Este trabajo está dedicado a la memoria de:

Juana Mora Muñoz (1909-2004), mi madre, quién me dio mucho más que la vida.

Amancio Pedro Villanueva Salmerón (1941-2004), camarada y amigo entrañable, de quién recibí apoyo en los momentos más difíciles en mi vida de estudiante.

PRESENTACIÓN

La Universidad Autónoma del Estado de Hidalgo (UAEH) y la Sociedad Matemática Mexicana (SMM) se complacen en presentar esta primera publicación conjunta de la obra *Introducción a la Teoría de Grupos* del Dr. Fernando Barrera Mora, Profesor Investigador del Centro de Investigación en Matemáticas (CIMA) de la UAEH y miembro activo de la SMM.

La edición de esta obra se enmarca en el programa que está desarrollando la presente gestión rectoral de la UAEH, una de cuyas componentes es impulsar la elaboración de libros de texto, para integrar un acervo propio que incida directamente en la formación de sus estudiantes, así como dar a conocer, a nivel nacional, las obras que producen sus profesores investigadores. Esta estrategia coincide con el propósito fundamental que persigue la SMM para difundir la actividad matemática nacional.

Es importante señalar que la UAEH y la SMM trabajaron en estrecha colaboración para realizar el exitoso XXXVI Congreso Nacional de la SMM, celebrado en las instalaciones de la UAEH en octubre de 2003, y con la publicación conjunta de esta obra se inicia una, aún más cercana, vinculación entre el Comité de Publicaciones Electrónicas de la SMM y el Consejo Editorial de la UAEH, que conducirá a la consecución de objetivos académicos comunes.

Reiteramos el beneplácito por la edición de esta obra que nos impulsa a continuar desarrollando una participación activa de los miembros del CIMA de la UAEH en las actividades científicas de la SMM.

Lic. Juan Manuel Camacho Bertrán
Rector de la UAEH

Dr. Alejandro Díaz Barriga Casales
Presidente de la SMM

Índice general

0.1. Introducción

La teoría de grupos tiene su origen en el trabajo de E. Galois [2] sobre solubilidad por radicales de la ecuación $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$. Sin embargo, algunos resultados de la teoría de grupos habían aparecido con anterioridad en trabajos de otros matemáticos, entre los que se encuentra Cauchy [24]. Por lo anterior, es pertinente señalar que el término *grupo* es acuñado y usado sistemáticamente por Galois en su trabajo[1]: "Memoir on the Conditions for Solvability of Equations by Radicals" [6], página 101. Dado que el trabajo de Galois citado versa sobre las raíces de polinomios, el concepto de grupo usado por Galois se restringe a lo que hoy llamamos el *grupo de permutaciones de n elementos*.

La formulación axiomática de la teoría de grupos como se conoce actualmente, se inicia con el trabajo de H. Weber: "Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie". Math. Ann. **43** (1893), 521-549, página 522.

Hoy en día, la teoría de grupos es una de las áreas de matemáticas que más aplicaciones tiene. Éstas van desde las ciencias exactas hasta la música. En las ciencias exactas, las aplicaciones incluyen áreas tales como geometría algebraica, teoría de números y topología algebraica; en física y química su aplicación tiene lugar en el estudio de simetrías de las estructuras moleculares, mientras que en la música, una fuente que da cuenta de su aplicación es [16].

En este texto introductorio a la teoría de grupos presentamos una discusión de los conceptos y resultados básicos, pero fundamentales, que se presentan en un primer curso de teoría de grupos de una licenciatura en matemáticas. Como requisito para una mejor comprensión de los temas, esperamos que los lectores estén familiarizados con los resultados básicos de álgebra lineal, cálculo diferencial y con la notación estándar de la teoría de conjuntos. Los contenidos se pueden cubrir en un curso semestral de 60 horas.

La presentación de los temas está acompañada por listas de ejercicios que tienen la finalidad de auxiliar al lector en el aprendizaje de los contenidos y procesos necesarios para lograr un entendimiento profundo de los conceptos básicos de la teoría de grupos. Por esta razón, recomendamos al lector abordar y, de ser posible, resolver todos los ejercicios planteados en el texto. De

[1] Los interesados en estudiar la versión original de los trabajos de Galois pueden consultar [2].

manera adicional, presentamos un par de problemas abiertos, Problemas 3.3.1 y 3.3.2 página 98, que el lector interesado en la teoría de automorfismos de grupos puede explorar. Estos problemas tienen como finalidad mostrar al lector que desde un curso introductorio se pueden abordar problemas que lleven a nuevos resultados.

Los principales teoremas que se discuten en este texto son: el Teorema de Lagrange, el Teorema de la Correspondencia, los Teoremas de Isomorfismo, los Teoremas de Sylow, el Teorema Fundamental para grupos abelianos finitos y algunos resultados sobre grupos solubles y nilpotentes. También se presenta la clasificación de los grupos de orden ≤ 15. El estudio y clasificación de los grupos de orden 16 llevaría a un trabajo que sale de los objetivos del presente; sin embargo, para el lector interesado en este tema le sugerimos consultar [17], en donde se estudian algunos grupos de orden potencia de 2.

Para finalizar, quiero expresar mi agradecimiento a todas las personas que hicieron posible la elaboración de este trabajo, muy especialmente a los revisores por sus valiosas sugerencias y recomendaciones para mejorar la presentación del texto. Los errores que contenga la obra son de mi absoluta responsabilidad.

Pachuca, Hidalgo, septiembre de 2004

Fernando Barrera Mora

Prólogo

La Teoría de Grupos es la más poderosa e influyente de toda la Matemática. Su éxito es enorme, influye en casi toda la Matemática y en otras disciplinas científicas y artísticas. Un lego y un experto en la materia siempre resultan enormemente impactados del quehacer y creatividad de unos cuantos seres humanos dedicados a esta noble actividad, producto de la evolución del pensamiento humano.

Algunos sistemas numéricos son conocidos por el común de la gente, sin embargo, difícilmente perciben que realmente lo que se ha hecho en Teoría de Grupos, es extraer lo esencial de dichos sistemas y otras situaciones, a saber, dado un conjunto no vacío definimos una operación binaria en él, tal que cumpla ciertos axiomas, es decir, le damos una estructura de grupo.

Este texto está muy bien escrito, con un lenguaje muy preciso. El temario que posee es completo y expuesto breve y concisamente. A diferencia de otros textos extranjeros, el autor expone el mismo temario utilizando pocas páginas y lo hace de manera elegante.

El texto tiene una característica importante. Requiere de un buen trabajo desarrollado por el profesor al exponer cada tema así como el del alumno para asimilarlo. Esto es, el texto está escrito dejando un buen número de detalles en las demostraciones que le permiten al profesor exponer lo relevante, sugerir algunos detalles y a los alumnos la oportunidad de obtener formación matemática al trabajar en dichos detalles. Esta característica está realizada consciente y convincentemente por el autor. Algunos ejercicios son retos mayúsculos para el estudiante. Pero así es el aprendizaje serio de la Matemática.

Es un gusto enorme tener un libro bien escrito por un matemático mexicano, quien profesa un gran amor a su profesión plasmado a lo largo del texto y que tendrá una gran difusión al alcance de toda la comunidad matemática, en especial la hispanoamericana, que tanta necesidad tiene de acceder a libros como éste. Con esta publicación se inicia la serie de publicaciones de libros de texto que el Centro de Investigación en Matemáticas de la Universidad Autónoma del Estado de Hidalgo (UAEH) tiene planeada como parte del quehacer académico que le dio origen.

Esta primera edición se realiza en forma conjunta entre la UAEH y la Sociedad Matemática Mexicana (SMM) y tiene dos versiones, una electrónica que está a cargo de la SMM y la otra impresa que realiza la UAEH.

Emilio Lluis Puebla
Miembro del Comité Editorial de la Sociedad Matemática Mexicana

Capítulo 1

Definiciones y resultados generales

1.1. Algunas propiedades de los enteros

Es difícil, por no decir imposible[1], encontrar áreas de las matemáticas que no hagan uso de las propiedades aritméticas básicas de los enteros, la teoría de grupos no es la excepción. Con esto en mente, queremos iniciar la discusión de este trabajo presentando algunas propiedades de los enteros. Antes de iniciar, es importante aclarar aspectos relacionados con la notación y la terminología que usaremos en la discusión. Se usarán los símbolos usuales de la teoría de conjuntos para denotar, pertenencia, subconjuntos, complementos, etc. Sin mayor explicación se usarán algunas propiedades de los números reales y complejos. Los conjuntos de los números naturales, enteros, racionales, reales y complejos serán denotados por $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ respectivamente. El símbolo $\Rightarrow\Leftarrow$ lo usaremos para expresar que se ha llegado a una contradicción en algún argumento. El símbolo $\blacksquare$ se usará para indicar el fin de una prueba.

1.1.1. Aritmética en $\mathbb{Z}$

Es bien sabido que al considerar dos enteros a y b, el cociente de a por b no siempre deja residuo cero, lo que da lugar al concepto de *divisibilidad*, uno de los más importantes en *teoría de números*. De manera precisa se tiene:

[1]Este enunciado es una forma de parafrasear al Matemático L. Kronecker (1823-1891): *Dios creo a los números naturales, todo lo demás es producto del hombre.*

1.1.1 Definición *Si a y b son números enteros, se dice que b **divide** a a o que b es un **divisor** de a, denotado $b|a$, si existe un entero c tal que $a = bc$. Si no existe c tal que $a = cb$, se dice que b no es divisor de a y se denota por $b\nmid a$.*

Para subsanar el problema de la no divisibilidad se tiene el siguiente resultado, el cual de manera precisa establece la relación que guardan dos enteros al ser dividido uno por el otro.

1.1.1 Teorema (Algoritmo de la división) *Para cualesquiera $a, b \in \mathbb{Z}$, $b > 0$, existen únicos enteros r y q tales que $a = bq + r$, con $0 \leq r < b$.*

Demostración. `Caso I.` $a \geq 0$. En este caso podemos aplicar inducción. Si $a = 0$ se tiene $0 = b \cdot 0 + 0$, de esta manera se puede suponer que $a > 0$. Si $a = 1$ se tienen dos subcasos: si $b = 1$ entonces $1 = 1 \cdot 1 + 0$. Si $b > 1$, entonces $a = b \cdot 0 + a$. Supongamos $a > 1$ y apliquemos la hipótesis inductiva, es decir, se cumple que $a = bq + r$, con $0 \leq r < b$. Entonces $a + 1 = bq + 1 + r$. Como $r < b$, entonces $r + 1 \leq b$. Si $r + 1 = b$, se tiene $a + 1 = (b + 1)q + 0$. Si $r + 1 < b$, obtenemos $a + 1 = bq + (r + 1)$, con $0 \leq r + 1 < b$. De cualquier forma se tiene $a = bq + r$, con $0 \leq r < b$ como se afirmó.

`Caso II` $a < 0$, entonces $-a > 0$. Del Caso I, $-a = bq_1 + r_1$, $0 \leq r_1 < b$, de esto $a = b(-q_1) + (-r_1)$. Si $r_1 = 0$ hemos terminado, si $r_1 > 0$ entonces $0 < b < b + r_1$ y $a = b(-q_1 - 1) + (b - r_1)$, con $0 < b - r_1 < b$.

`Unicidad`. Supongamos $a = bq + r = bq' + r'$, entonces $b(q - q') = r' - r$. Si $r' > r$, se tiene $q - q' > 0$, es decir, $q - q' \geq 1$, de esta forma $b(q - q') = r' - r \geq b$ y de esto último, $r' \geq b + r$, $\Rightarrow\Leftarrow$. Si $r > r'$, entonces $q' - q > 0$ y nuevamente se tiene una contradicción, por lo que se debe tener $r = r'$ y $q - q' = 0$. ■

1.1.1 Observación El teorema anterior puede extenderse suponiendo $b \neq 0$. Si $b < 0$ entonces $-b > 0$ y por el teorema concluimos que $a = -bq + r = b(-q) + r$, con $0 \leq r < -b$.

1.1.2 Definición *Un entero $p \in \mathbb{N}\backslash\{1\}$ es primo, si los únicos divisores positivos de p son 1 y p.*

1.1.3 Definición *Dados $a, b \in \mathbb{Z}$, se dice que $d \in \mathbb{Z}^+$ es* ***un máximo común divisor****, abreviado* mcd*, de a y b si*

(i) $d \mid a$ *y* $d \mid b$.

(ii) Si otro entero d' satisface: $d' \mid a$ y $d' \mid b$ entonces se debe tener que $d' \mid d$.

1.1.2 Observación Si d y d_1 satisfacen (i) y (ii) entonces $d = d_1$. El máximo común divisor de a y b se denota por $\text{mcd}(a, b)$.

Demostración. Como d_1 satisface *(i)* y *(ii)*, entonces $d \mid d_1$. Cambiando los papeles entre d y d_1 y argumentando como antes se tiene que $d_1 \mid d$; dado que ambos son positivos se concluye lo deseado.

1.1.2 Teorema *Dados dos enteros a, b con al menos uno diferente de cero, entonces el* $\text{mcd}(a, b)$ *existe y* $\text{mcd}(a, b) = d = ax + by$*, para algunos enteros x, y.*

Demostración. Sea $S = \{ax + by | x, y \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Se tiene $\pm a, \pm b \in S$. Debido a que al menos uno de a ó b no es cero, entonces S tiene elementos positivos, de esta manera $S \cap \mathbb{N} \neq \emptyset$. Por el principio del buen orden en $\mathbb{N}$, existe un elemento mínimo $d \in S$. La demostración concluirá si probamos la siguiente: **Afirmación**. $d = \text{mcd}(a, b)$. Primeramente se mostrará que d divide a cualquier elemento de S. Sea $ax + by \in S$, por el algoritmo de la division, existen $q, r \in \mathbb{Z}$ tales que $ax + by = qd + r$, con $0 \leq r < d$. También se tiene que $d = ax_0 + by_0$, para algunos $x_0, y_0 \in \mathbb{Z}$, por lo que $ax + by - qd = ax + by - qx_0a - qy_0b = (x - qx_0)a + (y - qy_0)b = r$ y de esto se concluye que $r \in S$. La minimalidad sobre d implica $r = 0$. Como $a, b \in S$ entonces $d|a$ y $d|b$. Si $d_1 \mid a$ y $d_1 \mid b$, entonces $d_1 \mid ax_0 + by_0 = d$, y de ésto se tiene que $d = \text{mcd}(a, b)$. ■

1.1.4 Definición *Dos enteros a y b se dicen primos relativos si* $\text{mcd}(a, b) = 1$.

1.1.1 Corolario *Dados $a, b \in \mathbb{Z}$, a y b son primos relativos $\iff$ existen $a_0, b_0 \in \mathbb{Z}$ tales que $1 = aa_0 + bb_0$.*

Demostración. Del teorema anterior se tiene $\text{mcd}(a, b) = d = aa_0 + bb_0$, para algunos enteros a_0, b_0. Si $d = 1$ entonces $1 = aa_0 + bb_0$. Por otro lado, si $1 = aa_0 + bb_0$ y $d > 1$ entonces $d \mid aa_0 + bb_0 = 1 \Rightarrow\Leftarrow$. ■

1.1.2 Corolario *Si* $\mathrm{mcd}(a,c)=1$ *y* $c \mid ab$*, entonces* $c \mid b$*.*

Demostración. Ya que $\mathrm{mcd}(a,c)=1$, entonces del Corolario 1.1.1, existen $a_0, c_0 \in \mathbb{Z}$ tales que $1 = aa_0 + cc_0$. Multiplicando esta ecuación por b se tiene $b = baa_0 + bcc_0$. Por hipótesis $ab = cx$ para algún x, entonces $b = cxa_0 + cbc_0 = c(xa_0 + bc_0)$, es decir, $c \mid b$. ■

1.1.3 Corolario *Si* p *es primo y* $p \nmid a$*, entonces* $\mathrm{mcd}(a,p)=1$*.*

Demostración. Ya que p es primo, entonces los únicos divisores positivos de p son 1 y p. Como $p \nmid a$ entonces $\mathrm{mcd}(a,p)=1$. ■

1.1.4 Corolario *Si* p *es primo y* $p \mid ab$*, entonces* p *divide a alguno de* a *o* b*.*

Demostración. Si $p \nmid a$ entonces del Corolario 1.1.3, $\mathrm{mcd}(a,p)=1$. Del Corolario 1.1.2 se obtiene el resultado con $p = c$. ■

1.1.5 Corolario *Sean* a *y* b *enteros primos relativos que dividen a* c*, entonces* $ab \mid c$*.*

Demostración. Puesto que $\mathrm{mcd}(a,b)=1$, entonces existen enteros a_0 y b_0 tales que $1 = aa_0 + bb_0$. Multiplicando por c ambos miembros de esta ecuación se tiene $c = caa_0 + cbb_0$. Por hipótesis, a y b dividen a c, es decir, existen enteros x e y tales que $c = ax$ y $c = by$. De todo esto se tiene $c = caa_0 + cbb_0 = byaa_0 + axbb_0 = ab(ya_0 + xb_0)$, probando que ab divide a c. ■

1.1.3 Teorema (Teorema Fundamental de la Aritmética) . *Dado cualquier entero* $a \notin \{\pm 1, 0\}$*,* a *tiene una representación única (excepto por orden y signo) como producto de primos:* $a = \pm p_1^{e_1} \cdots p_r^{e_r}$*, con* $p_i \neq p_j$ *si* $i \neq j$*, y* $e_i \geq 1$ *para todo* $i = 1, 2, \ldots, r$*.*

Demostración. Es suficiente demostrar el teorema para $a > 1$.

Veamos la existencia de la representación de a como producto de primos.
Si $a = 2$, no hay nada que probar, entonces se puede suponer que el resultado se cumple para $a > 2$. Si $a+1$ es primo, hemos terminado. Si $a+1 = bc$, con $1 < b, c < a+1$, por la hipótesis inductiva, b y c tienen una factorización en primos, por lo tanto $a+1$ también.

Veamos la unicidad.
Supongamos que $a = p_1^{e_1} \cdots p_r^{e_r} = q_1^{a_1} \cdots q_s^{a_s}$ con p_i y q_j primos. De la ecuación anterior se tiene $p_i \mid q_1^{a_1} \cdots q_s^{a_s}$, entonces de una generalización obvia del

Corolario 1.1.4, $p_i \mid q_j$ para alguna j y de aquí $p_i = q_j$. Después de volver a enumerar, si es necesario, se puede suponer $i = j = 1$, y $e_1 \geq a_1$, de esta manera $p_1^{e_1-a_1} p_2^{e_2} \cdots p_1^{e_r} = q_2^{a_2} \cdots q_s^{a_s}$. Continuando con este argumento se muestra que $s = r, e_i = a_i$ y $p_i = q_i$, para todo i. ■

1.1.2. El Algoritmo Euclidiano

Euclides, en sus Elementos, indica un algoritmo para encontrar el mcd de a y b. Este algoritmo se basa en el algoritmo de la división, es por eso que algunas veces sus nombres se usan como sinónimos. El algoritmo de la división dice lo siguiente:

> *Dados $a, b, \in \mathbb{Z}$ con al menos uno diferente de cero, digamos $b \neq 0$, entonces existen $q_1, r_1, \in \mathbb{Z}$ tales que $a = bq_1 + r_1$, con $0 \leq r_1 < b$, si $b > 0$, ó $0 \leq r_1 < -b$, si $b < 0$.*

Sin perder generalidad podemos suponer $b > 0$, entonces de la ecuación $a = bq_1 + r_1$ se tiene: $d \mid a$ y $d \mid b \iff d \mid b$ y $d \mid r_1$ por lo que $\text{mcd}(a, b) = \text{mcd}(b, r_1)$. Si $r_1 \neq 0$, aplicando el algoritmo de la división a b y r_1 se tiene que existen q_2 y r_2 tales que $b = r_1 q_2 + r_2$. Argumentando como antes se tiene que $\text{mcd}(a, b) = \text{mcd}(b, r_1) = \text{mcd}(r_1, r_2)$. Una aplicación sucesiva del algoritmo de la división produce las siguientes ecuaciones y condiciones.

$$\begin{array}{cc} a = bq_1 + r_1 & 0 \leq r_1 < b \\ b = r_1 q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = r_2 q_3 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & \vdots \\ r_{n-2} = r_{n-1} q_n + r_n & 0 \leq r_n < r_{n-1}. \end{array}$$

Entonces se ha construido una sucesión decreciente de enteros no negativos $r_n < \cdots < r_2 < r_1$, de esta forma necesariamente $r_n = 0$, para algún n. De esto y lo observado antes se tiene

$$\text{mcd}(a, b) = \text{mcd}(b, r_1) = \cdots = \text{mcd}(r_{n-2}, r_{n-1}) = r_{n-1} \neq 0,$$

Lo que proporciona un método para calcular el máximo común divisor de dos enteros, conocido como *algoritmo de Euclides.*

A continuación se presenta un método práctico —este método se ha generalizado al caso de n enteros en [1]— para encontrar el mcd de dos enteros positivos, así como la combinación lineal tal que $\text{mcd}(a,b) = aa_0 + bb_0$. Este método está estrechamente ligado con el procedimiento para encontrar la forma normal de Smith de una matriz entera. La forma normal de Smith de una matriz entera, se obtiene aplicando operaciones elementales en las filas de una matriz con entradas enteras. Puesto que se estará trabajando en los enteros, se suprimirán los cocientes, y en su lugar se usará el algoritmo de la división. Sean a, b enteros, se puede suponer $a, b > 0$, más aún, $a \geq b$, entonces $a = bq_1 + r_1$, con $0 \leq r_1 < b$. Considere la matriz $A_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$, multiplicando la fila 2 por $-q_1$ y sumándola a la fila 1, se tiene $\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$ $\sim \begin{bmatrix} r_1 & 1 & -q_1 \\ b & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} b & 0 & 1 \\ r_1 & 1 & -q_1 \end{bmatrix} = A_1$ Examine si $r_1 = 0$, de ser así, hemos terminado el proceso. Si $r_1 \neq 0$ entonces $b = r_1q_2 + r_2$, de esta manera $\begin{bmatrix} b & 0 & 1 \\ r_1 & 1 & -q_1 \end{bmatrix} \sim \begin{bmatrix} r_2 & -q_2 & 1 + q_1q_2 \\ r_1 & 1 & -q_1 \end{bmatrix} = A_2$. Continuando con el proceso se llega a la siguiente matriz $A_n = \begin{bmatrix} r_n & * & * \\ r_{n-1} & a_0 & b_0 \end{bmatrix}$. Si $r_n = 0$, entonces $\text{mcd}(a,b) = r_{n-1} = aa_0 + bb_0$.

Nota. Si $\text{mcd}(a,b) = 1$, entonces las entradas *, * de A_n son a y b en algún orden y con signo.

1.1.3 Observación El método presentado anteriormente se aplica para encontrar el máximo común divisor de elementos que pertenezcan a un dominio entero[2] en el cual se cumpla el algoritmo euclidiano. Por ejemplo, el anillo de polinomios con coeficientes en $\mathbb{R}$ o $\mathbb{C}$.

1.1.1 Ejemplo *Encuentre el máximo común divisor de 32 y 28, así como los valores de x e y tales que* $\text{mcd}(32,28) = 32x + 28y$.

$\begin{bmatrix} 32 & 1 & 0 \\ 28 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 4 & 1 & -1 \\ 28 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 28 & 0 & 1 \\ 4 & 1 & -1 \end{bmatrix} \sim \begin{bmatrix} 0 & -7 & 8 \\ 4 & 1 & -1 \end{bmatrix}$.
De aquí se tiene $4 = 32 - 28$.

[2]Un dominio entero es un anillo conmutativo con identidad y sin divisores de cero.

1.1.2 Ejemplo *Encuentre* $\text{mcd}(47,5) = 47x + 5y$.

$$\begin{bmatrix} 47 & 1 & 0 \\ 5 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 2 & 1 & -9 \\ 5 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 5 & 0 & 1 \\ 2 & 1 & -9 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 19 \\ 2 & 1 & -9 \end{bmatrix} \sim$$
$$\begin{bmatrix} 2 & 1 & -9 \\ 1 & -2 & 19 \end{bmatrix} \sim \begin{bmatrix} 0 & 5 & -47 \\ 1 & -2 & 19 \end{bmatrix}.$$

De esto se tiene $\text{mcd}(47,5) = 1 = 47(-2) + 5(19)$.

1.1.3. Los Enteros Módulo n

Hay varias historias sobre la invención del juego de ajedrez. Una de las más conocidas es la que se refiere a un Rey, y se cree que ocurrió hace por lo menos dos mil años. La historia va más o menos como sigue. El soberano conoció del maravilloso invento y quedó tan satisfecho con las cualidades intelectuales del juego de ajedrez que mandó traer al inventor y le dijo que pidiera lo que quisiera a cambio de su invento. El inventor pidió que por el primer cuadro del tablero le diera un grano de trigo, dos por el segundo; cuatro por el tercero; ocho por el cuarto y así sucesivamente. El Rey le replicó que por qué su petición era tan modesta a la vez que le invitó a pedir algo más sustantivo. El inventor contestó que él consideraba buena paga su petición. El monarca ordenó que se cumpliera de inmediato el deseo del inventor del juego de ajedrez. Al cabo del tiempo, vino uno de sus súbditos a informar que las bodegas del reino se estaban quedando vacías y no se había satisfecho el compromiso con el inventor. Si el inventor hubiese sido un poco cruel con el Rey le hubiese dicho que sabía algo más respecto a la cantidad de granos que iba a recibir: al dividir tal cantidad por tres, deja residuo 0. Ayude al soberano a entender lo que está pasando con tan singular petición. El enunciado sobre el residuo que deja la cantidad de granos de trigo al ser dividida por tres, es un ejemplo que se puede abordar con la idea de congruencia en los números enteros. Ésta fue desarrollada por Gauss,[3] y es tal su importancia en el estudio de propiedades aritméticas de los enteros, que se

[3]Karl Friedrich Gauss (1777-1855) matemático alemán. A los 19 años demostró que el polígono regular de 17 lados se puede construir con regla y compás. Se dice que este resultado lo motivó a dedicarse al estudio de las matemáticas. Otros de sus grandes logros en su juventud fue la demostración del teorema fundamental del álgebra y la publicación de su obra Disquisitiones Arithmeticae (1801). La siguiente es una de sus frases célebres. "*Si otros reflexionaran sobre las verdades matemáticas, tan profunda y continuamente como lo he hecho, descubrirían lo mismo que yo*".

ha convertido en una parte esencial de la teoría de números. A continuación presentamos algunas de sus propiedades básicas.

Sean a, b y n números enteros, con $n > 0$. Se define la siguiente relación entre a y b:

$$a \text{ es congruente con } b \text{ módulo } n, \text{ si } n|a-b.$$

Lo anterior se denota por $a \equiv b \pmod{n}$. Se obtiene directamente de la definición de congruencia módulo n, que dos enteros son congruentes módulo n si y sólo si al dividirlos por n se obtiene el mismo residuo. Dado un entero a, denotaremos por $[a]_n$ al conjunto de todos los enteros que son congruentes con a módulo n, es decir,

$$[a]_n := \{x \in \mathbb{Z} \,|\, a \equiv x \pmod{n}\}.$$

Nótese que dado $a \in \mathbb{Z}$ y dividiéndolo por n, existe $r \in \mathbb{Z}$ tal que $0 \leq r < n$ y $a = qn + r$, de lo que se tiene

$$[a]_n = [r]_n := \{x \in \mathbb{Z} : x = nq + r,\ q \in \mathbb{Z}\} = n\mathbb{Z} + r.$$

Al conjunto $\{[r]_n \,|\, 0 \leq r < n\}$ se le llama: *Un conjunto reducido de clases residuales módulo n* ó simplemente *clases módulo n*. El término reducido se debe a que al tomar r y s tales que $0 \leq r, s < n$, se tiene $[r]_n \neq [s]_n$, mientras que si no se impone la condición que tienen r y s de ser menores que n, bien puede ocurrir que $a \neq b$ y $[a]_n = [b]_n$. Las siguientes son algunas de las propiedades básicas de las clases residuales.

1. Si $[a]_n \neq [b]_n$, entonces $[a]_n \bigcap [b]_n = \emptyset$.
2. $\mathbb{Z} = \bigcup_{r=0}^{n-1} [r]_n$, la unión es de conjuntos disjuntos.
3. Denotando por $\mathbb{Z}_n$ ó $\mathbb{Z}/n\mathbb{Z}$ al conjunto de clases módulo n, se tiene lo siguiente para cada par de elementos. Si $[a]_n = [a_1]_n$ y $[b]_n = [b_1]_n$, entonces $[a + b]_n = [a_1 + b_1]_n$. En efecto, las hipótesis garantizan que $a = nq + a_1$ y $b = nq_1 + b_1$, de esto se concluye $a - b = (q - q_1)n + (a_1 - b_1)$, equivalentemente, $[a + b]_n = [a_1 + b_1]_n$. Con lo mostrado antes se puede definir una operación en el conjunto de clases módulo n, llamada suma y dada por $[a]_n + [b]_n := [a + b]_n$. La operación suma en $\mathbb{Z}_n$ satisface las mismas propiedades que la suma de enteros.

4. Denotando por $\mathbb{Z}_n^*$ al conjunto $\{[a]_n \ : \ \text{mcd}(a,n) = 1\}$ e imitando lo hecho antes con la suma se puede definir una multiplicación dada por $[a]_n \cdot [b]_n := [ab]_n$ la cual satisface propiedades análogas a las de suma, en $(\mathbb{Z}, +)$. El elemento $[1]_n$ satisface $[a]_n \cdot [1]_n = [1]_n \cdot [a]_n = [a]_n$ para todo $[a]_n$ y se le llama **neutro multiplicativo** en $\mathbb{Z}_n^*$. Un caso de particular importancia ocurre cuando $n = p$ es un número primo. En este caso el conjunto de clases residuales módulo p es denotado por $\mathbb{F}_p$. Note que $\mathbb{F}_p^*$ tiene $p - 1$ elementos.

La verificación de las propiedades anteriores se deja como ejercicio.

Ejemplos

En esta parte estamos interesados en estudiar algunos ejemplos particulares de los enteros módulo n y describir los subconjuntos que tienen las mismas propiedades respecto a las operaciones definidas en ellos.

1. Describa los subconjuntos de $(\mathbb{Z}_6, +)$ que satisfacen las mismas propiedades que $(\mathbb{Z}_6, +)$, es decir, queremos saber cuáles son los subconjuntos de $\mathbb{Z}_6$ que tienen a la clase del cero, son cerrados bajo la suma y también contienen a los inversos de elementos que pertenecen a ellos. Primero, es claro que el conjunto $\{[0]_6\}$ satisface las propiedades requeridas. Si un subconjunto H contiene a la clase del 1, es decir, $[1]_6 \in H$ entonces debe contener a todos los elementos de $\mathbb{Z}_6$ (¿por qué?) Si un subconjunto contiene a la clase del 2, entonces debe contener a la clase del 4 y como el inverso de $[2]_6$ es $[4]_6$, entonces el conjunto $H = \{[0]_6, [2]_6, [4]_6\}$ satisface las propiedades requeridas. Si un subconjunto contiene a la clase del 3, debe contener al inverso de éste, que es el mismo. Entonces el conjunto $H_1 = \{[0]_6, [3]_6\}$ también satisface las propiedades. ¿Habrá otro subconjunto diferente a los mencionados que satisfaga las propiedades?

2. Con las ideas del caso anterior, explore los conjuntos: $\mathbb{Z}_8, \mathbb{Z}_{12}, \mathbb{Z}_{20}$.

3. Considere los conjuntos $\mathbb{Z}_{15}^*, \mathbb{Z}_{20}^*, \mathbb{Z}_{25}^*$ y haga una discusión para decidir cuáles de los subconjuntos de cada uno satisfacen las mismas propiedades, pero ahora con la multiplicación.

4. Haga lo mismo que en el caso anterior para $\mathbb{F}_7^*, \mathbb{F}_{11}^*$ y $\mathbb{F}_{13}^*$.

La teoría de los enteros módulo n tiene varias aplicaciones prácticas en otras disciplinas. Por ejemplo en criptografía y teoría de códigos ([3], Capítulo 4). Otra aplicación de la teoría de enteros módulo n ocurre en la teoría de matrices. Sea $A = (a_{ij})$ una matriz $n \times n$ con entradas enteras. Supongamos que $a_{ii} \equiv 1 \pmod 2$ para todo $i = 1, \ldots, n$ y $a_{ij} \equiv 0 \pmod 2$ para todo $i > j$. Entonces $|A| \equiv 1 \pmod 2$, en particular A no es singular.
Discusión. Tomando congruencia en las entradas de la matriz A, se tiene que la matriz resultante es triangular con unos en la diagonal. El resultado se obtiene notando que calcular el determinante conmuta con tomar congruencia en las entradas de la matriz. Las hipótesis anteriores pudieran ser muy restrictivas. El siguiente ejemplo ilustra como se pueden debilitar. Sea

$$A = \begin{pmatrix} 4 & 5 & 6 \\ 7 & 8 & 10 \\ 1 & 4 & 3 \end{pmatrix},$$

entonces tomando congruencias y calculando el determinante se tiene $|A| \equiv 1 \pmod 2$, por lo que A es no singular.

1.1.4. Ejercicios

1. Demuestre que $4n^2 + 4$ no es divisible por 19 para todo $n \in \mathbb{Z}$. ¿Se cumple lo mismo para todo primo de la forma $4k + 3$?

2. Sean a, b y c enteros positivos tales que $a^2 + b^2 = c^2$. Demuestre que 60 divide a abc.

3. Sea $n > 1$ entero. Demuestre que $2^{2^n} - 1$ tiene al menos n factores primos diferentes.

4. Sean a y p enteros con p primo. Demuestre que $a^p \equiv a \pmod p$.

5. Demuestre que 7 divide a $3^{2n+1} + 2^{n+2}$ para todo n entero no negativo.

6. Demuestre que $n^{13} - n$ es divisible por $2, 3, 5, 7$ y 13.

7. Sea $f(x)$ un polinomio en $\mathbb{Z}[x]$. Suponga que $f(0) \equiv f(1) \equiv 1 \pmod 2$. Demuestre que $f(x)$ no tiene raíces enteras. Generalice el problema anterior a: Suponga que $f(x) \in \mathbb{Z}[x]$ y para un $k > 0$ entero, $f(x)$ satisface $f(i) \not\equiv 0 \pmod k$, para todo $i = 0, 1, \ldots k-1$. ¿Puede tener $f(x)$ raíces enteras?

1.2. Generalidades sobre grupos

En esta sección se inicia la discusión concerniente a la teoría de grupos. Damos inicio con la siguiente:

1.2.1 Definición *Un grupo*[4] *es una pareja* $(G, \circ)$*, con* G *un conjunto no vacío,* $\circ$ *una función de* $G \times G \to G$ *llamada operación binaria y denotada por* $\circ(x, y) := x \circ y$*, la cual satisface:*

(i) La operación $\circ$ *es asociativa, es decir,* $x \circ (y \circ z) = (x \circ y) \circ z$ *para todos* $x, y, z \in G$*.*

(ii) Existe $e \in G$ *tal que* $e \circ x = x$*, para todo* $x \in G$ *(neutro por la izquierda).*

(iii) Dado $x \in G$*, existe* $x' \in G$ *tal que* $x' \circ x = e$ *(inverso por la izquierda).*

En la definición anterior no se requiere que e y x' sean únicos, sin embargo más adelante probaremos que estos elementos son, en efecto, únicos. En lo que sigue, la operación "$\circ$"la denotaremos simplemente por $x \circ y = xy$, (caso multiplicativo) ó $x \circ y = x + y$ (caso aditivo). La notación aditiva, por tradición, se usará cuando $x \circ y = y \circ x$, para todos $x, y \in G$. En este caso diremos que el grupo G es *abeliano*.[5]

Ejemplos de grupos

[4]De acuerdo a H. Wussing, [[24], páginas 247-248] la primera formulación del concepto de grupo, que tiene gran similitud con la actual, se encuentra en el trabajo de H. Weber: "Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie". Math. Ann. **43** (1893), 521-549, página 522.

[5]Este término se da en honor del matemático noruego H. Abel (1802-1829), quien fue el primero en trabajar, de manera sistemática, con este tipo de grupos al abordar el problema de la solubilidad por radicales de ecuaciones polinomiales.

1.2.1 Ejemplo *(a)* $(\mathbb{Z}, +)$ *es un grupo con la adición usual de enteros.*

(b) El conjunto de matrices inversibles $n \times n$*, con entradas en* $\mathbb{R}$ *y operación, el producto usual de matrices forma un grupo el cual se conoce como el grupo lineal general, denotado por* $GL(n, \mathbb{R})$*.*

(c) Sea X *un conjunto no vacío y* $S_X = \{f : X \to X \mid f \text{ es biyectiva}\}$*,* S_X *es un grupo con la operación composición de funciones, llamado el grupo de permutaciones en* X*. A los elementos de* S_X *se les llama permutaciones.*

(d) Sea $G = GL(n, \mathbb{R}) \times \mathbb{R}^n$*. Definiendo en* G *la operación* $(A, X) * (B, Y) := (AB, X + Y)$*, se verifica que* $(G, *)$ *es un grupo.*

(e) Sea G *el conjunto del ejemplo anterior, definiendo en* G *la operación*

$$(A, X) \circ (B, Y) := (AB, AY + X),$$

$(G, \circ)$ *es un grupo con* $(I, 0)$ *la identidad y* $(A^{-1}, -A^{-1}X)$ *el inverso de* (A, X)*.*

1.2.1 Observación Los dos últimos ejemplos muestran que en la definición de grupo, el mismo conjunto puede tener diferentes estructuras de grupo.

Como ya fue observado antes, en la definición de grupo no se requiere que el inverso y el neutro sean únicos, sin embargo resultan serlo. El siguiente resultado es auxiliar para mostrar eso y a partir de aquí, adoptaremos la notación $ab := a \circ b$.

1.2.1 Teorema *Sea* $(G, \circ)$ *un grupo y* $g \in G$*, entonces* $gg = g$ *implica* $g = e$*.*

Demostración. Existe un elemento $g' \in G$ tal que $g'g = e$, lo cual implica $g'(gg) = g'g = e$. Por otro lado, $g'(gg) = (g'g)g = eg = g$, de donde la conclusión se obtiene. ■

1.2.2 Teorema *Sea* G *un grupo. Entonces:*

(i) Existe un único elemento $e \in G$ *tal que* $eg = g$ *para todo* $g \in G$*. Además* $eg = ge = g$ *para todo* $g \in G$*.*

(ii) Para todo $g \in G$, existe un único $g' \in G$ tal que $g'g = e$. Además $g'g = gg' = e$.

Demostración. Primero mostraremos que $g'g = e$ implica $gg' = e$. Supongamos $g'g = e$, entonces $(gg')(gg') = g(g'g)g' = geg' = gg'$, invocando el Teorema 1.2.1 concluimos que $gg' = e$. Si $g \in G$, sea $g' \in G$ tal que $g'g = e$, entonces $ge = g(g'g) = (gg')g = eg = g$. Con esto hemos probado que $eg = ge = g$ para cualquier $g \in G$. Supongamos que existe e' tal que $e'g = g$, para todo $g \in G$, entonces en particular $e'e = e$. Como e también es una identidad izquierda y conmuta con todo $g \in G$ se tiene, $ee' = e'e$; esto y la ecuación anterior lleva a $e = e'$. De la definición de grupo, sea $g' \in G$ tal que $g'g = e$. Si existe otro $a \in G$ tal que $ag = e$, entonces $ae = ea = a$. Por otro lado, $ae = ag'g = agg' = eg' = g'$, de estas ecuaciones se concluye que $a = g'$. ■

El resultado anterior permite definir la *identidad* de un grupo y el *inverso* de cada elemento de G. El inverso de un elemento $g \in G$ se denotará por g^{-1}.

1.2.2 Observación Si G es un grupo, entonces las siguientes igualdades tienen lugar.

1. $(g^{-1})^{-1} = g$.
2. $(xy)^{-1} = y^{-1}x^{-1}$.

Sea G un grupo y $g \in G$, definimos por inducción las potencias de g como sigue: $g^2 := gg$, supongamos que se ha definido g^{n-1}, por inducción se define $g^n := gg^{n-1}$ para $n > 1$. Si $n < 0$, entonces $m = -n > 0$ y definimos $g^n := (g^{-1})^m$, finalmente, $g^0 := e$. Con las definiciones anteriores se tiene: (verificarlas)

i) $(g^n)^m = g^{nm} \ \forall \ g \in G, \ \text{y} \ \forall \ n, m \in \mathbb{Z}$.

ii) $g^n g^m = g^{n+m} \ \forall \ n, m \in \mathbb{Z}$.

1.2.2 Definición *Dado un grupo G y $g \in G$, se define el **orden** de g como el mínimo entero positivo n tal que $g^n = e$, si tal entero existe, de otra forma se dice que g tiene **orden infinito**. El orden de g se denotará por $|g| = n$.*

Cuando se estudia una estructura algebraica, es de gran importancia considerar los subconjuntos que heredan la misma estructura, pues en muchos casos la estructura original se determina en términos de las subestructuras. En nuestro caso, estamos interesados en considerar aquellos subconjuntos no vacíos de un grupo G que satisfacen las mismas propiedades que éste, cuando la operación se restringe a estos subconjuntos. Estos subconjuntos reciben un nombre, son llamados *subgrupos*. La siguiente definición precisa lo anterior.

1.2.3 Definición *Sea G un grupo, $H \subseteq G$, $H \neq \emptyset$. Se dice que H es un* ***subgrupo*** *de G si la operación de G restringida a H hace de éste un grupo.*

Si H es subgrupo de G, se usará la notación $H \leq G$ y se lee "H es subgrupo de G". En el contexto de grupos, no hay lugar a confundir la notación anterior con la relación de orden en un conjunto.

1.2.3 Observación Nótese que la definición de subgrupo implica $e \in H$, con e la identidad de G.

1.2.3 Teorema *Sea G un grupo, $H \subseteq G$, $H \neq \emptyset$. Entonces las siguientes condiciones son equivalentes.*

(i) H *es un subgrupo de* G.

(ii) *(a)* $\forall\ x, y \in H,\ \ xy \in H$,
(b) $\forall\ x \in H,\ \ x^{-1} \in H$.

(iii) *Para todos* $x, y \in H$ *se tiene* $xy^{-1} \in H$.

Demostración. $(i) \implies (ii)$ Es claro, pues al ser H un subgrupo se deben tener satisfechas las condiciones (a) y (b).
$(ii) \implies (iii)$ Dados $x, y \in H$, (b) implica $x, y^{-1} \in H$. La conclusión se obtiene de la parte (a).
$(iii) \implies (i)$. Primeramente notemos que al ser H no vacío, existe un $x \in H$ y de esto se concluye, tomando $x = y$, que $e = xx^{-1} \in H$. Ahora tomando $y = x$ y $x = e$ se obtiene $x^{-1} = ex^{-1} \in H$. Sólo falta demostrar que H es cerrado bajo la operación definida en G. Sean $x, y \in H$. Por lo probado, $z = y^{-1} \in H$. Aplicando la hipótesis a x y a z se tiene que $xz^{-1} = xy \in H$.
■

1.2.1 Ejercicio *Sea $G = GL(n, \mathbb{R})$, el grupo de matrices $n \times n$, no singulares, con entradas en $\mathbb{R}$. $H = \{A \in G \mid$ A tiene entradas en $\mathbb{Z}$ y $det(A) = \pm 1\}$. Demuestre que $H \leq G$.*

1.2.4 Teorema *Sea G un grupo, $\{H_\lambda\}_{\lambda \in I}$ una colección de subgrupos. Entonces*

$$H = \bigcap_{\lambda \in I} H_\lambda,$$

es un subgrupo de G.

Demostración. Directa, aplicando la parte *(iii)* del Teorema 1.2.3 ■

1.2.4 Observación La unión de subgrupos no es necesariamente un subgrupo, de hecho el siguiente ejercicio caracteriza cuando la unión de dos subgrupos es subgrupo.

1.2.2 Ejercicio *(a) Sean H y K subgrupos de G. Demuestre que $H \cup K \leq G \iff K \subseteq H \quad H \subseteq K$.*

(b) Sea G un grupo, $\mathcal{C}$ una cadena de subgrupos.[6] *Demuestre que la unión de los elementos de $\mathcal{C}$ es un subgrupo.*

Haciendo uso del ejercicio anterior se pueden construir muchos subconjuntos de un grupo que no son subgrupos. Esto tiene cierta analogía con los espacios vectoriales. De hecho, en el caso de espacios vectoriales, uno puede estar interesado en construir subespacios con ciertas propiedades. Por ejemplo, puede ser de interés que un cierto subconjunto esté contenido en un subespacio particular, bajo esa condición, se construye el subespacio deseado. Si el subespacio debe contener al subconjunto S, entonces el subespacio se construye tomando todas las posibles combinaciones lineales de elementos de S. ¿Podremos aplicar la idea de subespacios al caso de subgrupos? ¿Cómo interpretar las "combinaciones lineales.[en] un grupo? Si el subconjunto es S, un intento es definir el subgrupo generado por S como el conjunto de todos los elementos de la forma $s_1^{m_1} s_2^{m_2} \cdots s_r^{m_r}$, variando r en los enteros positivos,

[6]Recuerde: Una cadena es un conjunto parcialmente ordenado en el que cualesquiera dos elementos se relacionan. En nuestro caso, el orden es el inducido por la inclusión de subconjuntos.

$s_i \in S$ y los exponentes m_i en los enteros. ¿Es ésta la forma de sustituir la idea de combinaciones lineales? ¿Coincide esto con el enunciado del siguiente teorema?

1.2.5 Teorema *Sea G un grupo, S un subconjunto no vacío de G,*

$$\langle S\rangle := \{\ s_1^{i_1}\cdots s_n^{i_n} \mid s_i \in S,\ i_j = \pm 1,\ \ j = 1,\dots,n;\ \ n \in \mathbb{N}\}.$$

Entonces $\langle S\rangle \leq G$. De hecho este subgrupo es el mínimo que contiene a S. La minimalidad es en el siguiente sentido. $\langle S\rangle = \bigcap_{S\subseteq H\leq G} H$.

Demostración. En virtud del Teorema 1.2.3, es suficiente mostrar que dados dos elementos $x, y \in \langle S\rangle$, se tiene $xy^{-1} \in \langle S\rangle$. Para mostrar lo anterior basta observar que dado $y = s_1^{i_1}\cdots s_k^{i_k} \in \langle S\rangle$, $y^{-1} = s_k^{-i_k}\cdots s_1^{-i_1}$ con $i_j = \pm 1$, por lo tanto $y^{-1} \in \langle S\rangle$. De esto último se tiene lo deseado. Para mostrar lo restante, note que $\bigcap_{S\subseteq H\leq G} H \subseteq \langle S\rangle$, por ser $\langle S\rangle$ uno de los elementos sobre los cuales se toma la intersección. La inclusión de conjuntos se obtiene del hecho que los elementos de $\langle S\rangle$ son productos de elementos de S y $S \subseteq H$, por lo tanto $\langle S\rangle \subseteq \bigcap_{S\subseteq H\leq G} H$. ■

1.2.3 Ejercicio *Describa $\langle S\rangle$ para el caso especial $S = \{g\}$.*

1.2.4 Definición *Con la notación del teorema anterior, al subgrupo $\langle S\rangle$ se le llama el* ***subgrupo generado*** *por S. Un grupo G se dice* ***finitamente generado****, abreviado f.g., si G contiene un subconjunto finito S tal que $G = \langle S\rangle$. Si S tiene un solo elemento, G se dice cíclico.*

Recordemos que en el estudio de los espacios vectoriales, por ejemplo, cuando se les quiere representar como suma directa de subespacios con ciertas propiedades, las transformaciones lineales son de gran importancia, siendo la razón el hecho de que estas transformaciones preservan las operaciones en los espacios bajo consideración. En general, cuando se estudian estructuras algebraicas, son de gran importancia las funciones que preservan dichas estructuras. Con lo anterior en mente, nos interesa estudiar funciones de un grupo en otro, posiblemente el mismo, que preservan las operaciones, más precisamente, nos interesan las funciones que satisfacen la siguiente:

1.2.5 DEFINICIÓN *Sean* $(G, \circ)$ *y* $(G_1, *)$ *dos grupos,* $f : G \to G_1$ *una función.*

(i) Si $f(x \circ y) = f(x) * f(y), \ \forall \ x, y \in G$, f *se llama un* ***homomorfismo****.*

(ii) Si f *es inyectiva y satisface i),* f *se llama un* ***monomorfismo****.*

(iii) Si f *es suprayectiva y satisface i),* f *se llama un* ***epimorfismo****.*

(iv) Si f *satisface ii) y iii),* f *se llama un isomorfismo.*

Si $f : G \to G_1$ es un isomorfismo, se dice que G es isomorfo a G_1 y se usa la notación $G \cong G_1$.

1.2.5 OBSERVACIÓN La composición de homomorfismos, cuando esto tiene sentido, es nuevamente un homomorfismo.

1.2.6 OBSERVACIÓN "Ser isomorfos"define una relación de equivalencia en la clase de todos los grupos, cuyas clases de equivalencia están formadas precisamente por los grupos que son isomorfos.

En matemáticas, uno de los problemas fundamentales es poder clasificar a los diferentes objetos que se estudian. La clasificación es en el sentido de agrupar a todos aquellos que tengan las mismas propiedades. Por ejemplo, en álgebra lineal se tiene una clasificación de los espacios vectoriales finitamente generados en términos de su dimensión. Esto se precisa diciendo que dos espacios vectoriales finitamente generados son isomorfos si y sólo si tienen la misma dimensión. En lo referente a grupos, su clasificación es un problema mucho más complicado. Los grupos que son "clasificables"de manera similar a los espacios vectoriales finitamente generados, es decir, sustituyendo dimensión por cardinalidad, son los grupos cíclicos. En este sentido, cabe mencionar que uno de los problemas fundamentales de la teoría de grupos es la clasificación de estos, bajo isomorfismo.

1.2.6 DEFINICIÓN *Sea* $f : G \to G_1$ *un homomorfismo, se define:*

(i) el ***núcleo*** *de* f*, denotado* $\ker f = \{g \in G \mid f(g) = e_H\}$.

(ii) La ***imagen*** *de* f*, denotada* $\operatorname{Im} f = \{h \in G_1 \mid f(g) = h \ \text{ para algún } g \in G\}$.

1.2.4 EJERCICIO *Demostrar que* $\ker f \leq G$ *e* $\operatorname{Im} f \leq G_1$.

1.2.2 Ejemplo *Sean, H el grupo de permutaciones de $\mathbb{R}^n$ y G el grupo del Ejemplo 1.2.1(e), página 22, definiendo $\varphi : G \to H$ como sigue $\varphi(A, B) := F_{A,B}$ con $F_{A,B}(X) := AX + B$, se verifica que φ es un homomorfismo de grupos, de hecho un monomorfismo, por lo tanto la imagen de φ es un subgrupo de H, este subgrupo se llama el grupo de* ***transformaciones afines*** *de $\mathbb{R}^n$.*

1.2.1. Ejercicios

1. Sea d un entero libre de cuadrado, $\mathbb{Q}(\sqrt{d}) := \{a+b\sqrt{d} : a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$. Demuestre que $\mathbb{Q}(\sqrt{d}) \setminus \{0\}$ es un grupo con la multiplicación usual de los números complejos.

2. Sea m un entero positivo, $G = \{0, 1, \ldots, m-1\}$. Se define en G la siguiente operación: $a \circ b = a+b$, si $a+b < m$; $a \circ b = r$, con $a+b = m+r$ si $b + a \geq m$. ¿Es $(G, \circ)$ un grupo?

3. Sea $G = \mathbb{Z} \times \mathbb{Q}$, se define en G la operación

$$(a, b) \circ (c, d) := (a + c, 2^c b + d).$$

   ¿Es $(G, \circ)$ un grupo?

4. Sean $B = \{f : \mathbb{Z} \to \mathbb{Z} : f \text{ es una función}\}$ y $G = \mathbb{Z} \times B$. Se define en G la siguiente operación: $(m, f) \circ (n, g) = (m + n, h)$, con $h(z) := f(z - n) + g(z)$. ¿Es $(G, \circ)$ un grupo?

5. Una **isometría** de $\mathbb{R}^n$ es una función $f : \mathbb{R}^n \to \mathbb{R}^n$ tal que $\| x - y \| = \| f(x) - f(y) \|$ para todos $x, y \in \mathbb{R}^n$. Sea $f : \mathbb{R}^n \to \mathbb{R}^n$ una función tal que $f(0) = 0$. Demuestre que f es una isometría si y sólo si f preserva producto interno, es decir, $\langle f(x), f(y) \rangle = \langle x, y \rangle$ para todos $x, y \in \mathbb{R}^n$.

6. Una **función afín** f de $\mathbb{R}^n$ en $\mathbb{R}^n$ es una función $f = T + b$, con T transformación lineal no singular de $\mathbb{R}^n$ en $\mathbb{R}^n$ y $b \in \mathbb{R}^n$ fijo. Demuestre que una función $f : \mathbb{R}^n \to \mathbb{R}^n$ es una isometría si y sólo si f es afín, con T ortogonal. Demuestre que el conjunto de las isometrías de $\mathbb{R}^n$ es un grupo con la composición usual de funciones, a este grupo le denotaremos por $I(\mathbb{R}^n)$.

7. Sean S un subconjunto no vacío de $\mathbb{R}^n$, $I(S) = \{f \in I(\mathbb{R}^n) : f(S) \subseteq S, f^{-1}(S) \subseteq S\}$. Demuestre que $I(S)$ es un subgrupo de $I(\mathbb{R}^n)$.

8. Sea G un grupo de orden par. Demuestre que G contiene un elemento de orden 2 (caso especial del Teorema de Cauchy, Teorema 2.3.1, página 66).

9. (Este ejercicio cae fuera del contexto de la teoría de grupos, sin embargo es recomendable conocerlo). Sea V un espacio vectorial sobre $\mathbb{R}$ (de hecho sobre cualquier campo). Demuestre que V admite una base (sug. use el Lema de Zorn).

10. Sea X un conjunto con n elementos, $S_X = \{f : X \to X \mid f \text{es inyectiva}\}$. Demuestre que S_X forma un grupo con la operación composición de funciones y $|S_X| = n!$ En este caso S_X será denotado por S_n y se le llama el grupo de permutaciones de n elementos.

11. Sea G un grupo, $Z(G) = \{x \in G \mid xg = gx \ \forall \ g \in G\}$. Demuestre que $Z(G)$ es un subgrupo abeliano de G llamado el **centro** de G.

12. Caracterice los subgrupos de $(\mathbb{Z}, +)$.

1.3. Índice y el Teorema de Lagrange

Anteriormente notamos que la unión de subgrupos no siempre es un subgrupo. Esta propiedad es análoga al caso de subespacios vectoriales. Allí, se define la suma de subespacios, la cual siempre resulta ser un subespacio. ¿Cuál es la operación, en el caso de subgrupos, que sustituye a la suma en el caso de subespacios? Como en un grupo G se tiene solamente una operación, ésta debe ser usada para intentar dar una definición de "suma de subgrupos", o producto, dependiendo de cómo se denote a la operación. Con esto en mente se tiene la siguiente situación. Sea G un grupo, S y T subconjuntos no vacíos de G, se define el *producto* de S y T como: $ST := \{st \mid s \in S, \ t \in T\}$. Si $H \leq G$, $g \in G$, al producto $Hg = \{hg \mid h \in H\}$ le llamamos la *clase lateral derecha* de H en G representada por g. De forma análoga se define la *clase lateral izquierda* de H en G representada por g.
Si S y T son subgrupos, ¿es ST un subgrupo? De la definición de producto de los subgrupos S y T, se tiene que los elementos del producto son de la forma ab, con $a \in S$ y $b \in T$. Si el producto ha de ser un subgrupo se debe tener $xy^{-1} \in ST$, para todos $x, y \in ST$. Representando a x e y como se ha

definido en el producto, se tiene $xy = ab(cd)^{-1} = abd^{-}c^{-1}$ y este elemento no necesariamente pertenece a ST. Si Los elementos de S y T conmutan, se tendrá lo que se desea. Esto ocurre, por ejemplo, si el grupo que contiene a S y T es abeliano, o de manera menos restrictiva, si los elementos de S y los de T conmutan.
El análisis que hemos dado todavía no contesta la pregunta planteada, sin embargo, proporciona una respuesta parcial. La pregunta la podemos plantear para los grupos que no son abelianos. Para analizar la situación en grupos no abelianos es interesante saber algunas condiciones sobre tales grupos, por ejemplo, su cardinalidad. ¿Hay grupos no abelianos de orden pequeño? Es claro que los grupos con solo dos elementos son abelianos, pues el grupo consta de la identidad y otro elemento, el cual tiene que ser su propio inverso. Si un grupo tiene tres elementos, digamos $\{e, x, y\}$, entonces x e y son inversos uno del otro, de lo cual la conmutatividad se obtiene directamente. Si un grupo tiene cuatro elementos, digamos $\{e, x, y, z\}$, entonces al tomar una pareja, por ejemplo x, y, se tiene que $xy \notin \{x, y\}$ (¿por qué?), de esto se debe tener: $xy = e, z$.
Analizando como antes se llega a que $yx = e, z$ y en cualquiera de los casos se verifica que $xy = yx$. Como este análisis se puede hacer para toda pareja de elementos, se tiene que el grupo es abeliano.¿Qué ocurre con los grupos de cinco elementos? El análisis anterior es mucho más complicado por las diferentes posibilidades que ocurren al tomar dos elementos y multiplicarlos. Una idea que puede intentarse es considerar un elemento diferente de la identidad, x y considerar el subgrupo generado por éste, el cual debe tener al menos dos elementos. ¿Es posible que $\langle x \rangle$ sea diferente del total?
Pongamos $\langle x \rangle = H$. Si existe $a \in G \setminus H$, consideremos los siguientes subconjuntos de G: H y $Ha := \{ha \ : \ h \in H\}$. Si hubiese un elemento en la intersección, digamos, $z = ha$ se tendría que $h^{-1}z = a \in H$, lo cual es imposible. De esto se tiene $H \cup Ha$ es un subconjunto de G que contiene $2|H|$ elementos. Como este número tiene que ser menor o igual que cinco, debe ocurrir que $|H|$ es dos, es decir $H = \{e, x\}$, por lo que existe $b \in G$ el cual no pertenece a $H \cup Ha$. Un cálculo sencillo muestra que los conjuntos H, Ha y Hb son ajenos a pares, entonces su unión produce 6 elementos de G, lo cual es imposible. Esta contradicción muestra que $G = \langle x \rangle$. En resumen, se ha probado que un grupo con cinco elementos es cíclico, por lo tanto, abeliano. La discusión anterior la podemos resumir diciendo:

1.3.1 Observación Los grupos de orden menor o igual que cinco son abelianos.

Consideremos el conjunto S_3 que consiste de las funciones biyectivas de $\{1,2,3\}$ en sí mismo (llamadas permutaciones). Con la operación, composición de funciones, S_3 es un grupo. Los elementos de S_3 pueden ser descritos explícitamente como sigue: $S_3 = \{(1),(123),(12),(13),(23),(132)\}$. La notación (1) significa la permutación identidad. El elemento (123) significa la permutación que transforma el uno al dos, el dos al tres y el tres al uno. La permutación (12) es la función que fija al tres, al dos lo transforma en uno y al uno en dos. Con estas aclaraciones se tiene que los siguientes subconjuntos son subgrupos de S_3: $S = \{(1),(12)\}$ y $T = \{(1),(13)\}$, su producto es $ST = \{(1),(12),(13),(132)\}$. Si ST fuese subgrupo, debiera contener al elemento $(13)(12) = (123)$, pero este no es el caso. Resumiendo, hemos encontrado un grupo, S_3 y dos subgrupos cuyo producto no es subgrupo. Anteriormente fue observado que si los elementos de S conmutan con los de T, entonces ST es subgrupo. Notemos que si los elementos de S y T conmutan, entonces los conjuntos ST y TS son iguales, es decir, $ST = TS$. ¿Será esta condición necesaria? La respuesta la proporciona el siguiente teorema.

1.3.1 Teorema *Sean H y K subgrupos de G. Entonces HK es subgrupo $\iff$ $HK = KH$.*

Demostración. $(\Longrightarrow)$ Supongamos que HK es subgrupo, sea $hk \in HK$ entonces $(hk)^{-1} \in HK$, por lo tanto $(hk)^{-1} = h_1k_1$ con $h_1 \in H$ y $k_1 \in K$. De la última ecuación se concluye que $hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$, es decir, $HK \subseteq KH$. Un argumento análogo prueba que $KH \subseteq HK$.
$(\Longleftarrow)$ Supongamos que $HK = KH$. Sean $x, y \in HK$, aplicando el Teorema 1.2.3, basta mostrar que $xy^{-1} \in HK$. De la elección de x e y se tiene $x = hk$, $y = h_1k_1$, y de estas dos últimas ecuaciones se concluye que $xy^{-1} = hkk_1^{-1}h_1^{-1} = hh_2k_2$, para algunos $h_2 \in H$ y $k_2 \in K$, por lo tanto $xy^{-1} \in HK$. ■

1.3.1 Corolario *En un grupo abeliano, el producto (finito) de subgrupos es un subgrupo.*

1.3.2 Observación $Hg = H \iff g \in H$.

1.3.3 Observación El producto de subconjuntos de un grupo es asociativo. La prueba de las dos observaciones anteriores se deja como ejercicio.

1.3.1 Ejercicio *Sea G un grupo, S un subconjunto finito no vacío de G. Si $SS = S$ entonces S es un subgrupo. ¿Qué ocurre si S no es finito?*

1.3.2 Teorema *Sea G un grupo, $H \leq G$, entonces $Ha = Hb \iff ab^{-1} \in H$.*

Demostración. $\Longrightarrow$ Si $Ha = Hb$ entonces $(Ha)b^{-1} = (Hb)b^{-1} = H$, la conclusión se sigue de la Observación 1.3.2.
$\Longleftarrow$ Si $ab^{-1} \in H$ entonces nuevamente la Observación 1.3.2 implica $Hab^{-1} = H$. El resultado se obtiene multiplicando a la derecha por b en la ecuación anterior. ■

1.3.2 Ejercicio *Sean H y K subgrupos finitos de G. Demuestre que $|HK||H \cap K| = |H||K|$.*

Sugerencia: Note que $HK = \cup Hk$, la unión se toma sobre los elementos de K. También, $Hk = Hk_1 \iff kk_1^{-1} \in H$ y esto último sucede $\iff (H \cap K)k = (H \cap K)k_1$. Por otro lado, K es la unión ajena de clases módulo $H \cap K$, entonces el número de conjuntos diferentes en $\cup Hk$ es el índice de $H \cap K$ en K.

1.3.3 Teorema *Sea G un grupo, $H \leq G$. Entonces las clases laterales derechas de H en G constituyen una partición de G.*

Demostración. Claramente $G = \bigcup_{g \in G} Hg$, por lo tanto basta mostrar que si dos clases laterales derechas se intersecan, deben ser iguales. Sean Ha y Hb clases laterales derechas tales que $Ha \cap Hb \neq \emptyset$, entonces existe $x \in Ha \cap Hb$, por lo que $x = ha = h_1 b$, con $h, h_1 \in H$. La última ecuación implica $ab^{-1} = h^{-1}h_1 \in H$, ahora la conclusión se obtiene del Teorema 1.3.2. ■

1.3.4 Teorema *Sea G un grupo, $H \leq G$, $\mathfrak{R} = \{Hg \mid g \in G\}$ y $\mathfrak{L} = \{gH \mid g \in G\}$. Entonces $|\mathfrak{R}| = |\mathfrak{L}|$.*

Demostración. Consideremos la asignación $Ha \to a^{-1}H$ y demostremos que ésta define una función biyectiva. Si $Ha = Hb$, entonces $b^{-1}H = a^{-1}H$, pues $Ha = Hb \iff ab^{-1} \in H \iff ab^{-1}H = H \iff b^{-1}H = a^{-1}H$, es decir, la asignación anterior define una función que le denotaremos f. Del argumento anterior también se obtiene que f es inyectiva; la suprayectividad de f se obtiene directamente, pues $f(Hb^{-1}) = bH$. ■

1.3.1 Definición *Sean H y G como en el teorema anterior, se define el **índice** de H en G como $|\mathfrak{L}| = |\mathfrak{R}|$ y se denota por $[G : H]$.*

1.3.5 Teorema (Lagrange) *Sea G un grupo finito, $H \leq G$, entonces $|G| = [G : H]|H|$.*

Demostración. Como las clases laterales derechas forman una partición de G, entonces existen $g_1, \ldots, g_t$ elementos de G tales que $G = \cup Hg_i$, unión disjunta, $t = [G : H]$. Para terminar la prueba basta probar que $|H| = |Ha|$ para cualquier $a \in G$. Sea $a \in G$, defínase $f_a : H \to Ha$ como sigue $f_a(h) = ha$ (translación por a). Se verifica sin mayor problema que f_a es biyectiva, por lo tanto $|H| = |Ha|$, de esta última ecuación se tiene:

$$|G| = \sum_{i=1}^{t} |Hg_i| = \sum_{i=1}^{t} |H| = t|H| = [G : H]|H|. \blacksquare$$

Recordemos la definición de grupo cíclico.

1.3.2 Definición *Un grupo G se dice **cíclico** si $G = \langle g \rangle$, para algún $g \in G$.*

El siguiente resultado es una de las consecuencias útiles e inmediatas del Teorema de Lagrange.

1.3.6 Teorema *(a) Sea G un grupo tal que $|G| = p$, con p primo. Entonces G es cíclico, de hecho, $G = \langle g \rangle$ para cualquier $g \neq e$.*

(b) Si G es un grupo finito, H y K son subgrupos de G tales que $K \subset H \subset G$, entonces $[G : K] = [G : H][H : K]$.

Demostración. (a) Directa del Teorema de Lagrange.
(b) Por el Teorema de Lagrange, $|G| = |H|[G : H] = |K|[G : K]$ y $|H| = |K|[H : K]$. La conclusión se obtiene combinando estas ecuaciones. $\blacksquare$

1.3.7 Teorema *Sea G un grupo, $a \in G$ tal que $m = |\langle a \rangle| < +\infty$, entonces:*

(i) $m = |a|$ (orden de a).

(ii) Si $k \in \mathbb{Z}$ es tal que $a^k = e$, entonces m divide a k.

Demostración. (i) Como $\langle a \rangle$ es finito, entonces existe un entero positivo m tal que el conjunto $\{e, a, \ldots, a^{m-1}\}$ tiene m elementos y a^m es uno de estos elementos. Si $a^m = a^i$ con $0 < i \leq m - 1$, entonces $a^{m-i} = e$, contradiciendo que los elementos elegidos son diferentes, por lo tanto se debe tener $a^m = e$.

Nótese que m es el menor entero positivo con la propiedad $a^m = e$, es decir $m = |a|$. Para concluir la prueba mostraremos que $\langle a \rangle = \{e, a, a^2, \ldots, a^{m-1}\}$. Recordemos que $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$. Dado $k \in \mathbb{Z}$, existen r y q, números enteros tales que $k = mq + r$, con $0 \leq r < m$. De esto se tiene $a^k = a^{mq}a^r = a^r \in \{e, a, a^2, \ldots, a^{m-1}\}$, probando *(i)*. Si $a^k = e$, del argumento anterior se tiene $a^r = e$, las condiciones sobre r y m implican que $r = 0$, es decir, m divide a r, probando *(ii)*.

1.3.4 Observación Si $|G| < +\infty$, entonces $|g|$ divide a $|G|$ y $g^{|G|} = e$ para todo $g \in G$.

1.3.1. Ejercicios

1. Sea G un grupo, $x, y \in G$ tales que $xy = yx$ y $(|x|, |y|) = 1$. Demuestre que $|xy| = |x||y|$. De hecho este resultado se cumple en una situación más general. ¿Cuál es el orden de xy si $xy = yx$?

2. Sea G el grupo de matrices con entradas en $\mathbb{Q}$,

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ y } \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

   elementos de G. Demuestre que A y B tienen órdenes primos relativos y AB tiene orden infinito. ¿Contradice esto al Ejercicio 1?

3. Sean H y K subgrupos de G. Demuestre que $|HK||H \cap K| = |H||K|$.

4. Sea G un grupo abeliano, $T(G) = \{g \in G \mid g^n = e \text{ para algún } n\}$. Demuestre que $T(G)$ es un subgrupo de G. A este subgrupo se le llama el **subgrupo de torsión** de G. Compare con el Ejercicio 2.

5. Sea G un grupo que contiene un número finito de subgrupos. Demuestre que G es finito.

6. Dado un entero positivo n, se define la *función de Euler* $\varphi(n)$ como la cardinalidad del conjunto $\{1 \leq a \leq n \mid \text{mcd}(a, n) = 1\}$. Sean n y m enteros positivos primos relativos. Demuestre que $n^{\varphi(m)} \equiv 1 \pmod{m}$.

7. Sea G un grupo finito, S y T subconjuntos de G no vacíos. Demuestre que $G = ST$ ó $|G| \geq |S| + |T|$.

8. Sea G un grupo de orden $p^k m$ con $(p, m) = 1$, $H \leq G$ tal que $|H| = p^k$ y $K \leq G$ tal que $|K| = p^d$, $0 < d \leq k$ y K no contenido en H. Demuestre que HK no es subgrupo (equivalentemente $HK \neq KH$)

9. Sea a un entero > 1 y $n \in \mathbf{N}$. Demuestre que $n|\varphi(a^n - 1)$.

1.4. Subgrupos normales y grupo cociente

El concepto de subgrupo normal es uno de los más importantes en teoría de grupos y teoría de Galois. De hecho, de acuerdo con Wussing [[24], página 105], este concepto es descubierto por Galois al estudiar la estructura de lo que definió como el grupo de una ecuación. En lo que sigue mostraremos como a partir de un grupo y un subgrupo normal se puede construir un grupo, llamado grupo cociente, el cual es de utilidad para obtener propiedades del grupo original.

1.4.1 Definición *Sea G un grupo, $N \leq G$. Se dice que N es un* ***subgrupo normal*** *si $gNg^{-1} = N$ para todo $g \in G$. Cuando N es normal lo denotaremos por $N \lhd G$.*

1.4.1 Observación Si H es un subgrupo de G, y $g \in G$, gHg^{-1} es un subgrupo de G llamado *subgrupo conjugado de H* y $|gHg^{-1}| = |H|$. Note que H es normal $\iff$ H coincide con todos sus conjugados.

1.4.1 Teorema *Las siguientes condiciones sobre un subgrupo N son equivalentes.*

(i) *N es normal.*

(ii) *$gNg^{-1} \subseteq N$ para todo $g \in G$.*

(iii) *$gN = Ng$ para todo $g \in G$.*

Demostración. $(i) \Longrightarrow (ii)$ Es claro.
$(ii) \Longrightarrow (iii)$ Por hipótesis $gNg^{-1} \subseteq N$ para todo $g \in G$, de esta condición obtenemos $gN \subseteq Ng$ y tomando g^{-1} en lugar de g se concluye $Ng \subseteq gN$, obteniendo la igualdad.
$(iii) \Longrightarrow (i)$ Directo de la hipótesis. ■

El siguiente resultado, de gran importancia, muestra como construir el grupo cociente.

1.4.2 Teorema (Grupo cociente) *Sea G un grupo, $N \lhd G$, $\mathfrak{L}$ y $\mathfrak{R}$ los conjuntos de clases laterales izquierda y derecha, respectivamente. Entonces $\mathfrak{L} = \mathfrak{R}$, más aún, estos conjuntos forman un grupo el cual es llamado grupo cociente módulo N y se denota por G/N.*

Demostración. La primera parte del teorema es consecuencia del teorema anterior, pues toda clase izquierda es una clase derecha con el mismo representante. Pongamos $G/N = \mathfrak{R}$. Sean Na y Nb elementos de G/N, entonces $NaNb = Na(a^{-1}Na)b = NNab = Nab$, lo cual muestra que el producto de dos clases derechas es otra clase derecha. Mostraremos que esta operación está bien definida, pues si $Na = Na_1$ y $Nb = Nb_1$ entonces, procediendo como antes se concluye que $Nab = Na_1b_1$, es decir, se ha definido en G/N una operación la cual satisface:

(i) Asociatividad. Se tiene de la Observación 1.3.3.

(ii) Existencia de identidad. Tomando la clase $Ne = N$, con e la identidad en G, se demuestra que $NaNe = Na$ para toda clase Na.

(iii) Existencia de inversos. Dada una clase Na, tomando Na^{-1} se cumple que $Na^{-1}Na = Ne = N$.

De las condiciones anteriores se concluye que G/N, con la operación de clases definida, es un grupo. ■

1.4.1 Corolario *Si G es finito y $N \lhd G$, entonces*

$$\left|\frac{G}{N}\right| = \frac{|G|}{|N|}.$$

Demostración. Por el Teorema de Lagrange se tiene $|G| = [G : N]|N|$. La conclusión se tiene notando que $[G : N]$ es la cardinalidad del grupo cociente. ■

Los siguientes ejemplos de grupos cociente son de gran importancia en teoría de números y álgebra lineal.

(a) Sea $G = \mathbb{Z}$ con la suma usual de enteros. Sabemos que G es abeliano y por ende todos sus subgrupos son normales. Dado $m \in \mathbb{Z}$ positivo, se verifica directamente que $m\mathbb{Z} = \{mq : q \in \mathbb{Z}\}$ es un subgrupo de $\mathbb{Z}$. Para un $n \in \mathbb{Z}$, $m\mathbb{Z} + n = \{mq + n : q \in \mathbb{Z}\}$ es la clase lateral derecha de $m\mathbb{Z}$ en $\mathbb{Z}$.

Afirmación: Las clases laterales de $m\mathbb{Z}$ en $\mathbb{Z}$ son: $m\mathbb{Z}, m\mathbb{Z}+1, \ldots, m\mathbb{Z}+(m-1)$. En efecto, si $0 \leq i, j < m$ y $m\mathbb{Z}+i = m\mathbb{Z}+j$ entonces m divide a $i-j$, la hipótesis sobre i, j implica $i = j$. Dado $n \in \mathbb{Z}$, por el algoritmo de la división, existen enteros q y r tales que $n = mq + r$ y $0 \leq r < m$, entonces $m\mathbb{Z} + n = m\mathbb{Z} + r$, probando lo afirmado.

Note que dos enteros a y b son congruentes módulo $m \iff a - b \in m\mathbb{Z}$. Si $[a]$ denota a la clase de congruencia módulo m entonces $[a] = m\mathbb{Z} + a$. De la afirmación anterior también se tiene que el grupo cociente $\mathbb{Z}/m\mathbb{Z}$ tiene cardinalidad m. Obsérvese que este ejemplo ya se discutió al considerar los enteros módulo n.

(b) Sea V un espacio vectorial sobre $\mathbb{R}$, W un subespacio, en particular W es un subgrupo de $(V, +)$ el cual es abeliano, entonces el grupo cociente V/W también lo es. Dado $r \in \mathbb{R}$ y $(W + \alpha) \in V/W$ se define una multiplicación por escalar como $r(W + \alpha) := W + r\alpha$, es claro que esta multiplicación no depende del representante de la clase $W + \alpha$ y se prueba sin dificultad que hace de V/W un espacio vectorial. Si V tiene dimensión finita, digamos n y W es un subespacio de dimensión m entonces la dimensión de V/W es $n - m$. La demostración se deja como ejercicio.

1.4.1. Ejercicios

1. Sea G un grupo, H un subgrupo de G de índice 2. Demuestre que H es normal. Este es un caso especial del siguiente resultado. Si H es un subgrupo de G tal que $[G : H]$ es el menor primo que divide a $|G|$ entonces H es normal.

2. Demuestre que la intersección de cualquier colección de subgrupos normales es un subgrupo normal.

3. Sea $H \triangleleft G$ tal que $[G : H] = n$. Demuestre que $y^n \in H$ para todo $y \in G$.

4. Sea G un grupo y G' el subgrupo generado por todos los elementos de la forma $xyx^{-1}y^{-1}$, con $x, y \in G$. A G' se le llama el subgrupo *derivado* o subgrupo *conmutador* de G. Demuestre que $G' \triangleleft G$ y G/G' es abeliano. De hecho G' es el menor subgrupo normal con tal propiedad, es decir,

si H es subgrupo normal de G, entonces G/H es abeliano si y sólo si $G' \subseteq H$.

5. Sea G un grupo. Entonces los siguientes enunciados son equivalentes

   a) $G'' = \{e\}$ (G'' es el derivado del derivado)

   b) Existe un subgrupo normal H tal que H y $\dfrac{G}{H}$ son abelianos.

   A un grupo que satisface las condiciones anteriores se le llama *metabeliano*.

6. Sea G un grupo, $H \leq G$ tal que $G' \leq H$. Demuestre que $H \triangleleft G$.

7. Sea G un grupo finito, $H \triangleleft G$ tal que $(|H|, [G : H]) = 1$. Demuestre que H es el único subgrupo de G con orden $|H|$.

8. Sea $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$. Demuestre que S^1 es un grupo con la operación producto de números complejos y $S^1 \cong \mathbb{R}/\mathbb{Z}$; $\mathbb{R}$ grupo aditivo.

9. a) Si $H \leq G$ demuestre que para todo $g \in G$, $gHg^{-1} \leq G$.

   b) Demuestre que
   $$W = \bigcap_{g \in G} gHg^{-1} \triangleleft G$$

   c) Demuestre que $H \triangleleft G \iff H = H^x := \{xhx^{-1} : h \in H\}, \forall\, x \in G$.

1.5. Grupos cíclicos

En el estudio y clasificación de los grupos, los más sencillos a considerar son los generados por un elemento, es decir los grupos cíclicos. El entender las propiedades y estructura de estos es de gran importancia, pues como se probará más adelante, todo grupo abeliano finito se descompone como producto directo de grupos cíclicos. Antes de iniciar la discusión de los grupos cíclicos, presentamos dos ejemplos de grupos que, se probará, son isomorfos. El primero se conoce como el grupo de las *raíces n-ésimas de la unidad* y el segundo fue introducido desde el inicio de la discusión.
Sea $C_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Con la multiplicación usual de complejos, C_n es un grupo, e invocando la fórmula de De Moivre, [22] página 22, se obtiene

$C_n = \{e^{(2\pi ki)/n} \mid 0 \leq k \leq n-1\}$. Declarando $\zeta_n = e^{(2\pi i)/n}$ se concluye que $C_n = \langle \zeta_n \rangle$, es decir, C_n es un grupo cíclico con n elementos.
Recordemos la definición de congruencia módulo un entero. Sea n un entero positivo, se define en $\mathbb{Z}$ una relación como

$$a \equiv b \,(\mathrm{mod}\, n) \quad \text{si } n \text{ divide a } a-b$$

y se verifica sin dificultad que esta relación es una relación de equivalencia que divide a $\mathbb{Z}$ en n clases, llamadas las clases de residuos módulo n. El conjunto de clases de residuos lo denotamos por $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ldots, \overline{n-1}\}$. Se verifica sin dificultad que las clases de residuos forman un grupo cíclico con n elementos.
Sea G un grupo cíclico digamos $G = \langle g \rangle$, entonces $G = \{g^n \mid n \in \mathbb{Z}\}$. Ya sabemos que si $|G| < +\infty$, entonces $G = \{e, g, \ldots, g^{m-1}\}$, con $|G| = m$.

1.5.1 Teorema *Sean G y H grupos cíclicos. Entonces $G \cong H \iff |G| = |H|$.*

Demostración. $\Longrightarrow$ Se tiene de la definición de isomorfismo.
$\Longleftarrow$ Sean $G = \langle g \rangle$ y $H = \langle h \rangle$. Defínase $\varphi : G \to H$ por $\varphi(g^i) := h^i$. Se verifica fácilmente que φ es un homomorfismo y además:

(i) φ es inyectiva, pues si $\varphi(g^i) = \varphi(g^j)$ entonces $h^i = h^j$. Si h tiene orden infinito, entonces la ecuación $h^i = h^j$ implica que $i = j$. Si h tiene orden finito, entonces de la ecuación $h^i = h^j$ se concluye que $|h|$ divide a $i - j$. Como $0 \leq i, j < |g| = |h|$, se debe tener $i = j$.

(ii) φ es suprayectiva, pues dado cualquier elemento de H, digamos h^i, tomamos g^i y se tiene $\varphi(g^i) = h^i$. ■

1.5.2 Teorema *Sea G un grupo cíclico, entonces los subgrupos y los cocientes de G también son cíclicos.*

Demostración. Sea H un subgrupo de G, si $H = \{e\}$ no hay nada que probar, por lo tanto podemos suponer que $H \neq \{e\}$. Sea $G = \langle g \rangle$, como $H \leq G$, existe $n \geq 1$ tal que $g^n \in H$, sea m el menor entero positivo tal que $g^m \in H$. Se afirma que $H = \langle g^m \rangle$. Claramente $\langle g^m \rangle \subseteq H$. Sea $h \in H$, como $h \in G$ entonces $h = g^k$ para algún k. Aplicando el algoritmo de la división a m y k, concluimos que existen q y r, enteros tales que $k = qm + r$ y $0 \leq r < m$, por lo tanto $h = g^k = g^{qm+r} = g^{mq}g^r$; de esta última ecuación se concluye que

$g^r \in H$. La minimalidad de m implica que $r = 0$. La conclusión se obtiene, pues $H \subseteq \langle g^m \rangle$. ■
El Teorema 1.5.1 caracteriza a los grupos cíclicos en términos de su cardinalidad, como una consecuencia de éste se tiene: *cualquier grupo cíclico infinito es isomorfo a los enteros.*

1.5.3 Teorema *Sea G un grupo finito, entonces G es cíclico $\iff$ para todo divisor k de $|G|$ existe un único subgrupo cíclico G_k de G con $|G_k| = k$.*

Demostración. $\Longleftarrow$ Es claro.
$\Longrightarrow$ Sea G cíclico con $|G| = n$. Por el Teorema 1.5.2 los subgrupos de G son cíclicos. Sea k un divisor de n, mostraremos que G contiene un único subgrupo de orden k. Sea $b = g^{n/k}$, con $G = \langle g \rangle$, claramente se tiene $|b| = k$. Sea H un subgrupo de orden k, digamos $H = \langle c \rangle$, para algún c. Para concluir la prueba es suficiente mostrar que $c \in \langle b \rangle$. Se tiene que $c = g^m$ para algún m. Como $|H| = k$, entonces $c^k = g^{mk} = e$ y como $|g| = n$, se concluye que n divide a mk, por lo tanto existe q tal que $mk = qn$, de donde se obtiene $m = (n/k)q$, concluyendo $c = g^m = g^{(n/k)q} = (g^{n/k})^q \in \langle b \rangle$. ■

NOTA. El teorema anterior se puede enunciar debilitando las hipótesis: *Un grupo finito G es cíclico, si y sólo sí para cada divisor del orden de G existe a lo más un subgrupo de ese orden.* Se puede obtener una prueba de esta versión usando un resultado sobre grupos nilpotentes o usando una propiedad de la función de Euler. (Ver Teorema 4.3.6)

1.5.4 Teorema *Sea n un natural, entonces existe un único grupo cíclico de orden n, salvo isomorfismo.*

Demostración. Tome las raíces n-ésimas de la unidad ó $\mathbb{Z}/n\mathbb{Z}$ y aplique el Teorema 1.5.1. ■

1.5.1. Ejercicios

1. Sea G un grupo cíclico de orden n. ¿Cuántos generadores tiene G?

2. Sea G un grupo abeliano finito tal que la ecuación $x^n = e$ tiene a lo más n soluciones para cada n. Demuestre que G es cíclico.

3. Sean H y K subgrupos normales de G tales que $K \cap H = \{e\}$. Demuestre que $hk = kh \ \forall \ h \in H$ y $\forall \ k \in K$.

4. Si el orden de G es pq, con p y q primos diferentes y G tiene subgrupos normales de orden p y q respectivamente. Demuestre que G es cíclico.

5. Sea G un grupo no abeliano, $Z(G)$ el centro de G. Demuestre que $G/Z(G)$ no es cíclico.

1.6. Los teoremas de isomorfismo

Anteriormente comentamos sobre la importancia de clasificar a los grupos vía isomorfismo. En este sentido es importante estudiar propiedades de homomorfismos de un grupo en otro, pues un caso especial de homomorfismos es el que lleva a la condición de isomorfismo, ¿cuál es esa condición? Un primer intento de gran utilidad es iniciar considerando una función de un grupo en el otro y tratar de ver si esta función es un homomorfismo. Para ilustrar estas ideas consideremos la siguiente situación. Sea $G = \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} : m \in \mathbb{Z} \right\}$. Con el producto usual de matrices, se verifica que G es un grupo. ¿Se puede definir un homomorfismo entre G y $\mathbb{Z}$? Un primer intento es relacionar un elemento de G con un entero para definir una función. Por ejemplo, se puede proponer una función que a cada entero m le asocie el elemento $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ de G. Un cálculo sencillo muestra que la suma de enteros es transformado en el producto de matrices, es decir, si denotamos a la función descrita antes por ϕ se tiene:

$$\phi(m + m_1) = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m_1 \\ 0 & 1 \end{pmatrix}.$$

Una vez establecido esto, es directo verificar que ϕ es biyectiva, en otras palabras, ϕ es un isomorfismo. En el ejemplo anterior resultó relativamente sencillo encontrar un isomorfismo entre los grupos propuestos, sin embargo hay situaciones en las cuales no se tendrá una forma inmediata de establecer un homomorfismo entre los grupos bajo consideración. Supongamos que se tienen dos grupos G_1 y G y un homomorfismo $f : G \to G_1$. Estamos interesados en analizar las siguientes posibilidades:

1. Si f es inyectiva, G_1 contiene un subgrupo isomorfo a G, a saber, la imagen de f.

2. Si f es biyectiva, $G \cong G_1$.

3. Si f no es inyectiva, su núcleo es diferente de la identidad. Llamémosle N. Para cualquier $g \in G$ y cualquier $n \in N$ se tiene: $f(gng^{-1}) = f(g)f(n)f(g)^{-1} = f(g)f(g)^{-1} = e_1$, con e_1 la identidad en G_1. Esto muestra que N es normal en G. ¿Hay alguna relación entre Im f y G/N? El siguiente resultado da la respuesta.

1.6.1 Teorema (Primer Teorema de Isomorfismo) *Sea $f : G \to G_1$ un homomorfismo con núcleo N, entonces $N \lhd G$ y $G/N \cong$ Im f.*

Demostración. Ya mostramos antes que N es normal. Sea $F : G/N \to \text{Im } f$ definida por $F(Na) := f(a)$. F está bien definida pues si $Na = Nb$ entonces $ab^{-1} \in N$ por lo tanto $f(ab^{-1}) = e_1$, lo cual implica que $f(a) = f(b)$. La normalidad de N implica que F es un homomorfismo. La biyectividad de F se verifica fácilmente. ■

1.6.1 Ejemplo *Sea $G = GL(n, \mathbb{C}) = \{A \in \mathfrak{M}_{n\times n}(\mathbb{C}) \mid |A| \neq 0\}$, $H = \{A \in G \mid |A| = 1\}$. Se verifica que $H \lhd G$ y G/H es abeliano, de hecho $G/H \cong \mathbb{C}^*$.*

El siguiente teorema muestra que los subgrupos normales de un grupo G, están determinados por homomorfismos de G en algún otro grupo.

1.6.2 Teorema *Sea G un grupo, $H \leq G$. Entonces $H \lhd G \iff H = \ker f$, para algún homomorfismo f.*

Demostración. $\Longleftarrow$ Se obtiene del Comentario 3 antes del teorema anterior. $\Longrightarrow$ Sea $H \lhd G$, considere G/H y defínase $\pi : G \to G/H$ como sigue:

$$\pi(a) := Ha.$$

Haciendo uso del hecho que H es normal en G, se verifica fácilmente que π es un homomorfismo con núcleo H. ■
Si π está definido como en el teorema anterior, se le llama la proyección natural.

1.6.1 Ejercicio *Sea G un grupo, H y K subgrupos. Supongamos que uno de estos es normal. ¿Es HK un subgrupo? ¿Es HK un subgrupo normal?*

1.6.3 Teorema (Segundo Teorema de Isomorfismo) *Sea G un grupo, H y K subgrupos. Supongamos que $K \lhd G$. Entonces $K \cap H \lhd H$ y $H/(K \cap H) \cong (KH)/K$.*

Demostración. Puesto que $K \cap H \subseteq H$, esto y la normalidad de K implican que $g(K \cap H)g^{-1} \subseteq K \cap H \subseteq H$ para todo $g \in H$, entonces $K \cap H \lhd H$. Claramente $K \lhd KH$. Sea $\varphi : H \to HK/K$ definido como por $\varphi(a) = Ka$. De la normalidad de K se tiene que φ es un homomorfismo, el cual es suprayectivo. Por otro lado se verifica sin dificultad que el núcleo de φ es $H \cap K$. Finalmente, el resultado se obtiene aplicando el Teorema 1.6.1 (Primer Teorema de Isomorfismo). ■

1.6.4 Teorema (Tercer Teorema de Isomorfismo) *Sea G un grupo, H y K subgrupos normales tales que $K \subseteq H \subseteq G$. Entonces $H/K \lhd G/K$ y*

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

Demostración. Sea $Ka = Kb$. La condición $K \subseteq H$ implica que $Ha = Hb$, por lo tanto se puede definir $\varphi : G/K \to G/H$ como sigue, $\varphi(Ka) := Ha$. Es claro que φ es un epimorfismo y $Ka \in \operatorname{Ker}\varphi \iff Ha = H \iff a \in H \iff Ka \in H/K$. La conclusión se obtiene del Teorema 1.6.1 (Primer Teorema de Isomorfismo). ■

Cuando se tiene un subgrupo normal $N \neq \{e\}$ en un grupo finito G, el cociente G/N resulta tener cardinalidad menor que la de G. En este sentido, el grupo cociente G/N es más pequeño y posiblemente sea más fácil estudiarlo. Algo que fuese deseable es que conociendo propiedades de G/N se pudieran obtener propiedades de G. Si esto fuese así, entonces debe haber una forma de obtener relaciones entre los subgrupos de G/N y los subgrupos de G, pero ¿cuáles de estos subgrupos? El siguiente resultado contesta la pregunta planteada, estableciendo una correspondencia biyectiva entre los subgrupos de G que contienen a N y los subgrupos de G/N. De hecho, esta correspondencia preserva normalidad e índices, más precisamente:

1.6.5 Teorema (Teorema de la correspondencia) *Sea G un grupo, $K \lhd G$ y $\pi : G \to G/K$ la proyección natural. Entonces π define una correspondencia biyectiva entre los subgrupos de G que contienen a K y los subgrupos de G/K. Si el subgrupo de G/K correspondiente a S es S^*, entonces:*

(i) $S^* = S/K = \pi(S)$.

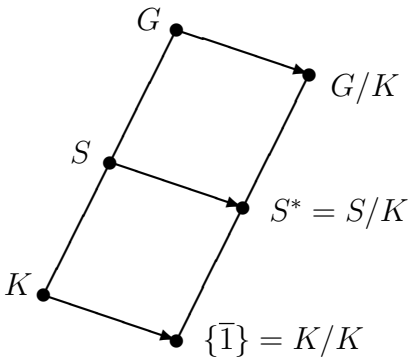
(ii) $T \subseteq S \iff T^* \subseteq S^*$ *y en este caso* $[S : T] = [S^* : T^*]$.

iii) $T \lhd S \iff T^* \lhd S^*$, *entonces* $S/T \cong S^*/T^*$.

A grandes rasgos, el teorema anterior se puede interpretar como sigue: Los subgrupos que están contenidos en K, desaparecen en el cociente y los que no lo están, aplicando el Segundo Teorema de Isomorfismo, dan origen a subgrupos de la forma

$$\frac{KH}{K} \cong \frac{H}{H \cap K}$$

lo que puede ser interpretado como las traslaciones de H módulo K. El siguiente diagrama ilustra la situación en el teorema anterior.



Demostración. Es claro que si $K \leq S \leq G$, entonces $S/K \leq G/K$. Sean S y T subgrupos de G que contienen a K tales que $S/K = T/K$. Se probará que $S = T$. Por simetría basta probar que $S \subseteq T$. Sea $a \in S$, entonces $Ka = Kb$ para algún $b \in T$, por lo tanto $ab^{-1} \in K \subseteq T$ y como $b \in T$ entonces $a \in T$, de esto se concluye que la correspondencia es inyectiva.
Sea $S^* \leq G/K$ y $S = \pi^{-1}(S^*)$. Se verifica directamente que $S \leq G$, además $\pi(S) = \pi(\pi^{-1}(S^*)) = S^*$, pues por definición de S, $\pi(S) \subseteq S^*$ y como π es sobre, entonces dado $x \in S^*$ existe y tal que $\pi(y) = x$, por lo tanto $S^* \subseteq \pi(S)$.

Hasta aquí se ha probado la parte (*i*) y que π define una correspondencia biyectiva.
(*ii*) Es claro que π preserva inclusiones, entonces resta probar que si $K \subseteq S \subseteq T$, se debe tener $[T : S] = [T^* : S^*]$, esto equivale a probar que existe una correspondencia biyectiva entre las clases S^*t^* y las clases St.
Dado $St \in \{St \mid t \in T\}$, $\pi(St) := S^*t^*$. Esta correspondencia entre clases está bien definida pues si $St = St_1$, entonces $tt_1^{-1} \in S$, por tanto $t^*t_1^{*-1} \in S^*$. El argumento anterior también prueba que π es inyectiva en el conjunto de clases; por otro lado se verifica directamente que π es suprayectiva.
(iii) Si $T \lhd S$, entonces $gTg^{-1} = T$ para todo $g \in S$ y de esto obtenemos $\pi(T) = \pi(gTg^{-1}) = \pi(g)T^*\pi(g)^{-1} = T^*$. Dado cualquier $x \in S^*$, x es de la forma $x = \pi(g)$, para algún $g \in S$, por lo tanto $xT^*x^{-1} = \pi(g)T^*\pi(g)^{-1} = \pi(gTg^{-1}) = \pi(T) = T^*$, probando que $T^* \lhd S^*$.
Recíprocamente, si $T^* \lhd S^*$, debemos mostrar que $gTg^{-1} \subseteq T$ para todo $g \in S$. Dado $x \in T$, $\pi(gxg^{-1}) = \pi(g)\pi(x)\pi(g^{-1}) \in \pi(g)T^*\pi(g)^{-1} = T^*$, por lo tanto $gxg^{-1} \in T = \pi^{-1}(T^*)$, es decir, $gTg^{-1} \subseteq T$. Por último, como $K \lhd G$ entonces K es normal en cualquier subgrupo de G, de esto y aplicando el Tercer Teorema de Isomorfismo se concluye: $S^*/T^* = (S/K)/(T/K) \cong S/T$, probando la última parte de (iii).

■

1.6.1. Ejercicios

1. Sea G un grupo y $a \in G$. Se define $f_a : G \to G$ por $f_a(g) = aga^{-1}$. Demuestre que f_a es un isomorfismo.

2. Sean H y G grupos, $f : G \to H$ un homomorfismo. Demuestre:

   (a) $f(a^n) = f(a)^n$ para todo $n \in \mathbb{Z}$,

   (b) $g(\ker f)g^{-1} \subseteq \ker f$ para todo $g \in G$.

3. Sea G el grupo aditivo de $\mathbb{Z}[x]$(polinomios con coeficientes en $\mathbb{Z}$) y H el grupo multiplicativo de los números racionales positivos. Demuestre que $G \cong H$.

4. a) Sea G un grupo tal que $x^2 = e$ para todo $x \in G$. Demuestre que G es abeliano.

b) Un grupo G es abeliano si y sólo si la función $f : G \to G$ dada por $f(x) = x^{-1}$ es un homomorfismo.

5. Sea $f : G \to H$ un homomorfismo, $a \in G$ tal que $|a| < +\infty$. Demuestre que $|f(a)|$ divide a $|a|$.

6. Sea G un grupo finito. Suponga que existe un entero $n > 1$ tal que la función $f(x) = x^n$ es un homomorfismo. Demuestre que la imagen y el núcleo de f son subgrupos normales de G.

7. Un grupo G se dice simple, si los únicos subgrupos normales son la identidad y el mismo. Sea G un grupo simple. Si $f : G \to H$ es un homomorfismo tal que $f(g) \neq e_H$, para algún $g \in G$, entonces f es inyectivo.

1.7. Producto directo de grupos

Uno de los problemas fundamentales en álgebra, al estudiar estructuras, es poder "descomponer" los objetos bajo estudio en términos de elementos más simples de entender. Por ejemplo, al estudiar a los números enteros, se tiene que estos se representan como producto de primos (Teorema Fundamental de la Aritmética). Cuando se estudian matrices no singulares, se tiene que éstas se representan como producto de matrices elementales. Si el objeto bajo estudio es un espacio vectorial de dimensión finita junto con un operador T, éste se puede representar como suma directa de subespacios T-invariantes con propiedades adicionales (Teorema de la descomposición primaria).
En el estudio de grupos, un problema de gran importancia es la "descomposición" de un grupo como "producto" de subgrupos. Este resulta ser un problema de gran dificultad, sin embargo, bajo buenas hipótesis (abeliano y finito) la respuesta es satisfactoria, Teorema 3.1.9. El proceso de factorizar, resulta mucho más difícil que el de multiplicar. ¿Pero qué es multiplicar grupos? Nos referimos al producto directo de grupos que a continuación discutimos.

Sean H y K grupos, $G = H \times K$ el producto cartesiano. Se define en G una operación como sigue:

$$(h_1, k_1) \circ (h_2, k_2) := (h_1 h_2, k_1 k_2).$$

Se verifica sin dificultad que con esta operación G es un grupo.

1.7.1 Definición *Sean H, K y G como antes, G se llama el* ***producto directo externo*** *de H y K.*

Si G es el producto directo externo de H y K entonces G contiene dos subgrupos $\overline{H}$ y $\overline{K}$ isomorfos a H y K respectivamente. Estos subgrupos se hacen explícitos de la siguiente manera

$$\overline{H} = H \times \{1\}, \qquad \overline{K} = \{1\} \times K.$$

Se verifica que $\overline{H}, \overline{K} \lhd G$, $\overline{H} \cap \overline{K} = \{e\} \subseteq G$, y $G = \overline{H}\,\overline{K}$. Cuando un grupo G contiene subgrupos de tal forma que las condiciones anteriores se cumplen, se dice que G es el ***producto directo interno*** de $\overline{H}$ y $\overline{K}$. ¿Cuál es la diferencia entre producto directo externo e interno? ¿Encuentra alguna analogía con el caso de espacios vectoriales?

1.7.1 Observación El producto directo externo de grupos es "conmutativo" y "asociativo", más precisamente:

(i) $H \times K \cong K \times H$

(ii) $(H \times K) \times L \cong H \times (K \times L)$.

De la parte (ii) de la observación anterior se concluye que dada una colección de grupos $H_1, \ldots, H_n$, el producto $H_1 \times \cdots \times H_n$ es único salvo isomorfismo, es decir, el producto es independiente del orden y forma de asociar los factores.

1.7.1 Ejercicio *Sean H y K grupos. Demuestre que $H \times K$ es abeliano $\iff$ H y K lo son.*

1.7.2 Ejercicio *Sean $m, n \in \mathbb{N}$ primos relativos. Demuestre que $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$. Concluya que si $n = \prod_{i=1}^{k} p_i^{e_i}$ es la factorización de n en primos, entonces $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$. Este Ejercicio es conocido como el* ***Teorema Chino del Residuo****.*

1.7.1 Teorema *Sea G un grupo, H y K subgrupos normales de G tales que $G = HK$ y $H \cap K = \{e\}$. Entonces $G \cong H \times K$.*

Demostración. Sea $g \in G$, entonces $g = hk$ con $h \in H$ y $k \in K$. La condición $H \cap K = \{e\}$ implica que h y k son únicos, pues si $g = hk = h_1k_1$ entonces

$h_1^{-1}h = k_1k^{-1} \in H \cap K = \{e\}$. Definamos $\varphi : G \to H \times K$ por $\varphi(g) = (h, k)$, la normalidad de H y K junto con $H \cap K = \{e\}$ implican que φ es un homomorfismo, el cual resulta ser un isomorfismo. ■

1.7.2 Teorema *Sean $G = H \times K, H_1 \lhd H,\ K_1 \lhd K$. Entonces*

$$H_1 \times K_1 \lhd G \qquad \text{y} \quad \frac{G}{H_1 \times K_1} \cong \frac{H}{H_1} \times \frac{K}{K_1}.$$

Demostración. Sean $\pi_H : H \to H/H_1,\ \pi_K : K \to K/K_1$ las proyecciones naturales, $F : G \to H/H_1 \times K/K_1$ definida por $F(h, k) := (H_1h, K_1k)$. La normalidad de H_1 y K_1 implica que F es un epimorfismo. Nótese que $(h, k) \in \ker F \iff (h, k) \in H_1 \times K_1$. El resultado se obtiene del Primer Teorema de Isomorfismo (Teorema 1.6.1). ■

1.7.1 Ejemplo *Sea G un grupo abeliano de orden p^2, p primo, entonces*

$$G \cong \begin{cases} \mathbb{Z}/p^2\mathbb{Z} \\ \mathbb{Z}/p\,\mathbb{Z} \times \mathbb{Z}/p\,\mathbb{Z} \end{cases}$$

Solución. Sea $a \in G \setminus \{e\}$, entonces $|a| = p$ ó $|a| = p^2$. Si $|a| = p^2$ para algún a, entonces $G \cong \mathbb{Z}/p^2\mathbb{Z}$. Si $|a| = p$ para todo $a \neq e$ entonces existen a y b en G tales que $|a| = |b| = p$ y $\langle a\rangle \neq \langle b\rangle$, estas condiciones implican que $\langle a\rangle \cap \langle b\rangle = \{e\}$, como G es abeliano entonces $\langle a\rangle, \langle b\rangle \lhd G$. También se tiene que $G = \langle a\rangle\langle b\rangle$, aplicando el Teorema 1.7.1 se concluye que $G \cong \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}/p\,\mathbb{Z} \times \mathbb{Z}/p\,\mathbb{Z}$.
Nota. Más adelante se probará que los grupos de orden p^2, p un primo, son abelianos.

1.7.1. Ejercicios

1. Sean m y n enteros positivos primos relativos. Demuestre que $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

2. Sea G un grupo, H y K subgrupos tales que $[G : H]$ y $[G : K]$ son finitos y primos relativos. Demuestre que $G = HK$

3. Sea G un grupo finito, H y K subgrupos normales tales que $|H||K| = |G|$. Suponga que una de las siguientes condiciones se cumple $H \cap K = \{e\}$ o $HK = G$. Demuestre que $G \cong H \times K$.

4. Sean H y K subgrupos de un grupo G. Suponga que $hk = kh$ para todo $h \in H$ y para todo $k \in K$, más aún, suponga que todo elemento de G se escribe de manera única como producto de un elemento de H y un elemento de K. Demuestre que $G \cong H \times K$.

5. Construya grupos no abelianos de orden 12, 18, 24. De hecho construya ejemplos de grupos no abelianos de orden $6n$, para todo entero $n \geq 1$.

6. Sea $\{G_\alpha\}$ una familia de grupos. ¿Cómo define el producto directo de los elementos de la familia? ¿Puede darle estructura de grupo?

7. Sea G un grupo no abeliano de orden 8. ¿Puede ser G isomorfo al producto directo de dos grupos de cardinalidad mayor que uno?

8. Sea G un grupo finito que contiene un subgrupo simple H de índice dos. Demuestre que H es el único subgrupo normal propio ó G contiene un subgrupo K de orden dos tal que $G \cong H \times K$.

Capítulo 2

Grupos de permutaciones y acciones de grupo

2.1. El grupo de permutaciones y el teorema de Cayley

Desde el punto de vista histórico, una de las fuentes originales de la teoría de grupos, consiste en considerar las permutaciones de las raíces de un polinomio con la finalidad de poder clasificar aquellos cuyas raíces se pueden expresar por medio de radicales. Esto se enmarca en el contexto de la imposibilidad de resolver la ecuación general de grado n por radicales. Nuestro interés en esta sección es presentar una discusión de la cual se desprenda que los grupos de permutaciones son universales en el sentido de contener subgrupos isomorfos a uno dado (Teorema de Cayley), más precisamente:

2.1.1 Teorema (Cayley 1878) *Todo grupo G es isomorfo a un subgrupo de un grupo de permutaciones.*

Demostración. Sea $X = G$ considerado como conjunto, S_X el grupo de permutaciones de elementos de X. Definamos $\varphi : G \to S_X$ por $\varphi(g) := f_g$, en donde $f_g(x) = gx$.
Afirmación: φ es un monomorfismo. Sean $x, y \in G$, entonces $\varphi(xy) = f_{xy}$, evaluando f_{xy} en un elemento arbitrario de G se verifica que $f_{xy} = f_x \circ f_y$, es decir φ es un homomorfismo, la inyectividad de φ se obtiene directamente. ■

2.1.1 Corolario *Si $|G| = n$, entonces $G \hookrightarrow S_n$.* ■

El Teorema de Cayley establece que todo grupo es isomorfo a un subgrupo de un grupo de permutaciones. Una desventaja de este teorema es que si $|G| = n$, entonces G está sumergido en un grupo que resulta ser muy "grande", pues su cardinalidad es $n!$ Una pregunta natural es: ¿podemos mejorar el resultado en el sentido de encontrar otro grupo con menos elementos, de manera que la conclusión del teorema siga siendo válida? En esta dirección tenemos el siguiente:

2.1.2 Teorema (Generalización del Teorema de Cayley) *Sea G un grupo, H un subgrupo y $X = \{gH \mid g \in G\}$. Entonces existe un homomorfismo $\theta : G \to S_X$ tal que $\ker\theta$ es un subgrupo maximal contenido en H normal en G.*

Demostración. Sea $\theta : G \to S_X$ definido por $\theta(g) := f_g$, con $f_g(bH) := gbH$. Se verifica directamente que θ es un homomorfismo. Sea $K = \ker\theta$, si $g \in K$ entonces $f_g(bH) = gbH = bH$ para todo $b \in G$, en particular, para $b = e$ se tiene $gH = H$, de donde se concluye $g \in H$. Mostraremos ahora que K es maximal. Sea N un subgrupo normal contenido en H. Dado $x \in N$, la normalidad de N implica que para todo $g \in G$, $g^{-1}xg \in N \subseteq H$ por lo tanto $g^{-1}xgH = H$, lo cual implica $xgH = gH$ para todo $g \in G$, y de esto se tiene $x \in \ker\theta = K$, terminando la prueba. ■

2.1.2 Corolario *Sea G un grupo finito el cual contiene un subgrupo $H \neq G$ tal que $|G|$ no divide a $[G : H]!$ Entonces H contiene un subgrupo normal no trivial. En particular G no es simple.* ■

2.1.1 Ejercicio *Sea G un grupo finito, $H \leq G$ tal que $[G : H] = p$, con p el menor primo que divide a $|G|$. Demuestre que $H \lhd G$. (Sugerencia. Use el método del Teorema 2.1.2, página 52).*

2.1.2 Ejercicio *Sea G un grupo de orden 99 y suponga que tiene un subgrupo de orden 11, (más adelante mostraremos que un grupo de orden 99 tiene un subgrupo de orden 11, lo cual se obtiene aplicando el Teorema de Cauchy, Teorema 2.3.1, página 66). Demuestre que este subgrupo es normal.*

Antes de continuar con el estudio de los grupos de permutaciones, presentaremos la clasificación de los grupos de orden p^2 y $2p$ con p primo, obteniendo como consecuencia la clasificación de los grupos de orden ≤ 10 excepto los de orden $8 = 2^3$.

2.1.3 Teorema *Sea G un grupo, H y K subgrupos de G.*

(i) Si $G = HK$, entonces para todo $x \in G$ existe un $k \in K$ tal que $H^x = H^k$.

(ii) Si H, K son subgrupos propios y $G = HK$, entonces H y K no son conjugados.

(iii) Si H es subgrupo propio, entonces $G \neq HH^x \; \forall \; x \in G$.

Demostración. i) Dado $x \in G$; por hipótesis se tiene $x = kh$, con $k \in K$ y $h \in H$. De esto obtenemos $H^x = H^{kh} = khHh^{-1}k^{-1} = kHk^{-1}$.
(ii) Si $K = H^x$ para algún $x \in G$, entonces aplicando la parte *(i)* se concluye que $K = H^x = H^k$ y esta última ecuación implica que $H = K$, por lo tanto $G = HH = H$, lo cual es imposible.
(iii) Es consecuencia de *(ii)*. ■

2.1.3 Corolario *Si G tiene orden p^2, con p un número primo, entonces todo subgrupo es normal.*

Demostración. Sean, H un subgrupo propio de G y $g \in G$. Es claro que $|H^g| = |H|$. También se tiene que $|HH^g| = \dfrac{|H^g||H|}{|H^g \cap H|} = \dfrac{p^2}{|H^g \cap H|}$. Por el Teorema de Lagrange se tiene

$$|H^g \cap H| = \begin{cases} 1 \\ p \end{cases} .$$

Si $|H^g \cap H| = 1$ entonces $|H^g H| = p^2 = |G|$, y de esto se concluye $G = H^g H$, contradiciendo la parte (iii) del teorema anterior, por lo que se debe tener $|H^g \cap H| = p = |H|$ y de esto $H^g \cap H = H$, concluyendo $H^g \subseteq H$, es decir, H es normal en G.
Otra prueba directa se obtiene aplicando el Ejercicio 2.1.1, página 52. ■

2.1.4 Teorema *Sea G un grupo de orden p^2, con p un número primo. Entonces G es abeliano.*

Demostración. Si G tiene un elemento de orden p^2, hemos terminado, por lo tanto podemos suponer que todos los elementos de $G \setminus \{e\}$ son de orden p. Sean $a, b \in G \setminus \{e\}$. Si $\langle a \rangle = \langle b \rangle$ entonces claramente $ab = ba$. Podemos

suponer que $\langle a\rangle \neq \langle b\rangle$, de lo cual se tiene, $\langle a\rangle \cap \langle b\rangle = \{e\}$, pues a y b tienen orden primo. Por el corolario anterior, $\langle a\rangle$ y $\langle b\rangle$ son subgrupos normales de G, entonces $aba^{-1}b^{-1} \in \langle a\rangle \cap \langle b\rangle = \{e\}$, es decir $ab = ba$. ■

2.1.4 Corolario *Si G tiene orden p^2, p un número primo, y no es cíclico, entonces G contiene $p+1$ subgrupos de orden p.*

Demostración. Un argumento como en el teorema anterior demuestra que $a \in G \setminus \{e\}$ está contenido en un único subgrupo de orden p, cada subgrupo de orden p contiene $p-1$ elementos diferentes de la identidad. Sean $H_1, \ldots, H_k$ los subgrupos de G de orden p. Definiendo $S_i = H_i \setminus \{e\}$ se tiene que $S_i \cap S_j = \emptyset$ para $i \neq j$ y $\cup S_i = G \setminus \{e\}$ por lo tanto

$$\left|\bigcup_i S_i\right| = \sum_{i=1}^{k} |S_i| = k(p-1) = p^2 - 1,$$

esto último implica $k = p+1$. ■

2.1.1 Observación El teorema anterior y el Ejemplo 1.7.1 página 48, clasifican los grupos de orden p^2.

En el siguiente teorema se estudian los grupos de orden $2p$, p primo impar. El caso general, es decir, $|G| = pq$, con p y q primos diferentes se hará después de haber discutido los teoremas de Sylow.

2.1.5 Teorema *Sea p un primo, entonces:*

(i) Si $p = 2$, hay dos grupos (no isomorfos) de orden $2p = 4$ los cuales son abelianos.

(ii) Si p es impar, hay dos grupos (no isomorfos) de orden $2p$: Uno es cíclico y el otro es no abeliano.

Demostración. Primero mostraremos que un grupo de orden $2p$, con p un número primo impar, contiene un elemento de orden p. Sea $g \in G \setminus \{e\}$, entonces $|g| \in \{2, p, 2p\}$. Si G contiene un elemento de orden $2p$, G es cíclico y por lo tanto contiene elementos de orden p. Si todos los elementos de G son de orden 2, G es abeliano (ejercicio), y de esto, todos los subgrupos son normales.

Sea $g \in G \setminus \{e\}$, entonces $|G/\langle g\rangle| = p$ lo cual implica que $G/\langle g\rangle$ es cíclico, por lo que debe existir $x \in G \setminus \langle g\rangle$ tal que $\langle \bar{x}\rangle = G/\langle g\rangle$. Por otro lado se tiene el hecho siguiente. Si $f : G \to H$ es un homomorfismo y $g \in G$ tiene orden finito, entonces $|f(g)|$ divide a $|g|$. De esto se concluye que p divide a $|x|$, lo cual es imposible. De lo anterior se concluye que G contiene necesariamente elementos de orden p, los cuales generan grupos normales, pues son de índice 2.

(i) Si $p = 2$ entonces $|G| = 2^2 = 4$ por lo tanto G es abeliano. El Ejemplo 1.7.1 garantiza que los grupos de orden 4 son isomorfos a uno de los siguientes

$$\mathbb{Z}_4, \qquad \mathbb{Z}_2 \times \mathbb{Z}_2.$$

(ii) Supongamos que p es impar. Por lo probado antes y la hipótesis sobre el orden de G se tiene que existen elementos a, $b \in G$ tales que $|a| = 2$ y $|b| = p$. También se tiene que $\langle b\rangle \lhd G$, por lo tanto existe $i \in \mathbb{Z}$ tal que $aba^{-1} = b^i$, de la última ecuación se obtiene $a(aba^{-1})a^{-1} = ab^ia^{-1} = b^{i^2}$, como a tiene orden 2 la anterior ecuación se reduce a $b^{i^2} = b$, lo que a la vez implica $b^{i^2-1} = e$, como b tiene orden p entonces p divide a $i - 1$ ó p divide a $i + 1$.

Caso I. $i = 1 + pk$, entonces $aba^{-1} = b^{1+pk} = b$ por lo tanto $ab = ba$ y esto implica que G contiene un elemento de orden $2p$, es decir G es cíclico.

Caso II. Si $i = pk - 1$, entonces $aba^{-1} = b^{pk-1} = b^{-1}$, es decir G no es abeliano. Para terminar la prueba se debe mostrar que hay un grupo no abeliano de orden $2p$. En general para cada $n \in \mathbb{N}$ existe un grupo no abeliano de orden $2n$ llamado el grupo diédrico construido como sigue: Sea P_n un polígono regular de n lados. Una simetría de P_n es una biyección $P_n \to P_n$ que preserva distancias y manda vértices adyacentes a vértices adyacentes. Sea D_n el conjunto de simetrías de P_n, se verifica que D_n es un grupo no abeliano de orden $2n$. ■

Con los resultados probados hasta aquí, estamos preparados para clasificar los grupos de orden ≤ 10 excepto los de orden 8, lo cual se hará más adelante. Sea G un grupo no abeliano de orden 6, entonces los elementos de orden 2 no generan subgrupos normales, pues de otra forma G tendría un subgrupo normal de orden 2 y un subgrupo normal de orden 3 cuya intersección sería la identidad, por lo tanto G sería isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_3$ el cual es abeliano. Sea b un elemento de orden 2 en G, $H = \langle b\rangle$, $X = \{gH \mid g \in G\}$. Como $|H| = 2$ entonces $|X| = 3$. Aplicando el Teorema 2.1.2 página 52, y el hecho que H no es normal se concluye que G es isomorfo a un subgrupo de $S_X = S_3$ de orden 6 por lo tanto $G \cong S_3$. Los resultados obtenidos los podemos resumir en la siguiente tabla

Cuadro 2.1: Grupos de orden ≤ 10, no incluyendo los de orden 8

Orden	*grupos abelianos*	*grupos no abelianos*
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6$	S_3
7	$\mathbb{Z}_7$	
8		
9	$\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$	
10	$\mathbb{Z}_{10}$	D_5

Después de esta disgresión regresamos a la discusión del grupo de permutaciones. Sea X un conjunto no vacío, $\sigma \in S_X$ y $x \in X$, se dice que σ fija a x si $\sigma(x) = x$. En lo que sigue, si $|X| = n$ supondremos que $X = \{1, 2, \ldots, n\}$ y $S_X = S_n$. Dado $\sigma \in S_n$, usaremos la siguiente notación para designar a σ

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix},$$

lo cual significa $\sigma(k) = i_k$. Por ejemplo $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, significa $\sigma(1) = 2,\ \sigma(2) = 1,\ \sigma(3) = 3$.

2.1.1 Definición *Sean $i_1, \ldots, i_r$ enteros distintos en el intervalo $[\![1, n]\!]$, $\sigma \in S_n$ tales que $\sigma(i_1) = i_2,\ \sigma(i_2) = i_3, \ldots, \sigma(i_r) = i_1$ y $\sigma(j) = j$ para todo $j \notin \{i_1, i_2, \ldots, i_r\}$, en este caso σ se llama* ***un r-ciclo*** *ó un* ***ciclo de longitud*** *r y se denota por $\sigma = (i_1\, i_2\, \ldots\, i_r)$. Si $r = 1$, σ es la identidad; si $r = 2$, σ se llama una* ***transposición****.*

2.1.1 Ejemplo *Sea $\sigma \in S_4$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, σ es un 4-ciclo, $\sigma =$* $(1\,2\,3\,4)$.

2.1.2 Ejemplo *Sea $\sigma \in S_5$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = (1\,3\,2)(4)(5) =$* $(1\,3\,2)$.

De los ejemplos anteriores se concluye que es importante declarar en dónde se encuentra definida la función σ, pues en el ejemplo 2 σ puede ser considerada como un elemento de S_3.

2.1.2 Definición *Sean $\sigma, \beta \in S_n$, σ y β se dicen* ***disjuntas*** *o* ***ajenas*** *si*

(i) $\sigma(x) \neq x \implies \beta(x) = x$,

(ii) $\beta(x) \neq x \implies \sigma(x) = x$.

En general el producto de permutaciones no es conmutativo, sin embargo en el caso que σ y β sean disjuntas entonces sí conmutan, ver el Ejercicio 2 página 61, al final de esta sección. Como ya se mencionó antes, uno de los problemas fundamentales cuando se estudian estructuras algebraicas es poder "factorizar" los elementos de la estructura en términos de elementos más simples. El siguiente resultado para permutaciones, es el análogo al Teorema Fundamental de la Aritmética para los enteros.

2.1.6 Teorema *Toda permutación $\sigma \in S_n \backslash \{e\}$ se puede expresar de manera única, salvo orden, como producto de ciclos ajenos de longitud ≥ 2.*

Demostración. La prueba consiste en dos etapas:

(A) Factorizar a σ como producto de ciclos ajenos.

(B) Mostrar que la factorización es única salvo orden.

(A) Sea $\sigma \in S_n$, $X = \{x : \sigma(x) \neq x\}$ y $k := |X|$. Aplicaremos inducción sobre k. Si $k = 0$ entonces σ es la identidad y no hay nada que probar. Supongamos que $k > 0$, es decir, existe $i_1 \in [\![1, n]\!]$ tal que $\sigma(i_1) = i_2 \neq i_1$. Sea $i_3 = \sigma(i_2), \ldots,$. Existe un mínimo r tal que $\sigma(i_r) = i_1$ (la existencia se obtiene, por ejemplo, usando que σ tiene orden finito). Sea

$$\sigma'(x) = \begin{cases} \sigma(x) & \text{si } x \in \{i_1, \ldots, i_r\}, \\ x & \text{en otro caso.} \end{cases}$$

Si $r = k$, entonces $\sigma = \sigma'$ y como σ' es un ciclo ya hemos terminado. Si $r < k$ defínase

$$\sigma''(x) = \begin{cases} \sigma(x) & \text{si } x \in X \setminus \{i_1, \ldots, i_r\}, \\ x & \text{en otro caso.} \end{cases}.$$

Note que σ'' mueve $k-r$ elementos, por hipótesis inductiva σ'' es producto de ciclos ajenos y claramente σ' y σ'' son disjuntas y $\sigma = \sigma'\sigma''$, con esto terminamos la parte (A).
(B) Supongamos que $\sigma = \beta_1 \cdots \beta_t = \gamma_1 \cdots \gamma_s$ con β_i y γ_j ciclos de longitud ≥ 2. Sea $i_1 \in [\![1, n]\!]$ tal que $\beta_1(i_1) \neq i_1$, entonces existe γ_j tal que $\gamma_j(i_1) \neq i_1$; como los γ_j conmutan podemos suponer que $\gamma_1(i_1) \neq i_1$ por lo tanto $\gamma_1(i_1) = \beta_1(i_1) = \sigma(i_1)$, esta última ecuación implica que $\gamma_1^m(i_1) = \beta_1^m(i_1)$ para todo m, también se tiene que γ_1 y β_1 son ciclos de la misma longitud pues en la factorización de σ son los únicos que mueven a i_1. Por otro lado se tiene que $\gamma_1^m(i_1) = i_{1+m}$, para $0 \leq m < r$ y $\beta_1^m(i_1) = i_{1+m} = \gamma_1(i_m) = \beta_1(i_m)$, por lo tanto $\beta_1 = \gamma_1$ en $\{i_1, \ldots, i_r\}$ y como ambas fijan el complemento de $\{i_1, \ldots, i_r\}$, entonces $\gamma_1 = \beta_1$. Ahora una hipótesis inductiva sobre el mínimo de $\{s, t\}$ muestra la unicidad y la igualdad $t = s$. ■

2.1.5 Corolario *El orden de σ en S_n es igual al mínimo común múltiplo de los órdenes de sus ciclos.* ■

2.1.6 Corolario *Toda permutación $\sigma \in S_n$ puede representarse, no de manera única, como producto de transposiciones.*

Demostración. Es suficiente probar que todo ciclo es producto de transposiciones, más aún, es suficiente probar que un ciclo de la forma $(1\,2 \ldots r)$ es producto de transposiciones, lo cual se obtiene de la siguiente ecuación

$$(1\,2\,\ldots\,r) = (1\,r)(1\,r-1)\cdots(1\,3)(1\,2). \qquad \blacksquare$$

2.1.3 Ejercicio *Sea p un número primo. Demuestre que los únicos elementos de orden p en S_n son los p-ciclos o productos de p ciclos.*

El siguiente resultado muestra que si bien en el teorema anterior no hay unicidad en la representación de una permutación, al menos se tiene un invariante módulo 2 en cuanto al número de transposiciones que aparecen en la factorización. Más precisamente:

2.1.7 Teorema *Sea $\sigma \in S_n$, entonces el número de transposiciones en la factorización de σ siempre es par ó siempre es impar.*

Demostración. Sean $x_1, \ldots, x_n$ números reales diferentes, definamos

$$P(x_1, \ldots, x_n) = \prod_{i<j}(x_i - x_j),$$

entonces dado $\sigma \in S_n$, σ actúa en $P(x_1, \ldots, x_n)$ como sigue

$$P^\sigma(x_1, \ldots, x_n) := \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}).$$

Si σ es una transposición, se verifica fácilmente que $\sigma(P) = -P$, por lo tanto si $\sigma = \tau_1 \cdots \tau_k$, con τ_i transposición para todo i, entonces $\sigma(P) = (-1)^k P$, de esto se obtiene el resultado. ■

2.1.3 Definición *Una permutación $\sigma \in S_n$ se dice **par** (**impar**) si σ se puede representar como producto de un número par (impar) de transposiciones. Se define el signo de σ como:*

$$\operatorname{sgn}\sigma = \begin{cases} 1 & \text{si } \sigma \text{ es par} \\ -1 & \text{si } \sigma \text{ es impar.} \end{cases}$$

2.1.8 Teorema *Sea $n \geq 2$, $A_n := \{\sigma \in S_n \mid \sigma \text{ es par}\}$. Entonces A_n es el único subgrupo de S_n de índice 2.*

Demostración. Sea $\varphi : S_n \to \{1, -1\}$ definido por $\varphi(\sigma) := \operatorname{sgn}\sigma$, se verifica directamente que φ es un homomorfismo y $\ker\varphi = A_n$, por lo tanto $S_n/A_n \cong \{1, -1\}$ y $[S_n : A_n] = 2$. Sea $H \leq S_n$ tal que $[S_n : H] = 2$, como $[S_n : A_n] = 2$ basta mostrar que $A_n \subseteq H$ y como A_n está generado por los 3-ciclos (Ejercicio 5, página 62), entonces es suficiente mostrar que H contiene a los 3-ciclos. Sea $\sigma \in S_n$, entonces $\sigma^2 \in H$, pues H tiene índice 2 en S_n, en particular si σ es un 3-ciclo $\sigma^4 = \sigma \in H$. ■

2.1.4 Definición *Al subgrupo A_n definido en el teorema anterior se le llama **grupo alternante**.*

2.1.5 Definición *Dado un grupo G se define la **relación de conjugación** en G como sigue: si $x, y \in G$ se dice que x es conjugado de y, si existe un $g \in G$ tal que $x = gyg^{-1}$. En este caso se dice que x e y son conjugados.*

Se verifica fácilmente que ser conjugados define una relación de equivalencia cuyas clases se llaman *clases de conjugación* de G. Con esta terminología se tiene que si $[x]$ es una clase, entonces $[x] = \{gxg^{-1} \mid g \in G\}$ y $[x] = \{x\} \iff gx = xg \;\forall\; g \in G$, es decir, la clase de x tiene solamente un elemento si y sólo si x pertenece al centro de G.

2.1.2 Observación $Z(G) = G \iff G$ es abeliano.

2.1.4 Ejercicio *Sea G un grupo que contiene un elemento de orden $n > 1$ y exactamente dos clases de conjugación. Demuestre que $|G| = 2$.*

2.1.5 Ejercicio *Sea $G = GL(n, \mathbb{R})$, entonces dos elementos de G son conjugados $\iff$ representan a la misma transformación lineal de $\mathbb{R}^n$ en $\mathbb{R}^n$. ¿En que consiste Z(G)?*

2.1.6 Definición *Se dice que los elementos $\alpha, \beta \in S_n$ tienen la misma **estructura en ciclos**, si para cada $r \geq 1$ el número de r-ciclos en α es igual al número de r-ciclos en β.*

El siguiente resultado caracteriza a los elementos de S_n que son conjugados.

2.1.9 Teorema *Sean $\alpha, \beta \in S_n$, entonces α y β son conjugados $\iff$ tienen la misma estructura en ciclos.*

Demostración. Sea $\sigma = (a_1 \cdots a_k)$ un $k-ciclo$ en S_n y $\tau \in S_n$, pongamos $\tau(a_i) = b_i$, entonces $\tau\sigma\tau^{-1}(b_i) = \tau\sigma(a_i) = \tau(a_{i+1}) = b_{i+1}$, para $i \leq r-1$. Definiendo $b_{k+1} = b_1$ se tiene $\tau\sigma\tau^{-1} = (\tau(a_1) \cdots \tau(a_k))$. Supongamos que $\sigma = \sigma_1 \cdots \sigma_m$ es la descomposición de σ como producto de ciclos ajenos (incluyendo ciclos de longitud uno), entonces para cualquier $\tau \in S_n$, $\tau\sigma\tau^{-1} = \tau\sigma_1\tau^{-1}\tau\sigma_2\tau^{-1} \cdots \tau\sigma\tau^{-1}$, de esto se tiene, por lo anterior, que σ y cualesquiera de sus conjugados tienen la misma estructura en ciclos.
Supongamos que σ y ρ tienen la misma estructura en ciclos, digamos $\sigma = (a_1a_2 \cdots)(b_1b_2 \cdots) \cdots$, $\rho = (c_1c_2 \cdots)(d_1d_2 \cdots) \cdots$, en donde los ciclos aparecen en orden creciente en cada una de las permutaciones. Definiendo $\tau(a_i) = c_i$, $\tau(b_i) = d_i$, y así sucesivamente, uno verifica que $\tau\sigma\tau^{-1} = \rho$. ■

2.1.3 Observación Sea $1 < k \leq n$, entonces el número de k ciclos en S_n es

$$\frac{1}{k}\left[n(n-1)\cdots(n-k+1)\right]. \tag{2.1}$$

Demostración Un k-ciclo está determinado por k elementos $i_1, \ldots, i_k$ como sigue: fije i_1 entonces hay $k-1$ formas de enviar i_1 a los restantes valores, una vez fijado el elemento i_2 tal que $i_1 \to i_2$ se tienen $k-2$ posibles formas de elegir i_3 tal que $i_1 \to i_2 \to i_3$. De esta forma se tiene que dados los elementos $i_1, \ldots, i_k$ se pueden construir exactamente $(k-1)!$ diferentes k-ciclos. También

se tiene que existen $\binom{n}{k}$subconjuntos con k elementos. Multiplicando $(k-1)!\binom{n}{k}$ se tiene el resultado. ■

2.1.3 Ejemplo *Usando la ecuación 2.1, se concluye que en S_4 hay 8 ciclos de longitud 3.*

El siguiente resultado muestra que el recíproco del Teorema de Lagrange no es verdadero, es decir, existe un grupo finito G y un entero n el cual divide a $|G|$ pero G no contiene subgrupos de orden n.

2.1.10 Teorema *A_4 no contiene subgrupos de orden 6.*

Demostración. Supongamos que existe $H \leq A_4$ tal que $[A_4 : H] = 2$, entonces $\sigma^2 \in H$ para todo $\sigma \in A_4$, en particular si σ es un 3-ciclo $\sigma^2 \in H$, por lo tanto $\sigma = \sigma^4 \in H$. Por otro lado tenemos que A_4 es generado por 3-ciclos y por el Ejemplo 2.1.3, H contiene al menos 8 elementos, lo cual es una contradicción. ■

2.1.4 Observación El corolario al Teorema 4.3.3 muestra que para $n \geq 5$, A_n no contiene subgrupos de varios órdenes, generalizando el Teorema 2.1.10.

2.1.1. Ejercicios

1. El subconjunto $\{\sigma \in S_n | \sigma(n) = n\}$ es un subgrupo de S_n isomorfo a S_{n-1}.

2. Sean α y β dos permutaciones disjuntas, entonces $\alpha\beta = \beta\alpha$.

3. Sea $\alpha = \beta_1\beta_2 \ldots \beta_m$, con los β_i r_i-ciclos disjuntos. Demuestre que $|\alpha|$ es el mínimo común múltiplo de $\{r_1, r_2, \ldots, r_m\}$. Concluya que si p es primo entonces toda potencia de un p-ciclo es un p-ciclo, o la identidad.

4. Si $z_1, \ldots, z_n$ son números complejos distintos, se define

$$d = \Pi_{i<j}(z_i - z_j)$$

(cuando $z_1, \ldots, z_n$ son las raíces de un polinomio $f(x)$ de grado n, d^2 se llama el **discriminante** de $f(x)$.) Si σ es una permutación de

$\{z_1, \ldots, z_n\}$, demuestre que $\Pi_{i<j}(\sigma z_i - \sigma z_j) = \pm d$; más aún el producto es $d \iff \sigma$ es par.

5. Sea $n > 2$, entonces A_n es generado por 3-ciclos.

6. Demuestre que S_n puede ser generado por (12) y $(12 \ldots n)$. Si G es un subgrupo de S_n que cumple: para todo par de enteros (n, m) existe un $\sigma \in G$ tal que $\sigma(n) = m$ y contiene una transposición y un p-ciclo para algún primo $p > n/2$, entonces $G = S_n$. (P. X. Gallager, *The Large Sieve and Probabilistic Galois Theory, pág. 98.* Proceeding of the Symposia in Pure Mathematics of the American Math. Society, held at the St. Louis University, St. Louis Missouri, March 27-30, 1972. Published in 1973, vol. XXIV)

7. Demuestre que todo grupo finito puede ser incluido en un grupo el cual es generado por a lo más 2 elementos.

8. Sea G un subgrupo de S_n tal que contiene una permutación impar. Demuestre que $G \cap A_n$ tiene índice dos en G. Sugerencia: $S_n = A_n \cup \tau A_n$ para cualquier τ, permutación impar.

9. Sean X, Y dos conjuntos finitos ajenos. Denotemos por S_X y S_Y a los grupos de permutaciones de los elementos de X e Y respectivamente. Demuestre que $S_X \times S_Y$ es isomorfo a un subgrupo de $S_{X \cup Y}$. Concluya que $n!m!$ divide a $(n+m)!$ y de esto último que el producto de n enteros consecutivos es divisible por $n!$, por lo que los coeficientes binomiales son enteros.

2.2. Acción de un grupo en un conjunto

El Teorema de Cayley demuestra que los elementos de G pueden ser considerados como permutaciones de los elementos de un conjunto, es decir, $G \hookrightarrow S_X$ para algún X. Esto es un caso especial de una situación más general de gran utilidad para el estudio de un grupo, lo cual se precisa con la siguiente definición.

2.2.1 Definición *Sea G un grupo, X un conjunto no vacío. Se dice que G **actúa** en X, si existe un homomorfismo $\phi : G \to S_X$.*

Cuando G actúa en X, a la pareja (X, ϕ) se le llama un G-conjunto. Si G actúa en X entonces $\phi(g)$ es una permutación de X y esta permutación se abreviará g, por abuso de notación. Entonces $gx := \phi(g)(x)$ será la notación que adoptaremos. Los siguientes son algunos ejemplos de G-conjuntos.

1. Si $G \subseteq S_X$, entonces X es un G-conjunto, pues G se identifica con un subgrupo de S_X mediante la inclusión.

2. Cualquier grupo G es un G-conjunto (Teorema de Cayley).

3. Sea G un grupo, $H \leq G$ y $X = \{gH \mid g \in G\}$ entonces G actúa en X de la siguiente manera. $\varphi : G \to S_X$ está definida por $\varphi(g) := f_g$ con $f_g(aH) := gaH$. Note que ésta es la acción que se usó en la prueba del Teorema de Cayley generalizado (Teorema 2.1.2).

4. Sea G un grupo y $X = \{H \leq G\}$, entonces G actúa en X por conjugación, es decir, $\varphi : G \to S_X$ está definida por $\varphi(g) := f_g$ con $f_g(H) := H^g = gHg^{-1}$.

5. Todo grupo G actúa en sí mismo por conjugación, es decir la acción es la misma que en el ejemplo anterior salvo que el conjunto X es el propio G.

6. Sea $G = \{A \in GL(2, \mathbb{Z}) : |A| = 1\}$, $\mathcal{H} = \{z \in \mathbb{C} : Im(z) > 0\}$. Dado $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$; se define $Az := \dfrac{az + b}{cz + d}$. Se verifica sin dificultad que G actúa sobre $\mathcal{H}$. Al grupo G se le llama grupo modular sobre $\mathbb{Z}$.

2.2.2 Definición *Sea G un grupo y X un G-conjunto, dado $x \in X$ se define la* ***órbita*** *de x, denotada* $\operatorname{orb}(x) = O_x := \{gx \mid g \in G\}$.

Este ejemplo aclara en alguna medida el por qué del término órbita de x. Sea $X = \mathbb{R}^2$ y $G = \{T_\theta : \mathbb{R}^2 \to \mathbb{R}^2 \mid T_\theta(x, y) = (x\cos\theta - y\operatorname{sen}\theta,\ x\operatorname{sen}\theta + y\cos\theta)\}$. Es un hecho bien conocido de álgebra lineal que G forma un grupo con la operación composición de transformaciones. Dado $\vec{p} \in \mathbb{R}^2$, $\operatorname{Orb}(\vec{p}) = \{T(\vec{p}) \mid T \in G\}$ es un círculo (órbita) con centro en $\vec{0}$ y radio $\|\vec{p}\|$.

2.2.1 Observación Si X es un G-conjunto, las órbitas de elementos de X constituyen una partición de X, lo cual equivale a decir que la siguiente relación en X es una relación de equivalencia.

Sean x,$y \in X$, entonces x se relaciona con y si existe un $g \in G$ tal que $x = gy$. Si X es un G-conjunto, dado $x \in X$ considere $\mathrm{St}(x) := \{g \in G \mid gx = x\}$. Se verifica sin dificultad que $\mathrm{St}(x) \leq G$. A este subgrupo se le llama el *estabilizador* de x. El siguiente resultado relaciona la cardinalidad de la órbita de un elemento con el índice de su estabilizador.

2.2.1 Teorema *Sea X un G-conjunto, $x \in X$. Entonces existe una biyección entre los elementos de O_x y las clases laterales izquierdas de* $\mathrm{St}(x)$*, es decir* $[G : \mathrm{St}(x)] = |O_x|$.

Demostración. Sea $\varphi : O_x \to \{g\mathrm{St}(x) \mid g \in G\}$ definida como sigue $\varphi(gx) := g\mathrm{St}(x)$. Existe la posibilidad que para dos elementos diferentes g y g_1 en G se tenga $gx = g_1x$, lo que implica $x = g^{-1}g_1x$, es decir $g^{-1}g_1 \in \mathrm{St}(x)$, y esto a la vez implica $g\mathrm{St}(x) = g_1\mathrm{St}(x)$, probando que φ está bien definida. La función φ es inyectiva pues $\varphi(gx) = \varphi(g_1x) \iff g\mathrm{St}(x) = g_1\mathrm{St}(x), \iff g^{-1}g_1 \in \mathrm{St}(x) \iff g^{-1}g_1x = x \iff gx = g_1x$. La suprayectividad de φ se obtiene directamente pues dado $g\mathrm{St}(x)$, entonces $gx \in O_x$ y $\varphi(gx) = g\mathrm{St}(x)$. ■
En lo que sigue consideraremos dos casos especiales de G-conjuntos que son de gran importancia para el desarrollo teórico. Sea G un grupo, $X = G$ y considere la acción de G en X por conjugación, en este caso el estabilizador de un elemento x se llama el **centralizador**, denotado por $C_G(x) = \mathrm{St}(x)$. Se tiene $g \in C_G(x) \iff gxg^{-1} = x$. Como las órbitas de elementos en G constituyen una partición, entonces $G = \cup O_x$, unión disjunta. En este caso las clases de equivalencia se llaman clases de conjugación y $O_x = \{x\} \iff x \in Z(G)$, por lo tanto

$$G = Z(G) \bigcup \left(\bigcup_{x \notin Z(G)} O_x \right).$$

Si G es finito, de la ecuación anterior se obtiene

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} [G : C_G(x)]. \tag{2.2}$$

A la Ecuación 2.2 se le conoce como la ecuación de clases de G, la cual probará ser de gran importancia.
Sea G un grupo, considérese la acción del Ejemplo 4, página 63. En este caso a $\mathrm{St}\,(H) = \{g \in G \mid H = H^g\}$ se le llama el **normalizador** de H y se denota por $N_G(H)$. La órbita de H son todos los conjugados de éste.

2.2.2 Observación Un subgrupo H es normal $\iff N_G(H) = G \iff$ la órbita de H tiene un único elemento.

2.2.1. Ejercicios

1. Proporcione los detalles de las afirmaciones en los ejemplos presentados en esta sección.

2. Sea G un p-grupo finito (ver la Definición 2.3.1), X un G-conjunto finito tal que $\text{mcd}(|X|, p) = 1$. Demuestre que hay un $x \in X$ tal que $gx = x$ para todo $g \in G$.

3. Sea V un $\mathbb{F}_p$-espacio vectorial de dimensión d. Si $G \leq \text{GL}(d, \mathbb{F}_p)$ tiene cardinalidad p^n, demostrar que existe $v \in V \setminus \{0\}$ tal que $gv = v$ para todo $g \in G$.

2.3. p-grupos y los teoremas de Sylow

En el estudio de grupos finitos, un problema de mucha importancia es determinar si el grupo bajo estudio contiene subgrupos normales propios, esto lleva al problema de clasificar los grupos simples, lo que constituyó uno de los avances más significativos de las matemáticas en el siglo XX. Sin temor a equivocación, pudiera decirse que una primera aproximación al estudio de la existencia de subgrupos normales se hace con los *Teoremas de Sylow*. Esto se ilustra en lo que viene de la discusión. En esta sección también se discutirán algunas propiedades de una clase muy importante de grupos, los llamados p-grupos. Iniciamos con la siguiente:

2.3.1 Definición *Sea G un grupo, p un número primo. Se dice que G es un p-**grupo**, si todo elemento de G tiene orden potencia de p.*

Nótese que existe la posibilidad de que G sea infinito. En uno de los ejercicios que se han planteado con anterioridad, se pide probar que si un grupo finito tiene orden par entonces G debe tener elementos de orden 2. El primer teorema de esta sección es la generalización de este hecho al caso en que un grupo finito tiene cardinalidad divisible por un primo, es decir:

2.3.1 Teorema (Teorema de Cauchy) *Sean G un grupo finito y p un primo tal que $p \mid |G|$. Entonces G contiene al menos un elemento de orden*

p. Más precisamente, el número de elementos de orden p es congruente con -1 módulo p.

Demostración. ([8], Theorem 2.7), se define el siguiente subconjunto del producto cartesiano de G p veces: $X = \{(x_1, \ldots, x_p) : x_i \in G, x_1 \cdots x_p = e\} \backslash \{(e, \ldots, e)\}$, entonces la última componente x_p de los elementos de X queda completamente determinada por los primeros $p-1$ elementos, por lo tanto $|X| = |G|^{p-1} - 1$. En particular, $|X| \equiv -1$ (mód p). Sea $H = \langle c \rangle$ el grupo cíclico de orden p. Definamos $\varphi : H \to S_X$, (S_X denota al grupo simétrico en X), como sigue: $\varphi(c^i) = f_{c^i}$, con $f_{c^i}(x_1, \ldots, x_p) := (x_{i+1}, \ldots, x_p, x_1, \ldots, x_i)$. Por otro lado se tiene que $x_1 \cdots x_p = e \Rightarrow x_1^{-1} x_1 \cdots x_p x_1 = e$, lo que equivale a $x_2 x_3 \cdots x_p x_1 = e$; por inducción se prueba que $x_{i+1} \cdots x_p x_1 \cdots x_i = e$ y de aquí se obtiene que φ define un homomorfismo, es decir, H actúa en X, por lo tanto las órbitas de X bajo la acción definida por φ tienen uno o p elementos. Sea $\vec{x} = (x_1, \ldots, x_p) \in X$, entonces $|orb\ (\vec{x})| = 1 \iff \vec{x} = (x, \ldots, x) \iff x^p = e$. Sea $X_0 = \{\vec{x} \in X : |orb\ (\vec{x})| = 1\}$, entonces la cardinalidad de X_0 es igual al número de elementos en G de orden p y $|X| = |G|^{p-1} - 1 \equiv |X_0|$ (mód p), la conclusión se tiene. ■

2.3.1 Corolario (Pequeño Teorema de Fermat) *Sea n un entero positivo y p un número primo que no divide a n. Entonces $n^{p-1} \equiv 1$ (mód p).*

Demostración. Sea G un grupo de orden n y sean X y X_0 como en la demostración del teorema anterior. Dado que p no divide a n, entonces X_0 es vacío, por lo que $|X| = |G|^{p-1} - 1 = n^{p-1} - 1 \equiv 0$ (mód p). ■

2.3.2 Corolario *Sea G un grupo finito, G es un p-grupo $\iff |G| = p^n$ para algún n.*

Demostración. La prueba se obtiene aplicando los teoremas de Cauchy y Lagrange . ■

2.3.3 Corolario *Sea G un p-grupo finito con más de un elemento, entonces $|Z(G)| > 1$.*

Demostración. La ecuación de clases para G afirma que:

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} [G : C_G(x)].$$

Por el Corolario 2.3.2 $|G| = p^n$, para algún n. Si $G = Z(G)$, hemos terminado, en caso contrario cada término de la suma anterior es un múltiplo de p, pues los subgrupos $C_G(x)$ no son iguales a G para $x \notin Z(G)$. De esto se tiene que $|Z(G)| > 1$, equivalentemente, $Z(G) \neq \{e\}$. ■

2.3.4 Corolario *Los grupos de orden p^2 con p primo, son abelianos.*

Demostración. Por el Corolario 2.3.3, se tiene que $Z(G) \neq \{e\}$, lo cual a la vez implica que $G/Z(G)$ es cíclico. Ahora la conclusión se obtiene aplicando el Ejercicio 5, página 41. ■

Dado que la noción de subgrupo maximal se usará en la siguiente discusión, recordamos la definición.

2.3.2 Definición *Sea G un grupo, $M \leq G$. Se dice que M es **maximal** si $M \leq N \leq G$ implica $M = N$ ó $N = G$.*

2.3.3 Definición *Sea G un grupo, p un número primo. Un subgrupo P es un **p-subgrupo de Sylow** si P es un p-subgrupo maximal.*

2.3.1 Observación Sea G un grupo, entonces todo p-subgrupo está contenido en un p-subgrupo de Sylow.

Demostración. Éste es un ejercicio para aplicar el Lema de Zorn al conjunto $\mathfrak{F} = \{H \leq G \mid H \text{ es un } p\text{-subgrupo}\}$. ■
Antes de presentar la discusión de los teoremas de Sylow, quisiéramos ilustrar las ideas centrales que se usarán, abordando un ejemplo. También, con este ejemplo, se ilustra la utilidad que tiene el uso de la acción de un grupo en un conjunto.

2.3.1 Ejemplo *¿Cuántos grupos, no isomorfos, de orden 15 hay?*

Iniciamos la discusión de la pregunta haciendo una consideración sobre los subgrupos de G. Por el Teorema de Cauchy, G contiene subgrupos de orden 3 y 5 respectivamente y el grupo de orden 5 es normal, pues su índice es 3, el menor primo que divide a $|G|$. ¿Es normal el subgrupo de orden 3?
Sea P un subgrupo de orden 3, P es normal en $G \iff P^g = gPg^{-1} = P$ para todo $g \in G$, en otras palabras, P es normal si el conjunto de sus conjugados tiene un solo elemento. Esto lleva a considerar la acción, por conjugación, de G en el conjunto de sus subgrupos.

Sea $X = \{P^g \mid g \in G\}$, entonces X es la órbita de P bajo conjugación, de esto se tiene que G actúa por conjugación en X. Restringiendo esta acción a P, se tiene que para cualquier $Q \in X$, $[P : \mathrm{St}_P(Q)]$ es uno o tres, más precisamente, $[P : \mathrm{St}_P(Q)] = 1 \iff P = \mathrm{St}_P(Q) = N_G(Q) \cap P$, y esto último $\iff P \leq N_G(Q)$. Por otro lado, Q es normal en $N_G(Q)$ por lo que PQ es un subgrupo de $N_G(Q)$, y por ende, también de G. Este subgrupo tiene orden 3 ó 9 (¿por qué?). Por el teorema de Lagrange, G no tiene subgrupos de orden 9, por lo tanto $|PQ| = 3$ y de esto se tiene $P = Q$, es decir, el único elemento de X cuya órbita, respecto a la acción de P, tiene cardinalidad uno, es el mismo P. También tenemos que la cardinalidad de la órbita de un elemento es igual al índice de su estabilizador.
De todo esto se tiene que $|X| = \sum |\mathrm{Orb}_P(Q)| = 1 + 3k$, para algún k. Usando la ecuación que relaciona la cardinalidad de una órbita con el índice del estabilizador tenemos: $|X| = [G : N_G(P)]$, cuando a X se le considera como una órbita bajo la acción de G en el conjunto de sus subgrupos. Como $P \subseteq N_G(P)$, entonces $[G : N_G(P)] = |X|$ es uno o cinco, esto y lo que se ha probado antes da como resultado $|X| = 1$, probando que P es normal.
Hasta este punto se ha probado que G contiene subgrupos normales de orden 3 y 5, ahora es inmediato probar que G es cíclico. La discusión anterior la resumimos en la siguiente:

2.3.2 Observación Hay solamente un grupo de orden 15, salvo isomorfismo.

2.3.2 Teorema (Sylow) [1] *Sea G un grupo finito, P un p-subgrupo de Sylow de G y l_p el número de p-subgrupos de Sylow de G, entonces*

(i) $l_p \mid |G|$ *y* $l_p \equiv 1 \pmod{p}$.

(ii) Los p-subgrupos de Sylow son conjugados .

Demostración. (i) Consideremos la acción de G en sus subgrupos por conjugación. Si P es un p-subgrupo de Sylow, sea $X = \{P = P_1, P_2, \ldots, P_r\}$ el conjunto de subgrupos conjugados de P. Es directo verificar que si un subgrupo es maximal, sus conjugados también lo son, por lo tanto los elementos de

[1] En 1872, Sylow estableció los teoremas que hoy llevan su nombre para el caso de grupos de permutaciones. Frobenius los generalizó en 1887, [24].

X son p-subgrupos de Sylow. Como X es una órbita bajo la acción descrita, entonces G actúa en éste y, por restricción, P actúa en X.
Dado $Q \in X$, $[P : \mathrm{St}_P(Q)] = p^s$, para algún s. Se tiene que $s = 0$ si y sólo si $P = \mathrm{St}_P(Q) = N_G(Q) \cap P$, y esto último ocurre $\iff P \subseteq N_G(Q)$. Como Q es subgrupo normal de su normalizador, entonces PQ es un p-subgrupo de G que contiene a P y a Q. Por maximalidad de estos se debe tener $P = Q$. Con esto se ha probado que el único elemento de X que tiene órbita con un solo elemento, cuando se hace actuar P en él, es el mismo P. De este argumento se tiene que $|X| = r = \sum |\mathrm{Orb}_P(Q)| = 1 + pl$, para algún l, es decir, $|X| \equiv 1 \pmod{p}$.
Por otro lado, al considerar a X como la órbita de P bajo la acción de G se tiene $|X| = [G : N_G(P)]$ y éste es un divisor de $|G|$. Para concluir la prueba de *i)* debemos probar la parte *ii)*.
(ii) Supongamos que Q es un p-subgrupo de Sylow y que $Q \notin X$, en particular $Q \neq P_i$. El mismo argumento anterior muestra que Q actúa en X y sus órbitas bajo esta acción tienen cardinalidad múltiplos de p, lo que contradice lo ya probado. De lo anterior se obtiene que todo p-subgrupo de Sylow es conjugado a P y por lo tanto $l_p = r$. ■

2.3.3 Teorema (Sylow) *Sea G un grupo finito, p un número primo tal que $|G| = p^n m$ con $(p, m) = 1$. Entonces todo p-subgrupo de Sylow tiene cardinalidad p^n.*

Demostración. Basta mostrar que $\mathrm{mcd}([G : P], p) = 1$, con P un p-subgrupo de Sylow. Notemos que $[G : P] = [G : N(P)][N(P) : P]$, en donde $N(P)$ es el normalizador de P. Para probar que p es primo relativo con $[G : P]$ es suficiente mostrar que $\mathrm{mcd}(p, [G : N(P)]) = 1$ y $\mathrm{mcd}(p, [N(P) : P]) = 1$. La primera de estas condiciones se debe a que $[G : N(P)] = l_p \equiv 1 \pmod{p}$), l_p como en el teorema anterior. Para probar la segunda, basta mostrar que el grupo $\dfrac{N(P)}{P}$ no tiene elementos de orden p y aplicar el teorema de Cauchy, Teorema 2.3.1. Si $\bar{x} \in \dfrac{N(P)}{P}$ es un elemento tal que $\bar{x}^e$ es la identidad, entonces el grupo $\dfrac{\langle x, P\rangle}{P}$ es un p grupo, de hecho este grupo es el generado por $\bar{x}$. Es directo verificar que si un cociente es p-grupo y el denominador también lo es, entonces el numerador es p-grupo. De esto se tiene, por maximalidad de P, que $x \in P$ y con esto se termina la prueba. ■

2.3.5 Corolario *Sea G un grupo finito, p un número primo tal que $|G| = p^n m$. Entonces G contiene subgrupos G_i tales que $|G_i| = p^i$ para todo $i = 1, \ldots, n$. Más aún, los G_i se pueden elegir de forma que $G_i \lhd G_{i+1}$.*

Demostración. Por el teorema anterior G contiene subgrupos de orden p^n. El resto se obtiene aplicando un argumento inductivo sobre el orden de un p-grupo, ver Ejercicio 8, página 70. ■

2.3.1. Ejercicios

1. Sea G un grupo finito, $H \leq G$ y P un p-subgrupo de Sylow. Supongamos que $N(P) \subseteq H$. Demuestre que $N(H) = H$, en particular $N(N(P)) = N(P)$.

2. Sea G un grupo generado por $\{g_1, \ldots, g_n\}$, G' el subgrupo derivado de G, entonces $G' \leq \langle g_1, \ldots, g_{n-1} \rangle \iff \langle g_1, \ldots, g_{n-1} \rangle \lhd G$.

3. Sea G un grupo, $H \lhd G$. Suponga que H y G/H son p-grupos. Demuestre que G es p-grupo.

4. Sea G un grupo de orden pq, $p > q$, p y q primos. Demuestre:

   (a) G tiene un subgrupo de orden p y un subgrupo de orden q.

   (b) Si q no divide a $p - 1$ entonces G es cíclico. **Nota**. La discusión completa de los grupos de orden pq se hará más adelante.

5. Demostrar que los grupos de orden 15 son cíclicos.

6. Demostrar que un grupo de orden 28 tiene un subgrupo normal de orden 7.

7. Sea G un grupo de orden 28, si G tiene un subgrupo normal de orden 4 entonces G es abeliano.

8. Sea G un grupo de orden p^n con p primo. Si $0 \leq k \leq n$, demuestre que G contiene un subgrupo de orden p^k.

9. Sea G un p-grupo finito y $\{e\} \neq H \lhd G$. Demuestre que $H \cap Z(G) \neq \{e\}$.

10. Sea G un p-grupo finito, entonces todo subgrupo normal de orden p está contenido en $Z(G)$.

11. Demuestre que todo conjugado de un p-subgrupo de Sylow es un p-subgrupo de Sylow. Concluya que si para un primo p, G tiene solamente un p-subgrupo de Sylow P, entonces $P \triangleleft G$.

12. Sea G un grupo de orden pq, p y q primos, $p > q$ y P un subgrupo de orden p. Demuestre que $P \triangleleft G$.

13. Sea G un grupo de orden p^n, p primo y $H \neq G$ subgrupo. Demuestre que existe $x \in G \setminus H$ tal que $H^x = H$.

14. Sea G un grupo tal que $|G| = p^n$, $H \leq G$ con $|H| = p^{n-1}$, entonces $H \triangleleft G$.

15. Sea G un grupo de orden p^2q, con p y q primos. Demuestre que G no es simple.

16. Sea G un grupo finito, P un p-subgrupo de Sylow contenido en $Z(G)$. Demuestre que existe un subgrupo normal N tal que $P \cap N = \{e\}$ y $PN = G$.

17. Sea G un grupo finito, P un p-subgrupo de Sylow. Sea H un subgrupo normal de G, si $P \triangleleft H$ entonces $P \triangleleft G$.

18. Si G es un grupo de orden 36 ó 30 entonces G no es simple.

19. Demuestre que los grupos no abelianos cuyo orden es menor que 60 no son simples.

20. Sea p un número primo, G un grupo no abeliano de orden p^3. Demuestre que $Z(G) = G'$.

21. Un grupo G se dice **quasi-Hamiltoniano**[2], si para todo par de subgrupos H,K de G se tiene $HK = KH$. Si G es quasi-Hamiltoniano y $S = \{g_1, \ldots, g_n\} \subseteq G$, entonces $\langle S \rangle = \{g_1^{m_1} \cdots g_n^{m_n} \mid m_i \in \mathbb{Z}\}$.

---

[2]Un grupo se dice **Hamiltoniano**, si todos sus subgrupos son normales. Por ejemplo los grupos abelianos tienen esta propiedad. La clasificación de los grupos Hamiltonianos se hace en [9], Teorema 12.5.4, página 202.

22. Sea G un p-grupo el cual es quasi-Hamiltoniano, $\Omega_1 = \{g \in G \mid g^p = e\}$. Demuestre que Ω_1 es abeliano y satisface que $f(\Omega_1) \subseteq \Omega_1$, para todo isomorfismo f de G en G.

23. Sea G un p-grupo finito, H un subgrupo de G de índice p^2. Demuestre que H es normal en G ó H tiene p conjugados.

24. Sea G un p-grupo finito. Entonces G es cíclico $\iff$ G/G' es cíclico.

25. Sea G un p-grupo finito. Entonces G es cíclico $\iff$ G tiene un único subgrupo de índice p.

26. Sea G un p-grupo no abeliano de orden p^3. Demuestre que G contiene exactamente $p+1$ subgrupos maximales.

27. Sea G un p-grupo de orden p^n, con $n \geq 3$. Suponga que el subgrupo derivado tiene orden p^{n-2}. Concluya lo mismo que en el ejercicio anterior.

28. Sea $p \geq 3$ un número primo, S_p el grupo de permutaciones en p símbolos. ¿Cuántos p-subgrupos de Sylow contiene S_p?

2.4. Grupos de orden pq

En esta sección discutimos los grupos de orden pq, con p y q números primos. Podemos suponer que $p \neq q$, pues si $p = q$, sabemos que hay exactamente dos grupos de orden p^2: uno es cíclico de orden p^2 y el otro es suma directa de dos grupos cíclicos de orden p. Por lo dicho, supongamos que $p > q$. Aplicando el Teorema de Cauchy, se obtiene que existen dos elementos A y B en G tales que $|B| = p$ y $|A| = q$. Ahora, del Teorema 2.3.2 (Sylow) se concluye que el subgrupo generado por B es normal en G.
Sea l_q el número de q-subgrupos de Sylow de G, entonces otra aplicación del Teorema 2.3.2 (Sylow) da como resultado que l_q es de la forma $l_q = 1 + kq$ y divide a $|G|$, por lo que los únicos posibles valores de l_q son 1 y p.
Si $l_q = 1$, entonces el subgrupo generado por A es normal en G y de esto se tiene que G es cíclico. Si $l_q = p$ entonces q divide a $p-1$. Mostraremos que si esto último ocurre hay exactamente un grupo no abeliano de orden pq. Para construir el citado grupo, haremos un análisis con la finalidad de encontrar las condiciones que deben satisfacer los elementos del grupo y a partir de

esto poder construirlo. En el análisis supondremos que existe tal grupo de orden pq y no es abeliano. Procediendo como se hizo antes, se tiene que $\langle B\rangle$ es normal en G, por lo que

$$ABA^{-1} = B^m, \tag{2.3}$$

para algún entero positivo m, de hecho mayor que uno, pues si $m = 1$, A y B conmutan, de lo que se tendría que G es abeliano, contrario a lo supuesto. El primer aspecto que debemos discutir es la existencia de m que satisfaga la Ecuación (2.3), esto, con la finalidad de poderlo construir. De la ecuación $ABA^{-1} = B^m$ se tiene $A^2BA^{-2} = AB^mA^{-1} = (ABA^{-1})^m = B^{m^2}$. Por inducción se obtiene $A^kBA^{-k} = B^{m^k}$, para todo entero $k \geq 1$. Tomando $k = q$ en la ecuación previa, esta se transforma en $B = B^{m^q}$ y de esto obtenemos la condición que debe satisfacer m, es decir,

$$m^q \equiv 1 \pmod{p}. \tag{2.4}$$

Notemos que la hipótesis sobre q dividiendo a $p-1$ y usando el hecho que el grupo $\mathbb{F}_p^*$ es de orden $p-1$, nos permite concluir que este grupo contiene un elemento de orden q (Teorema de Cauchy). Tomemos m igual a un representante de este elemento. Con este m y otros ingredientes construiremos a G. Las condiciones que debe satisfacer G son:

1. $|G| = pq$
2. G contiene elementos A y B de orden q y p respectivamente los cuales satisfacen la Ecuación (2.3) y m satisface la Congruencia (2.4).
3. A y B generan a G.

A partir de esto encontraremos el conjunto G y la operación que lo hace un grupo satisfaciendo las condiciones requeridas. A partir de la Ecuación 2.3 hacemos un análisis para obtener la forma en que se deben operar los elementos de G, esto se fundamenta en el hecho que A y B generan a G. La Ecuación 2.3 equivale a: $AB = B^mA$. De esta última se tiene $AB^2 = B^mAB = B^{2m}A$, y por inducción concluimos que

$$AB^t = B^{mt}A, \tag{2.5}$$

para todo entero $t \geq 0$. Usando nuevamente la ecuación $AB = B^mA$ se tiene $A^2B = AB^mA = B^{m^2}A^2$ y aplicando inducción obtenemos

$$A^sB = B^{m^s}A^s. \tag{2.6}$$

De las Ecuaciones (2.5) y (2.6) se llega a la ecuación

$$B^a A^x B^b A^y = B^a B^{m^x b} A^{x+y} = B^{a+m^x b} A^{x+y}. \tag{2.7}$$

La Ecuación (2.7) indica la forma de multiplicar en G. Notemos que los exponentes en la ecuación referida pueden ser tomados satisfaciendo

$$1 \leq a, b \leq p \quad \text{y} \quad 1 \leq x, y \leq q.$$

Para construir a G tomamos los grupos de los esteros módulo p y q, denotados $\mathbb{F}_p$ y $\mathbb{F}_q$ respectivamente y definimos $G = \mathbb{F}_p \times \mathbb{F}_q$. De la Ecuación (2.7) se tiene que la posible operación en G debe estar dada por: $(a, x) * (b, y) = (a + m^x b, x + y)$. Para mostrar que $*$ es asociativa, efectuemos el siguiente cálculo.

$$\begin{aligned} [(a, x) * (b, y)] * (c, z) &= (a + m^x b, x + y) * (c, z) \\ &= (a + m^x b + m^{x+y} c, x + y + z) \\ &= (a + m^x (b + m^y c), x + y + z) \\ &= (a, x) * [(b, y) * (c, z)]. \end{aligned}$$

El elemento $(0, 0)$ es neutro respecto a esta operación. Dado (a, x), un cálculo directo muestra que $(-m^{q-x} a, -x)$ es su inverso. Con lo anterior se tiene que G es un grupo no abeliano de orden pq. Se puede probar que $K = \{(a, 0) \in G \ : \ a \in \mathbb{F}_p\} \lhd G$ y $Q = \{(0, x) \in G \ : \ x \in \mathbb{F}_q\}$ es un subgrupo de G, de hecho se tiene, $K \cong \mathbb{F}_p$ y $Q \cong \mathbb{F}_q$. Mostraremos que cualquier otro grupo no abeliano de orden pq es isomorfo al construido. Si G_1 es otro grupo no abeliano de orden pq, podemos suponer que este grupo tiene dos elementos A y B los cuales satisfacen la Ecuación (2.3), y de esto, la Ecuación (2.7).
Definamos $\phi : G \to G_1$ como $\phi(b, x) := B^b A^x$. De la Ecuación (2.7) y la operación definida en G se concluye que ϕ es un homomorfismo, de hecho un monomorfismo, pues si $B^b A^x = e$, identidad en G_1, se tiene $b = x = 0$, probando que ϕ es un monomorfismo. Como G y G_1 tienen la misma cardinalidad, ϕ es un isomorfismo.
Al grupo G se le llama **producto semi-directo** de $\mathbb{F}_p$ por $\mathbb{F}_q$, lo denotaremos por $G = \mathbb{F}_p \rtimes_m \mathbb{F}_q$ para diferenciarlo de $\mathbb{F}_p \times \mathbb{F}_q$, en donde se considera la operación entrada por entrada.
La notación $G = \mathbb{F}_p \rtimes_m \mathbb{F}_q$, es para enfatizar que la construcción depende del entero m.

2.4.1 Ejemplo *Sean $p = 7$ y $q = 3$, entonces hay un elemento de orden 3 en $\mathbb{F}_7^*$, por ejemplo $m = 2$ es un representante. El grupo no abeliano de orden 21 es $G = \mathbb{F}_7 \rtimes_m \mathbb{F}_3$ y la operación está dada por $(a, x) * (b, y) = (a + 2^x b, x + y)$. Construya la tabla de multiplicación de este grupo.*

2.4.2 Ejemplo *Construya varios ejemplos de grupos como los discutidos antes. Continue con $p = 11$ y $q = 5$. Note que con este método también obtiene los grupos no abelianos de orden 6 y 10, constrúyalos.*

Capítulo 3

Grupos abelianos finitos y automorfismos de grupos

3.1. Grupos abelianos finitos

En esta sección se presenta una discusión completa de los grupos abelianos finitos. El objetivo es clasificar dichos grupos bajo isomorfismo. Se probará que los grupos cíclicos juegan un papel similar a los números primos, es decir, se probará que un grupo abeliano finito se "factoriza" de manera única como producto de grupos cíclicos. Antes de iniciar haremos la siguiente nota aclaratoria. La operación en un grupo abeliano será denotada aditivamente, los productos directos se llamarán sumas directas y se usará el símbolo $\oplus$ para denotar suma directa.
En este capítulo se usarán algunas propiedades de los enteros módulo p, con p un número primo, por esta razón presentamos un resultado que resume las propiedades básicas de éstos. Recordemos que para el caso de un número primo p, a los enteros módulo p los hemos denotado por $\mathbb{F}_p$, página 19.

3.1.1 Teorema *Sea p un número primo. Entonces $\mathbb{F}_p$ y $\mathbb{F}_p^*$ son grupos con las operaciones de suma y producto de clases respectivamente. Además, la multiplicación distribuye con respecto a la suma, es decir, si $[a]_p, [b]_p$ y $[c]_p$ son elementos de $\mathbb{F}_p$, entonces $[a]_p([b]_p + [c]_p) = [a]_p[b]_p + [a]_p[c]_p$.*

Demostración. Demostraremos que $\mathbb{F}_p^*$ es grupo, dejando el resto de lo afirmado a cargo del lector, ver página 18.
Recordemos que la multiplicación de clases está dada por $[a]_p[b]_p := [ab]_p$. Es

inmediato verificar que la multiplicación no depende de los representantes y es asociativa. Solamente, resta probar que cada elemento no cero tiene un inverso multiplicativo.
Sea $[a]$ una clase no cero, entonces p y a son primos relativos. Aplicando el Corolario 1.1.1 se tiene que existen enteros n y m tales que $1 = an + pm$. Tomando clase módulo p se concluye que $[1]_p = [an]_p = [a]_p[n]_p$, es decir, $[n]_p$ es el inverso de $[a]_p$. ■

La siguiente definición es presentada solamente para dar coherencia a la terminología que se usará después.

3.1.1 Definición *Un campo es un conjunto no vacío K con dos operaciones. Una suma y un producto denotados por $+$ y $\cdot$ respectivamente. Estas operaciones satisfacen:*

1. *La pareja $(K, +)$ es un grupo abeliano con identidad 0.*
2. *El conjunto $(K^* = K \setminus \{0\}, \cdot)$ es un grupo abeliano con identidad 1.*
3. *El producto distribuye respecto a la suma, es decir, $a\cdot(b+c) = a\cdot b+a\cdot c$ para todos $a, b, c \in K$.*

3.1.1 Observación Sea p un número primo. Con la terminología y notación anterior, el conjunto de clases módulo p, $\mathbb{F}_p$ es un campo con p elementos.

3.1.2 Teorema *Sea G un grupo abeliano finito, entonces G es isomorfo a la suma directa de sus subgrupos de Sylow.*

Demostración. Como G es abeliano, entonces todo subgrupo es normal, en particular los subgrupos de Sylow lo son. Sean $P_1, P_2, \ldots, P_k$ los diferentes subgrupos de Sylow de G. Mostraremos que la siguiente condición se cumple

$$H_i = P_i \cap (P_1 + \cdots + \hat{P}_i + \cdots + P_k) = \{0\} \qquad \forall\, i = 1, \ldots, k.$$

La notación $\hat{P}_i$ significa que ese sumando no aparece.
Sea $a \in H_i$, entonces $|a|$ divide a $p_i^{e_i}$ y a $\prod_{j\neq i} p_j^{e_j}$ lo cual es posible solamente si $|a| = 1$. Por otro lado se tiene que $P_1 + \cdots + P_k$ es un subgrupo de G con cardinalidad $|G|$, por lo tanto son iguales, es decir dado $g \in G$ existen $g_i \in P_i$ tales que $g = g_1 + \cdots + g_k$, más aún, la representación de g es única.

En esta situación la suma de los P_i será denotada por $G = P_1 \oplus \cdots \oplus P_k$, la cual substituye a la notación $P_1 \cdots P_k$. ■
Recordemos que nuestro objetivo es mostrar que los grupos abelianos finitos se pueden representar como suma directa de grupos cíclicos, entonces el teorema anterior reduce el problema a p-grupos abelianos.

3.1.2 Definición *Un grupo abeliano G se dice **p-elemental**, si existe un número primo p tal que $px = 0$, para todo $x \in G$.*

3.1.3 Definición *Se dice que un subconjunto $\{a_1, a_2, \ldots, a_k\}$ de un grupo abeliano G **genera una suma directa**, si $\langle a_1, a_2, \ldots, a_k\rangle = \langle a_1\rangle \oplus \langle a_2\rangle \cdots \oplus \langle a_k\rangle$.*

3.1.3 Teorema *Sea G un grupo abeliano p-elemental finito. Entonces G es un espacio vectorial sobre $\mathbb{F}_p$. Si G es finito entonces G es isomorfo a una suma directa de grupos cíclicos de orden p. Note que el número de sumandos es precisamente la dimensión de G como $\mathbb{F}_p$-espacio vectorial, y se denotará por $d(G)$.*

Demostración. Dados $g \in G$ y $\overline{a} \in \mathbb{F}_p$, definimos $\overline{a}g := ag$. Esta definición no depende de la clase de a, pues si $\overline{a} = \overline{b}$ entonces p divide a $a - b$, por lo tanto $(a - b)g = 0$ lo cual implica que $ag = bg$. Los axiomas de espacio vectorial se satisfacen con la multiplicación definida antes. El resto de la afirmación se obtiene de los siguientes hechos.

1. Todo espacio vectorial de dimensión finita es isomorfo a un número finito de copias del campo sobre el cual está definido.

2. El grupo aditivo de $\mathbb{F}_p$ es cíclico de orden p. ■

3.1.4 Teorema *Todo grupo abeliano finito es suma directa de grupos cíclicos.*

Demostración. Por el Teorema 3.1.2 podemos suponer que G es un $p-$grupo, es decir, $|G| = p^n$ para algún número primo p y $n \geq 1$. De esto se tiene que existe un $m \leq n$ tal que $p^m G = 0$. La demostración la haremos por inducción sobre m. Si $m = 1$, entonces G es un $p-$grupo elemental y por el Teorema 3.1.3, $G \cong \mathbb{F}_p \times \cdots \times \mathbb{F}_p$ y $\mathbb{F}_p$ es cíclico como grupo abeliano. Supongamos $m > 1$ y el resultado cierto para todos los grupos G que satisfacen $p^{m-1}G = 0$. Sea $H = pG$, entonces $p^{m-1}H = p^{m-1}pG = 0$. Por

hipótesis inductiva H es representable como suma directa de grupos cíclicos, es decir, $H = \langle y_1\rangle \oplus \cdots \oplus \langle y_t\rangle$ con $y_i = pz_i$ y $z_i \in G$. Sea $k_i = |y_i|$, entonces, $0 = k_i y_i = k_i p z_i = p(k_i z_i)$ y de esto $k_i z_i \in G[p] := \{g \in G | pg = 0\}$. *Afirmación.*

1. $G[p]$ es un $p-$subgrupo elemental.
2. $\{z_1, \ldots, z_t\}$ y $\{k_1 z_1, \ldots, k_t z_t\}$ generan subgrupos cuya intersección es la identidad.

La parte 1 es fácil de probar y la parte 2 se probará en el siguiente teorema. Por la parte 2, $\{k_1 z_1, \ldots k_t z_t\}$ es un subconjunto l.i. en el $\mathbb{F}_p$ espacio vectorial $G[p]$. Completando este conjunto a un conjunto maximal que sea linealmente independiente, se tiene que existen $x_1, \ldots, x_r \in G[p]$ tales que $\{k_1 z_1, \ldots, k_t z_t, x_1, \ldots, x_r\}$ es una base. Nuevamente, la parte 2 garantiza que $\{z_1, \ldots, z_t\}$ genera una suma directa y por hipótesis sobre los $x_i's$, $\{x_1, \ldots, x_r\}$ también genera una suma directa. Sean $K = \langle z_1\rangle \oplus \cdots \oplus \langle z_t\rangle$ y $N = \langle x_1\rangle \oplus \cdots \oplus \langle x_r\rangle$.

Afirmación. $G = K \oplus N$.
(i) Mostraremos que $K \cap N = \{0\}$. Si $x \in K \cap N$, se tiene $x = n_1 z_1 + \cdots + n_t z_t = s_1 x_1 + \cdots + s_r x_r$ y también $px = 0$, entonces $0 = pn_1 z_1 + \cdots + pn_t z_t = n_1 y_1 + \cdots + n_t y_t$. Como los elementos y_i generan a H como suma directa, entonces $n_i y_i = 0$ para todo i, de lo que se obtiene $k_i | n_i$, es decir, $n_i = q_i k_i$. Sustituyendo en x se tiene $x = q_1 k_1 z_1 + \cdots + q_t k_t z_t = s_1 x_1 + \cdots + s_r x_r$. Ahora la condición sobre el conjunto $\{k_1 z_1, \ldots, k_t z_t, x_1, \ldots, x_r\}$ implica que $x = 0$.
(ii) Si $g \in G$, entonces $pg \in H = \langle y_1\rangle \oplus \cdots \oplus \langle y_t\rangle$ por lo que $pg = n_1 y_1 + \cdots + n_t y_t = n_1 p z_1 + \cdots + n_t p z_t$, y de esto $p(g - (n_1 z_1 + \cdots + n_t z_t)) = 0$ lo que a la vez implica $g - (n_1 z_1 + \cdots + n_t z_t) = m_1 k_1 z_1 + \cdots + m_t k_t z_t + l_1 x_1 + \cdots + l_r x_r$. De esta ecuación se obtiene $g = (n_1 + m_1 k_1) z_1 + \cdots + (n_t + m_t k_t) z_t + l_1 x_1 + \cdots + l_r x_r \in K + N$, probando lo afirmado. ■

3.1.5 Teorema *Sea G un p-grupo abeliano, $y_1, \ldots, y_n$ elementos no cero tales que*

$$\langle y_1, \ldots, y_n\rangle = \langle y_1\rangle \oplus \cdots \oplus \langle y_n\rangle.$$

i) Si $z_1, \ldots, z_n$ son elementos de G tales que $pz_i = y_i$ para todo i, entonces

$$\langle z_1, \ldots, z_n\rangle = \langle z_1\rangle \oplus \cdots \oplus \langle z_n\rangle.$$

ii) Si $k_1, \ldots, k_n$ son enteros tales que $k_i y_i \neq 0$ para todo i, entonces

$$\langle k_1 y_1, \ldots, k_n y_n \rangle = \langle k_1 y_1 \rangle \oplus \cdots \oplus \langle k_n y_n \rangle.$$

Demostración. i) Sea $w \in \langle z_i \rangle \bigcap \left(\sum_{j \neq i} \langle z_j \rangle \right)$ entonces

$$w = n_i z_i = \sum_{j \neq i} n_j z_j.$$

La hipótesis sobre los z_i's implica que $n_i y_i = p n_i z_i = \sum_{j \neq i} p n_j z_j = \sum_{j \neq i} n_j y_j$. Como los y_i's generan una suma directa, de la ecuación anterior se tiene $n_i y_i = 0 = \sum_{j \neq i} n_j y_j$, de lo cual se concluye que $|y_k|$ divide a n_k para todo $k = 1, \ldots, n$, entonces $n_k = |y_k| q_k$. Puesto que $y_i \neq 0$, se debe tener $|y_i| = p^{s_i} > 1$, de esto obtenemos:

$$w = \left(\frac{|y_i|}{p} \right) q_i p z_i = \left(\frac{|y_i|}{p} \right) q_i y_i = \sum_{j \neq i} \left(\frac{|y_i|}{p} \right) q_j y_j.$$

Ahora, la condición sobre los y_i's implica $w = 0$.

ii) Sea $w \in \langle k_i y_i \rangle \bigcap \left(\sum_{j \neq i} \langle k_j y_j \rangle \right)$, entonces $w = n_i y_i = \sum_{j \neq i} n_j y_j$, en donde $n_l = k_l m_l$ para todo $l = 1, \ldots, n$. La hipótesis sobre los y_i's implica que $|y_i|$ divide a n_i para todo i, por lo tanto $w = 0$. ■

3.1.6 Teorema *Todo grupo abeliano G puede ser representado como suma directa de grupos cíclicos*

$$G = C_1 \oplus \cdots \oplus C_s,$$

tales que $|C_{i+1}|$ divide a $|C_i|$ para todo $i = 1, \ldots, s-1$. A la descomposición anterior de G se le llama descomposición canónica.

Demostración. Sea $G = G_1 \oplus \cdots \oplus G_r$ la representación de G como suma de p_i-grupos. Por el Teorema 3.1.4, para cada i, $G_i = C_{i1} \oplus \cdots \oplus G_{in_i}$ y los sumandos

se pueden ordenar de manera que $|C_{i\,j+1}|$ divida a $|C_{ij}|$. Definamos $C_1 = C_{11} \oplus + \cdots \oplus C_{r1}$. Como cada C_{i1} es cíclico y $|C_{i1}|, |C_{l1}|$ son primos relativos para $i \neq l$, entonces C_1 es cíclico, más precisamente, si $C_{ij} = \langle \alpha_{ij} \rangle$, entonces $C_1 = \langle \alpha_{11} + \cdots + \alpha_{r1} \rangle$. Definiendo (en caso necesario) $C_2 = C_{12} \oplus \cdots \oplus C_{r2}$ se tiene que C_2 es cíclico (mismo argumento que antes) y $|C_2|$ divide a $|C_1|$. Un proceso inductivo termina la construcción de los $C_j's$ con las condiciones requeridas. ■

3.1.1 Ejercicio *Sea G un grupo abeliano expresado como $G = H_1 \oplus \cdots \oplus H_r$ y $n \in \mathbb{N}$, entonces $nG = nH_1 \oplus \cdots \oplus nH_r$.*

3.1.7 Teorema *Dos grupos abelianos finitos G y H son isomorfos si y sólo si cada $p-$parte de G es isomorfa a la $p-$parte de H, más precisamente, si para un primo p, G_p y H_p denotan a los correspondientes $p-$subgrupos de Sylow de G y H respectivamente, entonces $G \cong H \iff G_p \cong H_p$ para cada primo p.*

Demostración ($\Rightarrow$ Si $f : G \to H$ es un isomorfismo, $f_{|_{G_p}} : G_p \to H$ satisface $f(G_p) \subseteq H_p$, es decir, $f_{|_{G_p}} : G_p \to H_p$ y claramente es un isomorfismo.
$\Leftarrow$) Si $G_p \cong H_p$ para todo p, digamos que existe $f_p : G_p \to H_p$ isomorfismo. Definiendo $f : G \to H$ como sigue: si $G = G_{p_1} \oplus \cdots \oplus G_{p_r}$ y $g \in G$, $f(g) = f(g_1 + \cdots + g_r) := f_{p_1}(g_1) + \cdots + f_{p_r}(g_r)$. Se verifica fácilmente que f es un isomorfismo. ■

3.1.8 Teorema *Sea G un grupo abeliano finito, $H \leq G$ y sean $G = P_1 \oplus \cdots \oplus P_r$ y $H = Q_1 \oplus \cdots \oplus Q_s$ las descomposiciones de G y H como en el Teorema 3.1.6. Entonces $s \leq r$ y $|Q_j|$ divide a $|P_j|$ para todo $j = 1, \ldots, s$.*

Demostración. La demostración es por contradicción, es decir, supongamos que una de las siguientes condiciones se tiene.

1. Existe un j tal que $|Q_j| \nmid |P_j|$.
2. $s > r$.

Supongamos que 1 se cumple y sea $n = |P_j|$, entonces $nG = nP_1 \oplus \cdots \oplus nP_{j-1}$ y $nQ_j \neq \{0\}$. Sea $m := |nQ_i| > 1$ y consideremos el subgrupo G_1 de nG cuyos elementos tienen orden un divisor de m, es decir, $G_1 = \{x \in nG : mx = 0\}$. Si $x \in G_1$, entonces $x = nx_1 + \cdots + nx_{j-1}$, con $x_i \in P_i$ y $0 = mx = mnx_1 + \cdots + mnx_{j-1}$.

Como $x_i \in P_i$ y los P_i forman una suma directa, entonces $0 = mnx_i$ para todo i, de esto $nx_i \in G_1$, por lo tanto $x \in (G_1 \cap P_1) \oplus \cdots \oplus (G_1 \cap P_{j-1})$. Se tiene que $G_1 \cap P_i$ es cíclico de orden menor o igual que m, pues es un subgrupo del grupo cíclico P_i, y los elementos de G_1 tienen orden a lo más m.
De lo anterior concluimos que $|G_1| \leq m^{j-1}$. Por otro lado se tiene que para cada $i = 1, \ldots, j$, Q_i contiene un subgrupo T_i isomorfo a Q_j ($|Q_j|$ divide a $|Q_i|$ para $i = 1, \ldots j$ y Q_i es cíclico), entonces $nT_i \cong nQ_j$ y de aquí $mnT_i \cong mnQ_j = 0$, por lo tanto $nT_i \subseteq G_1$, para todo i. De esto $nT_1 \oplus \cdots \oplus nT_j \subseteq G_1$, lo cual implica que $m^j \leq |G_1| \leq m^{j-1}$, obteniéndose una contradicción, pues $m > 1$. Si $s > r$, entonces $s \geq r + 1$. Tomemos $j = r + 1, P_j = \{0\}$ y claramente se tiene $|Q_j| \nmid |P_j| = 1$. Aplicando el argumento anterior, para este caso, se llega a una contradicción. ■

3.1.9 Teorema (Fundamental de los Grupos Abelianos Finitos) *Sea G un grupo abeliano finito. Si*

$$G = C_1 \oplus \cdots \oplus C_r = D_1 \oplus \cdots \oplus D_s,$$

con C_i y D_i satisfaciendo las conclusiones del Teorema 3.1.6. Entonces $r = s$ y $|C_i| = |D_i|$.

Demostración. Hagamos $H = D_1 \oplus \cdots \oplus D_s \leq G$. Por el Teorema 3.1.8, $s \leq r$ y $|D_i|$ divide a $|C_i|$ para todo $i = 1, \ldots s$. Ahora poniendo $H = C_1 \oplus \cdots \oplus C_r$ y aplicando el mismo argumento se concluye $r \leq s$ y $|C_i|$ divide a $|D_i|$. ■

3.1.2 Observación Un homomorfismo de grupos abelianos preserva sumas, y de ser inyectivo, preserva sumas directas.

Demostración. Sea $f : H \oplus K \to G$, entonces $f(H \oplus K) = f(H) + f(K)$. Si f es inyectiva y $x \in f(H) \cap f(K)$, se tiene $x = f(h) = f(k)$ como f es inyectiva $h = k \in H \cap K = \{0\}$. Por lo tanto $x = 0$, luego $f(H \oplus K) = f(H) \oplus f(K)$. ■

3.1.1 Corolario *Dos $p-$grupos abelianos G y H son isomorfos $\iff$ G y H tienen el mismo número de sumandos cíclicos de cada orden.* ■

Se desea determinar el número de grupos abelianos no isomorfos de cardinalidad dada. Por el Teorema 3.1.7 el problema se reduce al caso en que la cardinalidad es potencia de un primo. Deseamos determinar el número de

grupos abelianos no isomorfos a pares de orden p^n con p primo. Si $|G| = p^n$ y $G = C_1 \oplus \cdots \oplus C_r$ con $|C_i| = p^{n_i}$, entonces se debe tener, Teorema 3.1.6, que $n_1 \geq n_2 \geq \cdots \geq n_r$. Por el Teorema 3.1.9, un grupo G_1 con $|G_1| = p^n$ es isomorfo a $G \iff$ el número de sumandos de cada orden en las descomposiciones de G y G_1 coinciden.

3.1.4 Definición *Dado un entero positivo n, una **partición** de n es una sucesión de enteros $1 \leq i_1 \leq i_2 \leq \cdots \leq i_r$ tal que $n = i_1 + i_2 + \cdots + i_r$. Al número de particiones de n lo denotaremos por $P(n)$.*

Ejemplos: $P(2) = 2$, $P(3) = 3$, $P(4) = 5$, $P(5) = 7$. En general, es difícil evaluar $P(n)$.

3.1.2 Ejercicio *Sea p un número primo, n un entero positivo y $P(n)$ el número de particiones de n. Demuestre que el número de grupos abelianos no isomorfos de orden p^n es $P(n)$. Si $m = \prod_{i=1}^{k} p^{n_i}$ es la descomposición de m como producto de primos, entonces el número de grupos abelianos no isomorfos de orden m es $\prod_{i=1}^{k} P(n_i)$.*

3.1.1 Ejemplo *Sea p un número primo, entonces hay exactamente 3 grupos abelianos no isomorfos de orden p^3:*

$$\mathbb{Z}/p^3\mathbb{Z}, \quad \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z} \quad \text{y} \quad \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}.$$

3.1.1. Ejercicios

1. Sea G un grupo abeliano de orden p^n. Demuestre lo siguiente.
   (a) Existe un entero $m \leq n$ tal que $x^{p^m} = e$ para todo $x \in G$.
   (b) El grupo G contiene elementos de orden p^m.

2. Sea G un grupo abeliano finito, si G contiene subgrupos de orden m y n respectivamente. Demuestre que G contiene un subgrupo de orden el mínimo común múltiplo de m y n.

3. Sea G un grupo abeliano de orden m y suponga que para todo primo p, divisor de m se tiene que G contiene exactamente $p-1$ elementos de orden p. Demuestre que G es cíclico.

4. Demuestre que un grupo abeliano finito G, es cíclico si y sólo si $G \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$, donde $p_1, \cdots, p_k$ son números primos diferentes.

5. Determine el número de grupos abelianos no isomorfos de orden 8, 100 y 16200. Escriba una lista de tales grupos.

6. En los siguientes ejercicios, φ denota la función de Euler. Sean m y n enteros positivos tales que m y n tienen los mismos factores primos. Demuestre que $m/n = \varphi(m)/\varphi(n)$.

7. Sean m y n enteros positivos primos relativos. Demuestre que $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$.

8. Sean m y n enteros positivos, $d = \text{mcd}(m, n)$. Demuestre que $\varphi(mn) = d\varphi(m)\varphi(n)/\varphi(d)$.

9. (Tucson Az. Oct. 24 1987) Sea G un grupo con dos subgrupos H_1 y H_2 de índice 2 tales que $H_1 \cap H_2 = e$. Demuestre que $G \cong C_2 \oplus C_2$.

10. Sea $n > 1$ un entero, G un grupo que tiene exactamente n elementos de orden n. Demuestre a lo más dos primos diferentes dividen a n.

11. Encuentre ejemplos de grupos que tengan exactamente 36 elementos de orden 36. De hecho, demuestre que hay infinidad de tales grupos.

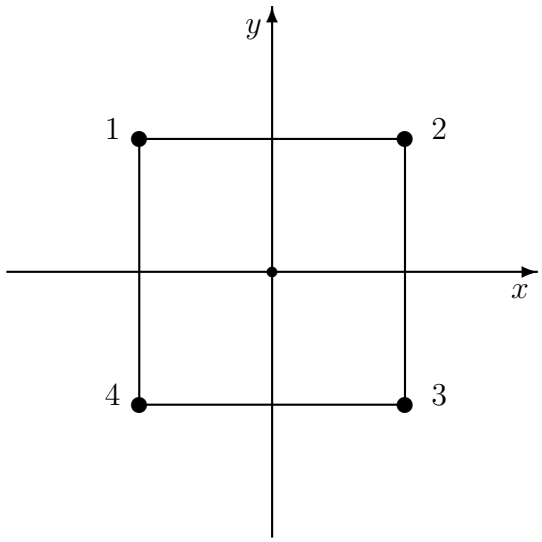
3.2. Clasificación de grupos de orden ≤ 15

En la sección anterior se hizo un estudio de los grupos abelianos finitos, en particular se estableció el teorema que describe su estructura, obteniéndose de esto su clasificación. En general, el estudio y clasificación de los grupos finitos es un problema muy difícil, cuya solución fue uno de los avances más significativos en matemáticas en el siglo XX.
En esta sección presentamos la clasificación de grupos cuyo orden es ≤ 15. El lector interesado en ir más lejos en la clasificación de grupos finitos puede consultar la referencia [17] enumerada en la bibliografía que aparece al final

del texto. Una pregunta natural es, ¿por qué el orden de los grupos que se clasifican es ≤ 15? La razón es que la clasificación de los grupos de orden $16 = 2^4$ requiere un análisis que nos llevaría fuera del contexto de este trabajo, ver la referencia citada antes. En la Tabla 1 omitimos los grupos de orden 8, lo cual se debió a que no teníamos una clasificación de los grupos abelianos finitos. En esta sección dicha tabla se extiende de manera que incluya a los grupos de orden menor o igual que 15. Iniciamos con la discusión de los grupos de orden 8.

3.2.1. Grupos no abelianos de orden 8

(a) El grupo diédrico. Considere un cuadrado centrado en el origen del plano cartesiano como se muestra en la siguiente figura.



Enumerando los vértices en el sentido que giran las manecillas del reloj, se definen las siguientes transformaciones de $\mathbb{R}^2 \to \mathbb{R}^2$:

R: rotación $\pi/2$ radianes.

T_x: reflexión alrededor del eje x.

T_y: reflexión alrededor del eje y.

$T_{1,3}$: reflexión alrededor de la diagonal 1 3.

$T_{2,4}$: reflexión alrededor de la diagonal 2 4.

Sea $D_4 = \{R^i, T_x, T_y, T_{1,3}, T_{2,4} \mid i = 1, 2, 3, 4\}$, D_4 es un grupo con la composición usual de funciones. Note que D_4 se puede identificar con un subgrupo de S_4, pues sus elementos quedan completamente determinados por su acción en los vértices del cuadrado. La identificación se puede dar por medio del isomorfismo que asocia a la rotación R con la permutación $(1\,2\,3\,4)$ y a la reflexión $T_{1\,3}$ con $(2\,4)$. Se verifica que D_4 tiene 5 subgrupos de orden 2 y 3 subgrupos de orden 4. Otra propiedad de este grupo es que contiene subgrupos que no son normales, por ejemplo $H_1 = \langle (1\,2\,3\,4)^2(2\,4)\rangle$ es un subgrupo de orden 2 el cual no es normal. Si $H = \langle (1\,2\,3\,4)^2, (2\,4)\rangle$ entonces $H_1 \lhd H \lhd D_4$, probando con esto que ser normal no es una propiedad transitiva. El grupo D_4 puede definirse en términos de generadores:

$$D_4 = \langle a, b \mid a^4 = b^2 = 1, \quad bab^{-1} = a^{-1}\rangle.$$

(b) El grupo de los cuaternios. Sea $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. Definiendo en

Q una multiplicación como sigue: $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$ y usando las reglas usuales de multiplicación por menos, Q resulta ser un grupo no abeliano con 8 elementos el cual tiene la propiedad que todo subgrupo es normal, pues el único subgrupo de orden 2 es $\{\pm 1\}$ y es normal. Los restantes subgrupos son de índice 2, por lo tanto normales. Uno verifica que Q contiene dos elementos a y b los cuales satisfacen:

$$a^4 = 1, \quad b^2 = a^2 \quad \text{y} \quad b^{-1}ab = a^{-1}. \qquad (*)$$

Un grupo con dos generadores que satisfacen $(*)$ se llamará el **grupo de los cuaternios**. Los grupos D_4 y Q tienen orden 8 y $D_4 \ncong Q$. El siguiente resultado muestra que los grupos construidos anteriormente son los únicos no abelianos de orden 8.

3.2.1 Teorema *Sea G un grupo no abeliano de orden 8. Entonces $G \cong D_4$ ó $G \cong Q$.*

Demostración. Como G no es abeliano, G no tiene elementos de orden 8, por lo que $|a| \in \{2, 4\}$ para todo $a \in G \setminus \{e\}$. Si $|a| = 2$ para todo a entonces G es abeliano. De los argumentos anteriores se concluye que G contiene al

menos un elemento a de orden 4, el cual genera un subgrupo normal. De esto último se obtiene $b^2 \in \langle a \rangle$ para todo $b \in G \setminus \{e\}$, es decir, $b^2 \in \{e, a, a^2, a^3\}$. Si $b^2 \in \{a, a^3\}$, entonces $|b| = 8$, lo cual es imposible, de esto se obtiene $b^2 \in \{e, a^2\}$. Por otro lado se tiene que $b^{-1}ab \in \langle a \rangle = \{e, a, a^2, a^3\}$. Como G no es abeliano, a no puede pertenecer al centro de G, pues de otra forma $|Z(G)| \geq 4$, lo cual implica que $G/Z(G)$ es cíclico y esto a la vez implica que G es abeliano, contradiciendo lo supuesto sobre G.
Hasta este punto podemos concluir que existe un $b \in G$ tal que $b^{-1}ab \neq a$. Si $b^{-1}ab = a^2$ entonces $b^{-2}ab^2 = b^{-1}a^2b = (b^{-1}ab)^2 = a^4 = e$ lo cual no puede ser. De los argumentos vertidos previamente se tiene que existe un $b \in G \setminus \{e\}$ tal que

$$b^2 = a^2 \qquad b^2 = e \quad \text{y} \quad b^{-1}ab = a^3 = a^{-1}.$$

Resumiendo la discusión anterior, se tienen las siguientes posibilidades:

(i) G contiene elementos a y b tales que $a^4 = e$, $b^2 = a^2$ y $b^{-1}ab = a^{-1}$

(ii) G contiene elementos a y b tales que $a^4 = b^2 = e$ y $b^{-1}ab = a^{-1}$.

La conclusión se obtiene de las propiedades que definen a los grupos diédrico y de los cuaternios. ■

3.2.2. Grupos no abelianos de orden 12

3.2.2 Teorema *Sea G un grupo no abeliano de orden 12 no isomorfo a A_4, entonces G contiene un elemento de orden 6.*

Demostración. Sea P un 3-subgrupo de Sylow de G, $X = \{gP \mid g \in G\}$. Argumentando como en la prueba del Teorema 2.1.2, página 52 y usando que G no es isomorfo a A_4, se concluye que $P \lhd G$. Por otro lado, $|P| = 3$, por lo que $P = \langle a \rangle$. La normalidad de P implica que G contiene exactamente 2 elementos de orden 3 los cuales son a y a^2, por lo tanto la órbita de a bajo conjugación contiene a lo más dos elementos, es decir, $|O_G(a)| = [G : \text{St } (a)] \leq 2$. Recuerde que St $(a) = \{g \in G \mid gag^{-1} = a\}$. La anterior desigualdad es equivalente a $|\text{St (a)}| \in \{6, 12\}$, de lo cual se obtiene que existe $b \in$ St (a) tal que $|b| = 2$ y $ab = ba$. Como a y b tienen órdenes primos relativos, entonces $c = ab$ tiene orden 6. ■

3.2.3 Teorema *Hay exactamente 3 grupos no abelianos de orden 12.*

Demostración. La demostración se terminará si mostramos que hay exactamente dos grupos no abelianos de orden 12 no isomorfos a A_4. Sea G un grupo de orden 12 no abeliano y no isomorfo a A_4. Por el Teorema 3.2.2, existe un $a \in G$ tal que $|a| = 6$.
Caso I. Si G contiene un elemento b de orden 4, entonces necesariamente $\langle b\rangle \cap \langle a\rangle \neq \{e\}$, pues de otra forma la normalidad de $\langle a\rangle$ implicaría que $\langle b\rangle\langle a\rangle$ es un subgrupo de orden 24, lo cual es imposible, por lo tanto los elementos a y b satisfacen $a^6 = b^4 = e$ y $a^3 = b^2$. También se tiene que $bab^{-1} = a^i$ para algún $i \in \{1, 2, 3, 4, 5\}$, pues $\langle a\rangle \lhd G$. Si $i = 1$, entonces a^2 y b conmutan, por lo tanto a^2b tiene orden 12, lo cual es imposible pues G no es abeliano.
Si $i = 2$, entonces $bab^{-1} = a^2$ y de aquí concluimos que $b^2ab^{-2} = ba^2b^{-1} = a^4$. Aplicando el hecho que $a^3 = b^2$ se obtiene $a = a^4$, lo cual no es posible. De manera similar se muestra que $i \notin \{3, 4\}$ por lo que necesariamente $i = 5$, es decir $bab^{-1} = a^5 = a^{-1}$ y esta última ecuación equivale a $aba = b$, lo que a la vez implica $abab = b^2 = a^3$, obteniendo que G está definido por generadores a y b los cuales satisfacen

$$a^6 = b^4 = e, \quad a^3 = b^2 = (ab)^2.$$

Este grupo será denotado por T.

Caso II. Si G no contiene elementos de orden 4, entonces existe un elemento de orden 2 tal que $b \notin \langle a\rangle$. Nuevamente la normalidad de $\langle a\rangle$ implica que $bab^{-1} = a^i$ para algún $i \in \{1, 2, 3, 4, 5\}$. Como $b \notin \langle a\rangle$, i no puede ser 1, pues $\langle a\rangle\langle b\rangle$ sería un subgrupo abeliano de orden 12. Si $i = 3$, entonces $bab^{-1} = a^3$, lo que implica $ba^2b^{-1} = a^6 = e$, y de esto se tiene que $a^2 = e$, contradiciendo que a tiene orden 6. Los casos $i \in \{2, 4\}$ se abordan como en el Caso I, obteniendo incompatibilidades. De lo anterior se concluye que G está generado por dos elementos a y b los cuales satisfacen

$$a^6 = b^2 = e, \quad bab^{-1} = a^{-1}.$$

En este caso G es isomorfo al grupo diédrico de orden 12. ■

Construcción del grupo T. Sean $C_3 = \langle k\rangle$ y $C_4 = \langle x\rangle$ grupos cíclicos de orden 3 y 4 respectivamente. Pongamos $T = C_3 \times C_4$ y definamos en T la siguiente operación.

$$(k^i, x^j)(k^l, x^r) := (k^{i+2^j l}, x^{j+r}).$$

Demuestre lo siguiente:

1. La operación definida hace de T un grupo con identidad $(1,1) = (k^0, x^0)$ y los elementos $a = (k^2, x^2)$ y $b = (1, x)$ satisfacen $a^6 = b^4 = (1,1)$, $b^2 = a^3 = (ab)^2$.

2. Los elementos $(k,1)$ y $(1,x)$ generan subgrupos de orden 3 y 4 respectivamente.

3. Determine el inverso de un elemento (k^l, x^j) y demuestre que el subgrupo generado por $(k,1)$ es normal en T.

4. El elemento a satisface: $\langle a^2\rangle \lhd \langle a\rangle \lhd T$ y $\langle a^2\rangle \lhd T$, es decir, en este ejemplo se cumple que la propiedad de ser normal es transitiva en un grupo no abeliano.

La siguiente tabla resume la clasificación de los grupos de orden ≤ 15.

Cuadro 3.1: Clasificación de grupos de orden ≤ 15

Orden	*grupos abelianos*	*grupos no abelianos*
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6$	S_3
7	$\mathbb{Z}_7$	
8	$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$Q,\ D_4$
9	$\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$	
10	$\mathbb{Z}_{10}$	D_5
11	$\mathbb{Z}_{11}$	
12	$\mathbb{Z}_{12},\ \mathbb{Z}_6 \times \mathbb{Z}_2$	$A_4,\ T,\ D_6$
13	$\mathbb{Z}_{13}$	
14	$\mathbb{Z}_{14}$	D_7
15	$\mathbb{Z}_{15}$	

3.3. Automorfismos de grupos

3.3.1 Definición *Sea G un grupo. Un isomorfismo de G en G se llama un* ***automorfismo*** *de G.*

3.3.1 Observación Si G es un grupo finito y f es un homomorfismo de G en G entonces f es un automorfismo $\iff$ f es epimorfismo $\iff$ f es monomorfismo.

Si G es un grupo, el conjunto de automorfismos de G denotado por $A = \operatorname{Aut} G$, forma un grupo con la composición de funciones. Dado un grupo G, existe un homomorfismo $\varphi : G \to \operatorname{Aut} G$ definido por $\varphi(g) := f_g$, en donde $f_g(a) = gag^{-1}$. La imagen de φ la denotaremos por $\operatorname{Inn}(G)$ y se llama el grupo de **automorfismos internos** de G. En el siguiente resultado se precisa la relación entre G e $\operatorname{Inn}(G)$.

3.3.1 Teorema *Sea G un grupo. Entonces* $\operatorname{Inn}(G) \lhd \operatorname{Aut} G$ *y* $G/Z(G) \cong \operatorname{Inn}(G)$.

Demostración. Sea φ el homomorfismo definido anteriormente, entonces $\varphi(g) = \mathrm{id}_G \iff f_g(a) = a \ \forall\ a \in G, \iff g \in Z(G)$. El Primer Teorema de Isomorfismo (Teorema 1.6.1) implica que $G/Z(G) \cong \operatorname{Inn}(G)$. Sean $f_g \in \operatorname{Inn}(G)$ y $\alpha \in \operatorname{Aut} G$, entonces $\alpha f_g \alpha^{-1} = f_{\alpha(g)}$ lo cual se verifica sin dificultad. ■

3.3.2 Observación Si $G \cong G_1$ entonces $\operatorname{Aut} G \cong \operatorname{Aut} G_1$. El recíproco es falso, por ejemplo tome S_3 y $\mathbb{Z}_2 \times \mathbb{Z}_2$. H. Leptin [11], ha probado un resultado muy profundo en esta dirección: **Sea p un número primo ≥ 5, G y H dos p-grupos. Entonces $G \cong H \iff \operatorname{Aut} G \cong \operatorname{Aut} H$.**

Determinar la estructura de los grupos de automorfismos es muy difícil, aun para grupos abelianos. Una idea de esto la obtendremos al determinar la estructura de los automorfismos de los grupos cíclicos.

3.3.2 Teorema *Sean H y K grupos finitos tales que* $(|H|, |K|) = 1$, *entonces* $\operatorname{Aut}(H \times K) \cong \operatorname{Aut} H \times \operatorname{Aut} K$.

Demostración. Por la observación anterior basta probar que

$$\operatorname{Aut}(H \times K) \cong \operatorname{Aut}(H \times \{1\}) \times \operatorname{Aut}(\{1\} \times K)$$

pues $H \times \{1\} \cong H$ y $\{1\} \times K \cong K$. Note que la condición $(|H|, |K|) = 1$ implica $|(h, k)| = |h||k|$ para todo $(h, k) \in H \times K$. Se verifica que un automorfismo de $H \times K$ induce automorfismos, por restricción, en $H \times \{1\}$ y en $\{1\} \times K$. Esta forma de inducir es en efecto un isomorfismo. ■

Una pregunta natural es suprimir la hipótesis sobre los órdenes de los grupos, es decir, si H y K son grupos finitos y sus órdenes no son primos relativos,

¿hay una relación entre $\operatorname{Aut}(H \times K)$ y $\operatorname{Aut} H \times \operatorname{Aut} K$? Intente con $H = K = C_2$, el grupo cíclico de órden 2.

3.3.3 Teorema *Sea G un grupo cíclico de orden n. Entonces*

$$\operatorname{Aut} G \cong (\mathbb{Z}/n\,\mathbb{Z})^* = \{\overline{a} \mid (n, a) = 1\}.$$

En particular $|\operatorname{Aut} G| = \varphi(n)$, con φ la función de Euler.

Demostración. Sea $f \in \operatorname{Aut} G$, entonces f queda bien determinado por su acción sobre un generador c de G, es decir $f(c) = c^{a_f}$. Como f es un automorfismo de $G = \langle c \rangle$, entonces $(a_f, n) = 1$. Definamos $\varphi : \operatorname{Aut} G \to (\mathbb{Z}/n\,\mathbb{Z})^*$ como $\varphi(f) := \overline{a_f}$. Uno verifica sin dificultad que φ es un isomorfismo. ■

Sabemos que $(\mathbb{Z}/n\mathbb{Z})^*$ es un grupo abeliano finito, entonces el Teorema Fundamental para grupos abelianos finitos garantiza que se puede representar como suma directa de grupos cíclicos, ¿cuales son los sumandos? En el siguiente resultado se inicia la descripción de éstos, probaremos que la primera aproximación para obtener la descomposición de $(\mathbb{Z}/n\mathbb{Z})^*$ está dada en términos de los factores primos de n.

3.3.4 Teorema *Sea $n = \prod_{i=1}^{k} p_i^{e_i}$ la factorización de n como producto de primos. Entonces $(\mathbb{Z}/n\,\mathbb{Z})^* \cong \prod_{i=1}^{k} (\mathbb{Z}/p_i^{e_i}\,\mathbb{Z})^*$.*

Demostración. La prueba se hará por inducción sobre el número de factores primos de n, para lo cual es suficiente probar, cambiando un poco la notación, que si $M = mn$ con $(n, m) = 1$ y $f : (\mathbb{Z}/M\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ definida por $f(x + M\mathbb{Z}) = (x + n\mathbb{Z}, x + m\mathbb{Z})$ entonces f es un isomorfismo. Se verifica sin dificultad que f está bien definida y es un monomorfismo, es decir, $f(x+M\mathbb{Z}) = (1+n\mathbb{Z}, 1+m\mathbb{Z}) \iff x \equiv 1 \pmod{n}$ y $x \equiv 1 \pmod{m}$, la hipótesis sobre n y m y lo anterior garantizan $x \equiv 1 \pmod{M}$.
El Ejercicio 1.7.2, sobre el Teorema Chino del Residuo página 47, garantiza que cuando la función anterior se considera en todo $(\mathbb{Z}/M\mathbb{Z})$, resulta ser suprayectiva, es decir, dado $(a+n\mathbb{Z}, b+m\mathbb{Z})$ con a y b enteros, existe $x+M\mathbb{Z}$ tal que $f(x+M\mathbb{Z}) = (a+n\mathbb{Z}, b+m\mathbb{Z})$. Es fácil ver que si a es primo relativo con n y b es primo relativo con m, entonces x es primo relativo con M, probando suprayectividad de f, es decir, f es un isomorfismo. ■

Dado que la función φ de Euler tiene propiedades muy importantes en teoría de números, algunas de las cuales se usarán más adelante, y que estamos en posición de probarlas, en el siguiente teorema se enuncian y prueban dichas propiedades básicas.

3.3.5 Teorema *Sea φ la función de Euler. Entonces*

(i) $\varphi(mn) = \varphi(n)\varphi(m)$ *si* $(m, n) = 1$ (propiedad multiplicativa).

(ii) $\varphi(p^e) = p^{e-1}(p-1)$, *p primo y* $e \geq 1$.

(iii) Si $n = \prod_{i=1}^{k} p_i^{e_i}$ *es la factorización de n como producto de primos, entonces* $\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$.

Demostración i) Se obtiene tomando cardinalidad en el isomorfismo $(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$.
ii) Se tiene que un entero k es primo relativo con $p^e \iff k$ es primo relativo con p. Los enteros entre 1 y p^e que no son primos relativos con p son precisamente de la forma ip con $i = 1, \ldots, p^{e-1}$. De lo cual la conclusión se obtiene.
iii) Aplicar las partes (i) y (ii). ■

El Ejercicio 2 página 40, afirma que si un grupo abeliano finito G tiene la propiedad que la ecuación $x^n = e$ tiene a lo más n soluciones para todo $n \leq |G|$, entonces G es cíclico. Una consecuencia de gran importancia es el siguiente teorema.

3.3.6 Teorema *Sea K un campo,entonces todo subgrupo finito de $K^* = K \setminus \{0\}$ es cíclico. En particular si $|K| < +\infty$, K^* es cíclico.*

Demostración. En todo campo la ecuación $x^n = 1$ tiene a lo más n soluciones[1], en particular si $G \leq K^*$ con $|G| < +\infty$, $x^n = 1$ tiene a lo más n soluciones para todo $n \leq |G|$. La conclusión se obtiene del ejercicio citado antes. ■

3.3.1 Corolario $(\mathbb{Z}/p\,\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\,\mathbb{Z}$ *con p primo.*

[1]Una propiedad importante de los polinomios con coeficientes en un campo establece: si α es raíz de un polinomio, entonces $x - \alpha$ lo divide.

Demostración. Como p es primo, entonces $\mathbb{Z}/p\,\mathbb{Z}$ es un campo con p elementos, por lo tanto $(\mathbb{Z}/p\,\mathbb{Z})^*$ es un grupo cíclico con $p-1$ elementos. ■

3.3.2 Corolario $\text{Aut}\,(\mathbb{Z}/p\,\mathbb{Z}) \cong \mathbb{Z}/(p-1)\,\mathbb{Z}$. ■

El Teorema 3.3.3 describe $\text{Aut}\,G$ con G cíclico de orden n, lo que haremos en seguida es describir la estructura de $(\mathbb{Z}/n\,\mathbb{Z})^*$ para tener una descripción completa de $\text{Aut}\,G$ en el caso cíclico.
El Teorema 3.3.8 determina la estructura de los grupos $(\mathbb{Z}/p_i^{e_i})^*$, en su demostración se requiere el siguiente resultado auxiliar.

3.3.7 Teorema *Sea p un número primo. Suponga que $a \equiv b \pmod{p^e}$ con $e \geq 1$, entonces*

$$a^{p^{n-e}} \equiv b^{p^{n-e}} \pmod{p^n} \qquad \forall\, n \geq e.$$

Demostración. Aplicaremos inducción sobre n. Si $n = e$ la conclusión es exactamente la hipótesis. Sea $k = n-e > 1$ y supongamos el resultado cierto para k, debiendo probarlo para $k+1$, lo cual se hará examinando la siguiente igualdad.

$$\begin{aligned} a^{p^{k+1}} - b^{p^{k+1}} &= (a^{p^k})^p - (b^{p^k})^p \\ &= (a^{p^k} - b^{p^k})(a^{p^k(p-1)} + \cdots + b^{p^k(p-1)}). \end{aligned}$$

La hipótesis sobre a y b implica $a \equiv b \pmod{p}$, de lo cual se obtiene

$$a^{p^k(p-1)} + \cdots + b^{p^k(p-1)} \equiv 0 \pmod{p},$$

entonces la hipótesis inductiva y la anterior congruencia implican

$$a^{p^{k+1}} - b^{p^{k+1}} = p^n l_1 p l_2$$

para algunos enteros l_1 y l_2, obteniendo finalmente

$$a^{p^{n+1-e}} \equiv b^{p^{n+1-e}} \pmod{p^{n+1}}). \qquad ■$$

3.3.8 Teorema *Sea p un primo, e un entero ≥ 1.*

i) Si $p = 2$ entonces

$$(\mathbb{Z}/2^e\,\mathbb{Z})^* \cong \begin{cases} \{1\} & si\ e = 1 \\ \mathbb{Z}/2\,\mathbb{Z} & si\ e = 2 \\ \mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/2^{e-2}\,\mathbb{Z} & si\ e \geq 3 \end{cases}$$

ii) Si p es impar entonces

$$(\mathbb{Z}/p^e\,\mathbb{Z})^* \cong \mathbb{Z}/(p-1)p^{e-1}\,\mathbb{Z}.$$

Demostración. i) Los casos $e = 1$ y $e = 2$ se obtienen directamente, por lo que supondremos $e \geq 3$. Mostraremos que

$$(\mathbb{Z}/2^e\,\mathbb{Z})^* = \langle -\overline{1}, \overline{5}\rangle \cong \mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/2^{e-2}\,\mathbb{Z}.$$

Para mostrar lo afirmado anteriormente iniciamos probando que $|\overline{5}| = 2^s \geq 2^{e-2}$, lo cual se obtiene si probamos que

$$5^{2^{e-3}} \equiv 1 + 2^{e-1} \text{ (mód } 2^e), \qquad \forall\, e \geq 3.$$

Pues si $s < e-2$, entonces $s \leq e-3$ y de esto $e-3 = s+l$. Sustituyendo este valor de $e-3$ en la congruencia anterior y usando que el orden de $\overline{5}$ es 2^s se tiene

$$5^{2^{e-3}} = (5^{2^s})^{2^l} \equiv 1 \text{ (mód } 2^e).$$

Usando la congruencia a probar se tendría que 2^e divide a 2^{e-1}, lo cual es imposible para $e > 1$.
Si $e = 3$ no hay nada que probar. Supongamos que la congruencia anterior se verifica para $e > 3$. Aplicando el Teorema 3.3.7 con $p = 2$, $a = 5^{2^{e-3}}$ y $b = 1 + 2^{e-1}$ se obtiene

$$\left(5^{2^{e-3}}\right)^2 = 5^{2^{e-2}} \equiv \left(1 + 2^{e-1}\right)^2 \text{ (mód } 2^{e+1}).$$

Un cálculo sencillo muestra que $(1 + 2^{e-1})^2 \equiv 1 + 2^e$ (mód 2^{e+1}), lo cual termina el paso inductivo. Por otro lado se tiene $|\overline{-1}| = 2$. Afirmamos que $\langle\overline{-1}\rangle \cap \langle\overline{5}\rangle = \{\overline{1}\}$, pues en caso contrario $5^k + 1$ es divisible por 2^e y como $e \geq 3$ entonces 4 divide a $5^k + 1$, lo cual es imposible debido a que 4 divide a $5^k - 1$. Con lo probado hasta aquí se tiene que $(\mathbb{Z}/2^e\,\mathbb{Z})^*$ contiene al subgrupo $\langle\overline{-1}\rangle\langle\overline{5}\rangle$ cuyo orden es $2 \cdot 2^s \geq 2 \cdot 2^{e-2} = 2^{e-1}$. También se tiene que $|(\mathbb{Z}/2^e\,\mathbb{Z})^*| = \varphi(2^e) = 2^{e-1}$, y esto implica

$$(\mathbb{Z}/2^e\,\mathbb{Z})^* = \langle\overline{-1}, \overline{5}\rangle \cong \mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/2^{e-2}\,\mathbb{Z}.$$

ii) Si $e = 1$, la conclusión es exactamente el Corolario 3.3.1. Supongamos $e \geq 2$. La conclusión *ii)* del Teorema 3.3.5 implica que $G = (\mathbb{Z}/p^e\,\mathbb{Z})^*$ tiene orden $(p-1)p^{e-1}$. La prueba concluirá si probamos que

$$G \cong \mathbb{Z}/(p-1)\,\mathbb{Z} \times \mathbb{Z}/p^{e-1}\,\mathbb{Z}.$$

Sea $f : (\mathbb{Z}/p^e\,\mathbb{Z})^* \to (\mathbb{Z}/p\,\mathbb{Z})^*$ el homomorfismo natural definido por $f(\bar{b}) = b+p\,\mathbb{Z}$. Es claro que f es sobre y su núcleo es $B = \{\bar{b} \in G \mid p \text{ divide a } b-1\}$. Por el Primer Teorema de Isomorfismo (Teorema 1.6.1), B es la p-parte de G, más aún, $G = B \times A$, con A un subgrupo de orden $p-1$. Note que el elemento $\overline{1+p} \in B$.
Afirmación: $B = \langle\overline{1+p}\rangle$. Puesto que $|B| = p^{e-1}$, es suficiente mostrar que

$$(1+p)^{p^{e-2}} \not\equiv 1 \text{ (mód } p^e),$$

pues la anterior no congruencia implicará que $|\overline{1+p}| = p^{e-1}$.
La no congruencia se probará por inducción, siendo inmediata para $e = 2$. Supongamos $e \geq 3$, entonces $n := e-2 \geq 1$. Como $1+p \equiv 1$ (mód p), el Teorema 3.3.7 implica $(1+p)^{p^{n-1}} \equiv 1$ (mód p^n) ó $(1+p)^{p^{e-3}} \equiv 1$ (mód p^{e-2}). Por hipótesis inductiva se tiene $(1+p)^{p^{e-3}} \not\equiv 1$ (mód p^{e-1}), por lo que $(1+p)^{p^{e-3}} = 1+kp^{e-2}$ con $(k,p) = 1$. Elevando a la p la anterior ecuación se obtiene

$$\begin{aligned}(1+p)^{p^{e-2}} &= \left(1+kp^{e-2}\right)^p \\ &= 1+pkp^{e-2}+\cdots+k^pp^{p(e-2)} \\ &\equiv 1+kp^{e-1} \text{ (mód } p^e).\end{aligned}$$

La condición sobre k implica $1+kp^{e-1} \not\equiv 1$ (mód p^e), de lo que se obtiene $(1+p)^{p^{e-2}} \not\equiv 1$ (mód p^e), probando lo afirmado. Por lo observado más antes, $G = A\times B$ con A un subgrupo de orden $p-1$. Por otro lado se tiene que $\dfrac{G}{B} = \dfrac{B\times A}{B} \cong A$, de donde se concluye

$$G \cong (\mathbb{Z}/p\,\mathbb{Z})^* \times \mathbb{Z}/p^{e-1}\,\mathbb{Z} \cong \mathbb{Z}/p^{e-1}(p-1)\,\mathbb{Z}. \quad \blacksquare$$

El teorema anterior tiene como corolario al siguiente resultado el cual es muy importante en teoría de números.

3.3.9 Teorema *Sea n un entero positivo, entonces $(\mathbb{Z}/n\,\mathbb{Z})^*$ es cíclico $\iff$ $n = 2, 4, p^e, 2p^e$ con $e \geq 1$ y p impar.*

Demostración. Si n tiene la forma indicada entonces el teorema anterior implica que $G = (\mathbb{Z}/n\,\mathbb{Z})^*$ es cíclico. Note que $(\mathbb{Z}/2p^e\,\mathbb{Z})^* \cong (\mathbb{Z}/p^e\,\mathbb{Z})^*$. El recíproco se obtiene notando que si $G = A \times B$ con A y B grupos abelianos de orden $2r$ y $2s$ respectivamente, entonces G no es cíclico pues para todo $(x,y) \in G$, $(x,y)^{2rs} = (1,1)$, es decir G no tiene elementos de orden

$|G| = 4rs$. Si n tiene dos factores primos impares, entonces el Teorema 3.3.4 implica que G tiene dos factores de orden par, por el comentario anterior G no es cíclico. Los restantes casos se tratan de manera análoga. ■
El Teorema 3.3.3 afirma que los automorfismos de un grupo cíclico, forman un grupo abeliano. El siguiente teorema caracteriza a los grupos abelianos con grupo de automorfismos abeliano.

3.3.10 Teorema *Sea G un grupo abeliano finito. Entonces* $\operatorname{Aut} G$ *es abeliano* $\iff$ *G es cíclico.*

Demostración. $\impliedby$ Teorema 3.3.3.
$\implies$ Como G es abeliano, entonces G tiene una descomposición canónica de la forma $G = C_1 \oplus \cdots \oplus C_k$, con C_i cíclico para todo $i = 1, \ldots, k$. Aplicaremos inducción sobre k. Lo supuesto sobre G garantiza que $k \geq 2$. Si $k = 2$ entonces $G = C_1 \oplus C_2$. Sean $\langle x \rangle = C_1, \langle y \rangle = C_2$ entonces los elementos de G se representan de manera única en la forma $ix + jy$, con $1 \leq i \leq |x|$ y $1 \leq j \leq |y|$. Definiendo f y g como:

$$f(ix + jy) := (i + j)x + jy, \quad g(ix + jy) := jx + iy,$$

se verifica que $f, g \in \operatorname{Aut} G$ (se prueba que f es inyectivo y g suprayectivo) y $f \circ g \neq g \circ f$, es decir, $\operatorname{Aut} G$ no es abeliano, contradiciendo la hipótesis sobre $\operatorname{Aut} G$. Supongamos que $k > 2$, entonces $G = C_1 \oplus C_2 \oplus C_3 \oplus \cdots \oplus C_k$. Mostraremos que $\operatorname{Aut}(C_1 \oplus C_2) \hookrightarrow \operatorname{Aut} G$, con lo que aplicando el caso $k = 2$ se concluirá que $\operatorname{Aut} G$ no es abeliano, contradiciendo nuevamente la hipótesis sobre $\operatorname{Aut} G$. Sea $f \in \operatorname{Aut}(C_1 \oplus C_2)$, f se extiende a un automorfismo de G como sigue

$$\overline{f}(c_1 + c_2 + \cdots + c_k) := f(c_1 + c_2) + c_3 + \cdots + c_k.$$

Con esto se ha mostrado lo que se quería. ■

3.3.1 Ejercicio *Sea G un grupo tal que* $\operatorname{Aut} G$ *es cíclico. ¿Puede ocurrir que G no sea abeliano? Sugerencia: revise el Teorema 3.3.1 y el Ejercicio 5 página 41.*

3.3.2 Ejercicio *Sea G un grupo abeliano finito tal que $|G| > 2$. Demuestre que* $|\operatorname{Aut} G|$ *es par.*

Concluya de los ejercicios anteriores que si G es un grupo finito, entonces $\operatorname{Aut} G$ no es cíclico de orden impar > 1.

3.3.3 Ejercicio *Sea G un grupo el cual contiene un subgrupo propio de índice ≤ 4. Demuestre que G no es simple.*

3.3.4 Ejercicio *Sea G un grupo abeliano de exponente k. Demuestre que $(\mathbb{Z}/k\,\mathbb{Z})^* \hookrightarrow \operatorname{Aut} G$. Sugerencia. Si $(a,k)=1$, la función $f_a : G \to G$ definida por $f_a(x) = x^a$ es un automorfismo de G.*

3.3.1 Problema *Sea G un grupo finito tal que $\operatorname{Aut} G$ es abeliano, ¿qué se puede decir de G?*

3.3.2 Problema *Dado un grupo finito G. ¿Cuáles son los grupos finitos que satisfacen $\operatorname{Aut} X = G$? Una referencia para estos problemas es: H.K. Iyer, Rocky Mountain Journal, vol. 9. 1979, páginas 653-670.*

3.3.1. Ejercicios

1. Sea G un grupo finito, $T \in \operatorname{Aut} G$ tal que $T(x) = x$ implica $x = e$. Demuestre que para todo $g \in G$ existe $x \in G$ con $g = x^{-1}T(x)$.

2. Sea G un grupo finito, $T \in \operatorname{Aut} G$. Si T satisface:

   a) $T(x) = x$ implica $x = e$

   b) $T^2 = id_G$.

   Demuestre que G es abeliano.

3. Sea G un grupo y $H \leq G$. Si para todo $f \in \operatorname{Aut} G$ se tiene que $f(H) \subseteq H$, H se dice característico.

   a) Para todo grupo G, $Z(G)$ es característico.

   b) Todo subgrupo normal de Sylow de G es característico.

   c) Si $K \triangleleft G$ y $(|K|, [G:K]) = 1$, entonces K es característico.

Capítulo 4

Grupos solubles y nilpotentes

En este último capítulo se considera una clase especial de grupos, los llamados grupos solubles. Estos grupos se relacionan estrechamente con problemas de solubilidad de ecuaciones polinomiales por radicales. Iniciamos haciendo explícitos algunos conceptos y terminología, entre estos el concepto de *subgrupo característico*, el cual en particular es normal.

4.1. Subgrupos característicos

4.1.1 Definición *Sea G un grupo, H y K subgrupos de G, $[H, K]$ denotará al subgrupo generado por $\{hkh^{-1}k^{-1} \mid h \in H, k \in K\}$. Note que si $H = K = G$, entonces $[H, K]$ es simplemente el subgrupo derivado de G.*

Aunque ya dimos la definición de subgrupo característico, dada su importancia, la hacemos explícita.

4.1.2 Definición *Sea G un grupo, $H \leq G$. Se dice que H es un* ***subgrupo característico*** *de G, denotado H $\operatorname{car} G$, si $f(H) \subseteq H$ para todo $f \in \operatorname{Aut} G$.*

4.1.1 Ejemplo

1. *Si G es un grupo y G' denota al subgrupo derivado de G, entonces G' es característico, pues dado f, automorfismo de G y $a, b \in G$, se tiene $f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1}$, por lo que $f(G') \subseteq G'$.*

2. *Si G es un grupo y $Z(G)$ denota al centro de G, entonces $Z(G)$ es característico, pues si $a \in Z(G)$, f es un automorfismo de G y $x \in G$, entonces existe $b \in G$ tal que $f(b) = x$, y de esto se obtiene $f(a)x =$*

$f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = xf(a)$, *probando que* $f(a) \in Z(G)$.

4.1.1 Observación Si H car G, entonces $H \lhd G$.

El siguiente resultado establece algunas propiedades elementales de subgrupos característicos.

4.1.1 Teorema *Sea G un grupo, H y K subgrupos de G.*

(i) *Si H* car *K y K* car *G, entonces H* car *G.*

(ii) *Si H* car *K y $K \lhd G$, entonces $H \lhd G$.*

(iii) *Si $H \lhd G$, entonces $f(H) \lhd G$ para todo $f \in \mathrm{Aut}\,(G)$.*

(iv) *Si $H \subseteq K$, H* car *G y K/H* car *G/H entonces K* car *G.*

Demostración. (i) Sea $f \in \mathrm{Aut}\,(G)$, como K car G entonces $f_{|K} \in \mathrm{Aut}\,(K)$; la hipótesis sobre H implica $f_{|K}(H) \subseteq H$, probando que H car G.
(ii) Dado $f_g \in \mathrm{Inn}\,G$, las hipótesis sobre H y K implican que $f_g(H) \subseteq H$, es decir $H \lhd G$.
(iii) Sean $f \in \mathrm{Aut}\,(G)$, $g \in G$ y $h \in H$. Mostraremos que $gf(h)g^{-1} \in f(H)$, lo cual se obtiene debido a que $g = f(x)$ para algún $x \in G$ y $xhx^{-1} \in H$.
(iv) Sea $f \in \mathrm{Aut}\,(G)$, lo supuesto sobre H implica que f induce un elemento $\overline{f} \in \mathrm{Aut}\,(G/H)$ definido por $\overline{f}(gH) = f(g)H$. La conclusión se obtiene invocando la hipótesis sobre K/H. ■

4.2. Grupos nilpotentes

Dado un grupo G, se define una sucesión de subgrupos como sigue:

$$L_1(G) = G,\ L_2(G) = [G, G], \ldots,\ L_i(G) = [L_{i-1}(G), G], \quad \forall\, i \in \mathbb{N}.$$

La sucesión antes definida tiene las siguientes propiedades

4.2.1 Teorema *Sea G un grupo, entonces:*

(i) *$L_i(G)$* car *G para todo i.*

(ii) $L_{i+1}(G) \subseteq L_i(G)$ *y* $L_i(G)/L_{i+1}(G) \subseteq Z(G/L_{i+1}(G))$ *para todo* i.

Demostración. (i) Aplicaremos inducción sobre i. Para $i = 1, 2$ es claro pues $L_1(G) = G$ y $L_2(G) = G'$, los cuales son característicos. En general se verifica fácilmente lo siguiente. Si $f : G \to G$ es un homomorfismo y H y K son subgrupos de G, entonces $f([H, K]) = [f(H), f(K)]$, en particular esto se cumple si $f \in \mathrm{Aut}\,(G)$ y $H = L_i(G)$.
(ii) La primera parte se obtiene notando que $L_i(G)$ es un subgrupo normal de G, y de esto se concluye que $[L_i(G), G] \subseteq L_i(G)$, es decir, $L_{i+1}(G) \subseteq L_i(G)$. La segunda parte se deduce de la primera y del hecho general siguiente, el cual es inmediato. Si H y K son subgrupos normales de G entonces $H/K \subseteq Z(G/K) \iff [H, G] \subseteq K$. ■

4.2.1 Definición *Un grupo G se dice* ***nilpotente*** *si existe $m \in \mathbb{N}$ tal que $L_m(G) = \{e\}$. Si m es el menor entero que satisface $L_m = \{e\}$, $m - 1$ se llama el índice de nilpotencia de G.*

4.2.1 Observación G es abeliano $\iff$ $L_2(G) = G' = \{e\}$, es decir, los grupos abelianos no triviales son de índice de nilpotencia uno.

En conexión con la sucesión $L_i(G)$, la cual es decreciente, hay otra, la llamada serie central definida como sigue: $Z_0(G) = \{e\}$, $Z_1(G) = Z(G)$, y en general para $i > 1$, $Z_i(G)$ es el subgrupo de G correspondiente a $Z(G/Z_{i-1}(G))$, bajo el teorema de la correspondencia. Aplicando inducción sobre i y el Teorema 4.1.1 *(iv)* se obtiene que $Z_i(G)$ car G para todo i. El siguiente resultado expresa la relación entre las sucesiones que se han definido y proporciona otra definición de grupo nilpotente.

4.2.2 Teorema *Un grupo G es nilpotente $\iff$ $Z_m(G) = G$ para algún m. Si G tiene índice de nilpotencia $m - 1$, éste es el menor entero tal que $Z_{m-1}(G) = G$.*

Demostración. $\Longleftarrow$ Supongamos que G tiene índice de nilpotencia $m - 1$. Mostraremos que $L_{m-r} \subseteq Z_r$ para todo $r \in [\![0, m-1]\!]$, en particular $L_1 = G \subseteq Z_{m-1}$ de lo cual la conclusión se obtendrá. La prueba es por inducción sobre r. Si $r = 0$, entonces $L_m = \{e\} = Z_0$. Supongamos que $L_{m-i} \subseteq Z_i$ y probemos que $L_{m-i-1} \subseteq Z_{i+1}$. El Teorema 4.2.1 *(ii)* garantiza que $L_{m-i-1}/L_{m-i} \subseteq Z(G/L_{m-i})$. En general se tiene el siguiente hecho.

4.2.1 Hecho *Sea $f : G \to G_1$ un epimorfismo, entonces $f(Z(G)) \subseteq Z(G_1)$.*

Demostración. (del Hecho) Sea $f(x) \in G_1$, con $x \in Z(G)$. Dado $y \in G_1$ existe $b \in G$ tal que $y = f(b)$, por lo tanto $yf(x) = f(b)f(x) = f(bx) = f(xb) = f(x)f(b) = f(x)y$. Una de las igualdades intermedias se tiene por pertenecer x al centro de G. ■
(Regreso a la prueba del teorema) Por hipótesis $L_{m-i} \subseteq Z_i$. Aplicando el Tercer Teorema de Isomorfismo (Teorema 1.6.4) se obtiene

$$\frac{G}{Z_i} \cong \frac{G/L_{m-i}}{Z_i/L_{m-i}},$$

de hecho el isomorfismo proviene de la proyección

$$\pi : \frac{G}{L_{m-i}} \to \frac{G}{Z_i}, \qquad \pi(gL_{m-i}) = gZ_i.$$

La proyección π es obviamente un epimorfismo, entonces se tiene la hipótesis necesaria para poder aplicar la Observación 4.2.1, es decir, $\pi(Z(G/L_{m-i})) \subseteq Z(G/Z_i)$. Como se notó antes, $L_{m-(i+1)}/L_{m-i} \subseteq Z(G/L_{m-i})$ y de esto $\pi(L_{m-(i+1)}/L_{m-i}) = L_{m-(i+1)}Z_i/Z_i \subseteq Z(G/Z_i) = Z_{i+1}/Z_i$. Probando la implicación.
$\Longleftarrow$ Supongamos que $Z_m(G) = G$ para algún m. Se probará que $L_{r+1} \subseteq Z_{m-r}$ para todo $r \in [\![0, m]\!]$, en particular $L_{m+1} \subseteq Z_0 = \{e\}$, lo que terminará la prueba. Aplicaremos inducción sobre r. Si $r = 0$, $L_1 = G = Z_m$. Supongamos que $L_i \subseteq Z_{m+1-i}$. Por definición de L_{i+1} y de Z_{m+1-i} se tiene $L_{i+1} = [L_i, G] \subseteq [Z_{m+1-i}, G]$ y $Z_{m+1-i}/Z_{m-i} \subseteq Z(G/Z_{m-i})$; esto último implica $[Z_{m+1-i}, G] \subseteq Z_{m-i}$, concluyendo que $L_{i+1} \subseteq Z_{m-i}$. ■

El siguiente resultado expresa algunas propiedades de grupos nilpotentes.

4.2.3 Teorema *(i) Los subgrupos e imágenes homomorfas de grupos nilpotentes son nilpotentes.*

(ii) El producto directo de grupos nilpotentes es nilpotente.

(iii) Los p-grupos finitos son nilpotentes.

Demostración. (i) En general se tiene que $H \leq G$ implica $L_i(H) \subseteq L_i(G)$, por lo tanto, si G es nilpotente, H es nilpotente. Supongamos que $H \lhd G$, entonces $Z(G)H/H \leq Z(G/H)$ y por inducción se deduce que la imagen de $Z_i(G)$ está contenida en $Z_i(G/H)$, por lo que $Z_m(G/H) = G/H$ para algún m.

(ii) Aplicando inducción sobre el número de factores es suficiente probar que si A y B son grupos nilpotentes, entonces $A \times B$ es nilpotente. Note que $Z(A \times B) = Z(A) \times Z(B)$. El resultado se obtiene aplicando el Teorema 1.7.2.
(iii) La conclusión se obtiene inmediatamente recordando que el centro de un p-grupo finito es no trivial. ■

4.2.4 Teorema *Sea G un grupo nilpotente y H un subgrupo propio, entonces $H \neq N_G(H)$.*

Demostración. Sea n el mayor entero tal que $Z_n \subseteq H$ y Z_{n+1} no está contenido en H, tal entero existe por ser $Z_m = G$ para algún m. La elección de n implica $Z_n \neq Z_{n+1}$. Por otro lado tenemos $[Z_{n+1}, G] \subseteq Z_n \subseteq H$, pues $Z_{n+1}/Z_n = Z(G/Z_n)$, por lo tanto $[Z_{n+1}, H] \subset [Z_{n+1}, G] \subseteq H$. De la definición de $N_G(H)$ y la última inclusión de conjuntos se obtiene $Z_{n+1} \subseteq N_G(H)$. ■

El siguiente resultado establece una equivalencia para grupos nilpotentes finitos, la cual resulta ser de gran utilidad en las aplicaciones.

4.2.5 Teorema *Sea G un grupo finito, entonces G es nilpotente $\iff$ G es isomorfo al producto directo de sus subgrupos de Sylow.*

Demostración. $\Longleftarrow$ Se obtiene combinando las partes *(ii)* y *(iii)* del Teorema 4.2.3.
$\Longrightarrow$ Es suficiente mostrar que los p-subgrupos de Sylow de G son normales, lo cual se tiene del Teorema 4.2.4 y del Ejercicio 1, página 70. ■

4.3. Grupos solubles

4.3.1 Definición *Un grupo G se dice **soluble**, si existe una sucesión de subgrupos*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

tal que $G_{i+1} \lhd G_i$ y G_i/G_{i+1} es abeliano para todo i. La sucesión anterior se llama una sucesión soluble.

4.3.1 Teorema *(i) Imágenes homomorfas y subgrupos de grupos solubles son solubles.*

(ii) Sea $H \lhd G$ tal que H y G/H son solubles, entonces G es soluble.

(iii) El producto directo de grupos es soluble $\iff$ *cada factor lo es.*

(iv) Los grupos nilpotentes son solubles.

(v) Si G *es soluble no trivial, entonces* $G' \neq G$.

Demostración. i) Sea $H \leq G$ con G soluble, entonces existe una sucesión

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

que satisface la Definición 4.3.1.
Afirmación: la sucesión

$$H = H \cap G_0 \supset H \cap G_1 \supset \cdots \supset H \cap G_n = \{e\}$$

también satisface la definición citada. La condición $G_{i+1} \lhd G_i$ implica

$$H \cap G_{i+1} \lhd H \cap G_i, \qquad \forall\, i = 1, \ldots, n-1.$$

Aplicando el Segundo Teorema de Isomorfismo, Teorema 1.6.3, página 42, se obtiene

$$\frac{H \cap G_i}{H \cap G_{i+1}} = \frac{H \cap G_i}{(H \cap G_i) \cap G_{i+1}} \cong \frac{G_{i+1}(H \cap G_i)}{G_{i+1}} \subseteq \frac{G_i}{G_{i+1}}.$$

Esto último y la hipótesis sobre G_i/G_{i+1} implican que $H \cap G_i/(H \cap G_{i+1})$ es abeliano, probando lo que se afirmó. Sea G soluble y $H \lhd G$, mostraremos que G/H es soluble. Sea

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

una sucesión soluble. Las condiciones $H \lhd G$ y $G_{i+1} \lhd G_i$ implican que $G = HG_0 \supset \cdots \supset HG_n = H \supset \{e\}$ satisface $(HG_{i+1})/H \lhd (HG_i)/H$ para todo i, pues dado $Hg_i(Hg_{i+1})Hg_i^{-1} = Hg_1g_{i+1}g_i^{-1} \in (HG_{i+1})/H$, $g_i \in G_i$, $g_{i+1} \in G_{i+1}$. Consideremos la sucesión de subgrupos de G/H:

$$\frac{G}{H} = \frac{HG_0}{H} \supset \cdots \supset \frac{HG_n}{H} = \{e\}.$$

Aplicando el Tercer Teorema de Isomorfismo, Teorema 1.6.4 página 43, a dos términos consecutivos de la sucesión anterior se obtiene

$$\frac{HG_i/H}{HG_{i+1}/H} \cong \frac{HG_i}{HG_{i+1}} = \frac{(HG_{i+1})G_i}{HG_{i+1}}. \qquad (*)$$

Por otro lado se tiene que $G_{i+1} \subseteq G_i \cap HG_{i+1} \subseteq G_i$. Aplicando nuevamente el Tercer Teorema de Isomorfismo obtenemos

$$\frac{G_i/G_{i+1}}{(G_i \cap HG_{i+1})/G_{i+1}} \cong \frac{G_i}{G_i \cap HG_{i+1}} \cong \frac{(HG_{i+1})G_i}{HG_{i+1}}. \qquad (**)$$

El último isomorfismo en la cadena anterior de isomorfismos se debe al Segundo Teorema de Isomorfismo, Teorema 1.6.3, página 42. Combinando $(*)$ y $(**)$ se concluye que el primer miembro de $(*)$ es abeliano, probando que G/H es soluble.
(ii) Si H y G/H son solubles, el Teorema de la correspondencia, Teorema 1.6.5, página 44, garantiza que existen subgrupos $G = G_0 \supset G_1 \supset \cdots \supset H$ tales que $G_{i+1} \lhd G_i$ y G_i/G_{i+1} es abeliano. La hipótesis sobre H completa la anterior sucesión a una soluble.
(iii) $\Longrightarrow$ Cada factor directo es isomorfo a un subgrupo de G. Aplicando la parte *(i)* del teorema se concluye que los factores son solubles.
$\Longleftarrow$ Se obtiene por inducción sobre el número de factores aplicando la parte *(ii)* del teorema, para lo cual hay que notar que si $G = G_1 \times \cdots \times G_n$ entonces $G/G_i \cong G_1 \times \cdots G_{i-1} \times G_{i+1} \times \cdots \times G_n$.
(iv) Si G es nilpotente, el Teorema 4.2.1, página 101 implica que la sucesión $\{L_i(G)\}$ es una sucesión soluble.
(v) Como G es soluble no trivial, existe un subgrupo propio G_1 tal que G/G_1 es abeliano y de esto se concluye que $G' \subseteq G_1$ por lo que $G \neq G'$. ■

Dado un grupo G se definen los conmutadores superiores de G como sigue $G' := [G, G]$, $G'' := [G', G']$, en general $G^{(i+1)} := [G^{(i)}, G^{(i)}]$ para todo $i \in \mathbb{N}$. El siguiente teorema proporciona una definición de grupo soluble en términos de los conmutadores de un grupo.

4.3.2 Teorema *Sea G un grupo, entonces G es soluble $\iff$ $G^{(n)} = \{e\}$ para algún n.*

Demostración. $\Longrightarrow$ Sea $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$ una sucesión soluble.
Afirmación. $G_i \supseteq G^{(i)}$ para todo i, en particular $G^{(n)} = \{e\}$. Aplicaremos inducción sobre i. Para $i = 0$ es claro. Supongamos que $G_i \supseteq G^{(i)}$, entonces $G^{(i+1)} := [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] = G_i'$. Por hipótesis G_i/G_{i+1} es abeliano, por lo tanto $G_{(i+1)} \supseteq G_i' \supseteq G^{(i+1)}$, concluyendo la prueba de lo afirmado.
$\Longleftarrow$ Los $G^{(i)}$'s constituyen una sucesión soluble, pues $G^{(i)}$ car G para todo i y $G^{(i)}/G^{(i+1)}$ es abeliano. ■

4.3.3 Teorema *Sea $n \geq 5$, $A_n \leq S_n$ el subgrupo alternante. Entonces $A_n = A_n'$.*

Demostración. Es suficiente mostrar que todo 3-ciclo es un conmutador, pues A_n es generado por 3-ciclos. Sea $(i\,j\,k\,)$ un 3-ciclo, es directo verificar que $(i\,j\,k\,)^{-1} = (k\,j\,i\,)$. Como $n \geq 5$, existen $l, m \in [\![1, n]\!] \setminus \{i, j, k\}$. Entonces

$$\begin{aligned}
[(i\,j\,k),\,(j\,k)(l\,m)] &= (i\,j\,k)(j\,k)(l\,m)(i\,j\,k)^{-1}\,[(j\,k)(l\,m)]^{-1} \\
&= (i\,j\,k)(j\,k)(l\,m)(k\,j\,i)(j\,k)(l\,m) \\
&= (i\,j\,k)(j\,k)(k\,j\,i)(j\,k) \\
&= (k\,j\,i) \\
&= (i\,j\,k)^{-1}.
\end{aligned}$$

La tercera igualdad se debe a que $(l\,m)$ es de orden 2 y conmuta con los ciclos ajenos a éste. En general se tiene $[x, y]^{-1} = [y, x]$, por lo tanto $(i\,j\,k) \in A_n'$. ■

4.3.1 Corolario *S_n no es soluble para todo $n \geq 5$.*

Demostración. Si S_n es soluble, entonces A_n también lo es, Teorema 4.3.1 *(i)*, página 104, entonces $A_n' \neq A_n$, Teorema 4.3.1 *(v)*, contradiciendo lo establecido en el Teorema 4.3.3. ■

4.3.4 Teorema *El subgrupo alternante A_n es simple para todo $n \geq 5$.*

Demostración. Primero daremos una prueba del Teorema 4.3.4 para el caso $n = 5$, después presentamos la prueba del caso general. Sea H un subgrupo normal maximal de A_5. El Teorema 4.3.3 y lo supuesto sobre H implican que A_5/H es simple y no abeliano de orden ≤ 60. Aplicando el Ejercicio 19, página 71, se tiene que $|A_5/H| = 60$, de lo que se concluye $H = \{e\}$, probando que A_n es simple. En la prueba del teorema se usará el siguiente:

4.3.1 Hecho *Si $n \geq 5$ entonces todos los 3-ciclos son conjugados en A_n.*

Demostración. (del hecho) Sea (ijk) un 3-ciclo, por el Teorema 2.1.9, página 60, existe $\sigma \in S_n$ tal que $(ijk) = \sigma(123)\sigma^{-1}$. Si $\sigma \in A_n$ hemos terminado, de otra forma defina $\tau = \sigma(45)$. Como σ es impar y (45) también, entonces $\tau \in A_n$. Uno verifica que $\tau(123)\tau^{-1} = (ijk)$. ■

Regreso a la prueba del Teorema 4.3.4. El Ejercicio 5, página 62, garantiza que A_n está generado por 3-ciclos. Por el hecho anterior, es suficiente mostrar

que si $H \neq \{e\}$ es un subgrupo normal en A_n, entonces H contiene un 3-ciclo. Como $|H| > 1$, entonces existe un primo p que divide al orden de H y por el Teorema de Cauchy, Teorema 2.3.1, página 66, existe $\sigma \in H$ tal que $|\sigma| = p$, entonces σ es producto de$p$-ciclos, digamos que el número de p-ciclos es k.
CASO I $p > 3$. Sea $\sigma = (a_1 a_2 \cdots a_p) \cdots$. Note que $(a_1 a_2 \cdots a_p)^{-1} = (a_1 a_p \cdots a_2)$, entonces se tiene por un cálculo directo, $\sigma(a_1 a_2 a_3)\sigma^{-1}(a_1 a_3 a_2) = (a_1 a_4 a_2) \in H$.
CASO II $p = 3$ y $k > 1$ (en el caso $k = 1$ no hay trabajo que realizar, pues σ es un 3-ciclo). Sea $\sigma = (a_1 a_2 a_3)(a_4 a_5 a_6) \cdots$ entonces se verifica que $\sigma(a_1 a_2 a_4)\sigma^{-1}(a_1 a_4 a_2) = (a_1 a_4 a_3 a_5 a_2) \in H$ y se ha regresado al caso I.
CASO III $p = 2$.

III(a) $k = 1$, digamos que $\sigma = (a_1 a_2)$, entonces $\sigma(a_1 a_2 a_3)\sigma^{-1}(a_1 a_3 a_2) = (a_1 a_2 a_3) \in H$.

III(b) $k = 2$, $\sigma = (a_1 a_2)(a_3 a_4)$, entonces $\sigma(a_1 a_2 a_5)\sigma^{-1}(a_1 a_5 a_2) = (a_1 a_2 a_3) \in H$.

III(c) $k > 2$, $\sigma = (a_1 a_2)(a_3 a_4)(a_5 a_6) \cdots$. Un cálculo directo demuestra que $\sigma(a_1 a_2 a_5)\sigma^{-1}(a_1 a_5 a_2) = (a_1 a_5)(a_2 a_6) = \sigma_1 \in H$ y se argumenta con σ_1 como en III(b). ■

4.3.5 Teorema (Extensión del Teorema 2.1.10) *Si $n \geq 5$ y $1 < k < n$, entonces A_n no contiene subgrupos de índice k.*

Demostración. Aplicar la técnica del Teorema 2.1.2 y el Teorema 4.3.4. ■

4.3.6 Teorema (Versión fuerte del Teorema 1.5.3) *Sea G un grupo finito.*
Entonces G es cíclico $\iff$ para cada divisor k, de $|G|$ existe a lo más un subgrupo de orden k.

Demostración. $(\Longrightarrow)$ La misma prueba que en el Teorema 1.5.3.
$(\Longleftarrow)$ La hipótesis sobre G y los teoremas de Sylow implican que los p-subgrupos de Sylow de G son normales, por lo tanto G es nilpotente, Teorema 4.2.5, página 103. Para terminar la prueba es suficiente mostrar que los subgrupos de Sylow de G son cíclicos, es decir el problema se ha reducido a probar que si un p-grupo P tiene a lo más un subgrupo de orden p^n para cada n, entonces P es cíclico. Sea $|P| = p^k$. Aplicaremos inducción sobre k, siendo

claro para $k = 1$. Supongamos que el resultado es cierto para todos los p-grupos con cardinalidad $< |P|$. Como P es un p-grupo, entonces el centro de P, $Z(P)$ tiene cardinalidad al menos p, de lo cual se obtiene $|P/Z(P)| < |P|$. El Teorema de la Correspondencia, Teorema 1.6.5, página 44, implica que $P/Z(P)$ contiene a lo más un subgrupo de orden p^n para cada n, por lo tanto la hipótesis inductiva implica que $P/Z(P)$ es cíclico, lo cual a la vez implica que P es abeliano. La conclusión final se obtiene aplicando el Teorema 3.1.9, página 83. ■

Nota Final. Durante la elaboración de este texto se consultaron varias referencias, entre las que se encuentran: [4], [5], [7], [9], [10], [11], [12], [13], [14], [15], [17], [18], [19], [20], [21], [23], [24]. En ellas, el lector interesado encontrará otros enfoques y discusiones mas amplias de los temas tratados aquí.

4.3.1. Ejercicios

1. Sea G un grupo de orden p^2q, con p y q primos. Demuestre que G es soluble. **Nota:** este resultado se cumple en una situación más general. Si $|G| = p^n q^m$ entonces G es soluble (Teorema de Burnside).

2. Sea $n \neq 4$, entonces S_n no tiene subgrupos de índice k, con $2 < k < n$. Sugerencia: use los Teoremas 2.1.2, 4.3.4 y el hecho que $Z(S_n) = \{e\}$ para $n \geq 3$.

3. Pruebe el siguiente caso especial del teorema de Burnside: Si $|G| = pq^n$ y $p < q$ entonces G es soluble.

4. Sea G un grupo finito no trivial. Si G es soluble, entonces G contiene un subgrupo normal abeliano $H \neq \{e\}$; si G no es soluble, entonces G contiene un subgrupo normal $H \neq \{e\}$ tal que $H = H'$.

5. Sea G un grupo finito. Entonces G es nilpotente $\iff$ todo subgrupo maximal es normal.

6. Demuestre que los siguientes enunciados son equivalentes.

   a) Todo grupo de orden impar es soluble.

   b) Todo grupo simple finito tiene orden par.

   Nota: El primer inciso fue probado por Feit y Thompson en 1963.

7. Sea G un grupo nilpotente de orden n y m un divisor de n. Demuestre que G contiene un subgrupo de orden m. ¿Es cierto el resultado para grupos solubles?

8. Sea G nilpotente. Demuestre que $|Z(G)| > 1$.

Bibliografía

[1] F. Barrera, O. Becerra, A. Clemente, and J. Serrano. Un método matricial para calcular el máximo común divisor. *Memorias del 7o. Coloquio de Investigación ESFM-IPN*, **1**:269–275, (1998).

[2] R. Bourgne and J.-P Azra. *Ecrits et Mémoires Mathématiques d'variste Galois*. Gauthier-Villars, Paris, France, 1962.

[3] D. M. Bressoud. *Factorization and Primality Testing*. Springer-Verlag, New York USA, first edition, 1989.

[4] K. David. Using commutators to prove A_5 is simple. *Am. Math. Monthly*, **8**, (1987).

[5] J. D. Dixon. *Problems in Group Theory*. Dover Publications Inc., New York USA, first edition, 1973.

[6] H. M. Edwards. *Galois Theory*. Springer-Verlag, New York USA, corrected third printing edition, 1998.

[7] D. Gorenstein. *Finite Groups*. Chelsea Publishing Company, New York USA, second edition, 1980.

[8] L.C. Grove. *Algebra*. Academic Press Inc., New York–London, first edition, 1983.

[9] M. Hall Jr. *Teoría de los grupos*. Editorial Trillas, México, 1973.

[10] J. T. Hallet and K. A. Hirsch. Torsion-free groups having finite automorphism groups. *J. of Algebra*, **2**, (1965).

[11] J. Hausen. The hypo residuum of the automorphism group of an abelian p-group. *Pacific J. of Math.*, **35**, (1970).

[12] I.N. Herstein. *Topics in Algebra*. John Wiley & Sons Inc., New York, second edition, 1975.

[13] T. Hungerford. *Algebra*. Springer-Verlag, New York, third edition, 1984.

[14] S. Lang. *Algebra*. Addison-Wesley Publishing Co., New York, first edition, 1969.

[15] H. Leptin. *Math. S.*, **73**:235–253, (1960).

[16] G. Mazzola. *The Topos of Music*. Birkhäuser , Germany, first edition, 2002.

[17] G.A. Miller. Determination of all the groups of order 64. *Am. J. Math.*, **52**, (1930).

[18] J. J. Rotman. *An Introduction to the Theory of Groups*. Springer-Verlag, New York, fourth edition, 1995.

[19] H.M. Stark. *An Introduction to Number Theory*. The MIT Press Cambridge, Massachusetts and London, second edition, 1979.

[20] L. Steen. The science of patterns. *Science*, **240**:611–616, (1988).

[21] M. Suzuki. *Group Theory*. Springer-Verlag, New York, first edition, 1986.

[22] J.V. Uspensky. *Theory of Equations*. Mcgraw-Hill Book Company, New York USA, first edition, 1948.

[23] H. De Vries and A. B. Miranda Miller. Groups with a small number of automorphisms. *Math. Zeitschr Bd.*, **68**, (1958).

[24] H. Wussing. *The Genesis of the Abstract Group Concept*. The MIT Press Cambridge, Massachusetts, London England, first edition, 1984.

Índice alfabético