UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE MATEMÁTICA

PROYECTO DE GRADO

CARACTERIZACIÓN DE GRUPOS NILPOTENTES FINITOS

Proyecto de grado presentado para la obtención del título de licenciado en Matemática

Por: Neiza Lina Solares Mamani

Tutor: Lic. Ramiro Choque Canaza

LA PAZ - BOLIVIA

2019

AGRADECIMIENTOS

Agradecer en especial a los profesores por compartir sus conocimientos: Ramiro Choque, quién fungió como asesor, a Zenon Condori, Ronnald Silva y Jaime Cazas.

A ti vida por permitirme verme y vivir en ella.

Este es un momento bonito que espero, perdure en el tiempo y el tiempo será el mejor juez.

Por su apoyo padres, gracias.

Índice general

CAPÍTULO 1

Introducción

1.1. Introducción

Hasta ahora, después de estudiar los grupos, subgrupos, cocientes y homomorfismos, el primer teorema genérico sobre grupos finitos que probamos es el teorema de Lagrange, el cual restringe el orden de los subgrupos que un grupo finito dado puede tener. Llegamos a un punto en el cual podemos probar los recíprocos parciales del teorema de Lagrange y que constituyen el inicio del estudio de los grupos finitos, a partir de los teoremas de Sylow. Presentaremos resultados sobre la teoría de p-grupos, y entre ellos los teoremas de Sylow.

Introduciremos el cálculo conmutador, es una de las herramientas mas importantes para estudiar grupos nilpotentes. El centro de un grupo y otras nociones que rodean el concepto de conmutatividad son definidos. Por definición el conmutador de dos elementos g, h en un grupo G es el elemento $[g, h] = g^{-1}h^{-1}gh$. Claramente $[g, h] = e$ cuando g y h conmutan. Esto conduce a una natural conexión entre elementos centrales y conmutadores triviales.

Perseguiremos el estudio de grupos en un nivel más profundo. Un método de investigación común en álgebra es romper una estructura compleja es simples subestructuras. Entonces puede ser posible en algún sentido sintetizar esas subestructuras para reconstruir la estructura original. Para esto el concepto básico es el de serie de un grupo G,

esto significa una cadena finita de subgrupos de G.

Probaremos el Teorema de Jordan-Hölder que proporciona detalles sobre una determinada serie, llamada serie de composición, afirma que el conjunto de grupos simples G_i (los factores de composición) esta unívocamente determinado por G, es decir no depende de la serie elegida. Se podría decir que los grupos simples juegan en la teoría de grupos finitos el papel que los números primos hacen en la teoría de números. Un grupo G es simple si no tiene subgrupos normales (salvo $\{e\}$ y G).

A partir de reiteradas operaciones de centros y conmutadores sobre el grupo G se generará la serie central, y en elgún número positivo la serie central se estabiliza. Así diremos que el grupo G es nilpotente. La clase de grupos nilpotentes es cerrada bajo subgrupos, la imagen homomórfica, grupos cocientes y productos directos finitos, por ejemplo, probaremos que cada subgrupo de un grupo nilpotente es subnormal, y así satisface el llamado condición normalizador. Entre los ejemplos clásicos de grupo nilpotente, cada p-grupo finito es nilpotente, p un número primo. Todo grupo abeliano es nilpotente, de esto lograremos probar el teorema de la estructura de grupos finitos abelianos.

Los grupos nilpotentes se encuentran entre las clases de grupos abelianos y solubles, es decir todo grupo abeliano es nilpotente y todo grupo nilpotente es soluble.

Para terminar exhibiremos un teorema sobre la caracterización de un grupo nilpotente finito, que nos permitirá determinar la nilotencia del grupo. Y para concluir un criterio de grupo nilpotente por el subgrupo de Frattini.

1.2. Justificación

La teoría de grupos nilpotentes finitos forma parte de la estructura de grupos finitos.

El teorema que consiste en demostrar equivalencias de otras propiedades de grupos, nos da una caracterización de grupos nilpotentes finitos que proporcionaran una elección para mostrar que un grupo es nilpotente finito. Esto deriva a criterio propio su elección para la demostración de proposiciones que impliquen la nilpotencia de un grupo, con el rigor de justificar su razonamiento.

1.3. Importancia y aportes

Los grupos nilpotentes son proximos a los grupos abelianos. Mas aún se parecen a los grupos abelianos, el caso particular es que todo grupo abeliano es nilpotente y no así el recíproco.

En la teoría de nudos, resultados pueden ser reescritos en términos de teoría de grupos, es el caso de que el invariante de nudos esta relacionada con la condición de nilpotencia, es decir "*El invariante de nudos F_G es constante si y sólo si el grupo G es nilpotente*". Hoy en día el alcance de la Teoría de Nudos se extiende por fuera del campo de la matemática, en Biología, en el estudio de replicación y recombinación del ADN. En física los grupos nilpotentes se relacionan con la cuatificación de la deformación (relacionada con la rotación).

1.4. Antecedentes

Un resultado ya conocido en teoría de grupos, antes de 1964 es el siguiente:

Si un grupo G es nilpotente, entonces todos sus subgrupos son subnormales. (*)

Una pregunta natural que surgió fue sobre la validez de la recíproca de (*). El primer paso en este sentido fue dado por R. Dedekind en (1897), que determinó todos los grupos finitos tal que cada uno de sus subgrupos sean normales. Mas tarde en 1933, R.Baer extendió este resultado para los grupos arbitrarios (infinitos).

Roseblade, en (1964), consiguió probar que para un grupo ser nilpotente, es suficiente que sus subgrupos sean subnormales.

1.5. Planteamiento del Problema

En la teoría del anillo, un elemento a se llama nilpotente si no es cero y este en alguna potencia positiva es cero. Un tratamiento análogo en teoría de grupos es el estudio de grupos nilpotentes. Es decir, aplicando reiteradas operaciones sobre el grupo, la serie ascendente se estabiliza alcanzando el grupo G y similarmente la serie descendente se estabiliza alcanzando el grupo trivial. Esto proporciona una clase de nilpotencia, que

es una medida de a qué distancia de un abeliano se encuentra un grupo nilpotente. Luego a partir del subgrupo subnormal, la condición de normalizador, el subgrupo maximal y el subgrupo de Sylow, se busca dar condiciones equivalentes que sean facilmente aplicables para determinar si el grupo es o no nilpotente finito.

1.5.1. Problema

A partir de las condiciones equivalentes que nos permitirán determinar la nilpotencia de un grupo finito, ¿cómo reunir tales condiciones y presentar una caracterización sobre grupos nilpotentes finitos?

1.6. Objetivos

Objetivo General: Establecer una caracterización sobre grupos nilpotentes finitos, a partir de la teoría a desarrollar.

Objetivo Específico:

* Introducir serie central de un grupo, empleando la noción del conmutador y el centro de un grupo.

* Estudiar propiedades de los grupos nilpotentes.

* Mostrar a partir de las afirmaciones del Teorema (1.1), el teorema de estructura de los grupos finitos abelianos.

1.7. Marco teórico

Los enunciados que forman parte del teorema tienen un significado preciso en la teoría de grupo nilpotente finito.

Teorema 1.1. *(Teorema sobre la Caracterización de Grupos Nilpotentes Finitos.) Sea G un grupo finito. Los siguientes son equivalentes:*

1. *G es nilpotente;*

2. *Cada subgrupo de G es subnormal en G;*

3. *G satisface la condición de normalizador;*

4. *Cada subgrupo maximal de G es normal en G;*

5. *Cada subgrupo Sylow de G es normal en G;*

6. *G es isomorfo al producto directo de sus subgrupos de Sylow;*

7. *Si $a, b \in G$ y $(|a|, |b|) = 1$, entonces a y b conmutan en G.*

1.8. Alcance

Estudio de la teoría de grupos nilpotentes finitos y teoría necesaria para demostrar el Teorema (1.1). Mas aún un criterio a partir del subgrupo de Frattini.

1.9. Metodología

1. **No presencial**: Trabajo personal del estudiante

   * Estudio de textos y artículos citados referentes al tema de estudio previos a la exposición.

   * Preparación y elaboración del trabajo de proyecto de grado.

2. **Presencial**: Interacción profesor-estudiante

   * Seminarios: Desarrollo del contenido teórico en pizarra y el uso de equipos de visualización, como apoyo a la presentación oral.

   * Tutorias: Resolución de las dudas que surjan durante el desarrollo del contenido teórico y seguimiento del trabajo.

   * Exposición/Defensa: Exposición y defensa del trabajo de proyecto de grado, utilizando los equipos oportunos para la visualización.

CAPÍTULO 2

Cálculo del Conmutador

En la primera sección, el conjugado de elementos y subgrupos como el centro de un grupo son definidos. Resultados y ejemplos que involucran el centro de un grupo son dados. En la segunda sección, trata las identidades relacionadas al grupo conmutador de elementos. Esto lleva a una conexión natural entre elementos centrales y el conmutador trivial. En la tercera y cuarta sección, el subgrupo conmutador como sus propiedades son presentados.

2.1. Conjugados y elementos centrales

Definición 2.1. Conjugados

Sean g, h elementos de un grupo G. El conjugado de g por h, denotado por g^h, es el elemento $h^{-1}gh$ de G.

Teorema 2.1. *Supongamos que g, h y k son elementos del grupo G. Entonces $(gh)^k = g^k h^k$, $(g^{-1})^h = (g^h)^{-1}$ y $(g^h)^k = g^{hk}$.*

Demostración.

$$(gh)^k = k^{-1}ghk = k^{-1}g(kk^{-1})hk = (k^{-1}gk)(k^{-1}hk) = g^k h^k.$$

$$(g^{-1})^h = h^{-1}g^{-1}h = (h^{-1}gh)^{-1} = (g^h)^{-1}.$$

$$(g^h)^k = (h^{-1}gh)^k = k^{-1}h^{-1}ghk = (hk)^{-1}g(hk) = g^{hk}.$$

□

Definición 2.2. Subgrupos Conjugados

Sean H y K subgrupos de un grupo G. Decimos que H y K son conjugados en G si hay un elemento g en G tal que $H = g^{-1}Kg$.

En particular, cada subgrupo normal de G es conjugado así mismo.

Definición 2.3. El centro $Z(G)$

Sea G un grupo, un elemento $g \in G$ es llamado central si este conmuta con cada elemento de G.

El conjunto de todos los elementos centrales de G es llamado el centro de G y es denotado por $Z(G)$. Así

$$Z(G) = \{g \in G : gh = hg \text{ para todo } h \in G\}$$

$$= \{g \in G : g^h = g \text{ para todo } h \in G\}.$$

- Es inmediato comprobar que si G es abeliano, si y sólo si $G = Z(G)$.
- El centro $Z(G)$ es un subgrupo normal abeliano de G.

Sean G y H grupos, entonces el producto directo de G y H será escrito como $G \times H$.

Teorema 2.2. *Sean H y K grupos, entonces $Z(H \times K) = Z(H) \times Z(K)$*

Demostración. Sea $(h,k) \in Z(H \times K)$ entonces $(h,k)(x,y) = (x,y)(h,k)$ para todo $(x,y) \in H \times K$ luego $(hx, ky) = (xh, yk)$, para todo $x \in H$ y para todo $y \in K$, tal que $hx = xh$ para todo $x \in H$ y $ky = yk$ para todo $y \in K$, por tanto $h \in Z(H)$ y $k \in Z(K)$ esto es $(h,k) \in Z(H) \times Z(K)$.

El recíproco se muestra de manera análoga. □

Corolario 2.3. *Si $G = G_1 \times \cdots \times G_n$, entonces $Z(G) = Z(G_1) \times Z(G_n)$.*

Teorema 2.4. *Sean G_1 y G_2 cualesquiera dos grupos, entonces*

$$\frac{(G_1 \times G_2)}{Z(G_1 \times G_2)} \cong \frac{G_1}{Z(G_1)} \times \frac{G_2}{Z(G_2)}$$

Demostración. El mapeo $\gamma : G_1 \times G_2 \to (\frac{G_1}{Z(G_1)}) \times (\frac{G_2}{Z(G_2)})$ definida por

$$\gamma(g_1, g_2) = (g_1 Z(G_1),\ g_2 Z(G_2))$$

es un homomorfismo sobreyectivo natural, cuyo kernel es $Z(G_1 \times G_2)$, en efecto $\gamma(g_1, g_2) = (g_1 Z(G_1),\ g_2 Z(G_2))$. Así por el primer teorema de isomorfismo se tiene

$$\frac{G_1 \times G_2}{Ker(\gamma)} \cong Im(\gamma).$$

Es decir

$$\frac{(G_1 \times G_2)}{Z(G_1 \times G_2)} \cong \frac{G_1}{Z(G_1)} \times \frac{G_2}{Z(G_2)}$$

□

Ejemplo 1. *Sea S_n el grupo simétrico sobre el conjunto $S = \{1, 2, \ldots, n\}$, y sea e el elemento identidad de S_n, S_1 tiene centro trivial pues $S_1 = \{e\}$. Mas aún, $Z(S_2) = S_2$, pues S_2 es abeliano.*

Mostraremos que $Z(S_n) = \{e\}$ para $n > 2$. Supongamos, lo contrario, que $Z(S_n)$ es no trivial. Sea $e \neq \sigma \in Z(S_n)$. Queremos encontrar $\tau \in S_n$ tal que $\sigma\tau \neq \tau\sigma$. Como $\sigma \neq e$, existe $a,\ b \in S$ $a \neq b$, tal que $\sigma(a) = b$. Sea $\tau \in S_n$ tal que $\tau(b) = c$ y $\tau(a) = a$, donde $c \in S - \{a,\ b\}$. Entonces

$$(\tau \circ \sigma)(a) = \tau(\sigma(a)) = \tau(b) = c \tag{2.1.1}$$

$$(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = b \tag{2.1.2}$$

En consecuencia de (2.1.1) y (2.1.2) se tiene $(\tau \circ \sigma)(a) \neq (\sigma \circ \tau)(a)$. Por tanto σ no esta en el centro de $Z(S_n)$. Luego la única permutación que esta en $Z(S_n)$ es e.

Ejemplo 2. *Sea A_n el grupo alternado sobre el conjunto $S = \{1, 2, \ldots, n\}$. Este es el subgrupo de S_n consistiendo de todas las permutaciones pares. Notemos que $A_1 = A_2 = \{e\}$, y A_3 es el grupo cíclico, pues tiene orden 3. Por tanto, $Z(A_n) = A_n$ para $n = 1, 2, 3$, pues los grupos son abelianos.*

El centro de A_4 es trivial, la prueba es similar al ejemplo 1, asumamos que $Z(A_4)$ es no trivial, sea $\sigma \neq e$ un elemento de $Z(A_4)$. Luego existe elementos $a, b \in S$, tal que $\sigma(a) = b$. Ahora sean $c, d \in S$ diferentes de a y b, y sea $\tau = (b\ c\ d)$. Luego

$(\sigma \circ \tau)(a) \neq (\tau \circ \sigma)(a)$, *contradicción.*

Ahora el grupo A_n *es simple (definición- 3.5) para* $n \geq 5$. *Entonces,* $Z(A_n) = A_n$ *o* $Z(A_n) = \{e\}$. *Si* $Z(A_n) = A_n$, *entonces* A_n *debería ser abeliano, esto no es cierto, pues*

$$(1\ 2\ 3)(3\ 4\ 5) \neq (3\ 4\ 5)(1\ 2\ 3).$$

Así A_n *no es abeliano. Por tanto* $Z(A_n) = \{e\}$ *para* $n \geq 5$.

2.1.1. Subgrupo central y el centralizador

Definición 2.4. Subgrupo central

Un subgrupo H *de un grupo* G *es llamado central si* $H \leq Z(G)$.

- Es inmediato comprobar que: Si $H \leq Z(G)$ entonces $H \trianglelefteq G$.

Relativo al centro de un grupo es el centralizador de un subconjunto de un grupo.

Definición 2.5. El centralizador

El centralizador de un subconjunto no vacío X *de un grupo* G *es:*

$$C_G(X) = \{g \in G : g^{-1}xg = x,\ \forall x \in X\} = \{g \in G : xg = gx,\ \forall x \in X\}$$

- Si $X = \{x\}$, entonces escribimos $C_G(x)$, el centralizador de x.
- $C_G(X) \leq G$.
- Si $X = G$, $C_G(G) = Z(G)$.
- $\bigcap_{x \in G} C_G(x) = Z(G)$.
- Si $H \leq G$, $C_G(H) = \bigcap_{h \in H} C_G(h)$.

2.1.2. El centro de un p-Grupo

Definición 2.6. *Sea* p *cualquier primo. Un grupo* G *es llamado un* p*-grupo si cada elemento de* G *tiene orden una potencia de* p.

Teorema 2.5. *Sea* G *un* p*-grupo finito no trivial para algún primo* p, *entonces* $Z(G) \neq \{e\}$.

Demostración. Supongamos que $|G| = n$. Consideremos la ecuación de clase de G

$$|G| = |Z(G)| + \sum_k [G : C_G(x_k)].$$

Sea $x_k \in G$ un elemento no central para algún $1 \leq k \leq n$, entonces $C_G(x_k)$ es un subgrupo propio de G, es decir $x_k \notin Z(G)$, entonces $C_G(x_k) \neq G$. Luego, $[G : C_G(x_k)]$ es una potencia positiva de p. Consecuentemente, cada sumando en la suma

$$\sum_k [G : C_G(x_k)]$$

es divisible por p. Como p divide $|G|$ por hipótesis, p también divide $|Z(G)|$. Por tanto, $Z(G)$ contiene elementos no triviales. Por tanto $Z(G)$ tiene al menos p elementos. □

2.2. El conmutador de elementos de un grupo

En esta sección definiremos el conmutador de elementos de un grupo.

Definición 2.7. *Sean g y h elementos de un grupo G. El conmutador de g y h, denotado como $[g, h]$ es:*

$$[g, h] = g^{-1}h^{-1}gh = g^{-1}g^h$$

Si g, h conmutan, se tiene $[g, h] = e$.

Así, el centro de G también se puede escribir como:

$$Z(G) = \{g \in G \mid [g, h] = e, \ \ \forall h \in G\}.$$

Sea $S = \{g_1, g_2, \ldots, g_n\}$ un conjunto de elementos de un grupo G. El conmutador, de peso $n \geq 1$ es definido recursivamente como sigue:

1. El conmutador simple de peso 1, escrito como $g_j = [g_j]$.

2. El conmutador simple de peso $n > 1$, escrito como $[g_1, g_2, \ldots, g_n] = [[g_1, \ldots, g_{n-1}], g_n]$.

Coleccionaremos algunas identidades que son de suma importancia.

Lema 2.1. *Sean x, y y z elementos de un grupo G.*

(i) $xy = yx[x, y]$.

(ii) $x^y = x[x, y]$.

(iii) $[x, y] = [y, x]^{-1}$.

(iv) $[x, y]^z = [x^z, y^z]$.

Demostración. (i) $xy = yx(x^{-1}y^{-1}xy) = yx[x, y]$.

(ii) $x^y = y^{-1}xy = x(x^{-1}y^{-1}xy) = x[x, y]$.

(iii) $[x, y] = x^{-1}y^{-1}xy = (y^{-1}x^{-1}yx)^{-1} = [y, x]^{-1}$.

(iv) $[x, y]^z = z^{-1}(x^{-1}y^{-1}xy)z = (z^{-1}xz)^{-1}(z^{-1}yz)^{-1}(z^{-1}xz)(z^{-1}yz) = [x^z, y^z]$. □

2.3. Subgrupo conmutador

La noción del conmutador de elementos de un grupo puede ser generalizado al conmutador de subconjuntos de un grupo.

Definición 2.8. *Sea G un grupo con $S = \{s_1, s_2, \ldots\}$ subconjunto de G. El subgrupo de G generado por S, se denota por*

$$\langle S\rangle = \langle\{s_1, s_2, \ldots\}\rangle,$$

es el subgrupo mas pequeño de G conteniendo a S.

El subgrupo $\langle S\rangle$ de G puede ser obtenido tomando la intersección de todos los subgrupos de G que contienen a S.

Un elemento típico de $\langle S\rangle$ es de la forma

$$s_{i_1}^{\mathscr{E}_1} s_{i_2}^{\mathscr{E}_2} \cdots s_{i_n}^{\mathscr{E}_n}$$

donde $s_{i_j} \in S$ y $\mathscr{E}_j \in \{-1, 1\}$ para $1 \leq j \leq n$.

Observación:

- Sea $g \in G$, entonces $\langle g\rangle$ es justo el subgrupo cíclico de G generado por g. Los elementos de $\langle g\rangle$ son de la forma:

$$\langle g\rangle = \{e, g, g^2, g^3, \ldots, g^n, \ldots \mid n \in \mathbb{Z}\}.$$

- Sean $g, h \in G$, entonces $\langle g, h\rangle$ es el subgrupo de G generado por g y h. Los elementos de $\langle g, h\rangle$ son de la forma:

$$\langle g, h\rangle = \{e, g, h, gh, g^2h^2, g^{-3}h^4, \ldots, g^m h^n, \ldots \mid m, n \in \mathbb{Z}\}.$$

Reescribiendo los elementos de $\langle g, h\rangle$

$$\langle g, h\rangle = \{e, g, h, gh, gghh, g^{-1}g^{-1}g^{-1}hhhh, \ldots, \underbrace{gg\cdots g}_{m-\text{veces}}\underbrace{hh\cdots h}_{n-\text{veces}}, \ldots \mid m, n \in \mathbb{Z}\}.$$

Así un elemento de $\langle g, h\rangle$ es de la forma $g_{i_1}^{\mathscr{E}_1}h_{i_2}^{\mathscr{E}_2}$, $\mathscr{E}_j \in \{-1, 1\}$ para $j = 1, 2$.

Definición 2.9. *Sean X_1 y X_2 subconjuntos no vacíos de un grupo G. Definimos el subgrupo conmutador de X_1 y X_2 como:*

$$[X_1, X_2] = \langle\{[x_1, x_2] |\ x_1 \in X_1,\ \ x_2 \in X_2\}\rangle$$

Así $[X_1, X_2]$ es el subgrupo de G generado por todos los conmutadores $[x_1, x_2]$, donde x_1 varía sobre X_1 y x_2 varía sobre X_2.

En el caso especial en que $X_1 = X_2 = G$, el subgrupo conmutador $[G, G]$ se denota por G', también nos referiremos a G' como el subgrupo derivado de G.

Remarca 1. *El conjunto de todos los conmutadores*

$$S = \{[x_1, x_2] \mid x_1 \in X_1,\ \ x_2 \in X_2\}$$

no necesariamente forma un subgrupo de G. Por ejemplo $[x_1, x_2]^{-1}$ puede no estar en S para algún $[x_1, x_2] \in S$.

La definición 2.9 puede ser generalizado. Si $\{X_1, X_2, \ldots\}$ es una colección no vacía de subconjuntos de G, entonces:

$$[X_1, X_2, \ldots, X_n] = [[X_1, \ldots, X_{n-1}], X_n],\ \ n \geq 2.$$

Note que $[X_1, X_2, \ldots, X_n]$ contiene todos los conmutadores simples de la forma $[x_1, x_2, \ldots, x_n]$, donde $x_1 \in X_1, \ldots, x_n \in X_n$.
Así $[X_1, X_2, \ldots, X_n] \geq \langle\{[x_1, x_2, \ldots, x_n] |\ x_i \in X_i,\ i = 1, \ldots, n\}\rangle$.

Lema 2.2. *Sea G cualquier grupo.*
(i) Si $H \leq G$ y $[G, G] \leq H$, entonces $H \trianglelefteq G$ y G/H es abeliano. Así, $[G, G] \trianglelefteq G$ y $G/[G, G]$ es abeliano.
(ii) Si $N \trianglelefteq G$ y G/N es abeliano, entonces $[G, G] \trianglelefteq N$.

Demostración. (i) Sea $g \in G$ y $h \in H$.

$$h^g = g^{-1}hg = hh^{-1}g^{-1}hg = h[h,\ g] \in H,$$

porque H contiene a $[G,\ G]$. Así $h^g \in H\ \ \forall h \in H$, luego $H \trianglelefteq G$. Sean g_1H y g_2H elementos de G/H. Entonces

$$[g_1H,\ g_2H] = [g_1,\ g_2]H = H.$$

Por tanto G/H es abeliano.
(ii) Si $gN,\ hN \in G/N$, para $g, h \in G$. Como G/N es abeliano, entonces $[gN,\ hN] = N$. Por lo tanto

$$[g,\ h]N = N \Leftrightarrow [g,\ h] \in N$$

luego $[G,G] \leq N$, para $g,\ h \in G$. Sea $n \in N$, $[g,\ h]^n = [g^n,\ h^n] \in [G,G]$. Se deduce que $[G,G] \trianglelefteq N$. □

Así el subgrupo conmutador de un grupo es el subgrupo normal mas pequeño, que induce un cociente abeliano.
El grupo factor $Ab(G) = G/[G,G]$ es llamado la *abelianización* de G.

Ejemplo 3. *Cualquiera dos elementos de un grupo abeliano conmutan. Así* $[G,G] = \{e\}$.

Ejemplo 4. *Calcularemos el subgrupo conmutador del grupo alternado* A_n *sobre el conjunto* $S = \{1, 2, \ldots, n\}$. *Es claro* $[A_n, A_n] = \{e\}$ *para* $n = 1, 2, 3$ *por el Ejemplo 3. Ahora calculemos el subgrupo conmutador de* A_4. *Notemos que* A_4 *contiene un único subgrupo normal no trivial*

$$K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$

es el grupo de Klein. Como $[A_4 : K] = 3$, *así* A_4/K *es abeliano. Por tanto* $[A_4, A_4] \trianglelefteq K$ *por Lema (2.2-ii), y así* $[A_4, A_4] = K$.
Consideremos, el caso cuando $n \geq 5$. *En este caso* A_n *es simple. Así, los únicos subgrupos normales son* $\{e\}$ *y* A_n. *Como* A_n *es no abeliano, entonces se sigue que* $[A_n, A_n] = A_n$.

Ejemplo 5. *Calcularemos el subgrupo conmutador del grupo simétrico S_n sobre el conjunto $S = \{1, 2, \ldots, n\}$. Por el Ejemplo 3, $[S_n, S_n] = \{e\}$ para $n = 1, 2$.*
Con el fin de encontrar $[S_n, S_n]$ para $n \geq 3$, usaremos el hecho que A_n es un subgrupo normal de índice 2 en S_n, y así S_n/A_n es un grupo abeliano. Primero, encontraremos $[S_3, S_3]$. Como S_3/A_3 es abeliano, por Lema (2.2-ii) $[S_3, S_3] \trianglelefteq A_3$. Mas aún, cada elemento de A_3 puede ser escrito como un conmutador de elementos en S_3, por ejemplo

$$(1\ 2\ 3) = [(2\ 3), (1\ 3\ 2)] \ \ y \ \ (1\ 3\ 2) = [(2\ 3), (1\ 2\ 3)].$$

Por tanto, A_3 esta contenido en $[S_3, S_3]$, así se tiene que $[S_3, S_3] = A_3$.
Mostraremos que, $[S_4, S_4] = A_4$. Sea $(a\ \ b\ c)$ cualquier 3-ciclo para $a, b, c \in S$ distintos. Este 3-ciclo puede ser escrito como el conmutador de elementos en S_4 como

$$(a\ \ b\ c) = [(a\ b), (a\ c\ b)].$$

Se sigue que $A_4 \leq [S_4, S_4]$ pues A_4 es generado por 3-ciclos. Como S_4/A_4 es abeliano, por Lema (2.2-ii) $[S_4, S_4] \trianglelefteq A_4$. Concluimos que $[S_4, S_4] = A_4$.
Finalmente, el caso cuando $n \geq 5$. De nuevo se tiene $[S_n, S_n] \trianglelefteq A_n$ pues S_n/A_n es abeliano. Luego, como el único subgrupo normal no trivial de S_n es A_n. Por tanto $[S_n, S_n] = A_n$.

2.4. Propiedades del subgrupo conmutador

Recogemos varias propiedades de subgrupo conmutador.

Definición 2.10. ***El normalizador:***
Sea G un grupo cualquiera, y sea S un subconjunto no vacío de G. El normalizador de S en G, denotado por $N_G(S)$, es

$$N_G(S) = \{g \in G \mid gS = Sg\}.$$

Sea H un subgrupo de G, entonces $N_G(H)$ es el subgrupo mas grande de G respecto a la relación de orden inclusión. Es decir, si $K \leq G$, entonces $K \leq N_G(H)$.
K con esa propiedad, decimos que K normaliza H, si $K \leq N_G(H)$. Claramente $N_G(H) = G$ si, y sólo si $H \trianglelefteq G$.

- $N_G(S) \leq G$.
- $C_G(S) \leq N_G(S)$.

Proposición 1. *Sea G un grupo cualquiera con subgrupos H y K.*
(i) $[H, K] = [K, H]$.
(ii) $[H, K] \leq H$ si, y sólo si K normaliza H. En particular, $[H, G] \leq H$ si, y sólo si $H \trianglelefteq G$.
(iii) Si $H_1 \leq G$ y $K_1 \leq G$ tal que $H_1 \leq H$ y $K_1 \leq K$, entonces $[H_1, K_1] \leq [H, K]$.

Demostración. (i) Por lema (2.1) (iii)

$$\begin{aligned}
[H, K] &= \langle\{[h, k] \mid h \in H,\ k \in K)\}\rangle \\
&= \langle\{[k, h]^{-1} \mid h \in H,\ k \in K\}\rangle \\
&= \langle\{([k,\ h]^{-1})^{-1} |\ h \in H,\ k \in K\}\rangle \\
&= \langle\{[k,\ h]|\ k \in K,\ h \in H\}\rangle \\
&= [K,\ H].
\end{aligned}$$

(ii) Si $[H, K] \leq H$, entonces $[h, k] \in H$ para cualquier $h \in H$ y $k \in K$, $h^{-1}k^{-1}hk \in H$. Esto significa que $k^{-1}hk \in H$, y consecuentemente, $k^{-1}Hk \leq H$.
Sea $h \in H$, entonces $h[h, k] = h^k \in H$. Sea $h_1 = h^k = k^{-1}hk \in k^{-1}Hk$, luego $H \leq k^{-1}Hk$. Por tanto $k^{-1}Hk = H$; es decir $k \in N_G(H)$, esto es $K \leq N_G(H)$.

Recíprocamente, como $K \leq N_G(H)$, esto es $k^{-1}Hk = H$. Sean $h \in H$, $k \in K$, entonces $k^{-1}hk \in H$, luego $h^{-1}k^{-1}hk \in H$, esto es $[h, k] \in H$. Por tanto $[H, K] \leq H$.
(iii) Para $h_1 \in H_1$ y $k_1 \in K_1$, $[h_1, k_1] = h_1^{-1}k_1^{-1}h_1k_1 \in [H, K]$. □

Proposición 2. *Sean G y H grupos, y sean G_1 y G_2 subgrupos de G. Si $\theta \in Hom(G,\ H)$, entonces $\theta([G_1,\ G_2]) = [\theta(G_1),\ \theta(G_2)]$.*

Demostración. Sean $g_{1_j} \in G_1$, $g_{2_j} \in G_2$, y $\varepsilon_j \in \{-1,\ 1\}$ para $1 \leq j \leq k$, entonces

$$\theta\left(\prod_{j=1}^{k}[g_{1_j},\ g_{2_j}]^{\varepsilon_j}\right) = \prod_{j=1}^{k}\theta\left([g_{1_j},\ g_{2_j}]\right)^{\varepsilon_j}$$

$$= \prod_{j=1}^{k} \theta\left(g_{1_j}^{-1} g_{2_j}^{-1} g_{1_j} g_{2_j}\right)^{\varepsilon_j}$$
$$= \prod_{j=1}^{k} \left[\theta\left(g_{1_j}\right)^{-1} \theta\left(g_{2_j}\right)^{-1} \theta\left(g_{1_j}\right) \theta\left(g_{2_j}\right)\right]^{\varepsilon_j}$$
$$= \prod_{j=1}^{k} \left[\theta\left(g_{1_j}\right),\ \theta\left(g_{2_j}\right)\right]^{\varepsilon_j}.$$

□

Lema 2.3. *Sea G un grupo y suponga que $N \trianglelefteq G$ y $H \leq G$. Entonces $[H, G] \leq N$ si, y sólo si $HN/N \leq Z(G/N)$.*

Demostración. Supongamos que $[H, G] \leq N$, y sea $hN \in HN/N$ con $h \in HN$. Por demostrar que $hN \in Z(G/N)$. Sea $gN \in G/N$ donde $g \in G$. Existe $h' \in H$ y $n \in N$ tal que $h = h'n$. Luego

$$[hN, gN] = [h'n, g]N = [h'nN, gN] = [h'N, gN] = [h', g]N = N$$

para todo $gN \in G/N$, donde $hN \in Z(G/N)$.
Recíprocamente, sea $h \in H$ y $g \in G$. Entonces $h = he \in HN$. Luego $hN \in HN/N$, y por hipótesis $hN \in Z(G/N)$. De donde $[hN, gN] = N$, es decir $[h, g]N = N$, y por tanto $[h, g] \in N$. Se sigue que $[H, G] \leq N$. □

Teorema 2.6. *Sea G un grupo. Si H y K son subgrupos normales de G, entonces $[H, K] \trianglelefteq G$.*

Demostración. Supongamos que $g \in G$ y $\prod_{i=1}^{n} [h_i, k_i]^{\mathscr{E}_i} \in [H, K]$, donde $h_i \in H$, $k_i \in K$, y $\mathscr{E}_i \in \{-1, 1\}$ por Teorema (2.1) y Lema (2.1-iv)

$$\left([h_1, k_1]^{\mathscr{E}_1} [h_2, k_2]^{\mathscr{E}_2} \cdots [h_n, k_n]^{\mathscr{E}_n}\right)^g = \left([h_1, k_1]^{\mathscr{E}_1}\right)^g \left([h_2, k_2]^{\mathscr{E}_2}\right)^g \cdots \left([h_n, k_n]^{\mathscr{E}_n}\right)^g$$
$$= \left([h_1^g, k_1^g]^{\mathscr{E}_1}\right) \left([h_2^g, k_2^g]^{\mathscr{E}_2}\right) \cdots \left([h_n^g, k_n^g]^{\mathscr{E}_n}\right)$$

esta contenido en $[H, K]$, pues H y K son subgrupos normales en G. Así $[H, K] \trianglelefteq G$. □

Corolario 2.7. *Sean $G_1, \ldots, G_n$ subgrupos normales de G, entonces $[G_1, \ldots, G_n]$ es subgrupo normal de G.*

CAPÍTULO 3

Series Normales

Definimos serie de un grupo dado. Se exponen varios resultados y propiedades de series normales y subnormales de un grupo G. De estos resultados el más destacado es el conocido teorema de Jordan Hölder.

3.1. Series: Subnormales, normales y de composición

Definición 3.1. Series

Dado un grupo G y un subgrupo J de G, una serie de J a G es una sucesión finita

$$J = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n = G \tag{3.1.1}$$

de subgrupos de G, donde cada G_i es un subgrupo de su sucesor.

Si $J = \{e\}$, diremos que (3.1.1) es también una serie de G.

✓ Los subgrupos G_i en esta serie son llamados *términos.*

✓ Si $G_i \trianglelefteq G_{i+1}$, el grupo factor $\dfrac{G_{i+1}}{G_i}$ es llamado un factor de la serie.

✓ La *longitud* de la serie es el número de inclusiones estrictas (o alternativamente, el número de factores no triviales).

✓ Una serie es llamado *propio* si dos términos no son iguales, esto es, $G_i < G_{i+1}$ para $i = 0, \ldots, n-1$.

✓ Una segunda serie $J = K_0 \leq K_1 \leq K_2 \leq \cdots \leq K_m = G$ es llamado un *refinamiento* de la primera serie si cada término G_i en (3.1.1), es también un término en la segunda serie.

✓ El refinamiento dada arriba es llamado propio si hay al menos un término, que no es un término de la primera serie.

Estudiaremos tres clases especiales de series dadas por:

Definición 3.2. ***(i)*** *La serie es llamada* normal *si* $G_i \trianglelefteq G$, *para* $i = 0, ..., n$.
(ii) *Una serie es llamada* subnormal *si* $G_{i-1} \trianglelefteq G_i$ *para* $1 \leq i \leq n$.
(iii) *Una serie subnormal propia de* G *es llamado una* serie de composición *de* G, *si este no tiene refinamiento subnormal propio. Los factores de una serie de composición son llamados factores de composición.*

Claramente, cada serie normal de un grupo es subnormal.

Afirmación 1. *Una serie subnormal no necesariamente es una serie normal.*

Demostración. Encontrar subgrupos H y K de D_4^* tales que $H \triangleleft K$ y $K \triangleleft D_4^*$ es decir $(H \triangleleft K \triangleleft D_4^*)$, pero H no es normal en D_4^*.

Recordemos al grupo D_4^* (simetrías del cuadrado). Consideremos un cuadrado cuyos vértices estén enumerados en forma consecutiva 1, 2, 3 y 4. Sea D_4^* el conjunto de las transformaciones del cuadrado.

$$D_4^* = \{R, R^2, R^3, R^4, T_x, T_y, T_{1,3}, T_{2,4}\}$$

donde: R es la rotación de 90^o (antihorario), R^2, R^3 y R^4 ó (e) rotación de 180^o, 270^o y 360^o (antihorario) respectivamente.
T_x es la reflexión sobre el eje x, T_y es la reflexión sobre el eje y, $T_{1,3}$ es la reflexión sobre la diagonal (1, 3), $T_{2,4}$ es la reflexión sobre la diagonal (2, 4).
D_4^* es un grupo bajo la composición de funciones. Además $|D_4^*| = 8$
Proponemos como subconjuntos de D_4^* a:

$$H = \{e, T_x\} \text{ y } K = \{e, R^2, T_x, T_y\}$$

notemos que tanto H como K son subgrupos de D_4^*, pues;

✓ $T_x \circ e = e \circ T_x \in H$. Así H es subgrupo de D_4^*.

✓ $R^2 \circ T_x = T_y = T_x \circ R^2 \in K$, $R^2 \circ T_y = T_x = T_y \circ R^2 \in K$, $T_x \circ T_y = R^2 \in K$, y $T_y \circ T_x = e \in K$. Luego K es subgrupo de D_4^*.

Mas aún $K \triangleleft D_4^*$ y $H \triangleleft K$, pues;

✓ Como $|K| = 4$, entonces $[D_4^* : K] = |D_4^*|/|K| = 8/4 = 2$, luego $K \triangleleft D_4^*$

✓ Como $|H| = 2$, entonces $[K : H] = |K|/|H| = 4/2 = 2$, luego $H \triangleleft K$.

Por tanto $H \triangleleft K \triangleleft D_4^*$ es una serie subnormal pero no es normal, pues existe $R \in D_4^*$ y $T_x \in H$ tal que $R^{-1}T_xR = T_y \notin H$. □

Afirmación 2. *La normalidad es no transitiva.*

Demostración. Es decir aún cuando se tenga que $K \lhd H \lhd G$, no se puede concluir que $K \lhd G$ en general. Un contraejemplo es el siguiente: Sea $G = A_4$ y sea $H = \{e, (12)(34), (13)(24), (14)(23)\}$. $H \lhd G$ y H es abeliano. H se conoce el grupo de Klein de 4 elementos. Sea $K = \{e, (12)(34)\}$, entonces K es un subgrupo de H y $K \lhd H$. Sin embargo, K no es normal en G ya que para el elemento $\lambda = (12)(34) \in K$ y para $\sigma = (123) \in G = A_4$, el conjugado

$$\sigma\lambda\sigma^{-1} = \sigma(12)(34)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)\sigma(4)) = (23)(14) \notin K$$

□

Ejemplo 6. *Todo grupo tiene al menos una serie subnormal, que es la trivial* $\{e\} \triangleleft G$.

Ejemplo 7. *Series subnormales de* Z_6

$$\{0\} \triangleleft \langle 2\rangle \triangleleft Z_6 \;\; y \;\; \{0\} \triangleleft \langle 3\rangle \triangleleft Z_6.$$

Definición 3.3. *Dos series normales S y T de un grupo G son equivalentes si existe una correspondencia biunívoca entre los factores de S y los factores de T, tales factores correspondientes son isomorfos.*

Dicho de otra manera: $\exists\ \sigma : I \to J$ biyectiva, $I,\ J$ conjuntos de índices de los términos $S_i,\ T_j$ respectivamente tal que para cada $\sigma(i) = j,\ \forall j$. Luego esta correspondencia

implica que el factor de S es equivalente al factor de T, es decir, $S_i/S_{i+1} \simeq T_j/T_{j+1}$. Dos series normales equivalentes deben contener el mismo número de términos, no necesariamente en orden equivalente ver ejemplo 7, y tienen la misma longitud.

Afirmación 3. *La equivalencia de serie normal es una relación de equivalencia, es decir: $S \sim T$ si y sólo si $S_i/S_{i+1} \simeq T_j/T_{j+1}$, si y sólo si hay una correspondencia 1-1 $I \leftrightarrow J$.*

Para ver que $\sim$ es una relación de equivalencia, hay que probar:
(i) Reflexiva: $S \sim S, \forall\ S$ serie normal.
(ii) Simétrica: Si $S \sim T \Rightarrow T \sim S$, $\forall\ S, T$ series normales.
(iii) Transitiva: Si $S \sim H$ y $H \sim T \Rightarrow S \sim T$, $\forall\ S,\ T$ y H series normales.

Demostración. (i) Es reflexiva, sea $Id : I \to I$ la función identidad, es una correspondencia biyectiva, luego $S_i/S_{i+1} \simeq S_i/S_{i+1}$, es decir $S \sim S$.
(ii) Si $f : I \to J$ es biyectiva, entonces existe $f^{-1} : J \to I$ que también es biyectiva, luego $T \sim S$.
(iii) Si $f : I \to K$ es biyectiva y $g : K \to J$ es biyectiva, luego $g \circ f : I \to J$ es biyectiva, luego $S \sim T$.
Por tanto $\sim$ es una relación de equivalencia. □

Lema 3.1. *(Zassenhaus) Sean A', A, B', B subgrupos de un grupo G tal que $A' \lhd A$ y $B' \lhd B$:*

1. $A'(A \cap B')$ es un subgrupo normal de $A'(A \cap B)$.
2. $B'(A' \cap B)$ es un subgrupo normal de $B'(A \cap B)$.
3. $\dfrac{A'(A \cap B)}{A'(A \cap B')} \simeq \dfrac{B'(A \cap B)}{B'(A' \cap B)}$.

Demostración. Mostremos que $(A \cap B') \lhd (A \cap B)$, si $c \in (A \cap B')$ y $x \in (A \cap B)$, entonces $x^{-1}cx \in (A \cap B')$. En efecto, como $c \in B'$, $x \in B$ y $B' \lhd B$, entonces $x^{-1}cx \in B'$; y como $c,\ x \in A$, entonces $x^{-1}cx \in A$, por tanto $x^{-1}cx \in (A \cap B')$. Análogamente $(A' \cap B) \lhd A \cap B$. Así si definimos $D := (A' \cap B)(A \cap B')$, tenemos que $D \lhd A \cap B$.

Definimos $f : A'(A \cap B) \to (A \cap B)/D$ como sigue: si $a \in A',\ c \in (A \cap B)$ $f(ac) = Dc$. Veamos que f esta bien definida, pues sean $a, a_1 \in A'$ y $c, c_1 \in A \cap B$ tenemos si

$$ac = a_1c_1 \Rightarrow c_1c^{-1} = a_1^{-1}a \in (A \cap B) \cap A' = A' \cap B \leq D. \tag{3.1.2}$$

Por otro lado, como D es normal, $cD = Dc$. Sea $d \in D$, entonces $dc = d(cc_1^{-1})(c_1c^{-1})c = (dcc_1^{-1})c_1$. Pero como $c_1c^{-1} \in D$ por (3.1.2), tenemos que $dc \in Dc_1$. Por lo tanto, $Dc \subset Dc_1$. Recíprocamente, $dc_1 = dc_1c^{-1}cc_1^{-1}c_1 = (dc_1c^{-1})c \in Dc$. Así, tenemos que $cD = Dc = Dc_1 = c_1D$ y $f(ac) = f(a_1c_1)$.

Luego f es suryectiva, pues $f(ec) = Dc$ con $e \in A',\ c \in (A \cap B)$. Y f es un epimorfismo, pues:

$$f[(a_1c_1)(a_2c_2)] = f(a_1a_3c_1c_2) = Dc_1c_2 = Dc_1Dc_2 = f(a_1c_1)f(a_2c_2)$$

$c_1a_2 = a_3c_1$ puesto que $A' \lhd A$.

Ahora mostremos que el $ker(f)$ es $A'(A \cap B')$. Si $ac \in ker(f)$ si y sólo si $c \in D$ esto es, si y sólo si $c = a_1c_1$ con $a_1 \in A' \cap B$ y $c_1 \in A \cap B'$. Por lo tanto $ac \in ker(f)$ si y sólo si $ac = (aa_1)c_1 \in A'(A \cap B')$. Luego $ker(f) = A'(A \cap B')$.

Por tanto:

$$ker(f) = A'(A \cap B') \lhd A'(A \cap B)$$

Análogamente, definimos el epimorfismo $g : B'(A \cap B) \to (A \cap B)/D$ como $g(bc) = Dc$ con $b \in B'$ y $c \in (A \cap B)$ y de forma similar (hecho anteriormente), se concluye que

$$ker(g) = B'(A' \cap B) \lhd B'(A \cap B)$$

Resumiendo, tenemos a $f : A'(A \cap B) \to (A \cap B)/D$ un epimorfismo cuyo $ker(f) = A'(A \cap B')$. Luego por el primer teorema de isomorfismo tenemos:

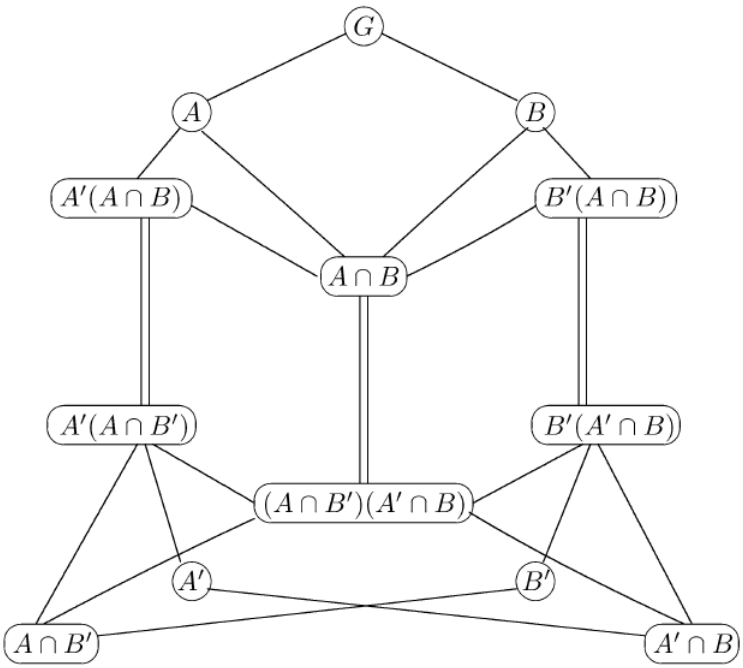
$$A'(A \cap B)/A'(A \cap B') \simeq (A \cap B)/D \tag{3.1.3}$$

Por otra parte $g : B'(A \cap B) \to (A \cap B)/D$ un epimorfismo cuyo $ker(g) = B'(A' \cap B)$. Luego por el primer teorema de isomorfismo tenemos:

$$B'(A \cap B)/B'(A' \cap B) \simeq (A \cap B)/D \tag{3.1.4}$$

Finalmente de (3.1.3) y (3.1.4) concluimos que:

$$A'(A \cap B)/A'(A \cap B') \simeq B'(A \cap B)/B'(A' \cap B).$$



□

Teorema 3.1. *(Teorema de Refinamiento de Schreier). Cualesquiera dos series normales de un grupo G tienen refinamientos normales que son equivalentes.*

Demostración. Supongamos las series normales para G

$$\mathscr{S}_1 : \{e\} = H_0 \lhd \cdots \lhd H_n = G, \text{ y}$$

$$\mathscr{S}_2 : \{e\} = J_0 \lhd \cdots \lhd J_m = G$$

Construiremos una nueva serie normal $\mathscr{S}_{1,2}$ por inserción de una copia de $\mathscr{S}_2$ entre cada término en $\mathscr{S}_1$, y una segunda nueva serie normal $\mathscr{S}_{2,1}$ por inserción de una copia de $\mathscr{S}_1$ entre cada término en $\mathscr{S}_2$; entonces tenemos que mostrar que $\mathscr{S}_{1,2}$ es equivalente a $\mathscr{S}_{2,1}$; tomaremos en cuenta que las repeticiones están permitidas.

Para $0 \leq r \leq n$ y $0 \leq s \leq m$, sean los subgrupos $K_{r,s}$ dada por

$$K_{r,s} = H_r(H_{r+1} \cap J_s),$$

donde asumimos que $H_{n+1} = H_n$ y $J_{m+1} = J_m$. Tenemos

$$K_{r,0} = H_r(H_{r+1} \cap \{e\}) = H_r \text{ y}$$

$$K_{r,m} = H_r(H_{r+1} \cap G) = H_r H_{r+1} = H_{r+1},$$

ya que $H_r \leq H_{r+1}$. Mas para $0 < s < m$,

$$K_{r,s} = H_r(H_{r+1} \cap J_s) \lhd H_r(H_{r+1} \cap J_{s+1}) = K_{r,s+1},$$

usando la parte (i) del Lema de Zassenhaus, sea $H_r = A'$, $H_{r+1} = A$, $J_s = B'$ y $J_{s+1} = B$. La serie subnormal $\mathscr{S}_{1,2}$ ahora puede ser definido por

$$\mathscr{S}_{1,2} : \{e\} = K_{0,0} \lhd K_{0,1} \lhd \cdots \lhd K_{0,m} \lhd K_{1,0} \lhd \cdots \lhd K_{1,m} \lhd K_{2,m} \lhd \cdots \lhd K_{n,m} = G.$$

Intercambiando H y J, definimos

$$L_{s,r} = J_s(J_{s+1} \cap H_r),$$

y la serie subnormal $\mathscr{S}_{2,1}$ es dada por usando la parte ii) del Lema de Zassenhaus

$$\mathscr{S}_{2,1} : \{e\} = L_{0,0} \lhd L_{0,1} \lhd \cdots \lhd L_{0,n} \lhd L_{1,0} \lhd \cdots \lhd L_{1,n} \lhd L_{2,n} \lhd \cdots \lhd L_{m,n} = G.$$

por (iii) en el Lema de Zassenhaus, obtenemos

$$\frac{K_{r,s+1}}{K_{r,s}} = \frac{H_r(H_{r+1} \cap J_{s+1})}{H_r(H_{r+1} \cap J_s)} \backsimeq \frac{J_s(J_{s+1} \cap H_{s+1})}{J_s(J_{s+1} \cap H_r)} = \frac{L_{s,r+1}}{L_{s,r}}.$$

Esto muestra que el conjunto de factores de $\mathscr{S}_{1,2}$ y $\mathscr{S}_{2,1}$ son equivalentes. Y tienen la mismo número de términos, que es $mn + m + n$. □

3.2. El teorema de Jordan - Hölder

Sea G es un grupo finito, podemos empezar con cualquier serie, por ejemplo $\{e\} \lhd G$, y seguir refinando hasta que se alcanza una serie de composición. Así cada grupo finito tiene una serie de composición.

Observación 1. *Si pensamos en una serie subnormal como una "factorización" del grupo, un refinamiento seria una factorización mayor, y una serie de composición sería como una factorización en factores primos.*

Definición 3.4. Subgrupo normal maximal

Diremos que K es un subgrupo normal máximal *de un grupo G, si K es un subgrupo normal propio de G y no hay subgrupo normal propio de G que contiene K, esto es, $K \lhd G$, y si $K \lhd J \lhd G$ entonces $J = K$ o $J = G$. Así un subgrupo máximal es siempre propio.*

Definición 3.5. *Un grupo G es simple, si sus únicos subgrupos normales son $\{e\}$ y G.*

Proposición 3. *Una serie es una serie de composición si y sólo si todos sus factores son grupos simples.*

Demostración. Por contradicción. Sea X/Y un factor de una serie en un grupo G. Si X/Y no es simple, hay un subgrupo W tal que $Y < W < X$ y $W \triangleleft X$; por el teorema de la correspondencia, la asignación $W \mapsto W/Y$ determina una biyección desde el conjunto de subgrupos de X que contiene Y al conjunto de subgrupos de X/Y ($Y \triangleleft X$). Esto implica que $W/Y \triangleleft X/Y$. Así obtenemos una nueva serie $Y \triangleleft W \triangleleft X$ que es un refinamiento propio de $Y \triangleleft X$. Esto es una contradicción, pues una serie de composición no tiene refinamientos propios.
Recíprocamente, por contradicción. Supongamos que la serie en G tiene un refinamiento propio. Sea $Y \triangleleft W \triangleleft X$ un refinamiento propio de $Y \triangleleft X$, luego W/Y es subgrupo normal propio de X/Y, luego X/Y no puede ser simple. □

Si N es un subgrupo normal de un grupo G, entonces todo subgrupo normal de G/N es de la forma H/N, donde H es un subgrupo normal de G, el cual contiene a N. Tenemos la siguiente propiedad.

Proposición 4. *$N \neq G$, G/N es simple si y sólo si N es maximal en el conjunto de todos los subgrupos normales M de G con $M \neq G$ (a tal subgrupo N se llama subgrupo normal maximal de G).*

Demostración. Supongamos por el absurdo que N no es un subgrupo normal maximal de G, es decir, existe H, tal que $N < H$ con $H \neq G$, $H \neq \{e\}$, $H \neq N$ tal que $H \triangleleft G$. Entonces como $H \triangleleft G$ y $N < H < G$, con $H \neq N$, $H \neq G$, $H \neq \{e\}$, luego $H/N \triangleleft G/N$. Así G/N tiene un subgrupo normal propio lo cual es absurdo, pues contradice que G/N sea simple.
Recíprocamente, supongamos por el absurdo que G/N no es simple, entonces tiene un subgrupo normal de la forma $M/N \triangleleft G/N$, con $N < M < G$ tal que $M \neq N$, $M \neq G$, $M \neq \{e\}$, por el teorema de la correspondencia $M \triangleleft G$.

Luego $N < M$ y $M \lhd G$ es absurdo, pues contradice que N sea subgrupo normal maximal. □

Teorema 3.2. *Todo grupo finito G tiene una serie de composición.*

Demostración. Si G es simple entonces $\{e\} \lhd G$ es una serie de composición de G. Si G no es simple, entonces G tiene al menos un subgrupo normal G_1 tal que $G_1 \lhd G$. Si G_1 es maximal, entonces $\{e\} \lhd G_1 \lhd G$ es una serie de composición de G. Si G_1 no es maximal, entonces G/G_1 no es simple y así tiene un subgrupo normal propio, que bajo el teorema de la correspondencia esta asociado a un subgrupo normal $G_2 \lhd G$ tal que $\{e\} \lhd G_1 \lhd G_2 \lhd G$. Si G_2 es maximal tenemos de la última serie que es serie de composición, si G_2 no es maximal procedemos como antes.
Como G es finito, el proceso anterior termina en un número finito de casos. Así todo grupo finito tiene una serie de composición $\{e\} \lhd G_1 \lhd G_2 \lhd \ldots \lhd G$. □

Lema 3.2. *Sea S es una serie de composición de un grupo G entonces cualquier refinamiento de S es equivalente a S.*

Demostración. Sea $S : \{e\} \lhd G_1 \lhd G_2 \lhd \ldots \lhd G$, una serie de composición. Entonces no tiene refinamientos propios, así los únicos posibles refinamientos de S son obtenidos insertando copias adicionales de cada G_i. Consecuentemente cualquier refinamiento de S tiene exactamente los mismos factores no triviales de S y es, por lo tanto, equivalente a S. □

Teorema 3.3. *(Jordan - Hölder) Cualesquiera dos series de composición de un grupo G son equivalentes. Por consiguiente cualquier grupo teniendo una serie de composición determina una única lista de grupos simples.*

Demostración. Por el teorema de refinamiento de Schreier, las series de composición S y T tienen refinamientos equivalentes. Pero todo refinamiento de una serie de composición S es equivalente a S, por el Lema (3.2). De esto resulta que dos series de composición son equivalentes. □

CAPÍTULO 4

Grupos Nilpotentes

El objetivo de este capitulo es introducir el estudio de grupos nilpotentes. Definimos un grupo nilpotente, como también la serie central inferior y superior de un grupo y se presenta una relación entre ellos. Luego damos numerosas propiedades de grupos nilpotentes.

4.1. La serie central inferior y superior

4.1.1. Series de subgrupos

Definición 4.1. *Sea G_1, G_2, $G_3, \ldots$ una sucesión de subgrupos de un grupo G.*
(i) Si $G_i \leq G_j$ para $1 \leq i \leq j$, entonces

$$G_1 \leq G_2 \leq G_3 \leq \cdots \tag{4.1.1}$$

es una serie ascendente.
(ii) Si $G_i \geq G_j$ para $1 \leq i \leq j$, entonces

$$G_1 \geq G_2 \geq G_3 \geq \cdots \tag{4.1.2}$$

es una serie descendente.

Una serie ascendente podría no alcanzar G. Si lo hace, entonces diremos que la serie termina en G. Similarmente, una serie descendente que alcanza la identidad, se dice que termina en la identidad. Si existe un entero $m > 1$ tal que $G_{m-1} \neq G_m$ y $G_m = G_{m+1} = G_{m+2} = \cdots$, entonces la serie se estabiliza en G_m.

4.1.2. Definición de un grupo nilpotente

Definición 4.2. *Un grupo G es llamado nilpotente si esta tiene una serie normal.*

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G \tag{4.1.3}$$

tal que $G_{i+1}/G_i \leq Z(G/G_i)$ para $i = 0, 1, \ldots, n-1$.

La longitud de una serie central mas corta es llamado la clase de nilpotencia de G o la clase de G.

Una definición equivalente de una serie central que involucra conmutadores es dada en el siguiente lema.

Lema 4.1. *Sea G un grupo con una serie*

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G \tag{4.1.4}$$

La serie (4.1.4) es central si, y sólo si $[G_{i+1}, G] \leq G_i$ para $0 \leq i \leq n-1$.

Demostración. Supongamos que la serie (4.1.4) es central, entonces $G_{i+1}/G_i \leq Z(G/G_i)$. En el Lema (2.3), tomando $H = G_{i+1}$ y $N = G_i$, se tiene $[G_{i+1}, G] \leq G_i$ para $0 \leq i \leq n-1$.

Recíprocamente supongamos que $[G_{i+1}, G] \leq G_i$ para $0 \leq i \leq n-1$. Afirmemos que la serie (4.1.4) es normal. Sea $g \in G$ y $g_i \in G_i$ para algún $i = 1, 2, \ldots, n$, por el Lema (2.1-ii), tenemos

$$g_i^g = g_i[g_i, g] \in G_i G_{i-1} = G_i,$$

así $G_i \trianglelefteq G$. De nuevo por el Lema (2.3), $G_{i+1}/G_i \leq Z(G/G_i)$ luego la serie (4.1.4) es central. □

El siguiente lema muestra que los únicos grupos nilpotentes con centro trivial es el grupo trivial.

Lema 4.2. *Sea G un grupo nilpotente no trivial, entonces $Z(G) \neq \{e\}$*

Demostración. Supongamos que $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$ es una serie central para G. Sea $G_i = \{e\}$ y $G_{i+1} \neq \{e\}$ 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, $Z(G) \neq \{e\}$. □

4.1.3. La serie central inferior

En este apartado veremos surgir la relación entre nilpotencia y conmutadores.
Una serie que es fundamental en el estudio de grupos nilpotentes es el de serie central inferior.
Sea G un grupo. Definimos $\gamma_1(G) = G \trianglelefteq G$ y $\gamma_2(G) = [G, G] = G' \trianglelefteq G$, luego por Corolario (2.7), $\gamma_n(G) \trianglelefteq G$ para todo $n \in \mathbb{N}$.
Mostremos que $\gamma_{n+1}(G) \leq \gamma_n(G)$ para todo $n \in \mathbb{N}$, por la Proposición (1-ii) como $\gamma_n(G) \trianglelefteq G$ entonces $\gamma_{n+1}(G) = [\gamma_n(G), G] \leq \gamma_n(G)$. Luego por el Lema (2.3), podemos ver que la serie de subgrupos de G a continuación es central (descendente)

Definición 4.3. *Sea G un grupo. La serie normal descendente*

$$G = \gamma_1(G) \trianglerighteq \gamma_2(G) \trianglerighteq \cdots \trianglerighteq \gamma_n(G) \trianglerighteq \gamma_{n+1}(G) \trianglerighteq \cdots \tag{4.1.5}$$

es llamado serie central inferior *de G, tal que $\gamma_{i+1}(G) = [\gamma_i(G), G]$ para todo $i \in \mathbb{N}$.*

Cada término en la serie es llamado *subgrupo central inferior* de G. Consideremos los siguientes casos a continuación:

Caso 1. Si $\gamma_i(G) = \{e\}$ para algún $i \geq 1$, entonces $\gamma_{i+1}(G) = [\gamma_i(G), G] = [\{e\}, G] = \{e\}$.

Caso 2. Si $\gamma_2(G) = G$, entonces $\gamma_3(G) = [\gamma_2(G), G] = [G, G] = \gamma_2(G) = G$. Continuando con este argumento se muestra que $\gamma_j(G) = G$ para todo $j \geq 1$.

Ejemplo 8. *Si G es un grupo abeliano, entonces $[G, G] = \{e\}$. Por el Caso 1, $\gamma_i(G) = \{e\}$ para todo $i \geq 2$.*

Ejemplo 9. *Encontraremos el subgrupo central inferior de A_n, por el Ejemplo (8), $\gamma_i(A_n) = \{e\}$ para $n = 1, 2, 3$ e $i \geq 2$, pues A_1, A_2 y A_3 son abelianos.*
Por el ejemplo (4) vimos que $[A_4, A_4] = K$. Luego afirmamos que $\gamma_i(A_4) = K$ para $i \geq 3$. Consideremos el caso $i = 3$. Podemos escribir cada elemento de K distinto de la identidad como

$$(a\ d)(b,\ c) = [(a\ c\ b), (a\ b)(c\ d)],$$

donde a, b, c, d son elementos distintos de $S = \{1, 2, 3, 4\}$. Como A_4 es generado por 3-ciclos, $K \leq [K, A_4]$. Consecuentemente, $K = [K, A_4] = \gamma_3(A_4)$ como afirmamos. Concluimos que $\gamma_i(A_4) = K$ para $i \geq 2$.
Si $n \geq 5$, entonces cada subgrupo central interior de A_n es igual A_n, esto por el Ejemplo (4) y el Caso 2.

Este ejemplo ilustra que la serie central inferior (4.1.5) no puede descender a la identidad, y en consecuencia, no puede ser una serie central en el sentido de la Definición (4.2).
Damos algunas propiedades útiles de subgrupo central inferior.

Lema 4.3. *Sea G un grupo. Consideremos una serie de subgrupos normales de G*

$$G = N_1 \trianglerighteq N_2 \trianglerighteq \cdots \trianglerighteq N_k \trianglerighteq N_{K+1} \trianglerighteq \cdots$$

serie central. Entonces $\gamma_n(G) \leq N_n$ para todo $n \in \mathbb{N}$.

Demostración. Como la serie es central, tenemos que $[N_k, G] \leq N_{k+1}$ para todo $k \in \mathbb{N}$.
Seguiremos por inducción sobre n, si $n = 1$, $\gamma_1(G) = N_1$.
Suponga por inducción que $\gamma_k(G) \leq N_k$ para algún $k \in \mathbb{N}$.

$$\gamma_{k+1}(G) = [\gamma_k(G), G] \leq [N_k, G] = N_{k+1}.$$

Por tanto para todo $n \in \mathbb{N}$, $\gamma_n(G) \leq N_n$. □

Lema 4.4. *Sean G y K grupos. Si $\varphi : G \to K$ es un homomorfismo, entonces $\varphi(\gamma_i(G)) = \gamma_i(\varphi(G))$ para cada $i \in \mathbb{N}$.*

Demostración. Por inducción sobre i. Si $i = 1$, entonces $\varphi(\gamma_1(G)) = \varphi(G) = \gamma_1(\varphi(G))$. Supongamos que $\varphi(\gamma_k(G)) = \gamma_k(\varphi(G))$ para algún $k \in \mathbb{N}$. En la segunda igualdad por la Proposición (2) tenemos

$$\varphi(\gamma_{k+1}(G)) = \varphi([\gamma_k(G),\ G]) = [\varphi(\gamma_k(G)),\ \varphi(G)]$$

$$= [(\gamma_k(\varphi(G)),\ \varphi(G)] = \gamma_{k+1}(\varphi(G)).$$

Por tanto para todo $i \in \mathbb{N}$, $\varphi(\gamma_i(G)) = \gamma_i(\varphi(G))$. □

Corolario 4.1. *Sea G un grupo y $N \trianglelefteq G$, entonces $\gamma_i(G/N) = \gamma_i(G)N/N$ para cada $i \in \mathbb{N}$.*

Demostración. Si $\pi : G \to G/N$ es el homomorfismo natural, entonces por Lema (4.4)

$$\gamma_i(G)N/N = \pi(\gamma_i(G)) = \gamma_i(\pi(G)) = \gamma_i(G/N).$$

□

4.1.4. La serie central superior

En esta parte nos apoyaremos en el concepto de centro de un grupo, para definir una otra serie importante de subgrupos. La cual es llamada *serie central superior.*
Esta serie se construye como sigue.
Sea G un grupo un grupo. Definimos $\mathscr{D}_0(G) = \{e\}$ y $\mathscr{D}_1(G) = Z(G)$.
Sea

$$\pi_1 : G \to G/\mathscr{D}_1(G)$$

un homomorfismo natural. Definimos

$$\mathscr{D}_2(G) = \pi_1^{-1}(Z(G/\mathscr{D}_1(G))),$$

tal que $\mathscr{D}_2(G)/\mathscr{D}_1(G) = Z(G/\mathscr{D}_1(G))$ así $\mathscr{D}_2(G)/\mathscr{D}_1(G) \trianglelefteq G/\mathscr{D}_1(G)$, luego $\mathscr{D}_2(G) \trianglelefteq G$ por el teorema de la correspondencia.
A continuación $\pi_2 : G \to G/\mathscr{D}_2(G)$ es homomorfismo natural. Y definimos

$$\mathscr{D}_3(G) = \pi_2^{-1}(Z(G/\mathscr{D}_2(G))).$$

Así, $\mathscr{D}_3(G)/\mathscr{D}_2(G) = Z(G/\mathscr{D}_2(G))$, como antes, $\mathscr{D}_3(G) \trianglelefteq G$ por el teorema de la correspondencia. Continuando de esta manera obtenemos $\mathscr{D}_i(G) \trianglelefteq G$.

Si $\pi_i : G \to G/\mathscr{D}_i(G)$ es el homomorfismo natural de G sobre $G/\mathscr{D}_i(G)$, entonces

$$\begin{aligned}\mathscr{D}_{i+1}(G) &= \pi_i^{-1}(Z(G/\mathscr{D}_i(G))) \\ &= \{g \in G \mid g\mathscr{D}_i(G) \text{ es central en } G/\mathscr{D}_i(G)\} \\ &= \{g \in G \mid (g\mathscr{D}_i(G))(h\mathscr{D}_i(G)) = (h\mathscr{D}_i(G))(g\mathscr{D}_i(G)) \text{ para todo } h \in G\} \\ &= \{g \in G \mid [g,h] \in \mathscr{D}_i(G) \text{ para todo } h \in G\}.\end{aligned}$$

Sea $N = \mathscr{D}_i(G)$ y $H = \mathscr{D}_{i+1}(G)$ en el Lema (2.3) tenemos que $[\mathscr{D}_{i+1}(G), G] \leq \mathscr{D}_i(G)$. Luego la serie a continuación es central (ascendente).

Definición 4.4. *Sea G un grupo. La serie normal ascendente*

$$\{e\} = \mathscr{D}_0(G) \trianglelefteq \mathscr{D}_1(G) \trianglelefteq \cdots \trianglelefteq \mathscr{D}_n(G) \trianglelefteq \mathscr{D}_{n+1}(G) \trianglelefteq \cdots \tag{4.1.6}$$

es llamado serie central superior *de G, tal que $\mathscr{D}_{i+1}(G)/\mathscr{D}_i(G) = Z(G/\mathscr{D}_i(G))$ para $i \geqslant 0$ y los términos son llamados* subgrupos central superior *de G.*

Consideremos los siguientes casos:

Caso 1. Si $\mathscr{D}_i(G) = G$ para algún $i \geq 0$, entonces

$$\begin{aligned}\mathscr{D}_{i+1}(G) &= \{g \in G \mid [g,h] \in \mathscr{D}_i(G) \text{ para todo } h \in G\} \\ &= \{g \in G \mid [g,h] \in G \text{ para todo } h \in G\} \\ &= G.\end{aligned}$$

Caso 2. Si $Z(G) = \{e\}$, entonces

$$\begin{aligned}\mathscr{D}_2(G) &= \{g \in G \mid [g,h] \in Z(G) \text{ para todo } h \in G\} \\ &= \{g \in G \mid [g,h] = \{e\} \text{ para todo } h \in G\} \\ &= Z(G) \qquad .\end{aligned}$$

Así, $\mathscr{D}_2(G) = \{e\}$. Continuando de esta manera, tenemos que $\mathscr{D}_j(G) = \{e\}$ para todo $j \geq 0$.

Ejemplo 10. *Si G es un grupo abeliano, entonces $\mathscr{D}_1(G) = G$. Así $\mathscr{D}_i(G) = G$ para todo $i \geq 0$ por el Caso 1.*

Ejemplo 11. *Si $n \geq 3$, entonces los subgrupos central superior de S_n son triviales, esto por el Ejemplo (1) y por el Caso 2. Lo mismo es cierto para el subgrupo central superior de A_n cuando $n > 3$ (ver Ejemplo 2). Esto ilustra que la serie central superior de un grupo no necesariamente asciende al grupo.*

Así como en la primera serie (serie central inferior), tenemos el siguiente lema.

Lema 4.5. *Sea G un grupo y*

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_k \trianglelefteq H_{k+1} \cdots$$

una serie central de subgrupos de G. Entonces $H_n \leq \mathscr{D}_n(G)$ para todo $n \in \mathbb{N}$.

Demostración. Seguiremos por inducción sobre $n \in \mathbb{N}$, si $n = 0$ es trivial. Suponga que $H_{k-1} \leq \mathscr{D}_{k-1}(G)$ para algún $k \in \mathbb{N}$.
Como la serie es central vale $H_k/H_{k-1} \leq Z(G/H_{k-1})$ entonces $[H_k, G] \leq H_{k-1} \leq \mathscr{D}_{k-1}(G)$. Entonces se sigue que $H_k/\mathscr{D}_{k-1}(G) \leq Z(G/\mathscr{D}_{k-1}(G))$ y por tanto $H_k \leq \mathscr{D}_k(G)$. Para todo $n \in \mathbb{N}$, $H_n \leq \mathscr{D}_n(G)$. □

4.2. Comparando series centrales

La serie central de un grupo nilpotente asciende al grupo mas rápido que cualquier otra serie central, mientras que una serie central inferior desciende a la identidad mas rápido que cualquier otra serie central. Esto es resaltado en el siguiente corolario.

Corolario 4.2. *Sea $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$ una serie central (ascendente) de un grupo nilpotente G, entonces:*
(i) $\gamma_i(G) \leq G_{n-i+1}$, para $1 \leq i \leq n+1$.
(ii) $G_i \leq \mathscr{D}_i(G)$, para $0 \leq i \leq n$.

Demostración. (i) Por inducción sobre i, si $i = 1$ se cumple. Supongamos que $\gamma_{i-1}(G) \leq G_{n-(i-1)+1} = G_{n-i+2}$ para algún $i \in \mathbb{N}$.

Para $i > 1$, por definición de serie central $G_{n-i+1}/G_{n-i} \leq Z(G/G_{n-i})$ entonces $[G_{n-i+1}, G] \leq G_{n-i}$. Por hipótesis de inducción, tenemos que $\gamma_i(G) = [\gamma_{i-1}(G), G] \leq [G_{n-i+2}, G] \leq G_{n-i+1}$, para $1 \leq i \leq n+1$.

(ii) Por el Lema 4.5. □

Teorema 4.3. *Sea G un grupo. Entonces, son equivalentes:*

(i) G es nilpotente.

(ii) Existe $n \in \mathbb{N}$ tal que $\mathscr{D}_n(G) = G$.

(iii) Existe $m \in \mathbb{N}$ tal que $\gamma_m(G) = \{e\}$.

(iv) Existen n_1, $n_2 \in \mathbb{N}$ tales que $\gamma_{n_1}(G) \leq \mathscr{D}_{n_2}(G)$.

Demostración. Notemos

$$\gamma_{n-k+1}(G) \leq N_k \leq \mathscr{D}_k(G) \tag{4.2.1}$$

para todo $k = 0, 1, \ldots, n$, donde $\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_n = G$ es una serie central cualquiera de G. La relación (4.2.1) es cierto, por el Teorema (4.2).

$(i) \Rightarrow (ii)$ En (4.2.1) si $k = n$, entonces $G = \gamma_1(G) \leq N_n \leq \mathscr{D}_n(G)$, luego $G \leq \mathscr{D}_n(G)$. Como $\mathscr{D}_n(G) \trianglelefteq G$. Por tanto existe $n \in \mathbb{N}$ tal que $\mathscr{D}_n(G) = G$, con $n = k$.

$(ii) \Rightarrow (iii)$ basta tomar $N_k = \mathscr{D}_k(G)$ para términos

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_n = G$$

de la serie central de G. Por tanto, en (4.2.1) si $k = 0$, $\gamma_{n+1}(G) \leq N_0 = \mathscr{D}_0(G) = \{e\}$. Por tanto existe $m \in \mathbb{N}$ tal que $\gamma_m(G) = \{e\}$, con $m = n + 1$.

$(iii) \Rightarrow (iv)$ En (4.2.1), haciendo $n_1 = n - k + 1$ y $n_2 = k$, se tiene $\gamma_{n_1}(G) \leq \mathscr{D}_{n_2}(G)$.

$(iv) \Rightarrow (i)$ Por inducción sobre n_1. Si $n_1 = 1$ entonces $G = \gamma_1(G) \leq \mathscr{D}_{n_2}(G)$, entonces $\mathscr{D}_{n_2}(G) = G$, pues $\mathscr{D}_{n_2}(G) \trianglelefteq G$.

Tomando $n_1 > 1$, observemos que $[\gamma_{n_1-1}(G), G] = \gamma_{n_1}(G) \leq \mathscr{D}_{n_2}(G)$. Como $\mathscr{D}_{n_2+1}(G) = \{g \in G |\ [g, G] \leq \mathscr{D}_{n_2}(G)\}$, tenemos que $\gamma_{n_1-1}(G) \leq \mathscr{D}_{n_2+1}(G)$.

Supongamos que $\gamma_{n_1-k}(G) \leq \mathscr{D}_{n_2+k}(G)$ para algún $k \in \mathbb{N}$. Observemos $[\gamma_{n_1-(k+1)}(G), G] = \gamma_{n_1-k}(G) \leq \mathscr{D}_{n_2+k}(G)$, como $\mathscr{D}_{n_2+k+1}(G) = \{g \in G |\ [g, G] \leq \mathscr{D}_{n_2+k}(G)\}$, entonces $\gamma_{n_1-(k+1)}(G) \leq \mathscr{D}_{n_2+k+1}(G)$.

Luego, podemos concluir que $G = \gamma_1(G) \leq \mathscr{D}_{n_1+n_2-1}(G)$, donde se sigue que existe

$n \in \mathbb{N}$ tal que $\mathscr{D}_n(G) = G$. Como

$$\{e\} = \mathscr{D}_0(G) \trianglelefteq \mathscr{D}_1(G) \trianglelefteq \cdots \trianglelefteq \mathscr{D}_n(G) = G$$

es una serie central de G, así G es nilpotente. □

Observación 2. *Sea G un grupo nilpotente. Luego en el Teorema (4.3)*

$$n_0 = min\{n \in \mathbb{N} : \mathscr{D}_n(G) = G\}.$$

y

$$m_0 = min\{m \in \mathbb{N} : \gamma_{m+1}(G) = \{e\}\}.$$

Mostremos que $n_0 = m_0$. Se sigue de (4.2.1) que $\gamma_{n_0-k+1}(G) \leq \mathscr{D}_k(G)$ para todo $k = 0, 1, \ldots, n_0$. Si k=0, $\gamma_{n_0+1}(G) \leq \mathscr{D}_0(G) = \{e\}$, y $\{e\} \leq \gamma_{n_0+1}(G)$. Por tanto $\gamma_{n_0+1}(G) = \{e\}$. Y como m_0 es el mínimo que satisface $\gamma_{m_0+1}(G) = \{e\}$, entonces $m_0 \leq n_0$.
Por otro lado, tomando $N_k = \gamma_{m_0-k+1}(G)$ para todo $k = 0, 1, \ldots, m_0$, los $N_{i's}$ forman una serie central de la forma

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{m_{0-1}} \trianglelefteq N_{m_0} = G,$$

por tanto de (4.2.1), $\gamma_{m_0-k+1}(G) = N_k \leq \mathscr{D}_k(G)$ para todo $k = 0, 1, \ldots, m_0$. Si $k = m_0$, $G = \gamma_1(G) = N_{m_0} \leq \mathscr{D}_{m_0}(G)$ y $\mathscr{D}_{m_0}(G) \trianglelefteq G$, por tanto $\mathscr{D}_{m_0}(G) = G$. Como n_0 es el mínimo que satisface $\mathscr{D}_{n_0}(G) = G$, entonces $n_0 \leq m_0$. Por tanto $n_0 = m_0$.

Definición 4.5. *Sea G un grupo nilpotente. Definimos la clase de nilpotencia de G, denotada por $cl(G)$*

$$cl(G) = n_0 = min\{n \in \mathbb{N} : \mathscr{D}_n(G) = G\} = min\{m \in \mathbb{N} : \gamma_{m+1}(G) = \{e\}\}$$

4.3. Propiedades elementales de grupos nilpotentes

Veremos algunos resultados fundamentales de grupos nilpotentes.

Teorema 4.4. *Sea G un grupo nilpotente de clase c.*

(1) Todo subgrupo de un grupo nilpotente es nilpotente de clase menor o igual a c.

(II) La imagen homomórfica de un grupo nilpotente es nilpotente, de clase menor o igual a c.

(III) El grupo factor de un grupo nilpotente es nilpotente de clase menor o igual a c.

Demostración. (I) Consideremos H un subgrupo de G, mostraremos que $\gamma_i(H) \leq \gamma_i(G)$ para $i \in \mathbb{N}$. Por inducción sobre i. Si $i = 1$, en que $\gamma_1(H) = H \leq G = \gamma_1(G)$. Supongamos que $\gamma_k(H) \leq \gamma_k(G)$ para algún $k \in \mathbb{N}$. Entonces $\gamma_{k+1}(H) = [\gamma_k(H),\ H] \leq [\gamma_k(G),\ G] = \gamma_{k+1}(G)$. Por tanto $\gamma_i(H) \leq \gamma_i(G)$ para $i \in \mathbb{N}$.
Como G es un grupo nilpotente de clase c, $\gamma_{c+1}(G) = \{e\}$. Así $\gamma_{c+1}(H) = \{e\}$, y H es nilpotente de clase a lo sumo c.

(II) Sea K un grupo y $\varphi \in Hom(G,\ K)$ por Lema (4.4), $\varphi(\gamma_i(G)) = \gamma_i(\varphi(G))$ para cada $i \in \mathbb{N}$. Como G es nilpotente, $\gamma_{c+1}(G) = \{e\}$ y φ es un homomorfismo.

$$\{e\} = \varphi(\gamma_{c+1}(G)) = \gamma_{c+1}(\varphi(G)).$$

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

(III) Supongamos que N es un subgrupo normal de G. Entonces por el Corolario (4.1)

$$\gamma_i(G/N) = (\gamma_i G)N/N$$

para cada $i \in \mathbb{N}$. Por ser G un grupo nilpotente de clase c, se tiene $\gamma_{c+1}(G)N/N = \{e\}N/N = \{e'\}$. Siendo así $\gamma_{c+1}(G/N) = \{e'\}$, donde se sigue que G/N es nilpotente. Además, $cl(G/N) \leq c = cl(G)$. □

Teorema 4.5. *Si $G_1, G_2, \ldots, G_n$ son grupos nilpotentes, entonces $G_1 \times G_2 \times \cdots \times G_n$ es nilpotente.*

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

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = H$$

$$\{e\} = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_n = K$$

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:

$$\{e\} = H_0 \times K_0 \trianglelefteq H_1 \times K_1 \trianglelefteq \cdots \trianglelefteq H_n \times K_n = H \times K$$

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. □

4.3.1. Subgrupo subnormal

Los subgrupos de grupos nilpotentes disfrutan de varias propiedades notables, una de las cuales es la subnormalidad.

Definición 4.6. *Un subgrupo H de un grupo G es llamado subnormal, si hay una serie subnormal de subgrupos de G que comienza en H y termina en G.*

Teorema 4.6. *Cada subgrupo de un grupo nilpotente es subnormal.*

Demostración. Sea H un subgrupo de un grupo nilpotente G de clase c, y consideremos el subgrupo $H\mathscr{D}_i(G)$ de G para $i = 1, 2, \ldots, c$. Como la serie central superior de G es normal, la serie a continuación resulta de multiplicar el subgrupo H a cada término de la serie central de G, tenemos

$$H = H\mathscr{D}_0(G) \trianglelefteq H\mathscr{D}_1(G) \trianglelefteq \cdots \trianglelefteq H\mathscr{D}_c(G) = G. \tag{4.3.1}$$

Afirmamos que (4.3.1) es una serie subnormal. Mostraremos que $H\mathscr{D}_i(G) \trianglelefteq H\mathscr{D}_{i+1}(G)$ lo que es equivalente a mostrar $H\mathscr{D}_{i+1}(G) \leq N_G(H\mathscr{D}_i(G))$ para $i = 1, 2, \ldots, c$.
Sean $h \in H$, $f \in \mathscr{D}_i(G)$ y $z \in \mathscr{D}_{i+1}(G)$, entonces

$$\begin{aligned}
(hf)^z &= h^z f^z = z^{-1}hzz^{-1}fz \\
&= z^{-1}hfz \\
&= hf[hf, z] \in H\mathscr{D}_i(G)[H\mathscr{D}_i(G), \mathscr{D}_{i+1}(G)] \\
&= H[H\mathscr{D}_i(G), \mathscr{D}_{i+1}(G)] \\
&= H\mathscr{D}_i(G),
\end{aligned}$$

por tanto, $z \in N_G(H\mathscr{D}_i(G))$, así $\mathscr{D}_{i+1}(G) \leq N_G(H\mathscr{D}_i(G))$ pues z fue tomado un elemento arbitrario. Luego $\mathscr{D}_{i+1}(G) \leq N_G(H\mathscr{D}_i(G))$ y $H \leq N_G(H\mathscr{D}_i(G))$, entonces $H\mathscr{D}_{i+1}(G) < N_G(H\mathscr{D}_i(G))$ la afirmación es probada. Así, (4.3.1) es una serie subnormal de H a G en c pasos. □

4.3.2. La condición de normalizador

Una importante característica de grupos nilpotentes es que todos sus subgrupos maximales son normales. De hecho esta propiedad conduce a una estructura para grupos finitos nilpotentes.

Definición 4.7. *Un grupo G satisface la condición normalizador, si H es un subgrupo propio de $N_G(H)$ siempre que H sea un subgrupo propio de G.*

Lema 4.6. *Si un grupo G satisface la condición normalizador, entonces cada subgrupo maximal de G es normal.*

Demostración. Sea M es un subgrupo maximal de G. Por hipótesis como G satisface la condición normalizador, M es un subgrupo propio de $N_G(M)$. Así $N_G(M) = G$ pues M es maximal de G. Por tanto, $M \lhd G$. □

Lema 4.7. *Si cada subgrupo de un grupo G es subnormal, entonces G satisface la condición normalizador.*

Demostración. Supongamos que H es un subgrupo propio de G. Como H es subnormal, se tiene la serie subnormal

$$H = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

para algún $n \in \mathbb{N}$. Como $H \lhd H_1$, de ahí H_1 normaliza H, es decir $H_1 < N_G(H)$. Luego $H < H_1 < N_G(H)$. Por tanto $H < N_G(H)$. □

Teorema 4.7. *Cada grupo nilpotente satisface la condición normalizador.*

Demostración. Esto es una consecuencia del Teorema (4.6) y el Lema (4.7). □

Corolario 4.8. *Cada subgrupo maximal de un grupo nilpotente es normal.*

Demostración. Se sigue del Teorema (4.7) y el Lema (4.6). □

CAPÍTULO 5

Grupos Nilpotentes Finitos

5.1. Grupos nilpotentes finitos

En esta sección daremos una caracterización de grupo nilpotente finito.

Teorema 5.1. *Cada $p-$grupo finito es nilpotente, donde p es cualquier primo.*

Demostración. Sea G un $p-$grupo finito de orden p^n para algún $n \in \mathbb{N}$. Usaremos el paso en que un $p-$**grupo finito tiene centro no trivial,** para construir una serie central superior.

Tenemos $Z(G)$ es no trivial, y así $G/Z(G)$ es un $p-$ grupo finito de orden p^r para algún $r \in \mathbb{N}$ con $r < n$. Luego tenemos que $G/Z(G)$ tiene centro no trivial. Pues, $Z(G/Z(G)) = \mathscr{D}_2(G)/Z(G)$ es un $p-$grupo finito de orden p^s para algún $s \in \mathbb{N}$ con $s < r$. Esto significa que $|Z(G)| < |\mathscr{D}_2(G)|$, por lo que $Z(G) < \mathscr{D}_2(G)$. Repitiendo este procedimiento, vemos que $|\mathscr{D}_i(G)| < |\mathscr{D}_{i+1}(G)|$ para $i \geq 0$, y así $\mathscr{D}_i(G)$ es un subgrupo propio de $\mathscr{D}_{i+1}(G)$ para $i \geq 0$. Y así, la serie central superior para G es estrictamente creciente. Como G es finito, la serie debería terminar en $\mathscr{D}_k(G) = G$ para algún $k \in \mathbb{N}$. Por tanto, G es nilpotente □

Definición 5.1. *Sea G un grupo finito de orden $p^n k$, donde p es un primo, $k \in \mathbb{N}$, y p no divide a k. Un subgrupo de G cuyo orden es p^n es llamado un* p-subgrupo de Sylow *de G.*

Teorema 5.2. *Sea G un grupo finito de orden $p^n k$, donde p es un primo, $k \in \mathbb{N}$, y p no divide a k.*
(i) G tiene al menos un subgrupo de orden p^i para cada $i = 1, \ldots, n$.
(ii) Cualquiera dos p-subgrupos de Sylow de G son conjugados.

Una consecuencia del Teorema 5.2 -(ii) es:

Corolario 5.3. *Sea p un primo, y supongamos que P es un p-subgrupo de Sylow de un grupo finito G. Entonces $P \trianglelefteq G$ si, y sólo si P es el único p-subgrupo de Sylow de G.*

Demostración. Si $P \trianglelefteq G$, entonces $N_G(P) = G$, mas aún sean P y Q dos p-subgrupos de Sylow de G, entonces existe $g \in G$ tal que $g^{-1}Pg = Q$ y como $g^{-1}Pg = P$, entonces $P = Q$. Por tanto P es el único p-subgrupo de Sylow de G.
Recíprocamente, si P es el único $p-$subgrupo de Sylow de G, entonces todo conjugado de P es igual a P, es decir $g^{-1}Pg = P$, $g \in G$. Por tanto $P \trianglelefteq G$. □

Teorema 5.4. *(Teorema sobre la Caracterización de Grupos Nilpotentes Finitos.)*
Sea G un grupo finito. Los siguientes son equivalentes:
(i) G es Nilpotente;
(ii) Cada subgrupo de G es subnormal en G;
(iii) G satisface la condición de normalizador;
(iv) Cada subgrupo maximal de G es normal en G;
(v) Cada subgrupo Sylow de G es normal en G;
(vi) G es isomorfo al producto directo de sus subgrupos de Sylow;
(vii) Si $a, b \in G$ y $(|a|, |b|) = 1$, entonces a y b conmutan en G.

Demostración. $(i) \Rightarrow (ii)$ por Teorema (4.6).
$(ii) \Rightarrow (iii)$ por Lema (4.7).
$(iii) \Rightarrow (iv)$ por Lema (4.6).
$(iv) \Rightarrow (v)$ por contradicción, para algún p divisor primo de $|G|$ existe un P $p-$ subgrupo de Sylow de G no es normal en G, es decir, $N_G(P) \neq G$ entonces $N_G(P) < G$.
Tomemos ahora M subgrupo maximal de G (posiblemente M sea $N_G(P)$) que contiene $N_G(P)$, que satisface

$$P \leq N_G(P) \leq M < G \tag{5.1.1}$$

Sea $g \in G$, un elemento arbitrario, tenemos $P^g \subseteq M^g \subseteq M$, la segunda inclusión es cierta pues M es normal. Tenemos que P y P^g son $p-$ subgrupos de Sylow de G contenidos en M entonces, P y P^g son $p-$ subgrupos de Sylow de M. Luego, por el segundo Teorema de Sylow, existe $x \in M$ tal que:

$$P^g = P^x \Leftrightarrow g^{-1}Pg = x^{-1}Px \Leftrightarrow (gx^{-1})^{-1}Pgx^{-1} = P,$$

entonces $gx^{-1} \in N_G(P)$ entonces $g \in N_G(P)x \subseteq N_G(P)M$.
Como g fue tomado arbitrario, se sigue que $G \subseteq N_G(P)M$ y como $N_G(P)M \subseteq G$, entonces $N_G(P)M = G$. Mas aún $G = N_G(P)M \leq M$ y $M < G$ entonces $G = M$, esto es absurdo, porque los subgrupos maximales son subgrupos propios. Por tanto (v) no puede ser falsa.
$(v) \Rightarrow (vi)$. Supongamos que G tiene orden $p_1^{r_1}p_2^{r_2}\cdots p_n^{r_n}$, donde los p_is son primos distintos y $r_i \in \mathbb{N}$. Mas aún, sean $P_i s$ p_i-subgrupos de Sylow correspondientes a los $p_i s$ primos. Luego como cada subgrupo de Sylow de G es normal entonces por el Corolario (5.3), estos subgrupos de Sylow son únicos y de orden $p_i^{r_i}$ para cada p_i.
Entonces para P_i, P_j para $i \neq j$ tienen intersección trivial, pues son únicos.
Como P_i, P_j son normales para $i \neq j$, tenemos $g_j^{-1}g_ig_j \in P_i$ entonces $g_i^{-1}g_j^{-1}g_ig_j \in P_i$; de forma similar $g_i^{-1}g_jg_i \in P_j$ entonces $g_j^{-1}g_i^{-1}g_jg_i \in P_j$. Por tanto

$$g_i^{-1}g_j^{-1}g_ig_j = [g_i, g_j] \in P_i \cap P_j = \{e\}.$$

Así, los elementos de P_i conmutan con cada elemento de P_j para $i \neq j$.
Ahora definimos la aplicación

$$\varphi : P_1 \times \cdots \times P_n \longrightarrow G$$

por

$$\varphi(g_1, \ldots, g_n) = g_1 \cdots g_n$$

la aplicación esta bien definida pues cada P_i subgrupo de Sylow es único.
Notemos lo siguiente, como cada elemento de P_i conmutan con cada elemento de P_j para $i \neq j$, entonces φ es un homomorfismo pues, sean $(g_1, \ldots, g_n)$ y $(h_1, \ldots, h_n)$ en $P_1 \times \cdots \times P_n$ tal que

$$\varphi((g_1, \ldots, g_n)(h_1, \ldots, h_n)) = \varphi(g_1h_1, \ldots, g_nh_n) = g_1h_1 \cdots g_nh_n$$

$$= g_1 \cdots g_n h_1 \cdots h_n = \varphi(g_1, \ldots, g_n)\varphi(h_1, \ldots, h_n)$$

Ahora mostremos que φ es inyectivo. Supongamos que

$$\varphi(h_1, \ldots, h_n) = h_1 \cdots h_n = e$$

para $h_i \in P_i$. Como h_i y h_j conmutan y tienen orden coprimo cuando $i \neq j$, tenemos

$$|h_1 h_2 \cdots h_n| = |h_1||h_2| \cdots |h_n| = 1.$$

Es decir $|h_1| = |h_2| = \cdots = |h_n| = 1$, y así $h_1 = h_2 = \cdots = h_n = e$. Luego el $ker\varphi$ es trivial. Esto prueba que φ es un homomorfismo inyectivo, como φ es un homomorfismo entre grupos finitos de igual orden, entonces φ es suryectivo. Se sigue que φ es un isomorfismo. Por tanto, G es un producto directo de sus subgrupos de Sylow.

$(vi) \Leftrightarrow (vii)$. Supongamos que $G = P_1 \times \cdots \times P_n$, donde los $P_i s$ son p_i-subgrupos de Sylow, correspondientes a los p_i primos distintos. Sean $g = g_1 \cdots g_n$ y $h = h_1 \cdots h_n$ elementos de orden coprimo en G, donde g_i, $h_i \in P_i$.

$$[g_i, g_j] = [h_i, h_j] = 1$$

para $i \neq j$, pues los P_i son subgrupos de Sylow normales y únicos. Luego $|g| = |g_1| \cdots |g_n|$ y $|h| = |h_1| \cdots |h_n|$. Luego, $|g|$ y $|h|$ son coprimos, sólo si $|g_i|$ ó $|h_i|$ es igual a 1 para cada $i = 1, 2, \ldots, n$, entonces g_i ó h_i son elementos triviales para cada $i = 1, 2, \ldots, n$. Concluimos que $gh = hg$.

Recíprocamente, supongamos que los elementos de orden coprimo conmutan. Sean $p_1, \ldots, p_n$ primos distintos divisores de G, y sean $P_1, \ldots, P_n$ los correspondientes subgrupos de Sylow asociados a los primos $p_i s$.

Mostraremos que los $P_i s$ subgrupos de Sylow son normales. Sea $g \in G$ y $h \in P_i$ para algún $i = 1, \ldots, n$. Si $g \in P_i$, entonces $h^g \in P_i$. Si $g \notin P_i$, entonces $g \in P_j$ con $j \neq i$, luego g y h tienen orden coprimo, por hipótesis ellos conmutan, es decir $[g, h] = e \Leftrightarrow gh = hg$, así $h^g = h \in P_i$. Por tanto $P_i \trianglelefteq G$. Mas aún, $G = P_1 P_2 \cdots P_n$, pues P_i y P_j son subgrupos de Sylow normales entonces conmutan para $i \neq j$.

Ahora afirmemos que $P := P_j \cap \prod_{i \neq j} P_i = \{e\}$. Por el Teorema de Lagrange, $|P|$ es un divisor de $|P_j|$ y también de $|\prod_{i \neq j} P_i|$. Mas aún $|\prod_{i \neq j} P_i|$ divide a $\prod_{i \neq j} |P_i|$, luego por transitividad $|P|$ divide a $\prod_{i \neq j} |P_i|$. Por tanto $|P|$ divide al máximo común divisor

de $|P_j|$ y $\prod_{i\neq j}|P_i|$, pero los $P_i s$ subgrupos de Sylow son normales únicos, es decir los órdenes de estos subgrupos son coprimos, por tanto $P = \{e\}$.
$(vii) \Rightarrow (i)$. Supongamos que elementos de orden coprimo conmutan. Por $(vii) \Rightarrow (vi)$, G es el producto directo de sus subgrupos de Sylow. Como los subgrupos de Sylow tienen orden potencia prima,es decir son p-grupos, cada uno de ellos es nilpotente por Teorema (5.1). Luego el producto de grupos nilpotentes es nilpotente por Teorema (4.5). Por tanto G es un grupo nilpotente finito. □

5.2. Subgrupo de Frattini

Definición 5.2. *Sea G un grupo, la intersección de todos los subgrupos maximales de G es llamado el subgrupo de Frattini de G, este es denotado $\Phi(G)$. Si G no tiene subgrupo maximal $\Phi(G) = G$, por convenio.*

Ejemplo 12. *(i)* $\Phi(A_5) = \{e\}$,
(ii) $\Phi(C_4 \times C_4) = C_2 \times C_2$,
(iii) $\Phi(C_{32}) = C_{16}$.

Lema 5.1. *(Argumento de Frattini). Sea G un grupo finito, $K \lhd G$, y P es un subgrupo de Sylow de K, entonces*

$$G = N_G(P)K.$$

Demostración. Para todo $g \in G$, tenemos

$$g^{-1}Pg \subseteq g^{-1}Kg = K,$$

ya que $P \leq K \lhd G$. Luego P y $g^{-1}Pg$ son subgrupos de Sylow de K además son conjugados en K. Por tanto, podemos encontrar $k \in K$ que satisface

$$k^{-1}(g^{-1}Pg)k = (gk)^{-1}P(gk) = P$$

entonces $gk \in N_G(P)$, luego $g \in N_G(P)k^{-1} \subseteq N_G(P)K$. Como $g \in G$ fue tomado arbitrario, entonces $G \subseteq N_G(P)K$ y como $N_G(P)K \subseteq G$, entonces $N_G(P)K = G$ □

Lema 5.2. $\Phi(G) \lhd G$.

Demostración. Si G no tiene subgrupo maximal, entonces $\Phi(G) = G$, el resultado se sigue. Un automorfismo asigna un subgrupo maximal a un subgrupo maximal, esto es una consecuencia del teorema de la correspondencia. Por lo tanto esto se mantiene para todo automorfismo interior,

$$f_g\, G \to G, \text{ definida por } f_g(M) = g^{-1}Mg$$

sea M subgrupo maximal de G, luego como M es maximal resulta $g^{-1}Mg = M$, así M es subgrupo normal de G. Luego la intersección de subgrupos normales es normal. Por tanto $\Phi(G) \lhd G$. □

Lema 5.3. *Sea G finito, $H \leq G$ y $G = H\Phi(G)$, entonces $H = G$.*

Demostración. Por contradicción, si $H \neq G$, entonces existe un subgrupo maximal J de G que contiene H, posiblemente J sea H si mismo. Luego $H \leq J$ y $\Phi(G) \leq J$ porque $\Phi(G)$ es la intersección de todos los subgrupos maximales de G. Como $G = H\Phi(G)$, luego $H\Phi(G) \leq J$ pues $\Phi(G) \trianglelefteq G$. Esto es absurdo. □

Teorema 5.5. *Sea G finito entonces $\Phi(G)$ es nilpotente.*

Demostración. Mostraremos que todos los subgrupos de Sylow de $\Phi(G)$ son normales en $\Phi(G)$. Si $\Phi(G) = \{e\}$ no hay nada que probar. Supongamos que $\Phi(G) > \{e\}$ y sea $\{e\} \neq P$ subgrupo de Sylow de $\Phi(G)$. Por el argumento de Frattini tenemos, $G = N_G(P)\Phi(G)$, pues $\Phi(G) \lhd G$. Luego por Lema (5.3) $N_G(P) = G$, que es $P \lhd \Phi(G)$. Esto se sigue para todos los subgrupos de Sylow P de $\Phi(G)$. □

Teorema 5.6. *Sea G finito, entonces G es nilpotente si y sólo si $G/\Phi(G)$ es nilpotente.*

Demostración. Sea G nilpotente, entonces sus grupos factores son nilpotentes por Teorema (4.4).

Recíprocamente, probaremos que todos los subgrupos de Sylow P de G, son normales en G. Ahora $P\Phi(G)/\Phi(G)$ es un p-subgrupo de Sylow de $G/\Phi(G)$ mostremos esta afirmación. Supongamos que $|G| = p^r m$, tal que $p \nmid m$, y $|P| = p^r$ pues P es p-subgrupo de Sylow de G. Supongamos que el orden de $G/\Phi(G)$ es

$$|G/\Phi(G)| = \frac{|G|}{|\Phi(G)|} = \frac{p^r m}{p^s} = p^{r-s}m,\ s < r$$

Luego

$$\left|\frac{P\Phi(G)}{\Phi(G)}\right| = \frac{|P\Phi(G)|}{|\Phi(G)|} = \frac{|P||\Phi(G)|}{|\Phi(G)||P\cap\Phi(G)|} = \frac{|P|}{|P\cap\Phi(G)|} = \frac{p^r}{p^s} = p^{r-s},$$

$P\cap\Phi(G)$ es un p-subgrupo de Sylow de $\Phi(G)$, $|\Phi(G)| = p^s$ y $|P\cap\Phi(G)| = p^s$. Por tanto $P\Phi(G)/\Phi(G)$ es un p-subgrupo de Sylow de $G/\Phi(G)$.
Como $G/\Phi(G)$ es nilpotente por hipótesis, esto muestra que

$$P\Phi(G)/\Phi(G) \lhd G/\Phi(G)$$

pues todos los subgrupos de *Sylow* son normales en grupos nilpotentes. Por el teorema de la correspondencia $P\Phi(G) \lhd G$. Como P es un p-subgrupo de Sylow de $P\Phi(G)$ y $P\Phi(G) \lhd G$, por el argumento de Frattini tenemos

$$G = N_G(P)P\Phi(G) = N_G(P)\Phi(G),$$

por el Lema 5.3 $G = N_G(P)$, así $P \lhd G$. Esto se sigue para todos los subgrupos de Sylow P de G. Por tanto G es nilpotente. □

Teorema 5.7. *Sea G finito, entonces G es nilpotente si y sólo si $G' \leq \Phi(G)$.*

Demostración. Sabemos, que si G es nilpotente si y sólo si todos sus subgrupos maximales son normales, por Teorema (5.4-iv). Sea H maximal, por hipótesis $H \lhd G$ y $H \neq G$, por Proposición (4) G/H es simple, es decir sus únicos subgrupos normales son $\{e\}$ y G/H. Así el orden de G/H es primo, en consecuencia G/H es cíclico (abeliano). Así $H \lhd G$ y G/H abeliano, entonces por Lema (2.2-ii) $G' \leq H$. Por tanto $G' \leq H$ para todo H maximal entonces $G' = \bigcap G' \leq \bigcap H = \Phi(G)$ así $G' \leq \Phi(G)$.
Recíprocamente, si $G' \leq \Phi(G)$, mostraremos que todo subgrupo maximal H de G es normal en G por Teorema (5.4-iv). Sea H un subgrupo maximal, luego $G' \leq \Phi(G) \leq H < G$.
Así $G' \leq H < G$ y $G' \lhd G$ esto por Lema (2.2-i),entonces $G' \lhd H$. Se sigue que $H/G' < G/G'$, pero como G/G' es abeliano, entonces $H/G' \lhd G/G'$, luego por el teorema de la correspondencia $H \lhd G$, esto se sigue para todos los subgrupos maximales H de G. Por tanto G es nilpotente. □

Para probar el teorema de estructura de grupos finitos abelianos, probaremos previamente lo siguiente

Teorema 5.8. *Sea G un p-grupo finito de orden p^n abeliano y C es un subgrupo de G cíclico del orden mayor posible, C generado por c, existe un subgrupo B de G de forma que $G = C \times B$.*

Notamos que G puede expresarse como el producto directo de un grupo cíclico de orden maximal en G y un subgrupo B de G llamado el complemento directo del subgrupo maximal. Este subgrupo B es también un p grupo, por tanto también lo podemos expresar como el producto directo de un subgrupo cíclico maximal de B y algún otro subgrupo de B. El proceso se repetirá y terminará en algún subgrupo cíclico, pues G es finito. Así G en el teorema (5.8) es el producto directo de subgrupos cíclicos.

Teorema 5.9. *(Teorema de estructura de los grupos finitos abelianos). Si G es un grupo finito abeliano, entonces G es producto directo de grupos cíclicos.*

Demostración. Como G es nilpotente, por Teorema (5.4-vi), G es producto directo de sus subgrupos de Sylow. Por Teorema (5.8) cada uno de los correspondientes subgrupos de Sylow se expresará como producto directo de cíclicos y por tanto G es producto directo de grupos cíclicos. □

Conclusiones

Todo grupo finito posee una serie, cuyos términos son sus subgrupos, y entre las series de un grupo, el mas destacado en el trabajo es el llamado serie central, para ello empleamos la noción del conmutador y el centro de un grupo.

Un grupo nilpotente, es un grupo que es casi abeliano, es decir, existe un natural n llamado la clase de nilpotencia, tal que aplicando la operación conmutación n-veces sobre el grupo G, siempre obtenemos la identidad, es decir la serie central descendente se estabiliza en algún n tal que $\gamma_{n+1}(G) = \{e\}$. De manera análoga mostramos que la serie central ascendente se estabiliza en el mismo n tal que $\mathscr{D}_n(G) = G$.

En toda estructura algebraica es común mostrar la cerradura bajo subgrupos, grupos cocientes, la imagen homomórfica y el producto directo finito de grupos. Y la clase de grupos nilpotentes cumple la cerradura de esas propiedades.

Vimos que todo grupo abeliano finito es nilpotente, y esta se escribe como el producto directo de sus subgrupos de Sylow. De aquí logramos mostrar el teorema de estructura de grupos abelianos finitos.

Caracterizar un grupo nilpotente finito, nos permitió mostrar criterios equivalentes para determinar si el grupo es o no nilpotente finito.

Para terminar todo grupo abeliano es un grupo nilpotente, pero no todo grupo nilpotente es abeliano. Mas aún, no habiendo definido qué es un grupo soluble, todo grupo nilpotente es soluble, pero no así el recíproco.

APÉNDICE A

Los Teoremas de Sylow

A.1. Acciones de grupos

Una *acción* de G en Y es una función

$$* : G \times Y \to Y$$

que asigna a cada elemento $\sigma \in G$ y $y \in Y$ un único elemento $\sigma * y \in Y$. Como G es un grupo, es natural pedir que esta acción de G en Y satisfaga las propiedades siguientes:
(i) Si e es el neutro de G, entonces para todo $x \in Y$ se tiene que $e * x = x$.
(ii) Si $\sigma\tau \in G$ y $x \in Y$, entonces $(\sigma\tau) * x = \sigma * (\tau * x)$.
Si Y es un conjunto en el cual se tiene una acción de G, diremos que Y es un G-conjunto.

Ejemplo 13. *Sea G cualquier grupo y sea $H \lhd G$ un subgrupo normal de G. Entonces, G actúa sobre H mediante conjugación, es decir, mediante la función $G \times H \to H$ dada por $\sigma * h = \sigma h \sigma^{-1}$. La propiedad (i) es cierta y para la propiedad (ii), sean $\sigma\tau \in G$ y $h \in H$. Entonces*

$$(\sigma\tau) * h = (\sigma\tau)h(\sigma\tau)^{-1} = \sigma(\tau h \tau^{-1})\sigma^{-1} = \sigma(\tau * h)\sigma^{-1} = \sigma * (\tau * h).$$

En particular, G actúa sobre sí mismo por conjugación.

Puntos fijos. Si un grupo G actúa sobre un conjunto Y, interesa saber como mueve G a los elementos de Y, y para esto suele ser útil estudiar los elementos de Y que no se

mueven, es decir que permanecen fijos bajo la acción de G, veamos desde dos puntos de vista:

(i) Si $\sigma \in G$ está dado, podemos considerar los elementos de Y que permanecen fijos bajo la acción de este σ y se define

$$Y^{\sigma} := \{x \in Y : \sigma * x = x\} \subseteq Y.$$

El conjunto Y^{σ} se llama el conjunto de puntos fijos de σ.

(ii) Si $x \in Y$ un elemento dado, consideramos el subconjunto de elementos del grupo G que dejan fijo a x, y se define

$$G_x := \{\sigma \in G : \sigma * x = x\} \subseteq G.$$

El conjunto G_x se llama el subgrupo *estabilizador* de x.

Lema A.1. *G_x es un subgrupo de G.*

Demostración. Claramente $e \in G_x$ pues $e * x = x$. Si $\tau, \sigma \in G_x$, entonces $(\tau\sigma) * x = \sigma * (\tau * x) = \tau * x = x$, y por lo tanto $\tau\sigma \in G_x$. Finalmente, si $\tau \in G_x$, entonces $\tau^{-1} * x = \tau^{-1} * (\tau * x) = (\tau^{-1}\tau) * x = e * x = x$ y así $\tau^{-1} \in G_x$. □

Órbitas. Si Y es un G-conjunto, se define la relación siguiente en Y: $x \sim y$ si existe $\sigma \in G$ tal que $\sigma * x = y$. Cuando $x \sim y$, diremos que x es G- equivalente a y. Ésta es una relación de equivalencia en Y ya que:

(i) Es *reflexiva*, $x \sim x$ pues $e * x = x$.

(ii) Es *simétrica*, si $x \sim y$ entonces existe $\sigma \in G$ tal que $\sigma x = y$ así $\sigma^{-1}y = \sigma^{-1}(\sigma x) = ex = x$ por tanto $y \sim x$.

(iii) Es *transitiva*, si $x \sim y$ y $y \sim z$, entonces existen $\sigma, \tau \in G$ tales que $\sigma x = y$ y $\tau y = z$. Se sigue que $(\tau\sigma)x = \tau(\sigma x) = \tau y = z$ así $x \sim z$.

Las clases de equivalencia de la relación anterior se llaman las *órbitas* de la acción de G en Y. A la órbita de $x \in Y$ la denotamos mediante

$$[x] = orb_G(x) = \{\sigma * x \in Y : \sigma \in G\}.$$

Ejemplo 14. *Si G es un grupo y G actúa sobre sí mismo por conjugación, es decir, $* : G \times G \to G$ esta dada por $\sigma * g = \sigma g \sigma^{-1}$, entonces para cada $g \in G$ su grupo de*

isotropía G_g es:

$$G_g = \{\sigma \in G : \sigma * g = g\} = \{\sigma \in G : \sigma g \sigma^{-1} = g\}$$

$$= \{\sigma \in G : \sigma g = g\sigma\} = C_G(g) \text{ es el centralizador de } g \text{ en } G$$

Notemos que las órbitas de esta acción son, para $\sigma \in G$:

$$orb(\sigma) = \{a \in G : \sigma \sim a\} = \{a \in G : a = b\sigma b^{-1} \text{ para algún } b \in G\},$$

es decir, la órbita $orb(\sigma)$ es la clase de conjugación de σ.

A.2. Los teoremas de Sylow

Si Y es un G- conjunto, con Y y G finitos y si r es el número de órbitas en Y de la acción de G, sean $x_1, \ldots, x_r$ representantes de cada una de las órbitas. Como éstas forman una partición de Y, se tiene que

$$\mid Y \mid = \sum_{i=1}^{r} \mid orb_G(x_i) \mid .$$

Notemos ahora que algunas de las órbitas pueden tener un solo elemento, y cuando esto sucede este elemento x no mueve ningún elemento de G, es decir, queda fijo bajo todo $\sigma \in G$, i.e., $\sigma x = x$ para todo $\sigma \in G$. Pongamos entonces

$$Y^G := \{x \in Y : \sigma x = x, \text{ para todo } \sigma \in G\},$$

es decir, Y^G es la unión de todas las órbitas con un solo elemento. Sea $s = \mid Y^G \mid$ y observe que $0 \leq s \leq r$. Si $x_1, \ldots, x_s$ son los elementos de las órbitas con un sólo elemento, y $x_{s+1}, \ldots, x_r$ son representantes de las órbitas con más de un elemento, entonces

$$|Y| = |Y^G| + \sum_{i=s+1}^{r} |orb_G(x_i)| \tag{A.2.1}$$

Ejemplo 15. *Si G es un grupo finito, $Y = G$ y se hace actuar G sobre sí mismo por conjugación, entonces las órbitas de la acción son las clases de conjugación de G. Observe ahora que las órbitas que tienen un sólo elemento $orb_G(x) = x$ satisfacen que*

$gxg^{-1} = x$, i.e., $gx = xg$ para todo $g \in G$ y por lo tanto x debe estar en el centro $Z(G)$ de G. Se sigue que

$$Y^G = Z(G).$$

Finalmente, si denotamos con $C_1, \ldots, C_t$ las clases de conjugación de G con más de un elemento, (A.2.1) se vuelve

$$|G| = |Z(G)| + \sum_{i=1}^{t} |C_i|$$

a la que se llama la ecuación de clases de G. Ahora, como $|C_i| = |orb_G(x_i)| = [G : G_{x_i}]$, la ecuación de clases se puede escribir como

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : G_{x_i}].$$

Teorema A.1. *Sea G un grupo de orden p^n, para p un entero primo y sea Y un G-conjunto finito. Entonces*

$$| Y | \equiv | Y^G | \ (módp).$$

Demostración. Como $|orb_G(x)| = [G : G_x]$ y por el teorema de lagrange $[G : G_x]$ divide a $|G| = p^n$, y por lo tanto $p \mid [G : G_x]$ y así p divide a $|orb_G(x_i)|$, para $s + 1 \leq i \leq r$. Entonces la igualdad $|Y| = |Y^G| + \sum_{i=s+1}^{r} |orb_G(x_i)|$ de la observación previa implica que p divide a $|Y| - |Y^G|$, como se quería. □

Teorema A.2. *(Cauchy). Si G es un grupo finito y p es un primo que divide a $|G|$, entonces G tiene un elemento de orden p y por lo tanto G tiene un subgrupo de orden p.*

Demostración. Sea Y el conjunto

$$Y = \{(\sigma_1, \ldots, \sigma_p) : \sigma_j \in G \text{ y } \sigma_1 \cdots \sigma_p = e\},$$

y observe que $Y \neq \emptyset$ ya que $(e, \ldots, e) \in Y$. Mostraremos que p divide a $|Y|$. En efecto, observando que $(\sigma_1, \ldots, \sigma_p) \in Y \Leftrightarrow \sigma_p = (\sigma_1, \ldots, \sigma_{p-1})^{-1}$, se sigue que las primeras $p - 1$ componentes de las p-adas de Y pueden ser cualesquiera elementos de G y la última (o la primera) componente está determinada por las otras $p - 1$ componentes; por lo tanto $|Y| = |G|^{p-1}$, y como p divide a $|G|$ por hipótesis, entonces p divide a $|Y|$

como se quería.

Consideremos ahora el ciclo $\theta = (1, 2, \ldots, p) \in S_p$ y hagamos actuar θ sobre Y mediante:

$$\theta \cdot (\sigma_1, \ldots, \sigma_p) := (\sigma_{\theta(1)}, \ldots, \sigma_{\theta(p)}) = (\sigma_2, \sigma_3, \ldots, \sigma_p, \sigma_1),$$

donde notamos que $\theta \cdot (\sigma_1, \ldots, \sigma_p) \in Y$, ya que si $(\sigma_1, \ldots, \sigma_p) \in Y$, por definición de Y se tiene que $\sigma_1(\sigma_2 \cdots \sigma_p) = e$, y por lo tanto $\sigma_1 = (\sigma_2 \cdots \sigma_p)^{-1}$ y así $(\sigma_2 \cdots \sigma_p)\sigma_1 = e$, i.e., $(\sigma_2, \ldots, \sigma_p, \sigma_1) \in Y$ como se quería. Se sigue que el grupo cíclico $\langle\theta\rangle$ actúa sobre Y, por iteración de la acción de θ.

Observe ahora que $|\langle\theta\rangle| = p$ y así, por el teorema anterior, se tiene que

$$|Y| \equiv |Y^{\langle\theta\rangle}|(mód p),$$

y como p divide a $|Y|$, la congruencia anterior implica que p divide a $|Y^{\langle\theta\rangle}|$.

Observe también que el ciclo θ (y por lo tanto el grupo $\langle\theta\rangle$) fija a $(\sigma_1, \ldots, \sigma_p)$ si y sólo si $\sigma_1 = \cdots = \sigma_p$. Y por otra parte como $(e, \ldots, e) \in Y^{\langle\theta\rangle}$ por lo que $Y^{\langle\theta\rangle}$ es no vacío y como p divide a $|Y^{\langle\theta\rangle}|$, se sigue que $Y^{\langle\theta\rangle}$ debe tener al menos p elementos y consecuentemente existe un $(\sigma, \ldots, \sigma) \in Y^{\langle\theta\rangle}$ con $\sigma \neq e$ tal que $\sigma^p = e$, es decir, σ tiene orden p como se quería.

Finalmente, el subgrupo cíclico generado por σ es de orden p ya que σ es de ese orden.

□

El normalizador de un subgrupo. Dado un grupo G, denotemos con Y a la familia de todos los subgrupos de G y hagamos actuar G en Y mediante conjugación: si $H \in Y$ y $\sigma \in G$, la acción está dada por

$$\sigma * H := \sigma H \sigma^{-1} \in Y.$$

claramente $e * H = eHe^{-1} = H$.

Y si $\sigma, \tau \in G$, entonces

$$(\sigma\tau) * H = (\sigma\tau)H(\sigma\tau)^{-1} = \sigma(\tau * H)\sigma^{-1} = \sigma * (\tau * H).$$

Ahora, dado un $H \in Y$ consideremos su subgrupo de isotropía

$$G_H := \{\sigma \in G : \sigma H \sigma^{-1} = H\},$$

y observe que $H \lhd G_H$ ya que claramente H es un subgrupo de G_H y es normal porque los elementos σ de G_H son tales que $\sigma H \sigma^{-1} = H$. Más aún, G_H es el mayor subgrupo de G que tiene a H como subgrupo normal, ya que si $K \subseteq G$ es tal que $H \lhd K$ entonces todos los elementos τ de K son tales que $\tau H \tau^{-1} = H$ y por lo tanto $\tau \in G_H$ ya que G_H consiste de todos los elementos de G que fijan a H bajo conjugación. El subgrupo G_H se llama el *normalizador* de H en G y lo denotaremos por $N_G(H)$.

Lema A.2. *Sea G un grupo finito. Si H es un subgrupo de orden una potencia de un primo p, entonces*

$$[N(H) : H] \equiv [G : H] (m\acute{o}dp).$$

Si H es un grupo finito cuyo orden es una potencia de un primo p, se dice que H es un p- grupo.

Demostración. Hagamos actuar G en el conjunto $Y = G/H$ de clases laterales izquierdas de H en G, mediante traslación izquierda, i.e., si $\sigma \in G$ y $\tau H \in G/H$, entonces $\sigma * \tau H = (\sigma\tau)H$. Claramente $Y = G/H$ resulta un G-conjunto y $|G/H| = [G : H]$ por el teorema de Lagrange. Para el subgrupo $H \subseteq G$ denotemos con Y^H al conjunto de puntos fijos de $Y = G/H$ bajo la acción de los elementos de H, i.e.,

$$Y^H = (G/h)^H := \{\tau H \in G/H : h * (\tau H) = \tau H \text{ para todos los } h \in H\}.$$

Observe ahora que

$$h(\tau H) = \tau H \Leftrightarrow \tau^{-1} h \tau H = H \Leftrightarrow \tau^{-1} h \tau \in H$$

y por lo tanto

$$h(\tau H) = \tau H \text{ para todos los } h \in H \Leftrightarrow \tau^{-1} h \tau \in H \text{ para todos los } h \in H$$

y este último sucede $\Leftrightarrow \tau \in N(H)$ y consecuentemente,

$$\tau H \in (G/H)^H \Leftrightarrow \tau H \in N(H)/H,$$

es decir la función $Y^H \to N(H)/H$ dada por $\tau H \mapsto \tau H$ es biyectiva y así

$$|(G/H)^H| = |N(H)/H| = [N(H) : H].$$

Finalmente, por 9.1 se tiene que $|G/H| = |Y| \equiv |Y^H| = |(G/H)^H|(módp)$, de donde se sigue

$$[N(H) : H] = |(G/H)^H| \equiv |G/H| = [G : H](módp).$$

□

Los teoremas de Sylow. Llegamos a un punto en el cual podemos probar los recíprocos parciales del teorema de Lagrange y que constituyen, de alguna forma, el inicio del estudio de los grupos finitos. Recordemos que el teorema de Lagrange nos dice que si G es un grupo finito, el orden de cualquier subgrupo H de G divide al orden de G. El recíproco no es cierto.

Definición A.1. *Sea p un número primo. Un p-subgrupo de Sylow de un grupo finito G es un p-subgrupo máximo P. Es decir, si Q es un p-subgrupo de G y $P \leq Q$, entonces $P = Q$.*

El primer teorema de Sylow nos dice que si G es finito, entonces G contiene subgrupos de orden ciertos divisores de $|G|$:

Teorema A.3. *(Primer teorema de Sylow). Sea G un grupo finito de orden n y supongamos que p es un primo tal que $n = p^m t$ con $m \geq 1$ y $p \nmid t$. Entonces, G contiene un subgrupo de orden p^j para todo j tal que $1 \leq j \leq m$.*

Demostración. Por inducción sobre j. Si $j = 1$, por el teorema de Cauchy G contiene un subgrupo de orden $p = p^1$. Supongamos ahora que el teorema es válido para $j < m$. Mostraremos que G contiene un subgrupo de orden p^{j+1}. En efecto, sea H un subgrupo de G de orden p^j. Como $j < m$ y $\mid G \mid = p^m t$, entonces $m - j \geq 1$ y así p divide a $p^{m-j}t = |G/H| = [G : H]$. El lema anterior implica que p divide a $[N(H) : H] = |N(H)/H|$. Aplicando de nuevo el teorema de Cauchy, se tiene que el grupo cociente $N(H)/H$ tiene un subgrupo K de orden p. Sea $\rho : N(H) \to N(H)/H$ el homomorfismo canónico y sea $L = \rho^{-1}(K) \subseteq N(H)$ la imagen inversa de K. Entonces L es un subgrupo de $N(H)$ que contiene a H (por el teorema de correspondencia entre subgrupos de $N(H)/H$ y subgrupos de $N(H)$ que contienen a H). Observe ahora que $K = \rho(L) = L/H$ y así $|K| = |L/H| = |L|/|H|$ por lo que

$$|L| = |K| \cdot |H| = p \cdot p^j = p^{j+1},$$

como se quería. □

Si G es un grupo finito de orden n y si p es un primo tal que $n = p^m t$ con $m \geq 1$ y $p \nmid t$, a un subgrupo $L \subseteq G$ de orden p^m se llama un *p-subgrupo de Sylow* de G. En otras palabras, un p-subgrupo de Sylow de G es un p-subgrupo de G de orden máximo.

Observación Si $L \subseteq G$ es un p-subgrupo de Sylow de G, entonces para todo $\sigma \in G$ el conjugado $\sigma L \sigma^{-1}$ también es un un p-subgrupo de Sylow de G. El segundo teorema de Sylow dice que cualesquiera dos p-subgrupos de Sylow de G son conjugados.

Teorema A.4. *(Segundo teorema de Sylow). Sea G un grupo finito de orden n y supongamos que H_1 y H_2 son dos p-subgrupos de Sylow de G. Entonces H_1 y H_2 son conjugados.*

Demostración. La idea es hacer que uno de los dos subgrupos, digamos H_2, actúe sobre las clases laterales izquierdas del otro, digamos sobre $Y = G/H_1$. La acción natural es por traslación izquierda: si $h \in H_2$ y $\sigma H_1 \in Y$, entonces $h(\sigma H_1) = (h\sigma)H_1$. Claramente Y es un H_2-conjunto y por teorema (A.1) se tiene que

$$|Y^{H_2}| \equiv |Y| (mód p),$$

y como H_1 es un p-subgrupo máximo en G, entonces $p \nmid |G/H_1| = |Y|$ por lo que la congruencia anterior implica que $|Y^{H_2}| \neq 0$. Sea pues $\sigma H_1 \in Y^{H_2} = (G/H_1)^{H_2}$. Entonces, $h(\sigma H_1) = \sigma H_1$ para todo $h \in H_2$ y así $\sigma^{-1} h \sigma H_1 = H_1$ para todo $h \in H_2$. Se sigue que $\sigma^{-1} h \sigma \in H_1$ para todo $h \in H_2$, i.e., $\sigma^{-1} H_2 \sigma \subseteq H_1$. Finalmente, como $|H_1| = |H_2| = |\sigma^{-1} H_2 \sigma|$, la inclusión anterior implica que $\sigma^{-1} H_2 \sigma = H_1$, como se quería. □

El tercer teorema de Sylow nos da información sobre el número de p-subgrupos de Sylow de un grupo finito G:

Teorema A.5. *(Tercer teorema de Sylow). Sean G un grupo finito de orden n y p un primo tal que $p|n$. Entonces, el número n_p de p-subgrupos de Sylow de G es congruente con 1, módulo p, y $n_p = [G : N_G(P)]$, donde P es cualquier p-subgrupo de Sylow de G; se sigue que n_p divide al orden n de G.*

Demostración. Sea H un p-subgrupo de Sylow de G y sea Y la familia de todos los p-subgrupos de Sylow de G. Hagamos actuar a H sobre Y mediante conjugación: si $h \in H$ y $L \in Y$, entonces $h * L := hLh^{-1}$. Por teorema (A.1) se tiene que

$$|Y| \equiv |Y^H|(módp).$$

Ahora como $Y^H = \{L \in Y : hLh^{-1} = L \text{ para todo } h \in H\}$, entonces $H \subseteq N(L)$ para todo $L \in Y^H$ y además $L \lhd N(L)$. Como H y L son p-subgrupos de Sylow de G, entonces lo son de $N(L)$ y por el segundo teorema de Sylow se sigue que H y L son conjugados en $N(L)$; pero como $L \lhd N(L)$, entonces su único conjugado es él mismo y así $H = L$. Hemos así mostrado que $Y^H = H$ y por lo tanto, la congruencia $|Y| \equiv |Y^H|(módp)$ implica que

$$|Y| \equiv 1(módp),$$

lo cual prueba la primera afirmación del teorema.

Para la segunda afirmación, hagamos actuar G en Y mediante conjugación.como todos los p-subgrupos de Sylow son conjugados entre sí entonces sólo hay una órbita de esta acción de G en Y, digamos $orb_G(H)$ para $H \in Y$. Se sigue que

$$|Y| = |orb_G(H)| = [G : G_H], \tag{A.2.2}$$

donde G_H es el subgrupo de isotropía de H, i.e., $G_H = N_G(H)$ es el normalizador de H en G. Ahora, como $[G : G_H]$ es un divisor de $|G|$ por el teorema de Lagrange, entonces A.2.2 implica que el número de p- subgrupos de Sylow, $|Y|$, divide a $|G|$, como se quería. □

Bibliografía

[1] Derek J. S. Robinson, *Abstract Algebra, 2nd Edition*, University of Illinois.

[2] Anthony E. Clement, Stephen Majewicz, Marcos Zyman, *The Theory of Nilpotent Groups*, Birkhauser 2017.

[3] Harvey E. Rose, *A Course on Finite Groups*, University of Bristol, 2009.

[4] Thiago Feipe da Silva, *Nilpotencia y p-Nilpotencia de Grupos Finitos*, Campina Grande-PB, 2015.

[5] Elizabeth Kravchenco, *Estructuras Algebraicas Series Normales y Subnormales*, 2006.

[6] Felipe Zaldivar, *Introducción a la teoría de grupos*, Sociedad Matemática Mexicana, 2006.

[7] Joseph A. Gallian, *Comtemporary Abstract Algebra, 9th Edition*, University of Illinois.