Universidad Mayor San Andrés
Facultad de Ciencias Puras y Naturales
Carrera de Matemática

Probabilidad de conmutatividad de grupos finitos

Presentado para la obtención del Título de Licenciado en Matemática

Autor

Univ. Cristhian Torres Apaza

Tutor

Lic. Ramiro J. Choque Canaza

La Paz - Bolivia

2023

Dedicatoria

Este proyecto de grado la dedico con todo mi cariño para mi madre Francisca Apaza Vargas y mi padre Flavio Torres Gironda y toda mi familia, quienes han puesto toda su confianza en mí para seguir creciendo profesional y académicamente.

Agradecimiento

Quiero expresar mi sincero agradecimiento, en primer lugar, a Dios por brindarme salud, fortaleza y capacidad; también hago un extenso reconocimiento a todos los docentes de la Carrera de Matemática, quienes me han dado las pautas para mi formación profesional y en particular a mi tutor Ramiro J. Choque Canaza.

Resumen

El estudio de la teoría de grupos, subgrupos, grupos cocientes y homomorfismos entre grupos ya sean finitos o infinitos es un área amplia y rica en teoría. El trabajo desarrollado a continuación toma como campo de estudio los grupos finitos y lo relaciona con el tema de probabilidad; donde estudiamos el número de casos favorables a un evento determinado, entre el número de casos posibles. Una pregunta bastante natural es: ¿Cuál es la probabilidad de que dos elementos tomados al azar de un grupo finito conmuten? Partiendo de esta cuestión analizaremos la *probabilidad de conmutatividad* o *grado de conmutatividad* de grupos específicos como ser el grupo Diedrico, entre otros, que desarrollaremos en el primer capítulo. Luego en el segundo capítulo de manera general, determinamos una formula mediante la relación de equivalencia dada por la conjugación, y su número de clases de equivalencia; además generamos propiedades para grupos específicos como ser el grado de conmutatividad de subgrupos, grado de conmutatividad de un producto cartesiano, entre otros. Este segundo mencionado nos servirá para determinar más grados de conmutatividad. En el tercer capítulo determinaremos cotas, pues la probabilidad que suceda un hecho determinado está ubicada en el intervalo $(0, 1]$; en nuestro caso, 1 es el grado de conmutatividad de grupos abelianos, y por el contrario, mostraremos que se puede hallar grupos cuyos grados de conmutatividad se acercan tanto a 0 como queramos. En cuanto a las cotas, determinaremos la cota superior $5/8$ como un límite para grupos no abelianos en general; también analizaremos las p-cotas, que es una relación entre números primos y el grado de

conmutatividad de un grupo dado, hallando cotas superiores e inferiores generadas por números primos. Por último, en el cuarto capítulo, desarrollaremos la probabilidad de conmutatividad de los grupos nilpotentes y los grupos solubles que son un caso especial pues son casi abelianos, determinaremos que tan conmutativos pueden ser.

Introducción

En un grupo no abeliano o, más generalmente, en una estructura algebraica no conmutativa, tiene sentido calcular la probabilidad de que dos elementos conmuten. Este problema fue abordado por primera vez en 1968 por Erdös y Turan [1] donde introdujeron el concepto de grado de conmutatividad como la probabilidad de que un elemento arbitrario x, en un grupo finito G, conmute con otro elemento arbitrario y en G. Después de eso, se ha desarrollado muchos estudios para determinar algunas cotas para este grado. Por ejemplo, Gustafson [2] y MacHale [6] demostraron independientemente en 1974 que para un grupo finito no abeliano G, el grado de conmutatividad $P(G) \leq 5/8$. Este concepto grado de conmutatividad se utiliza para determinar qué tanto de conmutatividad posee un grupo finito. La probabilidad de conmutatividad se puede obtener desarrollando una tabla de conmutatividad, por las clases de conjugación y utilizando centralizadores. Encontrar el grado de conmutatividad de un grupo finito es equivalente a encontrar el número de clases de conjugación del grupo o encontrar el número de caracteres irreducibles del grupo. Esto relaciona el grado de conmutatividad con muchas áreas de la teoría de grupos; hay muchas preguntas, y una larga historia de resultados, concernientes a la relación entre los caracteres irreducibles de un grupo y las propiedades teóricas de grupo, estudiada en la teoría de representación de grupos.

El presente proyecto de grado se centra en el campo de las matemáticas llamado teoría de grupos. Más específicamente, estudiamos la conmutatividad de

pares de elementos en grupos particulares y las probabilidades asociadas con ellos. Desarrollamos esta teoría en secciones generales y específicas. El primer capítulo contiene la definición y el cálculo del grado de conmutatividad de algunos grupos específicos. En el segundo capítulo, desarrollamos las propiedades generales del grado de probabilidad y su relación con las operaciones de los grupos; también desarrollamos el grado de conmutatividad de subgrupos y otras propiedades. El tercer capítulo está dedicado al estudio de las cotas del grado de conmutatividad de p-grupos y otros. El cuarto capítulo es el estudio del grado de probabilidad de grupos específicos como son los grupos nilpotentes y los grupos solubles. El trabajo también se centra principalmente en los grupos diédricos. El trabajo se presenta de una manera que permita al lector obtener una mejor comprensión de la teoría involucrada. En un curso regular de la teoría de grupos, se desarrolla las propiedades generales de los grupos, y la teoría de grado de conmutatividad de grupos es un tema de profundización y más en su aplicación.

Contenido

Capítulo 1

Grado de conmutatividad

1.1 Introducción

1.1.1 Medida

- Por *espacio medible* entendemos un par ordenado (Ω, B) que consta de un conjunto Ω y un σ -álgebra B de subconjuntos de Ω. Un subconjunto A de Ω se llama *medible* si $A \in B$.

- Una *medida* μ en un espacio medible (Ω, B) es una función $\mu : B \to [0, \infty]$ que satisface:

$$\mu(\phi) = 0$$
$$\mu(\bigcup_{i}^{\infty} E_i) = \sum_{i}^{\infty} \mu(E_i)$$

  para cualquier sucesión $\{E_i\}$ de conjuntos medibles disjuntos, es decir $E_i \cap E_j = \emptyset$, $E_i \in B$, $i \neq j$.

- (Ω, B, μ) se llama *espacio de medida*.

1.1.2 Medida de probabilidad

Sea (Ω, B, P) un espacio de probabilidad, donde Ω es denominado espacio muestral, B es un σ-álgebra de los subconjuntos de Ω y P es una *medida de probabilidad* la cual satisface:

1. $0 \leq P(E) \leq 1$, para $E \in B$
2. $P(\bigcup_i^\infty E_i) = \sum_i^\infty P(E_i)$, $E_i \cap E_j = \emptyset$, $E_i \in B$, $i \neq j$.
3. $P(\Omega) = 1$
4. $P(\emptyset) = 0$

Es inmediato verificar que, si $E, F \subset \Omega$, entonces $P(E^c) = 1 - P(E)$, $P(\emptyset) = 0$ y $P(E - F) = P(E) - P(E \cap F)$. Por el principio de inclusión y exclusión, $P(E \cup F) = P(E) + P(F) - P(E \cap F)$. Cuando $P(E) = 0$ decimos que el evento E es totalmente improbable y si $P(E) = 1$ significa que el evento E siempre ocurre. Como $P(E)$ está entre 0 y 1, el evento E presenta diferentes grados de ocurrencia.

Para el estudio que se desarrollará en el presente trabajo nuestro espacio muestral Ω sera un grupo G finito, y P sera una medida de probabilidad. Como calculamos la probabilidad en grupos finitos, la medida empleada será la medida del conteo (la cardinalidad de un conjunto).

En 1968 Erdös y Turán [1], investigaron algunos aspectos estadísticos de la teoría de grupos. Luego, en 1973 Gustafson [2], continuó con el tema del grado de conmutatividad. El *grado de conmutatividad* del grupo finito G se define como sigue

$$P(G) = \frac{|\{(x, y) \in G \times G : xy = yx\}|}{|G|^2},$$

que es la probabilidad de que dos elementos de G, elegidos al azar conmuten.

En 1975 Sherman [3], estudío la probabilidad de que un automorfismo de un grupo finito, fije un elemento arbitrario del grupo y, en 2011 Moghaddam [4]

presenta la probabilidad que un automorfismo de un grupo finito dado deje fijo un subconjunto; en general define

$$P_G(X) = \frac{|\{(g,x) \in G \times X : gx = x\}|}{|G|\,|X|},$$

donde G es un grupo que actúa sobre el conjunto X. En particular, si el grupo G actúa sobre sí mismo por conjugación, entonces la probabilidad anterior será $P(G)$.

En 2008 Pournaki, M. R. Sobhani [5] han estudiado y generalizado este concepto para un grupo G y $g \in G$,

$$P_g(G) = \frac{|\{(x,y) \in G \times G : [x,y] = g\}|}{|G|^2},$$

donde $[x,y] = x^{-1}y^{-1}xy$ es el conmutador de x e y. En particular, tenemos $P(G)$ cuando $g = 1$ el elemento identidad del grupo G y, $P_g(G) = 1$ si y sólo si G es un grupo abeliano y $g = 1$.

Es muy importante tener en cuenta que la probabilidad de conmutatividad no es la única medida de qué tan cerca está nuestro grupo de ser abeliano. Algunas otras medidas son: el tamaño del centro del grupo (una medida global que usa subgrupos), el tamaño de los centralizadores (una medida local que usa subgrupos), el tamaño de la abelianización (una medida que usa cocientes) y la ecuación de clase (una medida que usa clases de conjugación).

1.2 Definición de grado de conmutatividad

La *probabilidad de conmutatividad*, también llamada *grado de conmutatividad*, de un grupo finito es la probabilidad de que dos elementos elegidos al azar conmuten, y mide qué tan cerca está un grupo finito de ser abeliano. En todo el documento los grupos que consideraremos son finitos. Como nuestros grupos son finitos, la medida de probabilidad más natural debería ser aquella en la que los

elementos se eligen uniformemente al azar. Así que supongamos que a $G \times G$ se le asigna la distribución uniforme discreta. Sea $L(G)$ el evento,

$$L(G) = \{(x, y) \in G \times G : xy = yx\},$$

que es el conjunto de todos los pares de elementos que conmutan en G. La probabilidad de conmutatividad debe ser, por lo tanto, la probabilidad de que este evento $L(G)$ ocurra en G. Un resultado (x, y) para el cual $xy = yx$ se llama una *conmutatividad*. El conjunto de todas las *conmutatividades* es el evento "x e y conmutan" con $x, y \in G$ elegidos al azar es el conjunto $L(G)$.

Definición 1 *Sea G un grupo finito. Definimos la* ***probabilidad de conmutatividad*** *o* ***grado de conmutatividad*** *de G como*

$$P(G) = \frac{|L(G)|}{|G|^2}, \tag{1.1}$$

donde $L(G) = \{(x, y) \in G \times G : xy = yx\}$ es el conjunto de todas las conmutatividades.

El cociente $|L(G)| / |G|^2$ representa la cantidad de casos favorables para la conmutatividad sobre la cantidad casos posibles.

El conmutador de los elementos $g, h \in G$, denotado por $[g, h]$, se define como $g^{-1}h^{-1}gh \in G$. Se llama así porque $[g, h] = 1$ si y sólo si g y h conmutan. Entonces $L(G) = \{(x, y) \in G \times G : [x, y] = 1\}$ es una definición alternativa. El conjunto de todos los conmutadores de G no necesariamente forma un subgrupo de G, por esta razón consideramos el subgrupo generado por los conmutadores. Dado un grupo G, el subgrupo conmutador o subgrupo derivado es $G' = [G, G]$ se define como el subconjunto generado por todos los conmutadores $[g, h]$. Resulta que G' es un subgrupo normal y G/G' es el mayor cociente abeliano de G y por eso se llama su *abelianización*. Denotamos con $Z(G)$ al *centro* del grupo G que es el conjunto de todos los elementos de G que conmutan con todos los elementos

de G. Para $a \in G$, el conjunto $C_G(a)$ es el *centralizador* del elemento $a \in G$, que por definición es el conjunto $\{x \in G : xa = ax\}$ de los elementos de G que conmutan con a. Denotamos con $[G : C_G(a)]$ al cociente $|G| \,/\, |C_G(a)|$ llamado *indice del centralizador* $C_G(a)$ en G. La ecuación de clases de un grupo finito $G = \{x_1, \ldots, x_n\}$ es

$$|G| = |Z(G)| + \sum_{i=|Z(G)|+1}^{k(G)} [G : C_G(x_i)]$$

donde la sumatoria se realiza para $[G : C_G(x_i)] \geq 2$. Un análogo a esta ecuación es la "ecuación de grado" que afirma lo siguiente:

$$|G| = |G/G'| + \sum_{i=|G/G'|+1}^{k(G)} d_i^2$$

donde la sumatoria se realiza para $d_i \geq 2$. Una discusión más completa sobre la ecuación de grado se encuentra en el Capítulo 18 de [7].

La demostración del siguiente teorema se encuentra en cualquier texto de álgebra abstracta a excepción del la primera afirmación que es equivalente a la segunda.

Teorema 2 *Los siguientes afirmaciones son equivalentes para un grupo G.*

1. $P(G) = 1$
2. *G es abeliano*
3. $Z(G) = G$
4. $G' = \{1\}$
5. $C_G(a) = G$ *para todo* $a \in G$.
6. $G/G' \cong G$.

Demostración. Si $P(G) = 1$, entonces $|L(G)| = |G|^2$. Luego $L(G) = G^2$, y esto significa $xy = yx$ para todo $x, y \in G$. Así G es un grupo abeliano. Es inmediato observar que el razonamiento inverso también es cierto, lo que prueba que 1. es equivalente a 2. ∎

Según este resultado, para tener grados de conmutatividad diferentes de 1 debemos analizar grupos no abelianos.

Teorema 3 *Si G y H son grupos finitos isomorfos, entonces $P(G) = P(H)$.*

Demostración. Sea $f : G \to H$ un isomorfismo entre los grupos G y H. La función $\varphi : L(G) \to L(H)$ dada por $\varphi(x, y) = (f(x), f(y))$ está bien definida, puesto que si $(x, y) \in L(G)$, entonces $(x, y) \in G^2$ con $xy = yx$. Como f es un homomorfismo, $f(x)f(y) = f(y)f(x)$, con $(f(x), f(y)) \in H^2$. Luego $(f(x), f(y)) \in L(H)$. La inyectividad y sobreyectividad de φ son consecuencia de las mismas propiedades de f, lo que establece el resultado. ■

El recíproco del Teorema 3 no es cierto. El grupo diédrico D_3 y el grupo $D_3 \times \mathbb{Z}_2$ tienen el mismo grado de probabilidad y no son grupos isomorfos.

1.3 Ejemplos

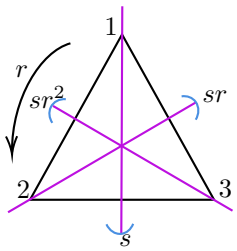
La tabla de ocurrencias de conmutatividades para un grupo G se llama la *tabla de conmutatividad*. Una tabla de conmutatividad contiene una entrada para cada par en el espacio muestral $G \times G$. Cada par ordenado en $L(G)$ está representado por 1 y todos los demás pares ordenados por 0. El grado de conmutatividad $P(G)$ es la proporción de entradas distintas de cero respecto al total de entradas en la tabla.

$\cdot$	1	r	r^2	s	sr	sr^2
1	1	1	1	1	1	1
r	1	1	1	0	0	0
r^2	1	1	1	0	0	0
s	1	0	0	1	0	0
sr	1	0	0	0	1	0
sr^2	1	0	0	0	0	1

Tabla 1.1: Tabla de conmutatividad del grupo D_3

El grupo diédrico D_3

De la clasificación de grupos finitos, sabemos que los grupos de orden menor o igual a 5 son todos abelianos, y por ende tienen grado de conmutatividad 1. El grupo no abeliano más pequeño es el **grupo diédrico** $D_3 = \langle r, s : r^3 = 1, s^2 = 1, sr = r^{-1}s\rangle$ de las simetrías de un triángulo equilátero generado por una rotación r y una reflexión s.



$$r = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad s = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$r^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad sr = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad sr^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Como el subgrupo generado por la rotación r es abeliano de orden 3, se tiene el cuadrado de 1 unos en la Tabla 1.1. En la diagonal principal también hay 1 unos ya que los elementos son los mismos y ellos conmutan. Los otros elementos de la tabla no conmutan, por ejemplo $sr^2 \cdot r = s$ y $r \cdot sr^2 = rr^{-2}s = r^{-1}s$ son diferentes. Hay en total $6^2 - 3^2 - 3 \cdot 3 = 18$ pares ordenados representados por 1 unos en la tabla, por lo que el grado de conmutatividad del grupo D_3 es

$$P(D_3) = P(G) = \frac{|L(G)|}{|G|^2} = \frac{18}{36} = \frac{1}{2}$$

significa que la probabilidad al tomar dos elementos de D_3 con reposición y que ellos conmuten es $0,5$. En otros términos, D_3 tiene grado de conmutatividad igual a $0,5$. La representación de los elementos de D_3 como permutaciones queda justificada, por el teorema de Cayley, un resultado de teoría de grupos que permite representar cualquier grupo como un grupo de permutaciones. Todo grupo finito

es isomorfo a un subgrupo de un grupo simétrico. Si el grupo es finito y tiene orden n, entonces es isomorfo a un subgrupo de S_n.

Los grupos abelianos tienen propiedades importantes y una de ellas es que su tabla de Cayley de los productos posibles es simétrica, y esta simetría también queda expresado por 1 unos en la tabla de conmutatividad del grupo. Una cuestión es si existen grupos que sean altamente abelianos, esto es, con grados de conmutatividad cercanos a 1 y, por otro lado, la existencia de grupos altamente no abelianos que serían aquellos que poseen grados de conmutatividad próximos a cero.

El grupo de cuaterniones

Los cuaterniones fueron introducidos por W. R. Hamilton en 1843, después de que él y otros matemáticos buscaron por muchos años un sistema numérico que describiera puntos del espacio tridimensional en forma similar a cómo los números complejos describen puntos del plano. Los cuaterniones son números hipercomplejos de la forma $a + bi + cj + dk$, donde a, b, c, d son números reales y las tres unidades imaginarias i, j, k tienen cuadrado igual a -1 y además

$$ij = k = -ji, \qquad jk = i = -kj, \qquad ki = j = -ik$$

El grupo de cuaterniones

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

es un grupo no abeliano de orden 8. El grupo de cuaterniones Q_8 tiene el mismo orden que el grupo diédrico D_4, pero una estructura diferente. Los subgrupos de Q_3 son $\{1\}$, $\{1, -1\}$, $\{1, -1, i, -i\}$, $\{1, -1, j, -j\}$, $\{1, -1, k, -k\}$ y Q_8.

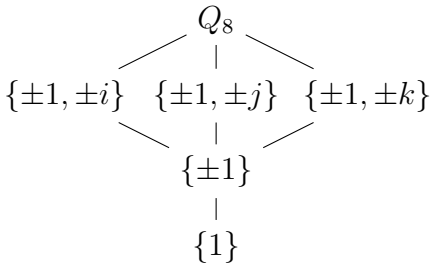


Figura 1.1: Diagrama de Heasse del grupo Q_8

Para determinar el grado de conmutatividad del grupo de cuaterniones, note que los elementos que no conmutan son $\pm i$ con $\pm j$ y $\pm k$. Son tres pares y las que se obtienen al conmutar, por conteo tenemos $2{\cdot}(2{\cdot}2)+2{\cdot}(2{\cdot}2)+2{\cdot}(2{\cdot}2) = 8+8+8 = 24$. Luego el grado de conmutatividad del grupo Q_8 es

$$P(Q_8) = \frac{64-24}{64} = \frac{40}{64} = \frac{5}{8} = 0,625$$

entonces el grupo Q_8 tiene "mayor conmutatividad" que el grupo diedrico D_3. El grupo Q_8 representado por generadores es

$$Q_8 = \left\langle a, b : a^4 = b^4 = 1,\ a^2 = b^2,\ ba = ab^3 \right\rangle$$

La multiplicación de la unidad imaginaria i por un número $a + ib$ equivale a una rotación del número complejo de 90^o, y en general la multiplicación de los números complejos y de los cuaterniones realizan rotaciones además de otros hechos geométricos.

El grupo de matrices $U(M_2(\mathbb{Z}_2))$

El conjunto $G = U(M_2(\mathbb{Z}_2))$ es el grupo de las unidades del anillo de matrices 2×2 con entradas en el campo $\mathbb{Z}_2$ de las clases residuales módulo 2. G es un grupo no abeliano. Los elementos de G son las matrices de determinante no cero

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

G es un grupo de orden 6. Por la clasificación de grupos de orden 6, G debe ser el grupo diédrico D_3. Entonces

$$P(G) = \frac{1}{2}.$$

Sea $r = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ y $s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Entonces $r^3 = 1$, $s^2 = 1$, $rs = sr^{-1}$, lo que prueba que G es isomorfo al grupo D_3.

En el siguiente capítulo probaremos que las conmutatividades están relacionadas con las clases conjugadas del grupo. Esto reduce el cálculo de las conmutatividades ya que es suficiente realizar cálculos sobre los representantes de las clases de conjugación.

1.4 Grado de conmutatividad de D_n

Si n es un entero positivo, entonces el grupo diedrico D_n es generado por dos elementos, la rotación r y la reflexión s que verifican las relaciones $r^n = s^2 = 1$ y $rs = sr^{-1}$. Por inducción se verifica que $r^k s = sr^{-k}$ y $sr^k = r^{-k}s$. Así $D_n = \{1, r, r^2, \ldots, r^{n-1}, s, rs, rs^2, \ldots, r^{n-1}s\}$. Para contar los elementos que conmutan observamos elementos de $D_n \times D_n$ en la siguiente tabla

	1	r	$\cdots$	r^{n-1}	s	rs	$\cdots$	$r^{n-1}s$
1	$(1,1)$		$\cdots$					$(1, r^{n-1}s)$
r	$\vdots$	(r,r)						
$\vdots$			$\ddots$					
r^{n-1}				(r^{n-1}, r^{n-1})				
s					(s,s)			
rs								
$\vdots$							$\ddots$	
$r^{n-1}s$	$(r^{n-1}s, 1)$							$(r^{n-1}s, r^{n-1}s)$

Tabla 1.2: Tabla de operaciones de D_n

De este se sigue inmediatamente el Teorema 4 para el caso n impar y par.

Teorema 4 *Si n es un entero positivo, entonces*

$$P(D_n) = \begin{cases} \frac{n+3}{4n}, & \textit{si } n \textit{ es impar;} \\ \frac{n+6}{4n}, & \textit{si } n \textit{ es par.} \end{cases}$$

Demostración. Los elementos de D_n son de la forma r^i o $r^i s$.

Caso 1 Si n es impar o par, los pares (r^i, r^j) conmutan para todo $0 \leq i, j < n$, ya que $r^i r^j = r^{i+j} = r^{j+i} = r^j r^i$. También conmutan los pares $(r^i s, 1)$, $(1, r^i s)$ y $(r^i s, r^i s)$ para $0 \leq i < n$.

Caso 2 El par $(r^i s, r^k)$ conmuta si y sólo si

$$r^i s \cdot r^k = r^k \cdot r^i s \Leftrightarrow r^{i-k} s = r^{i+k} s \Leftrightarrow r^{2k} = 1$$

sólo cuando $2k = n$.

Caso 3 Para $i > k$, el par $(r^i s, r^k s)$ conmuta si y sólo si

$$r^i s \cdot r^k s = r^k s \cdot r^i s \Leftrightarrow r^{i-k} = r^{k-i} \Leftrightarrow r^{2(i-k)} = 1$$

cuando $2(i-k) = n$.

1. Si n es impar, los casos 2 y 3 no se verifican, y el conteo se reduce al caso 1, por lo que hay $n^2 + 3n$ pares que conmutan. Por tanto,

$$P(D_n) = \frac{n^2 + 3n}{(2n)^2} = \frac{n+3}{4n}.$$

   Como $\lim_{n\to\infty} P(D_n) = \frac{1}{4}$, significa que para n impar grande, D_n tiene grado de conmutatividad próximo $\frac{1}{4} = 0,25$.

2. Si n es par, se debe contar las soluciones de ecuaciones en los casos 2 y 3.

   (a) $2k = n$, tiene solución única $k = n/2$, y los pares que conmutan son $(r^i s, r^{n/2})$ para $i = 0, 1, \ldots (n-1)$

   (b) $i = k + n/2$ donde $k = 0, 1, \ldots, (n/2 - 1)$ y los pares que conmutan son $(r^i s, r^k s)$.

   Considerando los pares invertidos, en total tenemos que

$$n^2 + 3n + n + n + \frac{n}{2} + \frac{n}{2} = n^2 + 6n$$

   de donde se sigue la conclusión.

■

En particular, $P(D_4) = \frac{4+6}{4\cdot 4} = \frac{10}{16} = \frac{5}{8}$.

Teorema 5 *Cada número primo puede aparecer como el denominador de $P(G)$ para algún grupo diédrico G.*

Demostración. Note que D_6 tiene grado de conmutatividad $1/2$, por lo que el resultado es cierto en el caso de primo par. Ahora, supongamos que queremos encontrar un grupo diédrico que tiene un primo impar de la forma $4n+3$ en el denominador de $P(G)$. Consideremos D_{2k}, cuyo grado de conmutatividad es

$$\frac{2k+6}{4\cdot 2k} = \frac{k+3}{4k}.$$

Queremos que sea un cociente de la forma $\frac{a_n}{4n+3}$, donde $(a_n, 4n+3) = 1$ y $a_n < 4n+3$. Esta condición se verifica con $a_n = n+1$. Ahora debemos resolver la ecuación

$$\frac{k+3}{4k} = \frac{n+1}{4n+3}.$$

Multiplicando y simplificando, encontramos que

$$\begin{aligned}(k+3)(4n+3) &= 4k(n+1)\\ 4kn+3k+12n+9 &= 4kn+4k\\ 12n+9 &= k.\end{aligned}$$

Por lo tanto, el grupo diédrico $D_{2(12n+9)} = D_{24n+18}$ tiene grado de conmutatividad $\frac{n+1}{4n+3}$. Esto significa que podemos encontrar ejemplos de grupos diédricos con grado de conmutatividad, cuyo denominador es un primo de la forma $4n+3$.

En el caso de primos de la forma $4n+1$, se plantea la ecuación

$$\frac{n+1}{4n+1} = \frac{k+3}{4k},$$

y se deduce que D_{8n+2} tiene la propiedad requerida. ∎

Capítulo 2

Propiedades algebraicas de $P(G)$

2.1 Una fórmula para $P(G)$

En el capítulo anterior hemos utilizado la definición para calcular el grado de conmutatividad de algunos grupos finitos. El problema es el conteo de las conmutatividades, elementos de $L(G)$, donde G es un grupo un grupo finito. El siguiente teorema expresa el problema de calcular el grado de conmutatividad en términos de las conjugadas del grupo G.

Sea $x \in G$. El centralizador de x en G es el subgrupo $C_G(x) = \{a \in G : ax = xa\}$ de elementos de G que conmutan con x. La clase conjugada del x es el conjunto $[x] = \{axa^{-1} : a \in G\}$ de las conjugaciones de x. El conjunto de todas las clases conjugadas $\{[x] : x \in G\}$ es una partición del grupo G. La correspondencia $\varphi : G/C_G(x) \to [x]$ dada por $\varphi(aC_G(x)) = axa^{-1}$ es una biyección, y tenemos

$$\frac{|G|}{|C_G(x)|} = |[x]|\,, \text{o bien}\, |C_G(x)| = \frac{|G|}{|[x]|}.$$

Por propiedades de las clases de equivalencia tenemos también que si $y \in [x]$, entonces $[x] = [y]$.

Teorema 6 *El grado de conmutatividad del grupo G es el cociente entre el número de clases conjugadas $k(G)$ sobre el orden de G, es decir*

$$P(G) = \frac{k(G)}{|G|}. \tag{2.1}$$

Demostración. Sea $(u, v) \in L(G)$, entonces $uv = vu$. Por definición de centralizador $v \in C_G(u)$, y así $(u, v) \in \{u\} \times C_G(u) \subset \bigcup_{x\in G}\{x\} \times C_G(x)$. Inversamente, si $(u, v) \in \bigcup_{x\in G}\{x\} \times C_G(x)$, entonces $(u, v) \in \{x\} \times C_G(x)$ para algún $x \in G$. Se sigue que $u = x$ y $vx = xv$, es decir $vu = uv$, en consecuencia $(u, v) \in L(G)$. Hemos probado que

$$L(G) = \bigcup_{x\in G} \{x\} \times C_G(x). \tag{2.2}$$

La familia de conjuntos $\{\{x\} \times C_G(x)\}_{x\in G}$ es disjunta, ya que para $x \neq y$ por propiedades del producto cartesiano,

$$(\{x\} \times C_G(x)) \cap (\{y\} \times C_G(y)) = (\{x\} \cap \{y\}) \times (C_G(x) \cap C_G(y)) = \emptyset.$$

Sean $[x_1], \ldots, [x_{k(G)}]$ todas las distintas clase conjugadas en el grupo G y sea $k(G)$ el número de clases conjugadas. Entonces de (2.2)

$$\begin{aligned}
|L(G)| &= \sum_{x\in G} |C_G(x)| \\
&= \sum_{x\in G} \frac{|G|}{|[x]|} \\
&= \sum_{i=1}^{k(G)} \sum_{x\in[x_i]} \frac{|G|}{|[x]|} && \text{por partición en clases conjugadas,} \\
&= \sum_{i=1}^{k(G)} \sum_{x\in[x_i]} \frac{|G|}{|[x_i]|} && \text{cambio de representante de clase,} \\
&= \sum_{i=1}^{k(G)} |[x_i]| \frac{|G|}{|[x_i]|} \\
&= \sum_{i=1}^{k(G)} |G| = k(G)\,|G|
\end{aligned}$$

se sigue que

$$P(G) = \frac{|L(G)|}{|G|^2} = \frac{k(G)\,|G|}{|G|^2} = \frac{k(G)}{|G|}$$

■

Note que de la demostración anterior tenemos la identidad

$$\sum_{x \in G} |C_G(x)| = |G|^2 P(G) \tag{2.3}$$

que emplearemos con mucha frecuencia.

Aunque la ecuación (2.1) nos presente una nueva forma de obtener $P(G)$ sigue siendo difícil de calcular, sin embargo facilita algunas demostraciones de grados de conmutatividad y cálculos como veremos más adelante. Por el momento calcular la probabilidad de conmutatividad de un grupo finito se convierte en una cuestión de contar el número de clases de conjugación del grupo. Para algunos grupos es posible calcular explícitamente las clases de conjugación.

Ejemplo 7 *El grado de conmutatividad del grupo de cuaterniones Q_8 es $\frac{5}{8}$.*

Demostración.

Determinación de las clases conjugadas. El grupo de cuaterniones $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ verifica las relaciones $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$. Note que $i^{-1} = -i$. Luego $[1] = \{x1x^{-1} : x \in Q\} = \{1\}$, $[-1] = \{-1\}$. Para calcular la clase conjugada de i, tenemos

$$jij^{-1} = ji(-j) = -jij = -jk = -i,$$

de forma análoga $kik^{-1} = -i$, así $[i] = \{\pm i\} = [-i]$. Del mismo modo $[j] = \{\pm j\} = [-j]$ y $[k] = \{\pm k\} = [-k]$. Luego tenemos 5 clases conjugadas. De donde el grado de conmutatividad del grupo de cuaterniones es $P(Q_8) = \dfrac{5}{8}$. ■

Ejemplo 8 *El grado de conmutatividad de los grupos simétricos S_3 y S_4 son $\frac{1}{2}$ y $\frac{5}{24}$ respectivamente.*

Demostración. El número de clase conjugadas del grupo simétrico S_n es igual al número de particiones del entero n. Las particiones de 3 son 3, $2+1$ y $1+1+1$, luego

$$P(S_3) = \frac{k(S_3)}{|S_3|} = \frac{3}{3!} = \frac{1}{2}.$$

Las particiones de 4 son 4, $3+1$, $2+2$, $2+1+1$, $1+1+1+1$ en total son 5. Luego

$$P(S_4) = \frac{k(S_4)}{|S_4|} = \frac{5}{4!} = \frac{5}{24}.$$

■

2.2 Grado de conmutatividad del producto directo

El producto de grupos es una forma de construir grupos a partir de dos grupos más pequeños, y puede usarse para construir un grupo más grande y también para calcular el grado de conmutatividad de grupos que se pueden expresar como producto de grupos. Sean G y H grupos, el producto de G y H es el grupo cuyos elementos son por pares ordenados: $G \times H = \{(a, b) : a \in G \text{ y } b \in H\}$ con la operación de grupo que se realiza componente a componente. El elemento identidad de $G \times H$ es $(1, 1)$, y el inverso de un elemento $(a, b) \in G \times H$ está dado por $(a, b)^{-1} = (a^{-1}, b^{-1})$. Más generalmente, podemos tomar cualquier lista de grupos $G_1, \ldots, G_n$ y formar el grupo producto $G_1 \times \cdots \times G_n$. El siguiente teorema relaciona el grado de conmutatividad del grupo producto con el grado de conmutatividad de cada factor.

Teorema 9 *Si G y H grupos finitos cualesquiera, entonces el grado de conmutatividad del grupo producto $G \times H$ es producto de los grados de conmutatividad de G con H, esto es*

$$P(G \times H) = P(G)P(H).$$

Demostración. Para que esta identidad sea cierta, debe ser posible realizar una biyección entre los conjuntos de conmutatividad. La forma natural de hacerlo, es definiendo $\varphi : L(G \times H) \to L(G) \times L(H)$ por

$$\varphi((a,b),(c,d)) = ((a,c),(b,d)).$$

Note que φ está bien definida y es fácil establecer que es una biyección. De donde $|L(G \times H)| = |L(G)|\,|L(H)|$, y como $|G \times H| = |G|\,|H|$, tenemos que

$$P(G \times H) = \frac{|L(G \times H)|}{|G \times H|^2} = \frac{|L(G)|}{|G|^2}\frac{|L(H)|}{|H|^2} = P(G)P(H).$$

Podemos dar otra demostración mediante las clases conjugadas y apelar al Teorema 6. Sea $(u,v) \in [(x,y)]$, entonces existe (a,b) tal que

$$(u,v) = (a,b)(x,y)(a,b)^{-1}. \tag{2.4}$$

Como la operación en el grupo producto $G \times H$ es componente a componente, (2.4) es equivalente a

$$u = axa^{-1} \text{ y } v = byb^{-1},$$

de donde $(u,v) \in ([x],[y])$ y se sigue inmediatamente que $[(x,y)] = ([x],[y])$; así

$$k(G \times H) = k(G) \cdot k(H).$$

Luego como consecuencia del Teorema 6

$$P(G \times H) = \frac{k(G \times H)}{|G \times H|} = \frac{k(G) \cdot k(H)}{|G|\,|H|} = \frac{k(G)}{|G|}\frac{k(H)}{|H|} = P(G)P(H)$$

como se quería. ■

Ejemplo 10 *El grado de conmutatividad de grupo diédrico D_6 es $\frac{1}{2}$*

Demostración. El grupo diédrico D_6 es isomorfo al grupo $D_3 \times \mathbb{Z}_2$. En la, Sección 1.3 hemos establecido que $P(D_3) = \dfrac{1}{2}$ y como $\mathbb{Z}_2$ es un grupo abeliano su grado de conmutatividad es 1, luego

$$P(D_6) = P(D_3 \times \mathbb{Z}_2) = P(D_3) \cdot P(\mathbb{Z}_2) = \frac{1}{2}.$$

■

Ahora podemos construir grupos cuyos grados de conmutatividad estén próximos a cero, por ejemplo, el producto de n grupos diédricos D_3 dado por $G_n = \prod_{i=1}^{n} D_3$ tiene grado de conmutatividad $P(G_n) = \dfrac{1}{2^n}$. Como $\lim_{n\to\infty} P(G_n) = 0$, significa que para n suficientemente grande, el grupo G_n es altamente no abeliano. Este resultado también muestra que 0 es un punto de acumulación del conjunto $A = \{P(G) : G \text{ es un grupo finito}\}$. ¿Existe otros punto de acumulación?

El Teorema 4 afirma que $P(D_n) = \frac{n+3}{4n}$ si n es impar y $P(D_n) = \frac{n+6}{4n}$ si n es par. Así, $\lim_{n\to\infty} P(D_n) = \dfrac{1}{4}$, de donde $\dfrac{1}{4}$ es también un punto de acumulación de A.

2.3 Grado de conmutatividad del grupo cociente

Lema 11 *Sean H y K subgrupos de G y $a, b \in G$ con $a \in H$. Entonces $a(H \cap K) = H \cap aK$.*

Demostración. Si $x \in a(H \cap K)$, entonces $x = au$ con $u \in H \cap K$, luego $x \in H \cap aK$. Inversamente, si $x \in H \cap aK$ entonces $x = ak$ con $x \in H$ y $k \in K$, y como $k = a^{-1}x \in H$, se sigue que $k \in H \cap K$, luego $x \in a(H \cap K)$. ■

Teorema 12 *Si N es un subgrupo normal de G, entonces $P(G/N) \geq \dfrac{P(G)}{P(N)}$.*

Demostración. Probaremos la primera parte. Por el Segundo Teorema de Isomorfismo

$$\frac{C_G(x)}{N \cap C_G(x)} \cong \frac{C_G(x)N}{N} \subset C_{G/N}(xN). \tag{2.5}$$

La última inclusión se justifica por lo siguiente. Si $unN \in \dfrac{C_G(x)N}{N}$, con $u \in C_G(x)$ y $n \in N$, entonces

$$(xN)(unN) = (xN)(uN) = xuN = uxN = (uN)(xN) = (unN)(xN)$$

y $unN \in C_{G/N}(xN)$. Aplicando cardinalidades a (2.5) obtenemos

$$\left|\frac{C_G(x)}{N \cap C_G(x)}\right| = \left|\frac{C_G(x)N}{N}\right| \leq \left|C_{G/N}(xN)\right|.$$

De donde

$$|C_G(x)| \leq \left|C_{G/N}(xN)\right| |N \cap C_G(x)|.$$

Sumando sobre los elementos x de G

$$|L(G)| = \sum_{x \in G} |C_G(x)| \leq \sum_{x \in G} \left|C_{G/N}(xN)\right| |N \cap C_G(x)|$$

Como las clases conjugadas forman una partición de G, tenemos que

$$\begin{aligned} |L(G)| &\leq \sum_{S \in G/N} \sum_{x \in S} \left|C_{G/N}(S)\right| |N \cap C_G(x)| \\ &= \sum_{S \in G/N} \left|C_{G/N}(S)\right| \sum_{x \in S} |N \cap C_G(x)|, \end{aligned} \tag{2.6}$$

donde $S = xN$ para algún $x \in G$. La última suma se puede escribir como $\sum_{x \in S} |N \cap C_G(x)| = \sum_{x \in S, z \in N \cap C_G(x)} 1$. Es inmediato mostrar la siguiente equivalencia: $x \in S$, $z \in N \cap C_G(x) \Leftrightarrow z \in N$, $x \in C_G(z) \cap S$. Luego

$$\sum_{x \in S, z \in N \cap C_G(x)} 1 = \sum_{z \in N, x \in C_G(z) \cap S} 1 = \sum_{z \in N} |C_G(z) \cap S|.$$

Cuando $C_G(z) \cap S \neq \emptyset$, sea $x_0 \in C_G(z) \cap S$, entonces $S = Nx_0$, luego por lema anterior

$$(C_G(z) \cap N)x_0 = C_G(z) \cap x_0N = C_G(z) \cap S.$$

Se deduce que $|C_G(z) \cap S| \leq |C_G(z) \cap N|$, ya que $C_G(z) \cap S$ puede ser vacío. Al insertar estos resultados en (2.6) tenemos

$$|L(G)| \leq |L(G/N)| \sum_{z \in N} |C_G(z) \cap N|.$$

De donde

$$|L(G)| \leq |L(G/N)| \cdot |L(N)|$$

al dividir por $|G|^2$

$$\frac{|L(G)|}{|G|^2} \leq \frac{|L(G/N)|}{|G|^2 / |N|^2} \cdot \frac{|L(N)|}{|N|^2}$$

se sigue

$$P(G) \leq P(G/N) \cdot P(N).$$

■

2.4 Grado de conmutatividad de subgrupos

Si H es un subgrupo del grupo G, en general H posee menos elementos que G, e incluso H puede ser el subgrupo trivial $\{1\}$ que es abeliano, luego esperamos que en general se verifique la desigualdad $P(G) \leq P(H)$. En lo que sigue aplicamos reiteradamente las propiedades de clases. Si H es un subgrupo del grupo G y $a, b \in G$, entonces $aH = bH$ si y sólo si $a = b \cdot h$ para algún $h \in H$, que equivale a $ab^{-1} \in H$.

Teorema 13 *Si H es un subgrupo de G, entonces*

$$\frac{P(H)}{[G : H]^2} \leq P(G) \leq P(H).$$

Demostración. Definimos $\varphi : C_G(x)/C_H(x) \to G/H$ por $\varphi(aC_H(x)) = aH$. Es una función, en efecto, si $aC_H(x) = bC_H(x)$, entonces $a = ub$ para algún $u \in C_H(x) = H \cap C_G(x)$. Entonces $aH = ubH = bH$. La función φ es inyectiva, ya que si $aH = bH$, con $a, b \in C_G(x)$, entonces $a = bh$ para algún $h \in H$. Entonces

$$aC_H(x) = bh(H \cap C_G(x)) = bC_H(x)$$

De ahí

$$[C_G(x) : C_H(x)] \leq [G : H]. \tag{2.7}$$

Por el Teorema de Lagrange y (2.7)

$$\begin{aligned} |C_G(x)| &= |C_H(x)|\,[C_G(x) : C_H(x)] \\ &\leq |C_H(x)|\,[G : H]. \end{aligned}$$

De donde,

$$|C_G(x)| \leq |C_H(x)|\,[G : H] \tag{2.8}$$

Sumando sobre los elementos de G obtenemos

$$\sum_{x\in G} |C_G(x)| \leq [G : H] \sum_{x\in G} |C_H(x)| \tag{2.9}$$

El primer miembro es $|L(G)|$, pero la sumatoria del segundo no representa todavía $|L(H)|$.

Si $x \in G$ y $y \in C_H(x)$ entonces $yx = xy$ y $y \in H$. En este caso, $xy = yx$ entonces $y \in H$ y $x \in C_G(y)$ de donde podemos reescribir el lado derecho de la ecuación (2.9) como sigue:

$$\sum_{x\in G} |C_G(x)| \leq [G : H] \sum_{y\in H} |C_G(y)| \tag{2.10}$$

Utilizando (2.8) en (2.10), obtenemos

$$\sum_{x\in G} |C_G(x)| \leq [G : H]^2 \sum_{x\in H} |C_H(y)|$$

que es equivalente a

$$|L(G)| \leq [G : H]^2\,|L(H)|$$

y así $P(G) \leq P(H)$.

Para la otra desigualdad, como $C_H(x) = C_G(x) \cap H \leq C_G(x)$, entonces

$$\begin{aligned} |G|^2 P(G) &= \sum_{x \in G} |C_G(x)| \\ &\geq \sum_{x \in G} |C_H(x)| \\ &\geq \sum_{x \in H} |C_H(x)| \\ &= |H|^2 P(H) \end{aligned}$$

de donde $P(G) \geq \dfrac{1}{[G : H]^2} P(H)$. ∎

Capítulo 3

Cotas al grado de conmutatividad

Hemos calculado la probabilidad de conmutatividad de algunos grupos, pero en general no es posible obtener una fórmula para $P(G)$ cuando G es un grupo finito arbitrario. Sin embargo, se puede determinar cotas para $P(G)$ bajo ciertas condiciones y de cierta clase de grupos, como los grupos no abelianos, los grupos solubles y los grupos nilpotentes.

Teorema 14 *Supongamos que* $|G/Z| = l$. *Entonces* $P(G) \geq \frac{2l-1}{l^2}$, *donde* $Z = Z(G)$ *es el centro del grupo* G.

Demostración. Asumimos la hipótesis $|G/Z| = l$. La figura 1.2 muestra la relación entre el centro Z y G, en el producto $G \times G$.

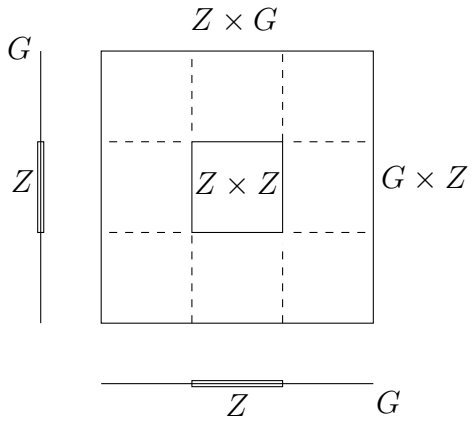


Figura 1.2: Diagrama cartesiano de $G \times G$

Note que $G \times Z$, $Z \times G$ y $Z \times Z$ son subconjuntos de $L = \{(x, y) \in G^2 : xy = yx\}$. Entonces por el principio de inclusión y exclusión

$$|L| \geq |G \times Z| + |Z \times G| - |Z \times Z|,$$

de donde

$$\begin{aligned} P(G) = \frac{|L|}{|G \times G|} &\geq \frac{|G \times Z| + |Z \times G| - |Z \times Z|}{|G|^2} \\ &= \frac{2|G|\,|Z| - |Z|^2}{|G|^2} \\ &= \frac{2l|Z|^2 - |Z|^2}{l^2|Z|^2} \\ &= \frac{2l-1}{l^2}. \end{aligned}$$

■

3.1 La cota $5/8$ para grupos no abelianos

Sea $Z(G)$ el centro del grupo G, de modo que $G/Z(G)$ es cíclico; entonces G es un grupo abeliano. En efecto, todo grupo cíclico es generado por un elemento, luego $G/Z(G) = \langle xZ(G)\rangle$ para algún $x \in G$. Sean $a, b \in G$, entonces $aZ(G) = x^n Z(G)$ para algún n. Luego $a = x^n u$ para algún $u \in Z(G)$ y del mismo modo, $b = x^m v$ para algún $v \in Z(G)$ y entero m. Entonces por estar los elementos u y v en el centro, $ab = x^n u \cdot x^m v = x^n x^m \cdot vu = x^m x^n \cdot vu = x^m v \cdot x^n u = ba$. Por otro lado, si G es un grupo de orden primo p, entonces G es cíclico. En efecto, como $|G| > 1$, entonces existe un elemento $a \in G$ diferente de 1. El grupo generado por a, $\langle a\rangle$, es un subgrupo no trivial y, por teorema de Lagrange, su orden divide a p. Como p es primo, $|\langle a\rangle| = |G|$ y así $\langle a\rangle = G$.

Los grupos abelianos tiene grado de conmutatividad 1. Ahora mostraremos una cota superior para el grado de conmutatividad de grupos no abelianos.

Teorema 15 *Sea G un grupo finito no abeliano. Entonces $P(G) \leq 5/8$*

Demostración. La ecuación de clase de grupos es dada por

$$|G| = |Z(G)| + \sum_{i=|Z(G)|+1}^{k(G)} |[x_i]|, \tag{3.1}$$

donde $x_1, \ldots, x_n$ son representantes de las clases conjugadas y en la sumatoria se supone $|[x_i]| \geq 2$. Insertando esta desigualdad en (3.1) obtenemos

$$|G| \geq |Z(G)| + 2(k(G) - |Z(G)|);$$

resolviendo para $k(G)$ se obtiene

$$k(G) \leq \frac{|G| + |Z(G)|}{2}. \tag{3.2}$$

Como G no es un grupo abeliano, entonces $G/Z(G)$ no es cíclico, luego $|G/Z(G)|$ no puede ser 2 ni 3, entonces $|G/Z(G)| \geq 4$, luego $|Z(G)| \leq \frac{|G|}{4}$, e insertando esto en (3.2)

$$k(G) \leq \frac{|G| + |G|/4}{2} = \frac{5}{8}|G|,$$

de donde $P(G) \leq 5/8$. ∎

Así, en resumen, dado un grupo finito G, la probabilidad $P(G)$ de que dos de sus elementos, elegidos al azar con reemplazo, conmuten es igual a $k(G)/|G|$, con $P(G) = 1$ si y sólo si G es abeliano y $P(G) \leq 5/8$ si G no es abeliano. Del Teorema 15 también se sigue que no existe ningún grupo no abeliano con grado de conmutatividad en el intervalo abierto $(5/8, 1)$. La cota $5/8$ puede ser alcanzada por varios grupos como muestra el siguiente teorema.

Teorema 16 *Sea G un grupo finito no abeliano tal que $|Z(G)| = |G|/4$. Entonces $P(G) = \frac{5}{8}$.*

Demostración. Como $|Z(G)| = |G|/4$ no es igual a $|G|$, entonces existe x en G tal que $x \notin Z(G)$. De las inclusiones $Z(G) \subset C_G(x) \subset G$, se sigue que

$$4 = [G : Z(G)] = [G : C_G(x)] \cdot [C_G(x) : Z(G)],$$

Como G no es abeliano, cada factor del segundo miembro no puede ser 1. En efecto, si $[G : C_G(x)] = 1$, entonces $G = C_G(x)$, de donde x conmuta con todo elemento de G, y así $x \in Z(G)$ lo que es una contradicción. Si $[C_G(x) : Z(G)] = 1$, entonces $C_G(x) = Z(G)$, de donde $x \in Z(G)$, lo que es una contradicción. Así, $[G : C_G(x)] = 2$ para todo $x \notin Z(G)$. Note que, si $x \in Z(G)$, entonces $C_G(x) = G$. Aplicando estos resultados y por la ecuación (2.3)

$$\begin{aligned}
|G|^2 P(G) &= \sum_{x\in G} |C_G(x)| \\
&= \sum_{x\in Z(G)} |C_G(x)| + \sum_{x\notin Z(G)} |C_G(x)| \\
&= \sum_{x\in Z(G)} |G| + \sum_{x\notin Z(G)} |C_G(x)| \\
&= |Z(G)|\,|G| + \sum_{x\notin Z(G)} \frac{|G|}{2} \\
&= \frac{|G|}{4}|G| + \frac{3|G|}{4}\cdot\frac{|G|}{2} \\
&= \frac{|G|^2}{4} + 3\frac{|G|^2}{8} \\
&= \frac{5|G|^2}{8},
\end{aligned}$$

entonces $P(G) = \frac{5}{8}$. ∎

Ejemplo 17 *En el grupo de cuaterniones Q_8, el orden de su centro es igual a $\frac{|Q_8|}{4}$.*

Demostración. Sea $a \in Z(Q_8)$. Entonces $ax = xa$ para todo $x \in Q_8$. En particular, $ai = ia$, $aj = ja$. Esto implica que $a \neq \pm j, \pm k, \pm i$. Luego $a = \pm 1$. Así, $|Z(Q_8)| = 2 = \frac{|Q_8|}{4}$. Por el teorema anterior, $P(Q_8) = \frac{5}{8}$. ∎

Los grupos de la forma $Q_8 \times \mathbb{Z}_n$ también tienen grado de conmutatividad 5/8. Otro grupo con grado de conmutatividad 5/8 es el grupo diédrico D_4.

3.2 Las p-cotas superiores

Por la dificultad de calcular el grado de conmutatividad $P(G)$, se busca cotas superiores e inferiores. Una es en función del centro del grupo y divisores primos de él. Para un primo p, un grupo G es un p-grupo si cada elemento de G tiene orden una potencia de p. Todo p-grupo tiene centro no trivial, así $|Z(G)| > 1$. El Teorema de Cauchy afirma que, si G es un grupo tal que p divide a $|G|$, entonces G contiene un p-subgrupo. Sea $|G| = p^n m$, donde p^n es la mayor potencia de p en $|G|$, el subgrupo de orden p^n es llamado un p-subgrupo de Sylow. Los grupos de orden primo son cíclicos. Si el cociente $G/Z(G)$ es cíclico, entonces G es un grupo abeliano. El siguiente teorema establece una cota superior para $P(G)$ en términos de un primo p.

Teorema 18 *Sea p el primo más pequeño que divide a $|G/Z(G)|$, donde G es un grupo no abeliano. Entonces*

$$P(G) \leq \frac{p^2 + p - 1}{p^3}.$$

Demostración. Como p divide a $|G/Z(G)|$, entonces existe un entero positivo u tal que $|G| = pu\,|Z(G)|$. Si $u = 1$, entonces $|G/Z(G)| = p$ un primo, entonces G es un grupo abeliano y $|G/Z(G)| = 1$, lo que es una contradicción. Así, $u > 1$. Como u divide a $|G/Z(G)|$, por la minimalidad de p, los factores primos de u son mayores o iguales a p, así $u \geq p$, utilizando la ecuación de clase.

$$|G| = |Z(G)| + \sum_{i=|Z(G)|+1}^{k(G)} [G : C_G(x_i)] \tag{3.3}$$

donde los x_i son representantes de las clases conjugadas y $x_i \notin Z(G)$. Sea $x \in G - Z(G)$. Entonces $[G : C_G(x)] > 1$, puesto que si $[G : C_G(x)] = 1$, entonces $G = C_G(x)$, esto implica que $x \in Z(G)$, lo que es una contradicción. Como $Z(G) \subset C_G(x) \subset G$, por propiedad de índices

$$pu = [G : Z(G)] = [G : C_G(x)] \cdot [C_G(x) : Z(G)].$$

Sea q un primo que divide a $[G : C_G(x)]$, entonces q divide a $[G : Z(G)]$, y por la minimalidad de p, $p \leq q \leq [G : C_G(x)]$. Insertando en la ecuación de clase (3.3)

$$|G| \geq |Z(G)| + p(k(G) - |Z(G)|).$$

Resolviendo la desigualdad para $k(G)$, tenemos

$$\frac{|G| + (p-1)\,|Z(G)|}{p} \geq k(G),$$

dividiendo por $|G|$

$$\frac{|G| + (p-1)\,|Z(G)|}{p\,|G|} \geq P(G).$$

Como $p \leq u$, se tiene que $1/u \leq 1/p$

$$\begin{aligned} P(G) &\leq \frac{|G/Z(G)| + (p-1)}{p\,|G/Z(G)|} = \frac{pu + (p-1)}{p^2 u} \\ &= \frac{1}{p} + \frac{p-1}{p^2 u} \leq \frac{1}{p} + \frac{p-1}{p^3} = \frac{p^2 + p - 1}{p^3}. \end{aligned}$$

■

La condición para la igualdad en la desigualdad del teorema anterior esta dada por el teorema siguiente.

Teorema 19 *Sea p un primo, si G no es un grupo abeliano con $|G| = p^3$, entonces $P(G) = \dfrac{p^2 + p - 1}{p^3}$.*

Demostración. Note que G es un p-grupo, luego tiene centro no trivial, $|Z(G)| > 1$. Primero probaremos que $|Z(G)| = p$. Como G no es abeliano, entonces $|Z(G)| < p^3$. Si $|Z(G)| = p^2$, entonces $[G : Z(G)] = p$, luego G sería un grupo abeliano, lo que es una contradicción. Consideremos la ecuación de clase

$$|G| = |Z(G)| + \sum_{i=|Z(G)|+1}^{k(G)} [G : C_G(x_i)]. \tag{3.4}$$

Si $x \in G - Z(G)$, entonces $|Z(G)| < |C_G(x)| < p^3$. Como G es p-grupo, tenemos que $|C_G(x)| = p^2$, y así $[G : C_G(x)] = p$. Reemplazando este en la ecuación de clase (3.4)

$$|G| = |Z(G)| + p(k(G) - |Z(G)|)$$

Resolviendo para $k(G)$ se obtiene

$$\begin{aligned} k(G) &= \frac{|G| + (p-1)\,|Z(G)|}{p} \\ &= \frac{p^3 + (p-1)p}{p} \\ &= p^2 + p - 1 \end{aligned}$$

Por lo tanto,

$$P(G) = \frac{p^2 + p - 1}{p^3}$$

■

Ejemplo 20 *Si G es un grupo de orden 8 (como el grupo Q_8 o D_4), su grado de conmutatividad es*

$$P(G) = \frac{2^2 + 2 - 1}{2^3} = \frac{5}{8}.$$

3.3 Las p-cotas inferiores

Teorema 21 *Sea p un entero primo y $n \in \mathbb{N}$ donde $n \geq 2$ tal que $|G/Z(G)| = p^n$. Entonces*

$$P(G) \geq \frac{p^n + p^{n-1} - 1}{p^{2n-1}}.$$

Demostración. De la ecuación de clase

$$|G| = |Z(G)| + \sum_{i=|Z(G)|+1}^{k(G)} [G : C_G(x_i)]. \tag{3.5}$$

Sea $x \in G - Z(G)$. Tenemos que $Z(G) \subset C_G(x) \subset G$ y por hipótesis $|G| = p^n\,|Z(G)|$. Por la ecuación de indices

$$p^n = [G : Z(G)] = [G : C_G(x)] \cdot [C_G(x) : Z(G)]\,.$$

Por divisibilidad, existe un entero v tal que

$$[G : C_G(x)] = p^v \tag{3.6}$$

donde $v < n$, ya que si $v = n$, entonces $C_G(x) = Z(G)$, luego $x \in Z(G)$ lo que es una contradicción. En (3.6) v puede asumir los valores $1, 2, \ldots, n-1$. Luego

$$[G : C_G(x)] \leq p^{n-1}.$$

Aplicando en la ecuación de clase (3.5)

$$|G| \leq |Z(G)| + p^{n-1}(k(G) - |Z(G)|).$$

Resolviendo la desigualdad para $k(G)$

$$k(G) \geq \frac{|G| + (p^{n-1} - 1)\,|Z(G)|}{p^{n-1}}.$$

Dividiendo por $|G|$

$$\begin{aligned} P(G) &\geq \frac{|G| + (p^{n-1} - 1)\,|Z(G)|}{p^{n-1}\,|G|} \\ &= \frac{|G/Z(G)| + p^{n-1} - 1}{p^{n-1}\,|G/Z(G)|} \\ &= \frac{p^n + p^{n-1} - 1}{p^{2n-1}}. \end{aligned}$$

■

3.4 Posibles valores de los grados de conmutatividad

En esta sección analizamos los grupos cuyo grado de conmutatividad es 5/8, y presentamos las condiciones bajo las cuales se verifica este resultado. Estas condiciones están en términos del orden del grupo cociente G/Z. Algunos otros valores que puede asumir $P(G)$ son también analizados en general en términos de G/Z.

Lema 22 *Si G/Z es cíclico, entonces $P(G) = 1$.*

Demostración. Sea $G/Z = \langle xZ \rangle$ el grupo generado por xZ. Sean $a, b \in G$, entonces

$$aZ = x^n Z \text{ y } bZ = x^m Z$$

para algunos enteros n y m. Luego, existen $z_1, z_2 \in Z$ tales que $a = x^n z_1$ y $b = x^m z_2$. Luego

$$ab = x^n z_1 \cdot x^m z_2 = z_1 z_2 x^n x^m = x^m z_2 \cdot x^n z_1 = ba.$$

De donde G es un grupo abeliano. ∎

La recíproca del Lema 22 es cierto, ya que, si $P(G) = 1$, entonces, por el Teorema 2, el grupo G es abeliano; luego el cociente $G/Z(G) = \{1\}$ es cíclico.

Teorema 23 *Sea G un grupo finito. Entonces $P(G) = \frac{5}{8}$ si y sólo si $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ el 4-grupo de Klein.*

Demostración. Supongamos que $P(G) = \frac{5}{8}$ y sea $|G/Z(G)| = \ell$, sea $x \in G - Z(G)$. No puede ser que $|[x]| = 1$; en ese caso, $[x] = \{x\}$, y se tendría que $x \in Z(G)$. Así, $|[x]| \geq 2$. Si $|[x]| > 2$, para algún x, entonces $[x] = [x_i]$ para algún x_i representante de la clase conjugada. En la ecuación de clase

$$|G| = |Z(G)| + \sum_{i=|Z(G)|+1}^{k(G)} |[x_i]| > |Z(G)| + 2(k(G) - |Z(G)|).$$

Resolviendo para $k(G)$

$$k(G) < \frac{|G| + |Z(G)|}{2},$$

de donde

$$P(G) < \frac{|G| + |Z(G)|}{2\,|G|} = \frac{\ell\,|Z(G)| + |Z(G)|}{2\ell\,|Z(G)|} = \frac{\ell + 1}{2\ell}.$$

Como $P(G) \neq 1$, por el Lema 22, $G/Z(G)$ no es un grupo cíclico y como los grupos de orden primo son ciclicos, entonces $\ell = |G/Z(G)| \geq 4$; y como $f(\ell) = \frac{\ell + 1}{2\ell} = \frac{1}{2} + \frac{1}{2\ell}$ es decreciente, entonces

$$f(\ell) \leq f(4)$$

luego

$$\frac{5}{8} = P(G) < f(\ell) \leq f(4) = \frac{5}{8}$$

lo que es una contradicción. Luego $|[x]| = 2$ para todo $x \notin Z(G)$. En la ecuación de clase

$$|G| = |Z(G)| + \sum_{i=|Z(G)|+1}^{k(G)} |[x_i]| = |Z(G)| + \sum_{i=|Z(G)|+1}^{k(G)} 2 = |Z(G)| + 2(k(G) - |Z(G)|),$$

y resolviedo la ecuación para $k(G)$

$$k(G) = \frac{|G| + |Z(G)|}{2}$$

Por la hipótesis asumida

$$\frac{5}{8}|G| = \frac{|G| + |Z(G)|}{2}$$

dividiendo por $|Z|$

$$\frac{5}{8}\ell = \frac{\ell + 1}{2}$$

y obtenemos $\ell = 4$. Así $|G/Z(G)| = 4$. Como $G/Z(G)$ no es cíclico y los únicos grupos de orden 4 son $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$, se deduce que $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ que es el 4-grupo de Klein.

Reciprocamente, supongamos que $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ y sea $x \in G - Z(G)$. Entonces $Z(G) \neq C_G(x)$ y $C_G(x) \neq G$. Luego

$$|Z(G)| < |C_G(x)| < |G|$$

de donde

$$1 < |C_G(x)/Z(G)| < |G/Z(G)| = 4$$

Como $C_G(x)/Z(G) \leq G/Z(G)$, y el orden de $C_G(x)/Z(G)$ divide al orden de $G/Z(G)$, concluimos que $|C_G(x)/Z(G)| = 2$, luego $|C_G(x)| = 2\,|Z(G)|$. Pero

$$|[x]| = |G/C_G(x)| = \frac{|G|}{2\,|Z(G)|} = \frac{1}{2} \cdot 4 = 2$$

para todo $x \notin Z(G)$. En la ecuación de clase

$$|G| = |Z(G)| + \sum_{i=|Z(G)|+1}^{k(G)} 2 = |Z(G)| + 2(k(G) - |Z(G)|).$$

Resolviendo para $k(G)$

$$k(G) = \frac{|G| + |Z(G)|}{2}$$

de donde

$$P(G) = \frac{|G| + |Z(G)|}{2\,|G|} = \frac{1}{2}(1 + \frac{|Z(G)|}{|G|}) = \frac{1}{2}(1 + \frac{1}{4}) = \frac{5}{8}$$

y queda completa la demostración. ∎

El siguiente resultado es más general que el Teorema 23.

Proposición 24 *Sea p el primo más pequeño que divide a $|G/Z(G)|$. Entonces $P(G) = \frac{p^2+p-1}{p^3}$ si y sólo si $|G/Z(G)| = p^2$.*

Demostración. Supongamos que $|G/Z(G)| = p^2$. Sea $x \in G - Z(G)$. Entonces

$$|Z(G)| < |C_G(x)| < |G|,$$

de lo cual

$$1 < |C_G(x)/Z(G)| < |G/Z(G)|.$$

Como $C_G(x)/Z(G)$ es un subgrupo de $G/Z(G)$, observando el orden del grupo se deduce que $|C_G(x)/Z(G)| = p$, es decir $|C_G(x)| = p\,|Z(G)|$. Luego $|G/C_G(x)| = |G|\,/p\,|Z(G)| = |G/Z(G)|/p = p$ para todo $x \notin Z(G)$. En la ecuación de clase

$$|G| = |Z(G)| + p(k(G) - |Z(G)|)$$

Resolviendo para $k(G)$ tenemos

$$k(G) = \frac{|G| + (p-1)|Z(G)|}{p}.$$

Como $|G| = p^2|Z(G)|$,

$$k(G) = \frac{p^2|Z(G)| + p|Z(G)| - |Z(G)|}{p},$$

dividiendo por $|G|$ obtenemos

$$P(G) = \frac{(p^2 + p - 1)|Z(G)|}{p^3|Z(G)|} = \frac{p^2 + p - 1}{p^3}.$$

Reciprocamente, supongamos que $P(G) = \dfrac{p^2 + p - 1}{p^3}$ y sea $|G/Z(G)| = \ell$. Para $x \in G - Z(G)$,

$$|[x]| = [G : C_G(x)] = [G : Z(G)]/[C_G(x) : Z(G)] > 1,$$

de donde resulta que $|[x]|$ divide a $[G : Z(G)]$. Luego $[G : Z(G)] = |[x]| \cdot k$ para algún entero k. Note que $|[x]| > 1$. Luego en $|[x]|$ hay factores primos de $[G : Z(G)]$, y por la minimalidad de p, se sigue que $|[x]| \geq p$ para cada $x \notin Z(G)$. Reemplazando en la ecuación de clase da

$$|G| \geq |Z(G)| + p(k(G) - |Z(G)|),$$

y resolviendo para $k(G)$

$$k(G) \leq \frac{|G| + (p-1)|Z(G)|}{p}.$$

El grado de conmutatividad es

$$\begin{aligned} P(G) &\leq \frac{|G| + (p-1)|Z(G)|}{p|G|} \\ &= \frac{\ell|Z(G)| + (p-1)|Z(G)|}{p\ell|Z(G)|} \\ &= \frac{\ell + p - 1}{p\ell} \end{aligned}$$

Por hipótesis

$$\frac{p^2 + p - 1}{p^3} \leq \frac{\ell + p - 1}{p\ell}.$$

Resolvemos para ℓ en términos de p como sigue

$$\begin{aligned}(p^3+p^2-p)\ell &\leq p^3\ell + p^4 - p^3\\ (p^2-p)\ell &\leq p^4 - p^3\\ \ell &\leq \frac{p^4-p^3}{p^2-p}\\ \ell &\leq p^2.\end{aligned}$$

Por lo tanto, $|G/Z(G)| \leq p^2$. Por la minimalidad de p, tenemos que $p \leq |G/Z(G)|$. Si $|G/Z(G)| = q$ es primo, entonces $G/Z(G)$ es cíclico y G es abeliano, luego $P(G) = 1 = \frac{p^2+p-1}{p^3}$ lo que es una contradicción. En el caso de que $|G/Z(G)|$ sea compuesto, tiene al menos dos factores y uno de ellos es p. Luego por la minimalidad de p, se sigue que $|G/Z(G)| \geq p^2$. Por consiguiente, $|G/Z(G)| = p^2$.

■

El siguiente resultado muestra la forma de los grupos G para los que se cumple $P(G) = (p^2+p-1)/p^3$.

Corolario 25 *Si* $P(G) = \dfrac{p^2+p-1}{p^3}$, *donde* p *es el primo más pequeño que divide a* $|G/Z(G)|$, *entonces* $G \cong P \times A$ *donde* P *es un* p*-grupo y* A *es abeliano.*

Demostración. Por la Proposición 24 $|G/Z(G)| = p^2$, luego G es nilpotente ya que los p-grupos son nilpotentes. Luego, para algún m,

$$G \cong P \times P_1 \times P_2 \times \cdots \times P_m$$

donde cada P_i es un p_i-subgrupo de Sylow de orden $p_i^{n_i}$ y P es un p-subgrupo de Sylow de orden p^n. Como $|G/Z(G)| = p^2$,

$$|Z(G)| = p^{n-2}p_1^{n_1}p_2^{n_2}\cdots p_m^{n_m}.$$

Además, para cada i, $P_i \subset Z(G)$ y cada p_i-subgrupo de Sylow es abeliano. Por lo tanto,

$$G \cong P \times A$$

donde $A = P_1 \times P_2 \times \cdots \times P_m$ es abeliano. ∎

La definición de los grupos nilpotentes será desarrollada en el siguiente capítulo y sus propiedades, serán especificadas en el Apéndice A.

Corolario 26 *Sea p un primo. Entonces $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$ si y sólo si $P(G) = \frac{p^2+p-1}{p^3}$, donde p es el primo más pequeño que divide a $|G/Z(G)|$.*

Demostración. Supongamos que $P(G) = \frac{p^2+p-1}{p^3}$, donde p es el primo más pequeño que divide a $|G/Z(G)|$. Por el Corolario 25, $G \cong P \times A$, donde P es un p-grupo y A es un grupo abeliano, de modo que $P(G) = P(P \times A) = P(P)$. Por lo tanto, sin pérdida de generalidad, suponga que G es un p-grupo. Entonces G es nilpotente. Se sigue que $G/Z(G) = \prod_{i=1}^{n} \mathbb{Z}_p$ para algún $n \in \mathbb{N}$. Por la Proposición 24, $|G/Z(G)| = p^2$, entonces $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Reciprocamente, tenemos que $|G/Z(G)| = p^2$. Por la Proposición 24, resulta que $P(G) = \frac{p^2+p-1}{p^3}$. ∎

Corolario 27 *Si $G/Z(G) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, entonces $P(G) = \frac{11}{27}$.*

Demostración. El resultado se sigue del Corolario 26. ∎

Capítulo 4

Cota inferior para los grupos nilpotentes

4.1 Grupos nilpotentes

Un grupo G es abeliano cuando $Z(G) = G$. Luego $G/Z(G) = \{1\}$. Si G no es un grupo abeliano, entonces $G/Z(G)$ es no trivial y consideremos su centro $Z(G/Z(G))$. Sea el epimorfismo canónico $\pi : G \to G/Z(G)$, donde $Z(G/Z(G)) \lhd G/Z(G)$, además que $\pi^{-1}(Z(G/Z(G))) \lhd G$. Definimos

$$Z_0(G) = \{1\} \text{ y } Z_1(G) = Z(G)$$

$$Z_i(G) = \pi_i^{-1}(Z(G/Z_{i-1}(G))), \text{ para } i > 1$$

donde $\pi_i : G \to G/Z_{i-1}(G)$. con $Z_i(G) \lhd G$ para todo $i > 1$.

Así, obtenemos la serie ascendente

$$\{1\} = Z_0(G) \lhd Z_1(G) \lhd Z_2(G) \lhd \cdots \tag{4.1}$$

donde $Z_{i+1} \lhd G$, $Z_i \lhd Z_{i+1}$ y $Z(G/Z_i(G)) \cong Z_{i+1}(G)/Z_i(G)$. Note que el grupo G puede ser alcanzado o no por los $Z_i(G)$.

Si existe un $n \in \mathbb{N}$ donde $Z_n(G) = G$, es decir.

$$\{1\} = Z_0(G) \lhd Z_1(G) \lhd Z_2(G) \lhd \cdots \lhd Z_n(G) = G$$

entonces diremos que G es un grupo nilpotente.

Definición 28 *Un grupo G es **nilpotente** si existe un entero positivo n tal que $Z_n(G) = G$.*

Otra caracterización de un grupo abeliano G es mediante el subgrupo derivado $G' = [G, G]$ generado por los conmutadores $[g_1, g_2]$ con $g_1, g_2 \in G$. Un grupo G es abeliano si $G' = \{1\}$. Ahora si G no es abeliano, entonces $G' \neq \{1\}$ y $G \rhd G' \rhd \{1\}$. Esto lleva a pensar en el grupo $G^2 = [G, G']$ tal que $G \rhd G' \rhd G^2$, en general tenemos la serie descendente

$$G \rhd G^1 \rhd G^2 \rhd G^3 \rhd \cdots \tag{4.2}$$

con $G^0 = G$ y donde $G^i = [G, G^{i-1}]$ para $i \geq 1$. La sucesión G^i en (4.2) puede alcanzar al grupo trivial $\{1\}$ o no.

Si existe un $n \in \mathbb{N}$ tal que $G^n = [G, G^{n-1}] = \{1\}$, es decir

$$G^0 = G \rhd G^1 \rhd G^2 \rhd G^3 \rhd \cdots \rhd G^n = \{1\}$$

diremos que G es un grupo nilpotente.

Definición 29 *Un grupo G es **nilpotente** si existe un entero positivo n tal que $G^n = \{1\}$.*

Teorema 30 *Para un grupo G, las siguientes afirmaciones son equivalentes:*

1. *G es un grupo nilpotente.*
2. *Existe $n \in \mathbb{N}$ tal que $Z_n(G) = G$.*
3. *Existe $n \in \mathbb{N}$ tal que $G^n = \{1\}$.*

Definición 31 *Si G es un grupo nilpotente, entonces la* ***clase de nilpotencia*** *de G o* ***clase*** *de G es la más pequeña $n \geq 0$ tal que $Z_n(G) = G$ y $G^n = \{1\}$.*

Ejemplo 32 *Todo grupo abeliano G es nilpotente.*

Demostración. Como G es abeliano, entonces $Z_1(G) = Z(G) = G$; el grupo G es alcanzado en el primer paso, por lo cual tiene clase de nilpotencia 1. Analogamente $G^0 = G$ y $G' = G^1 = \{1\}$. En particular, todo grupo cíclico es nilpotente. ■

Considerando que los grupos nilpotentes son un tipo especial de grupos, estos serán desarrollados en el Apéndice A; sin embargo, enumeraremos algunas de sus propiedades:

1. Cada subgrupo de un grupo nilpotente es nilpotente.
2. Todo grupo cociente de un grupo nilpotente es nilpotente.
3. Si $G_1, G_2, \cdots, G_n$ son grupos nilpotentes, entonces $G_1 \times G_2 \times \cdots \times G_n$ es nilpotente.
4. La imagen homomorfa de un grupo nilpotente es nilpotente.
5. Todo p-grupo finito es nilpotente.
6. Si $G/Z(G)$ es nilpotente, entonces G es nilpotente.
7. Sea G un grupo finito, las siguientes condiciones son equivalentes.
   - G es nilpotente.
   - Todo subgrupo de Sylow de G es un subgrupo normal.
   - G es isomorfo al producto directo de p_i-subgrupo de Sylow.

4.2 Cota inferior para grupos nilpotentes

En 1968, Erdös y Turan [1] demostraron que $k(G) \geq \log_2(\log_2 |G|)$. Sherman [3], proporcionó un cota inferior significativamente mayor para el grado de conmutatividad de los grupos nilpotentes demostrando que $k(G) \geq \log_2 |G|$ para grupos nilpotentes. Proporcionaremos una prueba del resultado de Sherman.

Lema 33 *Todo subgrupo normal N de un grupo G es unión de clases conjugadas.*

Demostración. En efecto, tenemos que $N \subset \bigcup_{n\in N}[n]$. Si $n \in N$, por ser N normal, se tiene que $gng^{-1} \in N$ para todo $g \in G$, esto es, $[n] \subset N$ para todo $n \in N$, luego $\bigcup_{n\in N}[n] \subset N$ y por tanto $N = \bigcup_{n\in N}[n]$. ∎

Teorema 34 *Si G es un grupo nilpotente finito de clase n, entonces*

$$P(G) \geq \frac{n\,|G|^{1/n} - n + 1}{|G|}.$$

Demostración. Como G es nilpotente, entonces existe un entero positivo n tal que

$$\{1\} = Z_0(G) \lhd Z_1(G) \lhd Z_2(G) \lhd \cdots \lhd Z_n(G) = G.$$

De donde,

$$\{1\} = Z_0 \subsetneq Z_1 \subsetneq Z_2 \subsetneq \cdots \subsetneq Z_n = G,$$

escribimos G en la forma

$$G = Z_0 \cup (Z_1 - Z_0) \cup (Z_2 - Z_1) \cup \cdots \cup (Z_n - Z_{n-1}) \tag{4.3}$$

donde cada $Z_i \lhd G$. Por el lema anterior tendremos que $Z_i = \bigcup_{i=1}^{t}[x_i]$ y $Z_{i-1} = \bigcup_{i=1}^{s}[y_i]$ son uniones de clases conjugadas disjuntas, entonces $Z_i - Z_{i-1} = Z_i - (Z_i \cap Z_{i-1})$ es unión de clases conjugadas disjuntas de G. Sea $x \in Z_i - Z_{i-1}$ y $g \in G$, entonces $xZ_{i-1} \in Z_i/Z_{i-1} = Z(G/Z_{i-1})$, luego

$$x^{-1}g^{-1}xgZ_{i-1} = x^{-1}Z_{i-1} \cdot g^{-1}Z_{i-1} \cdot xZ_{i-1} \cdot gZ_{i-1} = Z_{i-1}$$

de donde $g^{-1}xg \in xZ_{i-1}$, así $[x] \subseteq xZ_{i-1}$. Entonces

$$|[x]| \leq |xZ_{i-1}| = |Z_{i-1}|$$

ya que las clases laterales tienen el mismo número de elementos. Como $Z_i - Z_{i-1}$ es unión disjunta de clases conjugadas, digamos $Z_i - Z_{i-1} = \bigcup_{j=1}^{r_i}[x_j]$ donde r_i es el número de clases conjugadas de $Z_i - Z_{i-1}$, entonces

$$|Z_i - Z_{i-1}| = \left|\bigcup_{j=1}^{r_i}[x_j]\right| = \sum_{j=1}^{r_i}|[x_j]| \leq \sum_{j=1}^{r_i}|Z_{i-1}| = r_i\,|Z_{i-1}|$$

luego $r_i \geq \dfrac{|Z_i - Z_{i-1}|}{|Z_{i-1}|}$. De (4.3) contando las clases de conjugación y aplicando la desigualdad de la media aritmética-geométrica, se obtiene

$$\begin{aligned}
k(G) &= 1 + r_1 + r_2 + \cdots + r_n \\
&\geq 1 + \sum_{i=1}^{n} \frac{|Z_i - Z_{i-1}|}{|Z_{i-1}|} \\
&= 1 + \sum_{i=1}^{n} \frac{|Z_i| - |Z_{i-1}|}{|Z_{i-1}|} && \text{principio de sustracción} \\
&= 1 + \sum_{i=1}^{n} \left|\frac{Z_i}{Z_{i-1}}\right| - n \\
&\geq 1 + n\left(\prod_{i=1}^{n}\left|\frac{Z_i}{Z_{i-1}}\right|\right)^{1/n} - n && \text{desigualdad de la media A.G.} \\
&= 1 + n\,|G|^{1/n} - n,
\end{aligned}$$

de donde

$$P(G) \geq \frac{n\,|G|^{1/n} - n + 1}{|G|} \tag{4.4}$$

■

Del valor óptimo del segundo miembro de (4.4) tenemos el siguiente corolario.

Corolario 35 *Si G es un grupo nilpotente finito de clase n, entonces $P(G) > \dfrac{\log_2 |G|}{|G|}$.*

Demostración. Sea $f(x) = nx^{1/n} - n + 1 - \log_2 x$ donde x es un número real positivo.

Su derivada es

$$f'(x) = x^{1/n-1} - \frac{1}{x \ln 2} = \frac{1}{x}(\sqrt[n]{x} - \frac{1}{\ln 2}) = \frac{1}{x}(x - \frac{1}{(\ln 2)^n}) \cdot \varphi(x, n),$$

donde $\varphi(x, n) = \frac{1}{\sum_{i=0}^{n-1}(\sqrt[n]{x})^{n-1-i} \cdot \frac{1}{(ln2)^i}}$, es una expresión que no posee raíces para $x > 0$. Se deduce que f tiene punto crítico $x = 1/(\ln 2)^n$ que corresponde a un valor mínimo. Entonces $f(1/(\ln 2)^n) \leq f(|G|)$. Pero

$$\begin{aligned} f(\frac{1}{(\ln 2)^n}) &= n \cdot \frac{1}{\ln 2} - n + 1 - n \log_2 \left(\frac{1}{\ln 2}\right) \\ &= n \left(\frac{1}{\ln 2} - 1 + \log_2(\ln 2)\right) + 1 \\ &\geq \frac{1}{\ln 2} - 1 + \log_2(\ln 2) + 1 \\ &= \log_2(\ln 2) + \frac{1}{\ln 2} > 0 \end{aligned}$$

entonces $f(|G|) > 0$, de donde $n|G|^{1/n} - n + 1 - \log_2 |G| > 0$. Por el Teorema 34

$$P(G) > \frac{n|G|^{1/n} - n + 1}{|G|} > \frac{\log_2 |G|}{|G|}$$

■

4.3 La cota $1/2$ para grupos nilpotentes

En esta sección mostramos que $1/2$ es una cota superior del grado de conmutatividad de los grupos no nilpotentes. Luego mostramos que este es la cota superior mínima describiendo la clase de grupos no nilpotentes que tienen un grado de conmutatividad menor o igual a $1/2$.

Lema 36 *Sea G un grupo finito. Si $|G'| = 2$, entonces $G' \subset Z(G)$*

Demostración. Sea $G' = \{1, a\}$ con $a \neq 1$. Debemos demostrar que $a \in Z(G)$. Por reducción al absurdo, supongamos que $a \notin Z(G)$. Entonces existe un elemento b que no conmuta con a, es decir,

$$aba^{-1}b^{-1} \neq 1.$$

Pero $aba^{-1}b^{-1} \in G' = \{1, a\}$, entonces

$$aba^{-1}b^{-1} = a,$$

de donde $a = 1$ lo que es una contradicción. ■

Lema 37 *Si $G' \subset Z(G)$, entonces $G/Z(G)$ es abeliano.*

Demostración. Por hipótesis $[a, b] \in Z(G)$. Por propiedades de clases laterales

$$\begin{aligned}
[aZ(G), bZ(G)] &= aZ(G) \cdot bZ(G) \cdot (aZ(G))^{-1} \cdot (bZ(G))^{-1} \\
&= aZ(G) \cdot bZ(G) \cdot a^{-1}Z(G) \cdot b^{-1}Z(G) \\
&= a \cdot b \cdot a^{-1} \cdot b^{-1}Z(G) \\
&= [a, b]Z(G) \\
&= Z(G)
\end{aligned}$$

lo que significa que las clases laterales arbitrarias $aZ(G)$ y $bZ(G)$ conmutan. ■

Teorema 38 *Sea G es un grupo finito.*

1. *Si $P(G) > \frac{1}{2}$, entonces $|G'| < 3$*
2. *Si $P(G) > \frac{1}{2}$, entonces G es un grupo nilpotente.*

Demostración.

1. Supongamos que $P(G) > \frac{1}{2}$. Entonces $k(G) > \dfrac{|G|}{2}$. Por las cotas de la ecuación de grado

$$|G| = |G/G'| + \sum_{i=|G/G'|+1}^{k(G)} d_i^2,$$

donde $d_i \geq 2$. Luego

$$\begin{aligned} |G| &\geq |G/G'| + 4(k(G) - |G/G'|) \\ &> |G/G'| + 4(\frac{|G|}{2} - |G/G'|); \end{aligned}$$

dividiendo por $|G|$

$$1 > \frac{1}{|G'|} + 4(\frac{1}{2} - \frac{1}{|G'|}) = 2 - 3\frac{1}{|G'|}.$$

Resolviendo la inecuación para $|G'|$ nos da

$$|G'| < 3$$

2. Por la primera parte, $|G'| < 3$. Entonces $|G'|$ es 1 o 2.

Caso 1 Si $|G'| = 1$, entonces $G' = \{1\}$. Así, G es un grupo abeliano, luego G es un grupo nilpotente.

Caso 2 Si $|G'| = 2$, por el lema 36

$$G' \subset Z(G).$$

De donde G' es un grupo abeliano.

$$\begin{aligned} G^0 &= G \\ G^1 &= [G, G] = G' \\ G^2 &= [G, G'] \\ &= \left\langle aba^{-1}b^{-1} : a \in G, b \in G' \right\rangle \\ &= \{1\} \end{aligned}$$

ya que cuando $b \in G'$, entonces $b \in Z(G)$, así, la serie central superior termina después de dos términos y G es nilpotente de clase de nilpotencia 2, esto establece 2.

■

Nota. De la parte 2 del Teorema 38 se sigue que, si G no es un grupo finito nilpotente, entonces $P(G) \leq 1/2$, luego no existe grupos nilpotentes finitos con grado de conmutatividad en el intervalo abierto $(1/2, 1)$.

4.4 Grupos solubles

En esta sección, proporcionamos una cota superior del grado de conmutatividad de los grupos no solubles. Concluimos la sección describiendo todos los grupos con grado de conmutatividad $1/n$ en términos de la solubilidad del grupo.

Un grupo G es abeliano si $G' = \{1\}$. Construimos una sucesión de subgrupos de G con los subgrupos conmutadores, de la siguiente forma. Sea $G^{(0)} = G$, $G^{(1)} = G' = [G, G]$ el subgrupo conmutador de G. Sea $G^{(2)} = (G^{(1)})^{(1)} = [G^{(1)}, G^{(1)}]$. Entonces $G^{(2)} \subset G^{(1)} \subset G^{(0)}$. En general, sea $G^{(i+1)} = (G^{(i)})^{(1)} = [G^{(i)}, G^{(i)}]$ para $i \geq 0$. Tenemos la sucesión

$$G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots \tag{4.5}$$

llamado ***serie derivada*** o ***serie conmutador*** de G. En (4.5), el grupo trivial $\{1\}$ puede ser alcanzado o no.

Definición 39 *Sea G un grupo. Entonces G es un **grupo soluble** si $G^{(n)} = \{1\}$ para algún entero positivo n, es decir*

$$G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots \supset G^{(n)} = \{1\}.$$

*Si la serie derivada nunca llega al grupo trivial, se dice que G es **insoluble**.*

Al igual que los grupos nilpotentes, los grupos solubles son un caso especial de grupos, estos serán desarrollados en el Apéndice B; sin embargo, enumeraremos algunas de sus propiedades:

1. Todo grupo nilpotente es soluble.
2. Todo subgrupo de un grupo soluble es soluble.
3. Todo grupo cociente de un grupo soluble es soluble.
4. Si $G_1, G_2, \cdots, G_n$ son grupos solubles, entonces $G_1 \times G_2 \times \cdots \times G_n$ es soluble.
5. La imagen homomorfa de un grupo soluble es soluble.
6. Si G es un p-grupo finito entonces G es soluble.
7. Si $N \triangleleft G$ tal que N y G/N son solubles, entonces G es soluble.

Teorema 40 (Feit-Thompson) *Todo grupo finito de orden impar es soluble*

Ejemplo 41 *Los grupos de orden* $2k+1$ *con* $k \geq 0$ *son solubles.*

Teorema 42 (Burnside) *Sea* G *es un grupo de orden* $p^a \cdot q^b$ *con* p, q *primos y* a, b *enteros no negativos. Entonces* G *es soluble.*

Ejemplo 43 *Los grupos de orden* 30 *son solubles.*

Demostración. Escribimos $30 = 3 \cdot 10$, el número r_3, de 3-subgrupos Sylow de G, es tal que $r_3|10$ y $r_3 \equiv 1 \bmod 3$. Por lo tanto, el número de 3-subgrupos de Sylow es 1 o 10. Del mismo modo, el número r_5, de 5-subgrupos de Sylow, es tal que $r_5|6$ y $r_5 \equiv 1 \bmod 5$. Por lo tanto, el número de 5-subgrupos Sylow es 1 o 6. Si suponemos que $r_3 = 10$ y $r_5 = 6$, entonces por conteo $2 \cdot 10 + 4 \cdot 6 + 1 = 45 > 30$. Note que los 3-subgrupos Sylow son disjuntos por Teorema de Lagrange. Por tanto, $r_3 = 1$ o $r_5 = 1$. En el caso $r_3 = 1$, de los teoremas de Sylow se sabe que

cuando hay un unico subgrupo de Sylow, él es un subgrupo normal. Luego existe un subgrupo H normal en G de orden 3. Como el grupo cociente G/H tiene orden $10 = 2 \cdot 5$, por el Teorema de Burnside el grupo cociente G/H es soluble y luego G es soluble. ■

Lema 44 *Si $|G'| < 60$, entonces G es soluble.*

Demostración. Por el Teorema de Burnside, los grupos de orden $p^a q^b$ son solubles, luego cuando $|G'| < 60$ se deduce que G' es soluble salvo cuando $|G'| = 30$ o $|G'| = 42$. En el ejemplo 43 se verificó que cuando $|G'| = 30$, se tiene G' soluble. Análogamente, para $|G'| = 42$ se deduce que G' es soluble. Luego G' es soluble. Como el cociente G/G', es un grupo abeliano y es soluble y, por la Proposición 66, G es un grupo soluble. ■

Proposición 45 *Si $P(G) > 21/80$, entonces G es un grupo soluble.*

Demostración. Por la ecuación de grado

$$|G| = |G/G'| + \sum_{i=|G/G'|+1}^{k(G)} d_i^2,$$

donde $d_i \geq 2$. Se sigue que

$$|G| \geq |G/G'| + 4(k(G) - |G/G'|)$$

dividiendo por $|G|$ obtenemos

$$1 \geq \frac{1}{|G'|} + 4P(G) - \frac{4}{|G'|}$$

luego

$$\frac{21}{80} < P(G) \leq \frac{1}{4}\left(\frac{3}{|G'|} + 1\right) = \frac{3}{4}\frac{1}{|G'|} + \frac{1}{4}.$$

Resolviendo para $|G'|$

$$|G'| < 60$$

Por Lema 44, G es soluble. ∎

Nota. De la Proposición 45 se sigue que, si G no es un grupo finito soluble, entonces $P(G) \leq 21/80$, luego no existe grupos solubles finitos con grado de conmutatividad en el intervalo abierto $(21/80, 1)$.

4.5 Grupos con grados de conmutatividad $1/n$

Teorema 46 *Sea p primo. Entonces existe un grupo con grado de conmutatividad $1/p$. Este grupo es un producto directo de grupos solubles.*

Demostración. Realizamos inducción sobre p. Para $p = 2$, el Teorema 4 sobre grado de conmutatividad del grupo diédrico establece que $P(D_3) = \frac{1}{2}$ y, por el Teorema de Burnside D_3, es soluble ya que su orden es $6 = 2 \cdot 3$. Por cálculo directo, se establece el grado de conmutatividad del grupo alternante, $P(A_4) = \frac{1}{3}$. El orden de A_4 es $12 = 2^2 3$, y por el Teorema de Burnside, A_4 es un grupo soluble. Siguiente, suponemos que para todos los primos p_i menores que p, con $p > 3$, existe algún producto de grupos solubles H_i con $P(H_i) = \frac{1}{p_i}$. Realizando la división de p entre 4 se presentan los siguientes casos. Cuando $p \equiv 3 (\mathrm{mod}\, 4)$, entonces $p = 4m + 3$ para algún $m \in \mathbb{N}$. Tenemos

$$P(D_{3p}) = \frac{3(4m+3)+3}{4(3p)} = \frac{m+1}{p}.$$

Factorizando en primos tenemos que $m + 1 = p_1 p_2 \cdots p_s$, luego $p = 4m + 3 > m+1 > p_i$. Por la hipótesis de inducción, existe los grupos H_i tal que $P(H_i) = \frac{1}{p_i}$. Sea $M = \prod_{i=1}^{s} H_i$. Por Teorema 9,

$$P(M) = P(\prod_{i=1}^{s} H_i) = \prod_{i=1}^{s} P(H_i) = \prod_{i=1}^{s} \frac{1}{p_i} = \frac{1}{m+1}.$$

Aplicando el Teorema 9 una vez más al grupo $G = D_{3p} \times M$, vemos que el grado de conmutatividad de G es

$$P(G) = P(D_{3p})P(M) = \frac{m+1}{p} \cdot \frac{1}{m+1} = \frac{1}{p}.$$

■

Corolario 47 *Para cada $n \in \mathbb{N}$ hay un grupo soluble G con un grado de conmutatividad $1/n$.*

Demostración. Expresamos n como producto de primos, digamos $n = p_1 p_2 \cdots p_r$. Por el Teorema 46, existe un grupo soluble H_i tal que $P(H_i) = \frac{1}{p_i}$. Consideremos el grupo soluble. $G = H_1 \times H_2 \times \cdots \times H_r$. Entonces $P(G) = \frac{1}{n}$. ■

Este resultado establece que hay grupos con grados de probabilidad muy próximos a cero.

Conclusiones

Hemos visto que se puede calcular la probabilidad de conmutatividad, es decir, calcular la probabilidad de que dos elementos elegidos al azar conmuten; además se puede desarrollar diferentes propiedades, a saber:

1 Para cualquier grupo finito G, se puede calcular la probabilidad de conmutatividad dada por $P(G) = \frac{k(G)}{|G|}$ donde $k(G)$ es el número de clases conjugadas distintas de G.

2 La probabilidad de conmutatividad de un grupo, se puede extender al producto directo, subgrupos, subgrupo normal y grupo cociente; obtuvimos desigualdades para cada una.

3 Se puede construir grupos con grados de conmutatividad tan próximos a cero como se desee.

4 Para todo grupo finito no abeliano G, se cumple que $P(G) \leq \frac{5}{8}$ es decir, para todo grupo finito no abeliano, su grado de conmutatividad está en el intervalo $(0, \frac{5}{8}]$.

5 Se determino las p-cotas superiores e inferiores, para números p primos determinados.

6 Si G no es un grupo nilpotente, entonces $P(G) \leq \frac{1}{2}$.

7 Si G no es un grupo soluble, entonces $P(G) \leq \frac{21}{80}$.

8 Para cualquier número entero p primo, hay un grupo que es producto directo de grupos solubles con grado de conmutatividad $\frac{1}{p}$, es decir para cada primo p existe un grupo con grado de conmutatividad $\frac{1}{p}$, en general se demostró que para n natural existe un grupo soluble G con grado de conmutatividad $\frac{1}{n}$.

9 De modo particular para el grupo diédrico D_n, demostramos una fórmula general para calcular la probabilidad de conmutatividad de dichos grupos para n par o impar, además se halló la cota $\frac{1}{4}$ para el grupo diédrico.

Las características enumeradas con anterioridad, pueden ser profundizadas o extendidas a otras estructuras como los anillos.

Apéndice A

Grupos nilpotentes

Sea el epimorfismo canónico $\pi : G \to G/Z(G)$, donde $Z(G/Z(G)) \lhd G/Z(G)$, además que $\pi^{-1}(Z(G/Z(G))) \lhd G$. Definimos

$$Z_0(G) = \{1\} \text{ y } Z_1(G) = Z(G)$$

$$Z_i(G) = \pi_i^{-1}(Z(G/Z_{i-1}(G))), \text{ para } i > 1$$

donde $\pi_i : G \to G/Z_{i-1}(G)$. con $Z_i(G) \lhd G$ para todo $i > 1$.

Así, obtenemos la serie ascendente

$$\{1\} = Z_0(G) \lhd Z_1(G) \lhd Z_2(G) \lhd \cdots \tag{A.1}$$

donde $Z(G/Z_i(G)) \cong Z_{i+1}(G)/Z_i(G)$. Note que el grupo G puede ser alcanzado o no por los $Z_i(G)$.

Definición 48 *Si existe un $n \in \mathbb{N}$ donde $Z_n(G) = G$, es decir.*

$$\{1\} = Z_0(G) \lhd Z_1(G) \lhd Z_2(G) \lhd \cdots \lhd Z_n(G) = G$$

donde $Z(G/Z_i(G)) \cong Z_{i+1}(G)/Z_i(G)$, entonces diremos que G es un ***grupo nilpotente****.*

Otra caracterización de los grupos nilpotentes es mediante el subgrupo derivado $G' = [G, G]$ generado por los conmutadores $[g_1, g_2]$ con $g_1, g_2 \in G$, $G^2 = [G, G']$ tal que $G \triangleright G' \triangleright G^2$, en general tenemos la serie descendente

$$G \triangleright G^1 \triangleright G^2 \triangleright G^3 \triangleright \cdots \tag{A.2}$$

con $G^0 = G$ y donde $G^i = [G, G^{i-1}]$ para $i \geq 1$. La sucesión G^i en (A.2) puede alcanzar al grupo trivial $\{1\}$ o no.

Definición 49 *Si existe un $n \in \mathbb{N}$ tal que $G^n = [G, G^{n-1}] = \{1\}$, es decir*

$$G^0 = G \triangleright G^1 \triangleright G^2 \triangleright G^3 \triangleright \cdots \triangleright G^n = \{1\}$$

*diremos que G es un **grupo nilpotente**.*

Teorema 50 *Para un grupo G, las siguientes afirmaciones son equivalentes:*

1. *G es un grupo nilpotente.*
2. *Existe $n \in \mathbb{N}$ tal que $Z_n(G) = G$.*
3. *Existe $n \in \mathbb{N}$ tal que $G^n = \{1\}$.*

Definición 51 *Si G es un grupo nilpotente, entonces la **clase de nilpotencia** de G o **clase** de G es la más pequeña $n \geq 0$ tal que $Z_n(G) = G$ y $G^n = \{1\}$.*

Ejemplo 52 *Si $n \geq 3$, entonces el centro del grupo simétrico $G = S_n$ es el subgrupo trivial, $Z_0(G) = Z(G) = \{1\}$. Luego $Z_1(G)/Z_0(G) = Z(G/Z_0(G)) \cong Z(G) = \{1\}$, de donde $Z_2(G) = \{1\}$; en general $Z_i(G) = \{1\}$ y no alcanza a G. Luego S_n no es un grupo nilpotente para $n \geq 3$.*

Con un argumento similar se prueba del siguiente Teorema.

Teorema 53 *Sea G un grupo no trivial. Si $Z(G) = \{1\}$, entonces G no es nilpotente.*

Teorema 54 *Todo p-grupo finito G tiene centro no trivial, es decir, $Z(G) \neq \{1\}$.*

Demostración. Sea G un grupo de orden p^n. Por la ecuación de clase

$$p^n = |G| = |Z(G)| + \sum_{i=|Z(G)|+1}^{k(G)} [G : C_G(x_i)] = \sum_{i=|Z(G)|+1}^{k(G)} p^{u_i} \tag{A.3}$$

donde $|G : C_G(x_i)| = p^{u_i}$ con $u_i \geq 1$. Luego, de (A.3), por divisibilidad, se sigue que $p \mid |Z|$, luego $p \leq |Z|$ y por tanto $Z(G) \neq \{1\}$. ∎

A continuación listamos algunas propiedades de grupos nilpotentes.

Teorema 55 *Sea G un grupo.*

1. *Cualquier subgrupo de un grupo nilpotente es nilpotente, esto es, si $H \leq G$ con G nilpotente, entonces H es nilpotente.*

2. *El grupo cociente de un grupo nilpotente es nilpotente, esto es, si $N \lhd G$ y G es nilpotente, entonces G/N es nilpotente.*

3. *La imagen homomórfa de un grupo nilpotente es nilpotente, esto es, si $\varphi : G \to H$ es un homomorfismo de grupos con G nilpotente, entonces $\varphi(G)$ es nilpotente, donde G tiene clase de nilpotencia n.*

4. *Si $G/Z(G)$ es nilpotente, entonces G es nilpotente.*

Demostración.

1. Sea H un subgrupo del grupo nilpotente G. Tenemos $H^0 = H \subset G = G^0$, $H^1 = [H, H] \subset [G, G] = G^1$; en general, $H^i \subset G^i$ para todo $i \geq 1$. Como G es nilpotente, entonces $G^n = \{1\}$ para algún n. Luego $H^n = \{1\}$. Por tanto, H es nilpotente.

2. Sea $\pi : G \to H$ un homomorfismo sobreyectivo, donde $H = G/N$. Razonado inductivamente $H^0 = H = \pi(G) = \pi(G^0)$ y $H^1 = [H, H] = [\pi(G), \pi(G)] \subset$

$\pi([G,G]) = \pi(G^1)$. En general, $H^i \subset \pi(G^i)$ para cada $i \geq 1$. Como G es nilpontente, entonces existe entero positivo n tal que $G^n = \{1\}$, por lo que $H^n = \{1\}$, luego $H = G/N$ es nilpotente.

3. Sea φ un homomorfismo de G en H dado por, $\varphi(G^i) = (\varphi(G))^i$ para cada $i \in \mathbb{N}$. Como G es nilpotente de clase de nilpotencia n tendremos que, $\varphi(G^{n+1}) = \{1\}$ y como φ es un homomorfismo, se concluye.

$$\varphi(G^{n+1}) = (\varphi(G))^{n+1} = \{1\}.$$

Luego se sigue $\varphi(G)$ es nilpotente de clase de nilpotencia a lo sumo n.

4. Como $G/Z(G)$ es nilpotente existe una serie descendente $G/Z(G) = G^0 \triangleright G^1 \triangleright \cdots \triangleright G^n = \{1\}$, donde $G^i = \frac{H^i}{Z(G)}$ con $H^i \triangleleft G$, por lo tanto $[G/Z(G), H^i/Z(G)] \leq H^{i+1}/Z(G)$ para todo i, entonces $[G, H^i] \leq H^{i+1}$.

Consideraremos la serie: $G = H^0 \triangleright H^1 \triangleright H^3 \triangleright \cdots \triangleright H^n = \{1\}$ para afirmar que G es nilpotente. ■

Teorema 56 *Cualquier p-grupo finito es nilpotente.*

Demostración. Sea G un p-grupo de orden p^n donde p es es un entero primo. Realizamos una demostración por inducción sobre n. Si $n = 1$, entonces $|G| = p$ primo, y como los grupos de orden primo son cíclicos, G es abeliano, por lo que G es nilpotente. Asumimos la hipótesis de inducción para todo entero $< n + 1$. Sea G un grupo tal que $|G| = p^{n+1}$. Los p-grupos tienen centros no triviales, luego $|G/Z(G)| < p^{n+1}$. Por hipótesis de inducción $G/Z(G)$ es nilpotente. Por Teorema 55, G es nilpotente. ■

Lema 57 *Sea G un grupo nilpotente no trivial, entonces* $Z(G) \neq \{e\}$

Demostración. Supongamos que $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G$ es una serie central para G. Sea $G_i = \{e\}$ y $Gi + 1 \neq \{e\}$ para algún entero $i \geq 0$. Como la serie es central se tiene que $G_{i+1}/G_i \leq Z(G/G_i)$ luego resulta $\{e\} \neq G_{i+1} \leq Z(G)$. Por lo tanto, $Z(G) \neq \{e\}$. ■

Teorema 58 *Si $G_1, G_2, \ldots, G_n$ son grupos nilpotentes, entonces $G_1 \times G_2 \times \ldots \times G_n$ es nilpotente.*

Demostración. Probaremos para el caso $n = 2$. Sea $G = H \times K$, con H, K nilpotentes. Entonces existen series de la forma.

$$\{1\} = H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_m = H$$
$$\{1\} = K_0 \triangleleft K_1 \triangleleft \ldots \triangleleft K_n = K$$

entonces $[H, H_i] \leq H_{i-1}$ y $[K, K_i] \leq K_{i-1}$ respectivamente. Repitiendo términos si es necesario, podemos suponer que $n = m$ y se tiene:

$$\{1\} = H_0 \times K_0 \triangleleft H_1 \times K_1 \triangleleft \ldots \triangleleft H_n \times K_n = H \times K$$

como $[H \times K, H_i \times K_i] = [H, H_i] \times [K, K_i] \leq H_{i-1} \times K_{i-1}$, se concluye que $H \times K$ es nilpotente. ■

Teorema 59 *Si G es finito, las siguientes proposiciones son equivalentes:*

1. *G es nilpotente.*
2. *Cada subgrupo de Sylow de G es normal en G.*
3. *G es producto directo de p-grupos para algunos primos p.*

Este teorema esta relacionado con los teoremas de Sylow los cuales en la teoría de grupos, son herramientas importantes para el análisis de subgrupos de un grupo finito G, conocidos como subgrupos de Sylow.

Apéndice B

Grupos solubles

Sea $G^{(0)} = G$, $G^{(1)} = G' = [G, G]$ el subgrupo conmutador de G. Sea $G^{(2)} = (G^{(1)})^{(1)} = [G^{(1)}, G^{(1)}]$. Entonces $G^{(2)} \subset G^{(1)} \subset G^{(0)}$. En general, sea $G^{(i+1)} = (G^{(i)})^{(1)} = [G^{(i)}, G^{(i)}]$ para $i \geq 0$. Tenemos la sucesión

$$G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots \tag{B.1}$$

llamado ***serie derivada*** o ***serie conmutador*** de G. En (B.1), el grupo trivial $\{1\}$ puede ser alcanzado o no.

Definición 60 *Sea G un grupo. Entonces G es un* ***grupo soluble*** *si $G^{(n)} = \{1\}$ para algún entero positivo n; es decir,*

$$G = G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(n)} = \{1\}$$

donde $G^n \triangleleft G$. Si la serie derivada nunca llega al grupo trivial, se dice que G es ***insoluble****.*

Teorema 61 *Todo grupo nilpotente es soluble.*

Demostración. Como $Z_i(G)/Z_{i-1}(G)$ es abeliano, tenemos $Z_i(G)' \leq Z_{i-1}(G)$. Si $Z_n(G) = G$, entonces $G^{(n)} = (Z_n(G))^{(n)} \leq (Z_{(n-1)}(G))^{(n-1)} \leq \cdots \leq Z_0(G) = \{1\}$.

■

Corolario 62 *Cualquier p-grupo finito G es soluble.*

Proposición 63 *Todo subgrupo de un grupo soluble es soluble.*

Demostración. Tenemos $H^{(0)} = H \subset G = G^{(0)}$ y $H^{(1)} = [H, H] \subset [G, G] = G^{(1)}$; generalizando, $H^{(i)} \subset G^{(i)}$ para todo $i \geq 0$. Como G es soluble, entonces existe un entero positivo n tal que $G^{(n)} = \{1\}$, de donde se sigue que $H^{(n)} = \{1\}$, y por tanto H es soluble. ∎

Proposición 64 *La imagen homomórfa de un grupo soluble es soluble.*

Demostración. Sea $f : G \to H$ un epimorfismo de grupos con G un grupo soluble. Probaremos que $f(G^{(n)}) = H^{(n)}$ para todo entero $n \geq 1$. Un elemento de $G^{(1)} = [G, G]$ es de la forma $g = [x_1, y_1]^{\varepsilon_1}[x_2, y_2]^{\varepsilon_2} \cdots [x_s, y_s]^{\varepsilon_s}$ donde $\varepsilon_i \in \{-1, 1\}$. Se sigue inmediatamente que

$$f(g) = [f(x_1), f(y_1)]^{\varepsilon_1}[f(x_2), f(y_2)]^{\varepsilon_2} \cdots [f(x_s), f(y_s)]^{\varepsilon_s} \in [H, H] = H^{(1)},$$

lo que prueba que $f(G^{(1)}) \subset H^{(1)}$. Sea $h \in H^{(1)}$. Sin perdida de generalidad podemos asumir que $h = [u, v]$. Por ser f sobreyectivo, existe $x, y \in G$ tal que $f(x) = u$, $f(y) = v$. Luego $h = [f(x), f(y)] = f([x, y]) \in f(G^{(1)})$. Por tanto $f(G^{(1)}) = H^{(1)} = f(G)^{(1)}$. Asumimos la hipótesis de inducción para n y probamos para $n + 1$. Aplicando el caso $n = 1$ y la hipótesis de inducción tenemos que

$$f(G^{(i+1)}) = f((G^{(i)})^{(1)}) = f(G^{(i)})^{(1)} = (H^{(i)})^{(1)} = H^{(i+1)}.$$

Como G es un grupo soluble, entonces $G^{(n)} = \{1\}$. Luego $H^{(n)} = f(G^{(n)}) = f(\{1\}) = \{1\}$. Por tanto, H es soluble. ∎

Corolario 65 *Todo grupo cociente de un grupo soluble es soluble, esto es, si $N \lhd G$ y G es soluble, entonces G/N es soluble.*

Demostración. Consideremos el homomorfismo proyección $\pi : G \to G/N$ que es sobreyectivo. Por la Proposición 63, $\pi(G) = G/N$ es soluble. ∎

Proposición 66 *Si $N \lhd G$ tal que N y G/N son solubles, entonces G es soluble.*

Demostración. Supongamos que N y G/N son grupos solubles. Entonces existen enteros positivos n y m tales que $(G/N)^{(n)} = \{N\}$ y $N^{(m)} = \{1\}$. Consideremos la proyección $\pi : G \to G/H$. Si $x \in G^{(n)}$, entonces $\pi(x) \in \pi(G^{(n)}) = (G/H)^{(n)} = \{N\}$, luego $\pi(x) = N$, esto es, $xN = N$, luego $x \in N$. Así, $G^{(n)} \subset N$. Luego $G^{(m+n)} = (G^{(n)})^m \subset N^{(m)} = \{1\}$, de donde $G^{(m+n)} = \{1\}$. Por tanto, G es soluble. ■

Teorema 67 *Si $G_1, G_2, \cdots, G_n$ son grupos solubles, entonces $G_1 \times G_2 \times \cdots \times G_n$ es soluble.*

Demostración. Realizaremos la demostracion para $n = 2$, sea $G = H \times K$ donde H y K son grupos solubles, formaremos una serie normal abeliana: Comencemos con $G_0 = \{1_H\} \times \{1_K\}$ donde $1_H, 1_K$ son las identidades de H y K respectivamente. Sea $G_1 = G_{11} \times \{1_K\}$ donde G_{11} es el subgrupo no trivial más pequeño de H en una serie de composición para $\{1_H\} < G_{11} < G_{12} < \ldots < G_{1n_1} = H$ para H. Continuamos construyendo la serie de composición para G colocando estos subgrupos G_{1i} en secuencia en el primer factor de la serie de producto directo hasta llegar a $H \times \{1_K\}$.

Luego comienzamos a poner la secuencia de los subgrupos $G_{21}, G_{22}, \ldots G_{2n_2}$ en una serie de composición para K en el segundo factor hasta que llegue a $G = H \times K = G_{1n_1} \times G_{2n_2}$.

Un grupo de factores formado a partir de dos términos consecutivos de esta serie para G es naturalmente isomorfo a uno de los grupos de factores en una serie de composición para uno de los grupos H según nuestra construcción. Por lo tanto, estos grupos de factores son todos simples, por lo que de hecho hemos construido una composición, una serie de composición para G. Debido a que todos los grupos de factores en la serie de composición para H y K son abelianos, vemos

que los grupos de factores de la serie de composición para G son abelianos, por lo que G es un grupo soluble. ■

Teorema 68 (Burnside) *Sea G es un grupo de orden $p^a \cdot q^b$ con p, q primos y a, b enteros no negativos. Entonces G es soluble.*

El teorema fue demostrado por William Burnside (1904) utilizando la teoría de representación de grupos finitos.

Teorema 69 (Feit-Thompson) *Todo grupo finito de orden impar es soluble.*

En matemáticas, el teorema de Feit-Thompson, o teorema de orden impar, establece que cada grupo finito de orden impar es soluble. Fue probado por Walter Feit y John Griggs Thompson (1962, 1963).

Bibliografía

[1] P. Erdös and P. Turán. (1968). On some problems of statistical group theory, Acta. Math. Acad. Sci. Hung. 413-435.

[2] W. H. Gustafson. (1973). What is the probability that two group elements commute? Amer. Math. Monthly 1031-1034.

[3] G. J. Sherman. (1975). What is the probability an automorphism fixes a group element?, Amer. Math. Monthly 261-264.

[4] M.R.R. Moghaddam, F. Saeedi and E. Khamseh. (2011). The probability of an automorphism fixing a subgroup element of a finite group, Asian-Eur. J. Math. 4 (2), 301-308.

[5] Pournaki, M. R., Sobhani, R. (2008). ?Probabilidad de que el conmutador de dos elementos del grupo sea igual a un elemento dado?, J. Pure and Applied Algebra, vol. 212, págs. 727-734.

[6] MacHale, D. (1974). How commutative can a non-commutative group be? Math. Gaz, 199-202.

[7] Dummit, D. and Foote, M. (1999). Abstract Algebra. New Jersey: Prentice-Hall Inc., 2nd Ed.