Nuestro objetivo central ahora es probar los teoremas de Jordan-Hölder y Schreier sobre refinamientos isomorfos de cadenas subnormales y normales.

Definición 11.3.1. *Se denomina **cadena** de un grupo G a una sucesión finita totalmente ordenada de subgrupos de G comenzando en 1 y terminando en G:*

$$1 = H_0 \leq H_1 \leq \cdots \leq H_n = G. \tag{11.3.1}$$

*La cadena (11.3.1) se denomina **subnormal** si*

$$H_i \trianglelefteq H_{i+1}, \text{ para cada } 0 \leq i \leq n-1.$$

La cadena (11.3.1) se denomina ***normal*** *si*

$$H_i \trianglelefteq G, \text{ para } 0 \leq i \leq n.$$

Se dice que un subgrupo H de un grupo G es subnormal en G, lo cual denotamos por $H \trianglelefteq\trianglelefteq G$, si H es miembro de una cadena subnormal de G.

Los cocientes H_{i+1}/H_i, $0 \leq i \leq n-1$, se denominan ***secciones*** *de la cadena subnormal (11.3.1).*

Observación 11.3.2. Para los grupos abelianos los conceptos de cadena, cadena subnormal y normal coinciden. Evidentemente en el caso general toda cadena normal es subnormal.

Ejemplo 11.3.3. (i) $0 < 6\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z}$ y $0 < 45\mathbb{Z} < 15\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z}$ son cadenas de $\mathbb{Z}$ con secciones $6\mathbb{Z}/0 \cong \mathbb{Z}$, $3\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_2$, $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$; $45\mathbb{Z}/0 \cong \mathbb{Z}$, $15\mathbb{Z}/45\mathbb{Z} \cong \mathbb{Z}_3$, $3\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}_5$, $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$.

(ii) $1 < 2\mathbb{Z} < \mathbb{Z} < \mathbb{Q}_p$ es una cadena de $\mathbb{Q}_p$ con secciones $2\mathbb{Z}/1 \cong \mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$, $\mathbb{Q}_p/\mathbb{Z} = \mathbb{C}_{p^\infty}$.

(iii) $1 < \mathbb{C}_p < \mathbb{C}_{p^2} < \cdots < \mathbb{C}_{p^n}$ es una cadena de $\mathbb{C}_{p^n}$ con secciones isomorfas a $\mathbb{C}_p$.

(iv) $1 < \langle g \rangle < K = \{1, f^2, g, f^2g\} < D_4$ es una cadena subnormal no normal de D_4 con secciones isomorfas a $\mathbb{Z}_2$.

(v) $1 < \langle a^2 \rangle < \langle b \rangle < Q_8$; $1 < \langle a^2 \rangle < \langle a \rangle < Q_8$; $1 < \langle a^2 \rangle < \langle ab \rangle < Q_8$ son cadenas normales de Q_8 con secciones isomorfas a $\mathbb{Z}_2$. Nótese que en Q_8 toda cadena es normal ya que todos sus subgrupos son normales.

(vi) $1 < \{1, (12)(34)\} < A_4' = \{1,\ (12)(34), (13)(24),\ (14)(23)\} < A_4$ es una cadena subnormal no normal de A_4 con secciones $\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3$. En efecto, $\{1, (12)(34)\}$ no es normal en A_4 : $(123)^{-1}(12)(34)(123) = (13)(24)$.

Definición 11.3.4. *Sean*

$$1 = H_0 \leq H_1 \leq \cdots \leq H_n = G, \tag{11.3.2}$$

$$1 = K_0 \leq K_1 \leq \cdots \leq K_m = G \tag{11.3.3}$$

cadenas del grupo G.

(i) *(11.3.3) es un* ***refinamiento*** *de (11.3.2) si $\{H_0, \ldots, H_n\} \subseteq \{K_0, \ldots, K_m\}$.*

(ii) *Sean (11.3.2) y (11.3.3) cadenas subnormales (normales) de G. Se dice que ellas son* ***isomorfas*** *si $n = m$ y existe $\pi \in S_n$ tal que*

$$H_{i+1}/H_i \cong K_{\pi(i)+1}/K_{\pi(i)},\ 0 \leq i \leq n-1.$$

Ejemplo 11.3.5. (i) $0 < \mathbb{Z}_2 < \mathbb{Z}_6 < \mathbb{Z}_{12} < \mathbb{Z}_{24} < \mathbb{Z}_{48}$ es un refinamiento de la cadena $0 < \mathbb{Z}_2 < \mathbb{Z}_{12} < \mathbb{Z}_{48}$.

(ii) $0 < \mathbb{Z}_2 < \mathbb{Z}_6 < \mathbb{Z}_{24}$ y $0 < \mathbb{Z}_4 < \mathbb{Z}_{12} < \mathbb{Z}_{24}$ son cadenas normales isomorfas de $\mathbb{Z}_{24}$: $\mathbb{Z}_2/0 \cong \mathbb{Z}_2 \cong \mathbb{Z}_{24}/\mathbb{Z}_{12}$; $\mathbb{Z}_{24}/\mathbb{Z}_6 \cong \mathbb{Z}_4 \cong \mathbb{Z}_4/0$ $\mathbb{Z}_6/\mathbb{Z}_2 \cong \mathbb{Z}_3 \cong \mathbb{Z}_{12}/\mathbb{Z}_4$.

Una última definición para luego probar los principales resultados de esta sección.

Definición 11.3.6. *Sea (11.3.1) una cadena subnormal del grupo G. Se dice que (11.3.1) es una* ***cadena de composición*** *de G si*

$$H_{i+1}/H_i \text{ es simple para cada } 0 \leq i \leq n-1.$$

Si (11.3.1) es normal se dirá entonces que es una ***cadena principal*** *de G.*

Proposición 11.3.7. *Sea G un grupo con cadena subnormal (normal)*

$$1 = H_0 \leq H_1 \leq \cdots \leq H_n = G.$$

Sea $K \leq G$. Entonces

(i) $1 = K_0 \leq K_1 \leq \cdots \leq K_n = K$, *con $K_i = H_i \cap K$ es una cadena subnormal (normal) de K. Además $K_{i+1}/K_i \hookrightarrow H_{i+1}/H_i$, $0 \leq i \leq n-1$.*

(ii) *Si $K \trianglelefteq G$ entonces*

$$1 = \overline{H_0} \leq \overline{H_1} \leq \cdots \leq \overline{H_n} = G/K, \text{ con } \overline{H_i} = H_iK/K$$

es una cadena subnormal (normal) de G/K,. También, la sección $\overline{H_{i+1}}/\overline{H_i}$ es una imagen homomorfa de H_{i+1}/H_i, $0 \leq i \leq n-1$.

Demostración. (i) Sea $H_i \trianglelefteq H_{i+1}$ y sea $K_i = H_i \cap K$, con $K \leq G$. Entonces $K_i \trianglelefteq K_{i+1}$. En efecto, sea $x \in K_{i+1}$, $a \in K_i$, entonces $x \in H_{i+1} \cap K$ y $a \in H_i \cap K$, $x^{-1}ax \in H_i \cap K = K_i$ (caso subnormal).

Sea $H_i \trianglelefteq G$ y sea $x \in K$, $b \in K_i = H_i \cap K$. Entonces $x^{-1}bx \in H_i \cap K = K_i$ (caso normal). Evidentemente $K_0 = 1$ y $K_n = K$. Ahora, $\frac{K_{i+1}}{K_i} = \frac{K_{i+1}}{K_{i+1} \cap H_i} \cong \frac{K_{i+1}H_i}{H_i} \leq \frac{H_{i+1}}{H_i}$

(ii) Nótese que $\overline{H_i}$ es la imagen de H_i mediante el homomorfismo canónico.

$$j : G \to G/K;$$

por lo tanto, como $H_i \trianglelefteq H_{i+1}$, entonces $j(H_i) = \overline{H_i} \trianglelefteq j(H_{i+1}) = \overline{H_{i+1}}$. Por ser j sobre y $H_i \trianglelefteq G$, entonces $j(H_i) = \overline{H_i} \trianglelefteq G/K$. Evidentemente $\overline{H_0} = 1$ y $\overline{H_n} = G/K$. Ahora,

$$\frac{\overline{H_{i+1}}}{\overline{H_i}} = \frac{\frac{H_{i+1}K}{K}}{\frac{H_iK}{K}} \cong \frac{H_{i+1}K}{H_iK} \cong \frac{H_{i+1}}{H_i(H_{i+1}\cap K)} \cong \frac{\frac{H_{i+1}}{H_i}}{\frac{H_i(H_{i+1}\cap K)}{H_i}}.$$

□

En la demostración anterior se usó la siguiente forma generalizada del teorema de isomorfismo:

$$A \trianglelefteq B \leq G,\ H \trianglelefteq G; \text{ entonces } \frac{BH}{AH} \cong \frac{B}{A(B\cap H)}.$$

En efecto, $BH = HB$ ya que $H \trianglelefteq G$; $AH = HA$ ya que $H \trianglelefteq G$; evidentemente $AH \leq BH$, $AH \trianglelefteq BH$ ya que $A \trianglelefteq B$ y $H \trianglelefteq G$. Consideremos el homomorfismo natural $\alpha : B \to BH \to BH/AH$, $b \to b \to \overline{b} := bAH$ Nótese que α es sobre y que $\ker(\alpha) = B \cap AH$. En efecto, sean $\overline{bh} \in BH/AH$. Entonces $\alpha(b) = \overline{bh}$ ya que $\overline{b} = \overline{bh}$ $(bhb^{-1} \in H \leq AH)$; $\alpha(b) = \overline{1} \Rightarrow b \in AH \Rightarrow b \in B \cap AH$. Resta probar que $B \cap AH = A(B \cap H)$ $x \in B \cap AH \Rightarrow x = ah$, nótese que $h = a^{-1}x \in B$ ya que $x \in B$ y $a^{-1} \in A \leq B$; $\Rightarrow x \in A(B \cap H)$. Sea ahora $z \in A(B \cap H) \Rightarrow z = ah$, con $h \in B \cap H \Rightarrow z \in AH$ y $z \in B$. Esto demuestra la afirmación.

Lema 11.3.8 (Lema de Zassenhaus). *Sean G un grupo, H, $K \leq G$ y $H^* \trianglelefteq H$, $K^* \trianglelefteq K$. Entonces*

(i) $H^*(H \cap K^*) \trianglelefteq H^*(H \cap K)$.

(ii) $K^*(H^* \cap K) \trianglelefteq K^*(H \cap K)$.

(iii) $H^*(H \cap K)/H^*(H \cap K^*) \cong K^*(H \cap K)/K^*(H^* \cap K) \cong (H \cap K)/[(H^* \cap K)(H \cap K^*)]$.

Demostración. Probemos inicialmente que los productos de subgrupos indicados son realmente grupos.

$H^*(H \cap K)$ es un grupo: ya que $H^* \trianglelefteq H$, entonces $H^*(H \cap K) = (H \cap K)H^*$.

$K^*(H \cap K)$ es un grupo: ya que $K^* \trianglelefteq K$. entonces $K^*(H \cap K) = (H \cap K)K^*$.

$H^*(H \cap K^*)$ es un grupo: ya que $H^* \trianglelefteq H$.

$K^*(H^* \cap K)$ es un grupo: ya que $K^* \trianglelefteq K$.

$(H^* \cap K)(H \cap K^*)$ es un grupo: nótese que $H^* \cap K$, $H \cap K^* \trianglelefteq H \cap K$; por tal razón $(H^* \cap K)(H \cap K^*) \trianglelefteq H \cap K$.

Podemos ya probar las afirmaciones del lema.

(i) $H^*(H \cap K^*) \trianglelefteq H^*(H \cap K)$: Consideremos la función

$$\theta : H^*(H \cap K) \to (H \cap K)/[(H^* \cap K)(H \cap K^*)]$$
$$\theta(hx) := xL,$$

con $L := [(H^* \cap K)(H \cap K^*)]$, $h \in H^*$, $x \in H \cap K$.

θ está bien definida: $h_1, h_2 \in H^*$, $x_1, x_2 \in H \cap K$ tales que $h_1x_1 = h_2x_2 \Rightarrow \theta(h_1x_1) = x_1L, \theta(h_2x_2) = x_2L$. Entonces $x_1x_2^{-1} = h_1^{-1}h_2 \in H^* \cap (H \cap K) = H^* \cap K \subseteq L \Rightarrow x_1L = x_2L \Rightarrow \theta(h_1x_1) = \theta(h_2x_2)$.

θ es un homomorfismo: como $H^* \trianglelefteq H$ entonces $x_1H^* = Hx_1^*$ para $x_1 \in H \cap K$, por tal razón

$$\theta(h_1x_1h_2x_2) = \theta(h_1h_3x_1x_2) = x_1x_2L = x_1Lx_2L = \theta(h_1x_1)\theta(h_2x_2)$$

θ es evidentemente sobre. $\theta(hx) = L \Leftrightarrow xL = L \Leftrightarrow x \in L \Leftrightarrow hx \in H^*L \Leftrightarrow hx \in H^*(H^* \cap K)(H \cap K^*) = H^*(H \cap K^*) \Rightarrow \ker(\theta) = H^*(H \cap K^*)$

Hemos probado que $H^*(H \cap K^*) \trianglelefteq H^*(H \cap K)$ y además $\frac{H^*(H\cap K)}{H^*(H\cap K^*)} \cong \frac{(H\cap K)}{L}$.

(ii) Se prueba como (i) y se establece la última parte de (iii). □

Teorema 11.3.9 (Teorema de Schreier). *Cualesquiera dos cadenas subnormales (normales) de un grupo tienen refinamientos isomorfos.*

Demostración. Sea G un grupo y sean

$$1 = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_n = G, \tag{11.3.4}$$

$$1 = K_0 \leq K_1 \leq K_2 \leq \cdots \leq K_m = G \tag{11.3.5}$$

dos cadenas subnormales de G. Para cada $0 \leq i \leq n-1$ insertamos entre H_i y H_{i+1} una sucesión ordenada de subgrupos (no necesariamente diferentes)

$$H_i = H_i(H_{i+1} \cap K_0) \leq H_i(H_{i+1} \cap K_1) \leq \cdots . \leq H_i(H_{i+1} \cap K_m) = H_{i+1}.$$

Sea $H_{i,j} = H_i(H_{i+1} \cap K_j)$, $0 \leq i \leq n-1$, $0 \leq j \leq m$. Nótese que $H_{i,m} = H_{i+1} = H_{1+i,0}$, $0 \leq i \leq n-1$. Según el lema de Zassenhaus se obtiene una nueva cadena subnormal de G que es refinamiento de (11.3.4):

$$\begin{aligned} 1 = H_{0,0} \leq H_{0,1} \leq \cdots \leq H_{0,m-1} \leq H_{1,0} \leq H_{1,1} \leq \cdots \leq H_{1,m-1} \\ \leq H_{2,0} \leq H_{2,1} \leq \cdots \leq H_{2,m-1} \leq H_{3,0} \leq \cdots \leq H_{n-1,0} \\ \leq H_{n-1,2} \leq \cdots . \leq H_{n-1,m-1} \leq H_n = G \end{aligned} \tag{11.3.6}$$

Nótese que esta nueva cadena subnormal tiene $nm+1$ subgrupos (no necesariamente diferentes). Lo mismo podemos hacer con la cadena (11.3.5) obteniéndose la cadena subnormal (11.3.7) que es refinamiento de (11.3.5) y que contiene también $nm+1$ subgrupos (no necesariamente diferentes):

$$\begin{aligned} 1 = K_{0,0} \leq K_{0,1} \leq \cdots \leq K_{0,n-1} \leq K_{1,0} \leq K_{1,1} \leq \cdots \leq K_{1,n-1} \\ \leq K_{2,0} \leq K_{2,2} \leq \cdots \leq K_{2,n-1} \leq K_{3,0} \leq \cdots \leq K_{m-1,0} \\ \leq K_{m-1,2} \leq \cdots \leq K_{m-1,n-1} \leq K_m = G, \end{aligned} \tag{11.3.7}$$

donde $K_{j,i} = K_j(K_{j+1} \cap H_i)$, $0 \leq j \leq m-1$, $0 \leq i \leq n$, $K_{j+1,0} = K_{j,n} = K_{j+1}$, $0 \leq j \leq m-1$. Nótese que para cada $0 \leq i \leq n-1$ y $0 \leq j \leq m-1$

$$\frac{H_{i,j+1}}{H_{i,j}} \cong \frac{K_{j,i+1}}{K_{j,i}}. \tag{11.3.8}$$

En efecto, $\frac{H_{i,j+1}}{H_{i,j}} = \frac{H_i(H_{i+1} \cap K_{j+1})}{H_i(H_{i+1} \cap K_j)} \cong \frac{K_j(K_{j+1} \cap H_{i+1})}{K_j(K_{j+1} \cap H_i)}$; el último isomorfismo es debido al lema de Zassenhaus.

Sean

$$I = \{(i,j) \mid 0 \leq i \leq n-1, 0 \leq j \leq m-1\} \cup \{(n,0)\},$$
$$J = \{(r,s) \mid 0 \leq r \leq m-1, 0 \leq s \leq n-1\} \cup \{(m,0)\}$$

los conjuntos que indizan (11.3.6) y (11.3.7), respectivamente. Sea

$$I' := \{k \in \mathbb{Z} \mid 0 \leq k \leq nm\},$$

nótese que I, J, I' son equipotentes $|I| = |J| = |I'| = nm + 1$. Podemos entonces indizar (11.3.6) y (11.3.7) por medio de I' :

$$\begin{array}{cc} I \to I' & J \to I' \\ (i,j) \to im + j & (r,s) \to rn + s \\ (n,0) \to nm & (m,0) \to mn \\ 0 \leq i \leq n-1 & 0 \leq r \leq m-1 \\ 0 \leq j \leq m-1 & 0 \leq s \leq n-1 \end{array}$$

En la nueva notación:

$$H_{i,j} = H_{im+j}\ ,\ H_{n,0} = H_{nm},\ 0 \leq i \leq n-1,\ 0 \leq j \leq m-1;$$
$$K_{r,s} = K_{rm+s}\ ,K_{m,0} = K_{mn},\ 0 \leq r \leq m-1,\ 0 \leq s \leq n-1.$$

Sea ahora S_{nm} el conjunto de permutaciones del conjunto $I_0 := \{0, 1 \ldots, nm-1\}$. Entonces la función

$$I_0 \to I_0$$
$$\pi : k = im + j \to jn + i,\ \ 0 \leq i \leq n-1,\ 0 \leq j \leq m-1$$

es tal que $\pi \in S_{nm}$ y además:

$$H_{k+1}/H_k = H_{im+j+1}/H_{im+j} = H_{i,j+1}/H_{i,j},$$
$$K_{\pi(k)+1}/K_{\pi(k)} = K_{jn+i+1}/K_{jn+i} = K_{j,i+1}/K_{j,i};$$

según (11.3.8) $H_{k+1}/H_k \cong K_{\pi(k)+1}/K_{\pi(k)}$, $k \in I_0$.

Con esto termina la prueba del teorema para el caso subnormal. Para el caso normal basta observar que $H_i \trianglelefteq G$, $0 \leq i \leq n$ y $K_j \trianglelefteq G$, $0 \leq j \leq m$, y entonces $H_{i,j} \trianglelefteq G$, $K_{j,i} \trianglelefteq G$. □

Teorema 11.3.10 (Teorema de Jordan-Hölder). *Cualesquiera dos cadenas de composición (principales) de un grupo son isomorfas.*

Demostración. Sean $\{H_i\}$ y $\{K_j\}$ dos series de composición (principales) del grupo G. Según el teorema 11.3.9 ambos tienen refinamientos isomorfos. Pero como H_i es maximal en H_{i+1} $0 \leq i \leq n-1$ y K_j es maximal en K_{j+1}, $0 \leq j \leq m-1$, entonces los refinamientos coinciden con las cadenas iniciales. □

Corolario 11.3.11. *Si el grupo G tiene una cadena de composición (principal) y N es un subgrupo normal propio de G, entonces G tiene una cadena de composición (principal) que contiene a N.*

Demostración. La cadena $1 < N < G$ es subnormal y normal en G. Consideremos inicialmente el caso subnormal. Sea $\{H_i\}$ una cadena de composición de G. Según el Teorema 1, $1 < N < G$ tiene un refinamiento subnormal isomorfo a un refinamiento de $\{H_i\}$. Pero como $\{H_i\}$ es de composición, entonces dicho refinamiento de $1 < N < G$ es una serie de composición. De manera análoga se argumenta el caso principal. □

11.4. Grupos solubles

Teorema 11.4.1. *Sea G un grupo. Entonces las siguientes condiciones son equivalentes:*

(i) *G posee una cadena subnormal con secciones abelianas.*

(ii) *La cadena de conmutantes*

$$G \geq G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(m)} \geq \cdots$$

del grupo G se estabiliza en 1 después de un número finito de pasos, donde

$$G^{(k)} := [G^{(k-1)}, G^{(k-1)}],\ k \geq 1;\ G^{(0)} := G.$$

(iii) *G posee una cadena normal con secciones abelianas.*

Demostración. (i) ⇒(ii): supóngase que

$$1 = H_0 \leq H_1 \leq \cdots \leq H_n = G$$

es una cadena subnormal de G con secciones abelianas. Puesto que $H_{n-1} \trianglelefteq G$ y G/H_{n-1} es abeliano entonces de acuerdo con la proposición 11.2.4, $G' \leq H_{n-1}$. Supóngase inductivamente que $G^{(k)} \leq H_{n-k}$, $1 \leq k \leq n$. De nuevo, como $H_{n-k-1} \trianglelefteq H_{n-k}$ y H_{n-k}/H_{n-k-1} es abeliano $(H_{n-k})' \leq H_{n-k-1}$, pero $(G^{(k)})' \leq (H_{n-k})'$, luego $G^{(k+1)} \leq H_{n-k-1}$. Así pues por inducción, $G^{(n)} \leq H_{n-n} = 1 \Rightarrow G^{(n)} = 1$.

(ii) ⇒(iii): según la proposición 11.2.2, $G^{(k)} \trianglelefteq G$, para cada $1 \leq k \leq n$.

(iii) ⇒(i): evidente. □

Definición 11.4.2. *Un grupo G se dice que es* ***soluble*** *si satisface una cualquiera de las condiciones del teorema anterior.*

Corolario 11.4.3. (i) *Si G es soluble entonces cada subgrupo de G es soluble y cada imagen homomórfica de G es soluble.*

(ii) *$G_1 \times \cdots \times G_n$ es soluble $\Leftrightarrow$ G_i es soluble, para cada $1 \leq i \leq n$.*

Demostración. (i) Es consecuencia directa de la proposición 11.3.7.

(ii) $\Rightarrow$): consecuencia (i).

$\Leftarrow$): se $k := \max\{k_i\}_{1\leq i\leq n}$, donde k_i es el ***grado de solubilidad*** de G_i, es decir, el menor entero positivo k tal que $G^{(k)} = 1$. Pero $[G_1 \times \cdots \times G_n, G_1 \times \cdots \times G_n] = [G_1, G_1] \times \cdots \times [G_n, G_n]$, luego $G_1 \times \cdots \times G_n$ es soluble de grado k. □

Ejemplo 11.4.4. (i) Todo grupo abeliano es soluble. El concepto de solubilidad tiene entonces interés para los grupos no abelianos.

(ii) S_3 es soluble: $[S_3, S_3] = A_3$, $[A_3, A_3] = 1$.

(iii) S_4 es soluble: $[S_4, S_4] = A_4$, $[A_4, A_4] = V$, $\quad [V, V] = 1$.

(iv) S_n no es soluble para $n \geq 5$: $[S_n, S_n] = A_n$, $\quad [A_n, A_n] = A_n$.

(iv) $[Q_8, Q_8] = \langle a^2 \rangle$, $[\langle a^2 \rangle, \langle a^2 \rangle] = 1 \Rightarrow Q_8$ es soluble.

11.5. Ejercicios

1. Sea G un grupo y sean $L, M \subseteq G$ no vacíos. Entonces $[L, M] = [M, L]$.

2. Sea G un grupo y $K \trianglelefteq G$. Entonces pruebe que el conmutante K' de K es normal en G.

3. Sea $\varphi : G_1 \to G_2$ un homomorfismo de grupos. Pruebe que $\varphi(G_1') \subseteq G_2'$. Además, si φ es sobre entonces $\varphi(G_1') = G_2'$

4. Demuestre que

$$\begin{aligned} b^{-1}[a, c]b &= [ab, c]\,[b, c]^{-1} \\ a\,[b, a]\,a^{-1} &= [a^{-1}, b], \\ [a, b]^{-1} &= [b, a]. \end{aligned}$$

5. Sean A, B, C subgrupos normales de G. Entonces $[AB, C] = [A, C]\,[B, C]$.

6. Calcule $[D_4, D_4]$, $[D_n, D_n]$.

7. Calcule $[G_{pq}, G_{pq}]$.

8. Calcule $[T, T]$.

9. Encuentre refinamientos isomorfos de las cadenas normales

$$0 < 60\mathbb{Z} < 20\mathbb{Z} < \mathbb{Z},$$
$$0 < 45\mathbb{Z} < 48\mathbb{Z} < \mathbb{Z}.$$

10. Encuentre todas las cadenas de composición de $\mathbb{Z}_{60}$ y muestre que son isomorfas.

11. Encuentre todas las cadenas de composición de $S_3 \times \mathbb{Z}_2$ y pruebe que son isomorfas.

12. ¿Es D_4 soluble?

13. ¿Es D_n soluble?

14. ¿Es G_{pq} soluble?

15. ¿Es T soluble?

16. Determine $Z(T)$, $Z(G_{pq})$

Solución. Comencemos calculando la tabla del grupo T a partir de las relaciones que definen este grupo, $a^6 = 1$, $b^2 = a^3$, $ba = a^{-1}b$:

$\cdot$	1	a	a^2	a^3	a^4	a^5	b	ab	a^2b	a^3b	a^4b	a^5b
1	1	a	a^2	a^3	a^4	a^5	b	ab	a^2b	a^3b	a^4b	a^5b
a	a	a^2	a^3	a^4	a^5	1	ab	a^2b	a^3b	a^4b	a^5b	b
a^2	a^2	a^3	a^4	a^5	1	a	a^2b	a^3b	a^4b	a^5b	b	ab
a^3	a^3	a^4	a^5	1	a	a^2	a^3b	a^4b	a^5b	b	ab	a^2b
a^4	a^4	a^5	1	a	a^2	a^3	a^4b	a^5b	b	ab	a^2b	a^3b
a^5	a^5	1	a	a^2	a^3	a^4	a^5b	b	ab	a^2b	a^3b	a^4b
b	b	a^5b	a^4b	a^3b	a^2b	ab	a^3	a^2	a	1	a^5	a^4
ab	ab	b	a^5b	a^4b	a^3b	a^2b	a^4	a^3	a^2	a	1	a^5
a^2b	a^2b	ab	b	a^5b	a^4b	a^3b	a^5	a^4	a^3	a^2	a	1
a^3b	a^3b	a^2b	ab	b	a^5b	a^4b	1	a^5	a^4	a^3	a^2	a
a^4b	a^4b	a^3b	a^2b	ab	b	a^5b	a	1	a^5	a^4	a^3	a^2
a^5b	a^5b	a^4b	a^3b	a^2b	ab	b	a^2	a	1	a^5	a^4	a^3

De la tabla se observa que el centro de T es $\{1, a^3\} \cong \mathbb{Z}_2$. De otra parte, G_{pq} es el grupo no abeliano de orden pq donde p, q son primos distintos ; esto implica que $G_{pq}/Z(G_{pq})$ no puede ser cíclico (véase la proposición 11.2.5). En cosencuencia el único orden posible de $Z(G_{pq})$ es 1, es decir, $Z(G_{pq}) = 1$.

Bibliografía

[1] **Cohn, P.M.**, *Basic Algebra: groups, rings and fields*, Springer, 2003.

[2] **Corry, L.**, *Modern Algebra and the Rise of Mathematical Structures*, Springer, 2003.

[3] **Herstein, I.N.**, *Topics in Algebra*, 2nd. edition, John Wiley, 1975.

[4] **Hungerford, T.W.**, *Algebra*, Springer, 2003.

[5] **Kargapolov M.I. and Merzljakov, J. I.**, *Fundamentals of the Theory of Groups*, 2nd ed., translated from the Russian by R. G. Burns, Springer, 1979.

[6] **Kostrikin, A.I.**, *Introducción al Álgebra*, Mir, 1980.

[7] **Lang, S.**, *Algebra*, Springer, 2004. iv

[8] **Lezama, O. and Villamarín, G.**, *Anillos, Módulos y Categorías*, Facultad de Ciencias, Universidad Nacional de Colombia, 1994. iv

[9] **Lezama, O.**, *Cuadernos de Álgebra, No. 3: Módulos*, SAC^2, Departamento de Matemáticas, Universidad Nacional de Colombia, sede de Bogotá, `www.matematicas.unal.edu.co/sac2` 115

[10] **Lezama, O.**, *Cuadernos de Álgebra, No. 5: Cuerpos*, en preparación. 121

[11] **Robinson, D.**, *A Course in the Theory of Gropus*, Springer, 1982.

[12] **Spindler, K.**, *Abstract Algebra with Applications, Vol. I, II*, Marcel Dekker, 1994.

[13] **van der Waerden, B.L.**, *Algebra, Vol. I, II*, Springer, 1991.