# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE CIENCIAS

# SOBRE GRUPOS FINITOS CON TODOS SUS SUBGRUPOS PROPIOS NILPOTENTES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A:

**FRANCISCO GONZÁLEZ BAYONA**

DIRECTOR DE TESIS:
DOCTOR JUAN MORALES RODRÍGUEZ

CIUDAD UNIVERSITARIA, CD. MX. 2018

1. Datos del alumno
González
Bayona
Francisco
55 44 93 75 16
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas
309051297

2. Datos del tutor
Dr
Juan
Morales
Rodríguez

3. Datos del sinodal 1
Dr
Hugo Alberto
Rincón
Mejía

4.Datos del sinodal 2
Dr
Emilio Esteban
Lluis
Puebla

5. Datos del sinodal 3
Mat
José Roberto
de la Vega
Martínez

6. Datos del sinodal 4
Dra
María del Carmen
Gómez
Laveaga

7. Datos del trabajo escrito
Sobre grupos finitos con todos sus subgrupos propios nilpotentes
37 p
2018

# Agradecimientos

Mi sincero agradecimiento al Dr. Juan Morales Rodríguez y a José Roberto de la Vega Martínes por su ayuda, sugerencias e ideas brindadas al realizar este trabajo, así como a quienes con sus observaciones enriquecieron este trabajo. En particular los profesores Hugo Rincón, María del Carmen Gomez y Emilio Lluis.

Con amor a Moni que me ha impulsado, apoyado y ha estado a mi lado para darme ánimo.

# Índice General

## Introducción

El propósito de este trabajo es estudiar, siguiendo a Reinhold Baer, los grupos finitos no nilpotentes con todos sus subgrupos propios nilpotentes. Para ello primero se recuerdan algunas propiedades de los $p$-grupos finitos y de los grupos abelianos finitos que son ejemplos de grupos nilpotentes. Se define grupo nilpotente finito, se caracterizan los grupos de esta clase y se estudian algunas de sus propiedades elementales.

Después se estudia la clase de los grupos finitos solubles no nilpotentes con todos sus subgrupos normales propios nilpotentes, se prueba que los grupos finitos con todos sus subgrupos propios nilpotentes son solubles. También se prueba un caso especial del célebre teorema de Maschke que nos será de utilidad.

Por último se presenta una caracterización de grupos finitos no nilpotentes con todos sus subgrupos propios nilpotentes que es el objetivo principal de este trabajo.

En el primer apartado de este trabajo se enuncian definiciones y resultados que se utilizan a lo largo de este estudio. La notación y convenciones que se usan en esta tesis coinciden, en general, con las usados por J.J. Rotman en [4]. Se consideró pertinente agregar las demostraciones de algunos de los resultados enunciados en este apartado.

**Definiciones y resultados preliminares:**

En este trabajo los grupos considerados son finitos, a menos que se especifique lo contrario.

**Definición.** Si $X$ es un subconjunto de un grupo $G$, el subgrupo generado por $X$, denotado como $\langle X\rangle$, es la intersección de todos los subgrupos de $G$ que contienen a $X$.
Si $X$ es un conjunto finito $\{x_1,...,x_n\}$, en lugar de $\langle\{x_1,...,x_n\}\rangle$ escribimos $\langle x_1,...,x_n\rangle$.

**Teorema.** Si $X$ es un subconjunto no vacío de un grupo $G$, el subgrupo generado por $X$ es el subconjunto formado por todos los productos de la forma $x_1^{\alpha_1}...x_n^{\alpha_n}$, con $n \geqslant 1$, todas las $x_i$ elementos de $X$ y $\alpha_i = \pm 1$ para cualquier $i$.

**Definición.** Un grupo $G$ es cíclico si es generado por un solo elemento, es decir, si existe $g$ en $G$, tal que $\langle g\rangle = G$.

**Definición.** Un grupo $G$ es abeliano si para cualquier par de elementos $a$ y $b$ de $G$, $ab = ba$.

**Definición.** Si $H$ y $K$ son subconjuntos de un grupo $G$, su producto $HK$ es $\{hk|h \in H, k \in K\}$, y $H^{-1} = \{h^{-1}|h \in H\}$.
Si $H = \{h\}$ en lugar de $\{h\}K$ se escribe simplemente $hK$.

**Definición.** Si $H$ es un subgrupo de $G$, una clase izquierda de $H$ es el subconjunto $gH$ para algún elemento $g$ de $G$. De igual forma una clase derecha de $H$ es el subconjunto $Hg$ para algún elemento $g$ de $G$.

**Teorema.** Sea $G$ un grupo, $H$ un subgrupo de $G$ y $a$ y $b$ elementos de $G$. $aH = bH$ si y sólo si $a^{-1}b$ es un elemento de $H$, de igual forma $Ha = Hb$ si y sólo si $ba^{-1}$ es un elemento de $H$.

**Teorema.** Si $G$ es un grupo y $H$ un subgrupo de $G$, el conjunto de las clases izquierdas (o derechas) forman una partición de $G$ y cada elemento de la partición tiene $|H|$ elementos.

**Teorema.** Si $G$ es un grupo y $H$ es subgrupo de $G$, existe una biyección entre las clases izquierdas y las clases derechas de $H$ en $G$.

**Definición.** Si $G$ es un grupo y $H$ es un subgrupo de $G$, el índice de $H$ en $G$ es el número de clases izquierdas de $H$ en $G$ y se denota como $[G : H]$.

**Definición.** Si $X$ es un subconjunto de un grupo $G$, el orden de $X$, denotado como $|X|$, es el número de elementos de $X$.

**Definición.** Si $g$ es un elemento de un grupo $G$, el orden de $g$ es $|\langle g\rangle|$.

**Definición.** Un grupo $G$ de orden $2n$ es llamado diédrico si es generado por dos elementos $s$ y $t$ de órdenes $n$ y dos respectivamente que cumplen que $tst = s^{-1}$. Dicho grupo se denota como $D_{2(n)}$.

**Teorema (Lagrange).** Si $G$ es un grupo y $H$ es un subgrupo de $G$, $|G| = |H|[G : H]$.

**Teorema.** $G$ es un grupo cíclico si y sólo si para cada número natural $n$, divisor de su orden, $G$ tiene un único subgrupo de orden $n$.

**Teorema.** Si $G$ es un grupo abeliano y el entero positivo $m$ divide el orden de $G$, $G$ tiene un subgrupo de orden $m$.

**observación.** El grupo de permutaciones pares de un conjunto de cuatro elementos denotado como $A_4$, tiene orden doce y no tiene subgrupos de orden seis.

**Teorema.** Si $G$ es un grupo no trivial que no tiene subgrupos no triviales, $G$ es de orden primo.

**Demostración.** Si $g$ es un elemento de $G$ diferente del idéntico, el subgrupo generado por $g$ tiene que ser todo $G$ por lo que $G$ es cíclico, y al ser cíclico tiene un subgrupo por cada divisor de su orden, pero como no tiene subgrupos no triviales entonces $G$ tiene orden primo.

**Definición.** Un subgrupo $M$ de un grupo $G$ es máximo si está contenido propiamente en $G$ y no existen subgrupos propios de $G$ que contengan propiamente a $M$.

**Teorema.** Si $G$ es un grupo que tiene un único subgrupo máximo, $G$ es cíclico.

**Demostración.** Sea $M$ el único subgrupo máximo de $G$ y tomemos $g$ un elemento de $G$ que no sea elemento de $M$. Si $g$ no generara a todo $G$ , el subgrupo generado por $g$ estaría contenido en el único subgrupo máximo $M$ lo cual sería una contradicción. Por lo tanto $g$ genera a todo $G$ y $G$ es cíclico.

**Observación.** En el teorema anterior la hipótesis de que $G$ sea finito es necesaria. $\mathbb{Z}_5 \times \mathbb{Q}$ tiene como único subgrupo máximo a $\mathbb{Q}$, sin embargo no es cíclico.

**Teorema.** Si $G$ es un grupo y $K \leq H \leq G$, entonces $[G:K] = [H:K][G:H]$.

**Demostración.**
$[G:K]|K| = |G| = [G:H]|H| = [G:H][H:K]|K|$, por lo que $[G:K] = [G:H][H:K]$.

**Teorema.** Si $G$ es un grupo, un subconjunto $H$ de $G$ es un subgrupo si y solo si $HH = H = H^{-1}$.

**Teorema.** Si $G$ es un grupo y $H$ y $K$ son subgrupos de $G$, el producto $HK$ es un subgrupo de $G$ si y solo si $HK = KH$.

**Demostración.** Primero supongamos que $HK$ es un subgrupo de $G$, por lo tanto $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. Inversamente, si suponemos que $HK = KH$, se tiene $(HK)(HK) = H(KH)K = H(HK)K = HK$ y $(HK)^{-1} = (KH)^{-1} = H^{-1}K^{-1} = HK$.

**Teorema.** Si $H$ y $K$ son subgrupos de $G$, se tiene que $|H||K| = |HK||H \cap K|$.

**Demostración.** Consideremos la función $F : H \times K \longrightarrow HK$; $F(h,k) = hk$. Se puede dar una relación de equivalencia en $H \times K$ en donde dos elementos están relacionados si tienen la misma imagen, y como $F$ es suprayectiva el número de clases de equivalencia es $|HK|$ y dado que $|H \times K| = |H||K|$, solo faltaría probar que la cardinalidad de cada clase de equivalencia es $|H \cap K|$. Para esto supongamos

que $h$ y $k$ son elementos de $H$ y $K$ respectivamente, entonces si $g$ es un elemento de la intersección de $H$ y $K$ ocurre que $hk = hgg^{-1}k$ y así $(hg, g^{-1}k)$ está en la clase de equivalencia de $(h, k)$, por lo que cada clase de equivalencia tiene al menos $|H \cap K|$ elementos.
Ahora supongamos que la pareja $(h', k')$ está en la clase de equivalencia de $(h, k)$, eso significa que $hk = h'k'$ por lo que $h'^{-1}h = k'k^{-1}$ y de ahí se tiene que $k'k^{-1}$ es un elemento de $H \cap K$. Además $h' = hkk'^{-1})$. Por lo tanto $(h, k) = (h(kk'^{-1}, (k'k^{-1})k)$ y eso prueba que cada clase de equivalencia tiene $|H \cap K|$ elementos.

**Definición.** Se dice que un subgrupo $N$ de $G$ es normal, y se denota como $N \trianglelefteq G$, si para cualquier elemento $g$ de $G$ se tiene que $gNg^{-1} = N$.

**Teorema.** $N$ es un subgrupo normal de un grupo $G$ si y sólo si para cualquier $g$ elemento de $G$ se tiene que $gN = Ng$.

**Teorema.** Si $G$ es un grupo abeliano, cualquier subgrupo de $G$ es normal.

**Observación.** El hecho de que $H \trianglelefteq N \trianglelefteq G$ no implica que $H \trianglelefteq G$. Por ejemplo consideremos al grupo de permutaciones de un conjunto de cuatro elementos denotado como $S_4$, que tiene como subgrupo normal al grupo de Klein $V = \{1, (12)(34), (13)(24), (14)(23)\}$. El grupo $H = \{1, (12)(34)\}$ es normal en $V$, sin embargo $H$ no es normal en $S_4$.

**Observación.** Para todo número natural $n \geqslant 2$, $n \neq 4$, $A_n$ es el único subgrupo normal propio no trivial de $S_n$. Para $n = 4$ los únicos subgrupos normales propios no triviales de $S_4$ son $V$ y $A_4$.

**Definición.** Un subgrupo $N$ de $G$ es un subgrupo normal máximo si $N$ es un subgrupo normal propio de $G$, y no existen subgrupos normales propios de $G$ que contengan propiamente a $N$.

**Definición.** Un subgrupo $N$ de $G$ es un subgrupo normal mínimo si $N$ es un subgrupo normal de $G$ diferente de la identidad, y no existen subgrupos normales no triviales de $G$ contenidos propiamente en $N$.

**Definición.** Decimos que un subgrupo $A$ de $G$ es subnormal en $G$ si existen $A_1, ..., A_d$ subgrupos de $G$ tales que:

$$A = A_1 \trianglelefteq A_2 \trianglelefteq ... \trianglelefteq A_d = G$$

Cuando un subgrupo $A$ de $G$ es subnormal en $G$ escribimos $A \trianglelefteq\trianglelefteq G$.

**Ejemplo.** El grupo $H = \{1, (12)(34)\}$ es un subgrupo normal de $V$, que es un subgrupo normal de $S_4$, por lo que $H \trianglelefteq\trianglelefteq S_4$ pero $H \ntrianglelefteq S_4$.

Por otro lado observemos que los subgrupos de orden dos de $S_3$ no son normales en $S_3$ y por motivos de orden tampoco pueden ser subnormales.

**Teorema.** Si $G$ es un grupo y $A$, $B$ Y $C$ son subgrupos de $G$ tales que $A \trianglelefteq\trianglelefteq B \trianglelefteq\trianglelefteq C$, entonces $A \trianglelefteq\trianglelefteq C$.

**Teorema.** Si $N$ es un subgrupo de $G$ y $[G:N]=2$, se tiene que $N$ es un subgrupo normal de $G$.

**Definición.** Al conjunto formado por las clases izquierdas (o derechas) de $N$ se le denota como $G/N$.

**Teorema.** Si $N$ es un subgrupo normal de un grupo $G$, $G/N$ es un grupo con la operación $aNbN = abN$.

**Definición.** Un grupo no trivial $G$ es simple si no tiene subgrupos normales no triviales.

**Observación.** Si un grupo $G$ es simple, cualquier subgrupo propio no trivial no es subnormal.

**Ejemplo.** Cualquier grupo de orden primo es simple; $A_n$ con $n \geqslant$ es simple. Évariste Galois conocía la simplicidad de $A_5$.

**Teorema.** Si $G$ es un grupo, $N$ un subgrupo normal de $G$ y $H$ un subgrupo de $G$ que cumple que $(|H|,[G:H])=1$, entonces también $(|H\cap N|,[N:H\cap N])=1$.

**Demostración.**

$$[HN:N] = |HN|/|N| = \frac{|H||N|}{|H\cap N||N|} = \frac{|H|}{|H\cap N|} = [H:H\cap N].$$

También, $[HN:H][H:H\cap N] = [HN:H\cap N] = [HN:N][N:H\cap N]$, por lo que $[HN:H] = [N:H\cap N]$. Esta última igualdad se usará más adelante.
Por la hipótesis sabemos que $(|H|,[G:H])=1$.
Debido a que $[HN:H]$ es un divisor de $[G:H]$, entonces $(|H|,[HN:H])=1$, y así $(|H|,[N:H\cap N])=1$.
Como $|H\cap N|$ es un divisor de $|H|$, concluimos que $(|H\cap N|,[N:H\cap N])=1$. ■

A un subgrupo $H$ de $G$ que cumple que $(|H|,[G:H])=1$ se le llama subgrupo de Hall de $G$. Lo que se acaba de probar es que si $N$ es un subgrupo normal de $G$ y $H$ un subgrupo de Hall de $G$ entonces $H\cap N$ es un subgrupo de Hall de $N$.

Con las hipótesis del teorema anterior, también es cierto que $HN/N$ es un subgrupo de Hall de $G/N$. En efecto, como $|HN/N| = |H|/|H\cap N|$, se tiene que $|HN/N|$ divide a $|H|$, además $[G/N : HN/N] = [G:HN]$, y como $[G:H]=[HN:H][G:HN]$, entonces $[G/N:HN/N]$ divide a $[G:H]$ y así, como por hipótesis $(|H|,[G:H])=1$, entonces también $(|HN/N|,[G/N:HN/N])=1$.

**Observación.** Si $N$ no es un subgrupo normal de $G$, puede ocurrir que $H\cap N$ no sea un subgrupo de Hall de $N$ aunque $H$ lo sea de $G$. Por ejemplo, consideremos el grupo $S_5$, y el subgrupo $H=\langle\{(1,2),(1,2,3,5)\}\rangle$, que es isomorfo a $D_{2(4)}$, que es un subgrupo de Hall de $S_5$ pues es de orden 8, pero si consideramos a $N$ el subgrupo de permutaciones de $S_5$ que deja fijo al 5, su intersección con $H$ es no trivial pues contiene al menos a $(1,2)$ pero no contiene a todo $H$, por lo que la intersección no puede ser un subgrupo de Hall de $N$.

**Definición.** Una función $F$ de un grupo $G$ a un grupo $H$, es un homomorfismo, si para cualesquiera $a$ y $b$ elementos de $G$, $F(ab)=F(a)F(b)$.

**Definición.** Una función $F$ de un grupo $G$ a un grupo $H$, es un isomorfismo, si $F$ es un homomorfismo y es biyectiva. Decimos que dos grupos son isomorfos si existe un isomorfismo de un grupo en el otro.

**Definición.** Un automorfismo de un grupo $G$, es un isomorfismo de $G$ en $G$.

**Teorema.** Los automorfismos de un grupo forman un grupo con la operación de composición de funciones.

**Definición.** Si $F : G \longrightarrow H$ es un homomorfismo, el nucleo de $F$ es el subgrupo de todos los elementos $g$ en $G$ tales que $F(g) = 1$.

**Teorema fundamental del homomorfismo.** Si $F : G \longrightarrow H$ es un homomorfismo de grupos cuyo núcleo es $K$, $K$ es un subgrupo normal de $G$ y $G/K$ es isomorfo a la imagen de $G$ bajo $F$.

Se tienen los siguientes dos teoremas importantes de isomorfismos.

**Teorema.** Si $N$ y $H$ son subgrupos del grupo $G$ y $N$ es normal, ocurre que $N \cap H$ es normal en $H$ y los grupos $H/N \cap H$ y $NH/N$ son isomorfos.

**Teorema.** Si $H$ y $K$ son subgrupos normales del grupo $G$ y $K \leqslant H$, entonces $H/K$ es normal en $G/K$ y además $(G/K)/(H/K) \cong G/H$.

**Teorema de la correspondencia.** Si $K$ es un subgrupo normal del grupo $G$, y $\varphi : G \longrightarrow G/K$ el homomorfismo canónico dado por $\varphi(g) = gK$, se tiene que la función $\Psi$ entre los subgrupos de $G$ que contienen a $K$ y los subgrupos de $G/K$ dada por $\Psi(H) = \varphi(H)$ es una biyección. Además, si $N_1$ y $N_2$ son subgrupos de $G$ que contienen a $K$, se tiene que $N_1 \leqslant N_2$ si y sólo si $\varphi(N_1) \leqslant \varphi(N_2)$, y en este caso $[N_2 : N_1] = [\varphi(N_2) : \varphi(N_1)]$, además $N_1 \trianglelefteq N_2$ si y sólo si $\varphi(N_1) \trianglelefteq \varphi(N_2)$.

**Teorema (ley de Dedekind).** Si $K$ y $L$ son subgrupos de $G$ y $H$ es un subgrupo de $L$, entonces $HK \cap L = H(K \cap L)$.

**Demostración.** Sea $l \in HK \cap L$, $l = hk$ con $h$ elemento de $H$ y $k$ elemento de $K$, observemos que $k = h^{-1}l$ es un elemnto de $L$ por lo que $l$ es un elemento de $H(K \cap L)$.
Inversamente, si $hx$ es un elemento de $H(K \cap L)$ con $h$ un elemento de $H$ y $x$ un elemento de $K \cap L$, $H$ es un elemento de $HK$ y $x$ es un elemento de $L$ por lo que $hx$ es un elemento de $HK \cap L$.

Observemos que en particular si $HK = G$ se tiene que $L = H(K \cap L)$.

**Definición.** El centro de un grupo $G$ denotado como $Z(G)$ es el subconjunto de los elementos $g$ de $G$ tales que $ga = ag$ para cualquier $a$ elemento de $G$.

**Teorema.** El centro de un grupo $G$ es un subgrupo normal.

**Teorema.** Si $G$ es un grupo, $H$ un subgrupo de $G$, $K$ un subgrupo de $Z(G) \cap H$ y $H/K$ es cíclico, entonces $H$ es abeliano.

**Demostración.** Sean $a$ y $b$ elementos de $H$, y sea $hK$ un elemento que genera a todo $H/K$, se tiene que $a = h^n k_1$ y $b = h^m k_2$, como $K$ es un subgrupo del centro de $G$ y las potencias de un elemento conmutan entre si, $ab = h^n k_1 h^m k_2 = h^n h^m k_2 k_1 = h^m k_2 h^n k_1 = ba$.

**Definición.** Si $H$ y $K$ son grupos, su producto directo $H \times K$ es el grupo de las parejas ordenadas $(h,k)$ con $h \in H$ y $k \in K$ con la operación $(h,k)(h',k') = (hh',kk')$.

**Teorema.** Si $H$ y $K$ son subgrupos normales de $G$, con $H \cap K = 1$, se tiene que $HK$ y $H \times K$ son isomorfos.

**Teorema.** Si un grupo $G$ es el producto directo de los subgrupos $H_1$ y $H_2$, cuyos órdenes son primos relativos, cualquier subgrupo $K$ es el producto directo de $K \cap H_1$ y $K \cap H_2$.

**Demostración.** $K \cap H_1 \trianglelefteq K$ pues si tomamos $k \in K$ y $h \in K \cap H_1$, entonces $khk^{-1} \in H_1$ (ya que $H_1 \trianglelefteq G$) y además es claro que $khk^{-1} \in K$ pues estamos multiplicando elementos de $K$. Análogamente $K \cap H_2 \trianglelefteq K$.
Luego, como $H_1 \cap H_2 = 1$, entonces el producto de $K \cap H_1$ con $K \cap H_2$ es un producto directo en $K$. Sabemos que todo elemento $k \in K$ es el producto $k = h_1 h_2$ con $h_i \in H_i$, $h_1$ y $h_2$ conmutan, pues por la normalidad de $H_1$ y $H_2$ en $G$ el producto $h_1 h_2 h_1^{-1} h_2^{-1} \in H_1 \cap H_2 = 1$.Por otro lado los órdenes de $h_1$ y $h_2$ son primos relativos, entonces el orden de $k$ es el orden de $h_1$ por el orden de $h_2$, y el producto directo de $\langle h_1 \rangle \langle h_2 \rangle$ es $\langle k \rangle$ pues $\langle k \rangle \leqslant \langle h_1 \rangle \langle h_2 \rangle$ y el orden de $k$ es igual a la cardinalidad de $\langle h_1 \rangle \langle h_2 \rangle$. Por lo que $h_1, h_2 \in K$ y así $K$ es el producto directo de $K \cap H_1$ y $K \cap H_2$.

**Corolario.** Si $G$ es el producto directo de $n$ subgrupos $H_1, \ldots, H_n \leq G$ cuyos órdenes son primos relativos, entonces cualquier subgrupo $K \leq G$ es el producto directo de $K \cap H_1, K \cap H_2, \ldots, K \cap H_n$.

**Teorema.** Si $G$ es un grupo abeliano y $g \in G$ tiene orden máximo, existe $H$ un subgrupo de $G$ tal que $\langle g \rangle \times H = G$.

**Definición.** Si $G$ es un grupo y $p$ un primo, se dice que $G$ es un $p$-grupo abeliano elemental si $G$ es abeliano y todos los elementos de $G$ son de orden $p$.

**Teorema.** Si $G$ es un $p$-grupo abeliano elemental, entonces $G$ es un espacio vectorial sobre el campo de Galois de $p$ elementos $GF(p)$, y su grupo de automorfismos coincide con el grupo general lineal de $G$ visto como espacio vectorial sobre $GF(p)$.

**Definición.** Si $G$ es un grupo y $X$ un conjunto no vacío, una acción de $G$ sobre $X$ es una función $\alpha : G \times X \longrightarrow X$ que cumple las siguientes dos propiedades:
**(1)** $\alpha(1,x) = x$ para cualquier $x$.
**(2)** $\alpha(gh,x) = \alpha(g,\alpha(h,x))$.
En adelante se denotará a $\alpha(g,x)$ como $gx$.

**Definición.** Si $G$ es un grupo que actúa sobre un conjunto $X$, la órbita de un elemento $x \in X$ es el subconjunto $O(x) = \{gx | g \in G\}$.

**Teorema.** El conjunto formado por las órbitas de los diferentes elementos de $X$ forman una partición de $X$.

Una órbita de $X$ es alguna órbita $O(x)$ para algún elemento $x$ de $X$.

**Teorema.** Si un grupo $G$ actúa sobre un conjunto $X$ y $C$ es el conjunto que de todas las órbitas de $X$, entonces $|X| = \Sigma_{O \in C}|O|$.

**Definición.** Si $G$ es un grupo que actúa sobre un conjunto $X$, y $x$ es un elemento de $X$, el estabilizador $x$ denotado como $G_x$ es el conjunto $\{g \in G | gx = x\}$.

**Teorema.** El estabilizador de cualquier elemento $x \in X$ es un subgrupo de $G$.

**Ejemplo.** Si $G$ es un grupo, $\alpha : G \times G \longrightarrow G$ definida como $\alpha(x, y) = yxy^{-1}$ es una acción de $G$ sobre si mismo, llamada conjugación. Las órbitas de $G$ bajo esta acción son llamadas clases de conjugación. El estabilizador $G_g$ de un elemento $g$ resulta ser el conjunto de todos los elementos en $G$ que conmutan con él y se le llama el centralizador de $g$ en $G$ denotado como $C_G(g)$.

También $G$ actúa por conjugación sobre el conjunto de todos los subgrupos de $G$. Si $H$ es un subgrupo de $G$, Al estabilizador $G_H$ bajo esta acción se le llama el normalizador de $H$ en $G$, y se denota como $N_G(H)$.

**Teorema.** Si un grupo $G$ actúa sobre un conjunto $X$, la cardinalidad de una órbita es igual al índice en $G$ del estabilizador de cualquier elemento $x$ en la órbita.

**Observación.** El resultado anterior implica que el número de conjugados de cualquier elemento $g \in G$ es el índice en $G$ de su centralizador, y que el número de conjugados de cualquier subgrupo $H$ de $G$ es $[G : N_G(H)]$.

**Definición.** Si $G$ es un grupo y $H$ es un subgrupo de $G$, definimos $H^G$ como el subgrupo de $G$ generado por $\{ghg^{-1} | g \in G; h \in H\}$. Tambien para un número natural $n$ definimos $H^n$ como el subgrupo de $G$ generado por $\{h^n | h \in H\}$.

**Teorema (Cauchy).** Si $G$ es un grupo y $p$ un primo que divide al orden de $G$, entonces $G$ contiene un elemento de orden $p$.

**Demostración.** Probaremos primero el caso en el que $G$ es abeliano.
Si $p||G|$, $|G| = pm$. La prueba se hará por inducción sobre $m$, y la base inductiva es clara ya que si $m = 1$ tenemos que $G$ es un grupo cíclico de orden primo y el elemento generador resulta ser el elemento de orden $p$ buscado.
Para el paso inductivo consideremos un elemento $x \in G$ cuyo orden $n$ es mayor que 1, si $p|n$ tenemos que el orden de $x^{n/p}$ es $p$ y así $x^{n/p}$ es el elemento buscado, pero si $p \nmid n$, al ser $G$ abeliano, $\langle x \rangle \trianglelefteq G$ por lo que $G/\langle x \rangle$ es un grupo que tiene como orden $pm/n$. Es claro que $n \nmid p$ por lo que $m/n$ es un entero menor que $m$. Así por la hipótesis de inducción, tenemos que existe un elemento $y \in G/\langle x \rangle$ que tiene orden $p$.
Consideremos ahora el homomorfismo canónico de $G$ en $G/\langle x \rangle$ que envia a cada elemento $g \in G$ a su clase izquierda $g\langle x \rangle$. Tiene que existir un elemento $y'$ en $G$ tal que su imagen sea $y$, esto implica que el orden de $y'$ es $pk$, por lo que $y'^k$ es un elemento de G que tiene orden $p$.
Ahora consideremos el caso en el que $G$ no es abeliano. Tomemos a $1 \neq x \in G$, el número de elementos conjugados de $x$ es $[G : C_G(x)]$. Si $x$ no es un elemento de $Z(G)$ entonces $|C_G(x)| < |G|$, y si $p||C_G(x)|$

entonces esta prueba se podría terminas con un razonamiento inductivo, por lo que ahora supondremos que $p \nmid |C_G(x)|$. Como $|G| = [G : C_G(x)]|C_G(x)|$ entonces tiene que ocurrir que $p|[G : C_G(x)]$. y si ahora tomamos un elemento $x_i$ en cada clase de conjugación de $G$ que no está formada por un solo elemento. Tenemos la siguiente cuenta:

$$|G| = |Z(G)| + \Sigma_i [G : C_G(x_i)].$$

Y sabemos por lo anterior que para toda $i$, $p|[G : C_G(x_i)]$, por lo que $p||Z(G)|$, sin embargo $Z(G)$ es abeliano y por el resultado anterior tenemos que $Z(G)$ tiene un elemento de orden $p$, y así tambien $G$ tiene un elemento de orden $p$, que es lo que se quería probar.■

La última igualdad dada en la demostración anterior es conocida como la ecuación de clases.
A continuación se da otra demostración del teorema de Cauchy, realizada por J.H. McKay, que no utiliza esa ecuación y que ilustra los diferentes conceptos de acción de grupos que hemos introducido.

**Demostración (Teorema de Cauchy).** Sea $C_p$ un grupo cíclico de orden primo $C_p = \{a, a^2, ..., a^p\}$ Definamos $X = \{(g_a, ..., g_{a^p}) \in G \times ... \times G | g_a g_{a^2} ... g_{a^p} = 1\}$. Notemos que la cardinalidad de $X$ es $|G|^{p-1}$ pues las primeras $p-1$ entradas de los elementos de $X$ se pueden elegir con libertad, sin embargo la $p$-ésima entrada tiene que ser $(g_a g_{a^2} ... g_{a^{p-1}})^{-1}$. Podemos hacer actuar al grupo cíclico de orden primo $C_p$ sobre $X$ de manera que si $a^k$ es un elemento de $C_p$ entonces la acción de $a^k$ sobre los elementos de $X$ sea $a^k(g_{a^1}, ..., g_{a^p}) = (g_{a^k a}, ..., g_{a^k a^p}) = (g_{a^{k+1}}, ..., g_{a^p}, g_a, ..., g_{a^k})$. El producto $(g_{a^{k+1}} ... g_{a^p})(g_a ... g_{a^k})$ es 1 pues el producto $(g_a ... g_{a^k})(g_{a^{k+1}} ... g_{a^p})$ es 1.
Bajo esta acción las órbitas de $X$ tienen 1 o $p$ elementos, las órbitas de un solo elemento son las de $p$-adas que tienen todas las entradas iguales, de la forma $(g, ..., g)$ con $g$ un elemento de $G$ que cumple que $g^p = 1$. Claramente $(1, ..., 1)$ es uno de esos elementos cuya órbita tiene solo un elemento, pero si suponemos que es el único elemento de $X$ cuya órbita es de un solo elemento tendríamos que $|X| = |G|^{p-1} = 1 + np$ para $n \geqslant 0$ algún entero, pero eso significaría que $|G|^{p-1} \equiv 1 (mod p)$, lo cual es una contradicción pues habíamos supuesto que $p||G|$. Así $G$ debe tener un elemento de orden $p$.

**Definición.** Si $G$ es un grupo y $a$ y $b$ son elementos de $G$, el conmutador de $a$ y $b$ denotado como $[a, b]$, es el elemento $aba^{-1}b^{-1}$. Si $H$ y $K$ son subgrupos de $G$ se define el interderivado de $H$ con $K$ como el subgrupo de $G$ generado por el conjunto $\{[h, k] | h \in H; k \in K\}$ y se denota como $[H, K]$. Al interderivado $[G, G]$ lo llamaremos el subgrupo conmutador o derivado de $G$ y se denotará como $G'$.

**Teorema.** Un subgrupo $N$ de un grupo $G$ es normal si y sólo si $[N, G] \leqslant N$.

**Demostración.** Si $N$ es un subgrupo normal de $G$, para cualquier $n$ elemento de $N$ y $g$ elemento de $G$, se tiene que $[n, g]$ es un elemento de $N$. Por lo que $[N, G] \leqslant N$.
Recíprocamente, si $g$ es un elemento de $G$, y $n$ un elemento de $N$, como $ngn^{-1}g^{-1}$ es un elemento de $N$, $gn^{-1}g^{-1}$ también lo es, por lo que $N$ es un subgrupo normal de $G$.

**Teorema.** Sean $H$ y $K$ grupos, $J \trianglelefteq H$ y $L \trianglelefteq K$, entonces $J \times L$ es un subgrupo normal de $H \times K$.

**Teorema.** Si $H_1$ y $H_2$ son subgrupos de $H$ y $K_1$ y $K_2$ son subgrupos de $K$, entonces $[H_1 \times K_1, H_2 \times K_2] = [H_1, H_2] \times [K_1, K_2]$.

**Demostración.** Sean $H$ y $K$ grupos, $h_1$ y $h_2$ elementos de $H$ y $k_1$ y $k_2$ elementos de $K$, entonces se tiene que $[(h_1,k_1),(h_2,k_2)] = (h_1h_2h_1^{-1}h_2^{-1}, k_1k_2k_1^{-1}k_2^{-1}) = ([h_1,h_2],[k_1,k_2])$.

**Teorema.** Sea $G$ es un grupo y $H$ es un subgrupo de $G$. $H \trianglelefteq G$ y $G/H$ es abeliano si y sólo si $G' \leq H$.

**Demostración.** Supongamos que $H \trianglelefteq G$ y que $G/H$ es abeliano, entonces para cualesquiera $a,b \in G$ tenemos que:

$$Hab = HaHb = HbHa = Hba \Longrightarrow ab(ba)^{-1} \in H \Longrightarrow aba^{-1}b^{-1} \in H$$

Por lo tanto $G' \leqslant H$.
Recíprocamente, si ahora suponemos que $G' \leqslant H$, para cualquier $h \in H$ y $g \in G$ tenemos que $ghg^{-1}h^{-1} \in H$ y como $h^{-1} \in H$ ocurre que $ghg^{-1} \in H$, por lo que $H \trianglelefteq G$.
Ahora observemos $G/H$, tenemos que para cualesquiera $a,b \in G$, ocurre que $aba^{-1}b^{-1} \in H$ por lo que $abH = baH$ y así $G/H$ resulta ser un grupo abeliano.

**Definición.** Si $G$ es un grupo, y $p$ un número primo, se dice que $P$ es un $p$-subgrupo de Sylow de $G$ si $|P|$ es la potencia mas grande de $p$ que divide a $|G|$.

**Definición.** Un subgrupo $H$ de $G$ es un subgrupo de Sylow si es un $p$-subgrupo de Sylow para algún primo $p$.

**Definición.** Un grupo primario es un $p$-grupo para algún primo $p$.

**Definición.** Si $p$ es un primo, y $G$ un grupo, se dice que $G$ es un $p'$-grupo si su orden no es divisible por $p$.

**Teorema (Sylow).**Si $G$ es un grupo y $p$ un primo que divide al orden de $G$ se tiene que:

**(1)**Existe al menos un $p$-subgrupo de Sylow de $G$.

**(2)**Si $P$ es un $p$-subgrupo de Sylow de $G$ y $H$ es algún $p$-subgrupo de $G$, existe $g \in G$ tal que $H$ es un subgrupo de $gPg^{-1}$. En particular, dos $p$-subgrupos de Sylow de $G$ son conjugados.

**(3)**Si $n$ es el número de $p$-subgrupos de Sylow de $G$, $n = [G : N_G(P)]$ donde $P$ es algún $p$-subgrupo de Sylow de $G$.

**Teorema.** Si $G$ es un grupo, $P$ un $p$-subgrupo de Sylow de $G$ y $N$ un subgrupo normal, $P \cap N$ resulta ser un $p$-subgrupo de Sylow de $N$ (notemos que un subgrupo de Sylow de $G$ es un subgrupo de Hall de $G$, por lo que este resultado es un caso particular de un teorema anterior, sin embargo daremos una demostración donde usamos los teoremas de Sylow).

**Demostración.** Tenemos que $P \cap N$ es un subgupo de algún $p$-subgrupo de Sylow de $N$, nombremos $P^*$ a dicho subgrupo de Sylow, queremos probar que $P \cap N$ es $P^*$. Para ello observemos que $P^* \leqslant gPg^{-1} \cap N$ para algún $g$, por lo que tenemos lo siguiente:

$$P^* \leqslant gPg^{-1} \cap N = gPg^{-1} \cap gNg^{-1} = g(P \cap N)g^{-1}.$$

Así $P^*$ y $P \cap N$ tienen la misma cardinalidad, por lo que $P \cap N = P^*$ es un $p$-subgrupo de Sylow de $N$.

**Observación.** El teorema anterior no necesariamente es cierto si el subgrupo $N$ no es normal en $G$. Por ejemplo si consideramos al grupo de permutaciones $S_5$, tiene como un 3-subgrupo de Sylow $\langle(125)\rangle$ pero la intersección con el subgrupo de $S_5$ que deja invariante al 5 es el subgrupo trivial, que no es un 3-subgrupo de Sylow de dicho subgrupo.

**Teorema.** Si $P$ es un $p$-subgrupo de Sylow de $G$, y $H$ un subgrupo de $G$ tal que $N_G(P) \leqslant H$, entonces $H$ coincide con su normalizador en $G$.

**Demostración.** Como $N_G(P) \leqslant H$, se tiene que $P \leqslant H$. Sea $x$ un elemento del normalizador de $H$ en $G$, eso significa que $xHx^{-1} = H$ por lo que $xPx^{-1} \leqslant H$ y como tanto $P$ como $xPx^{-1}$ son $p$-subgrupos de Sylow de $H$, existe $h$ un elemento de $H$ tal que $hxPx^{-1}h^{-1} = P$, lo que significa que $hx \in N_G(P)$ pero como $N_G(P) \leqslant H$, eso significa que $hx = h^* \in H$ por lo que $x = h^{-1}h^* \in H$ lo que nos dice que $N_G(H) \leqslant H$ y por lo tanto $N_G(H) = H$.

**Definición.** Si $G$ es un grupo, el subgrupo de Frattini de $G$ denotado como $\phi(G)$ es la intersección de todos los subgrupos máximos de $G$.

**Definición.** Si $G$ es un grupo se dice que $g \in G$ es no generador si al generar $X \cup \{g\}$ a $G$, también el conjunto $X$ genera a $G$.

**Teorema.** El conjunto de todos los elementos no generadores de un grupo $G$ coincide con el subgrupo de Frattini de $G$.

**Demostración.** Si $g$ es un elemento no generador de $G$, $M$ un subgrupo máximo y suponemos que $g$ no es un elemento de $M$, entonces el subgrupo $\langle M \cup \{g\}\rangle$ es todo $G$ sin embargo al ser $M$ un subgrupo máximo no genera a $G$ lo cual es una contradicción pues habíamos supuesto que $g$ era un elemento no generador. Por lo tanto $g$ es un elemento de $M$ y como $M$ era un subgrupo máximo arbitrario de $G$ entonces $g$ es un elemento del subgrupo de Frattini de $G$.
Recíprocamente, si $g$ es un elemento de $\phi(G)$ y suponemos que $X \cup \{g\}$ genera a $G$ entonces si $\langle X\rangle$ no fuera todo $G$ estaría contenido en un subgrupo máximo $M$ de $G$, sin embargo por hipótesis $g$ también es un elemento de dicho subgrupo máximo por lo que $G = X \cup \{g\} \leqslant M$, lo cual es una contradicción pues habíamos supuesto que $X \cup \{g\}$ generaba a $G$. Por lo tanto $g$ debe ser un elemento no generador de $G$.

**Teorema.** Si $G$ es un grupo y $H$ un subgrupo de $G$ tal que $G = \phi(G)H$, entonces $G = H$.

**Demostración.** Si $H \neq G$, $H$ está contenido en algún subgrupo máximo $M$ de $G$ por lo que $G = \phi(G)H < M$, lo cual es una contradicción que viene de suponer que $H$ es diferente de $G$.

**Teorema.** Si $G$ es un grupo y $S$ un subgrupo de Sylow del subgrupo de Frattini $\phi(G)$, se tiene que $S$ es un subgrupo normal de $G$.

**Demostración.** Para cualquier $g \in G$ se tiene que $gSg^{-1} < \phi(G)$, por que $\Phi(G)$ es un subgrupo característico de $G$, por lo que existe $h \in \phi(G)$ tal que $gSg^{-1} = hSh^{-1}$, lo que implica que $h^{-1}g \in N_G(S)$ y podemos ver a $g$ como el producto $hh^{-1}g \in \phi(G)N_G(S)$, entonces el grupo $G$ es igual al producto $\phi(G)N_G(S)$ y así $N_G(S) = G$ y $S$ resulta ser un subgrupo normal de $G$.

**Definición.** Se dice que un subgrupo $H$ de $G$ es característico, si para cada automorfismo $\alpha$ de $G$, ocurre que $\alpha(H) \leqslant H$.

**Teorema.** Un subgrupo $H$ de $G$ es característico en $G$ si y solo si para cada automorfismo $\alpha$ de $G$ se iene que $\alpha(H) = H$.

**Ejemplo.** $\phi(G)$ es un subgrupo característico de $G$, ya que si $M_1, M_2, ..., M_n$ son todos los subgrupos máximos de $G$ y $\alpha$ un automorfismo de $G$, por ser $\alpha$ inyectiva se tiene que $\alpha(\phi(G)) = \alpha(M_1 \cap ... \cap M_n) = \alpha(M_1) \cap ... \cap \alpha(M_n)$ pero la imagen de cualquier subgrupo máximo de $G$ bajo un automorfismo también es un subgrupo máximo de $G$ y por ser $\alpha$ un automorfismo las imagenes de dos subgrupos máximos diferentes son diferentes, por lo que $\alpha(\phi(G)) = \phi(G)$.

Otros ejemplos de subgrupos característicos de un grupo son su centro y su derivado o conmutador.

**Teorema.** Si $H$ es un subgrupo característico de $K$, y $K$ es un subgrupo característico de $G$, ocurre que $H$ es un subgrupo característico de $G$.

**Teorema.** Si $H$ es un subgrupo característico de $G$ entonces es normal en $G$.

**Demostración.** Si $g$ es un elemento de $G$, conjugar a los elementos de $G$ por $g$ es un automorfismo, y como $H$ es un subgrupo característico de $G$ entonces se tiene que $gHg^{-1} = H$.

**Teorema.** Si $H$ es un subgrupo característico de un subgrupo normal de $G$, entonces $H$ es un subgrupo normal de $G$.

**Teorema.** Si $H \leqslant K \leqslant G$, $H$ es característico en $G$ y $K/H$ es característico en $G/H$, se tiene que $K$ es característico en $G$.

**Demortración.** Sea $F$ un automorfismo de $G$, por demostrar que $F(K) \leq K$.
Como $H$ es característico en $G$, induce un automorfismo $F^*$ en $G/H$ de la siguiente manera: $F^*(gH) = F(g)H$.
Si $k \in K$, $F(k) \in F(k)H = F^*(kH) = k'H$ con $k' \in K$ por que $K/H$ es característico en $G/H$, lo que implica que $k'^{-1}F(k) \in H$ y por lo tanto $F(k) \in K$.

**Teorema (Argumento de Frattini).** Sean $G$ un grupo, $N$ un subgrupo normal de $g$, y $P$ un $p$-subgrupo de Sylow de $N$, entonces $G = N_G(P)N$.

**Demostración.** Sea $G$ un elemento de $G$. Como $N$ es un subgrupo normal de $G$ se tiene que $gPg^{-1} \leqslant gNg^{-1} = N$, por lo que $gpg^{-1}$ también es un $p$-subgrupo de Sylow de $N$. Por el teorema de Sylow existe $h$ elemento de $N$ tal que $gPg^{-1} = hPh^{-1}$ por lo que $h^{-1}gP(h^{-1}g)^{-1} = P$, lo que nos dice que $h^{-1}g$ es un elemento de $N_G(P)$ por lo que $G$ es un elemento de $HN_G(P)$ y entonces $G = HN_G(P)$.

**Definición.** El $n$-ésimo subgrupo derivado de $G$ denotado como $G^{(n)}$ se define inductivamente como $G^{(0)} = G$; $G^{(n)} = (G^{(n-1)})'$.

**Definición.** Decimos que un grupo $G$ es soluble si existe un número natural $n$ para el cual $G^{(n)} = 1$.

**Definición.** Si $G$ es un grupo, una serie normal de $G$ es una serie $G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \ldots$ tal que $G_i$ es un subgrupo normal de $G$ para cualquier $i$.

**Definición.** Si $G$ es un grupo, una serie subnormal de $G$ es una serie $G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \ldots$ tal que $G_{i+1}$ es un subgrupo normal de $G_i$ para cualquier $i$.

**Teorema.** Las siguientes condiciones para un grupo $G$ son equivalentes:
**(1)** El grupo $G$ es soluble.
**(2)** Existe una serie normal $G = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_n = 1$ tal que $G_i/G_{i+1}$ es abeliano para cualquier $i$.
**(3)** Existe una serie subnormal $G = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_n = 1$ tal que $G_i/G_{i+1}$ es abeliano para cualquier $i$.

**Ejemplos.** Todo grupo abeliano es soluble.

El grupo $S_3$ es soluble, tiene la serie $S_3 \geqslant A_3 \geqslant 1$ que cumple con (2).

El grupo $D_{2(n)}$ es soluble ya que es generado por dos elementos $a$ y $b$ de órdenes 2 y $n$ respectivamente por lo que la serie $D_{2(n)} \geqslant \langle b \rangle \geqslant 1$ cumple con (2).

Si $n \geqslant 5$, $S_n$ no es soluble porque $A_n$ es el único subgrupo normal propio no trivial de $S_n$ y no es abeliano.

**Teorema.** Si $G$ es soluble, cualquier subgrupo y cualquier cociente de $G$ tambien son solubles.

**Teorema.** Si $N$ es un subgrupo normal de $G$ y tanto $N$ como $G/N$ son solubles, $G$ también es soluble.

**Teorema.** El producto directo finito de grupos solubles es soluble.

**Teorema.** Si $G$ es un grupo no trivial simple y soluble, $G$ es de orden primo.

**Demostración.** Como $G$ es simple no tiene subgrupos normales no triviales, pero por ser soluble tiene una serie normal $1 = G_0 < G_1 = G$ cuyo único cociente $G/1 \cong G$ es abeliano, así cualquier subgrupo de $G$ es normal en $G$, por lo que $G$ no tiene ningún subgrupo no trivial y por lo tanto $G$ es de orden primo.

**Teorema.** $G$ es un grupo soluble si y sólo si existe una serie $G = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_n = 1$ tal que $G_{i+1} \trianglelefteq G_i$ y $G_i/G_{i+1}$ tiene orden primo para cualquier $i$.

**Corolario.**Si $G$ es un grupo soluble entonces al menos uno de sus subgrupos máximos es normal.

**Demostración.** Existe una serie $G = G_0 \geqslant G_1 > \ldots \geqslant G_n = 1$ tal que $G_{i+1} \trianglelefteq G_i$ y $G_i/G_{i+1}$ tiene orden primo para cualquier $i$, en dicha serie $G_1$ es el subgrupo máximo normal buscado.

**Teorema.** Si $G$ es un grupo soluble y $M$ un subgrupo normal máximo de $G$ entonces el índice en $G$ de $M$ es primo.

**Demostración.** Como $G$ es soluble, $G/M$ es soluble, y como $M$ es un subgrupo normal máximo de $G$, $G/M$ es simple, así $G/M$ es de orden primo, por lo tanto $[G:M]$ es primo.

**Observación.** En el teorema anterior, la hipótesis de que el grupo sea soluble es necesaria. $A_5$ es un grupo simple, por lo que el único subgrupo normal máximo que tiene es el subgrupo trivial.

**Teorema.** Todo grupo de orden menor que 60 es soluble.

**Teorema.** $A_5$ no es soluble.

**Demostración.** $A_5$ es simple no abeliano.

**Definición.** El grupo especial lineal denotado como $SL(n,F)$, es el grupo de matrices invertibles de $n \times n$ con elementos en el campo $F$, cuyo determinante es uno.

**Teorema.** Cualquier subgrupo normal $N$ de $SL(n,F)$, con $n \geqslant 2$ y $|F| > 3$, está contenido en el centro de $SL(n,F)$.

**Teorema.** Si $n \geqslant 2$ y $F$ es un campo de orden mayor que tres, se tiene que el grupo $PSL(n,F) = SL(n,F)/Z(SL(n,F))$, llamado grupo proyectivo lineal especial, es simple no abeliano.

**Capítulo 1.**

En este capítulo veremos algunas propiedades de $p$-grupos y de grupos nilpotentes. También caracterizaremos esta segunda clase de grupos.

Recordemos que si $p$ es un número primo, un $p$-grupo es un grupo en el cual todos los elementos tienen como orden una potencia de $p$.

**Teorema.**
Un grupo $G$ es un $p$-grupo si y sólo si $|G| = p^n$ para algún $n \in \mathbf{N}$.

**Demostración.**
Supongamos que $G$ es un $p$-grupo, si existiera un primo $q \neq p$ que divide al orden de $G$, en virtud del teorema de Cauchy $G$ tendría un elemento de orden $q$, lo cual sería una contradicción.
Recíprocamente, si $|G| = p^n$, por el teorema Lagrange el orden de cada elemento de $G$ es un divisor de $p^n$.■

Ahora recordaremos algunas propiedades de los $p$-grupos.

**Teorema.** Si $G$ es un $p$-grupo no trivial y $N$ un subgrupo normal no trivial de $G$, se tiene que la intersección de $N$ y $Z(G)$ es no trivial.

**Demostración.**
Podemos suponer que $G$ no es abeliano (por lo que $|G| = p^n$ con $n > 2$).
Cada clase de conjugación de $G$ tiene $p^s$ elementos para algúna $s$, y las clases de conjugación forman una partición de $G$.
Para cualquier elemento $x$ del centro de $G$ su clase de conjugación es $\{x\}$ de solo un elemento, y por ser $N$ un subgrupo normal de $G$, $N$ es unión de clases de conjugación de $G$, así si $N$ interseca al centro de $G$ trivialmente, la única clase de conjugación de un elemento contenida en $N$ es $\{1\}$, y $|N| = 1 + p^{s_1} + ... + p^{s_r}$ con $s_i > 0$ para toda $i$. Como $N$ es un $p$-grupo no trivial $p||N|$, además $p|p^{s_1} + ... + p^{s_r}$ por lo que $p|1$ lo cual es una contradicción. Por lo tanto $N$ interseca al centro de $g$ de manera no trivial.■

Si tomamos $N = G$, la propiedad anterior nos dice que el centro de un $p$-grupo no trivial nunca es trivial.

**Corolario.** Si $p$ es un primo y $G$ es un grupo de orden $p^2$, $G$ es abeliano.

**Demostración.** Si suponemos que $G$ no es abeliano, el centro de $G$ es de orden $p$, por lo que $G/Z(G)$ es un grupo cíclico de orden primo y entonces $G$ es abeliano, lo cual es una contradicción.

**Corolario.** Si $G$ es un $p$-grupo no trivial y $N$ un subgrupo normal mínimo de $G$, $N$ está contenido en el centro de $G$.

**Demostración.** $N$ es un subgrupo normal no trivial de $G$, por lo que $N \cap Z(G) = N'$ es no trivial, pero $N'$ es un subgrupo normal de $G$, y $N' \leqslant N$. Como $N$ es un subgrupo normal mínimo de $G$, se tiene que $N = N'$ y por lo tanto $N \leqslant Z(G)$.■

**Teorema** Si $G$ es un $p$-grupo de orden $p^n$ existe una serie normal $1 = H_0 \lhd H_1 \unlhd \ldots \unlhd H_n = G$ tal que $|H_i| = p^i$ para toda $i$.

**Demostración.** Podemos suponer que el grupo no es abeliano. La prueba se hará por inducción sobre $n$.
Sea $G$ un grupo de orden $p^n$ y $H_1$ un subgrupo de orden $p$ del centro de $G$. $G/H_1$ es un $p$-grupo de orden $p^{n-1}$, por hipótesis de inducción existe $1 = H_1/H_1 \lhd H_2/H_1 \unlhd \ldots \unlhd H_n/H_1 = G/H_1$, una serie normal de $G/H_1$, tal que $|H_i/H_1| = p^{i-1}$ para cualquier $i$.
Así $1 = H_0 \lhd H_1 \unlhd \ldots \unlhd H_n = G$ es una serie normal de $G$ con $H_i$ de orden $p^i$ para toda $i$.

**Teorema.** En la serie normal del teorema anterior se cumple que para toda $0 \leqslant i \leqslant n-1$, $H_{i+1}/H_i \leqslant Z(G/H_i)$.

**Demostración.** $G/H_i$ es un $p$-grupo no trivial, y como $|H_{i+1}/H_i| = p$, $H_{i+1}/H_i$ es un subgrupo normal mínimo de $G/H_i$, por lo tanto $H_{i+1}/H_i \leqslant Z(G/H_i)$.■

**Teorema.** Si $G$ es un $p$-grupo, cualquier subgrupo propio de $G$ es un subgrupo propio de su normalizador.

**Demostración.**
Supongamos que $H$ es un subgrupo propio de $G$ y no es normal en $G$, sea $X$ el conjunto de todos los subgrupos de $G$ conjugados de $H$, tenemos que $|X| = [G : N_G(H)] \neq 1$, además sabemos que H actua en X por conjugación y eso implica que la órbita de cada conjugado de $H$ tiene cardinalidad una potencia de $p$ debido a que $H$ que es un $p$-grupo. Es claro que $\{H\}$ es una órbita de cardinalidad 1 bajo la acción de $H$ y como todas las órbitas tienen como cardinalidad una potencia de $p$, y forman una partición de $X$, tienen que existir al menos $p-1$ órbitas más diferentes de $H$ cuya cardinalidad sea 1. Tenemos que existe al menos un conjugado $gHg^{-1}$ de $H$ con $g$ un elemento no trivial de $G$ que cumple que su órbita es de cardinalidad 1. Entonces $agHg^{-1}a^{-1} = gHg^{-1}$ para toda $a \in H$, lo cual significa que $g^{-1}ag \in N_G(H)$ pero como tenemos que $gHg^{-1} \neq H$ tiene que existir al menos una $a \in H$ tal que $gag^{-1}$ no esté en $H$, por lo cual ya tenemos que $H < N_G(H)$.

**Teorema.** Si $G$ es un $p$-grupo y $M$ es un subgrupo máximo de $G$, entonces $M \lhd G$, y además $[G : M] = p$.

**Demostración.**
Como $M < G$ entonces $M < N_G(M)$ pero como $M$ es un subgrupo máximo de $G$ entonces debe ocurrir que $N_G(M) = G$, lo cual implica que $M \lhd G$. Además, si $G/M$ tuviera un subgrupo propio no trivial, por el teorema de la correspondencia tendría que existir un subgrupo propio de $G$ que contiene a $M$, lo cual es una contradicción debido a que $M$ es un subgrupo máximo de $G$. Como $G/M$ no puede tener subgrupos propios no triviales debe ser un grupo cíclico de orden primo, lo cual nos dice que $[G : M] = p$.■

**Teorema.** Si $G$ es un grupo abeliano o un $p$-grupo, todos los subgrupos de Sylow de $G$ son normales.
Es claro que esta propiedad es cierta para $G$ un $p$-grupo ya que el único subgrupo de Sylow que tiene

es el mismo, y también es clara si $G$ es un grupo abeliano ya que todos sus subgrupos son normales, y así los de Sylow deben serlo.

**Teorema.** Si x y y son elemenotos de G con $(O(x), O(y)) = 1$ entonces $xy = yx$.

Si $G$ es un $p$-grupo y tiene dos elementos cuyos órdenes son primos relativos al menos uno de ellos debe ser la identidad, por lo que conmutan.■

Algunas de las propiedades anteriores de los $p$-grupos caracterizan a la clase de los grupon nilpotentes finitos que estudiaremos posteriormente.

**Teorema.**
Si $G$ es un $p$-grupo, entonces $G/\phi(G)$ es un $p$-grupo abeliano elemental.

**Demostración.**
Primero probaremos que $G/\phi(G)$ es abeliano, y para eso probaremos que $G' \leqslant \phi(G)$.
Sea $M$ un subgrupo máximo de $G$. Por la propiedad **(3)** $G/M$ tiene cardinalidad $p$ por lo que es abeliano, y así $G' \leqslant M$. Como $M$ era un subgrupo máximo arbitrario de $G$ entonces $G' \leqslant \phi(G)$ y $G/\phi(G)$ es abeliano.
Ahora queremos probar que cualquier elemento no trivial de $G/\phi(G)$ tiene orden $p$, para ello supongamos que $g$ es un elemento de $G$ y no es elemento de $\phi(G)$, queremos ver que $g^p$ pertenece a todos los subgrupos máximos de $G$.
Tomemos $M$ un subgrupo máximo de $G$, por la propiedad **(3)** $gM$ es un elemento de orden $p$ de $G/M$ por lo que $g^pM = (gM)^p = M$ y $g^p \in M$, como $M$ es un subgrupo máximo arbitrario de $G$ entonces $g^p \in \phi(G)$ y $G/\phi(G)$ resulta ser abeliano elemental.

**Teorema.**
Si $G$ es un $p$-grupo, $N \lhd G$ y $G/N$ es un grupo abeliano elemental, entonces $\Phi(G) \leqslant N$.

**Demostración.**
Supongamos que $N \trianglelefteq G$ tal que $G/N$ es un grupo abeliano elemental. Supongamos también que existe un elemento $x \in \Phi(G)$ tal que $x$ no está en $N$, sabemos que $xN \in G/N$ y que el orden de $xN$ es $p$. Además $\langle xN \rangle$ es un sumando directo de $G/N$ pues $G/N$ es un $p$-grupo abeliano elemental, por lo que $G/N = \langle xN \rangle \times H/N$ para algún $H < G$, y por otro lado sabemos que $[G : H] = [G/N : H/N] = p$, lo que significa que $H$ es un subgrupo máximo de $G$ y $x$ no es elemento de $H$. Tenemos una contradicción pues habíamos supuesto que $x \in \Phi(G)$.
Por lo tanto $\Phi(G) \leqslant N$.■

A continuación definiremos los grupos nilpotentes, veremos algunas propiedades elementales de tales grupos y presentaremos una caracterización de ellos.

**Definición.** Un grupo $G$ es nilpotente si tiene una serie central, esto es una serie normal $1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_n = G$ tal que $G_{i+1}/G_i \leqslant Z(G/G_i)$ para toda $i$.

**Lema.** Si $1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_n = G$ es una serie normal de un grupo $G$, para cualquier $i$ se tiene que la serie es central si y solo si $[G_{i+1}, G] \leqslant G_i$ para cualquier $i$.

**Demostración.** $[G_{i+1}, G] \leqslant G_i$ si y solo si para cualesquiera $h \in G_{i+1}$ y $g \in G$ se tiene que $[h, g]G_i = G_i$ y esto ocurre si y solo si $hG_i gG_i h^{-1}G_i g^{-1}G_i = G_i$ que pasa si y solo si $G_{i+1}/G_i \leqslant Z(G/G_i)$.■

Es inmediato de la definición que los grupos abelianos son nilpotentes y que cada grupo no trivial nilpotente tiene centro no trivial, por lo que tanto el grupo simétrico $S_n$, con $n \geqslant 3$, como el grupo alternante $A_n$, con $n \geqslant 4$, no son nilpotentes.
También es inmediato de la definición que cada grupo nilpotente es soluble.

**Teorema.** Los $p$-grupos finitos son nilpotentes.

**Demostración.** Anteriormente se probó que los $p$-grupos finitos tiene una serie normal cuyos cocientes consecutivos son de orden primo, y que dicha serie normal es una serie central.■

**Observación.** En el teorema anterior, la hipótesis de que los $p$-grupos sean finitos es necesaria. Existen ejemplos de $p$-grupos infinitos cuyo centro es trivial, por lo que no son nilpotentes.

Veamos algunas propiedades elementales de los grupos nilpotentes.

**Teorema.** Los subgrupos y cocientes de un grupo nilpotente son nilpotentes, y el producto directo de dos grupos nilpotentes es nilpotente.

**Demostración.** Sea $K$ un subgrupo de $G$ un grupo nilpotente, haremos ver que $K$ es nilpotente.
Como $G$ es nilpotente existe una serie central $1 = G_0 \leqslant ... \leqslant G_n = G$ por lo que debe de existir una $i$ tal que $K \leqslant G_i$.
Consideremos la serie normal de $K$ dada por $1 = G_0 \cap K \leqslant ... \leqslant G_i \cap K = K$. Para cualquier $j$ se tiene que $[G_j \cap k, K] \leqslant [G_j, G] \leqslant G_{j-1}$, además $[G_j \cap k, K] \leqslant K$ por lo que $[G_j \cap k, K] \leqslant G_{j-1} \cap K$. Así existe una serie central para $K$ por lo que $K$ es nilpotente.

Si $N$ es un subgrupo normal de $G$, la serie normal de $G/N$ dada por $1 = G_0N/N \leqslant ... \leqslant G_nN/N = G/N$ es una serie central de $G/N$ pues para cualquier $i$ ocurre que $[G_iN/N, GN/N] = [G_i, G]N/N \leqslant G_{i-1}N/N$.

Solo falta probar que el producto $G \times H$ con $G$ y $H$ grupos nilpotentes es nilpotente. Como $H$ es nilpotente existe una serie central $1 = H_0 \leqslant ... \leqslant H_m = H$. Se pueden insertar los términos repetidos que sean necesarios para que las series centrales de $G$ y de $H$ tengan la misma longitud, es decir $n = m$.
Así la serie normal de $G \times H$ dada por $1 = G_0 \times H_0 \leqslant ... \leqslant G_n \times H_n = G \times H$ es una serie central de $G \times H$ pues para cualquier $i$ tenemos que $[G_i \times H_i, G \times H] = [G_i, G] \times [H_i, H] \leqslant G_{i-1} \times H_{i-1}$.

**Teorema.** Si $G$ es un grupo, $M$ y $N$ subgrupos de $G$ tales que $G/M$ y $G/N$ son nilpotentes, $G/(M \cap N)$ es nilpotente.

**Demostración.** $G/M \times G/N$ es nilpotente, y el homomorfismo $F : G \longrightarrow G/M \times G/N$ dado por $F(g) = (gM, gN)$ tiene como imagen un subgrupo nilpotente pues es un subgrupo de $G/M \times G/N$, sin embargo la imagen de $F$ es isomorfa a $G/(M \cap N)$, lo cual concluye la prueba.■.

El teorema anterior es cierto para todas las clases de grupos que sean cerradas bajo productos directos y formación de subgrupos, por ejemplo la clase de los grupos abelianos, o la clase de los grupos solubles.

En general no es cierto que si $G$ tiene un subgrupo normal $N$, tal que $N$ y $G/N$ son nilpotentes, también $G$ es nilpotente. Un ejemplo es $S_3$ que no es nilpotente pues su centro es trivial pero $A_3 \lhd S_3$ y tanto $A_3$ como $S_3/A_3$ son nilpotentes. Sin embargo tenemos el siguiente resultado.

**Teorema.**Si $G$ es un grupo con centro no trivial, y $H$ es un subgrupo del centro de $G$ tal que $G/H$ es nilpotente, entonces $G$ es nilpotente.

**Demostración.** Supongamos que $1 = G_0/H \leqslant ... \leqslant G_n/H = G/H$ es una serie central de $G/H$. Haremos ver que $1 \leqslant G_0 \leqslant ... \leqslant G_n = G$ es una serie central de $G$.
Para cualquier $i$ se tiene que $[G_i/H, G/H] = [G_i, G]H/H$ y además $[G_i/H, G/H] \leqslant G_{i-1}/H$, por lo tanto $[G_i, G] \leqslant G_{i-1}$.■

**Teorema.** Si $G$ es un grupo nilpotente y $S$ es un subgrupo propio de $G$, entonces $S$ es un subgrupo propio de su normalizador en $G$.

**Demostración.** Como $G$ es nilpotente, existe una serie central $1 = G_0 \leqslant G_1 \leqslant ... \leqslant G_n = G$, y como $S$ es un subgrupo propio de $G$, existe una $j$ para la cual $G_j$ ya no está contenido en $S$, pero $G_{j-1}$ si lo está.
Tomemos $x$ un elemento de $G_j$ que no esté en $S$, $[x, G] \leqslant [G_j, G] \leqslant G_{j-1} \leqslant S$, y como $[x, S] \leqslant [x, G]$, se tiene que $xsx^{-1}s^{-1}$ es un elemento de $S$ para cualquier $s \in S$, por lo que $x \in N_G(S)$. Así $S$ está contenido propiamente en su normalizador en $G$.

**Corolario.** Cualquier subgrupo máximo de un grupo nilpotente es normal.

**Teorema.** Si $N$ es un subgrupo normal no trivial de un grupo nilpotente $G$, $N$ interseca al centro de manera no trivial.

**Demostración.** Como $G$ es nilpotente, existe una serie central $1 = G_0 \leqslant G_1 \leqslant ... \leqslant G_n = G$, como $N$ es no trivial, existe una $j$ tal que $N \cap G_{j+1}$ es no trivial pero $N \cap G_j$ es trivial.
Tomemos un elemento $a \neq 1$ en $N \cap G_{j+1}$, como la serie es central se tiene que $[G_{j+1}, G] \leqslant G_j$ y como $N$ es un subgrupo normal de $G$, $[N, G] \leqslant N$, por lo que $[a, G] \leqslant G_j \cap N = 1$. Así para cualquier $g$ elemento de $G$ se tiene que $[a, g] = 1$ por lo que $a \in Z(G)$. Por lo tanto existe un elemento no trivial en la intersección de $N$ con el centro de $G$.

**Corolario.** si $N$ es un subgrupo normal mínimo de un grupo nilpotente $G$, $N$ está contenido en el centro de $G$.

A continuación definiremos la serie central descendente y la serie central ascendente de un grupo $G$.

**Definición.**
Si $G$ es un grupo, no necesariamente finito, sean $C_1 = G$; y para cada $i \geqslant 1$, $C_{i+1} = [C_i, G]$.

Probaremos por inducción que para cualquier $i$ ocurre que $C_i$ es un subgrupo de $C_{i-1}$, y $C_i$ es característico en $G$.

Para $i = 1$ es claro que $G$ es un subgrupo característico de $G$. Supongamos para alguna $i$ que $C_i$ es un subgrupo característico de $G$ y sea $F$ un automorfismo de $G$, entonces $F(C_{i+1}) = F([C_i, G]) = [F(C_i), F(G)] = [C_i, G] = C_{i+1}$, por lo que $C_{i+1}$ también es un subgrupo característico de $G$.

Además $C_i \leqslant C_{i-1}$, porque $C_i = [C_{i-1}, G] \leqslant C_{i-1}$ pues $C_{i-1}$ es caracteristico en $G$.

**Definición.** A la serie $G = C_1 \geqslant C_2 \geqslant C_3 \geqslant ...$ se le llama la serie central descendente de $G$.

Ahora definamos la serie central ascendente.

**Definición.** Para un grupo no necesariamente finito $G$, sean $Z_0 = \{1\}$, $Z_1 = Z(G)$. $Z_2$ el subgrupo de $G$ que cumple que $Z(G/Z_1) = Z_2/Z_1$. Inductivamente definimos $Z_{i+1}$ como el subgrupo de $G$ que cumple que $Z(G/Z_i) = Z_{i+1}/Z_i$.
Por construcción $Z_i \leqslant Z_{i+1}$.
Probaremos por inducción que para cualquier $i$, $Z_i$ es un subgrupo característico de $G$.
Para $i = 0$ se tiene que $Z_0 = \{1\}$ es característico en $G$, ahora supongamos que para alguna $i$ se tiene que $Z_i$ es un subgrupo característico de $G$, como $Z_{i+1}/Z_i = Z(G/Z_i)$, $Z_{i+1}/Z_i$ es un subgrupo característico de $G/Z_i$ y por lo tanto $Z_{i+1}$ es un subgrupo característico de $G$.

**Definición.** A la serie $1 \leqslant Z_1 \leqslant Z_2 \leqslant Z_3 \leqslant ...$ del grupo $G$, se le llama la serie central ascendente de $G$.

**Teorema.**

Si $G$ es un grupo, las siguientes tres condiciones son equivalentes:
**(0)** $G$ es nilpotente.
**(1)** La serie central ascendente de $G$ llega hasta $G$.
**(2)** La serie central descendente de $G$ llega hasta 1.

**Demostración.**

**(0)** implica **(1)**:
Sea $G = G_1 \geqslant G_2 \geqslant ... \geqslant G_{n+1} = 1$ una serie central de $G$. Se probará por inducción sobre $j$ que $G_{n+1-j} \leqslant Z_j$.
Para el caso base, si $j = 0$ entonces $G_{n+1} = 1 = Z_0$.
Ahora supongamos que para alguna $j$ ocurre que $G_{n+1-j} \leqslant Z_j$. Tenemos que $G_{n+1-(j+1)}/G_{n+1-j} \leqslant Z(G/G_{n+1-j})$. Ahora considérese $h \in G_{n+1-(j+1)}$ y cualquier elemento $g \in G$ sabemos que $hG_{n+1-j}gG_{n+1-j} = gG_{n+1-j}hG_{n+1-j}$, por lo que $hgh^{-1}g^{-1} \in G_{n+1-j}$, pero por hipótesis de inducción $G_{n+1-j} \leqslant Z_j$, por lo que $hgh^{-1}g^{-1} \in Z_j$, pero entonces $hZ_jgZ_j = gZ_jhZ_j$, lo que significa que $hZ_j \in Z(G/Z_j)$ y por lo tanto $h \in Z_{j+1}$ y entonces tenemos que $G_{n+1-(j+1)} \leqslant Z_{j+1}$.

**(1)** implica **(2)**:
Se probará por inducción sobre $i$ que $C_{i+1} \leqslant Z_{n-i}$ (nótese que para $i = n$ ocurre que $C_{n+1} \leqslant Z_0 = 1$ lo que nos diría que la serie central descendente llega a 1).
Para el caso base, si $i = 0$ entonces $C_1 = Z_n = G$.
Ahora supongamos que para alguna $i$ ocure que $C_{i+1} \leqslant Z_{n-i}$, entonces ocurre lo siguiente:

$$C_{i+2} = [C_{i+1}, G] \leqslant [Z_{n-i}, G] \leqslant Z_{n-i-1}$$

.

**(2)** implica **(0)**:

Si suponemos que la serie central descendente de $G$ llega hasta 1, haremos ver que la serie $G = C_0 \geqslant ... \geqslant C_n = 1$ es una serie central de $G$. Es claro que es una serie normal pues los subgrupos $C_i$ son característicos en $G$ y además por como está contruida la serie central descendente tenemos que $[C_i, G] = C_{i+1}$ de donde se tiene que $C_i / C_{i+1} \leqslant Z(G/C_{i+1})$.

**Teorema.**

Si $G$ es un grupo finito, las siguientes cinco condiciones son equivalentes:
**(0)** $G$ es nilpotente.
**(3)** Cualquier subgrupo máximo de $G$ es normal en $G$.
**(4)** Los subgrupos de Sylow de $G$ son normales en $G$.
**(5)** $G$ es producto directo de sus subgrupos de Sylow.
**(6)** Si $S$ es un subgrupo propio de $G$, entonces $S < N_G(S)$.

**Observación.** Existen ejemplos de $p$-grupos infinitos cuyo centro no es trivial, y en los cuales cada subgrupo propio está contenido propiamente en su normalizador, pero no son nilpotentes.

**Demostración.**

**(3)** implica **(4)**:

Supongamos que existe un subgrupo de Sylow $P$ de $G$ que no es normal. Tenemos que $P \leqslant N_G(P) < G$, y así tiene que existir un subgrupo $M$ máximo de $G$ que contenga al normalizador en $G$ de $P$ ($P \leqslant N_G(P) \leqslant M$). Entonces tenemos que $P$ es un subgrupo de Sylow de $M$. Por hipótesis $M \triangleleft G$ por lo que si tomamos cualquier elemento $g \in G$ ocurre que $gPg^{-1}$ es un subgrupo de Sylow de $M$, y así tiene que existir $m \in M$ tal que $mPm^{-1} = gPg^{-1}$, por lo que $P = m^{-1}gPg^{-1}m$ y eso nos dice que $m^{-1}g \in N_G(P)$ y entonces tenemos que $g = m(m^{-1}g)$ como un producto en $MN_G(P)$ de donde obtenemos la siguiente contradicción, $G = MN_G(P) \leqslant M$ y así debe ocurrir que todos los subgrupos de Sylow de $G$ sean normales en $G$.

**(4)** implica **(5)**:

Si $|G| = p_1^{n_1}...p_s^{n_s}$ con los $p_i$ primos diferentes que dividen el orden de $G$, sea $\{P_1, ..., P_s\}$ un conjunto de subgrupos de Sylow de $G$ con $P_i$ un $p_i$-subgrupo de Sylow de $G$ para cada $1 \leqslant i \leqslant s$.
Como el producto de dos subgrupos normales de $G$ resulta ser un subgrupo normal de $G$ tenemos que $P_1...P_s$ es un subgrupo de $G$. Además, por motivos de orden, para cada $1 < i \leqslant s$, $P_i \cap P_1...P_{i-1} = 1$, y por motivos de orden $G = P_1 \times ... \times P_s$, lo cual nos dice que $G$ es el producto directo de sus subgrupos de Sylow.

**(5)** implica **(0)**

Ya probamos que los $p$-grupos finitos son nilpotentes, y que los productos directos de grupos nilpotentes son nilpotentes, entonces al ser $G$ producto directo de sus subgrupos de Sylow resulta ser nilpotente.

**(0)** implica **(6)**:

Probaremos que si $H < G$ entonces el normalizador de $H$ en $G$ crece ($H < N_G(H)$).
Esto se debe a que tiene que existir una $i$ para la cual $C_{i+1} \leq H$ y además $C_i \nleq H$, entonces $[C_i, H] \leqslant [C_i, G] = C_{i+1} \leqslant H$, por lo que $C_i \leqslant N_G(H)$ y eso nos dice que $H < N_G(H)$ por lo que $G$ cumple la equivalencia **(6)** de ser nilpotente.

**(6)** implica **(3)**:
Si tomamos $M < G$ un subgrupo máximo, tenemos que $M$ tiene que ser un subgrupo propio de $N_G(M)$, pero al ser $M$ máximo tiene que ocurrir que $N_G(M) = G$ y eso nos dice que $M \lhd G$.■

A continuación daremos otras dos caracterizaciones importantes de grupos finitos nilpotentes.

**Teorema.** Un grupo $G$ es nilpotente si y solo si $G' \leqslant \Phi(G)$.

**Demostración.**Si $M$ es un subgrupo máximo de $G$, $G'$ está contenido en $M$ por lo que $M$ es un subgrupo normal de $G$.
Recíprocamente, si todos los subgrupos máximos de $G$ son normales en $G$ y $M$ es un subgrupo máximo cualquiera, $G/M$ no tiene subgrupos no triviales, por lo que es un grupo cíclico de orden primo y así $G'$ está contenido en $M$, pero $M$ era un subgrupo máximo cualquiera, lo que implica que $G'$ está contenido en $\Phi(G)$.

**Teorema.** Sea $G$ un grupo, $G$ es nilpotente si y solo si $G/\Phi(G)$ es nilpotente.

**Demostración.** Si $P$ un $p$-subgrupo de Sylow de $G$, $P\Phi(G)/\Phi(G)$ es un $p$-subgrupo de Sylow de $G/\Phi(G)$ que es nilpotente, por lo que $P\Phi(G)/\Phi(G) \trianglelefteq G/\Phi(G)$, y así por el teorema de la correspondencia $P\Phi(G) \trianglelefteq G$, entonces por el corolario del argumento de Frattini tenemos lo siguiente:

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

Por la ultima igualdad tiene que ocurrir que $N_G(P) = G$ pues de lo contrario estaría contenido en un subgrupo máximo $M$ al igual que $\Phi(G)$ y llegaríamos a la contradicción $G = M$.
Así tenemos que $P \trianglelefteq G$ y $G$ es nilpotente.
Recíprocamente, si $G$ es nilpotente también lo es cualquier cociente de $G$, por lo que $G/\Phi(G)$ es nilpotente.■

Daremos otras dos caracterizaciones de grupo finito nilpotente.

**Teorema.** Un grupo finito $G$ es nilpotente si y sólo si cualquier subgrupo es subnormal en $G$.

**Demostración.** Supongamos que cualquier subgrupo de $G$ es subnormal, si tomamos un subgrupo propio $H$ de $G$ se tiene que $H \trianglelefteq\trianglelefteq G$, entonces en la serie subnormal de $H$ en algún momento contiene un subgrupo $K$ de $G$ tal que $H$ es un subgrupo propio de $K$ y además $H \lhd K$ lo que implica que $K \leqslant N_G(H)$ y así $H$ es un subgrupo propio de su normalizador.
Recíprocamente, si tomamos $H$ un subgrupo de $G$, podemos construir una serie subnormal para $H$ dada por $H < N_G(H) < N_G(N_G(H)) < ... < G$ y eso nos dice que $H \trianglelefteq\trianglelefteq G$.

**Teorema.** Un grupo $G$ es nilpotente si y sólo si para cualesquiera dos elementos $x$ y $y$ de $G$ tales que $(O(x), O(y)) = 1$ se tiene que $xy = yx$.

**Demostración.** Supongamos que $G$ es nilpotente, sean $P_1, ..., P_s$ los subgrupos de Sylow de $G$, $G = P_1 \times, ..., \times P_s$, sean $x$ y $y$ dos elementos de $G$ cuyos órdenes son primos relativos. $x = x_1 ... x_s$ con $x_i \in p_i$ para toda $i$, $y = y_1 ... y_s$ con $y_i \in p_i$ para toda $i$.
$O(x) = O(x_1)...O(x_s)$, y $O(y) = O(y_1)...O(y_s)$, así si para alguna $i$, $x_i \neq 1$, entonces $y_i = 1$, y si para alguna $i$, $y_i \neq 1$, entonces $x_i = 1$.
Por lo tanto $xy = (x_1 y_1)...(x_s y_s) = (y_1 x_1)...(y_s x_s) = yx$.
Recíprocamente, sea$\{p_1, ..., p_s\}$ el conjunto de todos los primos diferentes que dividen el orden de $G$ y sea $\{P_1, ..., P_s\}$ un conjunto de subgrupos de Sylow de $G$, con $|P_i| = p_i^{n_i}$. Por motivos de orden $P_1 \cap P_2 = 1$ lo que significa que todos los elementos de $P_1$ conmutan con todos los elementos de $P_2$, así $P_1 P_2$ es un subgrupo de $G$. Para cualquier $i \geqslant 2$ si $P_1 P_2 ... P_i$ es un subgrupo de $G$, por motivos de orden $P_1 P_2 ... P_i \cap P_{i+1} = 1$ por lo que $P_1 P_2 ... P_i P_{i+1}$ es un subgrupo de $G$, lo que implica que $P_1 P_2 ... P_s$ es un subgrupo de $G$.
Para probar que $G$ es isomorfo al producto directo de sus subgrupos de Sylow solo hace falta ver que $P_i$ es normal para cualquier $i$, pero esto ocurre ya que para cualquier $j$, se tiene que $P_j \leqslant N_G(P_i)$, por lo que $G \leqslant N_G(P_i)$ y $P_i \trianglelefteq G$.■

Otras propiedades y resultados de grupos nilpotentes son los siguientes.

**Teorema.** Si $A, B \trianglelefteq G$ son nilpotentes entonces el producto $AB$ también es nilpotente.

**Demostración.**
Supongamos que $p_1, ..., p_r$ son todos los primos diferentes que dividen el orden de $AB$, como $|A|, |B| \mid |AB|$ entonces podemos decir que $|A| = p_1^{a_1} ... p_r^{a_r}$ y también que $|B| = p_1^{b_1} ... p_r^{b_r}$ donde puede ocurrir que algunas $a_i$ o $b_i$ sean cero. Entonces por ser $A$ y $B$ nilpotentes $A = A_1 \times ... \times A_r$ y $B = B_1 \times ... \times B_r$ donde para cada $1 \leqslant i \leqslant r$, $A_i$ y $B_i$ son el $p_i$-subgrupo de Sylow de $A$ y $B$ respectivamente, o el subgrupo trivial en caso de que $a_i = 0$ o $B_i = 0$.
Como todos los subgrupos $A_i$ y $B_i$ son característicos en $A$ y $B$ entonces son normales en $G$, por lo que para toda $i$ $A_i B_i$ es un subgrupo normal de $G$. sea $H = \langle A_1 B_1, ..., A_r B_r \rangle$, como cada $A_i B_i \leqslant AB$ entonces $H \leqslant AB$, además es claro que $A = \langle A_1, ..., A_r \rangle \leqslant H$ y análogamente $B \leqslant H$ de donde tenemos que $AB \leqslant H$ y por lo cual $AB = H$.
Por motivos de orden $A_i B_i \cap A_j B_j = 1$ siempre que $i \neq j$, y debido a su normalidad tenemos que los probuctos $A_i B_i A_j B_j$ son productos directos, por lo tanto:

$$AB = H = A_1 B_1 \times ... \times A_r B_r.$$

Y es claro que $A_i B_i$ es $p_i$ -subgrupo de Sylow de $AB$, por lo que $AB$ es producto directo de sus subgrupos de Sylow y por lo tanto es nilpotente.

**Teorema.** Para cualquier grupo $G$ su subgrupo de Frattini $\Phi(G)$ es nilpotente.

**Demostración.** Ya se probó que los subgrupos de Sylow de $\Phi(G)$ son normales.

**Teorema.** Si $G$ es un grupo nilpotente y $n$ es un divisor del orden de $G$, entonces $G$ tiene un subgrupo $H$ de orden $n$.

**Demostración.** Sea $p_1^{a_1} ... p_r^{a_r}$ la factorización de $n$ en producto de primos distintos. $G$ es producto directo de sus subgrupos de Sylow y para cualquier $i$ el $p_i$-subgrupo de Sylow de $G$ tiene un subgrupo $P_i$ de orden $p_i^{a_i}$. Así $H = P_1 \times ... \times P_r$ es un subgrupo de $G$ de orden $n$.

**Corolario.** Si $G$ es un grupo abeliano y $n$ es un divisor del orden de $G$, entonces $G$ tiene un subgrupo $H$ de orden $n$.

## Capítulo 2

En este capítulo, se caracteriza la clase de los grupos que no son nilpotentes pero cuyos subgrupos propios sí lo son, que es el objetivo principal de este trabajo. Para ello, primero caracterizamos los grupos no nilpotentes cuyos subgrupos normales propios son nilpotentes y se prueban tres resultados que son necesarios para la caracterización mencionada. El primero de ellos es un resultado útil sobre los conceptos de solubilidad y nilpotencia, y el segundo es importante porque es un caso particular del teorema de Maschke, que es uno de los pilares de la teoría de representaciones de grupos.

Comencemos observando los siguientes ejemplos:

**Ejemplo 1.**
El grupo de las permutaciones de 3 elementos $S_3$ tiene más de un 2-subgrupo de Sylow, por lo que no es nilpotente, sin embargo cualquier subgrupo propio es abeliano, por lo que es nilpotente.

**Ejemplo 2.**
El grupo diédrico $D_{2(15)}$ de orden 30 es generado por dos de sus elementos $a$ y $b$ de órdenes dos y quince respectivamente con $aba^{-1} = b^{-1}$.
El subgrupo $H = \langle b \rangle$ es el único subgrupo de $D_{2(15)}$ de orden 15, por lo que es un subgrupo característico. $H$ por ser cíclico tiene un único subgrupo $Q$ de orden tres y un único subgrupo $P$ de orden 5 por lo que $P$ y $Q$ también son característicos en $D_{2(15)}$.
Veamos que $H$, $Q$ y $P$ son los únicos subgrupos normales propios no triviales de $D_{2(15)}$.
Como $D_{2(15)}/H$ es de orden 2 entonces $D'_{2(15)} \leqslant H$. Como $aba^{-1} = b^{-1}$ se tiene que $[a,b] = b^{-2}$ y como $b^{-2}$ tiene orden quince $\langle [a,b] \rangle = H \leqslant D'_{2(15)}$, por lo tanto $H = D'_{2(15)}$.
$D_{2(15)}$ tiene quince subgrupos de orden dos por lo que los subgrupos de ese orden no son normales y $D_{2(15)}$ no es nilpotente.
Los subgrupos $X$ de orden seis y diez no son normales en $D_{2(15)}$ pues si lo fueran el cociente $D_{2(15)}/X$ sería abeliano y por lo tanto $D'_{2(15)} \leqslant X$ lo que sería una contradicción.
Los subgrupos $\langle a, b^3 \rangle$ y $\langle a, b^5 \rangle$ son isomorfos a $D_{2(5)}$ y $D_{2(3)}$ que son grupos no nilpotentes de ordenes diez, y seis respectivamente.
Hemos visto que $D_{2(15)}$ no es nilpotente, que todos sus subgrupos normales propios son nilpotentes y que tiene subgrupos propios no nilpotentes.

Comenzaremos caracterizando a todos los grupos que como $D_{2(15)}$ son solubles, no nilpotentes pero con todos sus subgrupos normales propios nilpotentes.

**Teorema.**
Sea $G$ un grupo soluble. Las siguientes propiedades son equivalentes.

**(1)** $G$ no es nilpotente pero todos sus subgrupos normales propios son nilpotentes.

**(2)** **(a)** $G$ es el producto de un $q$-grupo cíclico no trivial $Q$ y un $q'$-grupo nilpotente no trivial que coincide con $G'$ ($q$ un primo ).

**(b)** $M = G' \times Q^q$ es el único subgrupo normal máximo de $G$.

**Demostración.**
**(1)** implica **(2)**:
Sea $M$ el producto de todos los subgrupos normales de $G$, $M$ es nilpotente, y como $G$ no lo es, $M$ debe ser un subgrupo propio de $G$ que contiene a todos los subgrupos normales de $G$, por lo que $M$ es el único subgrupo normal máximo de $G$. Además como $G$ es soluble $[G:M]=q$ con $q$ un primo.
Como $G$ no es nilpotente existe un primo $p$ diferente de $q$ que divide al orden de $G$, y $M$ contiene a todos los subgrupos primarios de $G$ que no son $q$-grupos. Además como $M$ es nilpotente estos subgrupos de Sylow de $G$ son únicos y característicos en $G$.
Llamemos $N$ al producto de todos los subgrupos de Sylow de $G$ que no son $q$-grupos.
Si $Q$ es un $q$-subgrupo de Sylow de $G$ entonces $G=NQ$ y $Q\cap M$ es el $q$-subgrupo de Sylow de $M$, por lo que $M=N\times(Q\cap M)$.
Ahora demostraremos que $N=G'$.
Como $G/N$ es un $q$-grupo con un único subgrupo normal máximo $M/N$, entonces $G/N$ tiene un único subgrupo máximo, por lo que es cíclico, lo que implica que $G'\leqslant N$, y como $G/N\cong Q$, $Q$ es cíclico.
Además, $[G:G']=[G:N][N:G']$, por lo que $q$ divide al orden de $G/G'$. Como $G/G'$ es un grupo abeliano, tiene subgrupos para cada divisor de su orden, por lo que si $p$ es un primo que divide al orden de $G/G'$, este tiene un subgrupo normal $L/G'$ cuyo índice es $p$ por lo que $L$ sería un subgrupo normal máximo de $G$ y entonces $L=M$ y $p=q$, así $[N:G']=1$ y $N=G'$.
Se probó que $G=G'Q$ con $G'$ un $q'$-grupo nilpotente, y que el único subgrupo máximo $M$ de $G$ es el producto directo $G'$ y $Q^q=M\cap Q$.
Ahora hagamos notar que **(2)** implica **(1)**. Observemos que si $G$ fuera nilpotente entonces cualquier subgrupo máximo sería normal, pero como $G$ tiene un único subgrupo normal máximo, $G$ solo podría tener un subgrupo máximo, por lo que sería cíclico y $G'$ sería trivial, lo que contradice a **(2)(a)**.Por lo tanto $G$ no es nilpotente.
Además cualquier subgrupo normal de $G$ está contenido en $G'\times Q^q$ que es nilpotente pues es producto de grupos nilpotentes.■

**Lema 1 (Iwasawa-Schmidt).**
Si todo subgrupo propio de un grupo $G$ es nilpotente, se tiene que el grupo $G$ es soluble.
**Demostración:**
Supongamos que el lema es falso.
Sea $G$ un contraejemplo de orden mínimo, es decir que $G$ es un grupo no soluble con todos sus subgrupos propios nilpotentes de orden mínimo. Probaremos que $G$ es simple.
Si $G$ tuviera un subgrupo $N$ normal no trivial, $N$ sería nilpotente y por lo tanto soluble. Además si $S/N$ es un subgrupo propio de $G/N$, se tiene que $S$ es un subgrupo propio de $G$ y por lo tanto $S$ es nilpotente y $S/N$ es nilpotente, así cada subgrupo de $G/N$ es nilpotente y como el orden de $G/N$ es menor que el orden de $G$, $G/N$ es soluble, lo que implica que $G$ es soluble y tenemos una contradicción.
Por otro lado como $G$ no es cíclico, tiene cuando menos dos subgrupos máximos, cada uno con al menos dos elementos. Probaremos que cualquier par de subgrupos máximos diferentes de $G$ tiene intersección trivial.
Supongamos que $M_1$ y $M_2$ es la pareja de subgrupos máximos diferentes de $G$ cuya intersección es de orden máximo y nombremos a dicha intersección $S$. La intersección es un subgrupo propio de $M_1$, pues si fuera igual $M_1$ estaría contenido en $M_2$, y eso contracide la suposición de que $M_1$ y $M_2$ eran dos subgrupos máximos diferentes de $G$. De igual manera la intersección $S$ es un subgrupo propio de $M_2$.
Como $M_1$ es nilpotente $S<N_{M_1}(S)=M_1\cap N_G(S)$, y como $G$ es simple, si $S$ fuera un subgrupo no trivial se tendría que $N_G(S)<G$, por lo que existe un subgrupo máximo $L$ de $G$ que contiene a $N_G(S)$, y así

$S < M_1 \cap N_G(S) \leqslant M_1 \cap L$ lo cual es una contradicción pues habíamos supuesto que $S$ era la intersección de orden máximo entre pares de subgrupos máximos diferentes de $G$.Hemos probado que cada pareja de subgrupos máximos de $G$ se intersecan trivialmente.
Por otro lado si $M$ es un subgrupo máximo de $G$ entonces es igual a su normalizador pues $G$ es simple. Si el orden de $G$ es $n$ y el orden de $M$ es $m$, $[G:M] = n/m$. Sean $M = M_1, M_2, ..., M_{n/m}$ todos los subgrupos conjugados de $M$. Cada subgrupo conjugado de $M$ es un subgrupo máximo de $G$ de orden $m$, entonces $(m-1)n/m = n - n/m$ es la cantidad de elementos en $M_1 \cup ... \cup M_{n/m}$ diferentes de la identidad.
Como $G$ es simple $2 < n/m = [G:M]$, por lo que $n.n/m < n-2 < n-1$ lo que implica que $G$ tiene subgrupos máximos que no son conjugados de $M$. Además como $2 \leqslant m$ entonces $1/m \leqslant 1/2$ y así $n/2 = n - n/2 \leqslant n - n/m$ y como $n/2 - 1/2 < n/2$ ocurre que $(n-1)/2 < n - n/m$.
Si tomamos a $H$ otro subgrupo máximo de $G$ que no es conjugado de $M$ y el orden de $H$ es $h$, el número de elementos no triviales de todos los subgrupos conjugados de $H$ es $n - n/h$ y de igual forma $(n-1)/2 < n - n/h$ y así los elementos diferentes de la identidad que se encuentran en algún subgrupo conjugado de $M$ o algún subgrupo conjugado de $H$ son $(n-n/m)+(n-n/h) \leqslant n-1$, y además $2((n-1)/2) < (n-n/m)+(n-n/h) \leqslant n-1$ por lo que llegamos a la contradicción $n-1 < n-1$, por lo tanto $G$ es soluble. ■

**Lema 2 (Maschke)**.
Si $G$ es un grupo de automorfismos de un $p$-grupo abeliano elemental $A$, $p$ no divide al orden de $G$, y $S$ es un subgrupo de $A$ invariante bajo $G$, existe un subgrupo $T$, invariante bajo $G$ tal que $A = S \times T$.

**Demostración.**
Como $A$ es un $p$-grupo abeliano elemental, es un espacio vectorial sobre el campo de Galois de $p$ elementos $GF(p)$.
La idea de la demostración consiste en encontrar un operador lineal $\beta$ de $A$ que tenga como imagen a $S$, y que conmute con todos los elementos de $G$. Esto implicará que su núcleo $T$ es invariante bajo $G$, y que $A = S \times T$.
Sea $\theta$ una proyección de $A$ sobre $S$, se tiene que $S$ es la imagen de $\theta$. Además para cualquier automorfismo $g$, elemento de $G$, la composición $g^{-1}\theta g$ es un operador de $A$ cuya imagen está contenida en $S$, pues $g(S) = S$ y $\theta$ es una proyección sobre $S$.
Sea $\beta$ el operador $\Sigma_{g\in G}(g^{-1}\theta g)$. Si $\gamma$ es la restricción de $\beta$ a $S$ entonces $\gamma$ es un endomorfismo de $S$, además para cualquier elemento $s \neq 0$ de $S$, $\gamma(s) = \beta(s) = (\Sigma_{g\in G}(g^{-1}\theta g))(s) = \Pi_{g\in G}(g^{-1}\theta g)(s) = \Pi_{g\in G} g^{-1}\theta(g(s)) = \Pi_{g\in G} g^{-1}(g(s)) = \Pi_{g\in G} s = s^{|G|} \neq 1$ ya que $p$ no divide al orden de $G$, por lo cual $\gamma$ es un automorfismo de $S$. Así tenemos que la imagen de $A$ bajo $\beta$ es $S$.
Faltaría ver es que $\beta$ conmuta con todos los elementos de $G$, sin embargo para cualquier elemento $x$ de $G$ ocurre que $x^{-1}\beta x = x^{-1}(\Sigma_{g\in G}(g^{-1}\theta g))x = \Sigma_{g\in G}((gx)^{-1}\theta(gx)) = \Sigma_{g\in G}(g^{-1}\theta g) = \beta$. Hemos probado que $\beta$ conmuta con todos los elementos de $G$.

Sea $T$ el núcleo de $\beta$, para ver que $A$ es el producto directo de $S$ y $T$ basta ver que su intersección es trivial, ya que $dim(ST) = dim(S) + dim(T) - dim(S \cap T)$, pero si $x$ es un elemento de $S \cap T$ significa que $\beta(x) = 1$ pero como $x$ es un elemento de $S$ y $\beta$ es una función biyectiva en $S$, $x = 1$ y la intersección de $S$ con $T$ es trivial. Tenemos que $dim(ST) = dim(S) + dim(T) = dim(im(\beta)) + dim(ker(\beta)) = dim(V)$. ■

**Lema 3.** Si $G$ es un grupo soluble no nilpotente y tiene un único subgrupo normal propio no trivial, todos sus subgrupos propios son abelianos.

**Demostración.** $G$ es soluble y no es abeliano porque no es nilpotente, por lo que $G'$ es el único subgrupo normal no trivial de $G$. Así el índice en $G$ de $G'$ es primo.
Basta probar que cualquier subgrupo máximo de $G$ es abeliano pues cualquier subgrupo de $G$ está contenido en algún subgrupo máximo.
Sea $M$ un subgrupo máximo de $G$, si $M = G'$ entonces $M' = G'' = 1$ por lo que $M$ es abeliano. Si $M$ fuera diferente de $G'$, por ser un subgrupo máximo, $MG' = G$ y como $G'$ es abeliano se tiene que $M \cap G' \trianglelefteq G'$ y además $M \cap G' \trianglelefteq M$ por lo que $M \cap G'$ es un subgrupo normal de $G$ y así $M \cap G'$ debe ser $G'$ o 1. Si la intersección es $G'$, entonces $G'$ es un subgrupo de $M$, por lo que $M \triangleleft G$ y $M$ resulta ser $G'$, si es 1 entonces $G/G' = MG'/G' \cong M/1 \cong M$ por lo que $M$ es abeliano.

**Observación.** Si $n \geqslant 5$ el grupo $S_n$ tiene sólo un subgrupo normal propio no trivial, pero tiene subgrupos propios no abelianos, por lo que la hipótesis de que $G$ sea soluble es necesaria en el lema 3.

**Observación.** La hipótesis de que $G$ no sea nilpotente no es necesaria en el lema 3, si $G$ es nilpotente, $G$ tiene solo un subgrupo máximo, pues cualquier subgrupo máximo es normal, por lo que $G$ es un $p$-grupo pues para cada primo $q$ que divide el orden de $G$, existe un subgrupo $H$ de índice $q$ en $G$, por lo que $H$ es máximo y normal en $G$. Por lo tanto $G$ es cíclico y todos sus subgrupos son abelianos. La hipótesis de que $G$ no sea nilpotente se agrega en el lema 3 para no considerar el caso en el que $G$ es abeliano en la demostración, y para que las hipótesis coincidan con las condiciones del teorema que se prueba a continuación.

Ahora caracterizaremos a los grupos que como $S_3$ no son nilpotentes pero todos sus subgrupos propios si lo son.

**Teorema:**
Si $G$ es un grupo las siguientes tres condiciones son equivalentes.

(1) $G$ no es nilpotente pero todos sus subgrupos propios son nilpotentes.

(2) (a) Existen $p$ y $q$ primos diferentes tales que $G = PQ$ con $P$ un subgrupo de $G$ de orden $p^m$ que coincide con $G'$ y $Q$ un $q$-subgrupo cíclico de $G$ de orden $q^n$ $(m, n \geq 1)$. Además $G$ tiene un único subgrupo normal máximo $M$ y $M = P \times Q^q$.

(b) $Z(G) = \Phi(G) = P^p \times Q^q$.

(c) $M = PZ(G)$, y $M/Z(G)$ es el único subgrupo normal de $G/Z(G)$.

(3) (a) $Z(G) = \Phi(G)$.

(b) $G/Z(G)$ no es nilpotente pero todos sus subgrupos propios son abelianos.

**Demostración:**
Se probará que **(1)** implica **(2)**.
En virtud del teorema que se enuncia al principio de este capítulo, para probar que se cumple **(2)(a)** lo único que falta hacer ver es que el $q'$-subgrupo nilpotente $N$ que coincide con $G'$ es un $p$-grupo. Como $N$ contiene a todos los subgrupos de Sylow de $G$ que no son $q$-grupos, $N = P_1 \times ... \times P_k$ con $P_i$ un $p_i$-subgrupo de Sylow de $G$. Si suponemos que $k \geqslant 2$ entonces $P_iQ$ es un subgrupo propio de $G$ por lo que es nilpotente, y todos los elementos de $Q$ conmutan con todos los elementos de $P_j$ para cualquier $j$, por lo que todos los elementos de $Q$ conmutan con todos los elementos de $N$, además como $Q$ es cíclico todos sus elementos conmutan entre si, y como $G = NQ$ entonces $Q$ esta contenido en el centro de $G$ y es un subgrupo normal de $G$, por lo que todos los subgrupos de Sylow de $G$ son normales y $G$ es nilpotente, lo cual es una conradicción. Por lo tanto $K = 1$ y $N$ es un $p$-grupo con $p \neq q$.

Para probar **(2)(b)** se observará primero que $Z(G) \leqslant \Phi(G)$, para ello supongamos que existe un subgrupo máximo $M$ de $G$ que no contiene al centro, entonces el producto $MZ(G)$ es todo $G$, por lo que $G/Z(G) \cong M/M \cap Z(G)$ que es nilpotente pues $M$ es nilpotente, así $G$ sería nilpotente, lo que es una contradicción y por lo tanto $Z(G) \leqslant \Phi(G)$.

Ahora probaremos que $\Phi(G) \leqslant Z(G)$.
Observemos que $Q$ no es un subgrupo normal de $G$ pues si lo fuera $G$ sería nilpotente. El subgrupo normal generado por $Q$, y denotado $Q^G$ coincide $G$ pues de no ser así tendría que ser un subgrupo de el único subgrupo normal máximo $M$ y entonces también $Q$ sería un subgrupo de $M$ lo cual es una contradicción pues el $[G : M] = q$ y $Q$ es un $q$-subgrupo de Sylow de $G$. Además como $Q^q$ es el $q$-subgrupo de Sylow de $M$ y $M$ es nilpotente $Q^q$ conmuta con todos los elementos de $P$ y también con todos los elementos de $Q$ pues $Q$ es cíclico, por lo que $Q^q$ es un subgrupo del centro de $G$.
Por otro lado si $Q$ es un $q$-subgrupo de Sylow de $G$, $Q$, está contenido en algún subgrupo máximo $L$ de $G$ y como $\Phi(G)$ también es un subgrupo de $L$, $Q\Phi(G)$ es un subgrupo propio de $G$ y por lo tanto es nilpotente. Como $P \cap \Phi(G) \lhd G$ entonces $Q(P \cap \Phi(G))$ es un subgrupo de $Q\Phi(G)$ y es nilpotente. Así todos los elementos de $Q$ conmutan con todos los elementos de $P \cap \Phi(G)$ y como esto ocurre para cualquier $q$-subgrupo de Sylow de $G$, entonces todos los elementos de $Q^G = G$ conmutan con todos

los elementos de $P \cap \Phi(G)$, por lo que $P \cap \Phi(G) \leqslant Z(G)$.
Tenemos que $Q^q \leqslant Z(G) \leqslant \Phi(G)$, además como $PQ^q$ es un subgrupo máximo de $G$, $\Phi(G) = (PQ^q) \cap \Phi(G)$. Así por la ley de Dedekind $\Phi(G) = (PQ^q) \cap \Phi(G) = (P \cap \Phi(G))Q^q \leqslant Z(G)$.
Por lo tanto $\Phi(G) = Z(G)$.

Ahora probaremos que $Z(G) = P^p \times Q^q$.
Si ocurriera que $P \cap Z(G) = P^p$, por la ley de Dedekind tendríamos que $Z(G) = \Phi(G) = M \cap \Phi(G) = (P \times Q^q) \cap Z(G) = (P \cap Z(G))Q^q = P^p Q^q$.
Probaremos entonces que $P \cap Z(G) = P^p$. Primero observemos que se cumplen las siguientes dos propiedades.
**(i)** $P \cap Z(G) < P$.
**(ii)** Si $X$ es un subgrupo normal de $G$ y un subgrupo propio de $P$, $X$ está contenido en el centro de $G$.

**Demostración de (i).** Si $P \cap Z(G) = P$ entonces $G' = P \leqslant Z(G)$ por lo que $G/Z(G)$ sería abeliano y $G$ sería nilpotente, lo cual sería una contradicción.

**Demostración de (ii).** $|XQ| = |X||Q| < |P||Q| = |G|$, por lo que $XQ$ es nilpotente y todos los elementos de $Q$ conmutan con todos los elementos de $X$ y como esto pasa para cualquier $q$-subgrupo de Sylow de $G$ entonces todos los elementos de $G = Q^G$ conmutan con todos los elementos de $X$ y así $X \leqslant Z(G)$.

Demostremos que $P \cap Z(G) = P^p$. Observemos que $P^p$ es un subgrupo característico de $P$ y por lo tanto un subgrupo normal de $G$. Nombremos a $G^* = G/P^p$ y $P^* = P/P^p$. Por el teorema de la correspondencia $P^* \lhd G^*$.
Consideremos ahora la función $\varphi : G^* \longrightarrow aut(P^*)$ tal que para $gP^p \in G^*$ y $xP^p \in P^*$, $\varphi(gP^p)(xP^p) = (gxg^{-1})P^p$. $\varphi$ es un homomorfismo, nombremos como $\Gamma$ a la imagen de $\varphi$. probaremos que $\Gamma$ es un $q$-grupo viendo que todos los elementos de $\Gamma$ tiene como orden una potencia de $q$.
$G^*/P^* \cong G/P \cong Q$, eso significa que si tomamos un elemento $gP^p = g^*$ en $G^*$ va a existir una potencia de $q$ que sea el orden de $g^*P^*$ es decir que $(g^*)^{q^n} \in P^*$ para algún $n$, por lo que $g^{q^n}$ es un elemento de $P$ y como $P/P^p$ es abeliano, para cualquier elemento $xP^p$ de $P/P^p$ ocurre

$$(\varphi(g^*))^{q^n}(xP^p) = \varphi((g^*)^{q^n})(xP^p) = (g^{q^n} x g^{-q^n})P^p = xP^p.$$

Por lo tanto $\Gamma$ es un $q$-grupo.

Como $P^p$ es un subgrupo normal de $G$ y está contenido propiamente en $P$, en virtud de **(ii)** $P^p$ es un subgrupo del centro de $G$ y entonces $P^p$ está contenido en $P \cap Z(G)$. Consideremos al grupo $T = (P \cap Z(G))/P^p$, si $tP^p$ es un elemento de $T$ entonces $\varphi(gP^p)(tP^p) = gtg^{-1}P^p = tP^p$ por lo que $T$ es invariante bajo cualquier elemento de $\Gamma$.

Como $P^*$ es un $p$-grupo abeliano elemental, $\Gamma$ es un grupo de automorfismos de $P^*$ y $T$ un subgrupo de $P^*$ invariante bajo $\Gamma$; en virtud del teorema de Maschke existe $U = W/P^p$ subgrupo de $P^*$ invariante bajo todo automorfismo de $\Gamma$, por lo que $W$ es un subgrupo normal de $G$. Si $W$ fuera un subgrupo propio de $P$ entonces por **(ii)** $W$ estaría contenido en el centro de $G$ y ocurriría que $W = P \cap W = P \cap (Z(G) \cap W) = (P \cap Z(G)) \cap W = P^p$, y $P/P^p = (P \cap Z(G))/P^p \times P^p/P^p = (P \cap Z(G))/P^p$ lo que implica que $P \cap Z(G) = P$ y eso es una contradicción. Por lo tanto $W = P$ y $(P \cap Z(G))/P^p = 1$ lo que implica que $P^p = P \cap Z(G)$, y hemos probado que se cumple **(2)(b).**

Para terminar la demostración de que **(1)** implica **(2)** solo falta probar que se cumple **(2)(c)**.
Sabemos que $M = P \times Q^q$ es el unico subgrupo normal máximo de $G$, como $P$ y el centro de $G$ son subgrupos de $M$ y $Q^q$ es un subgrupo del centro de $G$ se tiene que $M = PQ^q \leqslant PZ(G) \leqslant M$ y de ahí que $M = PZ(G)$.
Solo falta probar que $M/Z(G)$ es el único subgrupo normal de $G/Z(G)$.
Primero probaremos que $M/Z(G)$ es un subgrupo normal mínimo de $G/Z(G)$. Supongamos que $X$ es un subgrupo normal de $G$ que contiene al centro de $G$ y esta contenido en $M$, entonces $X = Z(G)X = Z(G)(X \cap M) = Z(G)(X \cap PZ(G))$ pero por la ley de Dedekind $X \cap PZ(G) = Z(G)(X \cap P)$ por lo que $X = Z(G)(X \cap P)$.
Supongamos que $X$ es un subgrupo propio de $M$, entonces tiene que ocurrir que $X \cap P$ sea un subgrupo propio de $P$ pues si la interseccion fuera igual a $P$, $P$ estaría contenido en $X$ y como el centro de $G$ también es un subgrupo propio de $X$ ocurriría que $M = PZ(G) \leqslant X$ lo que seria una contradicción.
Como $X \cap P \lhd G$ y $X \cap P$ es un subgrupo propio de $P$ entonces $X \cap P$ es un subgrupo del centro de $G$, por lo que $X$ coincide con el centro de $G$ y así $M/Z(G)$ es un subgrupo normal mínimo de $G/Z(G)$.

Supongamos que $L/Z(G)$ es un subgrupo normal mínimo de $G/Z(G)$, eso significa que $L$ contiene al centro de $G$ y está contenido en $M$ pues $M$ es el único subgrupo normal máximo de $G$, por lo que $L/Z(G)$ es un subgrupo de $M/Z(G)$ pero como $M/Z(G)$ es normal mínimo entonces $L = M$ y así $M/Z(G)$ es el único subgrupo normal mínimo de $G/Z(G)$.

Como $M/Z(G)$ es el único subgrupo normal mínimo y el único subgrupo normal máximo de $G/Z(G)$ es el único subgrupo normal de $G/Z(G)$ por lo que se ha probado **(2)(c)**.

Ahora probaremos que **(2)** implica **(3)**.
Solo hace falta probar **(3)(b)**.
Supongamos que $G/Z(G)$ es nilpotente. como $Q$ es un grupo cíclico generado por un elemento $x$, $Q^q$ está generado por $x^q$ por lo que $Q^q$ es un subgrupo propio de $Q$. Por otro lado Si tomamos un subgrupo máximo $M$ de $P$, entonces $M$ es normal en $P$ y $[P : M] = p$ por lo que $x^p$ está en $M$ para cualquier $x$ en $P$ y $P^p$ está contenido en $M$ que es un subgrupo propio de $P$, así tanto $p$ como $q$ dividen al orden de $G/Z(G)$ por lo que tiene al menos dos subgrupos de Sylow diferentes y por lo tanto dos subgrupos normales diferentes, lo cual contradice **(2)(c)**, entonces $G/Z(G)$ no puede ser nilpotente.
Por otro lado como $G'$ coincide con $P$ es soluble, y $G/G'$ también es soluble pues es isomorfo a $Q$, así $G$ es soluble y también $G/Z(G)$ es un grupo soluble, y no es nilpotente. Además tiene un único subgrupo normal no trivial, por lo tanto por el lema anterior todos sus subgrupos propios son abelianos.

Se probará que **(3)** implica **(1)**.
$G$ no es nilpotente por que $G/Z(G)$ no es nilpotente.
Basta probar que cualquier subgrupo máximo de $G$ es nilpotente. supongamos que $M$ es un subgrupo máximo de $G$, entonces contiene a $\Phi(G) = Z(G)$, y además $M/Z(G)$ es abeliano por lo que $M \geqslant Z(G) \geqslant 1$ es una serie central de $M$ y $M$ es nilpotente.

Para terminar el trabajo haremos notar que existen grupos no solubles, con todos sus subgrupos normales propios nilpotentes, y que tienen subgrupos propios no nilpotentes.

**Ejemplo 3.**

Consideremos el grupo $SL(n,F)$ con $n \geqslant 2$ y $|F| > 3$.
Sabemos que el grupo $PSL(n,F) = SL(n,F)/Z(SL(n,F))$ es simple y no abeliano por lo que no es soluble. Entonces $SL(n,F)$ no es soluble, pues de serlo $PSL(n,F)$ lo sería.
También sabemos que si $N \trianglelefteq SL(n,F)$, entonces $N \subseteq Z(SL(n,F))$ por lo que todos los subgrupos normales de $SL(n,F)$ son abelianos y por lo tanto nilpotentes, sin embargo si todos los subgrupos propios de $SL(n,F)$ fueran nilpotentes entonces en virtud del teorema de Iwasawa-Schmidt $SL(n,F)$ sería soluble y eso sería una contradicción. Por lo tanto $SL(n,F)$ tiene un subgrupo propio no nilpotente.

# Bibliografía

[ 1 ] Alperin, J.L. y Rowen, B.B., "Groups and Representations", Springer-Verlag, New York, 1995.

[ 2 ] Feit, W., Characters of finite groups", W.A. Benjamin, New York, 1967.

[ 3 ] Morales, J., "Sopra alcune classi di gruppi minimali non-P", Academia Nazionale dei Lincei, Roma, 1985.

[ 4 ] Rotman, J.J., An introduction to the Theory of Groups", 4a ed., Springer-Verlag, New York, 1995.

[ 5 ]Kurzweil, H. y Stellmacher, B., "The Theory of Finite Groups", Springer-Verlag, New York, 2000.

[ 6 ] Baer, R., "Topics in Finite Groups (Minimal classes)", Istituto Matemático Ulisse Dini, Firenze, 1975.

[ 7 ] Guido, Z., "Topics on Finite Solvable Groups", Istituto Nazionale di Alta Matematica Francesco Severi, Roma, 1982.

**Notación.**

| | |
|---|---|
| $\mathbb{Z}$ | Números enteros. |
| $\mathbb{Z}_p$ | Números enteros modulo $p$. |
| $(a,b)$ | Máximo común divisor de $a$ y $b$. |
| $x \equiv y (m\acute{o}d n)$ | $n$ divide a $x-y$. |
| $M_n(F)$ | Matrices de $n \times n$ con coeficientes en el campo $F$. |
| $B \subseteq A$ | $B$ es un subconjunto de $A$. |
| $B \subset A$ | $B$ es un subconjunto propio de $A$. |
| $A \cap B$ | Intersección de $A$ y $B$. |
| $A \cup B$ | Unión de $A$ y $B$. |
| $A \times B$ | Producto cartesiano de los conjuntos $A$ y $B$. |
| 1 | Elemento identidad del grupo $G$. |
| $H \leqslant G$ | $H$ es un subgrupo del grupo $G$. |
| $H < G$ | $H$ es un subgrupo propio del grupo $G$. |
| $H \trianglelefteq G$ | $H$ es un subgrupo normal del grupo $G$. |
| $H \triangleleft H$ | $H$ es un subgrupo normal propio del grupo $G$. |
| $H \ntrianglelefteq G$ | $H$ no es un subgrupo normal del grupo $G$. |
| $G \cong H$ | Los grupos $G$ y $H$ son isomorfos. |
| $\|G\|$ | Orden de $G$. |
| $[G:H]$ | Índice de $H$ en $G$. |
| $xH$ | Clese lateral izquierda de $H$. |
| $G/H$ | Grupo cociente de $G$ en $H$. |
| $H \cong G$ | $H$ es isomorfo a $G$. |
| $\langle X \rangle$ | Subgrupo generado por $X$. |
| $\langle x_1, \ldots, x_n \rangle$ | Subgrupo generado por $\{x_1, \ldots, x_n\}$. |
| $H \leqslant_{car} G$ | $H$ es un subgrupo característico de $G$. |
| $[x,y]$ | Conmutador de $x$ con $y$ ($[x.y] = xyx^{-1}y^{-1}$). |
| $[A,B]$ | Subgrupo generado por $\{[a,b] \| a \in A, b \in B\}$. |
| $G'$ | Subgrupo derivado de $G$ ($[G,G]$). |
| $G^{(k+1)}$ | Subgrupo derivado de $G^K$. |
| $Z(G)$ | Centro de $G$. |
| $G_x$ | Estabilizador de $x$ bajo la acción de $G$. |
| $C_G(x)$ | Centralizador de $x$ en $G$. |
| $N_G(H)$ | Normalizador en $G$ de $H$. |
| $G_1 \times \ldots \times G_n$ | Producto directo de los grupos $G_1, \ldots, G_n$. |
| $\varphi(G)$ | Imagen de $G$ bajo $\varphi$. |
| $Aut(G)$ | Grupo de automorfismos de $G$. |
| $S_n$ | Grupo de permutaciones de un conjunto de $n$ elementos. |
| $A_n$ | Grupo de permutaciones pares de un conjunto de $n$ elementos. |
| $D_{2(n)}$ | Grupo dihedrico de orden $2n$. |
| $GL(n,F)$ | Grupo de matrices invertibles de tamaño $n \times n$ con coeficientes en el campo $F$. |
| $SL(n,F)$ | Grupo de matrices con determinante 1, tamaño $n \times n$ y coeficientes en el campo $F$. |
| $PSL(n,F)$ | Grupo proyectivo lineal especial ($SL(n,F)/Z(SL(n,F))$). |
| $I$ | Matrix identidad. |
| $id$ | Función identidad. |
| $GL(V)$ | Grupo de transformaciones lineales invertibles sobre el $F$-espacio vectorial $V$. |
| $Car(F)$ | Característica del campo $F$. |
| $\phi(G)$ | Subgrupo de Frattini de un grupo $G$. |
| $GF(p)$ | Campo de Galois de $p$ elementos. |