UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

SOBRE EL P-Q TEOREMA DE BURNSIDE

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A:

JOSÉ ROBERTO DE LA VEGA MARTÍNEZ

DIRECTOR DE TESIS:
DR. JUAN MORALES RODRÍGUEZ
2011

Hoja de Datos del Jurado

1. Datos del alumno
   De la Vega
   Martínez
   José Roberto
   55 36 07 27
   Universidad Nacional Autónoma de México
   Matemáticas
   300098600

2. Datos del tutor
   Dr.
   Juan
   Morales
   Rodríguez

3. Datos del sinodal 1
   M. en C.
   Manuel Gerardo
   Zorrilla
   Noriega

4. Datos del sinodal 2
   Dra.
   María del Carmen Heréndira
   Gómez
   Laveaga

5. Datos del sinodal 3
   Dra.
   Bertha María
   Tomé
   Arreola

6. Datos del sinodal 4
   Dr.
   Emilio Esteban
   Lluis
   Puebla

7. Datos del trabajo escrito
   Sobre el p-q Teorema de Burnside
   41 p
   2011

Índice general.

Introducción.

El *p-q* Teorema de Burnside, que asegura que todo grupo finito cuyo orden es divisible por a lo más dos primos es soluble, es uno de los primeros grandes resultados de la teoría de grupos en el siglo XX. La demostración dada por William Burnside en 1904 es breve y elegante, pero requiere de la teoría de carácteres introducida por Georg Frobenius. Pasaron más de sesenta años antes de que Bender, Goldschmidt y Matsuyama dieran la primera demostración del resultado de Burnside que fuese independiente de la teoría de carácteres. Sin embargo, esta demostración resultó ser más larga y compleja.

Durante los años 1975 y 1976, el profesor Guido Zappa impartió un curso en la "Scuola di perfezionamiento in Matematica" de la Universidad de Florencia por encargo del "Istituto Nazionale di Alta Matematica", en el cual se da una demostración del p-q Teorema de Burnside sin usar teoría de carácteres. Esta demostración también se debe esencialmente a Goldschmidt, Bender y Matsuyama. Con más precisión, Goldschmidt había dado la demostración del teorema para el caso impar usando una idea de Bender, y por su cuenta Matsuyama había dado la prueba del caso par; Bender, independientemente de Matsuyama, dio una prueba válida para ambos casos. Bender pronto vio cómo simplificar su demostración utilizando procedimientos de Matsuyama. Bender no había publicado este último resultado en esas fechas, pero compartió con el profesor Zappa sus ideas en una carta, informándolo en una forma sintética acerca de esta demostración y autorizándolo a hacer uso de ella en la publicación de su libro "Topics on Finite Solvable Groups", basado en las notas del curso que impartió.

La elaboración del presente trabajo consistió en la comprensión y redacción de esta prueba.

En la sección de Prerrequisitos se encuentran los resultados elementales que necesité para las demostraciones. Una demostración utilizando teoría de carácteres se revisa en el Apéndice A.

La notación en este trabajo es la usual, en particular es la presentada en [6].

Capítulo 1.
Prerrequisitos.

1.1 Definiciones.

Definición. Sea G un grupo finito y p un primo que divida al orden de G. H es un *p-subgrupo de Sylow* si el orden de H es p^n y p^{n+1} ya no divide el orden de G.

Definición. Sea G un grupo finito y P un p-subgrupo de G con p un primo. P es un *subgrupo central* de G si existe S_p un p-subgrupo de Sylow de G tal que $P \leq Z(S_p)$.

Definición. Un grupo M de permutaciones de un conjunto finito I se llama *regular* si para cada $h \in I$, sólo la identidad de M fija a h. Un grupo A de automorfismos en un grupo finito G se dice *regular* si el grupo de permutaciones inducido por A en el conjunto $G - \{1\}$ es regular.

Definición. Sea G un grupo y $G = H_0 \geq H_1 \geq H_2 \geq \ldots H_r = \langle 1 \rangle$ una cadena de subgrupos normales de G. Un automorfismo α de G se dice que estabiliza esta cadena si $\alpha(H_i) = H_i$ $(i = 1, \ldots, r)$ y α induce la identidad en cada factor $\frac{H_{i-1}}{H_i}$.

Definición. Sea G un grupo. Una serie de subgrupos $G = G_0 \geq G_1 \geq \ldots \geq G_r = \langle 1 \rangle$ se llama una *serie subnormal* de G si $G_{i+1} \trianglelefteq G_i$ para toda i.

Definición. Sea G un grupo. Una serie subnormal de G se llama una *serie de composición* de G si cada cociente sucesivo $\frac{G_i}{G_{i+1}}$ es simple.

Definición. Sea G un grupo. Una serie subnormal que cumple que $G_i \trianglelefteq G$ para toda i se llama *serie normal* de G.

Definición. Sea G un grupo. El conmutador de x y y con $x, y \in G$ es $[x,y] = x^{-1}y^{-1}xy$. Sean A y B subconjuntos no vacíos de G. El subgrupo $\left\langle [x,y] \mid x \in A, y \in B \right\rangle$ se denota $[A,B]$ y se llama el *interderivado* de A y B.

Definición. Sea G un grupo. Sean A, B y C subconjuntos no vacíos de G y a, b y c elementos de A, B y C respectivamente. $[A,B,C] = [[A,B],C]$ y $[a,b,c] = [[a,b],c]$.

Definición. Sea G un grupo. El *grupo derivado* de G (G') es el subgrupo $[G,G]$.

Definición. Sea G un grupo. Sean $Z_0 = \langle 1 \rangle$, $Z_1 = Z(G)$, $\frac{Z_i}{Z_{i-1}} = Z\left(\frac{G}{Z_{i-1}}\right)$ con $i > 1$. La serie $Z_0 \leq Z_1 \leq Z_2 \leq \ldots \leq Z_n \leq \ldots$ se conoce como *serie central ascendente* de G.

Definición. Sea G un grupo. Sean $G_1 = G$, $G_i = [G_{i-1}, G]$ con $i > 1$. La serie $G_1 \geq G_2 \geq \ldots \geq G_n \geq \ldots$ se conoce como *serie central descendente* de G.

Definición. Sea G un grupo. Si en la serie central ascendente de G existe n con $Z_n = G$, el grupo G se llama *nilpotente*.

Definición. Sea G un grupo. La serie de subgrupos $G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \ldots \geq G^{(n)} \geq \ldots$ de un grupo G donde $G^{(0)} = G$ y $G^{(k+1)} = G^{(k)\prime}$, el grupo derivado de $G^{(k)}$, se llama la *serie derivada* de G.

Definición. Un grupo cuya serie derivada termina en la identidad se llama *soluble*.

Definición. Sea P un p-grupo. El *subgrupo de Thompson* de P (denotado $J(P)$) es el subgrupo generado por los subgrupos abelianos elementales de P de orden máximo.

Definición. Sea G un grupo. El *soclo* de G es el producto de todos los subgrupos normales minimales de G. Si G es un p-grupo, el soclo de G se denota $\Omega_1(G)$.

Definición. Sea G un grupo finito y p un primo. $O_p(G)$ es el producto de todos los subgrupos normales de orden una potencia de p. De forma equivalente, $O_p(G)$ es la intersección de todos los p-subgrupos de Sylow de G.

Definición. Sea G un grupo. El *subgrupo de Fitting* de G (denotado $F(G)$) es el producto de todos los subgrupos normales nilpotentes de G.

Definición. Sea G un grupo y p y q primos distintos. $O_{p,q}(G)$ es el subgrupo de G que cumple con $\frac{O_{p,q}(G)}{O_p(G)} = O_q\left(\frac{G}{O_p(G)}\right)$.

1.2 Algunos teoremas útiles.

Teorema 1. Sea G un p-grupo finito (p primo), y N un subgrupo normal de G. Sea α un automorfismo de G de orden q^r (q primo, $q \neq p$, $r \geq 0$) que estabiliza la cadena $\langle 1 \rangle \leq N \leq G$. Entonces α es el automorfismo identidad.

Demostración:
Sea $x \in G$. Entonces $xN = \alpha'(xN) = \alpha(x)N$, con α' el automorfismo inducido por α en $\frac{G}{N}$, así que $\alpha(x) = xh$ con $h \in N$. Por inducción vemos que $\alpha^n(x) = \alpha^{n-1}(xh) = \alpha^{n-1}(x)\alpha^{n-1}(h) = xh^{n-1}h = xh^n$ ya que α induce la identidad en N, entonces se tiene que $\alpha^{q^r}(x) = xh^{q^r}$, pero $\alpha^{q^r} = 1$, así que $x = \alpha^{q^r}(x) = xh^{q^r}$, es decir, $h^{q^r} = 1$. Como el orden de los elementos distintos de la identidad es una potencia de p, se tiene que $h = 1$, y por lo tanto, $\alpha(x) = x$ para todo $x \in G$, es decir, α es el automorfismo identidad. ■

Teorema 2 (**Relación de Dedekind**). Sea G un grupo y X, Y y Z subgrupos de G tales que $Y \leq X$. Se tiene que $X \cap (YZ) = Y(X \cap Z)$.

Teorema 3. Sea G un p-grupo. Entonces $\Omega_1(G) = \Omega_1(Z(G))$.

Demostración:
Sea N un subgrupo normal minimal de G. Como G es un p-grupo, $N \cap Z(G) \neq \langle 1 \rangle$, donde $N \cap Z(G) \leq Z(G)$ y $N \cap Z(G) \trianglelefteq G$, por la minimalidad de N, $N = N \cap Z(G)$. Al ser N subgrupo de $Z(G)$, todo subgrupo de N es normal en G, nuevamente por la minimalidad de N, N no tiene subgrupos propios no triviales, entonces N es de orden p, y N es subgrupo normal minimal de $Z(G)$, por ello $\Omega_1(G) \leq \Omega_1(Z(G))$.
Sea M normal minimal de $Z(G)$. M es normal en G y es de orden p por la razón dada anteriormente, así que es normal minimal en G, entonces $\Omega_1(G) = \Omega_1(Z(G))$. ■

Teorema 4. Sea G un grupo y H, K y L subgrupos de G tales que $[K,L,H] = \langle 1 \rangle$ y $[L,H,K] = \langle 1 \rangle$. Entonces $[H,K,L] = \langle 1 \rangle$.

Demostración:
Primero veamos que si a, b, c pertenecen a un grupo, entonces $(b^{-1}[a,b^{-1},c]b)(c^{-1}[b,c^{-1},a]c) = (a^{-1}[c,a^{-1},b]a)^{-1}$.

$b^{-1}[a,b^{-1},c]b = b^{-1}([a,b^{-1}]^{-1}c^{-1}[a,b^{-1}]c)b = b^{-1}((ba^{-1}b^{-1}a)c^{-1}(a^{-1}bab^{-1})c)b = a^{-1}b^{-1}ac^{-1}a^{-1}bab^{-1}cb$.

Análogamente, $c^{-1}[b,c^{-1},a]c = b^{-1}c^{-1}ba^{-1}b^{-1}cbc^{-1}ac$.

Y también $(a^{-1}[c,a^{-1},b]a)^{-1} = (c^{-1}a^{-1}cb^{-1}c^{-1}aca^{-1}ba)^{-1} = a^{-1}b^{-1}ac^{-1}a^{-1}cbc^{-1}ac$.

Entonces $(b^{-1}[a,b^{-1},c]b)(c^{-1}[b,c^{-1},a]c) =$
$(a^{-1}b^{-1}ac^{-1}a^{-1}bab^{-1}cb)(b^{-1}c^{-1}ba^{-1}b^{-1}cbc^{-1}ac) =$
$a^{-1}b^{-1}ac^{-1}a^{-1}(b(a(b^{-1}(c(bb^{-1})c^{-1})b)a^{-1})b^{-1})cbc^{-1}ac =$
$a^{-1}b^{-1}ac^{-1}a^{-1}cbc^{-1}ac = (a^{-1}[c,a^{-1},b]a)^{-1}$.

Sean $l \in L$, $h \in H$, y $k \in K$. Entonces $[k,l^{-1},h] = 1$ y $[l,h^{-1},k] = 1$, y por lo tanto $(l^{-1}[k,l^{-1},h]l)(h^{-1}[l,h^{-1},k]h) = 1$, pero por lo visto antes se tiene que $(l^{-1}[k,l^{-1},h]l)(h^{-1}[l,h^{-1},k]h) = (k^{-1}[h,k^{-1},l]k)^{-1}$, y como $k^{-1}[h,k^{-1},l]k = 1$, entonces $[h,k^{-1},l] = 1$. Entonces para todo $l \in L$, $h \in H$, y $k \in K$ se tiene que $[h,k,l] = 1$. Sea $x \in [H,K]$ y $y \in L$, x es de la forma $[a_1,b_1][a_2,b_2]\ldots[a_n,b_n]$ con $a_i \in H$ y $b_i \in K$. Por inducción sobre n veamos que $[x,y] = 1$. Si $n = 1$ entonces $[x,y] = x^{-1}y^{-1}xy = [a_1,b_1]^{-1}y^{-1}[a_1,b_1]y = [a_1,b_1,y] = 1$, supongamos ahora que $x = [a_1,b_1][a_2,b_2]\ldots[a_n,b_n]$, entonces $[x,y] = x^{-1}y^{-1}xy =$
$[a_n,b_n]^{-1}\ldots[a_2,b_2]^{-1}[a_1,b_1]^{-1}y^{-1}[a_1,b_1][a_2,b_2]\ldots[a_n,b_n]y =$
$[a_n,b_n]^{-1}\ldots[a_2,b_2]^{-1}([a_1,b_1]^{-1}y^{-1}[a_1,b_1]y)y^{-1}[a_2,b_2]\ldots[a_n,b_n]y =$
$[a_n,b_n]^{-1}\ldots[a_2,b_2]^{-1}([a_1,b_1,y])y^{-1}[a_2,b_2]\ldots[a_n,b_n]y =$
$[a_n,b_n]^{-1}\ldots[a_2,b_2]^{-1}(1)y^{-1}[a_2,b_2]\ldots[a_n,b_n]y = [x',y]$ con $x' = [a_2,b_2]\ldots[a_n,b_n]$, entonces por hipótesis de inducción $[x,y] = [x',y] = 1$. Entonces $[[H,K],L] = [[H,K,L] = \langle 1 \rangle$. ■

Teorema 5 (**Teoremas de Sylow**). Sea G un grupo finito y p un primo que divide al orden de G.

a) G tiene al menos un p-subgrupo de Sylow.
b) Todos los p-subgrupos de Sylow son conjugados.
c) Todo p-subgrupo de G está contenido en algún p-subgrupo de Sylow.
d) El número de p-subgrupos de Sylow de G es congruente con 1 módulo p.
e) El número de p-subgrupos de Sylow de G divide a $[G : P]$ con P un p-subgrupo de Sylow.

Teorema 6 (**Argumento de Frattini**). Sea G un grupo finito, N un subgrupo normal de G, y P un p-subgrupo de Sylow de N. Entonces $G = N_G(P)N$.

Teorema 7. Sea G un grupo finito. Las siguientes propiedades son equivalentes:

a) G es nilpotente.
b) Todo subgrupo de Sylow de G es normal en G.
c) G es producto directo de sus subgrupos de Sylow.
d) Todo subgrupo maximal de G es normal en G.
e) La serie central descendente de G llega a $\langle 1 \rangle$.
f) Si A es subgrupo de G, entonces $A \lneqq N_G(A)$.

Teorema 8. Los grupos nilpotentes son solubles.

Teorema 9. Los p-grupos finitos son nilpotentes.

Teorema 10. Sea G un grupo y sea $N \leq G$. $N \trianglelefteq G$ y $\frac{G}{N}$ es abeliano si y sólo si $G' \leq N$.

Teorema 11. Sea G un grupo finito soluble, entonces $C_G(F(G)) \leq F(G)$.

Demostración:
Supongamos que $C_G(F(G)) \nsubseteq F(G)$. Entonces $F(G) \lneqq F(G)C_G(F(G))$. Como $F(G)$ y $C_G(F(G))$ son normales en G, $F(G)C_G(F(G))$ es normal en G, y $\frac{F(G)C_G(F(G))}{F(G)}$ es un subgrupo normal de $\frac{G}{F(G)}$ no trivial, por lo tanto existe un subgrupo normal minimal de $\frac{G}{F(G)}$ contenido en $\frac{F(G)C_G(F(G))}{F(G)}$. Sea $\frac{N}{F(G)}$ un subgrupo normal minimal de $\frac{G}{F(G)}$ contenido en $\frac{F(G)C_G(F(G))}{F(G)}$. Como G es soluble, $\frac{G}{F(G)}$ también lo es por el Teorema S4, y siendo $\frac{N}{F(G)}$ subgrupo normal minimal entonces es abeliano elemental porque todo subrupo normal minimal es producto directo de grupos simples isomorfos entre sí (la demostración de este hecho se puede revisar en [1]) y por los Teoremas S2 y S4, por lo tanto $N' \leq F(G)$. Como $F(G) \leq N$, entonces por la relación de Dedekind (Teorema 2) se tiene que $N \cap F(G)C_G(F(G)) = F(G)(N \cap C_G(F(G)))$, y como $N \leq F(G)C_G(F(G))$, entonces $N = F(G)(N \cap C_G(F(G)))$.

Sea $M = N \cap C_G(F(G))$. Sea $x \in F(G)$ y $y \in N$, y es de la forma $y = zt$ con $z \in F(G)$ y $t \in M$, entonces $[x,y] = x^{-1}y^{-1}xy = x^{-1}t^{-1}z^{-1}xzt$, pero como $t \in M \leq C_G(F(G))$, entonces t conmuta con x y z, así que $[x,y] = x^{-1}z^{-1}xz = [x,z]$. Por lo tanto, para todo S subgrupo de $F(G)$ se tiene que $[S,N] \leq [S,F(G)]$, ya que todo generador de $[S,N]$ es un generador de $[S,F(G)]$. Como $F(G)$ es nilpotente ya que el producto de subgrupos normales nilpotentes es nilpotente, por el Teorema 7 su serie central descendente llega al $\langle 1 \rangle$, entonces existe un entero m tal que $F(G)_m = \langle 1 \rangle$. Como $N_2 = N' \leq F(G)$, entonces por inducción se tiene que $N_{k+1} \leq F(G)_k$ ya que $N_{k+1} = [N_k, N] \leq [F(G)_{k-1}, F(G)] = F(G)_k$, usando la hipótesis de inducción $N_k \leq F(G)_{k-1}$, por esto tenemos que $N_{m+1} \leq F(G)_m = \langle 1 \rangle$, y por lo tanto N es nilpotente, y al ser normal en G, $N \leq F(G)$, por lo cual $\frac{N}{F(G)}$ es trivial, contradiciendo su minimalidad. ■

Teorema 12. Sea $n, q \in \mathbb{N}$ con q una potencia de un primo, n distinto de 2 ó q distinto de 2. El subgrupo derivado de $GL(n,q)$ es $SL(n,q)$.

Cuando $q, n = 2$, $GL(2,2)$ es un grupo no abeliano de orden 6, por lo tanto es isomorfo a S_3, del cual se sabe que su derivado es A_3, un subgrupo propio de S_3, pero los elementos de $GL(2,2)$ son matrices de determinante 1, por lo cual $GL(2,2) = SL(2,2)$, siendo esta la razón por la que la hipótesis del Teorema 12 excluye este caso.

1.3 Teoremas sobre solubilidad.

Teorema S1. Todo grupo G abeliano es soluble.

Demostración:
Como G es abeliano, $[x,y] = x^{-1}y^{-1}xy = 1$ para todo x y y en G, entonces el derivado de G es trivial, por lo cual la serie derivada de G es $\langle 1 \rangle \leq G$, por lo tanto G es soluble. ■

Teorema S2. Un grupo G simple soluble es de orden un número primo.

Demostración:
Como G es soluble, G' no puede ser G, por el Teorema 10 es un subgrupo normal propio, pero al ser G simple no posee subgrupos normales propios no triviales, por lo tanto $G' = \langle 1 \rangle$, es decir, G es

abeliano, pero un grupo simple y abeliano no tiene subgrupos propios no triviales, y todo grupo no trivial sin subgrupos propios no triviales es finito y de orden primo. ■

Teorema S3. Sea G un grupo. Las siguientes condiciones son equivalentes.

a) G es soluble.

b) G tiene una serie normal en el que todo cociente sucesivo es abeliano.

c) G tiene una se serie subnormal en el que todo cociente sucesivo es abeliano.

Demostración:
Como H' es característico en H para todo grupo H, tenemos que $G^{(k)}$ es normal en G para toda k, entonces la serie derivada de G es una serie normal de G, y por el Teorema 10 cada cociente sucesivo de la serie derivada es abeliano.
Si G tiene una serie normal, entonces esta serie es una serie subnormal.
Supongamos que G tiene una serie subnormal, $G = G_0 \geq G_1 \geq \ldots \geq G_r = \langle 1 \rangle$, donde cada cociente sucesivo es abeliano. Veamos por inducción que $G^{(i)} \leq G_i$.

Como $\frac{G}{G_1}$ es abeliano, por el Teorema 10 tenemos que $G^{(1)} = G' \leq G_1$.

Supongamos que $G^{(i-1)} \leq G_{i-1}$. Entonces $G^{(i)} = G^{(i-1)\prime} \leq (G_{i-1})'$, y como $\frac{G_{i-1}}{G_i}$ es abeliano, entonces $(G_{i-1})' \leq G_i$, por lo cual $G^{(i)} \leq G_i$.
Entonces tenemos que $G^{(r)} \leq G_r = \langle 1 \rangle$, por lo cual la serie derivada de G termina en la identidad, es decir, G es soluble. ■

Teorema S4. Sea G un grupo soluble. Si H es un subgrupo de G, entonces H es soluble, además, si H es normal en G, entonces $\frac{G}{H}$ también es soluble.

Demostración:
Como H es subgrupo de G, tenemos que $H^{(k)} \leq G^{(k)}$ por inducción, ya que si tenemos que $H^{(k)} \leq G^{(k)}$, los generadores del derivado de $H^{(k)}$ son generadores del derivado de $G^{(k)}$, entonces $H^{(k+1)} \leq G^{(k+1)}$, esto quiere decir que la serie derivada de H termina en la identidad ya que eso ocurre con la serie derivada de G.
Si H es normal en G, consideremos una serie normal de G, $G = G_0 \geq G_1 \geq \ldots \geq G_r = \langle 1 \rangle$, la cual existe por el Teorema S3 y además $\frac{G_i}{G_{i+1}}$ es abeliano para toda i. Consideremos la serie $\frac{G}{H} = \frac{G_0 H}{H} \geq \frac{G_1 H}{H} \geq \ldots \geq \frac{G_r H}{H} = \langle 1 \rangle$. Como $G_i \trianglelefteq G$ y $H \trianglelefteq G$, entonces $G_i H \trianglelefteq G$, por lo cual $\frac{G_i H}{H} \trianglelefteq \frac{G}{H}$, es decir, la serie es normal. Como $G_i H = G_i(G_{i+1}H)$ se tiene que $\left(\frac{G_i H}{H}\right)/\left(\frac{G_{i+1}H}{H}\right) \cong \frac{G_i H}{G_{i+1}H}$ por el segundo Teorema de Isomorfismo, y $\frac{G_i H}{G_{i+1}H} = \frac{G_i(G_{i+1}H)}{G_{i+1}H} \cong \frac{G_i}{G_i \cap (G_{i+1}H)}$ por el primer Teorema de Isomorfismo. Entonces, como $G_{i+1} \leq G_i \cap (G_{i+1}H)$, por el segundo Teorema de Isomorfismo tenemos que $\frac{G_i}{G_i \cap (G_{i+1}H)} \cong \left(\frac{G_i}{G_{i+1}}\right)/\left(\frac{G_i \cap (G_{i+1}H)}{G_{i+1}}\right)$, pero este último es un cociente de $\frac{G_i}{G_{i+1}}$, el cual es abeliano, entonces el cociente es abeliano, eso quiere decir que cada cociente sucesivo de la serie de $\frac{G}{H}$ es abeliano, entonces por el Teorema S3, $\frac{G}{H}$ es soluble. ■

Teorema S5. Sea G un grupo que tiene un subgrupo normal N tal que N y $\frac{G}{N}$ son solubles, entonces G es soluble.

Demostración:
Siendo N y $\frac{G}{N}$ solubles tienen una serie subnormal por el Teorema S3, $N = N_0 \geq N_1 \geq \ldots \geq N_r = \langle 1 \rangle$ y $\frac{G}{N} = \frac{G_0}{N} \geq \frac{G_1}{N} \geq \ldots \geq \frac{G_s}{N} = \langle 1 \rangle$, y por el segundo Teorema de Isomorfismo tenemos que $\left(\frac{G_i}{N}\right)/\left(\frac{G_{i+1}}{N}\right) \cong \frac{G_i}{G_{i+1}}$, asi que los cocientes sucesivos de la serie $G = G_0 \geq G_1 \geq \ldots \geq G_s$ son abelianos, y por el Teorema de la correspondencia $G_{i+1} \trianglelefteq G_i$, entonces la serie

$G = G_0 \geq G_1 \geq \ldots \geq G_s = N = N_0 \geq N_1 \geq \ldots \geq N_r = \langle 1 \rangle$ es una serie subnormal de G y por el Teorema S3 G es soluble. ■

Teorema S6. Sean G y H grupos solubles. $G \times H$ es soluble.

Demostración:
El subgrupo $\{1\} \times H$ es un subgrupo normal de $G \times H$, y como $\{1\} \times H \cong H$, entonces $\{1\} \times H$ es soluble, además $\frac{G\times H}{\{1\}\times H} \cong G$, por lo cual también es soluble, entonces por el Teorema S5 $G \times H$ es soluble. ■

Teorema S7. Sea G un grupo que tiene una serie de composición. G es soluble si y sólo si todos los cocientes sucesivos de la serie tienen orden primo.

Demostración:
Si G es soluble, consideremos un cociente de la serie de composición, $\frac{H}{K}$, donde $K \trianglelefteq H \leq G$, entonces por el Teorema S4, tanto K como H son solubles y $\frac{H}{K}$ también, entonces, siendo $\frac{H}{K}$ un cociente de una serie de composición, es un grupo simple soluble, y por ende es de orden primo.
Si cada cociente de la serie de composición de G tiene orden primo, entonces cada cociente de la serie es un grupo abeliano, entonces la serie de composición es una serie subnormal con cocientes abelianos, así que por el Teorema S3 G es soluble. ■

Teorema S8. Todo p-grupo finito es soluble.

Demostración:
Sea G un p-grupo finito, al ser finito tiene una serie de composición, pero cada cociente de la serie, al ser simple, es de orden p, entonces por el Teorema S7 G es soluble. ■

Teorema S9. Un grupo finito G no es soluble si y sólo si existen elementos no triviales a, b, c de G de orden x, y y z respectivamente tales que $(x,y) = (x,z) = (y,z) = 1$ y $xy = z$.

Teorema S10. Sea G un grupo soluble de orden mn con m y n primos relativos. Entonces G tiene un subgrupo de orden m.

Teorema S11. Sea G un grupo finito. Si para cualquier divisor m del orden de G tal que $\left(m, \frac{|G|}{m}\right) = 1$ se tiene que existe un subgrupo de G de orden m, entonces G es soluble.

El Teorema S11 es un resultado obtenido por P. Hall el cual generaliza el p-q Teorema de Burnside, sin embargo la demostración de este teorema se basa en él.

Capítulo 2.
Teorema p-q de Burnside.

En todos los resultados que se verán a continuación, los grupos se considerarán de orden finito.

2.1 Algunos lemas necesarios para la demostración del p-q Teorema de Burnside.

Lema 1. Sea V un p-grupo abeliano y A un q-grupo abeliano elemental regular de automorfismos de V (p, q primos distintos, V y A distintos de la identidad). Entonces $|A| = q$.

Demostración:
Siendo A un q-grupo su orden es q^m con $m \geq 1$, supongamos entonces que $|A| \gneqq q$, es decir que $m \gneqq 1$.

Siendo A abeliano elemental, existe B subgrupo de A con $|B| = q^2$ y además existen $B_1, B_2, \ldots, B_{q+1}$ con $|B_i| = q$, $B_i \cap B_j = \langle 1 \rangle$ y $B = \bigcup_{i=1}^{q+1} B_i$ (donde $B_i = \langle b_i \rangle$ con $b_i \neq 1$ y $b_i \notin B_j$ con $j \lneqq i$).
Sea $b' \in B$ con $b' \neq I$, $v \in V$ con $v \neq 1$, entonces

$$b'\left(\prod_{b\in B} b(v)\right) = \prod_{b\in B} b'(b(v)) = \prod_{b\in B}[b' \circ b](v) = \prod_{b\in B} b(v)$$

ya que al variar b entre los elementos de B, $b' \circ b$ varia entre todos los elementos de B, y siendo V abeliano el orden de los factores no es relevante.
Entonces b' deja fijo a $\prod_{b\in B} b(v)$, y como $b' \neq I$ entonces $\prod_{b\in B} b(v) = 1$, ya que al ser A regular B también lo es, y al ser $b' \neq I$, b' solo fija a la identidad de V.
De forma análoga podemos ver que para toda $i = 1, 2, \ldots, q+1$ se tiene que $\prod_{b_i\in B_i} b_i(v) = 1$. Entonces

$$1 = \prod_{i=1}^{q+1} 1 = \prod_{i=1}^{q+1}\left(\prod_{b_i\in B_i} b_i(v)\right) = \prod_{i=1}^{q+1}\left(I(v)\prod_{\substack{b_i\in B_i\\ b_i\neq I}} b_i(v)\right) = \prod_{i=1}^{q+1}\left(v\prod_{\substack{b_i\in B_i\\ b_i\neq I}} b_i(v)\right) =$$

$$= v^q I(v)\prod_{i=1}^{q+1}\left(\prod_{\substack{b_i\in B_i\\ b_i\neq I}} b_i(v)\right) = v^q \prod_{b\in B} b(v) = v^q 1 = v^q$$

Esto es una contradicción, ya que todo elemento de V distinto de la identidad es de orden una potencia de p y $q \neq p$.Por lo tanto, $|A| = q$. ■

Lema 2. Sea G un grupo tal que $G = VB$ donde B es un p-subgrupo normal y V un q-subgrupo abeliano elemental (p, q primos distintos). Entonces B es generado por los centralizadores en B de los subgrupos U de índice q en V.

Demostración:
Sea $A = \langle C_B(U) | U \leq V y [V:U] = q\rangle$. Entonces $A \leq B$.
Supongamos que G es un contraejemplo de orden mínimo, entonces $A \lneqq B$.

Si $x \in V$ y U es subgrupo de V con $[V{:}U] = q$, entonces se probará que $x^{-1}C_B(U)x = C_B(x^{-1}Ux)$:

Sea $x^{-1}bx \in x^{-1}C_B(U)x$, donde $b \in C_B(U)$, y sea $x^{-1}ux \in x^{-1}Ux$. con $u \in U$, entonces $(x^{-1}bx)x^{-1}ux(x^{-1}bx)^{-1} = x^{-1}b(xx^{-1})u(xx^{-1})b^{-1}x = x^{-1}(bub^{-1})x = x^{-1}ux$ ya que $b \in C_B(U)$, entonces $x^{-1}bx \in C_B(x^{-1}Ux)$, es decir, $x^{-1}C_B(U)x \leq C_B(x^{-1}Ux)$.

Sea $b \in C_B(x^{-1}Ux)$, como B es normal se tiene que $xbx^{-1} \in B$, ahora sea $u \in U$, entonces $(xbx^{-1})u(xbx^{-1})^{-1} = xb(x^{-1}ux)b^{-1}x^{-1} = xx^{-1}uxx^{-1} = u$ ya que $b \in C_B(x^{-1}Ux)$, esto quiere decir $xbx^{-1} \in C_B(U)$, entonces $b = x^{-1}(xbx^{-1})x \in x^{-1}C_B(U)x$, así que $x^{-1}C_B(U)x = C_B(x^{-1}Ux)$.

Veamos que $x^{-1}Ax = A$:

Sea $a \in A$, entonces $a = b_1b_2 \ldots b_n$ donde $b_i \in C_B(U_i)$ con $U_i \leq V$ y $[V{:}U_i] = q$, entonces $x^{-1}ax = x^{-1}(b_1b_2 \ldots b_n)x = (x^{-1}b_1x)(x^{-1}b_2x) \ldots (x^{-1}b_nx)$ y como $x^{-1}U_ix$ es subgrupo de V de índice q y $x^{-1}C_B(U)x = C_B(x^{-1}Ux)$, entonces $x^{-1}ax$ es producto de elementos de centralizadores en B de subgrupos de V de ídice q, así que $x^{-1}ax \in A$.

De lo anterior se concluye que $V \leq N_G(A)$, veamos ahora que $V \leq N_G(N_B(A))$:

Sea $v \in V$ y $b \in N_B(A)$, $v^{-1}bv \in B$ ya que B es normal, sea $a \in A$, entonces $(v^{-1}bv)^{-1}a(v^{-1}bv) = (v^{-1}b^{-1}v)a(v^{-1}bv) = v^{-1}b^{-1}(vav^{-1})bv = v^{-1}(b^{-1}a'b)v = v^{-1}a''v = a'''$, ya que $v \in N_G(A)$ y $b \in N_B(A)$, entonces $v^{-1}bv \in N_B(A)$ y por ello $v \in N_G(N_B(A))$, por lo tanto $V \leq N_G(N_B(A))$.

Como $V \leq N_G(N_B(A))$, entonces $N_B(A) \trianglelefteq VN_B(A)$, además como $N_B(A) \leq B$, al ser B p-subgrupo, $N_B(A)$ es p-subgrupo, entonces $VN_B(A)$ cumple las hipótesis del lema, y al ser B nilpotente y A un subgrupo de él, $A \lneqq N_B(A)$, y como $A^* = \langle C_{N_B(A)}(U) | U \leq V y [V{:}U] = q \rangle$ es subgrupo de A ya que $C_{N_B(A)}(U) \leq C_B(U)$, entonces $VN_B(A)$ es contraejemplo del lema. Como $VN_B(A) \leq G = VB$ y VB es producto directo ya que V es q-grupo y B es p-grupo, se sigue que $B = N_B(A)$, es decir, A es normal en B. $\frac{B}{A}$ es abeliano, pues de no serlo su centro $\frac{N}{A} = Z\left(\frac{B}{A}\right)$ es característico en $\frac{B}{A}$ y por lo tanto normal en $\frac{G}{A}$, y es no trivial pues $\frac{B}{A}$ es un p-grupo, entonces N cumple que $A \lneqq N \lneqq B$ y $N \trianglelefteq G$, pero VN sería contraejemplo de menor orden que G.

Como $V \leq N_G(A)$ y $B = N_B(A)$, entonces $G = N_G(A)$, por lo tanto $A \trianglelefteq G$. Si nombramos $\overline{V} = \frac{VA}{A}$, vemos que $\frac{G}{A}$ cumple las hipótesis del lema ya que $\overline{V}$ es un q-subgrupo abeliano elemental y $\frac{B}{A}$ es normal en $\frac{G}{A}$. Si suponemos que $A \neq \langle 1 \rangle$, por la minimalidad de G tenemos que

$$\frac{B}{A} = \left\langle C_{\frac{B}{A}}(\overline{U}) | [\overline{V}{:}\overline{U}] = q \right\rangle,$$

así que existe $\overline{U} \leq \overline{V}$ con $[\overline{V}{:}\overline{U}] = q$ y $C_{\frac{B}{A}}(\overline{U}) \neq \langle 1 \rangle$, y $\overline{U} = \frac{UA}{A}$ para alguna $U \leq V$ la cual cumple $[V{:}U] = q$. Los elementos de U inducen un subgrupo de $Aut\left(\frac{B}{A}\right)$, así que $C_{\frac{B}{A}}(U) \neq \langle 1 \rangle$, entonces $C_B(U) \nleq A$, una contradicción, entonces se tiene que $A = \langle 1 \rangle$. Como $\frac{B}{A}$ es abeliano, entonces B es abeliano.

Sea $d \in B$, $d \neq 1$ tal que $C_V(d)$ tiene orden máximo. Si $v \in V$ y $u \in C_V(d)$, entonces $u^{-1}(v^{-1}dv)u = v^{-1}(u^{-1}du)v = v^{-1}dv$ ya que V es abeliano, así que $u \in C_V(v^{-1}dv)$ y $C_V(d) \leq C_V(v^{-1}dv)$. Sea H el subgrupo generado por los conjugados de d en G, veamos que $C_V(H) = C_V(d)$:

Como $d \in H$, claramente $C_V(H) \leq C_V(d)$.

Sea $v \in C_V(d)$ y $h \in H$, $h = \prod b_i^{-1}a_i^{-1}da_ib_i$ con $a_i \in V$ y $b_i \in B$, entonces $v^{-1}hv = v^{-1}\left(\prod b_i^{-1}a_i^{-1}da_ib_i\right)v = \prod v^{-1}b_i^{-1}(a_i^{-1}da_i)b_iv = \prod v^{-1}(a_i^{-1}da_i)(b_i^{-1}b_i)v =$

$\prod v^{-1}(a_i^{-1}da_i)v = \prod a_i^{-1}da_i = \prod(a_i^{-1}da_i)(b_i^{-1}b_i) = \prod b_i^{-1}(a_i^{-1}da_i)b_i = h$,
ya que $B \trianglelefteq G$, $a_i^{-1}da_i \in B$ y B es abeliano. Entonces $C_V(d) \leq C_V(H)$.

Además, para toda $h \in H$, $C_V(d) \subset C_V(h)$, y por la maximalidad de $C_V(d)$, tenemos que $C_V(d) = C_V(h)$.

Sea $W = C_V(H)$ y veamos que $\frac{V}{W}$ induce un grupo regular de automorfismos M de H.
Sea $M = \{\varphi_{vW} : H \to H \mid \varphi_{vW}(h) = vhv^{-1},\ vW \in \frac{V}{W}\}$.
Sean $v_1W, v_2W \in \frac{V}{W}$ con $v_1W = v_2W$, entonces $v_2^{-1}v_1 \in W$, por lo cual $v_1^{-1}v_2hv_2^{-1}v_1 = h$, entonces $v_1hv_1^{-1} = v_2hv_2^{-1}$, es decir $\varphi_{v_1W}(h) = \varphi_{v_2W}(h)$, por lo tanto estan bien definidas los elementos de M.
Como los elementos de M son funciones que consisten en conjugar, son claramente automorfismos.
Sea $\varphi_{vW} \in M$ y $h \in H$ con $h \neq 1$ tal que $\varphi_{vW}(h) = h$, entonces $vhv^{-1} = h$, por lo cual $v \in W$, entonces el único elemento de M que fija a los elementos de H es la identidad, por lo tanto M es regular.

Como M es isomorfo a $\frac{V}{W}$ y V es abeliano elemental, entonces M también es abeliano elemental, y al ser H subgrupo de B, H es un p-grupo abeliano, por lo tanto se cumplen las hipótesis del Lema 1, entonces $\left|\frac{V}{W}\right| = |M| = q$. Entonces $C_B(W) \leq A$. $W = C_V(d)$, por ello d conmuta con todo elemento de W, entonces $d \in C_B(W) \leq A$ y como $d \neq 1$, entonces $A \neq \langle 1 \rangle$, una contradicción. Entonces $A = B$, es decir, $B = \langle C_B(U) | U \leq V y [V{:}U] = q \rangle$. ■

Lema 3 (**Teorema de Baer-Suzuki**). Sea G un grupo finito, p un primo y K una clase de conjugación de G. Si para todo $x, y \in K$, $\langle x,y \rangle$ es un p-grupo, entonces $K \subseteq O_p(G)$.

Demostración:
Supongamos que $K \not\subseteq O_p(G)$.
Como K es una clase de conjugación, $\langle K \rangle$ es normal en G, por lo cual $\langle K \rangle$ no es un p-grupo, ya que de serlo $K \subseteq \langle K \rangle \leq O_p(G)$, lo cual contradice nuestra suposición. Tampoco K es un p-grupo por la misma razón.
Sea P un p-subgrupo de Sylow de G, como K no es un p-grupo entonces $K \not\subseteq P$. Sea $x \in K$ con $x \notin P$, como $\langle x,y \rangle$ es un p-grupo para todo $y \in K$, en particular $\langle x \rangle = \langle x,x \rangle$ es un p-grupo, por lo tanto x es un p-elemento. Sea Q un p-subgrupo de Sylow que contenga a x, entonces, como $x \in K \cap Q$ y $x \notin K \cap P$, se sigue que $K \cap Q \neq K \cap P$.

Sean P y Q p-subgrupos de Sylow tales que $K \cap Q \neq K \cap P$ y $K \cap P \cap Q$ sea de orden máximo. Por el teorema de Sylow existe $z \in G$ tal que $z^{-1}Pz = Q$, así que $z^{-1}(K \cap P)z = (z^{-1}Kz) \cap (z^{-1}Pz) = K \cap Q$, entonces $|K \cap P| = |z^{-1}(K \cap P)z| = |K \cap Q|$. Si $K \cap P \subseteq Q$, se tendría que $K \cap P \subseteq K \cap Q$, lo cual implicaría que $K \cap P = K \cap Q$, por lo cual $K \cap P \not\subseteq Q$ y análogamente $K \cap Q \not\subseteq P$.

Sea $D = \langle K \cap P \cap Q \rangle$. Como $D \leq P$, un subgrupo maximal de P que contenga a D es un subgrupo maximal de P y sería de índice p, de esta forma podemos construir una cadena de subgrupos $D = P_0 \leq P_1 \leq \ldots \leq P_n = P$ tales que $[P_i : P_{i-1}] = p$. Como $D \subseteq Q$ y $K \cap P \not\subseteq Q$, entonces $K \cap P \not\subseteq D$, además como $K \cap P_0 = K \cap D \subseteq D$, entonces existe una i tal que $K \cap P_{i-1} \subseteq D$ y $K \cap P_i \not\subseteq D$. Entonces existe $x \in K \cap P_i$ tal que $x \notin D$.

Como P_{i-1} es de índice p en P_i, entonces es normal, y como $x \in K \cap P_i \subseteq P_i$, entonces $x^{-1}P_{i-1}x = P_{i-1}$. Como $D \leq P_{i-1}$, se tiene que $K \cap P_{i-1} \subseteq K \cap D \subseteq K \cap P_{i-1}$, es decir,

$K \cap P_{i-1} = K \cap D$, y por lo tanto $x^{-1}(K \cap D)x = x^{-1}(K \cap P_{i-1})x = (x^{-1}Kx) \cap (x^{-1}P_{i-1}x) = K \cap P_{i-1} = K \cap D$, entonces $x^{-1}\langle K \cap D\rangle x = \langle K \cap D\rangle$. Pero $K \cap P \cap Q = K \cap (K \cap P \cap Q) \subseteq K \cap \langle K \cap P \cap Q\rangle = K \cap D$, entonces $D = \langle K \cap P \cap Q\rangle \leq \langle K \cap D\rangle$, y además como $K \cap D \subseteq D$, se tiene que $\langle K \cap D\rangle \leq D$, por lo tanto $D = \langle K \cap D\rangle$, entonces $x^{-1}Dx = x^{-1}\langle K \cap D\rangle x = \langle K \cap D\rangle = D$, por lo cual x cumple que $x \in K \cap P$, $x \notin D$ y $x \in N(D)$. Análogamente existe y que cumple que $y \in K \cap Q$, $y \notin D$ y $y \in N(D)$.

Como x y y están en K, entonces $\langle x,y\rangle$ es un p-grupo y dado que sus generadores están en $N(D)$, entonces $\langle x,y\rangle \leq N(D)$, y al ser subgrupo del normalizador se tiene que $\langle x,y\rangle D$ es un subgrupo de G y D es normal en $\langle x,y\rangle D$, y siendo D y $\langle x,y\rangle$ p-grupos, entonces $\langle x,y\rangle D$ es un p-grupo también. Sea R un p-subgrupo de Sylow de G que contenga a $\langle x,y\rangle D$. Como $D \leq P \cap R$, entonces $K \cap D \subseteq K \cap P \cap R$, pero $x \in K \cap P$, y como $x \in R$, entonces $x \in K \cap P \cap R$, y como $x \notin D$, $x \notin K \cap D$, se sigue que $K \cap P \cap Q \subseteq K \cap D \subsetneq K \cap P \cap R$, entonces $|K \cap P \cap Q| \leq |K \cap P \cap R|$. Análogamente $|K \cap P \cap Q| \leq |K \cap Q \cap R|$. Por la maximalidad de $|K \cap P \cap Q|$, dado que R es un p-subgrupo de Sylow, se tiene por un lado que $K \cap R = K \cap P$ y por el otro que $K \cap R = K \cap Q$, pero esto implica que $K \cap P = K \cap Q$, lo cual contradice nuestra suposición en P y en Q. Entonces $K \subseteq O_p(G)$. ■

Lema 4. Sea G un grupo finito de orden par, y x un elemento de G de orden 2. Si $x \notin O_2(G)$, entonces existe un elemento y distinto de la identidad de orden impar tal que $xyx = y^{-1}$.

Demostración:
Supongamos que para todo $z \in G$ el orden de $zxz^{-1}x$ es de orden una potencia de 2. Entonces $\langle x, zxz^{-1}x\rangle = \langle x\rangle\langle zxz^{-1}x\rangle$ es un 2-grupo. Como claramente $zxz^{-1}x \in \langle x, zxz^{-1}\rangle$ y $zxz^{-1} \in \langle x, zxz^{-1}x\rangle$, entonces $\langle x, zxz^{-1}x\rangle = \langle x, zxz^{-1}\rangle$, así que para todo elemento x_1 en la clase conjugada de x se tiene que $\langle x, x_1\rangle$ es un 2-grupo.

Para todo x_2 y x_3 en la clase de conjugación de x, la función $f : \langle x, x_1\rangle \to \langle x_2, x_3\rangle$ que cumple con $f(x) = x_2$ y $f(x_1) = x_3$ es un isomorfismo por lo tanto $\langle x_2, x_3\rangle$ es un 2-grupo también, así que por el Lema 3 se sigue que la clase conjugada de x es un subconjunto de $O_2(G)$, en particular $x \in O_2(G)$, lo cual es una contradicción. Entonces existe $z \in G$ tal que el orden de $zxz^{-1}x$ no es una potencia de 2, entonces su orden es de la forma $2^k m$ con $k \geq 0$ y 2 no divide a m, sea $y = (zxz^{-1}x)^{2^k}$, el orden de y es m, es decir, y es de orden impar. Como se cumple que $x(zxz^{-1}x)x = xzxz^{-1}(xx) = (zxz^{-1}x)^{-1}$, entonces $xyx = x\left((zxz^{-1}x)^{2^k}\right)x = (x(zxz^{-1}x)x)^{2^k} = ((zxz^{-1}x)^{-1})^{2^k} = ((zxz^{-1}x)^{2^k})^{-1} = y^{-1}$. ■

Lema 5. Sea $G = BQ$ con B un p-subgrupo normal y Q un q-subgrupo, p y q primos distintos, y A un subgrupo normal de B. Si $[Q,B] \leq A$, entonces $B = AC_B(Q)$.

Demostración:
Como $[Q,B] \leq A$, entonces para todo $a \in A$ y $q \in Q$ se tiene que $q^{-1}aqa^{-1} = a'$ con $a' \in A$, pero entonces se tiene que $q^{-1}aq = a'a \in A$, por lo tanto Q normaliza a A, entonces AQ es un subgrupo de G, además, sea $aq \in AQ$ y $bq_1 \in BQ$, entonces $(bq_1)^{-1}aq(bq_1) = q_1^{-1}(b^{-1}ab)(b^{-1}qbq^{-1})qq_1 = q_1^{-1}a_1[b,q^{-1}]qq_1 = q_1^{-1}a_1a_2qq_1 \in AQ$, ya que A es normal en B y $[Q,B] \leq A$, por lo tanto AQ es normal en G.

Como $|AQ| = |A||Q|$ por que $A \cap Q = \langle 1\rangle$, entonces Q es un q-subgrupo de Sylow de AQ, y por el argumento de Frattini se tiene que $G = AN_G(Q)$, entonces $B = AN_B(Q)$, ya que si $b \in B$, entonces al ser b elemento de G se tiene que $b = ag \in AN_G(Q)$, pero entonces $g = a^{-1}b \in B$, por lo tanto $g \in N_B(Q)$, entonces $b \in AN_B(Q)$. Sea $x \in Q$ y $y \in N_B(Q)$, tenemos que $[x,y] = x^{-1}y^{-1}xy =$

$x^{-1}q \in Q$, ya que y normaliza a Q, y además tenemos que $[x,y] = x^{-1}y^{-1}xy = by \in B$, ya que B es normal en G, y siendo que $B \cap Q = \langle 1 \rangle$, se tiene que $[x,y] = 1$, entonces se tiene que $y \in C_B(Q)$, es decir, $N_B(Q) = C_B(Q)$. Entonces $B = AC_B(Q)$. ■

Lema 6. Sea A el grupo de automorfismos de un grupo abeliano elemental de orden p^2 y sea q un divisor de $|A|$, p y q primos impares distintos. Entonces todos los q-subgrupos del derivado de A son cíclicos.

Demostración:
A es isomorfo a $GL(2,p)$ y como p es impar, entonces por el Teorema 12 el derivado de $GL(2,p)$ es $SL(2,p)$. Como $GF(p)$ es el campo primo de $GF(p^2)$, podemos verlo como un subcampo, y así considerar a $SL(2,p)$ como subgrupo de $SL(2,p^2)$. Como el grupo multiplicativo de $GF(p^2)$ es de orden $p^2 - 1$, entonces existe un elemento $b \in GF(p^2)$ de orden $p^2 - 1$, entonces la matriz

$$\begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}$$

tiene determinante 1, por lo tanto es un elemento de $SL(2,p^2)$ y genera un subgrupo cíclico C de orden $p^2 - 1$. Tenemos que q es un primo impar distinto a p y q divide al orden de $GL(2,p)$ que es $(p^2 - 1)(p - 1)p$, lo que implica que q divide a $p^2 - 1 = (p - 1)(p + 1)$, ya que q no divide a p, y por ello no divide a $p^2 + 1$ ya que q no es par

El orden de $SL(2,p^2)$ es $p^2(p^4 - 1) = p^2(p^2 + 1)(p^2 - 1)$, y como q no divide a $p^2(p^2 + 1)$, entonces un q-subgrupo de Sylow de C es q-subgrupo de Sylow de $SL(2,p^2)$, pero un subgrupo de C es cíclico ya que C es cíclico, y al ser todos los q-subgrupos de Sylow conjugados, entonces todo q-subgrupo de Sylow de $SL(2,p^2)$ es cíclico. Como $SL(2,p) \leq SL(2,p^2)$, todo q-subgrupo de $SL(2,p)$ está contenido en algún q-subgrupo de Sylow de $SL(2,p^2)$, por lo tanto es cíclico. ■

Lema 7. Sea p, q primos impares distintos y X un grupo finito tal que $[X : O_{p,q}(X)] = p$. Sea Z el soclo de $O_p(X)$, y supongamos que $\frac{X}{C_X(Z)}$ no tiene p-subgrupos de Sylow normales. Entonces, si P es un p-subgrupo de Sylow de X, $J(P)$ es normal en X.

Como observación, el soclo de un grupo es característico en este, y siendo $O_p(X)$ normal en X, tenemos que Z es normal en X, por ello tiene sentido hablar de $\frac{X}{C_X(Z)}$.

Demostración:
Supongamos que $J(P) \leq O_p(X)$. Si tomamos un subgrupo abeliano elemental de orden máximo de P, éste está contenido en $O_p(X)$, y al ser $O_p(X)$ un p-subgrupo normal de X está contenido en todo p-subgrupo de Sylow, por ello es también subgrupo abeliano elemental de orden máximo en $O_p(X)$, por lo tanto $J(P) \leq J(O_p(X))$, y un subgrupo abeliano elemental de orden máximo de $O_p(X)$ está contenido en P, y como un subgrupo abeliano elemental de orden máximo de P está en $O_p(X)$, entonces también es subgrupo abeliano elemental de orden máximo de P, entonces $J(P) = J(O_p(X))$.

Como $J(O_p(X))$ es característico en $O_p(X)$ ya que la imagen de todo subgrupo abeliano elemental de orden máximo bajo todo automorfismo es otro abeliano elemental de orden máximo, entonces $J(P)$ también lo es, y por lo tanto normal en X.

Supongamos ahora que $J(P) \nleq O_p(X)$. Entonces debe existir un subgrupo abeliano elemental de orden máximo A de P tal que $A \nleq O_p(X)$. Sea $A_0 = A \cap O_p(X)$. Entonces

$$[A : A_0] = \frac{|A|}{|A \cap O_p(X)|} = \frac{|A||O_p(X)|}{|O_p(X)||A \cap O_p(X)|} = \frac{|AO_p(X)|}{|O_p(X)|} = [AO_p(X) : O_p(X)].$$

Como $AO_p(X) \leq P$, entonces

$$[A : A_0] = [AO_p(X) : O_p(X)] = \frac{|AO_p(X)|}{|O_p(X)|} \leq \frac{|P|}{|O_p(X)|} = [P : O_p(X)],$$

además, como $P \cap O_{p,q}(X) = O_p(X)$ ya que $O_p(X)$ es el p-subgrupo de Sylow de $O_{p,q}(X)$, entonces

$$[P : O_p(X)] = \frac{|P|}{|O_p(X)|} = \frac{|P||O_{p,q}(X)|}{|P \cap O_{p,q}(X)||O_{p,q}(X)|} = \frac{|PO_{p,q}(X)|}{|O_{p,q}(X)|} \leq \frac{|X|}{|O_{p,q}(X)|} = [X : O_{p,q}(X)] = p.$$

Y como $A \nleq O_p(X)$, entonces $A \neq A_0$, por lo cual $[A : A_0] > 1$, entonces $[A : A_0] = p$.

Por el Teorema 3, $Z \leq \Omega_1(Z(O_p(X))) \leq Z(O_p(X))$, y al ser $A_0 \leq O_p(X)$, los elementos de Z y A_0 conmutan. Sea z un elemento distinto a la identidad de algún subgrupo normal minimal de $O_p(X)$, como $\langle z \rangle$ es un subgrupo normal de $O_p(X)$ ya que todo subgrupo normal minimal está contenido en el centro, entonces $\langle z \rangle$ es el subgrupo normal minimal, y como todo subgrupo de $\langle z \rangle$ sería normal en $O_p(X)$, se tiene que $\langle z \rangle$ es isomorfo a $\mathbb{Z}_p$, entonces Z es producto de subgrupos isomorfos a $\mathbb{Z}_p$, por lo cual es abeliano elemental, y como los elementos de Z y A_0 conmutan, entonces $A_0 Z$ es abeliano y el orden de todo elemento de $A_0 Z$ es p, por lo tanto es abeliano elemental. Como $A_0 Z \leq O_p(X) \leq P$, entonces $|A_0 Z| \leq |A|$ ya que A es un p-subgrupo abeliano elemental de orden máximo en P, entonces

$$[Z : Z \cap A] = [Z : (Z \cap O_p(X)) \cap A] = [Z : Z \cap A_0] = [ZA_0 : A_0] = \frac{|A_0 Z|}{|A_0|} \leq \frac{|A|}{|A_0|} = [A : A_0] = p.$$

Sea $a \in Z \cap A$, como A es abeliano, entonces a conmuta con todo elemento de A, y al estar en Z entonces $a \in C_Z(A)$, es decir, $Z \cap A \leq C_Z(A)$, por lo tanto

$$[Z : C_Z(A)] = \frac{|Z|}{|C_Z(A)|} \leq \frac{|Z|}{|Z \cap A|} = [Z : Z \cap A] \leq p.$$

Sea B el generado de los conjugados de A, sea $b \in B$ y $x \in X$, es de la forma $b = a_1 a_2 \ldots a_n$ con a_i en algún conjugado de A, entonces $x^{-1}bx = x^{-1}(a_1 a_2 \ldots a_n)x = (x^{-1}a_1 x)\ldots(x^{-1}a_n x) \in B$ ya que cada $(x^{-1}a_i x) \in x^{-1}Ax$, entonces B es normal en G. Si todo conjugado de A estuviera contenido en P, entonces $B \leq P$, y por ello B sería un p-grupo, pero entonces al ser un p-grupo normal de X, $A \leq B \leq O_p(X)$, lo cual contradice la suposición de que $A \nleq O_p(X)$, entonces existe algún conjugado de A que no está contenido en P.

Sea $\overline{A}$ un conjugado de A no contenido en P. De forma análoga a A se tiene que $[Z : Z \cap \overline{A}] \leq [\overline{A} : \overline{A_0}]$, donde $[\overline{A} : \overline{A_0}] = p$ si $\overline{A} \nleq O_p(X)$, o $[\overline{A} : \overline{A_0}] = 1$ de otra forma, por lo tanto $[Z : Z \cap \overline{A}] \leq p$, entonces $[Z : C_Z(\overline{A})] \leq [Z : Z \cap \overline{A}] \leq p$, y siendo Z abeliano, $C_Z(A)C_Z(\overline{A})$ es un subgrupo de Z ya que $C_Z(A)C_Z(\overline{A}) = C_Z(\overline{A})C_Z(A)$. Entonces

$$[Z : C_Z(A) \cap C_Z(\overline{A})] = \frac{|Z|}{|C_Z(A) \cap C_Z(\overline{A})|} = \frac{|Z||C_Z(A)||C_Z(\overline{A})|}{|C_Z(A) \cap C_Z(\overline{A})||C_Z(A)||C_Z(\overline{A})|} = \frac{|Z||C_Z(A)C_Z(\overline{A})|}{|C_Z(A)||C_Z(\overline{A})|} =$$
$$[Z : C_Z(A)][C_Z(A)C_Z(\overline{A}) : C_Z(\overline{A})] \leq p^2,$$

pues $[Z : C_Z(A)] \leq p$ y $[Z : C_Z(A)C_Z(\overline{A})][C_Z(A)C_Z(\overline{A}) : C_Z(\overline{A})] = [Z : C_Z(\overline{A})] \leq p$.

Veamos que $C_Z(A) \cap C_Z(\overline{A}) = C_Z(\langle A, \overline{A} \rangle)$.

Sea $z \in C_Z(A) \cap C_Z(\overline{A})$ y $a \in \langle A, \overline{A} \rangle$, entonces a es producto de elementos de A ó $\overline{A}$, entonces como z está en $C_Z(A) \cap C_Z(\overline{A})$, z conmuta con todo elemento de A y $\overline{A}$, entonces z conmuta con cada elemento que conforma a, por lo tanto con a misma, por lo tanto $z \in C_Z(\langle A, \overline{A} \rangle)$.

Sea $z \in C_Z(\langle A, \overline{A} \rangle)$, como z conmuta con todo elemento de $\langle A, \overline{A} \rangle$, en particular z

conmuta con todo elemento de A y con todo elemento de $\overline{A}$, por lo tanto $z \in C_Z(A)$ y $z \in C_Z(\overline{A})$, es decir, $z \in C_Z(A) \cap C_Z(\overline{A})$.

Como $C_Z(A) \cap C_Z(\overline{A}) = C_Z(\langle A, \overline{A} \rangle)$, entonces $[Z : C_Z(\langle A, \overline{A} \rangle)] = [Z : C_Z(A) \cap C_Z(\overline{A})] \leq p^2$.

Como $Z \leq Z(O_p(X))$, entonces todo elemento de $O_p(X)$ conmuta con todo elemento de Z, por lo cual $O_p(X) \leq C_X(Z)$. Como $O_p(X)$ es el p-subgrupo de Sylow de $O_{p,q}(X)$ entonces p no divide a $[O_{p,q}(X) : O_p(X)]$, por lo tanto $[X : O_p(X)] = [X : O_{p,q}(X)][O_{p,q}(X) : O_p(X)] = p[O_{p,q}(X) : O_p(X)]$, así que p^2 no divide a $[X : C_X(Z)]$. Como $\frac{X}{C_X(Z)}$ tiene al menos dos p-subgrupos de Sylow y el generado de dos p-subgrupos de Sylow distintos no puede ser un p-grupo, entonces el orden de $\frac{X}{C_X(Z)}$ es pq^s con $s \geq 1$. Sea $P_1 = \frac{PC_X(Z)}{C_X(Z)}$, entonces P_1 es un p-subgrupo de Sylow de $\frac{X}{C_X(Z)}$. Como $p = |P_1| = \left|\frac{PC_X(Z)}{C_X(Z)}\right| = \left|\frac{P}{P \cap C_X(Z)}\right|$ por los Teoremas de Isomorfismo, $P \cap C_X(Z)$ tiene índice p en P, además $O_p(X) \leq P \cap C_X(Z)$ ya que está contenido en P y en $C_X(Z)$, y $O_p(X)$ tiene índice p en P así que $O_p(X) = P \cap C_X(Z)$, y como $A \nleq O_p(X)$, entonces $A \nleq C_X(Z)$, así que $A \cap C_X(Z)$ es un subgrupo propio de A, entonces $\frac{|AC_X(Z)|}{|C_X(Z)|} = \frac{|A||C_X(Z)|}{|C_X(Z)||A \cap C_X(Z)|} = \frac{|A|}{|A \cap C_X(Z)|}$, lo cual es una potencia de p distinta de 1, y como $1 \lneqq \left|\frac{AC_X(Z)}{C_X(Z)}\right| \leq \left|\frac{PC_X(Z)}{C_X(Z)}\right| = p$, entonces $P_1 = \frac{AC_X(Z)}{C_X(Z)}$. Sea $\overline{P_1}$ un subgrupo de Sylow de $\frac{X}{C_X(Z)}$ distinto a P_1, entonces existe $xC_X(Z)$ tal que $x^{-1}C_X(Z)P_1xC_X(Z) = \overline{P_1}$, entonces

$$\overline{P_1} = x^{-1}C_X(Z)\left(\frac{AC_X(Z)}{C_X(Z)}\right)xC_X(Z) = \frac{x^{-1}AC_X(Z)x}{C_X(Z)} = \frac{x^{-1}Axx^{-1}C_X(Z)x}{C_X(Z)} = \frac{\overline{A}C_X(Z)}{C_X(Z)}$$

con $\overline{A}$ un conjugado de A, el cual no puede estar contenido en P, ya que de otra forma $\overline{P_1}$ estaría contenido en $\frac{PC_X(Z)}{C_X(Z)} = P_1$ y por lo tanto serían el mismo grupo de Sylow. Siendo P_1 y $\overline{P_1}$ dos p-subgrupos de Sylow de $\frac{X}{C_X(Z)}$, $\langle P_1, \overline{P_1} \rangle$ no puede ser un p-grupo ni puede ser abeliano, ya que si fuera abeliano entonces $\langle P_1, \overline{P_1} \rangle = P_1\overline{P_1}$ y entonces sería un p-grupo, y al ser subgrupo de $\frac{X}{C_X(Z)}$ el orden de $\langle P_1, \overline{P_1} \rangle$ es pq^t con $t \geq 1$, entonces si Q es un q-subgrupo de Sylow de $\langle P_1, \overline{P_1} \rangle$, $\langle P_1, \overline{P_1} \rangle = P_1 Q$ con $|Q| = q^t$

Sea K el grupo de automorfismos inducido por $\langle A, \overline{A} \rangle$ en Z, y sea $\varphi : \frac{\langle A, \overline{A} \rangle C_X(Z)}{C_X(Z)} \to K$ con $\varphi(aC_X(Z)) = \phi_a$, donde ϕ_a es la conjugación por a, veamos que φ es un isomorfismo.

Sean $aC_X(Z), bC_X(Z) \in \frac{\langle A, \overline{A} \rangle C_X(Z)}{C_X(Z)}$ con $aC_X(Z) = bC_X(Z)$, entonces $a^{-1}b \in C_X(Z)$, por lo cual $z(a^{-1}b) = (a^{-1}b)z$, entonces $aza^{-1} = bzb^{-1}$, entonces $\phi_a^{-1} = \phi_b^{-1}$, por lo cual $\phi_a = \phi_b$, así que φ está bien definida.
Sean $aC_X(Z), bC_X(Z) \in \frac{\langle A, \overline{A} \rangle C_X(Z)}{C_X(Z)}$, $z \in Z$, entonces $\phi_{ab}(z) = (b^{-1}a^{-1})z(ab) = b^{-1}(a^{-1}za)b = b^{-1}(\phi_a(z))b = \phi_b(\phi_a(z)) = (\phi_b \bullet \phi_a)(z)$, por lo tanto φ es un homomorfismo.
Sean $aC_X(Z) \in \ker\varphi$, entonces para toda z en Z se tiene que $\phi_a(z) = z$ ya que ϕ_a es la identidad en Z, pero $z = \phi_a(z) = a^{-1}za$, por lo cual a conmuta con todo elemento de Z, así que $a \in C_X(Z)$, por lo tanto φ es inyectiva.
Sea $f \in K$, entonces $f = \phi_a$ para alguna $a \in \langle A, \overline{A} \rangle$, entonces $\varphi(aC_X(Z)) = f$, por lo tanto φ es sobreyectiva.

Como $\frac{\langle A, \overline{A} \rangle C_X(Z)}{C_X(Z)} = \left\langle \frac{AC_X(Z)}{C_X(Z)}, \frac{\overline{A}C_X(Z)}{C_X(Z)} \right\rangle = \langle P_1, \overline{P_1} \rangle$, entonces $K \cong \langle P_1, \overline{P_1} \rangle = P_1 Q$.

Sea $z \in C_Z(\langle A, \overline{A} \rangle)$ y $\phi_a \in K$, entonces $\phi_a(z) = a^{-1}za = a^{-1}az = z$, ya que $a \in \langle A, \overline{A} \rangle$, entonces todo elemento de K fija a todo elemento de $C_Z(\langle A, \overline{A} \rangle)$, entonces $\psi_{\phi_a} : \frac{Z}{C_Z(\langle A, \overline{A} \rangle)} \to \frac{Z}{C_Z(\langle A, \overline{A} \rangle)}$ definido por $\psi_{\phi_a}(zC_Z(\langle A,\overline{A}\rangle)) = \phi_a(z)C_Z(\langle A,\overline{A}\rangle)$ es un automorfismo de $\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}$ inducido por K. Sea H el grupo de automorfismos de $\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}$ inducidos por K. Sea $f : K \to H$ con $f(\phi_a) = \psi_{\phi_a}$, f es claramente sobreyectiva, se observa que $f(\phi_a \circ \phi_b) = f(\phi_a) \circ f(\phi_b)$, por lo tanto f es un homomorfismo. Sea $N = \ker f$, sea $\phi_a \in \ker f$ de orden una potencia de q, ϕ_a deja fijo a $C_Z(\langle A,\overline{A}\rangle)$, y ψ_{ϕ_a}, su automorfismo inducido, deja fijo a $\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}$, como Z es un p-grupo, por el Teorema 1 se tiene que ϕ_a es la identidad. Entonces el orden de N divide a p, pero $N \trianglelefteq K \cong P_1Q$, pero si $N \neq \langle 1\rangle$ entonces N sería un p-subgrupo de Sylow normal, el cual no existe en P_1Q ya que P_1Q tiene al menos dos p-subgrupos de Sylow distintos, entonces $N = \langle 1\rangle$. Por lo tanto $H \cong K \cong P_1Q$. $\left|\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}\right| \leq p^2$, si $\left|\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}\right| = 1$ entonces K sería trivial, y como $K \cong P_1Q$, P_1Q también sería trivial, por lo tanto $\left|\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}\right| \neq 1$. Por otro lado, si $\left|\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}\right| = p$, se tendría que $Aut\left(\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}\right) \cong \mathbb{Z}_{p-1}$, pero H es un subgrupo de $Aut\left(\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}\right)$ de orden pq^t, lo cual no es posible, así que $\left|\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}\right| = p^2$, y como Z es abeliano elemental, entonces $\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}$ también lo es, por lo cual $Aut\left(\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}\right) \cong GL(2,p)$. Como $H \cong P_1Q$, entonces $H = P_2Q_2$ con P_2 un subgrupo de orden p y Q_2 un subgrupo normal de orden q^t. Si $[P_2,Q_2] = \langle 1\rangle$, es fácil ver que $H \cong P_2 \times Q_2$, pero entonces P_2 sería normal en H, lo cual no es posible porque tiene más de un p-subgrupo de Sylow, entonces $[P_2,Q_2] \neq \langle 1\rangle$. Sea $R = [P_2,Q_2]$, como $H = P_2Q_2$ con P_2 p-grupo, Q_2 q-grupo normal y R un subgrupo normal de Q_2 ya que $[p,q] = (p^{-1}q^{-1}p)q = q'q \in Q_2$, entonces por el Lema 5 se tiene que $Q_2 = RC_{Q_2}(P_2)$. Si $R \leq C_{Q_2}(P_2)$, entonces $Q_2 = C_{Q_2}(P_2)$, por lo cual $[P_2,Q_2] = \langle 1\rangle$, pero como $[P_2,Q_2] \neq \langle 1\rangle$, entonces $R \nleq C_{Q_2}(P_2)$, así que $[P_2,R] \neq \langle 1\rangle$. Como $R = [P_2,Q_2] \leq [H,H] \leq Aut\left(\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}\right)'$, entonces R es un q-subgrupo del derivado de $Aut\left(\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}\right)$, que es $SL(2,p)$, entonces por el Lema 6 R es cíclico. Dado que q divide al orden de H y H es un subgrupo de $Aut\left(\frac{Z}{C_Z(\langle A,\overline{A}\rangle)}\right) \cong GL(2,p)$, entonces q divide al orden de $GL(2,p)$ que es $(p-1)(p+1)(p-1)p$, entonces $q \lneqq p$. Como R es un q-grupo cíclico, $R \cong \mathbb{Z}_{q^s}$ con $s \geq 1$, su grupo de automorfismos es isomorfo a $U(\mathbb{Z}_{q^s})$, y su orden es el valor de la función de Euler en q^s, es decir $q^s - q^{s-1} = q^{s-1}(q-1)$, pero como $p > q$, p no divide al orden de $Aut(R)$, entonces como los automorfismos de R inducidos por P_2 tienen orden una potencia de p, entonces P_2 sólo induce el automorfismo identidad en R, es decir que para todo $p \in P_2$ y para todo $r \in R$, $r = \phi_p(r) = p^{-1}rp$, es decir $[r,p] = r^{-1}p^{-1}rp = 1$, entonces $[P_2,R] = \langle 1\rangle$, lo cual es una contradicción ya que $[P_2,R]$ debía ser no trivial. Entonces nuestra suposición de $J(P) \nleq O_p(X)$ no puede ser cierta, por lo cual $J(P) \leq O_p(X)$ y entonces $J(P)$ es normal en X. ■

Lema 8. Sea G un grupo soluble de orden p^aq^b, con p y q primos distintos, y $O_p(G) = \langle 1\rangle$. Entonces para todo subgrupo N de G que contenga a $O_q(G)$, $O_p(N) = \langle 1\rangle$.

Demostración:
Como $O_q(G)$ es normal en G entonces es normal en cualquier subgrupo de G que lo contenga, como N. Dado que $O_p(N) \cap O_q(G) = \langle 1\rangle$ y siendo ambos normales en N, entonces $O_p(N)O_q(G) = O_p(N) \times O_q(G)$, por lo cual los elementos de $O_p(N)$ y los de $O_q(G)$ conmutan, entonces $O_p(N) \leq C_G(O_q(G))$. Sea $H = C_G(O_q(G))$, como $O_q(G)$ es normal en G, entonces H también es normal en G, y como $O_q(H)$ es característico en H, entonces $O_q(H)$ es normal en G, y al ser q-grupo entonces $O_q(H) \leq O_q(G)$.

Sea P un p-subgrupo de Sylow de $O_{q,p}(H)$, entonces $O_{q,p}(H) = PO_q(H)$. Como $P \leq H = C_G(O_q(G))$, $PO_q(G)$ es un subgrupo de G porque $O_q(G)$ es normal y además P es normal en él ya que los elementos de P conmutan con los elementos de $O_q(G)$, por lo tanto $PO_q(G) \cong P \times O_q(G)$, y al ser $O_q(H) \leq O_q(G)$ entonces $PO_q(H) \cong P \times O_q(H)$ y por lo tanto P es característico en $PO_q(H) = O_{q,p}(H)$, pero además $O_{q,p}(H)$ es característico en H y H es normal en G, entonces P es normal en G, por ello $P \leq O_p(G) = \langle 1 \rangle$. Como $O_{q,p}(H) = O_q(H)$, se sigue que H es un q-grupo. Como $O_p(N) \leq H$, al ser H un q-grupo y $O_p(N)$ un p-grupo, entonces $O_p(N) = \langle 1 \rangle$. ■

Lema 9. Sea M un grupo soluble de orden $p^a q^b$, p y q primos impares distintos. Sea M_p un p-subgrupo de Sylow de M, y Z el soclo de M_p. Si $C_M(Z) = M_p$ y $O_q(M) = \langle 1 \rangle$, entonces $J(M_p)$ es normal en M.

Demostración:
Supongamos que no es cierto, y sea M un contraejemplo de orden mínimo.
Como $J(M_p)$ no es normal en M, entonces existe A un subgrupo abeliano elemental de orden máximo de M_p que no está contenido en $O_p(M)$, ya que si todo subgrupo abeliano elemental de orden máximo de M_p estuviera en $O_p(M)$, entonces estarían contenidos en todo conjugado de M_p ya que $O_p(M)$ está contenido en todo p-subgrupo de Sylow de M, por lo cual $J(M_p) \leq J(\overline{M_p})$, y al ser isomorfos $\overline{M_p}$ y M_p también lo son $J(M_p)$ y $J(\overline{M_p})$, entonces $J(M_p) = J(\overline{M_p})$, y entonces $J(M_p)$ sería normal en M.

Sea $N = AO_{p,q}(M)$, entonces $O_p(M) \leq N$, y entonces

$$O_q\left(\frac{M}{O_p(M)}\right) = \frac{O_{p,q}(M)}{O_p(M)} \leq \frac{AO_{p,q}(M)}{O_p(M)} = \frac{N}{O_p(M)}.$$

Sean $P_1, P_2, ..., P_n$ los p-subgrupos de Sylow de N, $\frac{P_i O_p(M)}{O_p(M)} = \frac{P_i}{O_p(M)}$ es entonces un p-subgrupo de Sylow de $\frac{N}{O_p(M)}$ para toda i; sea $\frac{K}{O_p(M)}$ un p-subgrupo de Sylow de $\frac{N}{O_p(M)}$, como K es de orden una potencia de p está contenido en algún p-subgrupo de Sylow P de N, entonces $\frac{K}{O_p(M)} \leq \frac{PO_p(M)}{O_p(M)} = \frac{P}{O_p(M)}$ donde $\frac{P}{O_p(M)}$ es un p-subgrupo de Sylow de $\frac{N}{O_p(M)}$, por lo tanto $\frac{K}{O_p(M)} = \frac{P}{O_p(M)}$. Los subgrupos $\frac{P_i}{O_p(M)}$ son entonces todos los p-subgrupos de Sylow de $\frac{N}{O_p(M)}$, por lo tanto

$$O_p\left(\frac{N}{O_p(M)}\right) = \bigcap_{i=1}^{n} \frac{P_i}{O_p(M)} = \frac{\bigcap_{i=1}^{n} P_i}{O_p(M)} = \frac{O_p(N)}{O_p(M)}.$$

Pero $O_p\left(\frac{M}{O_p(M)}\right) = \frac{O_p(M)}{O_p(M)} = \langle 1 \rangle$. Entonces, como $\frac{N}{O_p(M)}$ contiene a $O_q\left(\frac{M}{O_p(M)}\right)$ y $O_p\left(\frac{M}{O_p(M)}\right) = \langle 1 \rangle$, entonces por el Lema 8 también $O_p\left(\frac{N}{O_p(M)}\right) = \langle 1 \rangle$, por lo cual $\frac{O_p(N)}{O_p(M)} = O_p\left(\frac{N}{O_p(M)}\right) = \langle 1 \rangle$, por lo tanto $O_p(N) = O_p(M)$. Por otra parte N contiene a $O_p(M)$ y al ser $O_q(M) = \langle 1 \rangle$, nuevamente por el Lema 8 se tiene que $O_q(N) = \langle 1 \rangle$.

Como $O_{p,q}(M) = O_p(M)S$ con S un q-subgrupo de Sylow de $O_{p,q}(M)$, entonces $|N| = |AO_{p,q}(M)| = |AO_p(M)S| = \frac{|AO_p(M)||S|}{|AO_p(M) \cap S|} = |AO_p(M)||S|$ ya que $AO_p(M)$ es un p-grupo y S un q-grupo, por lo tanto $AO_p(M)$ es un p-subgrupo de Sylow de N. Sea $N_p = N \cap M_p$. Como $O_p(M)$ está contenido en todo p-subgrupo de Sylow de M, entonces está en M_p, y al ser A un subgrupo de M_p, entonces $AO_p(M) \leq N_p$, por lo tanto N_p es un p-subgrupo de Sylow de N. Siendo M_p un p-grupo, su soclo Z está contenido en su centro por el Teorema 3, entonces todo subgrupo normal minimal de M_p es de orden primo, ya que los subgrupos normales minimales de M_p están en Z y todo subgrupo del centro es normal. Por lo tanto Z es abeliano elemental, entonces AZ es abeliano elemental, y al ser A abeliano elemental de orden máximo, entonces $AZ = A$, por lo tanto $Z \leq A \leq AO_p(M) \leq N_p$. Como

$C_M(Z) = M_p$, entonces $C_N(Z) = N \cap C_M(Z) = N \cap M_p = N_p$. Como todo subgrupo normal minimal de M_p está contenido en N_p, y al ser estos normales minimales en N_p ya que son de orden primo, entonces Z está contenido en el soclo Z_0 de N_p, por lo tanto $C_N(Z_0) \leq C_N(Z) = N_p$, pero como Z_0 está contenido en el centro de N_p, $N_p \leq C_N(Z_0)$, así que $N_p = C_N(Z_0)$. Entonces al ser N un subgrupo de M con N_p un p-subgrupo de Sylow de N que cumple que $C_N(Z_0) = N_p$ y que $O_q(N) = \langle 1 \rangle$, entonces N cumple las hipótesis del teorema. Supongamos que N es un subgrupo propio de M. por la minimalidad de M se tiene que $J(N_p)$ es normal en N, por lo cual $J(N_p) \leq O_p(N)$, y al ser A un subgrupo abeliano elemental de orden máximo en M_p y que está contenido en N_p, entonces también es de orden máximo en N_p, por lo tanto $A \leq J(N_p) \leq O_p(N) = O_p(M)$, contradiciendo la suposición en A, por lo tanto $M = N = AO_{p,q}(M)$ con A un p-grupo abeliano elemental.

Como $\frac{O_{p,q}(M)}{O_p(M)} = O_q\left(\frac{M}{O_p(M)}\right)$, entonces $\frac{O_{p,q}(M)}{O_p(M)}$ es normal en $\frac{M}{O_p(M)} = \frac{AO_{p,q}(M)}{O_p(M)}$, entonces $\frac{O_{p,q}(M)}{O_p(M)}$ es normalizado por $\frac{AO_p(M)}{O_p(M)}$, el cual es isomorfo al subgrupo abeliano elemental $\frac{A}{A \cap O_p(M)}$. Entonces $\left(\frac{O_{p,q}(M)}{O_p(M)}\right)\left(\frac{AO_p(M)}{O_p(M)}\right)$ es un subgrupo con $\frac{O_{p,q}(M)}{O_p(M)}$ un q-subgrupo normal y $\frac{AO_p(M)}{O_p(M)}$ un p-subgrupo abeliano elemental, entonces por el Lema 2, $\frac{O_{p,q}(M)}{O_p(M)}$ es generado por los centralizadores en $\frac{O_{p,q}(M)}{O_p(M)}$ de los subgrupos de $\frac{AO_p(M)}{O_p(M)}$ de índice p. Al menos uno de los centralizadores no es centralizado por $\frac{AO_p(M)}{O_p(M)}$, ya que al ser $\frac{O_{p,q}(M)}{O_p(M)}$ generado por los centralizadores, si todos los centralizadores fueran centralizados por $\frac{AO_p(M)}{O_p(M)}$ entonces $\frac{O_{p,q}(M)}{O_p(M)}$ sería centralizado por $\frac{AO_p(M)}{O_p(M)}$, si suponemos que eso pasara entonces si tomamos $a \in AO_p(M)$ y $o \in O_{p,q}(M)$, como $\frac{AO_p(M)}{O_p(M)}$ centraliza a $\frac{O_{p,q}(M)}{O_p(M)}$, tenemos que $aoO_p(M) = oaO_p(M)$, es decir, $a^{-1}o^{-1}ao \in O_p(M)$, y entonces $o^{-1}ao \in AO_p(M)$, por lo cual $O_{p,q}(M)$ normaliza a $AO_p(M)$, así que $AO_p(M)$ es normal en M y siendo $AO_p(M)$ un p-subgrupo normal de M tenemos que $A \leq AO_p(M) \leq O_p(M)$, lo cual es una contradicción, por lo tanto existe un centralizador que no es centralizado por $\frac{AO_p(M)}{O_p(M)}$.

Sea $\frac{L}{O_p(M)}$ uno de esos centralizadores y sea $\frac{K}{O_p(M)}$ el subgrupo de índice p de $\frac{AO_p(M)}{O_p(M)}$ del cual es centralizador. Sea $R = LAO_p(M)$. Como $\frac{K}{O_p(M)}$ es normal en $\frac{AO_p(M)}{O_p(M)}$ por ser de índice p y $\frac{K}{O_p(M)}$ es normalizado por $\frac{L}{O_p(M)}$ ya que lo centraliza, entonces K es normalizado por $LAO_p(M) = R$, y al ser K subgrupo de R entonces K es normal en R, y siendo K un p-grupo, entonces $K \leq O_p(R)$. Como $AO_p(M)$ es subgrupo de Sylow de $N = M$ y está contenido en R, entonces $O_p(R) \leq AO_p(M)$. Pero K es de índice p en $AO_p(M)$, por lo cual, si $K \lneqq O_p(R)$, entonces $O_p(R) = AO_p(M)$, y por lo tanto $\frac{AO_p(M)}{O_p(M)}$ es normal en $\frac{R}{O_p(M)}$, al igual que $\frac{L}{O_p(M)}$, entonces al ser sus órdenes primos relativos, se tiene que $\frac{AO_p(M)}{O_p(M)}$ y $\frac{L}{O_p(M)}$ conmutan elemento a elemento, es decir, $\frac{AO_p(M)}{O_p(M)}$ centraliza a $\frac{L}{O_p(M)}$, una contradicción. Entonces tenemos que $K = O_p(R)$, por lo cual A no puede estar contenido en $O_p(R)$.

Sea $M_p \cap R = R_p$, como $M_p = AO_p(M) \leq R$ se tiene que R_p es un p-subgrupo de Sylow de R. Como A es un subgrupo abeliano elemental de orden máximo de M_p, entonces también lo es de R_p, entonces $A \leq J(R_p)$. Entonces $J(R_p) \nleq O_p(R)$, por lo cual $R_p \nleq O_p(R)$. Usado los mismos argumentos en R que se usaron en N, se tiene que $O_q(R) = \langle 1 \rangle$ y que $C_R(\Omega_1(R_p)) = R_p$, y R cumple las hipótesis del teorema, pero como $J(R_p) \nleq O_p(R)$, entonces $J(R_p)$ no es normal en R, siendo entonces que R es un contraejemplo con $R \leq M$. Siendo M de orden mínimo, $R = M$. Como K era de índice p en $AO_p(M)$ y $K = O_p(R) = O_p(M)$, entonces $O_p(M)$ es de índice p en $AO_p(M)$, por lo tanto el índice de $O_{p,q}(M)$ en M es

$$\frac{|AO_{p,q}(M)|}{|O_{p,q}(M)|} = \frac{|AO_p(M)||S|}{|O_p(M)||S|} = \frac{|AO_p(M)|}{|O_p(M)|} = p.$$

Sea $Y = \Omega_1(O_p(M))$. Supongamos que $Z \leq O_p(M)$. Entonces todo subgrupo normal minimal de M_p está contenido en $O_p(M)$, por lo que cada subgrupo normal minimal de M_p lo es también de $O_p(M)$, entonces $Z \leq Y$. Por hipótesis $C_M(Z) = M_p$, y como $C_M(Y) \leq C_M(Z)$, entonces $C_M(Y) \leq M_p$. Entonces $C_M(Y)$ es un p-grupo, y al ser Y normal en M, entonces $C_M(Y)$ es normal en M también, por lo tanto $C_M(Y) \leq O_p(M)$. Además Y está en el centro de $O_p(M)$, por lo cual $O_p(M) \leq C_M(Y)$, entonces $O_p(M) = C_M(Y)$, y $\frac{M}{C_M(Y)} = \frac{M}{O_p(M)}$. Como $[M : O_{p,q}(M)] = p$ y $[O_{p,q}(M) : O_p(M)] = q^s$ con $s \geq 1$, entonces $\frac{M}{O_p(M)}$ tiene orden pq^s, $\frac{O_{p,q}(M)}{O_p(M)}$ es un subgrupo normal de orden q^s, pero no tiene subgrupo normal de orden p, entonces debe tener al menos dos p-subgrupos de Sylow distintos de orden p, entonces $\frac{M}{C_M(Y)}$ tiene al menos dos p-subgrupos de Sylow distintos de orden p, con lo cual M cumple las hipótesis del Lema 7, entonces $J(M_p)$ es normal en M, contradiciendo la hipótesis.

Entonces supongamos que $Z \nleq O_p(M)$. Como

$$[M_p : O_p(M)] = \frac{|M_p|}{|O_p(M)|} = \frac{|M \cap M_p|}{|M_p \cap O_{p,q}(M)|} = \frac{|M||M_p||M_pO_{p,q}(M)|}{|M_p||O_{p,q}(M)||MM_p|} = \frac{|M||M_pO_{p,q}(M)|}{|O_{p,q}(M)||MM_p|} = p\frac{|M_pO_{p,q}(M)|}{|MM_p|} = p\frac{|M_pO_{p,q}(M)|}{|M|},$$

y como $O_{p,q}(M) \leq O_{p,q}(M)M_p \leq M$, entonces $O_{p,q}(M)M_p = O_{p,q}(M)$ ó $O_{p,q}(M)M_p = M$, si $O_{p,q}(M)M_p = O_{p,q}(M)$ entonces $[M_p : O_p(M)] = p\frac{|O_{p,q}(M)|}{|M|} = 1$, pero como $A \leq M_p$ y $A \nleq O_p(M)$, entonces $O_{p,q}(M)M_p = M$, por lo tanto $[M_p : O_p(M)] = p$, entonces $M_p = ZO_p(M)$. Sea $a \in Z$ con $a \notin O_p(M)$, $x \in O_p(M)$ y b un q-elemento de M. $b^{-1}xb \in O_p(M)$ por ser éste normal, y como $a \in Z$ y $C_M(Z) = M_p = ZO_p(M)$, entonces $a \in C_M(O_p(M))$, entonces $b^{-1}xb = a^{-1}(b^{-1}xb)a = (a^{-1}b^{-1}a)(a^{-1}xa)(a^{-1}ba) = (a^{-1}b^{-1}a)x(a^{-1}ba)$, entonces $x = (ba^{-1}b^{-1}a)x(a^{-1}bab^{-1})$, entonces, para todo Q un q-subgrupo de Sylow de M, se tiene que $[a, Q]$ centraliza a $O_p(M)$. Sea Q un q-subgrupo de Sylow de M, como $Q \leq O_{p,q}(M)$ y $O_{p,q}(M)$ es normal, tenemos que $[a, Q] \leq O_{p,q}(M)$, por lo tanto $[a, Q] \leq C_{O_{p,q}(M)}(O_p(M))$. Como $O_p(M)$ es un p-subgrupo de Sylow normal de $O_{p,q}(M)$, entonces $C_{O_{p,q}(M)}(O_p(M)) = P\overline{Q}$, con $\overline{Q}$ un q-subgrupo de Q y P un p-subgrupo de $O_p(M)$, y como todo elemento de $\overline{Q}$ conmuta con todo elemento de P, entonces $C_{O_{p,q}(M)}(O_p(M)) \cong P \times \overline{Q}$. Por lo tanto $\overline{Q}$ es característico en $C_{O_{p,q}(M)}(O_p(M))$. Veamos que $C_{O_{p,q}(M)}(O_p(M))$ es caracterísitco en $O_{p,q}(M)$:

Sean $f \in Aut(O_{p,q}(M))$, $c \in C_{O_{p,q}(M)}(O_p(M))$, y $w \in O_p(M)$.
Como w es un p-elemento, la imagen inversa w' bajo f es también un p-elemento, y siendo que $O_p(M)$ es normal en $O_{p,q}(M)$, $O_p(M)$ es el único p-subgrupo de Sylow de $O_{p,q}(M)$, por lo tanto $w' \in O_p(M)$.
$f(c)^{-1}wf(c) = f(c^{-1})f(w')f(c) = f(c^{-1}w'c) = f(w') = w$.
Entonces $f(c) \in C_{O_{p,q}(M)}(O_p(M))$, por lo tanto $C_{O_{p,q}(M)}(O_p(M))$ es característico en $O_{p,q}(M)$.

$\overline{Q}$ *car* $P\overline{Q}$ *car* $O_{p,q}(M)$ *car* M, por ello $\overline{Q}$ es normal en M, por lo tanto $\overline{Q} \leq O_q(M) = \langle 1 \rangle$, esto es $[a, Q] \leq P \leq O_p(M)$. Como también $[O_p(M), Q] \leq O_p(M)$, entonces $[\langle O_p(M), a \rangle, Q] \leq O_p(M)$, esto es $[M_p, Q] \leq O_p(M) \leq M_p$. Entonces M_p es normal en $M_pQ = M$, contradiciendo que $O_p(M) \lneq M_p$. Por lo tanto el contraejemplo M no puede existir, así que el teorema es verdadero. ■

2.2 Lemas de Thompson y Matsuyama.

Lema de Thompson. Sea G un grupo tal que $G = MPQ$ con M un p-subgrupo normal, P un p-subgrupo y Q un q-subgrupo (p y q primos distintos). Si $P \leq C_G(Q)$ y $C_M(P) \leq C_G(Q)$, entonces $M \leq C_G(Q)$.

Demostración:
Como $C_M(Q) \leq C_Q(Q)$, basta probar $M = C_M(Q)$. Supongamos que $M \neq C_M(Q)$. Llamemos $K = C_M(Q)$
Como todo elemento de K conmuta con todo elemento de Q, Q normaliza a K. Como M es normal en G, P normaliza a M, y como $P \leq C_G(Q)$, P normaliza a Q. Además Q normaliza a P ya que P centraliza a Q.
Sean $m \in K, p \in P$ y $q \in Q$, entonces, como P normaliza a M, $m' = pmp^{-1} \in M$, y como $P \leq C_G(Q)$ y $m \in K$, entonces m' conmuta con q, por lo cual $m' \in K$, entonces P normaliza a K.
Como K es normalizado por P y por Q, entonces K es normalizado por $PQ = P \times Q$.
Como M es un p-subgrupo, $K \lneqq N_M(K)$.

Sea $h \in P \times Q$ y $m \in N_M(K)$, $hmh^{-1} \in M$ ya que $P \times Q$ normaliza a M, y como $P \times Q$ normaliza a K, $hmh^{-1}K(hmh^{-1})^{-1} = K$, entonces $hmh^{-1} \in N_M(K)$, es decir, $P \times Q$ normaliza a $N_M(K)$.
Sea S un subgrupo de $N_M(K)$ normalizado por $P \times Q$ que contenga propiamente a K tal que no exista algún subgrupo propio de S normalizado por $P \times Q$ que contenga propiamente a K. Como $S \leq N_M(K)$, K es normal en S. $P \times Q$ induce un grupo de automorfismos en $\frac{S}{K}$ por conjugación, ya que S es normalizado por $P \times Q$. Si $\frac{S}{K}$ tuviera un subgrupo característico propio $\frac{T}{K}$, entonces T sería normalizado por $P \times Q$, por lo cual $T = K$, entonces $\frac{S}{K}$ no tiene subgrupos característicos propios no triviales, por ello es abeliano elemental. Como $P \times Q$ normaliza a S, en particular P normaliza a S, entonces PS es un subgrupo de G, y siendo P y S p-subgrupos, entonces $\frac{PS}{K}$ es un p-grupo con $\frac{S}{K}$ un subgrupo normal de él, por lo tanto su intersección con el centro de $\frac{PS}{K}$ es no trivial. Sea $\frac{L}{K} = Z(\frac{PS}{K}) \cap \frac{S}{K}$. Sea $a \in P$, como $\frac{L}{K} \leq Z(\frac{PS}{K})$, en particular se tiene que $a^{-1}laK = lK$ para toda $l \in L$, entonces $l^{-1}a^{-1}la \in K \leq L$, por lo cual $a^{-1}la \in L$, entonces L es normalizado por P. Sea $b \in Q$ y $l \in L$, como $\frac{L}{K} \leq \frac{S}{K}$ y S es normalizado por Q, $b^{-1}(lK)b = (b^{-1}lb)K \in \frac{S}{K} \leq \frac{PS}{K}$, sea $as \in PS$, entonces

$$(b^{-1}(lK)b)(asK) = (b^{-1}lb)K(asK) = (b^{-1}lbas)K = (b^{-1}labs)K$$

ya que P centraliza a Q, y como Q normaliza a S, $(b^{-1}labs)K = (b^{-1}las'b)K$, ahora, como $\frac{L}{K} \leq Z(\frac{PS}{K})$, tenemos que $las'K = as'lK$, por lo cual $b^{-1}(las'K)b = b^{-1}(as'lK)b$, entonces

$$(b^{-1}las'b)K = (b^{-1}as'lb)K = (ab^{-1}s'lb)K = (asb^{-1}lb)K,$$

ya que como $bs = s'b$, se tiene que $sb^{-1} = b^{-1}s'$, y finalmente tenemos que $(asb^{-1}lb)K = (asK)(b^{-1}(lK)b)$, entonces $b^{-1}(lK)b \in Z(\frac{PS}{K})$, es decir, $b^{-1}(lK)b \in \frac{L}{K}$, entonces $b^{-1}(lK)b = l'K$, por lo cual $l'^{-1}b^{-1}lb \in K \leq L$, es decir, $b^{-1}lb \in L$, por lo cual L es normalizado por Q, es decir, L es normalizado por $P \times Q$, y al ser $\frac{L}{K}$ no trivial y no existir subgrupo entre K y S normalizado por $P \times Q$, se tiene que $L = S$, entonces $\frac{S}{K} = Z(\frac{PS}{K}) \cap \frac{S}{K}$, es decir, $\frac{S}{K} \leq Z(\frac{PS}{K})$.

Sea $p_1 \in P$ y $s \in S$, como $\frac{S}{K} \leq Z(\frac{PS}{K})$, se tiene que $sKp_1K = p_1KsK$, es decir, $sp_1K = p_1sK$, entonces $s^{-1}p_1^{-1}sp_1 \in K$, por lo cual $[S,P] \leq K$, y como $K = C_M(Q)$, entonces $[S,P,Q] = [[S,P],Q] \leq [K,Q] = \langle 1 \rangle$. Como $P \leq C_G(Q)$, entonces $[P,Q] = \langle 1 \rangle$, por lo cual $[P,Q,S] = [[P,Q],S] = [\langle 1 \rangle,S] = \langle 1 \rangle$. Por el Teorema 4, tenemos que $[[Q,S],P] = [Q,S,P] = \langle 1 \rangle$, y como S es normalizado por Q y $S \leq M$, tenemos que $[Q,S] \leq C_M(P) \leq K$. Entonces para todo

$q_1 \in Q$, q_1 induce el automorfismo identidad en $\frac{S}{K}$, ya que para toda $s \in S$ se tiene que $s^{-1}q_1^{-1}sq_1 \in K$, es decir, $sK = (q_1^{-1}sq_1)K = q_1^{-1}(sK)q_1$, y como $K = C_M(Q)$, cada elemento de Q induce la identidad en K, y al ser S y K normalizados por Q, por el Teorema 1 cada elemento de Q induce la identidad en S, es decir, $q^{-1}sq = s$, entonces S conmuta con todo elemento de Q, es decir, $S \leq C_M(Q) = K$, contradiciendo el hecho de que S contenía propiamente a K. Entonces $M = C_M(Q)$, es decir, $M \leq C_G(Q)$. ■

Lema XX. Sea X un grupo soluble de orden $p^a q^b$ (p, q primos distintos) y P un p-subgrupo de X. Entonces $O_q(N_X(P)) \leq O_q(X)$.

Demostración:
Dividamos la demostración en dos casos, cuando $O_q(X) = \langle 1 \rangle$, y cuando es no trivial.
Supongamos que $O_q(X) = \langle 1 \rangle$. Supongamos también que $O_q(N_X(P)) \neq \langle 1 \rangle$. Sea $Q = O_q(N_X(P))$ y $M = O_p(X)$. Como Q y P son normales en $N_X(P)$, y como $Q \cap P = \langle 1 \rangle$, si hacemos $G = MPQ$, tenemos que $P \leq C_G(Q)$, ya que al ser P y Q normales en $N_X(P)$, entonces se normalizan entre si, entonces para todo $a \in P$ y $b \in Q$, $a^{-1}b^{-1}ab \in P \cap Q$, por lo cual $a^{-1}b^{-1}ab = 1$, es decir, $ab = ba$.

Sea $H = C_M(P)$, como Q normaliza a M se tiene que $[H,Q] \leq [M,Q] \leq M$, pero como $H \leq C_M(P) \leq C_X(P) \leq N_X(P)$ y $Q \trianglelefteq N_X(P)$, entonces $[H,Q] \leq [N_X(P),Q] \leq Q$, así que $[H,Q] \leq M \cap Q = \langle 1 \rangle$, entonces $H \leq C_G(Q)$, es decir, $C_M(P) \leq C_G(Q)$. Por el lema de Thompson se tiene que $O_p(X) = M \leq C_G(Q)$, así que $[Q,M] = \langle 1 \rangle$, entonces $Q \leq C_X(M)$, por lo cual $C_X(M)$ no puede ser un p-grupo.

Como $C_X(M)$ no es un p-grupo, entonces $C_X(M)$ no es subgrupo de M, así que $M \lneqq MC_X(M)$. Como $M \trianglelefteq X$, entonces X induce un grupo de utomorfismos en M, sea $a \in C_X(M)$, $x \in X$ y $m \in M$, como la conjufación por x en M es automorfismo existe $m' \in M$ tal que $x^{-1}m'x = m$, entonces $x^{-1}axm = x^{-1}axx^{-1}m'x = x^{-1}am'x = x^{-1}m'ax = x^{-1}m'xx^{-1}ax = mx^{-1}ax$, entonces $x^{-1}ax \in C_X(M)$, por lo cual es normal en X, entonces $MC_X(M) \trianglelefteq X$, y por el terorema de la correspondencia $\frac{MC_X(M)}{M} \trianglelefteq \frac{X}{M}$. Sea $\frac{N}{M}$ un subgrupo normal minimal de $\frac{X}{M}$ contenido en $\frac{MC_X(M)}{M}$. Como $\frac{N}{M}$ es normal minimal, es producto directo de subgrupos simples isomorfos, y al ser X soluble, $\frac{X}{M}$ es soluble y $\frac{N}{M}$ también, por lo cual $\frac{N}{M}$ es abeliano elemental, entonces $\frac{N}{M}$ es de orden p^c o q^c. Si $\frac{N}{M}$ tuviese orden p^c, N sería un p-subgrupo normal de X, por lo cual $N \leq O_p(X) = M$, por lo cual sería $\frac{N}{M}$ trivial, entonces $\frac{N}{M}$ es de orden q^c. Sea S un q-subgrupo de Sylow de N, $MS \leq N$ ya que M es normal en N, y como $\frac{N}{M}$ es de orden q^c y $M \cap S = \langle 1 \rangle$, entonces $|MS| = |M|q^c = |N|$, por lo tanto $N = MS$. Cada elemento de $C_X(M)$ induce el automorfismo identidad en M, entonces $MC_X(M)$ únicamente induce automorfismos interiores en M, por lo tanto los automorfismos inducidos son de orden una potencia de p, como S es subgrupo de $MC_X(M)$, y S es un q-grupo, los elementos de S inducen únicamente el automorfismo identidad en M, es decir, para todo $s \in S$ y $m \in M$, $s^{-1}ms = m$, entonces M conmuta con S elemento a elemento, por lo tanto lo normaliza, entonces S es normal en N, y siendo q-subgrupo de Sylow es característico en N, por lo tanto normal en X, entonces $S \leq O_q(X) = \langle 1 \rangle$, lo cual es una contradicción.

Supongamos ahora que $O_q(X) \neq \langle 1 \rangle$. Sea $N = O_q(X)$.
Si $\frac{H}{N}$ fuese un q-subgrupo normal de $\frac{X}{N}$, H sería un q-subgrupo normal de X, entonces $X \leq N$ y por ende, $\frac{H}{N}$ sería trivial, por lo tanto $\frac{X}{N}$ no tiene q-subgrupos normales no triviales, entonces $O_q(\frac{X}{N}) = \langle 1 \rangle$, y como $\frac{PN}{N}$ es un p-subgrupo de $\frac{X}{N}$, por la primer parte de la demostración tenemos que $O_q\left(N_{\frac{X}{N}}(\frac{PN}{N})\right) \leq O_q(\frac{X}{N}) = \langle 1 \rangle$.

Veamos que $\frac{N_X(P)N}{N} = N_{\frac{X}{N}}(\frac{PN}{N})$.

Sea $hN \in \frac{N_X(P)N}{N}$ con $h \in N_X(P)$ y $pN \in \frac{PN}{N}$, entonces $h^{-1}NpNhN = h^{-1}phN = p'N \in \frac{PN}{N}$, entonces $hN \in N_{\frac{X}{N}}(\frac{PN}{N})$.

Sea $hN \in N_{\frac{X}{N}}(\frac{PN}{N})$ con $h \in X$, entonces $h^{-1}N(\frac{PN}{N})hN = \frac{PN}{N}$, entonces si $pnN \in \frac{PN}{N}$, $h^{-1}pnhN = p'n'N$, entonces $(p'n')^{-1}h^{-1}pnh \in N$, entonces $(p'n')^{-1}h^{-1}pnh = n''$, y se sigue $h^{-1}pnh = p'n'n'' \in PN$, entonces $h^{-1}PNh = PN$, entonces $h^{-1}Ph \leq PN$.

Como N es un q-grupo, $|PN| = |P||N|$, entonces P y $h^{-1}Ph$ son p-subgrupos de Sylow de PN, entonces existe $ak^{-1} \in PN$ tal que $kPk^{-1} = ka^{-1}Pak^{-1} = h^{-1}Ph$, es decir, existe $k \in N$ tal que $k^{-1}h^{-1}Phk = P$. Entonces $hk \in N_X(P)$, y $hN = hkN \in \frac{N_X(P)N}{N}$.

Entonces $\frac{N_X(P)N}{N} = N_{\frac{X}{N}}(\frac{PN}{N})$.

Entonces $O_q\left(\frac{N_X(P)N}{N}\right) = O_q\left(N_{\frac{X}{N}}(\frac{PN}{N})\right) = \langle 1 \rangle$ y como $\frac{N_X(P)N}{N} \cong \frac{N_X(P)}{N_X(P)\cap N}$, entonces $O_q\left(\frac{N_X(P)}{N_X(P)\cap N}\right) = \langle 1 \rangle$.

Sea R un q-subgrupo normal de $N_X(P)$, entonces $\frac{R(N_X(P)\cap N)}{N_X(P)\cap N}$ es un q-subgrupo normal de $\frac{N_X(P)}{N_X(P)\cap N}$, pero como $O_q\left(\frac{N_X(P)}{N_X(P)\cap N}\right) = \langle 1 \rangle$ se sigue que $\frac{R(N_X(P)\cap N)}{N_X(P)\cap N} = \langle 1 \rangle$, entonces $R(N_X(P) \cap N) = N_X(P) \cap N$, es decir, $R \leq N_X(P) \cap N$, entonces $O_q(N_X(P)) \leq N_X(P) \cap N \leq N = O_q(X)$. ■

Lema de Matsuyama. Sea G un grupo con $G = AB$, donde A es un p-subgrupo de Sylow y B un q-subgrupo de Sylow (p y q primos distintos). Sea A_0 subgrupo normal no trivial de A y B_0 subgrupo normal no trivial de B. Si $\left\langle A_0^{B_0} \right\rangle = \left\langle c^{-1}dc \mid c \in B_0 \text{ y } d \in A_0 \right\rangle$ es un p-grupo, entonces G no es simple.

Demostración:
Sea X un conjugado de A_0, como A_0 es normal en A, $A \leq N_G(A_0)$, entonces $G = AB \leq N_G(A_0)B \leq G$, entonces $G = N_G(A_0)B$, si $g \in G$ es tal que $g^{-1}A_0g = X$, $g = ab$ con $a \in N_G(A_0)$ y $b \in B$, entonces $X = g^{-1}A_0g = b^{-1}a^{-1}A_0ab = b^{-1}A_0b$, entonces existe $b \in B$ tal que $X = A_0^b$ (es decir $b^{-1}A_0b$). Como B_0 es normal en B, b^{-1} induce un automorfismo en B_0, entonces para todo $b_0 \in B_0$ existe un único b_1 tal que $bb_0b^{-1} = b_1$, entonces $X^{b_0} = (A_0^b)^{b_0} = \left(A_0^{bb_0b^{-1}}\right)^b = (A^{b_1})^b$, así que $\langle X^{B_0} \rangle = \left\langle \left(A_0^{B_0}\right)^b \right\rangle = \left\langle A_0^{B_0} \right\rangle^b$, y siendo $\left\langle A_0^{B_0} \right\rangle$ un p-grupo, $\langle X^{B_0} \rangle$ también lo es. Siendo $\langle X^{B_0} \rangle$ generado por conjugados de X por elementos de B_0, es normalizado en B_0, y es también generado de conjugados de A_0. Sea P_0 un p-subgrupo maximal normalizado por B_0 que sea generado por conjugados de A_0, y sea P un p-subgrupo de Sylow de G que contiene a P_0.

Supongamos que $N_P(P_0) \neq P$, siendo P un p-grupo, es nilpotente, entonces $N_P(P_0) \lneqq N_P(N_P(P_0))$. Sea $k \in N_P(N_P(P_0))$ tal que $k \notin N_P(P_0)$. Como $P_0 \leq N_P(P_0)$, entonces $P_0^k \leq (N_P(P_0))^k = N_P(P_0)$, pero $P_0^k \neq P_0$. Como P_0 es generado por conjugados de A_0, existe C conjugado de A_0 tal que $C \leq P_0$ y $C^k \nleq P_0$, ya que $C^k \leq P_0^k$ y si para todo conjugado C de A_0 tal que $C \leq P_0$ pasara que $C^k \leq P_0$, tendríamos que $P_0 = P_0^k$. Como C^k es un conjugado de A_0, $\langle (C^k)^{B_0} \rangle$ es un p-grupo, y $C^k \leq P_0^k \leq N_P(P_0)$ y $B_0 \leq N_k(P_0)$ ya que B_0 normaliza a P_0, entonces $\langle (C^k)^{B_0} \rangle \leq N_k(P_0)$, entonces $P_0\langle (C^k)^{B_0} \rangle$ es un subgrupo normalizado por B_0, y siendo P y $\langle (C^k)^{B_0} \rangle$ p-grupos, su producto lo es también, y como $C^k \nleq P_0$, entonces $P_0 \lneqq P_0\langle (C^k)^{B_0} \rangle$, contradiciendo la maximalidad de P_0. Entonces $N_P(P_0) = P$.

Sea $h \in G$, como $G = PB$, entonces $h = kl$ con $k \in P$ y $l \in B$, como $k \in P = N_P(P_0) \leq N_G(P_0)$ y $l \in B \leq N_G(B_0)$, entonces $B_0 = B_0^l \leq (N_G(P_0))^l = (N_G(P_0))^{kl} = (N_G(P_0))^h$. Entonces B_0 está contenido en cada conjugado de $N_G(P_0)$,

$$B_0 \leq I = \bigcap_{h \in G} (N_G(P_0))^h,$$

por lo cual $I \neq \langle 1 \rangle$. Si P_0 no es normal en G, entonces $N_G(P_0) \neq G$, por lo cual $I \neq G$, pero I es normal en G, ya que si tomamos $c \in I$ y $w \in G$, como $c \in d^{-1} N_G(P_0) d$ para todo $d \in G$, entonces $w^{-1}cw \in (dw)^{-1} N_G(P_0)(dw)$, pero al variar d en G, entonces $w^{-1}cw \in d^{-1} N_G(P_0) d$ para todo $d \in G$, entonces $w^{-1}cw \in I$, y como I no es trivial, entonces G no es simple. Si P_0 es normal en G, como P_0 no es G al ser P_0 p-grupo y $\langle 1 \rangle \neq A_0^{b_0} \leq P_0$ para alguna $b_0 \in B_0$, entonces G tampoco es simple en este caso. ■

2.3 Demostración del p-q Teorema de Burnside.

p-q **Teorema de Burnside**. Todo grupo de orden $p^a q^b$ es soluble (p, q primos distintos).

Demostración:
Supongamos que es falso, y sea G un grupo finito no soluble cuyo orden es divisible por a lo más dos primos diferentes, es decir, un contraejemplo de orden mínimo.
Sea $|G| = p^a q^b$, p y q primos distintos. Observemos que $a, b > 0$, ya que en otro caso tendríamos un grupo con orden la potencia de un primo, por lo tanto sería soluble.

G tiene las siguientes seis propiedades, que se demostrarán después del teorema:

(a) G es simple.
(b) Lema de Bender. Si M es un subgrupo maximal de G, el subgrupo de Fitting $F(M)$ es o un p-grupo o un q-grupo.
(c) Un subgrupo maximal M de G no puede contener un p-subgrupo central propio y un q-subgrupo central propio a la vez.
(d) Ningún p-subgrupo central no trivial de G normaliza a algún q-subgrupo no trivial de G.
(e) G tiene orden impar.
(f) Sea M un subgrupo maximal de G con $F(M)$ un p-grupo. Entonces si M_p es un p-subgrupo de Sylow de M, entonces $J(M_p)$ es normal en M, y M_p es un p-subgrupo de Sylow de G.

Si M es un subgrupo maximal de G, por el lema de Bender el orden de $F(M)$ es la potencia de un primo. Supongamos sin pérdida de generalidad que $F(M)$ es un p-grupo.

Por (f) un p-subgrupo de Sylow M_p de M es también un p-subgrupo de Sylow de G y el subgrupo de Thompsom $J(M_p)$, el generado por los subgrupos abelianos elementales de orden máximo, es normal en M. Supongamos que existe $\overline{M}$ un subgrupo maximal de G distinto a M, tal que $F(\overline{M})$ es un p-grupo, y sea $\overline{M_p}$ un p-subgrupo de Sylow de $\overline{M}$.

Si $M_p = \overline{M_p}$, entonces $J(M_p) = J(\overline{M_p})$, y $J(M_p)$ sería normal en M y en $\overline{M}$, y por ello sería normal en $\langle M, \overline{M} \rangle = G$, por lo tanto $M_p \neq \overline{M_p}$. Entonces, por cada p-subgrupo M_p de Sylow de G, existe un único subgrupo maximal M de G que contiene a M_p con $F(M)$ un p-grupo. Sean M y $\overline{M}$ subgrupos maximales de G tales que sus subgrupos de Fitting son p-grupos y sean M_p y $\overline{M_p}$ subgrupos de Sylow de M y $\overline{M}$ respectivamente, al ser también subgrupos de Sylow de G son conjugados, entonces existe $g \in G$ tal que $g^{-1}M_p g = \overline{M_p}$, pero $\overline{M_p} = g^{-1}M_p g \leq g^{-1}Mg$, y al ser M maximal, $g^{-1}Mg$ también lo es, y al contener a $\overline{M_p}$, entonces $g^{-1}Mg = \overline{M}$, por lo cual los subgrupos maximales de G tales que su subgrupo de Fitting es un p-grupo son conjugados.

Como para todo subgrupo maximal de M de G se tiene que $F(M)$ es o un p-grupo o un q-grupo por (b), entonces existen solo dos clases de conjugación, llámense C_p y C_q, de subgrupos maximales, donde $M \in C_p$ si su subgrupo de Fitting es un p-grupo y $M \in C_q$ si su subgrupo de Fitting es un q-grupo.

Supongamos que $p^a > q^b$. Sean M_1 y M_2 dos subgrupos distintos de C_p tal que el orden de los p-subgrupos de Sylow de su intersección $|M_1 \cap M_2|_p$ sea máximo.

Supongamos que $|M_1 \cap M_2|_p \neq 1$. Sea P un p-subgrupo de Sylow de $M_1 \cap M_2$ y R un subgrupo maximal de G que contenga a $N_G(P)$. El centro de cada p-subgrupo de Sylow de G que contiene a P, al conmutar cada elemento de él con P, está contenido en $C_G(P) \leq N_G(P)$, entonces $N_G(P)$ contiene a algún p-subgrupo central, por lo tanto R también contiene a algún p-subgrupo central de G. Si $F(R)$ fuese q-grupo, cualquier p-subgrupo de R normalizaría a $F(R)$ ya que éste último es normal en R, y esto contradice a (d) pues $F(R) \neq \langle 1 \rangle$, entonces $F(R)$ es un p-grupo. El subgrupo $M_1 \cap R$ contiene a $M_1 \cap N_G(P) = N_{M_1}(P)$.

Si P fuese un p-subgrupo de Sylow de M_1, también lo sería de G, y por cuestiones de orden también lo sería de M_2, entonces al contener los dos subgrupos maximales de G el mismo subgrupo de Sylow de G serían iguales, por lo cual P no puede ser subgrupo de Sylow de M_1. Sea K un p-subgrupo de Sylow de M_1 que contenga a P. $P \lneqq K$, y por lo tanto, $P \lneqq N_K(P)$. Si H es un p-subgrupo de Sylow de $N_{M_1}(P)$ que contiene a $N_K(P)$, tendríamos que $P \lneqq H$, pero $N_{M_1}(P) \leq M_1 \cap R$, entonces si L es un p-subgrupo de Sylow de $M_1 \cap R$ que contiene a H, entonces $P \lneqq L$. Sea $|M_1 \cap R|_p$ el orden del p-subgrupo de Sylow de $M_1 \cap R$, entonces

$$|M_1 \cap M_2|_p = |P| \leq |L| = |M_1 \cap R|_p,$$

por la maximalidad de $|M_1 \cap M_2|_p$, se tiene que $M_1 = R$. Análogamente $M_2 = R$, entonces $M_1 = M_2$, una contradicción, por lo tanto $|M_1 \cap M_2|_p = 1$.

Si S_1 es un p-subgrupo de Sylow de M_1 y S_2 es un p-subgrupo de Sylow de M_2, entonces $S_1 \cap S_2 = \langle 1 \rangle$. Por lo tanto

$$|G| = p^a q^b \lneqq p^{2a} = |S_1 S_2| \leq |G|.$$

Esta contradicción aegura que no existe G un grupo de orden $p^a q^b$ que no sea soluble. ■

Ahora demostraremos que el contraejemplo de orden mínimo G del teorema anterior cumple con las propiedades antes mencionadas:

(**a**) G es simple.

Demostración:
Supongamos que G no es simple, entonces existe un subgrupo normal N de orden menor que G y de la forma $p^a q^b$, como G es minimal no soluble con orden la forma $p^a q^b$, entonces N es soluble, por el mismo argumento $\frac{G}{N}$ es soluble, entonces G sería soluble contradiciendo la hipótesis, entonces G es simple. ■

(**b**) **Lema de Bender**. Si M es un subgrupo maximal de G, entonces $F(M)$ es o un p-grupo o un q-grupo.

Demostración:
Siendo M maximal en G, es no trivial y de orden menor a G, por lo tanto M es soluble, por ello existe un subgrupo no trivial de M que es abeliano y normal en M, y por lo tanto normal y nilpotente, entonces $F(M)$ no es trivial. Supongamos que $|F(M)|$ es divisible por p y por q. Sea Z el soclo del centro de $F(M)$, como Z es producto de subgrupos normales minimales, cada uno de éstos es de orden primo. En efecto, al ser subgrupos del centro de un grupo, de tener subgrupos éstos últimos serían normales en $F(M)$, por lo tanto los subgrupos normales minimales son isomorfos a $\mathbb{Z}_p$ ó $\mathbb{Z}_q$, ya que p y q son los únicos primos que dividen al orden de $F(M)$, entonces $Z = Z_p \times Z_q$, con Z_p el p-grupo formado del producto de los $\mathbb{Z}_p$ y Z_q el q-grupo formado por el producto de los $\mathbb{Z}_q$. Y siendo

$F(M)$ nilpotente, es producto directo de sus subgrupos de Sylow S_p y S_q, entonces $Z(F(M)) \cong Z(S_p \times S_q) = Z(S_p) \times Z(S_q)$, pero el centro de grupos de orden una potencia de un primo distinta de 1 no es trivial, por lo tanto Z_p y Z_q no son triviales.

Sea H un subgrupo maximal de G que contiene a Z. Como $O_q(M) \trianglelefteq M$, entonces $O_q(M) \cap H$ es un q-subgrupo normal de $M \cap H$, por lo cual $O_q(M) \cap H \leq O_q(M \cap H)$.

Z_p es normal en M, ya que Z_p es normal en Z y Z_p es p-subgrupo de Sylow de Z, por lo tanto característico en Z, y Z *car* $Z(F(M))$ *car* $F(M)$ *car* M, por ello Z_p es normal en M, pero Z_p no puede ser normal en G porque G es simple por (1), y siendo M maximal, entonces $N_G(Z_p) = M$, así que $N_H(Z_p) = N_G(Z_p) \cap H = M \cap H$, entonces $O_q(M) \cap H \leq O_q(M \cap H) = O_q(N_H(Z_p))$, y como (dado que $|H| \leq |G|$) H es soluble y Z_p es un p-subgrupo de H, entonces por el lema XX, $O_q(N_H(Z_p)) \leq O_q(H)$, entonces $O_q(M) \cap H \leq O_q(H)$. Análogamente $O_p(M) \cap H \leq O_p(H)$. Como $F(M)$ es nilpotente, $F(M) = S_p \times S_q$, además siendo que los subgrupos de Sylow son normales en un grupo nilpotente, y $F(M)$ es característico en M, entonces $S_p = O_p(M)$ y $S_q = O_q(M)$, entonces $F(M) = O_p(M)O_q(M)$, así que

$$F(M) \cap H = O_p(M)O_q(M) \cap H = [O_p(M) \times O_q(M)] \cap H =$$
$$(O_p(M) \cap H)(O_q(M) \cap H) \leq O_p(H)O_q(H) = F(H).$$

Entonces $Z_p \leq F(M) \cap H \leq F(H)$, por lo cual $Z_p \leq O_p(H)$ y análogamente $Z_q \leq O_q(H)$.

Como $F(H) = O_p(H) \times O_q(H)$ los elementos de $O_p(H)$ conmutan con los de $O_q(H)$, entonces $O_p(H) \leq C_G(O_q(H)) \leq C_G(Z_q)$ y también $O_q(H) \leq C_G(Z_p)$, pero $C_G(Z_p) \leq N_G(Z_p) = M$ y $C_G(Z_q) \leq M$, entonces $F(H) \leq M$, en particular, Z^*, el soclo del centro de $F(H)$, está contenido en M. Usando el mismo argumento de Z y H en Z^* y M se tiene que $F(M) \leq H$.

Como $F(M) \cap H \leq F(H)$, entonces $F(M) = F(M) \cap H \leq F(H)$, y análogamente $F(H) \leq F(M)$, entonces $F(M) = F(H)$ y como $F(H) = F(M) \trianglelefteq M$, y $\langle H \cup M \rangle \leq N_G(F(H))$. Si $H \neq M$, $\langle H \cup M \rangle = G$ ya que M es maximal, entonces $G = N_G(F(H))$, es decir, $F(H) \trianglelefteq G$, una contradicción debido a la simplicidad de G, por lo tanto $H = M$, es decir, M es el único subgrupo maximal de G que contiene a Z.

Sea M_p un p-subgrupo de Sylow de M, G_p un p-subgrupo de Sylow de G que contiene a M_p y G_q un q-subgrupo de Sylow de G. Si $M_p = G_p$, como $G = G_pG_q$, entonces $G = M_pG_q$, G_q contiene a $O_q(M)$ y por cada conjugado $\overline{G_q}$ de G_q existe $t \in M_p$ tal que $t^{-1}G_qt = \overline{G_q}$. Sea $R = \bigcap_{t \in M_p} t^{-1}G_qt$, si $x \in R$ y $g \in G$, se tiene que $x \in gt^{-1}G_qtg^{-1}$ para todo $t \in M_p$ ya que x está en todos los conjugados de G_q, para todo $t \in M_p$ existe $a \in G_q$ tal que $x = gt^{-1}atg^{-1}$, entonces $g^{-1}xg = t^{-1}at \in t^{-1}G_qt$. Como esto vale para todo $t \in M_p$, entonces $g^{-1}xg \in R$, es decir, R es normal en G. Pero M normaliza a $O_q(M)$, entonces M_p normaliza a $O_q(M)$, entonces $O_q(M) = t^{-1}O_q(M)t \leq t^{-1}G_qt$ para toda $t \in M_p$, así que $\langle 1 \rangle \lneqq O_q(M) \leq R \leq G_q \lneqq G$, entonces R es un subgrupo propio no trivial de G normal, contradiciendo la simplicidad de G, por lo tanto $M_p \lneqq G_p$, por lo cual $M_p \lneqq N_{G_p}(M_p)$ al ser G_p un p-grupo, entonces existe $g \in N_{G_p}(M_p)$ tal que $g \notin M_p$. Entonces, $M_p = g^{-1}M_pg \leq g^{-1}Mg$. Como M es maximal y M no es normal en G, $M = N_G(M)$, y como g no está en M, se tiene que $M^g = g^{-1}Mg \neq M$. Entonces existe un conjugado de M que contiene a M_p, M^g.

Como $Z_p \trianglelefteq M$, $g^{-1}Z_pg \trianglelefteq M^g$, así que $g^{-1}Z_pg \leq O_p(M^g)$. Como $M_p \leq M^g$ y M_p es un p-subgrupo de Sylow de M, M_p es un p-subgrupo de Sylow de M^g también, así que $O_p(M^g) \leq M_p$, entonces $g^{-1}Z_pg \leq O_p(M^g) \leq M_p \leq M$. Si $g^{-1}Z_qg \leq M$, se tendría que $g^{-1}Zg = g^{-1}Z_pZ_qg \leq M$, es decir,

$Z \leq M^{g^{-1}} \neq M$, entonces Z estaría contenido en un subgrupo maximal distinto de M, lo cual se probó no era posible, entonces $g^{-1}Z_q g \nleq M$.

Como $Z_q \trianglelefteq M$, M^g normaliza a $g^{-1}Z_q g$, pero $Z_p \leq O_p(M) \leq M_p \leq M^g$, entonces Z_p normaliza a $g^{-1}Z_q g$. Sea H el conjunto de subgrupos de índice p de Z_p. Como $Z_p(g^{-1}Z_q g)$ es un subgrupo ya que Z_p normaliza a $g^{-1}Z_q g$, entonces $g^{-1}Z_q g$ es normal en $Z_p(g^{-1}Z_q g)$, y al ser Z_p abeliano elemental, por el lema 2, $g^{-1}Z_q g = \left\langle C_{g^{-1}Z_q g}(U) | U \in H \right\rangle$. Si Z_p no es cíclico, los elementos de H tendrían que ser no triviales. Por cada $U \in H$, $C_G(U) \lneqq G$, ya que U es no trivial y si su centralizador fuera G entonces sería normal en G, y $Z \leq C_G(U)$ ya que $U \leq Z$ y Z es abeliano, entonces cualquier subgrupo maximal de G que contenga a $C_G(U)$ contendría a Z, entonces el único subgrupo maximal de G que contiene a $C_G(U)$ es M, por lo cual $C_{g^{-1}Z_q g}(U) \leq C_G(U) \leq M$, y $g^{-1}Z_q g \leq M$, una contradicción, entonces Z_p es cíclico, y de forma análoga Z_q también, así que $Z = Z_p \times Z_q \cong \mathbb{Z}_p \times \mathbb{Z}_q (\cong \mathbb{Z}_{pq})$, por lo cual Z es cíclico. Como $Z_p(g^{-1}Z_q g)$ es un subgrupo isomorfo a Z, es abeliano, entonces $g^{-1}Z_q g$ centraliza a Z_p, pero el centralizador de Z_p en G está contenido en M, entonces $g^{-1}Z_q g \leq C_G(Z_p) \leq M$, contradicción. En conclusión, $|F(M)|$ no puede ser dividido por p y por q. ■

(**c**) Un subgrupo maximal M en G no puede contener un p-subgrupo central propio y un q-subgrupo central propio a la vez.

Demostración:
Sea M un subgrupo maximal de G. Por el Lema de Bender (2), $F(M)$ es o un p-grupo o un q-grupo. Supongamos que $F(M)$ es un q-grupo. Sea G_q un q-subgrupo de Sylow de G que contenga a $F(M)$. Entonces $Z(G_q) \leq C_G(F(M))$. Como $Z(F(M))$ es normal en $C_G(F(M))$, y al ser característico $Z(F(M))$ en $F(M)$, $Z(F(M))$ es normal en M, entonces $Z(F(M))$ es normal en $C_G(F(M))M$, si $C_G(F(M)) \nleq M$, entonces, como $F(M) \neq \langle 1 \rangle$, $\langle 1 \rangle \lneqq Z(F(M)) \trianglelefteq C_G(F(M))M = G$, una contradicción. Entonces $C_G(F(M)) \leq M$, es decir, $C_G(F(M)) = C_M(F(M))$. Pero por el Teorema 11, $C_M(F(M)) \leq F(M)$, entonces $Z(G_q) \leq F(M) \leq M$. Entonces $Z(G_q)$ es un q-subgrupo central de G contenido en M.

Supongamos que M contiene un p-subgrupo central $B_0 \neq \langle 1 \rangle$. Sea B un p-subgrupo de Sylow de G tal que $B_0 \leq Z(B)$. Sea $A_0 = Z(G_q)$ y $A = G_q$. Es claro que $A_0 \trianglelefteq A$ y $B_0 \trianglelefteq B$, además como $A_0 \leq F(M)$ y $B_0 \leq M$, $\langle b^{-1}A_0 b | b \in B_0 \rangle \leq \langle m^{-1}A_0 m | m \in M \rangle \leq F(M)$, entonces $\langle b^{-1}A_0 b | b \in B_0 \rangle$ es un q-grupo no trivial, por el lema de Matsuyama G no es simple, contradiciendo (1), entonces M no contiene un p-subgrupo central. ■

(**d**). Ningún p-subgrupo central no trivial de G normaliza a algún q-subgrupo no trivial de G.

Demostración:
Supongamos que un p-subgrupo central no trivial H de G normaliza a un q-subgrupo no trivial K de G. Sea S un q-subgrupo de Sylow de G que contenga a K. Entonces $N_G(K)$ contiene a H y a $Z(S)$, el cual no es trivial, y como $N_G(K) \neq G$, existe un subgrupo maximal M de G que lo contiene. Entonces M contiene a H y al q-subgrupo central $Z(S)$, contradiciendo a (3). ■

(**e**). G tiene orden impar. [1]

Demostración:
Supongamos que G tiene orden par, entonces $|G| = 2^a q^b$. $O_2(G) \trianglelefteq G$ y como G no es un 2-grupo, entonces $O_2(G) \lneqq G$, pero como G es simple por (1), entonces $O_2(G) = \langle 1 \rangle$. Sea S un 2-subgrupo de Sylow, como el centro de S es no trivial tomemos $a \in Z(S)$ de orden 2, entonces $\langle a \rangle$ es un

[1] Vea comentario al final del Apéndice A.

2-subgrupo central de G. Como $a \notin O_2(G)$, por el lema 4, existe un q-elemento b no trivial de G tal que $a^{-1}ba = b^{-1}$. Entonces se tiene que $a^{-k}b^r a^k = b^{(-1)^k r} \in \langle b \rangle$, por lo cual $\langle a \rangle$ es un 2-subgrupo central que normaliza a $\langle b \rangle$, lo que contradice a (4). ■

(**f**). Sea M un subgrupo maximal de G con $F(M)$ un p-grupo. Entonces si M_p es un p-subgrupo de Sylow de M, entonces $J(M_p)$ es normal en M, y M_p es un p-subgrupo de Sylow de G.

Demostración:
Sea $Z = \Omega_1(Z(M_p))$, y sea P un p-subgrupo de Sylow de G que contiene a M_p. Como $F(M)$ es un p-grupo normal de M, entonces $F(M) \leq M_p$.

Sea N un subgrupo normal minimal de P, N es por lo tanto de orden p. Por ser P un p-grupo, $N \cap Z(P) \neq \langle 1 \rangle$, y al ser N minimal, entonces $N \leq Z(P)$, por lo cual N centraliza a $F(M)$, así que $N \leq N_G(F(M))$. Pero $M \leq N_G(F(M))$, y siendo M maximal en G y $G \neq N_G(F(M))$ pues $F(M) \neq \langle 1 \rangle$ y G es simple por (1), entonces $M = N_G(F(M))$, así que $N \leq M$, por lo cual $N \leq M \cap P = M_p$, y, siendo que N es normal en P, N es normal en M_p, entonces $\Omega_1(P) \leq \Omega_1(M_p)$, y por el Teorema 3, $\Omega_1(Z(P)) \leq \Omega_1(Z(M_p)) = Z$. Si existiese un q-subgrupo no trivial de G contenido en $C_G(\Omega_1(Z(P)))$, entonces el p-grupo $\Omega_1(Z(P))$ normalizaría a ese q-subgrupo, contradiciendo a (4), entonces $C_G(\Omega_1(Z(P)))$ es un p-grupo, y como $\Omega_1(Z(P)) \leq Z$, entonces $C_G(Z) \leq C_G(\Omega_1(Z(P)))$, por lo cual $C_G(Z)$ es un p-grupo, y $C_M(Z)$ tambien. $M_p \leq C_M(Z)$ ya que $Z \leq Z(M_P)$, y al ser $C_M(Z)$ un p-grupo está contenido en un p-subgrupo de Sylow de M el cual contendría a M_p, entonces M_p es ese grupo de Sylow y por lo tanto $M_p = C_M(Z)$. Como $F(M)$ es un p-grupo, $O_q(M) = \langle 1 \rangle$, entonces, como p y q son primos impares por (5), por el Lema 9, $J(M_p) \trianglelefteq M$.

Supongamos que M_p no es un p-subgrupo de Sylow de G. Siendo M_p subgrupo propio de algún p-subgrupo P de Sylow de G, su normalizador en él crece. Sea $H = N_P(M_p)$. Dado que la imagen de un subgrupo abeliano elemental de orden máximo de un grupo bajo un automorfismo es también un subgrupo abeliano elemental de orden máximo, entonces $J(M_p)$ es característico en M_p, y por lo tanto, normal en H, entonces $H \leq N_G(J(M_p))$. Pero $J(M_p)$ es normal en M, por lo cual $G = \langle M, H \rangle \leq N_G(J(M_p))$, contradiciendo que G es simple. Por lo tanto M_p es un p-subgrupo de Sylow de G. ■

Apéndice A.
Demostración del Teorema de Burnside usando Teoría de Caracteres.

Definición. Sea G un grupo y V un $\mathbb{C}$-espacio vectorial. Una *representación lineal* de G en V es un homomorfismo $\rho : G \to GL(V)$. A la dimensión de V se le conoce como el *grado de la representación lineal*. Dos representaciones ρ y ρ' de G en V y V' respectivamente se les dice isomorfas si existe un isomorfismo f entre V y V' y si $f \circ \rho(s) = \rho'(s) \circ f$ para todo $s \in G$.

Definición. La representación $\rho : G \to GL(1,\mathbb{C}) = \mathbb{C}^*$ con $\rho(g) = 1$ para todo $g \in G$ es conocida como la *representación trivial o principal* de G.

Definición. Sea R un anillo y G un grupo. El *anillo de grupo* de G sobre R, denotado por RG, es el anillo formado por las R-combinaciones lineales formales finitas de G con el producto definido por

$$\left(\sum_{x\in G}\alpha_x x\right)\left(\sum_{y\in G}\beta_y y\right) = \sum_{x\in G}\sum_{y\in G}\alpha_x\beta_y xy$$

Si F es un campo, FG es un F-álgebra llamado álgebra de grupo.

Definición. Sea $\rho' : G \to S_G$ tal que $\rho'(h)g = hg$, como G y $p'(h)(G)$ son bases de $\mathbb{C}G$ se puede extender $\rho'(h)$ a una transformación lineal biyectiva de $\mathbb{C}G$. La representación lineal $\rho : G \to GL(\mathbb{C}G)$ donde $\rho(g)$ es la extensión de $\rho'(g)$ se le conoce como la *representación regular*.

Definición. Sea $\rho : G \to GL(V)$ una representación lineal de grado finito y $W \leq V$. Decimos que W es *G-invariante* si $\rho(g)w \in W$ para todo $g \in G$ y $w \in W$.

Definición. Sea $\rho : G \to GL(V)$ una representación lineal de grado finito y $W \leq V$. Si W es G-invariante a la restricción de ρ a W se le conoce como *subrepresentación*.

Definición. Sea $\rho : G \to GL(V)$ una representación lineal. Si V es un espacio no trivial y ningún subespacio propio no trivial es G-invariante entonces se dice que ρ es *irreducible*.

Definición. Si V es suma directa de subespacios W_i G-invariantes, decimos que ρ es *suma directa de las restricciones* ρ_i de ρ en W_i. Se cumple que $\rho(g)v = \sum_i p_i(g)w_i$, donde $v = \sum_i w_i$.

Teorema B1 (**Maschke**). Toda representación lineal de un grupo finito es suma directa de representaciones irreducibles.

Definición. Sea $\rho : G \to GL(V)$ una representación lineal de grado finito. La función $\chi : G \to \mathbb{C}$ donde $\chi(g)$ es la traza de la matriz asociada a $\rho(g)$ se le llama el *carácter de la representación ρ*.

Teorema B2. Toda representación irreducible de un grupo finito G es sumando directo de la representación regular.

Teorema B3. El número de representaciones irreducibles no isomorfas de un grupo finito G es finito y es igual al número de clases de conjugación de G.

Definición. Los caracteres correspondientes a las repesentaciones irreducibles se denotan como χ_1, ..., χ_r, con r el número de clases de conjugación y χ_1 el carácter de la representación trivial. Al grado de la representación cuyo carácter es χ_i se le denota f_i.

Definición. Sea ρ una representación lineal y χ su carácter. El núcleo de ρ es $\{x \in G \mid \chi(x) = \chi(1)\}$ y se le conoce como el *núcleo* de χ y se denota K_χ. Si χ_i es un carácter irreducible denotamos el núcleo como K_i. El conjunto $\{x \in G \mid |\chi(x)| = \chi(1)\}$ se denota por Z_χ. Si χ_i es un carácter irreducible entonces se denota por Z_i.

Definición. Sean g_1,..., g_r representantes de las clases de conjugación de G, y $k_i = [G : C_G(g_i)]$, sean ρ_1, ..., ρ_r las representaciones irreducibles de G, ρ_1 la representación trivial y χ_i el carácter de ρ_i. La siguiente tabla es conocida como la *Tabla de carácter*:

$$\begin{array}{c|cccc}
 & 1 & k_2 & \cdots & k_r \\
 & 1 & g_2 & \cdots & g_r \\
- & - & - & - & - \\
\chi_1 & 1 & 1 & \cdots & 1 \\
\chi_2 & f_2 & \chi_2(g_2) & \cdots & \chi_2(g_r) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\chi_r & f_r & \chi_r(g_2) & \cdots & \chi_r(g_r)
\end{array}$$

Teorema de ortogonalidad por renglón. Para todo $1 \leq i,j \leq r$ se tiene que

$$\delta_{ij} = \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \frac{1}{|G|} \sum_{t=1}^{r} k_t \chi_i(g_t)\overline{\chi_j(g_t)}$$

Teorema de ortogonalidad por columna. Para todo $1 \leq i,j \leq r$ se tiene que

$$\sum_{t=1}^{r} \chi_t(g_i)\overline{\chi_t(g_j)} = \frac{|G|}{k_i}\delta_{ij} = |C_G(g_i)|\delta_{ij}$$

Teorema B4. $Z_\chi \leq G$ y $K_\chi \trianglelefteq G$ para cualquier carácter de G, y si χ es irreducible, entonces $\frac{Z_\chi}{K_\chi} = Z\left(\frac{G}{K_\chi}\right)$.

Teorema B5. Si G es no abeliano y simple, entonces $Z_i = \{1\}$ para toda i.

Definición. Sea $x \in \mathbb{C}$. x es un *entero algebraico* si es raíz de algún polinomio mónico con coeficientes enteros.

Teorema B6. El conjunto de números racionales que son enteros algebraicos es el conjunto de los números enteros.

Teorema B7. Los enteros algebraicos forman un subanillo de $\mathbb{C}$.

Teorema B8. Sea χ un carácter de G. $\chi(g)$ es un entero algebraico para todo $g \in G$.

Teorema B9. Si χ es un carácter irreducible de G y sea $g \in G$, entonces $[G : C_G(g)]\frac{\chi(g)}{\chi(1)}$ es un entero algebraico.

Teorema B10. Sea χ un carácter irreducible de G. Entonces $\chi(1)$ divide a $|G|$.

Teorema B11. Sea χ un carácter de G, sea $g \in G$ y sea $\gamma = \frac{\chi(g)}{\chi(1)}$. Si γ es un entero algebraico, entonces $|\gamma| = 1$.

Teorema B12. Si G tiene una clase de conjugación no trivial de orden la potencia de un primo, entonces G no es simple.

Demostración:
Supongamos que G es simple y que $g_i \neq 1$ es un repesentante de la clase de conjugación de orden p^n (con p primo y $n > 0$), por el teorema de la ortogonalidad por columna tenemos:

$$\sum_{t=1}^{r} \chi_t(g_i)\overline{\chi_t(1)} = |C_G(g_i)|\delta_{ij} = 0,$$

ya que g_i no pertenece a la clase de conjugación del 1, y como $\chi_t(1)$ es un número entero entonces tenemos que:

$$0 = \frac{0}{p} = \frac{1}{p}\sum_{t=1}^{r} \chi_t(g_i)\chi_t(1) = \frac{1}{p} + \sum_{t=2}^{r} \frac{\chi_t(g_i)\chi_t(1)}{p}.$$

Entonces tenemos que $\sum_{t=2}^{r} \frac{\chi_t(g_i)\chi_t(1)}{p} = -\frac{1}{p}$, y por el teorema B6 un racional no entero no es un entero algebraico, por ende $\sum_{t=2}^{r} \frac{\chi_t(g_i)\chi_t(1)}{p}$ tampoco lo es, pero como los enteros algebraicos forman un subanillo de $\mathbb{C}$ por el teorema B7, entonces algún $\frac{\chi_t(g_i)\chi_t(1)}{p}$ no debe ser entero algebraico con $2 \leq t \leq r$. Como $\chi_t(g_i)$ es un entero algebraico por el teorema B8, entonces $\frac{\chi_t(1)}{p}$ no es entero algebraico, pero al ser racional tenemos que $p \nmid \chi_t(1)$ y además $\chi_t(g_i) \neq 0$. Entonces tenemos que $[G : C_G(g_i)] = p^n$ es primo relativo con $\chi_t(1)$ así que existen $a, b \in \mathbb{Z}$ tales que

$$a[G : C_G(g_i)] + b\chi_t(1) = 1,$$

entonces tenemos que

$$\frac{\chi_t(g_i)}{\chi_t(1)} = a[G : C_G(g)]\frac{\chi_t(g_i)}{\chi_t(1)} + b\chi_t(g_i),$$

pero por el teorema B9 esto es una combinación lineal de enteros algebraicos, por lo tanto $\frac{\chi_t(g_i)}{\chi_t(1)}$ es un entero algebraico, y por el teorema B11,

$$\left|\frac{\chi_t(g_i)}{\chi_t(1)}\right| = 1,$$

es decir,

$$|\chi_t(g_i)| = |\chi_t(1)| = \chi_t(1).$$

Entonces $g \in Z_t$. Como G tiene una clase de conjugación no trivial, entonces G es no abeliano, y como es simple, por el teorema B5 tenemos que $Z_t = \{1\}$, entonces $g = 1$, una contradicción, por lo tanto G no es simple. ■

Teorema B13. Todo grupo G de orden $p^a q^b$ con p, q primos diferentes y $a, b > 0$ no es simple.

Demostración:
Como todo subgrupo de un grupo abeliano es normal supongamos que G es no abeliano. Si G es simple, entonces $Z(G) = \langle 1 \rangle$.
Sean C_i las distintas clases de conjugación no triviales de G, por la ecuación de clases se tiene que:

$$|G| = |Z(G)| + \sum_i |C_i|$$

Como G es simple, por el teorema B12 cada clase de conjugación no trivial de G tiene orden divisible por al menos dos primos distintos, pero el orden de cada clase de conjugación es un divisor del orden de G, por lo cual el orden de cada clase de conjugación no trivial es dividido por p y por q, por lo que $p|\sum_i |C_i|$, y como $p||G|$, se tiene que $p||Z(G)|$, una contradicción, por lo tanto G no es simple. ■

p-*q* **Teorema de Burnside**. Todo grupo de orden $p^a q^b$ es soluble (p, q primos distintos).

Demostración:
Inducción sobe $a + b$.

Si $a + b = 1$, entonces G tiene orden un número primo, y al ser cíclico es soluble.

Supongamos que cualquier grupo de orden $p^r q^s$ con $r + s < a + b$ es soluble.

Si a ó b son cero, entonces G tiene como orden una potencia de un número primo, por lo tanto es soluble.

Supongamos que $a, b > 0$, por el teorema B13 sabemos que G no es simple, y al no ser simple, G tiene un subgrupo normal propio no trivial N. Por inducción, N y $\frac{G}{N}$ son solubles, y por lo tanto, G es soluble. ■

Apéndice B.
Teorema de Feit - Thompson.

Prop. Las siguientes dos proposiciones son equivalentes.

(**1**) Si G es un grupo finito simple no abeliano, entonces G es de orden par.

(2) Teorema de Feit - Thompson (1963)
Si G es un grupo finito de orden impar, entonces G es soluble.

Demostración:
Supongamos que (**1**) es cierto y sea G un grupo finito de orden impar.
Supongamos que G es simple; si G no fuera soluble entonces G sería no abeliano, pero el Teorema de Burnside nos dice que entonces G sería de orden par, por lo tanto G debe ser soluble.
Supongamos ahora que G no es simple, usemos inducción sobre el orden de G. Como G no es simple existe N subgrupo normal propio de G no trivial, como el orden de G es impar, se tiene que $\frac{G}{N}$ y N tambien son de orden impar, entonces por inducción $\frac{G}{N}$ y N son solubles, por lo tanto G también lo es.

Supongamos válido el Teorema de Feit - Thompson y sea G un grupo de orden impar.
Al ser de orden impar, el Teorema de Feit - Thompson dice que G es soluble, si G fuera simple, tendríamos que el derivado de G es $\langle 1 \rangle$ ó G, pero al ser soluble el derivado de G debe ser $\langle 1 \rangle$, por lo tanto G es abeliano. ■

Observación:
El contraejemplo mínimo G que surge en la demostración del p-q Teorema de Burnside es de orden impar. El teorema de Feit - Thompson nos indica que este grupo G es soluble, con lo que podemos concluir que este grupo G no existe y terminar así la demostración del p-q Teorema de Burnside. El Teorema de Feit - Thompson fue conjeturado por Burnside en el año 1911, y fue demostrado por Feit y Thompson durante el Año de la Teoría de Grupos Finitos, llevado a cabo en la Universidad de Chicago en el período escolar 1960-1961. Su demostración original es de 255 páginas, y requiere una base de conocimientos sumamente grande, que incluye la teoría de carácteres.

Notación.

$H \leq G$	H es subgrupo de G.
$H \lneqq G$	H es subgrupo propio de G.
$H \nleq G$	H no es subgrupo de G.
$H \trianglelefteq G$	H es subgrupo normal de G.
$H \; car \; G$	H es subgrupo característico de G.
$H \cong G$	Hes isomorfo a G.
$\langle g \rangle$	Subgrupo cíclico generado por g.
$[G : H]$	Índice de H en G.
$\frac{G}{H}$	Cociente de H en G.
G'	Subgrupo derivado de G.
$G^{(n)}$	n-ésimo subgrupo derivado de G.
$Z(G)$	Centro de G.
$Aut(G)$	Grupo de automorfismos de G.
$N_G(H)$	Normalizador de H en G.
$N_G(h)$	Normalizador de h en G.
$C_G(H)$	Centralizador de H en G.
$C_G(h)$	Centralizador de h en G.
$C_G(A)$	Si $A \leq Aut(G)$. $C_G(A) = \{g \in G \mid f(g) = g$ para toda $f \in A\}$.
$[A, B]$	Interderivado de A y B.
$J(G)$	Subgrupo de Thompson de G.
$\Omega_1(G)$	Soclo de G, cuando G es un p-grupo.
$F(G)$	Subgrupo de Fitting de G.
$O_p(G)$	Subgrupo generado por los subgrupos normales de G de orden una potencia de p.
$O_{p,q}(G)$	Subgrupo que cumple que $\frac{O_{p,q}(G)}{O_p(G)} = O_q\left(\frac{G}{O_p(G)}\right)$.
$GL(n, q)$	Grupo de matrices invertibles de $n \times n$ con entradas en el campo de orden q.
$SL(n, q)$	Grupo de matrices de $n \times n$ con entradas en el campo de orden q cuyo determinante es 1.
$GF(p^a)$	Campo de orden p^a.
$\mathbb{Z}_n$	Grupo de las clases residuales de $\mathbb{Z}$ módulo n bajo la suma.
$U(\mathbb{Z}_n)$	Grupo formado por los elementos de $\mathbb{Z}_n$ que tienen inverso multiplicativo.

$A^b = b^{-1}Ab$

$A^B = \{b^{-1}ab \mid a \in A, b \in B\}$

Bibliografía.

[1] J. L. Alperin, Rowen B. Bell, *Groups and Representations*.
Department of Mathematics, University of Chicago (1995), pag. 179-183.
[2] H. Bender, *A group theoretic proof of Burnside's* $p^a q^b$*-theorem*.
Math. Z. (1972), pag. 327-338.
[3] W. Burnside, *On groups of order* $p^\alpha q^\beta$.
Proc. London Math. Soc. (2) 2 (1904), pag. 432-437.
[4] W. Feit, J.G. Thompson, *Solvability of groups of odd order.*
Pacific J. Math. 13 (1963), pag. 775-1029.
[5] D. Goldschmidt, *A group theoretic proof of the* $p^a q^b$*-theorem for odd primes.*
Math. Z. 113 (1970), pag. 373-375.
[6] G. Gorestein, *Finite groups.*
Harper and Row, New York (1968).
[7] H. Matsuyama, *Solvability of groups of order* $2^a q^b$.
Osaka J. of Math. 10 (1973), pag. 375-378.
[8] G. Zappa, *Topics on finite solvable groups.*
Istituto Nazionale di Alta Matematica Francesco Severi, Roma (1982).