33
2ej.

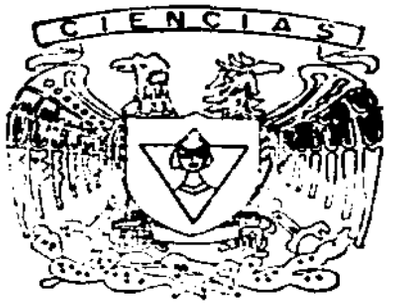
UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

Sobre el Teorema $p^{\alpha}q^{\beta}$ de Burnside

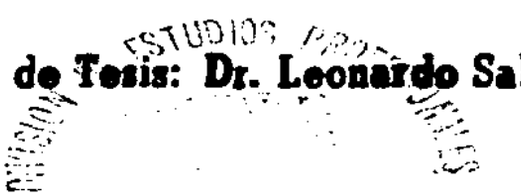
T E S I S
Que para obtener el título de
M A T E M A T I C O
p r e s e n t a

MIGUEL ANGEL PIZAÑA LOPEZ



FACULTAD DE CIENCIAS
UNAM

Director de Tesis: Dr. Leonardo Salmerón Castro



1997

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

M. en C. Virginia Abrín Batule
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
P r e s e n t e

Comunicamos a usted que hemos revisado el trabajo de Tesis:

Sobre el Teorema $p^{\alpha}q^{\beta}$ de Burnside.

realizado por Miguel Angel Pizaña López,

con número de cuenta 8955530-7 **, pasante de la carrera de** Matemático.

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dr. Leonardo Salmerón Castro.
Propietario	Dr. Francisco Javier González Acuña
Propietario	Dr. José Antonio de la Peña Mena
Suplente	Dr. Alberto Gerardo Raggi Cárdenas
Suplente	Dr. Ernesto Vallejo Ruiz

Consejo Departamental de Matemáticas

Dr. Manuel Falconi Magaña

FACULTAD DE CIENCIAS
CONSEJO DEPARTAMENTAL
DE
MATEMATICAS

Sobre el Teorema $p^{\alpha}q^{\beta}$ de Burnside

Director: Dr. Leonardo Salmerón Castro.
Por: Miguel Angel Pizaña López.
U.N.A.M.

Para Violeta

Agradecimientos

Quisiera agradecer a los profesores que me han enseñado toda el álgebra que sé : Leonardo Salmerón, Gerardo Raggi, Martha Rzedowski, Gabriel Villa, Helmut Bender, Joseph Rottman, Michio Suzuki, Daniel Gorenstein y Marshal Hall, entre otros.

Un agradecimiento especial a Ernesto Vallejo por la traducción del alemán del artículo [Ben II] y a Leonardo Salmerón por su dedicación.

Índice

Introducción

Al inicio de este siglo* , Burnside prueba el siguiente teorema:

Teorema. Todo grupo de orden $p^a q^b$, con p y q números primos, es soluble.

Esta proposición se ha convertido en un teorema clásico y fundamental en la teoría de grupos finitos. Variantes de la prueba de Burnside (que usa teoría de caracteres) se pueden encontrar en la actualidad en muchos libros de texto, por ejemplo: [Asc 35.13, p. 186], [Gor 4.3.3, p.131] y [Hal 16.8.7, p. 301].

Encontrar una prueba al teorema de Burnside que no utilice teoría de caracteres representó durante largo tiempo un reto. Suzuki [Suz II, 1977 5.4.25] presenta (¿por primera vez en un libro de texto?) una demostración sin caracteres, debida a los trabajos de Goldschmidt [Gol 1970] y Matsuyama [Mat 1973], y señala (pág. 216):

> This is a famous theorem of Burnside who proved this in the early twentieth century as an application of character theory. The theorem is pretty and very useful. The original proof of Burnside is short and clear. However, in spite of the efforts of many mathematicians to prove the theorem whitout using character theory, such a proof has been obtained only quite recently.

Goldschmidt, por su parte, utiliza el teorema $Z(J)$ de Glauberman [Gla], considerado una "herramienta pesada", y afirma que Thompson (en [Fei 1963] y [Tho 1968]) *esboza* una prueba libre de caracteres para este resultado. Considerando que [Fei] es un artículo que consta de 255 densas páginas, creemos que tal *esbozo* es bastante difuso. Además, en estos dos artículos no encontramos más que un señalamiento al que pudiera referirse Goldschmidt [Tho p. 388]:

> Corollary 6 of Burnside is well known. The interested reader may extract the relevant results from [[Fei]] and the present paper, to give a new proof of Corollary 6.

---

* De hecho, el asunto es poco claro: el articulo de Burnside de 1904 [Bur] empieza diciendo:

"Having shown that all groups of order $p^\alpha q^\beta$ are solvable ..."

y a continuación explora alguna consecuencias de este resultado. La demostración más antigua que pudimos hallar se publicó en 1911, en el libro de texto de Burnside [Bur II]. Lo más extraño es que en todas las referencias que hemos investigado (todas las que están listadas en la bibliografía más otras tantas como ésas) nadie (ni el mismo Burnside) señala explícitamente el artículo en que el teorema fue publicado por primera vez. Ya que todos los autores utilizan expresiones semejantes a la que usamos al inicio de esta introducción para hablar de la fecha en que el teorema fue probado, suponemos que éste fue publicado entre 1900 y 1904.

El "corolario 6" mencionado por Thompson es precisamente el teorema de Burnside. [Fei] es el famoso articulo de Feit y Thompson en donde se demuestra el resultado (antes conocido como la conjetura de Burnside) que lleva sus nombres: "Todo grupo finito de orden impar es soluble". Este trabajo no sólo es bien conocido por la relevancia de sus resultados (y por su relación con el teorema fundamental de los grupos simples), sino además por lo inusual de su longitud.

Matsuyama, por otro lado, da una prueba simple y sin caracteres para el caso par del teorema de Burnside, complementando así el trabajo de Goldschmidt, pero reconoce:

> After finishing this work the autor has found that Bender [[Ben]] has also obtained a group theoretic proof of the theorem in the general case.

Así, llegamos a la conclusión de que Bender (en [Ben 1972]) es el primero en presentar una prueba completa del teorema de Burnside sin usar caracteres. Además, evita el uso de "herramientas pesadas". En sus propias palabras:

> This note supplements Goldschmidt's paper [[Gol]] which contains a very short and elegant character-free proof of Burnside's theorem concerning the solvability of groups of order $p^a q^b$, in case the primes p and q are odd.
> So it is mainly the object of this paper to present a relatively short and elementary proof of Burnside's theorem for groups of even order; although, since assuming the order to be even does not give a considerable advantage, the proof is organized so that it covers both cases.
> The proof is based on ideas of Thompson and Goldschmidt's note [[Gol]], and requires no heavy tools.

En efecto, aunque la prueba de Goldschmidt es corta (2 páginas) y muy elegante, utiliza herramientas pesadas (el teorema $Z(J)$ de Glauberman) y no considera el caso par. Bender toma las directrices marcadas por Goldschmidt, extirpa el uso del teorema de Glauberman (demuestra un resultado vagamente análogo: [Ben, Lemma 3]) y prueba el resultado sin restricciones de paridad; en contraste pierde algo de compacidad y de elegancia.

Las pruebas de Bender y Goldschmidt usan técnicas de "teoría local de grupos", de capital importancia en la teoría de grupos. En palabras de Aschbacher [Asc 1986 p.156]:

> Recall that if p is a prime then a *p-local subgroup* of G is the normalizer in G of a nontrivial p-subgroup of G. The local theory of groups investigates finite groups from the point of view of p-locals. A question of great interest in this theory is the relationship between the generalized Fitting subgroup of G and that of its local subgroups. Section 31 contains various results about such relationships. In the final chapter we'll get some idea of how such results are used to classify the finite simple groups.

La prueba de Bender tiene, desde el punto de vista formativo, una ventaja adicional: al prescindir del teorema de Glauberman, usa más veces y de más modos las técnicas locales.

El objetivo de este trabajo de tesis es presentar la prueba de Bender a un nivel accesible para el estudiante de licenciatura. Con este fin, presentamos aquí el material que está más allá del alcance de un curso básico de teoría de grupos, lo cual incluye tanto resultados y técnicas explícitas en el artículo de Bender, como conocimientos implícitamente supuestos.

Además del propio artículo de Bender [Ben], ha sido necesario desmenuzar el material de otros dos: [Alp] y [Ben II]. También se revisaron los resultados pertinentes de los libros de Gorenstein [Gor], Rotman [Rot] y Suzuki [Suz]. Cuando se consideró conveniente para mejorar la claridad de la exposición o reducir la longitud del trabajo, se han reescrito y/o adecuado fragmentos de pruebas, pruebas completas o incluso el enunciado mismo del resultado. En algunos casos fue necesario conjeturar, enunciar y probar el resultado que hacía falta para completar un argumento. En cada resultado se ha incluido una referencia a la fuente bibliográfica donde se hallan el enunciado y la prueba que más se parecen a los que se presentan. Usamos "[Piz]" para referirnos al presente trabajo cuando no conocemos otra fuente con un resultado semejante.

En los capítulos 0 al 2 presentamos el material preliminar ordenado por temas. Los capítulos 3 al 6 constituyen la prueba de Bender en sí y se corresponden bastante fielmente con las secciones 3 a 6 de [Ben].

0. Notación y resultados básicos

Este capítulo tiene el propósito de introducir la notación y los resultados básicos que se utilizarán a lo largo de toda la tesis y se presentan aquí, por completez y para hacer sobre la marcha algunas observaciones elementales en las que no se suele hacer énfasis en un curso básico. En su mayoría, el material aquí presentado es revisado en un curso básico de teoría de grupos, por ejemplo en la asignatura de *Álgebra Moderna I*, impartida en la Facultad de Ciencias de la UNAM. También en su mayoría, los resultados de este capítulo serán usados más adelante sin referencia explícita.

Se espera sin embargo, para la lectura completa de la tesis, que el lector no sólo esté familiarizado con el material que se aborda normalmente en un curso básico de teoría de grupos, sino que además tenga una madurez matemática propia de un licenciado en matemáticas y una cierta predisposición animosa hacia la teoría de grupos.

En particular, se espera que el lector esté familiarizado con los subgrupos normales, cocientes de grupos, teorema de la correspondencia, los teoremas de isomorfismo, presentaciones de grupos por generadores y relaciones, el teorema fundamental de los grupos abelianos finitos y los teoremas de Sylow. Además se espera que esté familiarizado con los conceptos y resultados más elementales de las teorías de campos, anillos y módulos. Adoptaremos la siguiente convención:

A lo largo de toda la tesis ***grupo*** significa ***grupo finito.***

Dado un grupo G, denotamos a su *orden* por $|G|$. Si x es un elemento de G, denotamos su *orden* por $|x|$ y si K es un subgrupo de G, su *índice* es denotado como $|G:K| := |G|/|K|$. El *exponente* de un grupo G, es el mínimo entero n tal que $x^n = 1$, para toda $x \in G$. A menos que se indique lo contrario usaremos notación multiplicativa. El grupo trivial se representará por 1 en notación multiplicativa y por 0 en notación aditiva.

Denotaremos por Z_n al *grupo cíclico* de n elementos, por S_n al *grupo simétrico* de grado n y, si X es un conjunto, denotamos por S_X al *grupo de permutaciones* de X. Decimos que G es *simple* si no tiene subgrupos normales propios.

Si p es un número primo, $|G|_p$ denota *la parte p del orden de G*, es decir, la máxima potencia de p que divide a $|G|$; decimos que G es un grupo *de tipo* (p,p) si $G \cong Z_p \times Z_p$; en el caso $p = 2$, decimos también que G es un *4-grupo* o un *grupo de Klein*.

G es un *p-grupo* si satisface $|G|_p = |G|$. Un *p-subgrupo* de G es un p-grupo que es subgrupo de G. Un *p-elemento* x de G es un elemento de orden p^n, para algún entero n.

Un *p-subgrupo de Sylow de* G es un subgrupo S de G tal que $|G|_p = |S|$; en este caso, también diremos que S es un *p-Sylow de* G. Denotamos por $Syl_p(G)$ al conjunto de todos los p-Sylows de G.

Si G es un grupo, G^* denota al conjunto $G - \{1\}$; si A es un anillo, A^* denota al conjunto de unidades (elementos invertibles) de A. A menos que se indique lo contrario, Z_n^* representa al grupo de unidades del anillo Z_n, en cualquier otro contexto se interpreta a Z_n como grupo y no como anillo.

Sean x y y elementos de G y A un subgrupo de G. Decimos que $x^y := y^{-1}xy$ es la *conjugación derecha* de x por y, ${}^yx := yxy^{-1}$ es la *conjugación izquierda*, generalmente (cuando en el contexto sea claro) omitiremos los adjetivos *izquierda* y *derecha*, en ambos casos decimos, genéricamente, que x^y y ${}^yx$ son *conjugados* de x. $A^x := x^{-1}Ax := \{x^{-1}ax \mid a \in A\}$ es el *conjugado derecho de* A *por* x y ${}^xA := xAx^{-1} := \{xax^{-1} \mid a \in A\}$ es el *conjugado izquierdo*. Note que el conjugado de un grupo es un grupo y que la conjugación es un isomorfismo.

CONCEPTOS BÁSICOS

Definición 0.1. Sean G un grupo; x, y, z elementos de G; y A, B y C subgrupos de G. Definimos:

(1) $[x,y] = xyx^{-1}y^{-1}$; $[x,y,z] = [[x,y],z]$,

(2) $[A,B] = \langle [a,b] \mid a \in A, b \in B \rangle$; $[A,B,C] = [[A,B],C]$,

(3) $N_B(A) = \{b \in B \mid {}^bA = A\}$,

(4) $C_B(A) = \{b \in B \mid ba = ab \ \ \forall a \in A\}$,

(5) $Z(G) = C_G(G)$,

(6) $G' = [G,G]$.

Decimos que $[x,y]$ es el *conmutador* de x y y, $[A,B]$ es el *conmutador* de A y B, $[x,y,z]$ y $[A,B,C]$ son respectivamente el *triple conmutador* de x, y y z y el *triple conmutador* de A, B y C. De manera semejante se suelen definir los *conmutadores superiores*, pero nosotros no haremos uso de ellos. Notemos que, por definición, el conmutador de A y B es siempre un grupo.

También, por definición, $N_B(A)$ es el *normalizador* de A en B y $C_B(A)$ es el *centralizador* de A en B. Diremos que B *normaliza* a A, si $B \subseteq N_G(A)$ (equivalentemente

$B = N_B(A)$, o bien, $[B, A] \subseteq A$). Claramente las condiciones $A^x = A$, ${}^xA = A$ y ${}^xA \subseteq A$ son equivalentes. Decimos que B *centraliza* a A, si $B \subseteq C_G(A)$ (equivalentemente $B = C_B(A)$, o bien, $[B, A] = 1$). Observe que $N_B(A)$ y $C_B(A)$ son siempre subgrupos de B y que $C_B(A) \lhd N_B(A)$.

Además, diremos que $Z(G)$ es el *centro* de G, y que G' es el *subgrupo derivado* de G. Note que si $A \lhd G$, entonces G/A es abeliano si y sólo si $G' = [G,G] \subseteq A$.

Denotaremos por $Aut(G)$ al grupo de automorfismos de G. Diremos que A es *característico* en G, y denotaremos esta relación por $A \, char \, G$, si $\varphi(A) = A$ para toda $\varphi \in Aut(G)$; Observamos que, como la conjugación es un automorfismo, todo subgrupo característico es normal.

Teorema 0.2. [Gor 2.2.1, 2.2.3] Sean G un grupo; x, y y z elementos de G; y A, B y C subgrupos de G. Entonces:

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

(2) $[x,yz] = [x,y] \cdot {}^y[x,z]$,

(3) $[xy,z] = {}^x[y,z] \cdot [x,z]$,

(4) ${}^x[x^{-1},y,z] \cdot {}^z[z^{-1},x,y] \cdot {}^y[y^{-1},z,x] = 1$,

(5) $[A,B] = [B,A]$,

(6) $[A,B] \lhd \langle A,B \rangle$,

(7) Si $[A,B,C] = 1$ y $[B,C,A] = 1$, entonces $[C,A,B] = 1$.

Demostración.

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

(2) $[x,yz] = xy(x^{-1}y^{-1}yx)zx^{-1}z^{-1}y^{-1} = (xyx^{-1}y^{-1})y(xzx^{-1}z^{-1})y^{-1} = [x,y] \cdot {}^y[x,z]$.

(3) $[xy,z] = xyzy^{-1}(z^{-1}x^{-1}xz)x^{-1}z^{-1} = x(yzy^{-1}z^{-1})x^{-1}(xzx^{-1}z^{-1}) = {}^x[y,z] \cdot [x,z]$.

(4) Si definimos $[[a,b,c]] := aba^{-1}ca$, tenemos:

$$\begin{aligned} {}^x[x^{-1},y,z] &= x[[x^{-1},y],z]x^{-1} = x[x^{-1}yxy^{-1},z]x^{-1} \\ &= x(x^{-1}yxy^{-1}zyx^{-1}y^{-1}xz^{-1})x^{-1} \\ &= (yxy^{-1}zy)(x^{-1}y^{-1}xz^{-1}x^{-1}) \\ &= [[y,x,z]] \cdot [[x,z,y]]^{-1}. \end{aligned}$$

Es decir ${}^x[x^{-1},y,z] = [[y,x,z]] \cdot [[x,z,y]]^{-1}$. De manera semejante,

$${}^z[z^{-1},x,y] = [[x,z,y]] \cdot [[z,y,x]]^{-1}$$

y

$${}^y[y^{-1},z,x] = [[z,y,x]] \cdot [[y,x,z]]^{-1}.$$

Concluimos que ${}^{x}[x^{-1},y,z]\cdot{}^{z}[z^{-1},x,y]\cdot{}^{y}[y^{-1},z,x]=1$.

(5) Según (1), los generadores de $[A,B]$ son simplemente los inversos de los generadores de $[B,A]$.

(6) Claramente $[A,B]$ es un subgrupo de $\langle A,B\rangle$. Si $a,a'\in A$ y $b\in B$, por (3) tenemos: ${}^{a}[a',b]=[aa',b]\cdot[a,b]^{-1}\in[A,B]$. Es decir, A normaliza a $[A,B]$. Usando (2) o (5) concluimos que B también normaliza a $[A,B]$. Por lo tanto, $[A,B]\lhd\langle A,B\rangle$.

(7) Sean $x\in A$, $y\in B$ y $z\in C$. Por hipótesis $[x^{-1},y,z]=1$ y $[y^{-1},z,x]=1$. Sustituyendo en (4), tenemos ${}^{z}[z^{-1},x,y]=1$. Luego, $[z^{-1},x,y]=1$, y concluimos que $[C,A,B]=1$. #

A la afirmación (7) del Teorema anterior, se le llama el *Lema de los tres subgrupos*. El resultado se debe a P. Hall y es considerado muy importante debido a sus múltiples consecuencias (ver por ejemplo [Suz II, p5]); nosotros tendremos ocasión de ver varias de ellas.

El siguiente Lema nos será útil en el estudio de los grupos nilpotentes de clase a lo más 2, que se definirán más adelante.

Lema 0.3. [Gor 2.2.2] Sean G un grupo y $x,y\in G$. Suponga que $z=[y,x]$ conmuta con x y y. Entonces, para toda i y j:

(a) $[y^{i},x^{j}]=z^{ij}$

(b) $(xy)^{i}=z^{i(i-1)/2}x^{i}y^{i}$.

Demostración. Probemos (a):

Procederemos por inducción sobre i:

Como $[y,x]=z$, tenemos $yxy^{-1}x^{-1}=z$, o bien $yxy^{-1}=zx$. Luego $yx^{j}y^{-1}=(yxy^{-1})^{j}$ $=(zx)^{j}=z^{j}x^{j}$, pues x y z conmutan. Entonces $[y,x^{j}]=(yx^{j}y^{-1})x^{-j}=z^{j}x^{j}x^{-j}=z^{j}$, probando con ello el caso base $i=1$. Note que, de paso, obtenemos la identidad $y^{-1}x^{-j}=x^{-j}y^{-1}z^{j}$, que usaremos a continuación.

Usaremos ahora, como hipótesis de inducción que vale la igualdad $y^{i-1}x^{j}y^{-(i-1)}x^{-j}=[y^{i-1},x^{j}]=z^{(i-1)j}$. Entonces $[y^{i},x^{j}]=y^{i}x^{j}y^{-i}x^{-j}=yy^{i-1}x^{j}y^{-(i-1)}(y^{-1}x^{-j})$ $=y(y^{(i-1)}x^{j}y^{-(i-1)}x^{-j})y^{-1}z^{j}=y(z^{(i-1)j})y^{-1}z^{j}=z^{ij}$, pues y y z conmutan.

Probemos ahora (b):
Procederemos por inducción en i:
El resultado es obvio para el caso base $i=1$. Usaremos a continuación, como hipótesis de inducción, que vale la igualdad $(xy)^{i-1} = z^{(i-1)(i-2)/2}x^{i-1}y^{i-1}$. También usaremos la siguiente identidad que se deriva de manera inmediata de (a): $y^{(i-1)}x = y^{(i-1)}xy^{-(i-1)}x^{-1}xy^{(i-1)} = \left[y^{(i-1)},x\right]xy^{(i-1)} = z^{(i-1)}xy^{(i-1)}$. Entonces: $(xy)^i = (xy)^{i-1}(xy)$ $= z^{(i-1)(i-2)/2}x^{(i-1)}\left(y^{(i-1)}x\right)y = z^{(i-1)(i-2)/2}x^{(i-1)}\left(z^{(i-1)}xy^{(i-1)}\right)y = z^{i(i-1)/2}x^iy^i$, pues z y x conmutan. #

Lema 0.4. [Gor 2.1.2] Sean G un grupo y A, B y C subgrupos de G, entonces:

(1) Si C normaliza a A y a B, entonces también normaliza a $N_A(B)$, a $C_A(B)$ y a $[A,B]$.

(2) A *char* $B \lhd G$ implica $A \lhd G$.

(3) A *char* B *char* G implica A *char* G.

(4) A *char* G, $A \subseteq B$ y B/A *char* G/A implican B *char* G.

Demostración. (1) Sean $a \in N_A(B)$ y $c \in C$. Como C normaliza a B, tenemos que $a,c \in N_G(B)$. Entonces $cac^{-1} \in N_G(B)$, además $cac^{-1} \in A$ (pues C normaliza a A). Luego, $cac^{-1} \in A \cap N_G(B) = N_A(B)$. Se sigue que ${}^cN_A(B) = N_A(B)$, para toda $c \in C$. Es decir, C normaliza a $N_A(B)$.

Sean $a \in C_A(B)$ y $c \in C$. Entonces, por hipótesis, $c \in N_G(B) \cap N_G(A)$, y también $a \in C_G(B) \cap A$. Como $C_G(B) \lhd N_G(B)$, tenemos que $cac^{-1} \in C_G(B) \cap A = C_A(B)$. Luego, C normaliza a $C_A(B)$.

Si $[a,b]$ (con $a \in A$ y $b \in B$) es un generador típico de $[A,B]$, tenemos ${}^c[a,b] = \left[cac^{-1},cbc^{-1}\right] \in [A,B]$, y el resultado se sigue.

(2) Como B es normal en G, para cada $x \in G$, podemos definir $\varphi_x : B \to B$, como $\varphi_x(y) = xyx^{-1}$ (para $y \in B$). Claramente $\varphi_x \in Aut(B)$. Como A *char* B, tenemos que $\varphi_x(A) = A$, es decir ${}^xA = A$. Se sigue que A es normal en G.

(3) Sea $\varphi \in Aut(G)$. Como B *char* G, tenemos $\varphi(B) = B$, y podemos tomar la restricción de φ en B; si denotamos por φ_B a esta restricción, tenemos $\varphi_B \in Aut(B)$. Dado que A *char* B resulta $\varphi(A) = \varphi_B(A) = A$.

(4) Sea $\varphi \in Aut(G)$. Definimos: $\overline{\varphi} : G/A \to G/A$, por $\overline{\varphi}(\overline{g}) = \overline{\varphi(g)}$. Veamos que $\overline{\varphi}$ está bien definida: Si $x,y \in G$ y $\overline{x} = \overline{y}$, tenemos $x = ya$ para alguna $a \in A$. Entonces $\varphi(x) = \varphi(ya) = \varphi(y)\varphi(a)$. Como A *char* G, $\varphi(a) \in A$ y en consecuencia $\overline{\varphi}(\overline{x}) = \overline{\varphi(x)}$ $= \overline{\varphi(y)} = \overline{\varphi}(\overline{y})$. También es claro que $\overline{\varphi}$ es un homomorfismo inyectivo, luego $\overline{\varphi} \in Aut(\overline{G})$, con $\overline{G} := G/A$. Si tomamos $\overline{B} := B/A$, tenemos que $\overline{\varphi}(\overline{B}) = \overline{B}$ (pues $\overline{B}$ *char* $\overline{G}$). Luego $\varphi(B) \subseteq BA = B$ y por lo tanto B *char* G. #

ACCIONES Y p-GRUPOS

Definición 0.5. Sean H y K dos grupos y X un conjunto. Una *acción de grupos* de H en K es un homomorfismo de grupos $\varphi: H \to Aut(K)$. Si es claro quién es φ o si no interesa su identidad, diremos simplemente que H *actúa* en K. Una *acción de conjuntos* de H en X es un homomorfismo de grupos $\psi: H \to S_X$ (donde S_X es el grupo de permutaciones de X); igual que antes, a menudo diremos simplemente que H *actúa* en X.

Note que S_X es el grupo de automorfismos del conjunto X en la categoría de conjuntos; asimismo, como $Aut(K)$ siempre es un subgrupo de S_K, tenemos que toda acción de grupos es una acción de conjuntos. Aunque ocasionalmente haremos énfasis en el tipo de acción de que se trate, en general omitiremos los calificativos *de grupos* y *de conjuntos* y dejaremos que sea el contexto el que determine cuál es el tipo de acción en cuestión: Si el objeto en el que se actúa es un conjunto no hay lugar a confusión; si es un grupo, supondremos que se trata de una acción de grupos a menos que se diga explícitamente lo contrario.

Observe que si H es un grupo y N es un subgrupo normal de H, entonces H actúa en N *por conjugación*; es decir, la función $\varphi: H \to Aut(N)$, dada por $\varphi(h)(x) = hxh^{-1}$, es una acción (de grupos) de H en N. También H actúa (con acción de conjuntos) en H *por translación*; esto es, la función $\varphi: H \to S_H$, dada por $\varphi(h)(x) = hx$, es una acción (de conjuntos) de H en H. Lo anterior sugiere notaciones alternativas para una acción dada: si φ es una acción de H en X (de cualquiera de los dos tipos), con $h \in H$ y $x \in X$, denotaremos a $\varphi(h)(x)$ como ${}^h x$ o como $h \cdot x$, siempre que no haya confusión posible.

Definición 0.6. Sea G un grupo, que actúa en un conjunto X y $x \in X$. Definimos:

$$G_x := \{g \in G \mid g \cdot x = x\},$$

$$G \cdot x := \{g \cdot x \mid g \in G\},$$

$$X_0 := \{y \in X \mid g \cdot y = y, \forall g \in G\}.$$

Decimos que G_x es el *estabilizador* de x en G; $G \cdot x$ es la *órbita* de x (*bajo la acción* de G); y X_0 es el *conjunto de puntos fijos* de X (*bajo la acción* de G). Observe que el estabilizador siempre es un grupo; si la acción es de grupos, X_0 también es un grupo; y que el conjunto de todas las órbitas forman una partición de X en clases de equivalencia.

Teorema 0.7. [Suz I, 1.7.12] Sea G un grupo actuando en un conjunto X. Entonces:

(1) $|G \cdot x| = [G:G_x]$, para toda $x \in X$.

(2) Si R es un conjunto de representantes de las clases de equivalencia de X, de tamaño mayor que uno, entonces:

$$|X| = |X_0| + \sum_{x \in R} [G:G_x].$$

Demostración. La biyección entre las clases laterales de G_x en G y los elementos de la órbita de x está dada por: $gG_x \mapsto g \cdot x$. La segunda afirmación se sigue de (1) y de que el conjunto de todas las órbitas de X forman una partición en clases de equivalencia de X. #

A la ecuación del inciso (2) del teorema anterior le llamaremos la *ecuación de clase* (hay casi tantas variantes de la ecuación de clase, todas ellas con el mismo nombre, como autores de libros de teoría grupos).

Note que si un G es un p-grupo, entonces todos los términos que aparecen en la sumatoria son múltiplos de p; si además X es un conjunto de tamaño no divisible por p, esto obliga a que $X_0 \neq \phi$. Del mismo modo, si G y X son p-grupos, y la acción es de grupos, entonces, ésta se restringe a una acción (de conjuntos) de G en $X^* := X - \{1\}$, pero entonces $|X^*|$ no es divisible por p, luego $X_0 \neq 1$. Concluimos que: "*Siempre que un p-grupo actúa en otro, el conjunto de puntos fijos es no trivial*". A lo largo de esta sección, quedará patente la utilidad de las observaciones hechas en este párrafo.

Es apenas creíble la cantidad de resultados importantes que se derivan de esta ecuación tan elemental y, en general, de las técnicas derivadas del concepto de acción. Veremos a lo largo de esta sección varias de sus consecuencias inmediatas y, a lo largo de la tesis, tendremos ocasión de constatar la importancia del concepto de acción. De hecho, como veremos a continuación, la prueba de uno de los teoremas más fundamentales en teoría de grupos finitos, el teorema de Sylow, no precisa esencialmente nada más que la ecuación de clase.

La siguiente prueba de los teoremas de Sylow está basada en una prueba de Wielandt y la presentemos aquí, pese a ser estándar, porque no hemos podido resistirnos a su elegancia.

Teorema 0.8. (Teoremas de Sylow) [Suz I, 2.2.2] Sean G un grupo y p un número primo; entonces:

(1) $|Syl_p(G)| = 1 + kp$, para algún número natural k, y $|Syl_p(G)|$ divide a $|G|$.

(2) Todo p-subgrupo de G está contenido en un p-Sylow de G.

(3) Todos los p-Sylows de G son conjugados entre sí.

Demostración. Sea G un grupo con $|G| = p^a m$ y $(p,m) = 1$. Sea $\mathscr{M} = \{A \subseteq G \mid |A| = p^a\}$. Es fácil y elemental verificar que p no divide a $\binom{p^a m}{p^a}$ (siempre que $(p,m) = 1$). Entonces $p \nmid |\mathscr{M}| = \binom{p^a m}{p^a}$. Si hacemos actuar a G en $\mathscr{M}$, por translación, se sigue que no todas las órbitas de $\mathscr{M}$ tiene un tamaño divisible por p ($\mathscr{M}$ es unión ajena de sus órbitas). Sea $X \subseteq \mathscr{M}$ una de tales órbitas y $A \in X$. Entonces, por el teorema anterior, $|X| = |G:G_A|$, como $p \nmid |X|$, tenemos que p^a divide a $|G_A|$ y, en particular, $p^a \leq |G_A|$. También podemos hacer actuar a G_A en A por translación, y entonces, si $a \in A$, tenemos $G_A \cdot a \subseteq A$ y $|G_A| = |G_A \cdot a| \leq |A| = p^a$. Se sigue que $|G_A| = p^a = |G|_p$ y así hemos construido un p-subgrupo de Sylow de G, a saber: G_A. En adelante, llamaremos P a ese subgrupo de Sylow.

Sea $\mathscr{S} = \{P^g \mid g \in G\}$. Si hacemos actuar a P en $\mathscr{S}$ por conjugación, tenemos de la ecuación de clase:

$$|\mathscr{S}| = |\mathscr{S}_0| + \sum_{X \in R} |P:P_X|$$

Pero $\mathscr{S}_0 = \{P\}$, pues si P' es otro elemento de $\mathscr{S}$ que se queda fijo bajo la acción de P, entonces P' es normalizado por P y PP' es un p-grupo. Luego $P \subseteq PP'$ y $|PP'| \leq p^a$ implican $P = P'$. Entonces:

$$|\mathscr{S}| = 1 + \sum_{X \in R} |P:P_X| \equiv 1 \bmod p$$

Sea B un p-subgrupo de G. Entonces, también B actúa en $\mathscr{S}$ por conjugación. Si $P' \in \mathscr{S}$ se queda fijo bajo la acción de B, entonces P' es normalizado por B y BP' es un p-grupo, luego $P' \subseteq BP'$ y $|BP'| \leq p^a$ implican que $BP' = P'$ y $B \subseteq P'$, con lo que todo p-subgrupo de G estaría contenido en un p-Sylow de G (conjugado a P). Si ése no fuera el caso, otra vez por la ecuación de clase, tendríamos:

$$|\mathscr{S}| = 0 + \sum_{X \in R} |B:B_X| \equiv 0 \bmod p$$

contrario a lo que sabemos. Entonces B está contenido en algún conjugado de P; en particular, todos los p-subgrupos de Sylow de G son conjugados entre sí y $\mathscr{S}$ es el conjunto de todos los p-Sylows de G. Finalmente, también por el teorema anterior (con G actuando en $\mathscr{S}$ por conjugación), tenemos $|\mathscr{S}| = |G:G_P|$, luego $|\mathscr{S}|$ divide a $|G|$. #

El siguiente lema presenta tres resultados elementales que son útiles con frecuencia.

Lema 0.9. [Suz I, 2.2.6] Sean G un grupo, $K \lhd G$, $G_p \in Syl_p(G)$ y $\pi: G \to G/K$ la proyección natural, entonces:

(1) $\pi(G_p) \in Syl_p(G/K)$.

(2) $K \cap G_p \in Syl_p(K)$.

(3) $G_p \lhd G$ si y sólo si G_p *char* G.

Demostración.
(1) Tenemos que:

$$|G/K : \pi(G_p)| = |G/K : (G_pK)/K| = \frac{|G|/|K|}{|G_p|/|K \cap G_p|} = \frac{|G|}{|G_p|} \cdot \frac{|K \cap G_p|}{|K|}$$

no puede ser divisible por p, pues $|K \cap G_p|$ es un divisor de $|K|$.

(2) Por otro lado, $K \cap G_p \subseteq K_p \subseteq G_p^x$, para algunas $K_p \in Syl_p(K)$ y $x \in G$. Luego, $G_p^x \cap K = K_p \in Syl_p(K)$. Como K es normal en G, conjugando por $y := x^{-1}$, tenemos $G_p \cap K = K_p^y \in Syl_p(K)$.

(3) Es obvio que G_p *char* G implica $G_p \lhd G$. Si $G_p \lhd G$, entonces, por los Teoremas de Sylow (todos los p-Sylows son conjugados entre sí), G_p es el único p-subgrupo de Sylow de G. Si $\varphi \in Aut(G)$, entonces $|\varphi(G_p)| = |G_p|$, luego $\varphi(G_p)$ también es un p-Sylow de G. Entonces $\varphi(G_p) = G_p$, es decir G_p *char* G. #

El siguiente resultado fundamental es considerado como una aplicación típica de los Teoremas de Sylow y nos será útil más adelante.

Teorema 0.10. (Argumento de Frattini) [Gor 1.3.7] Si $H \lhd G$ y P es un p-Sylow de H, entonces $G = HN_G(P)$.

Demostración. Sea $g \in G$. Como H es normal, $gPg^{-1} \subseteq H$, pero entonces gPg^{-1} es también un subgrupo de Sylow de H y tiene que ser conjugado a P en H, esto es: $gPg^{-1} = hPh^{-1}$ para alguna $h \in H$. Entonces, $h^{-1}gP(h^{-1}g)^{-1} = P$ y, así, $h^{-1}g \in N_G(P)$. Luego, $g = hn$, para alguna $n \in N_G(P)$, por tanto $G = HN_G(P)$. #

El lema siguiente, presenta una serie de resultados básicos sobre p-grupos que se derivan de la ecuación de clase.

Lema 0.11. [Suz I, 2.1.4; 2.1.6; 2.1.13] Sean P un p-grupo no trivial y K un subgrupo de P. Entonces:

(1) $1 \neq K \lhd P$ implica $K \cap Z(P) \neq 1$. En particular, $Z(P) \neq 1$.

(2) Si K es un subgrupo normal minimal en P, entonces $K \subseteq Z(P)$ y $K \cong Z_p$.

(3) $K \subsetneq P$ implica $K \subsetneq N_P(K)$.

(4) Si K es maximal en P, entonces $K \lhd P$ y $|P:K| = p$.

Demostración.

(1) Por la ecuación de clase, haciendo actuar a P en K por conjugación, tenemos:

$$|K| = |K_0| + \sum (\text{términos divisibles por } p)$$

Donde K_0 es el conjunto de puntos fijos de la acción. Como el orden de K es divisible por p, resulta que el orden de K_0 debe serlo a su vez. Como $1 \in K_0$, tenemos: $|K_0| \geq p$. Pero el conjunto de puntos fijos de la conjugación resulta ser $K_0 = C_K(P) = K \cap Z(P)$.

(2) Gracias a (1), tenemos $1 \neq K \cap Z(P) \lhd P$, luego, por la minimalidad de K, tenemos $K = K \cap Z(P) \subseteq Z(P)$. Entonces cualquier subgrupo de K es normal en P. De nuevo por la minimalidad de K, se sigue que K no tiene ningún subgrupo propio, es decir $K \cong Z_p$.

(3) Si $K \lhd P$, el resultado se sigue inmediatamente. Supongamos que $K \not\lhd P$. Sean $X := \{K^x \mid x \in P\}$ y $X' := X - \{K\}$. Entonces P actúa en X por conjugación, y X es la órbita de K bajo la acción de P. Sea P_K el estabilizador de K en P. Entonces $P_K = N_P(K)$ y, por el Teorema 0.7.(1), $1 \neq |X| = [P:P_K] = [P:N_P(K)] \equiv 0 \bmod p$. Luego $|X'| \equiv -1 \bmod p$. Ahora, K actúa en X', también por conjugación y de la ecuación de clase, tenemos:

$$|X'| = |X'_0| + \sum (\text{términos divisibles por } p)$$

Se sigue que $X'_0 \neq \phi$. Entonces K normaliza a alguna $K^x \neq K$ con $x \in P$. Tomando $y := x^{-1}$ resulta que K^y normaliza a K. Luego $K^y \subseteq N_P(K)$, es decir $K \subsetneq N_P(K)$.

(4) Si K es maximal en P, entonces, por (3), tenemos que $K \subsetneq N_P(K) \subseteq P$. Esto implica que $N_P(K) = P$, o bien $K \lhd P$. Por la maximalidad de K, P/K no tiene subgrupos propios, así $P/K \cong Z_p$ y por lo tanto $|P:K| = p$. #

Definición 0.12. Sean G un grupo y $\mathscr{M}$ una sucesión de subgrupos de G, de la forma:

$$\mathscr{M}:\ 1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G.$$

Entonces decimos que la *serie* $\mathscr{M}$ es *normal*, si $G_i \lhd G$ para toda i; *subnormal*, si $G_i \lhd G_{i+1}$ (para toda i); *de composición*, si es subnormal y cada G_{i+1}/G_i es simple; y *principal*, si es normal y de composición. En cualquiera de estos casos diremos que la longitud de la serie es n.

Presentamos a continuación una versión especialmente adaptada para p-grupos de los teoremas clásicos de Jordan-Hölder y Schreier que nos será útil repetidas veces.

Teorema 0.13. [Suz I, 2.1.12] Sea P un p-grupo de orden p^n, entonces:

(1) P tiene una serie principal de longitud n: $1 = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$. Se sigue que $P_i \lhd P$ y $|P_i : P_{i-1}| = p$, para toda i.

(2) Si $1 \subseteq P^0 \subsetneq P^1 \subsetneq \cdots \subsetneq P^r \subseteq P$ es una serie normal de P, entonces existe una serie principal de P de longitud n, que incluye a todos los P^i, para $0 \le i \le r$.

Demostración. Observe que (2) implica (1) (tomando la serie $1 = P^0 \subsetneq P^1 = P$, si $P \neq 1$).

Probemos (2). Procederemos por inducción en $|P|$. Sin pérdida de generalidad, podemos suponer que $P^0 \neq 1$. Sea N un subgrupo normal minimal de P que esté contenido en P^0. Por el Lema 0.11.(2), $N \cong Z_p$. Ahora, por hipótesis de inducción, P/N tiene una serie principal $1 = \overline{P_1} \subsetneq \ldots \subsetneq \overline{P_n} = P/Q$, de longitud $n-1$, que incluye a $\overline{P^0}, \ldots, \overline{P^r}$ (las imágenes de $P^0, \ldots, P^r$, bajo la proyección natural). Si ahora, para cada $i = 1, \cdots, n$, P_i es la imagen inversa de $\overline{P_i}$ según la proyección natural, entonces $1 = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$ es la serie deseada. #

Las acciones también nos permiten construir nuevos grupos a partir de grupos conocidos por medio del producto semidirecto, como se verá a continuación.

Teorema 0.14. [Gor 2.5.1] Sean H y K dos grupos y φ una acción de grupos de K en H. Entonces, el producto cartesiano $H \times K$, junto con la operación binaria definida por $(h', k)(h, k') = (h'({}^k h), kk')$ (recuerde que, en este caso, ${}^k h := \varphi(k)(h)$) es un grupo. Llamemos G al grupo así obtenido. Sean $i_1 : H \to H \times K$ e $i_2 : K \to H \times K$ las inclusiones naturales, $\overline{H} := i_1(H)$ y $\overline{K} := i_2(K)$ entonces:

(1) $G = \overline{H}\,\overline{K}$.

(2) $\overline{H} \lhd G$, $\overline{K} \subseteq G$.

(3) $\overline{H} \cap \overline{K} = 1$.

(4) La acción de K en H, se transforma (vía las inclusiones naturales) en la conjugación de $\overline{H}$ por elementos de $\overline{K}$.

Demostración. La demostración es una verificación de rutina. Ver por ejemplo [Gor 2.5.1]. #

Definición 0.15. Al grupo G del teorema anterior se le llama *un producto semidirecto (externo)* de H y K, y se denota por $H \rtimes K$. Cuando se quiere hacer énfasis en la acción que se utiliza, escribimos $H \rtimes_{\varphi} K$, y decimos que el grupo en cuestión es *el producto semidirecto* de H y K *respecto* a φ. También, si G es cualquier grupo y $\overline{H}$ y $\overline{K}$ son dos subgrupos cualesquiera de G que satisfacen (1)-(3) del teorema anterior, entonces decimos que G es *producto semidirecto (interno)* de $\overline{H}$ y $\overline{K}$ (en este caso $G \cong \overline{H} \rtimes_{\varphi} \overline{K}$, donde φ es la acción dada por la conjugación en $\overline{H}$ por elementos de $\overline{K}$).

Nota: Se suelen identificar los grupos H y K con $\overline{H}$ y $\overline{K}$ respectivamente, siempre que ello no cause confusión. Una vez hecho eso "desaparece la diferencia" entre los productos semidirectos externo e interno. Así, siempre que tengamos que un grupo K actúa en otro grupo H, podremos considerar que ambos son subgrupos de un tercer grupo $G = H \rtimes K$, de esta manera, podemos extender conceptos básicos como los *normalizadores*, *centralizadores*, *conmutadores*, etc. y las relaciones *normalizar*, *centralizar*, *conjugar*, etc. En particular, *actuar* y *normalizar* resultan ahora ser "sinónimos". Sin embargo, hay que tener cuidado si, por ejemplo, H y K ya son subgrupos de un cierto grupo G y la acción considerada de K en H no es la conjugación, o H y K se intersectan de manera no trivial. Note también que la notación $H \rtimes K$ puede representar varios grupos distintos (no isomorfos) según cuál sea la acción considerada. En particular, el producto directo de H y K siempre es un producto semidirecto de H y K (tomando la acción trivial).

El siguiente lema, que nos será útil más adelante, es un ejemplo más de una aplicación típica de la ecuación de clase, que además ilustra las convenciones del párrafo anterior.

Lema 0.16. [Piz 0.16] Suponga que un q-grupo Q actúa en el grupo L, con $|L| = kp^a$, donde p es un número primo, no necesariamente distinto de q. Suponga también que $q \nmid k$. Entonces Q normaliza a algún p-subgrupo de Sylow de L.

Demostración. Sea X el conjunto de todos los p-subgrupos de Sylow de L, entonces Q actúa en X (con acción de conjuntos) y por la ecuación de clase: $|X| = |X_0| + qs$, donde X_0 es el conjunto de todos los p-subgrupos de Sylow de L normalizados por Q. Por los teoremas de Sylow, $|X|$ divide a k, y en particular, $q \nmid |X|$. Se sigue que $|X_0|$ no puede ser cero. #

Los siguientes dos teoremas también ilustran el uso que haremos de las convenciones que aparecen en la nota de la definición del producto semidirecto; el segundo de ellos será uno de los teoremas más citados en la tesis. Necesitamos una definición:

Definición 0.17. Se dice que un grupo A que actúa en el grupo G *estabiliza* la serie subnormal: $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = 1$, si cada G_i es A-invariante y A actúa trivialmente en cada G_i/G_{i+1}.

Teorema 0.18. [Gor 5.3.1] Un grupo A que actúa en el grupo G estabiliza la serie subnormal: $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$ de G si y sólo si cada G_i es A-invariante y $[A, G_i] \subseteq G_{i+1}$ para toda i.

Demostración. A actúa trivialmente en cada G_i/G_{i+1} si y solamente si, para toda $\phi \in A$ y $g \in G_i$ existe una $g' \in G_{i+1}$ tal que $\phi(g) = g'g$, lo que es equivalente a $\phi(g)g^{-1} \in G_{i+1}$ o bien $\phi g \phi^{-1} g^{-1} \in G_{i+1}$ (recuerde que en el producto semidirecto de G_i con A, la acción de A se ve como conjugación) y esto último es equivalente a $[A, G_i] \subseteq G_{i+1}$. #

Teorema 0.19. [Gor 5.3.2] Sea A un p'-grupo que actúa en el p-grupo P. Si A estabiliza alguna serie subnormal de P, entonces A actúa trivialmente en P.

Demostración. Sea $P = P_0 \rhd P_1 \rhd \ldots \rhd P_n = 1$ la serie subnormal que A estabiliza. Procederemos por inducción.

A actúa en P_1 y actúa trivialmente en $P_n/1 = P_n$ (caso base). Además, A actúa trivialmente en P_1, por hipótesis de inducción. También, A actúa trivialmente en P_0/P_1 por hipótesis. Entonces, para toda $\phi \in A$ y $x \in P_0 = P$ se satisface $[\phi, x] \in P_1$, por el Teorema 0.18. Así, $\phi(x) = xz$ para alguna $z \in P_1$. Como ϕ actúa trivialmente en P_1 tenemos: $\phi^n(x) = xz^n$. Si tomamos n igual al orden de ϕ, resulta $x = \phi^n(x) = xz^n$. Luego, $z^n = 1$; pero $(n, p) = 1$ implica $z = 1$. Entonces $\phi(x) = x$. Y en consecuencia, A actúa trivialmente en P. #

SOLUBILIDAD Y NILPOTENCIA

Definición 0.20. Definimos la *serie central descendente* $G = L_0(G) \supseteq L_1(G) \supseteq L_2(G) \supseteq \ldots$, la *serie central ascendente* $1 = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \ldots$ y la *serie derivada* $G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \ldots$, por medio de las siguientes igualdades:

$$\text{(I)} \quad \begin{cases} L_0(G) = G \\ L_{i+1}(G) = [L_i(G), G] \end{cases} \qquad \text{(II)} \quad \begin{cases} Z_0(G) = 1 \\ \dfrac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\dfrac{G}{Z_i(G)}\right) \end{cases} \qquad \text{(III)} \quad \begin{cases} G^{(0)} = G \\ G^{(i+1)} = [G^{(i)}, G^{(i)}] \end{cases}$$

Note que $Z_1(G) = Z(G)$ y $G^{(1)} = G' = L_1(G)$. Teniendo en mente el Lema 0.4., es fácil ver que todos los $L_i(G)$, $Z_i(G)$ y $G^{(i)}$ son característicos en G.

Definición 0.21. Decimos que un grupo G es *nilpotente* si $Z_k(G) = G$ para algún entero k. Al mínimo entero k con esa propiedad se le llamará la *clase* del grupo nilpotente G; denotaremos a la clase de G por $cl(G)$. Diremos que G es *soluble*, si $G^{(s)} = 1$ para algún entero s.

Observe que $G = 1$ si y sólo si $cl(G) = 0$, y que G es abeliano si y sólo si $cl(G) = 1$.

Tenemos el siguiente teorema, fundamental para el estudio de los grupos nilpotentes.

Teorema 0.22. [Suz II, 4.2.5; Suz II, 4.2.12] Sea G un grupo. Entonces, las siguientes condiciones son equivalentes y caracterizan la nilpotencia:

(1) $Z_r(G) = G$, para algún entero r.

(2) $L_r(G) = 1$, para algún entero r.

(3) Para todo subgrupo propio H de G, $H \subsetneq N_G(H)$.

(4) Si H es un subgrupo maximal en G, entonces $H \lhd G$.

(5) $H \in Syl_p(G)$ implica $H \lhd G$.

(6) G es producto directo de sus Sylows.

Demostración.

(1)⇒(2) Probaremos que si (1) vale, entonces $L_j(G) \subseteq Z_{r-j}(G)$, para toda j. Esto implica el resultado deseado. Procederemos por inducción en j.
Si $j = 0$, $L_0(G) = G = Z_r(G)$, por hipótesis. Supongamos, por hipótesis de inducción, que $L_j(G) \subseteq Z_{r-j}(G)$. Como

$$\frac{Z_{r-j}(G)}{Z_{r-j-1}(G)} = Z\left(\frac{G}{Z_{r-j-1}(G)}\right),$$

tenemos que $L_{j+1}(G) = [L_j(G), G] \subseteq [Z_{r-j}(G), G] \equiv 1 \bmod Z_{r-j-1}(G)$. Así, resulta que $L_{j+1}(G) \subseteq Z_{r-j-1}(G)$, completando con ello la inducción.

(2)⇒(3) Como $L_0(G) = G$ y $L_r(G) = 1$, existe un entero k tal que $L_k(G) \not\subseteq H$ y $L_{k+1}(G) \subseteq H$. Luego $[L_k(G), H] \subseteq [L_k(G), G] \subseteq L_{k+1}(G) \subseteq H$. Esto quiere decir que $L_k(G) \not\subseteq H$ normaliza a H. Entonces $H \subsetneq N_G(H)$.

(3)⇒(4) Si H es un subgrupo maximal de G, por (3), tenemos que $H \subsetneq N_G(H) \subseteq G$ implica $N_G(H) = G$. Luego $H \lhd G$.

(4)⇒(5) Suponga que $H \in Syl_p(G)$ y $H \not\lhd G$. Entonces $N_G(H) \subsetneq G$. Sea M un subgrupo maximal de G que contenga a $N_G(H)$. Claramente $H \in Syl_p(M)$, y por (4), $M \lhd G$. Luego, por el argumento de Frattini, $G = MN_G(H) = M$, contrario a la elección de M.

(5)⇒(6) Obvio.

(6)⇒(1) Sea $G = P_1 \times P_2 \times \cdots \times P_s$ la descomposición como producto de Sylows de G. Es fácil verificar que $Z_k(G) = Z_k(P_1) \times Z_k(P_2) \times \cdots \times Z_k(P_s)$ para toda k. Es claro, por el Lema 0.11.(1), que todo p-grupo es nilpotente. Entonces podemos tomar $c = \max_{1 \le i \le s}\{cl(P_i)\}$ y así, $Z_c(G) = G$. #

Nota: Si $c = cl(G)$, en la parte "(1)⇒(2)" de la demostración del teorema anterior se prueba que $L_j(G) \subseteq Z_{c-j}(G)$ para toda j. Se sigue inmediatamente que si k es el mínimo número entero tal que $L_k(G) = 1$, entonces $k \le c$. De hecho es bien sabido que $k = c$, pero nosotros no haremos uso de ello.

También son útiles las siguientes propiedades de los grupos nilpotentes.

Lema 0.23. [Gor 2.3.3; Suz II, 4.2.14]

(1) Todo p-grupo es nilpotente.

(2) Cualquier subgrupo o imagen homomorfa de un grupo nilpotente es nilpotente.

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

(4) Sean G un grupo y H y K dos subgrupos nilpotentes y normales en G. Entonces también HK es nilpotente.

Demostración.

(1) En un p-grupo, el único Sylow es normal.

(2) Si H es un subgrupo de G, tenemos $L_k(H) \subseteq L_k(G)$. Si $N \lhd G$, entonces $(L_k(G)N)/N = L_k(G/N)$.

(3) Inmediato del Teorema 0.22.(6).

(4) Sean P_1 un p-Sylow de H y P_2 un p-Sylow de K. Entonces, como H y K son nilpotentes, P_1 *char* H y P_2 *char* K. Como H y K se normalizan mutuamente, P_1 y P_2 son subgrupos normales de HK. Ahora $P := P_1P_2 \in Syl_p(HK)$ y $P \lhd HK$. Ya que esto sucede para cada primo p, HK satisface la propiedad (5) del Teorema 0.22. #

A continuación se presentan algunas propiedades básicas de los grupos solubles que se derivan directamente de la definición.

Teorema 0.24. [Gor 2.4.1]

(1) Todo grupo nilpotente (y todo p-grupo) es soluble.

(2) Todo subgrupo e imagen homomorfa de un grupo soluble son solubles.

(3) Sean G un grupo y $N \lhd G$. Si N y G/N son solubles, entonces G también lo es.

(4) El producto directo de solubles es soluble.

(5) Si G es soluble no trivial, entonces $[G,G] \subsetneq G$.

Demostración.

(1) $G^{(k)} \subseteq L_k(G)$, para toda k.

(2) De manera semejante que en el Lema 0.23.(2).

(3) Si $(G/N)^{(k)} = 1$, $G^{(k)} \subseteq N$. Entonces $G^{(k+a)} \subseteq N^{(a)}$.

(4) Inmediato de (3).

(5) Inmediato de la definición. #

SUBGRUPOS NOTABLES

Definición 0.25. Sea π un conjunto de primos. Un *π-grupo* es un grupo cuyo orden es divisible solamente por los primos de π, un *π'-grupo* es un grupo cuyo orden sólo es divisible por los primos que no están en π. En el caso $\pi = \{p\}$, escribimos *p-grupo* (lo que coincide con nuestra definición previa) y *p'-grupo* respectivamente. Para cualquier grupo G, $\pi(G)$ denota el conjunto de primos que dividen a su orden.

Definición 0.26. Sean G un grupo y π un conjunto de primos; definimos $O_\pi(G)$ como el (único) π-subgrupo normal maximal de G, y $O_{\pi'}(G)$ como el (único) π'-subgrupo normal maximal. Cuando $\pi = \{p\}$, escribimos solamente $O_p(G)$ y $O_{p'}(G)$ respectivamente.

Definición 0.27. El *subgrupo de Fitting* de un grupo G, $F(G)$, es el (único) subgrupo nilpotente y normal maximal.

Nota: Claramente, $O_\pi(G)$, $O_{\pi'}(G)$ y $F(G)$ existen y son característicos (ver el Lema 0.23.(4)). Observe que, para cualquier grupo G, $O_p(G/O_p(G)) = 1$. Además $O_p(G)$ debe estar contenido en todos los p-subgrupos de Sylow de G.

Teorema 0.28. [Suz II, 4.2.17] $F(G) = \underset{p\in\pi(G)}{\times} O_p(G)$.

Demostración. Observamos que cada $O_p(G)$ es un p-grupo y por tanto es nilpotente, entonces $O_p(G) \subseteq F(G)$ para toda p. Además, cada $O_p(G)$ es normal en G, luego, $\underset{p\in\pi(G)}{\times} O_p(G) = = \langle O_p(G) \mid p \in \pi(G) \rangle \subseteq F(G)$. Por otro lado, cada p-Sylow de $F(G)$, F_p , es normal en $F(G)$ y, por tanto, característico en $F(G)$; como $F(G)$ es a su vez característico en G , cada F_p es característico en G y en particular normal. Luego $F_p \subseteq O_p(G)$ para toda p, y así tenemos: $F(G) \subseteq \underset{p\in\pi(G)}{\times} O_p(G)$. #

El siguiente resultado es una de las propiedades más importantes de los grupos solubles y es usado tantas veces durante el presente trabajo (algunas veces sin referencia explícita) que conviene aprenderlo y tenerlo presente.

Teorema 0.29. [Gor 6.1.3] Sea G un grupo soluble, entonces: $C_G(F(G)) \subseteq F(G)$. En particular, si G es un grupo soluble no trivial, $F(G) \neq 1$.

Demostración. Sean $F = F(G)$ y $C = C_G(F(G))$.

Demostraremos que $C \subseteq F$.

Claramente $C \lhd G$.

Para llegar a una contradicción, suponga que $C \not\subseteq F$.

Sea $B \subseteq C$, $B \lhd G$, $B \not\subseteq F$ minimal respecto a estas tres condiciones (B existe pues C cumple con las tres condiciones). Luego: $[B,B] \subseteq C$ y $[B,B] \lhd G$ obviamente, además $[B,B] \subsetneq B$ por ser B soluble. Por la minimalidad de B, tenemos $[B,B] \subseteq F$, y así: $[B,B,B] \subseteq [F,B] \subseteq [F,C] = 1$.

Entonces B es nilpotente y normal en G, es decir: $B \subseteq F$, contrario a lo supuesto. #

En el caso de un grupo nilpotente G, el Teorema anterior es inútil, pues en ese caso $F(G) = G$. El siguiente es un resultado análogo (más elemental y menos poderoso) para p-grupos.

Teorema 0.30. [Gor 5.3.12] Si M es un subgrupo del p-grupo P, maximal respecto a la propiedad de ser abeliano y normal, entonces $C_P(M) = M$.

Demostración. Supongamos que $C_P(M)$ contiene propiamente a M. Como $C_P(M)$ es normal en P, entonces, por el Teorema 0.13., tiene que existir un grupo N tal que $M \subseteq N \subseteq C_P(M)$ con $|N:M| = p$, y $N \lhd P$. Tómese ahora una $x \in N - M$, entonces $N = \langle M, x \rangle$ debe ser abeliano, pues $x \in N \subseteq C_P(M)$ contradiciendo la maximalidad de M. #

Definición 0.31. Sea G un grupo. Definimos $O_{p,q}(G)$ como el único subgrupo de G (necesariamente característico por el Lema 0.4.) tal que $O_{p,q}(G)/O_p(G) = O_q(G/O_p(G))$.

Nota: Observe que $O_{p,q}(G) = O_p(G) \rtimes Q$, para algún q-subgrupo Q de G. También:

$$O_q(G/O_{p,q}(G)) \cong O_q\left(\frac{G/O_p(G)}{O_q(G/O_p(G))}\right) = 1.$$

Definición 0.32. Un grupo es *elementalmente abeliano* si es isomorfo a algún $(Z_p)^\alpha$ para algún primo p y algún entero α. El *rango* de un p-grupo elementalmente abeliano es su dimensión como espacio vectorial sobre Z_p. El *p-rango* de un grupo G, denotado por $r_p(G)$, es el máximo entre los rangos de sus p-subgrupos elementalmente abelianos; escribiremos $r(G)$ si G es un p-grupo.

Definición 0.33. Si P es un p-grupo, definimos: $\Omega_1(P) = \langle x \in P \mid |x| = p \rangle$.

Note que $\Omega_1(P)$ *char* P y que $P \neq 1$ implica $\Omega_1(P) \neq 1$. Si P es abeliano, $\Omega_1(P)$ es elementalmente abeliano de rango máximo en P. En particular $P \neq 1$ implica que $\Omega_1(Z(P)) \neq 1$ es elementalmente abeliano. El siguiente teorema nos da más información del comportamiento de $\Omega_1(P)$ en un caso un poco más general que cuando P es abeliano.

Teorema 0.34. [Gor 5.3.9] Sea P un p-grupo de clase a lo más 2, $p \neq 2$. Entonces:

i) $\Omega_1(P)$ tiene exponente p.

ii) Si $P/Z(P)$ es elementalmente abeliano, entonces $(xy)^p = x^p y^p \quad \forall x, y \in P$.

Demostración. Como P es de clase a lo más 2, tenemos $[P,P,P] = 1$. Luego, si $z = [y,x]$, con x y y en P, entonces $z \in P' \subseteq Z(P)$ y por lo tanto, z conmuta con x y y.

Entonces, por el Lema 0.3.:

a) $[y^i, x^j] = z^{ij}$

b) $(xy)^i = z^{i(i-1)/2} x^i y^i$

Para probar que $\Omega_1(P)$ tiene exponente p, necesitamos probar que el producto de dos elementos de orden p es a su vez de orden p. Si x y y tienen orden p, tenemos de (a):

$$1 = [1,x] = [y^p, x] = z^p .$$

y usando también (b):

$$(xy)^p = z^{p\frac{(p-1)}{2}} x^p y^p = z^{p\frac{(p-1)}{2}} = 1 .$$

Así, $\Omega_1(P)$ es de exponente p.

Para finalizar, si $P/Z(P)$ es elementalmente abeliano y $y \in P$, $y^p \equiv 1 \bmod Z(P)$. Luego, $y^p \in Z(P)$, y $1 = [y^p, x] = z^p$. Por (b): $(xy)^p = x^p y^p$. #

Corolario 0.35. [Piz 0.35] Si $p \neq 2$ y $G \cong (Z_p \times Z_p) \rtimes Z_p$, entonces G tiene exponente p.

Demostración. Si G es abeliano, el resultado es claro. Si no, como G es un p-grupo, tenemos $Z(G) \neq 1$, luego $G/Z(G)$ es abeliano (pues $|G/Z(G)| \leq p^2$). Entonces $Z_2(G) = G$ y $cl(G) = 2$. El teorema anterior nos dice que $\Omega_1(G)$ tiene exponente p, pero en este caso $\Omega_1(G) = G$. #

Definición 0.36. *Contrario a la literatura estándar*, si P es un p-grupo, definimos:

$$J(P) = \langle A \subseteq P \mid A \text{ es elementalmente abeliano y } r(A) = r(P) \rangle.$$

Nota: Observe que $J(P)$ *char* P y que $J(P) \subseteq U \subseteq P$ implica $J(P) = J(U)$. Si G_p es un p-Sylow de G, son equivalentes:

(1) $J(G_p)$ *char* G,
(2) $J(G_p) \lhd G$ y
(3) $J(G_p) \subseteq O_p(G)$.

(1)$\Rightarrow$(2) y (2)$\Rightarrow$(3) son claras. Veamos (3)$\Rightarrow$(1). Si vale (3), entonces $J(G_p) \subseteq O_p(G) \subseteq G_p$, (pues $O_p(G)$ debe estar contenido en todos los p-Sylows de G); luego $J(G_p) = J(O_p(G))$, pero sabemos que $J(O_p(G))$ *char* $O_p(G)$ *char* G.

Observe también que, si p divide al orden de G y G no es un p-grupo, entonces $1 \neq J(G_p) \neq G$. La prueba del teorema de Burnside en el caso $q = 2$, se basa fuertemente en estas observaciones, probando que si G es un contraejemplo minimal al teorema de Burnside, entonces G debe ser simple y $J(G_p)$ debe ser normal en G, lo que constituye una contradicción.

Definición 0.37. Sea G un grupo. Definimos el *subgrupo de Frattini de* G, denotado por $\Phi(G)$, como la intersección de todos los subgrupos maximales de G.

El siguiente teorema establece dos de las principales propiedades del subgrupo de Frattini.

Teorema 0.38. [Gor 5.1.3] Sea G un grupo. Entonces $\Phi(G)$ *char* G. Si G es un p-grupo, $G/\Phi(G)$ es elementalmente abeliano.

Demostración. La primera afirmación es obvia pues todo automorfismo manda subgrupos maximales en subgrupos maximales. Sean G un p-grupo y M un subgrupo maximal de G. Por el Lema 0.11.(4), M es normal en G y tiene índice igual a p. Entonces $G/M \cong Z_p$, luego, si $x, y \in G$, tenemos $x^p, y^p \in M$ y $xyx^{-1}y^{-1} \in M$. Como esto sucede para cualquier maximal M de G obtenemos el resultado deseado. #

GRUPOS ESPECIALES

Definición 0.39. La *función φ de Euler* se define, para cualquier entero positivo n, como:

$$\varphi(n) = \left|\left\{x \in Z \middle| 1 \le x \le n, (n,x) = 1\right\}\right|.$$

Teorema 0.40. [Suz I, 1.6.10] $Aut(Z_n) \cong Z_n^*$, donde Z_n^* es el grupo multiplicativo de las unidades de Z_n (como anillo). $|Aut(Z_n)| = \varphi(n)$. Si la factorización en primos de n es $n = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$, tenemos $\varphi(n) = p_1^{n_1-1} \cdot (p_1 - 1) \cdot p_2^{n_2-1} \cdot (p_2 - 1) \cdots p_k^{n_k-1} \cdot (p_k - 1)$. Si $n = p^\alpha$, para un primo $p \neq 2$, $Aut(Z_n)$ es cíclico.

Demostración. Un automorfismo de Z_n está determinado por la imagen de la unidad de Z_n; la imagen debe ser un generador de Z_n, es decir una unidad del anillo. Entonces cada automorfismo determina, de esta manera, una unidad. La función correspondiente (de $Aut(Z_n)$ en Z_n^*) resulta ser un isomorfismo de grupos. Claramente $|Z_n^*| = \varphi(n)$. Si n y m son primos entre sí, tenemos $Z_{nm} \cong Z_n \times Z_m$, en donde cada factor es un subgrupo característico (todo grupo cíclico tiene un único subgrupo de cada orden que divide al orden del cíclico), luego $Aut(Z_{nm}) \cong Aut(Z_n) \times Aut(Z_m)$. En particular, si $(n,m) = 1$, $\varphi(nm) = \varphi(n)\varphi(m)$. Si $n = p^\alpha$, observamos que el número de enteros entre 1 y n que son divisibles por p es $p^\alpha / p = p^{\alpha-1}$, luego $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$. La prueba de la última afirmación es esencialmente aritmética y puede ser encontrada en [Rot 7.2]. #

Lema 0.41. [Suz II, 4.4.4] Sean p un número primo y K un p-grupo no trivial. Entonces:

(i) K tiene un único subgrupo de orden p si y sólo si no tiene subgrupos de tipo (p, p).

(ii) Si $p \neq 2$, entonces K es cíclico si y sólo si tiene un único subgrupo de orden p.

Demostración. Probemos primero (i):

La parte "sólo si" es trivial. Supongamos que K no tiene subgrupos de tipo (p, p). Entonces, como $\Omega_1(Z(K)) \neq 1$ es elementalmente abeliano y K no tiene subgrupos de tipo (p, p), $\Omega_1(Z(K)) \cong Z_p$. Si $Y \subsetneq K$ es otro subgrupo de orden p, entonces $Y \cdot \Omega_1(Z(K))$ sería un subgrupo de tipo (p, p).

El resto de la prueba demuestra (ii).

Supongamos que en efecto $p \neq 2$.

La parte "sólo si" es trivial.

Tenga en mente que un grupo cíclico tiene un único subgrupo de cada tamaño que divide a su orden.

Supondremos que (ii) es falso.

Sea K un contraejemplo minimal. Claramente, K no es abeliano. Como todo subgrupo de orden p^2 es abeliano, tenemos que $|K| \geq p^3$. También sabemos que todo subgrupo propio de K es cíclico.

Afirmamos que K tiene un único subgrupo de índice p^2:

Suponga que A_1 y A_2 son dos subgrupos distintos de índice p^2. Entonces existen N_1 y N_2, tales que $N_i \supseteq A_i$ y $|K:N_i| = p$. En consecuencia, $N_i \lhd K$ y cada N_i es cíclico, digamos $N_1 = \langle x \rangle$ y $N_2 = \langle y \rangle$. También $N_1 \neq N_2$, pues de otro modo $A_1 = A_2$. Luego $K = \langle x, y \rangle$. Puesto que $K/N_1 \cong Z_p$, tenemos $y^p \in \langle x \rangle$. Como $|y^p| = |y|/p = |x|/p \neq |x|$, resulta $y^p \in \langle x^p \rangle$. De manera semejante $x^p \in \langle y^p \rangle$. Luego $A_1 = \langle x^p \rangle = \langle y^p \rangle = A_2$.

Con esta contradicción hemos probado que, como se había afirmado, K tiene un único subgrupo de índice p^2.

Observe que también existe un único subgrupo de índice p^3, pues todo subgrupo de índice p^3 está contenido en uno de índice p^2, de los cuales sólo hay uno, y éste, por ser cíclico, contiene un único subgrupo de índice p (de índice p^3 en K).

Sea K_0 el único subgrupo de índice p^3. Entonces $x \in K$ implica que $\langle x \rangle$ contiene o está contenido en un subgrupo de K de índice p^3, es decir: $\langle x \rangle \subseteq K_0$ o $K_0 \subseteq \langle x \rangle$. Concluimos que $K_0 \subseteq Z(K)$. Luego K/K_0 no es cíclico (K sería abeliano) y tiene un único subgrupo de orden p (K tiene un único subgrupo de orden p^3). Por la minimalidad de K, se sigue que $K_0 = 1$ y $|K| = p^3$. Entonces una presentación (parcial) de K sería:

$$K = \langle x, y \,|\, |x| = p^2, |y| = p^2, \langle x^p \rangle = \langle y^p \rangle, \ldots \rangle$$

Sin pérdida de generalidad, cambiando nuestro generador x si fuera necesario, tenemos $y^p = x^{-p}$. Por el Lema 0.3.: $(xy)^p = z^{p(p-1)/2} x^p y^p = z^{p\left(\frac{p-1}{2}\right)}$, con $z = yxy^{-1}x^{-1} \in \langle x \rangle \cap \langle y \rangle$. Como $\langle x \rangle \cap \langle y \rangle = \langle x^p \rangle$, tenemos $z^p = 1$, y entonces $(xy)^p = 1$ (pues $p \neq 2$), pero $xy \notin \langle x \rangle$. Luego $\langle x^p \rangle$ no es el único subgrupo de orden p. #

Definición 0.42. Definimos el *grupo cuaternio* Q_8, y la familia de los *grupos diédricos* D_n, como sigue:

$$Q_8 = \langle x, y \,|\, x^4 = y^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle$$

$$D_n = \langle x, y \mid x^n = y^2 = 1, yxy^{-1} = x^{-1} \rangle.$$

Nota: Observe que $|Q_8| = 8$ y $|D_n| = 2n$; Q_8 tiene un único elemento de orden 2 y D_4 tiene 5; en particular $Q_8 \ncong D_4$. Cualquier texto elemental sobre teoría de grupos muestra que Q_8 y D_4 son los únicos grupos (hasta isomorfismo) no abelianos de orden 8.

Lema 0.43. [Piz 0.43] $|Aut(Q_8)| = 24$.

Demostración. Sabemos que Q_8 tiene la siguiente representación por generadores y relaciones: $Q_8 = \{x, y \mid x^4 = y^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1}\}$. Así, Q_8 consta de 8 elementos: el neutro, un único elemento de orden 2 ($x^2 = y^2$) y seis elementos de orden 4, a saber: $\{x, x^3, y, xy, x^2y, x^3y\}$. También, si u y v son cualesquiera dos elementos de orden 4, tales que $\langle u \rangle \neq \langle v \rangle$, entonces claramente $Q_8 = \langle u \rangle \langle v \rangle$ y satisfacen las mismas relaciones que x y y:

(1) $u^4 = v^4 = 1$, pues se escogieron de orden 4.

(2) $u^2 = v^2$, por que hay un único elemento de orden 2.

(3) $vuv^{-1} = u^{-1}$, ya que $[Q_8 : \langle u \rangle] = 2$ implica que $\langle u \rangle \lhd Q_8$, y entonces $\langle v \rangle$ actúa en $\langle u \rangle$, no trivialmente, pues de otro modo Q_8 sería abeliano; pero como $|Aut(\langle u \rangle)| = |Aut(Z_4)| = 2$, sólo hay una forma en que v puede actuar no trivialmente en $\langle u \rangle$, que es la que queremos.

Entonces, para construir un automorfismo de Q_8 basta mandar a x en cualquier elemento u de los 6 elementos de orden 4 que tiene Q_8, y después mandar a y en cualquiera de los restantes 4 elementos de orden 4 de $Q_8 - \langle u \rangle$. Luego $|Aut(Q_8)| = 6 \cdot 4 = 24$. #

Nota: De hecho, se puede ver que $Aut(Q_8) \cong S_4$ (ver por ejemplo [Rot Ej. 7.11]), pero nosotros no haremos uso de ello.

Definición 0.44. El *grupo general lineal*, denotado por $GL(n, p^\alpha)$, es el conjunto de todas las matrices no singulares de tamaño $n \times n$ con entradas en el campo de p^α elementos con la multiplicación normal de matrices. También definimos el *grupo especial lineal*, denotado por $SL(n, p^\alpha)$, como el subgrupo de $GL(n, p^\alpha)$ que consta de las matrices de determinante 1. Si V es un espacio vectorial de dimensión n sobre un campo finito K, de p^α elementos, denotamos por $GL(V)$ al grupo de todas las transformaciones lineales no singulares de V, y por $SL(V)$ al grupo de las transformaciones que tienen determinante 1. Claramente, cada vez que escogemos una base para V, tenemos un par de isomorfismos: $GL(n, p^\alpha) \cong GL(V)$ y $SL(n, p^\alpha) \cong SL(V)$. Identificaremos a $GL(V)$ con $GL(n, p^\alpha)$ y a $SL(V)$ con $SL(n, p^\alpha)$ siempre que no haya confusión posible.

Lema 0.45. [Gor 2.8.1] $|GL(n,p)| = (p^n-1)\cdot(p^n-p)\cdot(p^n-p^2)\cdots(p^n-p^{n-1})$ y $|SL(n,p)| = |GL(n,p)|/(p-1)$. Estaremos particularmente interesados en la forma de estas expresiones en el caso $n=2$: $|GL(2,p)| = p(p+1)(p-1)^2$ y $|SL(2,p)| = p(p+1)(p-1)$.

Demostración. Sea V un espacio vectorial sobre F_p de dimensión n en el que $GL(n,p)$ actúa. Sea $\{v_1, v_2, \ldots, v_n\}$ una base de V. Si $x \in GL(n,p)$, $\{x(v_1), x(v_2), \ldots, x(v_n)\}$ debe ser una base también y x está unívocamente determinado por esta segunda base. Entonces contar los elementos de $GL(n,p)$ es lo mismo que contar bases en V. Veamos de cuántas maneras se puede escoger una base $\{w_1, w_2, \ldots, w_n\}$ para V:

Observemos que w_1 puede ser cualquiera de los p^n-1 vectores no nulos de V; w_2 puede tomar el valor de cualquiera de los p^n-p vectores que no son múltiplos escalares de w_1; w_3 puede ser cualquiera de los p^n-p^2 vectores que no son combinación lineal de w_1 y w_2 ... si continuamos de esta manera obtenemos el primer resultado.

En el caso $n=2$ tenemos: $|GL(2,p)| = (p^2-1)(p^2-p) = p(p+1)(p-1)^2$.

Por otro lado, $det: GL(n,p) \to F_p^*$ es un homomorfismo de grupos sobreyectivo. Entonces $|GL(n,p): Ker(det)| = |F_p^*| = p-1$, pero $Ker(det) = SL(n,p)$ claramente. Así: $|SL(n,p)| = \dfrac{|GL(n,p)|}{(p-1)}$. En el caso $n=2$, tenemos:

$$|SL(2,p)| = \frac{p(p+1)(p-1)^2}{p-1} = p(p+1)(p-1). \#$$

Lema 0.46. [Gor 2.8.3] $SL(2,p)$ contiene subgrupos cíclicos de órdenes $p+1$ y $p-1$.

Demostración. El grupo $\left\{\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{pmatrix} \middle| \alpha \in F_p^*\right\} \subseteq SL(2,p)$ es isomorfo a F_p^* y, por tanto, cíclico de orden $p-1$.

Por otro lado, podemos pensar en el grupo aditivo de F_{p^2} como un F_p-espacio vectorial V de dimensión 2. Sea ω un generador del grupo cíclico $F_{p^2}^*$, entonces $|\omega| = p^2-1$. La multiplicación en F_{p^2} por ω induce una transformación lineal T_ω de V, con $T_\omega \in GL(2p)$. Si $L := \langle T_\omega \rangle$, L es cíclico de orden p^2-1. Ahora, observamos el homomorfismo $det: L \to F_p^*$: como $|L| = p^2-1$ y $|F_p^*| = p-1$, el núcleo K de este morfismo es un grupo cíclico y de orden múltiplo de $p+1$; en todo caso K contiene un subgrupo cíclico de orden $p+1$ y $K \subseteq SL(2,p)$. #

Lema 0.47. [Piz 0.47] Todo q-subgrupo de Sylow de $SL(2,p)$, con $q \neq 2$, es cíclico.

Demostración. Si $q = p$, es obvio por el Lema 0.45. Si no, como $q \neq 2$, observamos que q divide a $p+1$ o a $p-1$, pero no a ambos (pues de otro modo $rq = p+1$ y $sq = p-1$ implican que $(r-s)q = 2$ y entonces $q = 2$). Esto significa que un q-subgrupo de Sylow de

cualquiera de los dos subgrupos cíclicos del Lema 0.46. es también un q-subgrupo de Sylow de $SL(2,p)$. #

Lema 0.48. [Piz 0.48] Si $p \neq 2$, $SL(2,p)$ tiene un único elemento de orden 2.

Demostración. Las condiciones:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & d^2+bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ y } det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad-bc = 1,$$

se traducen en el sistema de ecuaciones:

(1) $a^2+bc=1$, (2) $d^2+bc=1$, (3) $b(a+d)=0$, (4) $c(a+d)=0$ y (5) $ad-bc=1$.

Entonces tenemos:

6) $a^2+2bc+d^2=2$ (sumando 1 y 2)
7) $bc=ad-1$ (de 5)
8) $a^2+2(ad-1)+d^2=2$ (sust. 7 en 6)
9) $a^2+2ad+d^2=4$ (de 8)
10) $(a+d)^2=4$ (de 9)
11) $(a+d)\neq 0$ (de 10 pues $p\neq 2$)
12) $b=0$ (de 3 y 11)
13) $c=0$ (de 4 y 11)
14) $a^2=1$ (de 1 y 12)
15) $d^2=1$ (de 2 y 12)
16) $ad=1$ (de 5 y 12)
17) $a=d=\pm 1$ (de 14, 15 y 16)

En el caso $a=d=1$ tenemos la identidad. El otro caso es: $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, que es el único elemento de orden 2 de $SL(2,p)$. #

1. Algunos teoremas clásicos

BURNSIDE

El resultado siguiente es una versión simplificada del Teorema de Burnside, que es el tema de este trabajo. El corolario que se deriva de él nos será útil más adelante.

Teorema 1.1. [Suz I, p104] Sean p y q números primos; entonces, todo grupo G de orden $p^a q$ es soluble.

Demostración. Sea G un grupo del orden descrito. Si G no es simple, entonces tiene un subgrupo normal propio N. Luego N y G/N son solubles, ya sea por hipótesis de inducción o porque todo p-grupo es soluble. Esto implica que G es soluble.

Probaremos a continuación que un grupo G de orden $p^a q$ no puede ser simple.

Para llegar a una contradicción, supongamos que G es simple.

Por los teoremas de Sylow, G contiene exactamente q p-subgrupos de Sylow. Sean S y T dos p-subgrupos de Sylow de G distintos, tales que su intersección $D = S \cap T$ sea maximal. Sea $H := N_G(D)$. Afirmamos que H tiene al menos 2 p-subgrupos de Sylow:

Como S es un p-grupo, $D \subsetneq S$ implica que $D \subsetneq N_S(D)$. Si P_0 fuera el único p-subgrupo de Sylow de H, entonces $D \subsetneq N_S(D) \subseteq P_0 \subseteq H$.

Si ahora P es un p-subgrupo de Sylow de G que contiene a P_0, tenemos $D \subsetneq N_S(D) \subseteq S \cap P$ y por la maximalidad de D, resulta que $S = P$; de forma semejante, $D \subsetneq N_T(D) \subseteq T \cap P$ y $T = P$. Así $S = T$, lo que es una contradicción.

Sabemos entonces que H es un subgrupo de orden $p^b q$ y por tanto, H tiene exactamente q p-subgrupos de Sylow, los cuales contienen todos a D puesto que $D \lhd H$.

Sean ahora P_0 y P_1 dos p-subgrupos de Sylow de H y P un p-subgrupo de Sylow de G que contiene a ambos, entonces $P_0 = P \cap H = P_1$. Como cada p-subgrupo de Sylow de H está contenido en algún p-subgrupo de Sylow de G, el resultado anterior, junto con el hecho de que H y G tienen igual número de subgrupos de Sylow, implica que existe una biyección entre los subgrupos de Sylow de H y los de G, biyección que a cada Sylow de H le asigna el único Sylow de G que lo contiene. Luego cada Sylow de G contiene un único Sylow de H, que a su vez contiene a D, entonces $D \subseteq \bigcap_{P \in Syl_p(G)} P$. Como hemos supuesto que G es simple y $\bigcap_{P \in Syl_p(G)} P$ es normal en G, resulta que $D = 1$. Por la maximalidad de D, cualesquiera dos p-subgrupos de Sylow de G se intersectan trivialmente.

Terminamos con un conteo elemental.

G tiene exactamente q p-subgrupos de Sylow, cada uno de ellos con $p^a - 1$ elementos no triviales. Dado que cada par de ellos se intersecta trivialmente, G tiene exactamente $q(p^a - 1)$ p-elementos no nulos. Luego, ya que $|G| = p^a q$, existen a lo más q

q-elementos. Existe un q-subgrupo de Sylow que contiene estos q elementos, luego no hay más q-subgrupos de Sylow, y el q-subgrupo de Sylow es normal. Contradicción. #

Corolario 1.2. [Piz 1.2] Sea G un grupo, con $|G| = pq^a$ y $G = \langle P_1, P_2, \ldots, P_m | P_i \in Syl_p(G) \rangle$; entonces el q-subgrupo de Sylow de G es normal.

Demostración. Tenemos $G = QP_1$, con Q un q-subgrupo de Sylow de G. Por el Teorema 1.1., G es soluble, entonces G debe contener un subgrupo normal N con $[G:N] = p$ o $[G:N] = q$. Si $[G:N] = p$ entonces N debe ser un q-subgrupo de Sylow normal de G, es decir, $Q = N \lhd G$ como queríamos probar. Mostraremos que $[G:N] = q$ no puede darse.

Si $[G:N] = q$, N contiene un p-subgrupo de Sylow de G; como todos los p-subgrupos de Sylow de G son conjugados y N es normal, N contiene a todos los p-subgrupos de Sylow de G. Luego: $G = \langle P_1, P_2, \ldots, P_m \rangle \subseteq N$, una contradicción. #

SCHUR

Definición 1.3. Si un grupo Q actúa en B, decimos que actúa *irreduciblemente* si B no tiene subgrupos Q-invariantes no triviales; y que actúa *fielmente* si ningún elemento no trivial de Q actúa trivialmente en B (así Q se inyecta en los automorfismos de B). Un *Q-endomorfismo* de A es un endomorfismo de A que conmuta con todos los automorfismos de A inducidos por la acción de Q.

Lema 1.4. (de Schur) [Suz I, p. 159] Si un grupo Q actúa irreduciblemente en un grupo abeliano (aditivo) A, el conjunto de todos los Q-endomorfismos de A es un anillo de división.

Demostración. Sea E_Q el conjunto de todos los Q-endomorfismos de A, sea $x \in Q$ y $\sigma \in E_Q$; entonces $x(\sigma A) = \sigma(xA)$, por tanto σA es Q-invariante. Si $\sigma \neq 0$, $\sigma A = A$ pues, como $Ker(\sigma)$ es Q-invariante y Q actúa irreduciblemente, tenemos que $Ker(\sigma) = \{0\}$. Luego, $\sigma \in Aut(A)$. Como también $\sigma^{-1} \in E_Q$, tenemos que E_Q es un anillo de división. #

Corolario 1.5. [Suz I, 2.5.21] Si A y Q son dos grupos abelianos y Q actúa fiel e irreduciblemente en A, entonces Q es cíclico.

Demostración. La acción de Q sobre A induce $Q \xrightarrow{\varphi} Aut(A) \subseteq End(A)$, con φ inyectivo. Como Q es abeliano, $\varphi(Q) \subseteq E_Q$. De hecho, $\varphi(Q) \subseteq Z(E_Q)$ y, por el Lema de Schur, $Z(E_Q)$ es un campo. Finalmente $\varphi(Q) \subseteq Z(E_Q)^*$ implica que $\varphi(Q) \cong Q$ es cíclico, pues todo subgrupo finito del grupo multiplicativo de un campo es cíclico (ver por ejemplo [Rot 2.16]). #

BAER-SUZUKI

Teorema 1.6. (Baer-Suzuki) [Alp] Un p-elemento x de un grupo G está en $O_p(G)$ si y sólo si cualesquiera dos conjugados de x generan un p-subgrupo de G.

Demostración. Una implicación es obvia. Probaremos que si cualesquiera dos conjugados de x generan un p-subgrupo, entonces $x \in O_p(G)$.

Sea K una clase de conjugación de p-elementos de G. Para llegar a una contradicción, supondremos que cualesquiera dos elementos de K generan un p-subgrupo de G y que $K \not\subseteq O_p(G)$.

Afirmamos que $\langle K \rangle$ no es un p-grupo, pues si lo fuera, por ser $\langle K \rangle$ invariante bajo conjugación, sería normal y entonces $\langle K \rangle \subseteq O_p(G)$ contrario a lo supuesto. Sea P un p-subgrupo de Sylow de G. Por la afirmación anterior $K \not\subseteq P$. Sea $y \in K - P$ y Q un p-subgrupo de Sylow de G tal que $y \in Q$. Claramente $K \cap P \neq K \cap Q$.

De entre todas las parejas de p-subgrupos de Sylow de G que cumplen con $K \cap P \neq K \cap Q$, escoja una tal que $|K \cap P \cap Q|$ sea máximo. Como P y Q son conjugados, tenemos $|K \cap P| = |K \cap Q|$. Luego $K \cap P \not\subseteq Q$ y $K \cap Q \not\subseteq P$.

Sean $D := \langle K \cap P \cap Q \rangle$ y $D = P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$ una serie subnormal tal que $|P_j : P_{j-1}| = p$. Como $D \subseteq Q$, tenemos que $K \cap P \not\subseteq Q$ implica $K \cap P \not\subseteq D$ y también $K \cap P \not\subseteq K \cap D$. Entonces, podemos escoger el entero positivo más pequeño i tal que $K \cap P_i \not\subseteq K \cap D$. Sea $x \in K \cap P_i$ con $x \notin D$. Afirmamos que x normaliza a D; pues como x normaliza a P_{i-1}, x normaliza a $K \cap P_{i-1} = K \cap D$ (por la elección de P_i) y, finalmente, x normaliza a $\langle K \cap D \rangle = D$ como se había dicho. De manera semejante existe $y \in K \cap Q$, $y \notin D$ tal que y normaliza a D.

Como $x, y \in K$, $\langle x, y \rangle$ es un p-grupo, por hipótesis, y como $\langle x, y \rangle$ normaliza a D, $\langle x, y, D \rangle$ es un p-grupo. Sea R un p-subgrupo de Sylow de G que contenga a $\langle x, y, D \rangle$. Entonces $K \cap P \cap R \supseteq (K \cap D) \cup \{x\}$, y por tanto $|K \cap P \cap R| > |K \cap D| = |K \cap P \cap Q|$. De manera similar $|K \cap Q \cap R| > |K \cap D| = |K \cap P \cap Q|$. Finalmente $K \cap P = K \cap R = K \cap Q$ por la elección maximal de $|K \cap P \cap Q|$, una contradicción. #

Teorema 1.7. (Baer) [Ben 2.12] Sea t una involución del grupo G tal que $t \notin O_2(G)$, entonces ${}^t g = g^{-1}$ para algún elemento $g \in G$ de orden impar $\neq 1$.

Demostración. En primer lugar observamos que ${}^t g = g^{-1}$ es equivalente a $tgt = g^{-1}$, es decir $gtgt = 1$, o lo que es lo mismo: gt es una involución.

Por el teorema de Baer-Suzuki (Teorema 1.6.), existen dos conjugados de t, ${}^{x_1}t$ y ${}^{x_2}t$ tales que $\langle {}^{x_1}t, {}^{x_2}t \rangle$ no es un 2-grupo. Entonces ${}^{x_1^{-1}}\langle {}^{x_1}t, {}^{x_2}t \rangle = \langle t, {}^{x_1^{-1}x_2}t \rangle$ tampoco lo es. Sea $s = {}^{x_1^{-1}x_2}t$, vemos entonces que todo elemento de $\langle s, t \rangle$ se puede representar como una

sucesión alternada de s's y t's y está caracterizado por la letra inicial de la sucesión y su longitud. Además toda sucesión de s's y t's de longitud impar es una involución, pues:

a) s y t son involuciones.
b) $ststst\cdots sts = s(tsts\cdots tst)$ y $tstst\cdots tst = t(stst\cdots sts)$
(es decir conjugados de involuciones por hipótesis de inducción.)

Sea $g \in \langle t,s\rangle$ un $2'$-elemento no trivial. Entonces $g=(ts)^r$ o $g=(st)^r$, y así $gt=(ts)^r t$ o $gt=(st)^{r-1}s$, que son sucesiones alternantes de s's y t's de longitud impar, y en cualquier caso gt es una involución. #

TRANSFER

Teorema 1.8. (del transfer) [Gor 7.3.2] Sean $H \le G$ grupos con $n=|G:H|$, A un grupo abeliano y $\phi: H \to A$ un homomorfismo. Sea $\{y_i\}$ un conjunto de representantes de clases laterales derechas de H en G. Para cada $x \in G$, escriba: $y_i x = h_i(x) y_{i(x)}$ con $h_i(x) \in H$. Si definimos:

$$\tau(x) = \phi\left(\prod_{i=1}^{n} h_i(x)\right)$$

Entonces:

(i) $\tau: G \to A$ es un homomorfismo.

(ii) τ no depende de la elección de las y_i's.

Demostración. Observamos que cada elemento de G se puede escribir de manera única como hy_i con h en H y y_i en $\{y_i\}$. Denotaremos $i'(x)$ por $\pi_x(i)$. También $h_i(x_1x_2)y_{\pi_{x_1x_2}(i)} = y_i x_1 x_2 = h_i(x_1)y_{\pi_{x_1}(i)}x_2 = h_i(x_1)h_{\pi_{x_1}(i)}(x_2)y_{\pi_{x_1}(\pi_{x_1}(i))}$ y en consecuencia resulta $h_i(x_1x_2) = h_i(x_1)h_{\pi_{x_1}(i)}(x_2)$ y $\pi_{x_1x_2}(i) = \pi_{x_2}(\pi_{x_1}(i))$. Es fácil ver que, para cualquier x, $\pi_x: \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ es una permutación. Luego:

$$\tau(x_1x_2) = \phi\left(\prod_{i=1}^{n} h_i(x_1x_2)\right) = \phi\left(\prod_{i=1}^{n} h_i(x_1)h_{\pi_{x_1}(i)}(x_2)\right) = \prod_{i=1}^{n}\phi(h_i(x_1))\phi(h_{\pi_{x_1}(i)}(x_2)) =$$

$$\prod_{i=1}^{n}\phi(h_i(x_1))\prod_{i=1}^{n}\phi(h_{\pi_{x_1}(i)}(x_2)) = \prod_{i=1}^{n}\phi(h_i(x_1))\prod_{i=1}^{n}\phi(h_i(x_2)) = \phi\left(\prod_{i=1}^{n} h_i(x_1)\right)\phi\left(\prod_{i=1}^{n} h_i(x_2)\right) =$$

$$\tau(x_1)\tau(x_2).$$

Usando que A es abeliano y que π_{x_1} es una permutación. Con esto queda probado el primer inciso.

Si ahora $\{y_i'\}$ es otro conjunto de representantes de clases laterales derechas de H en G, numerado de forma que y_i y y_i' estén en la misma clase lateral, entonces podemos

definir $h' \in H$ por medio de $y_i' = h' y_i$. Entonces, como $\pi_x'(i) = \pi_x(i)$, pues π_x simplemente representa la permutación que induce x en las clases laterales derechas de H en G, tenemos:

$$h_i'(x) h^{\pi_x(i)} y_{\pi_x(i)} = h_i'(x) y_{\pi_x(i)}' = y_i' x = h' y_i x = h' h_i(x) y_{\pi_x(i)}$$

y en particular:

$$h_i'(x) = h' h_i(x) \left(h^{\pi_x(i)}\right)^{-1}$$

Luego:

$$\tau'(x) = \prod_{i=1}^{n} \phi(h_i'(x)) = \prod_{i=1}^{n} \phi\left(h' h_i(x) \left(h^{\pi_x(i)}\right)^{-1}\right) = \prod_{i=1}^{n} \phi(h') \prod_{i=1}^{n} \phi(h_i(x)) \prod_{i=1}^{n} \phi\left(h^{\pi_x(i)}\right)^{-1} =$$

$$\prod_{i=1}^{n} \phi(h') \prod_{i=1}^{n} \phi(h_i(x)) \prod_{i=1}^{n} \phi(h')^{-1} = \prod_{i=1}^{n} \phi(h_i(x)) = \tau(x). \ \#$$

Definición 1.9. Al homomorfismo definido en el teorema anterior se le llama el *transfer* de G en A, respecto de H y ϕ.

Teorema 1.10. [Gor 7.3.3] Sea τ el transfer de G en A, respecto de H y ϕ. Entonces, para cada $x \in G$, existe un entero t, y un par de conjuntos: $\{r_i\}$ de naturales y $\{x_i\}$ de elementos de G, $1 \le i \le t$, tales que:

(i) $x_i x^{r_i} x_i^{-1} \in H, \ \forall i = 1, \ldots, t.$

(ii) $\sum_{i=1}^{t} r_i = n = |G:H|.$

(iii) $\tau(x) = \phi\left(\prod_{i=1}^{t} x_i x^{r_i} x_i^{-1}\right).$

Demostración. Usaremos el teorema anterior y su notación. Renumeramos los representantes de clases laterales y_i de tal manera que la permutación π_x tenga la siguiente descomposición en ciclos disjuntos:

$$\pi_x = (1, 2, \ldots, r_1)(r_1 + 1, \ldots, r_1 + r_2)(r_1 + r_2 + 1, \ldots, r_1 + r_2 + r_3) \ldots$$

Sea t el número de ciclos; entonces:

$$\sum_{i=1}^{t} r_i = n = |G:H| \ .$$

Sean $x_1 = y_1$, $x_2 = y_{r_1+1}$, ... , $x_t = y_{r_1+r_2+\cdots+r_{t-1}+1}$. Luego $x_i x^j$ está en la misma clase lateral derecha que el $(j+1)$-ésimo representante del i-ésimo ciclo, entonces $\{z_k\} = \{x_i x^j \mid 1 \le i \le t, \ 0 \le j \le r_i - 1\}$ es un conjunto completo de representantes de clase (escogemos la numeración de las z's para que z_k y y_k estén en la misma clase lateral). Como $x_i x^{r_i}$ y x_i están en la misma clase lateral derecha, $x_i x^{r_i} x_i^{-1} \in H$. Entonces $z_k x = h_k'(x) z_{\pi_x(k)}$ y $z_k = x_i x^j$, para algunas i y j con $1 \le i \le t$ y $0 \le j \le r_i - 1$. Si $j < r_i - 1$

resulta que $z_k x = x_i x^{j+1} = z_{k+1}$ lo que implica que $h_k^i(x) = 1$. Por otro lado, si $j = r_i - 1$, tenemos que $z_k x = x_i x^{r_i} = (x_i x^{r_i} x_i^{-1}) x_i$, es decir: $h_k^i(x) = x_i x^{r_i} x_i^{-1}$. #

Lema 1.11. (del transfer de Thompson) [Ben 2.6] Sea T un 2-Sylow del grupo simple $G \not\cong Z_2$, y $N \lhd T$ con T/N cíclico. Entonces toda involución $t \in G$ es conjugada de algún elemento de N.

Demostración. Sea t' una involución de G y supongamos que t' no es conjugada a ningún elemento de N para llegar a una contradicción. t' es, sin embargo conjugada de algún elemento t de T, pues T es de Sylow. Entonces t y ${}^s t \in T - N$ siempre que ${}^s t \in T$. En este caso:

$\phi(t)$ y $\phi(t^s)$ son involuciones en T/N (donde $\phi: T \to T/N$ es la proyección natural); además, como T/N es cíclico, tiene un único subgrupo de orden 2, y por ello $\langle \phi(t) \rangle = \langle \phi(t^s) \rangle$, es decir, $\phi(t) = \phi({}^s t)$; claramente también $\phi(t^n) = \phi({}^s(t^n))$ para cualquier natural n. Así pues, por el Teorema 1.10.,

$$\tau(t) = \phi\left(\prod_{i=1}^{s} x_i t^{r_i} x_i^{-1} \right),$$

donde $\tau: G \to T/N$ denota el transfer de G en T/N respecto a T y ϕ, para algunas $\{r_i\}$ naturales y $\{x_i\}$ elementos de G. Además $x_i t^{r_i} x_i^{-1} \in T$, lo que implica que $\phi(x_i t^{r_i} x_i^{-1}) = \phi(t^{r_i}) = \phi(t)^{r_i}$ y entonces:

$$\tau(t) = \prod_{i=1}^{s} \phi(t)^{r_i} = \phi(t)^{\sum_{i=1}^{s} r_i} = \phi(t)^{[G:T]}, \text{ por el Teorema 1.10.(ii)}$$

Finalmente $\phi(t)^{[G:T]}$ no puede ser trivial porque $[G:T]$ es impar. Puesto que $G \not\cong Z_2$, tenemos que el transfer de G en T/N con respecto a T y a ϕ, es un homomorfismo con kernel no trivial y concluimos que G no puede ser simple, contradicción. #

Necesitamos el siguiente lema auxiliar.

Lema 1.12. [Ben 2.7] Sea T un 2-grupo no abeliano tal que todo subgrupo normal de orden 4 es cíclico. Sea U uno de tales subgrupos normales. Entonces $C_T(U)$ es cíclico (y tiene índice 2 en T). Si T tiene un automorfismo de orden impar $\neq 1$, entonces $|T| = 8$.

Demostración. En primer lugar, como U es normal y en consecuencia T actúa por conjugación en U, observamos que $T/C_T(U)$ se inyecta en $Aut(U) \cong Aut(Z_4) \cong Z_2$. Luego, $|T: C_T(U)| \leq 2$. Supongamos que $C_T(U)$ no es cíclico para llegar a una contradicción.

Sea A un subgrupo abeliano maximal sujeto a $U \subseteq A \lhd T$; entonces, por el Teorema 0.30., $C_T(A) = A$. Además A debe ser cíclico, pues si no, $\Omega_1(A)$ es un subgrupo característico de A (por tanto normal en T) y, otra vez por el Teorema 0.13., $\Omega_1(A)$ contiene un subgrupo normal en T de orden 4, necesariamente isomorfo a $Z_2 \times Z_2$,

contradiciendo los supuestos sobre T. También tenemos que $A \subsetneq C_T(U)$, pues $C_T(U)$ no es cíclico. Ahora, por el Teorema 0.13., existe Y con $A \subseteq Y \subseteq C_T(U)$, $Y \lhd T$, $|Y:A| = 2$.

Sea $y \in Y - A$. Afirmamos que $Y' = [Y,Y] = [y,A]$.

Como $Y = yA \cup A$, tenemos:

$$[Y,Y] = \langle [A,A],[yA,A],[A,yA],[yA,yA] \rangle = \langle [yA,A],[yA,yA] \rangle .$$

Si $a, \bar{a} \in A$, usando las identidades (1) a (3) del Teorema 0.2., resulta:

$$[ya, y\bar{a}] = {}^{y}[a, y\bar{a}] \cdot [y, y\bar{a}] = {}^{y}\big([a,y]^{y}[a,\bar{a}]\big) \cdot \big([y,y]^{y}[y,\bar{a}]\big)$$
$$= {}^{y}[a,y]^{y}[y,\bar{a}] = [{}^{y}a, y][y, {}^{y}\bar{a}] = [y, {}^{y}a][y, {}^{y}\bar{a}] \in [y,A].$$

También: $[ya, \bar{a}] = {}^{y}[a,\bar{a}] \cdot [y,\bar{a}] = [y,\bar{a}] \in [y,A]$, y así, $Y' = [Y,Y] = [y,A]$, como se había afirmado.

Si ahora a es un generador de A, entonces $[y,a^r] = ya^r y^{-1} a^{-r} = {}^{y}(a^r) a^{-r} = ({}^{y}a \cdot a^{-1})^r$, pues A es abeliano y normal en T. Por tanto $[y,A] = \langle {}^{y}a \cdot a^{-1} \rangle = Y'$, en particular $Y' \subseteq A$. Veamos cómo actúa (por conjugación) Y en Y'. En primer lugar, observamos que y^2 está en A, pues $|Y:A| = 2$. Además, la acción de todo A sobre Y' es trivial, pues A es abeliano y $Y' \subseteq A$. Entonces basta con conocer la acción de y sobre Y' para reconstruir la acción de todo $Y = A \cup yA$. Si tomamos $x := {}^{y}a \cdot a^{-1}$, resulta ${}^{y}x = {}^{y}({}^{y}a \cdot a^{-1})$ $= ({}^{y^2}a) \cdot ({}^{y}a^{-1}) = a \cdot ({}^{y}a^{-1}) = x^{-1}$ y y actúa por inversión en Y'. En consecuencia, $U \subsetneq \langle x \rangle = Y'$, pues de lo contrario, tomamos $U = \langle u \rangle$, y tenemos $yuy^{-1} = u^{-1}$, pero $u \neq u^{-1}$ implica que $y \notin C_T(U)$, contradicción.

Concluimos que $|Y'| = 2$, pues U, $Y' \subseteq A$ que es cíclico y, como todo mundo sabe, el orden parcial (determinado por contención) de los subgrupos de un grupo cíclico resulta ser total (y Y no es abeliano por la maximalidad de A). Por otro lado, Y/Y' es abeliano y no cíclico (si no Y sería abeliano); entonces $Y/Y' \cong Z_{2^e} \times Z_{2^f}$, pues Y tiene dos generadores: y y a. Sea $\overline{V} = \Omega_1(Y/Y') \cong Z_2 \times Z_2$ que es un subgrupo característico. Si V es la imagen inversa de $\overline{V}$ ($V \subseteq Y$), V también es característico en Y (pues Y' también lo es). Como además $Y \lhd T$, tenemos: $V \lhd T$, $|V| = 8$ y V no es cíclico.

Por otro lado $V \cap A = U$ (pues $U/Y' \cong Z_2 \subseteq \overline{V}$ y V no es cíclico) Entonces V es abeliano, ya que $U \subseteq Z(V)$ implica que $[V:Z(V)] \leq 2$ y en consecuencia $Z(V) = V$. Concluimos que $V \cong Z_4 \times Z_2$ y $\Omega_1(V) \cong Z_2 \times Z_2$ es característico en V y por tanto normal en T, contradiciendo los supuestos sobre T. Así, $C_T(U)$ debe ser cíclico.

Para terminar, si $|T| \geq 16$ entonces $C_T(U)$ es el único subgrupo cíclico de índice 2, pues si C es otro de ellos,

$$|T| = |C \cdot C_T(U)| = \frac{|C||C_T(U)|}{|C \cap C_T(U)|} \text{ implica } |C \cap C_T(U)| = \frac{|C||C_T(U)|}{|T|} = \frac{|C_T(U)|}{2}.$$

Pero $|C_T(U)| \geq 8$ implica que $|C \cap C_T(U)| \geq 4$ y entonces $C \cap C_T(U) \supseteq U$, por ser $C_T(U)$ cíclico. Luego $C \subseteq C_T(U)$ y en consecuencia $C = C_T(U)$ pues ambos tienen el mismo índice en T. Si ahora $\sigma \in Aut(T)$ es un $2'$-automorfismo de T, éste debe actuar trivialmente en $C_T(U)$, ya que un 2-grupo cíclico no tiene $2'$-automorfismos. Además, si $t \in T$, $\sigma(t) = ta$ para alguna $a \in C_T(U)$ ($C_T(U)$ tiene índice 2 en T). Si $s = |a|$, $\sigma^s(t) = ta^s = t$ y en consecuencia σ es un 2-automorfismo. #

Ahora el Lema anterior y el Lema del transfer de Thompson nos permiten probar el siguiente resultado de estructura acerca de grupos simples:

Lema 1.13. [Ben 2.8] Sea T un 2-Sylow del grupo simple G. Si G tiene más de una clase de conjugación de involuciones, entonces cada involución centraliza algún U^g, para $U \lhd T$, $U \cong Z_2 \times Z_2$.

Demostración. Sea $N \lhd T$, $|T:N| = 2$; entonces, por el Lema 1.11., toda involución de G es conjugada a algún elemento de N. Notemos que N no puede ser cíclico, pues de serlo, tendría un solo elemento de orden 2 y habría una sola clase de conjugación de involuciones de G. Además, T tiene que contener un subgrupo de Klein ($\cong Z_2 \times Z_2$) normal U, pues de lo contrario, si todos los subgrupos normales de orden 4 fueran cíclicos, por el Lema 1.12., su centralizador N en T sería un subgrupo normal de T, cíclico de índice 2, que es justo lo que T no puede tener.

Tenemos que $C_T(U) \lhd T$. Observamos que $T/C_T(U)$ se inyecta en $Aut(U) \cong Aut(Z_2 \times Z_2) \cong S_3$, pero T es un 2-grupo, de modo que $T/C_T(U) \cong Z_2$. En particular $T/C_T(U)$ es cíclico y podemos aplicar el Lema 1.11.: si $t \in G$ es una involución, ${}^g t \in C_T(U)$ para alguna $g \in G$. Luego, $t \in C_T({}^{g^{-1}}U)$.#

SUBGRUPOS CRÍTICOS

Los subgrupos críticos son útiles en el estudio de los p'-automorfismos de p-grupos gracias al inciso (iii) del siguiente teorema. En el siguiente capítulo, cuando hayamos desarrollado más herramientas, presentaremos una versión más refinada de éste.

Teorema 1.14. [Gor 5.3.11] Todo p-grupo P posee un subgrupo característico C con las siguientes propiedades:

i) $cl(C) \leq 2$, $C/Z(C)$ es elementalmente abeliano.
ii) $[P,C] \subseteq Z(C)$.
iii) $C_P(C) = Z(C)$.
iv) Todo p'-automorfismo no trivial de P induce un automorfismo no trivial de C.

Demostración. Supongamos que existe un subgrupo característico C de P con la propiedad (iii); demostraremos que tal subgrupo debe satisfacer la propiedad (iv). Sea ψ un p'-automorfismo de P y $A = \langle \psi \rangle$. Suponga que ψ actúa trivialmente en C (la acción se restringe pues C *char* P); entonces tenemos $[C, A] = 1$, lo cual implica que $[C, A, P] = 1$. Además, $[P, C] \subseteq C$ (pues $C \trianglelefteq P$) y ello implica que $[P, C, A] = 1$. Concluimos que $[A, P, C] = 1$, por el teorema de los tres subgrupos. Por lo tanto $[A, P] \subseteq C_P(C) = Z(C) \subseteq C$ (ya que suponemos que C satisface (iii)). Así $[A, P] \subseteq C$. Entonces, por el Teorema 0.15., A estabiliza la serie subnormal $P \rhd C \rhd 1$ de P y, por el Teorema 0.16., A actúa trivialmente en P.

Por tanto, basta probar que existe tal subgrupo característico C que satisface (i), (ii) y (iii).

Sea M un subgrupo de P, maximal respecto a la propiedad de ser normal y abeliano. Entonces $C_P(M) = M$ por el Teorema 0.30. Suponga que M *char* P; entonces afirmamos que $C = M$ satisface los requerimientos, pues:

(iii) $C_P(C) = C = Z(C)$
(i) $C = Z(C)$ es de clase 1, $C/Z(C)$ es trivial.
(ii) $[P, C] \subseteq C = Z(C)$

Suponga, para el resto de la prueba, que no existe ningún M *char* P como el descrito.

Sea D un subgrupo abeliano característico maximal de P y sea M un subgrupo abeliano normal maximal de P. Por el supuesto anterior, $D \subsetneq M$. Tenemos: $M \subseteq H := C_P(D)$ pues M es abeliano, por tanto $D \subsetneq H$. Además, H es característico en P pues D lo es. Sean $\overline{P} := P/D$ y $\overline{H} := H/D \neq 1$, entonces $\overline{C} := \overline{H} \cap \Omega_1(Z(\overline{P})) \neq \overline{1}$ pues, por el Lema 0.11., $\overline{H} \cap Z(\overline{P}) \neq \overline{1}$. Afirmamos que C (la imagen inversa de $\overline{C}$ bajo la proyección $P \to \overline{P}$) cumple con las condiciones. El resto de la prueba se concentrará en verificar esto.

Sea K la imagen inversa de $\Omega_1(Z(\overline{P}))$; entonces K *char* P pues K/D *char* P/D y D *char* P (ver el Lema 0.4.). Así $C = H \cap K$ *char* P. Además $D \subseteq Z(C)$ ya que $C \subseteq H = C_P(D)$. También $Z(C)$ *char* P pues $Z(C)$ *char* C *char* P y entonces $Z(C) = D$ por la maximalidad de D. En consecuancia, tenemos $\overline{C} \subseteq Z(\overline{P})$ que implica $[\overline{P}, \overline{C}] = \overline{1}$ y por tanto $[P, C] \subseteq D = Z(C)$ y así:

(i) $C/Z(C) = \overline{C}$ es elementalmente abeliano y $cl(C) \leq 2$.
(ii) $[P, C] = Z(C)$.

Sea $Q = C_P(C)$. Supondremos que $Q \subsetneq C$ para llegar a una contradicción.

Como $C_C(C) = Z(C) = D$, resulta que $Q \cap C = D$. Además $Q \subseteq H$, pues Q centraliza a D (recuerde que $H = C_P(D)$). Entonces tenemos $\overline{Q} \subseteq \overline{H}$, $\overline{Q} \cap \overline{C} = \overline{1}$, $\overline{Q} \trianglelefteq \overline{P}$ y $\overline{Q} \neq \overline{1}$. Por otro lado, otra vez por el Lema 0.11., $\overline{Q} \cap \Omega_1(Z(\overline{P})) \neq \overline{1}$ y podemos concluir que $\overline{1} \neq \overline{Q} \cap \Omega_1(Z(\overline{P})) \subseteq \overline{H} \cap \Omega_1(Z(\overline{P})) = \overline{C}$; pero entonces $\overline{Q} \cap \overline{C} \neq \overline{1}$, lo que es una

contradicción con una expresión previa. Así concluimos que $Q \subseteq C$ y, así, $Q = Z(C)$, es decir:

(iii) $C_p(C) = Z(C)$. #

Definición 1.15. Un subgrupo con las características del teorema anterior se llama *subgrupo crítico*.

2. Acciones y p-grupos

TEOREMAS DE DESCOMPOSICIÓN

Teorema 2.1. [Ben 2.1] Sea $S \lhd X = ST$ con T un q-grupo y S un q'-grupo. Entonces $S = [T,S]C_S(T)$.

Demostración. Por el Teorema 0.2., $[T,S] \lhd X$. Si $s \in S$ y $t \in T$, tenemos $sts^{-1}t^{-1} \in [S,T] = [T,S]$, así $sts^{-1} \in [T,S]T$, luego: $sTs^{-1} \subseteq [T,S]T$, $\forall s \in S$. Si ahora $x \in X$, escriba $x = st$ con $s \in S$ y $t \in T$, entonces $xTx^{-1} = stTt^{-1}s^{-1} = sTs^{-1} \subseteq [T,S]T$, y así:

(1) $\quad xTx^{-1} \subseteq [T,S]T$, $\forall x \in X$.

Claramente $[T,S]T$ es un grupo (pues $[T,S]$ es normal en X). Afirmamos que:

(2) $\quad [T,S]T \lhd X$.

En efecto, si $x \in X$, entonces $x[T,S]Tx^{-1} = {}^x[T,S]{}^xT = [T,S][T,S]T = [T,S]T$ (usando 1).

Además, T es un q-subgrupo de Sylow de $[T,S]T$ ($[T,S]$ es un q'-grupo), luego, por el Argumento de Frattini (gracias a (2)): $X = [T,S] \cdot T \cdot N_X(T) = [T,S] \cdot N_X(T)$. Entonces:

$$S = S \cap X = S \cap \left([T,S] \cdot N_X(T)\right) = [T,S]N_S(T).$$

Finalmente, en este caso $C_S(T) = N_S(T)$. En efecto, $[N_S(T),T] \subseteq T$ pues $N_S(T)$ normaliza a T y $[N_S(T),T] \subseteq S$ ya que T normaliza a S y en consecuencia $[N_S(T),T] = 1$ dado que los órdenes de T y S son primos relativos; es decir: $N_S(T) \subseteq C_S(T)$ (la otra contención es obvia). #

Lema 2.2. [Suz I, 2.8.13] Suponga que un q-grupo Q actúa en un grupo G y $H \lhd G$, con H un q'-grupo Q-invariante. Entonces $C_G(Q)H/H = C_{G/H}(Q)$.

Demostración. Sea L tal que $H \subseteq L \subseteq G$ y $L/H = C_{G/H}(Q)$.

Por demostrar: $C_G(Q)H = L$.

Es claro que $C_G(Q)H \subseteq L$.

Probaremos que para cada primo $p \in \pi(L)$, existe un p-subgrupo de Sylow de L contenido en $C_G(Q)H$.

Sea $P \in Syl_p(L)$, $p \neq q$. Entonces HP es un grupo, pues H es normal. Además Q normaliza a HP, pues $P \subseteq L$ implica que $[Q,P] = 1 \bmod H$ y entonces $[Q,HP] \subseteq H \subseteq HP$.

Luego: $H \lhd HP \lhd HP \rtimes Q$ con HP un q'-grupo. Aplicando el Teorema 2.1., tenemos: $P \subseteq HP = H \cdot C_{HP}(Q) \subseteq H \cdot C_G(Q)$.

Resta probar que algún q-subgrupo de Sylow de L está contenido en $HC_G(Q)$.

Por el Lema 0.16., existe un q-subgrupo de Sylow Q_0 de L normalizado por Q. Entonces, $[Q,Q_0] \subseteq Q_0$. Además $[Q,Q_0] \subseteq H$, pues igual que antes $[Q,Q_0] = 1 \bmod H$. Luego $[Q,Q_0] \subseteq H \cap Q_0 = 1$, es decir $Q_0 \subseteq C_G(Q) \subseteq HC_G(Q)$. #

Lema 2.3. [Ben 2.3] Sea V un q-grupo elementalmente abeliano que actúa en el p-grupo B, $p \neq q$. Entonces $B = \langle C_B(U) \mid |V:U| = q \rangle$.

Demostración. Sea $A = \langle C_B(U) \mid |V:U| = q \rangle$. Ésta será una demostración larga. El método consistirá en ir reduciendo el problema a casos más fáciles, más manejables. Se demostrará en cada paso que sin pérdida de generalidad podemos suponer que:

1.- $A \lhd B$.
2.- B es abeliano.
3.- B es abeliano y V actúa irreduciblemente en B.
4.- B es abeliano y V actúa fiel e irreduciblemente en B.

Probaremos este último caso usando una consecuencia inmediata del Lema de Schur. A lo largo de la demostración U significa cualquiera de los subgrupos de V con índice q.

1.- S.P.G. $A \lhd B$.

Sean $B' = N_B(A) \subseteq B$ y $A' = \langle C_{B'}(U) \mid |V:U| = q \rangle$. Observamos que A es V-invariante, pues cada $C_B(U)$ lo es ya que V es abeliano (En efecto, si $c \in C_B(U)$, $v \in V$ y $u \in U$ tenemos $(vcv^{-1})u(vcv^{-1})^{-1} = vcv^{-1}uvc^{-1}v^{-1} = vcuc^{-1}v^{-1} = vuv^{-1} = u$ y, así, $vcv^{-1} \in C_B(U)$; esto es $C_B(U)$ es V-invariante).

También B' es V-invariante pues A lo es (si $v \in V$ y $n \in B' = N_B(A)$, $(vnv^{-1})A(vnv^{-1})^{-1} = vnv^{-1}Avn^{-1}v^{-1} = vnAn^{-1}v^{-1} = vAv^{-1} = A$, luego $vnv^{-1} \in N_B(A)$, y entonces $N_B(A)$ es V-invariante).

Veamos que $C_{B'}(U) = C_B(U)$. Sabemos que $C_{B'}(U) \subseteq C_B(U)$, ya que $B' \subseteq B$. Además $C_B(U) \subseteq C_{B'}(U)$, pues $C_B(U) \subseteq C_A(U) \subseteq C_{B'}(U)$ (porque $C_B(U) \subseteq A$ y $A \subseteq B'$). Entonces concluimos que $A' = A \lhd N_B(A) = B'$. Así tenemos que V es un q-grupo elementalmente abeliano que actúa en el p-grupo B' y $A' = \langle C_{B'}(U) \mid |V:U| = q \rangle \lhd B'$ y usando el teorema para el caso normal, tenemos $A' = B'$. Entonces $A = N_B(A)$ y, como en un p-grupo el único subgrupo que es su propio normalizador es el total, concluimos que $A = B$ y con esto queda demostrado el paso 1.

2.- S.P.G. B es abeliano.

Supondremos que el teorema vale cuando B es abeliano, y probaremos que vale cuando sólo $A \lhd B$. Usaremos inducción en el orden de B. Tomemos $B' = [B,B]$, entonces

$B' \subsetneq B$ pues B es un p-grupo (ver, por ejemplo el Teorema 0.24.). Entonces, por hipótesis de inducción, $B' = \langle C_{B'}(U) \mid |V:U| = q \rangle$. Por otro lado:

$$\frac{AB'}{B'} = \langle C_B(U) \mid |V:U| = q \rangle B'/B' = \langle C_B(U)B'/B' \mid |V:U| = q \rangle.$$

Por el Lema 2.2. $C_B(U)B'/B' = C_{B/B'}(U)$ y entonces:

$$\frac{AB'}{B'} = \langle C_{B/B'}(U) \mid |V:U| = q \rangle.$$

Pero B/B' es abeliano, luego para este grupo el teorema vale, y tenemos:

$$\frac{AB'}{B'} = \langle C_{B/B'}(U) \mid |V:U| = q \rangle = B/B'.$$

Y finalmente, por el teorema de la correspondencia, $AB'=B$. Pero $B' \subseteq A$, ya que $B' \subseteq B$ implica que $C_{B'}(U) \subseteq C_B(U)$. Resulta que $A=B$ y con ello concluimos el paso 2.

3.- S.P.G. B es abeliano y V actúa irreduciblemente en B.

Supondremos entonces que el teorema vale cuando B es abeliano y V actúa irreduciblemente en B y demostraremos que vale también cuando sólo B es abeliano. Usaremos inducción en el orden de B. Supondremos que V no actúa irreduciblemente en B. Podemos considerar B_0 un subgrupo de B minimal de entre los subgrupos de B que son V-invariantes y no triviales. Entonces $1 \neq B_0 \neq B$ y V actúa irreduciblemente en B_0. Tenemos

$$\begin{aligned} \frac{AB_0}{B_0} &= \langle C_B(U) \mid |V:U| = q \rangle B_0/B_0 \\ &= \langle C_B(U)B_0/B_0 \mid |V:U| = q \rangle \\ &= \langle C_{B/B_0}(U) \mid |V:U| = q \rangle && \text{(de nuevo por el Lema 2.2.)} \\ &= B/B_0 && \text{(por hipótesis de inducción).} \end{aligned}$$

Así, $AB_0 = B$ por el teorema de correspondencia, pero entonces $B_0 = \langle C_{B_0}(U) \mid |V:U| = q \rangle$ pues B_0 es V-irreducible. Así, $B_0 = \langle C_{B_0}(U) \mid |V:U| = q \rangle \subseteq \langle C_B(U) \mid |V:U| = q \rangle = A$ y en consecuencia $A = B$. Con lo que terminamos el paso 3.

4.- S.P.G. B es abeliano y V actúa fiel e irreduciblemente en B.

Ahora supondremos que el teorema vale cuando B es abeliano y V actúa fiel e irreduciblemente en B y demostraremos que también vale cuando sólo B es abeliano y V actúa irreduciblemente en B.

$\overline{V} = V/C_V(B)$ actúa fielmente en B. Si B_0 es un subgrupo de B que es $\overline{V}$-invariante no trivial, claramente es también $C_V(B)$-invariante, luego es $V \cong \overline{V} \times C_V(B)$-invariante (ya que V es elementalmente abeliano) y B no sería V-irreducible. Es decir, $\overline{V}$ actúa fiel e irreduciblemente en B. Entonces, aplicando el teorema en este caso, tenemos:

$$B = A' = \langle C_B(\overline{U}) \mid |\overline{V}:\overline{U}| = q \rangle = \langle C_B(C_V(B) \times \overline{U}) \mid |\overline{V}:\overline{U}| = q \rangle \subseteq \langle C_B(U) \mid |V:U| = q \rangle = A.$$

Y con esto termina el paso 4.

5.- Finalmente en este último caso, tenemos que V y B son abelianos y que V actúa fiel e irreduciblemente en B. Por el Corolario 1.5. al Lema de Schur, V tiene que ser cíclico y por tanto el teorema vale trivialmente. #

AUTOMORFISMOS DE p-GRUPOS

Lema 2.4. (Thompson) [Ben 2.2]

(i) Sea Q un p'-grupo que actúa en un p-grupo B. Si $C_B(A) \subseteq A$ con $A = C_B(Q)$, entonces $A = B$.

(ii) Sea $P \times Q$ el producto directo de un p-grupo P y de un p'-grupo Q que actúa en el p-grupo B. Si $[Q, C_B(P)] = 1$, entonces $[Q, B] = 1$.

(iii) Sea P un p-subgrupo del grupo soluble G. Entonces $O_{p'}(C_G(P)) \subseteq O_{p'}(G)$.

Demostración. (i) Supongamos de momento que Q es un q-grupo, $p \neq q$. Tenemos que $A = \{a \in B | aq = qa \ \forall q \in Q\}$ y $N_B(A) = \{n \in B | nAn^{-1} = A\}$. Entonces, $N_B(A)$ es Q-invariante, pues si $n \in N_B(A)$, $q \in Q$ y $a \in A$, existe una $\bar{a} \in A$ tal que $nan^{-1} = \bar{a}$. Luego, $(qnq^{-1})a(qnq^{-1})^{-1} = qnan^{-1}q^{-1} = q\bar{a}q^{-1} = \bar{a}$. Es decir, que $qnq^{-1} \in N_B(A)$ para toda $n \in N_B(A)$ y $q \in Q$. Pero entonces $N_B(A)Q$ es un subgrupo de BQ, pues Q normaliza a $N_B(A)$. Claramente $N_B(A) \lhd N_B(A)Q$ porque $N_B(A)$ es Q-invariante. Además obviamente $A \lhd N_B(A)$ y por tanto $n^{-1}anq = qn^{-1}an$, pues $n^{-1}an \in A = C_B(Q)$. En consecuencia $[Q, N_B(A)] \subseteq C_B(A) \subseteq A$, pues:

$$[q,n]a[q,n]^{-1} = qnq^{-1}n^{-1}anqn^{-1}q^{-1} = qnq^{-1}qn^{-1}ann^{-1}q^{-1} = qaq^{-1} = a.$$

Así, tenemos todas las condiciones del Teorema 2.1. para $T = Q$, $S = N_B(A)$ y $R = A = C_B(Q)$, y podemos concluir que $N_B(A) = A \cdot C_{N_B(A)}(Q)$. Observando también que $A = C_A(Q) \subseteq C_{N_B(A)}(Q) \subseteq C_B(Q) =: A$, tenemos que $N_B(A) = A$, pero sabemos que, en un p-grupo el único subgrupo que es su propio normalizador es el total, así que $A = B$ como se quería probar.

Si ahora quitamos la restricción de que Q sea un q-grupo, probaremos lo que se afirma en el inciso (i) usando el caso particular anterior:

Sea Q_q un p-Sylow de Q para cada $q \in \pi(Q)$. Observamos que Q_q actúa en B. Sea $A_q = C_B(Q_q)$; entonces $A = C_B(Q) = \bigcap_{q \in \pi(Q)} C_B(Q_q) = \bigcap_{q \in \pi(Q)} A_q$, pues Q está generado por sus subgrupos de Sylow. En particular $A \subseteq A_q$. Por hipótesis tenemos $C_B(A_q) \subseteq C_B(A) \subseteq A \subseteq A_q$. Aplicando el caso particular ya demostrado, tenemos $A_q = B$ para cada $q \in \pi(Q)$, y finalmente: $A = \bigcap_{q \in \pi(Q)} A_q = B$, con lo que queda probado el inciso (i).

(ii) Sea $X = B \rtimes (P \times Q)$; como P actúa en B, éstos forman un producto semidirecto: $B \rtimes P$ en donde Q actúa, asi $B \rtimes P$ y Q forman a su vez un producto

semidirecto: $X=(B\rtimes P)\rtimes Q$ y sabemos que Q actúa trivialmente en P. En algunos casos, escribiremos BP en lugar de $B\rtimes P$ para no cargar excesivamente la notación.

Tenemos que $P\subseteq C_{BP}(Q)$. Tomando centralizador en ambos lados obtenemos $C_{BP}(C_{BP}(Q))\subseteq C_{BP}(P)$, pues el centralizador invierte inclusiones.

Veamos que $C_{BP}(P)=C_B(P)C_P(P)$. Sean $b\in B$, $p\in P$. Si $bp\in C_{BP}(P)$, tenemos $bp\overline{p}=\overline{p}bp$ para toda $\overline{p}\in P$, pero $\overline{p}b=(\overline{p}b\overline{p}^{-1})\overline{p}=b'\overline{p}$ pues $B\lhd B\rtimes P$. Ahora por la unicidad de la representación de los elementos de $B\rtimes P$ como producto de un elemento de B y un elemento de P, obtenemos de $bp\overline{p}=\overline{p}bp=b'\overline{p}p$ que $b=b'$ y $p\overline{p}=\overline{p}p$, es decir $b\in C_B(P)$ y $p\in C_B(P)$, luego, $C_{BP}(P)\subseteq C_B(P)C_P(P)$ (la otra inclusión es obvia).

Así $C_{BP}(P)=C_B(P)C_P(P)\subseteq C_B(Q)P\subseteq C_{BP}(Q)$ (pues $[Q,C_B(P)]=1$ si y sólo si $C_B(P)\subseteq C_B(Q)$) y por tanto $C_{BP}(C_{BP}(Q))\subseteq C_{BP}(Q)$. Si en el inciso anterior tomamos $A=C_{BP}(Q)$ y reemplazamos B por $B\rtimes P$ tenemos $C_{B\rtimes P}(Q)=B\rtimes P$. En particular, $[Q,B]=1$, como quería probarse.

(iii) Sean $X=G/O_{p'}(G)$, $\overline{F}=O_p(X)$ y $U=O_{p'}(C_G(P))O_{p'}(G)$. Claramente $\overline{F}=F(X)$ es el subgrupo de Fitting de X. Sean F y $\overline{U}$ los correspondientes subgrupos a $\overline{F}$ y U según el teorema de la correspondencia.

Por el Lema 2.2. tenemos:

$$\overline{C_F(P)}=\frac{C_F(P)O_{p'}(G)}{O_{p'}(G)}=C_{F/O_{p'}(G)}(P)=C_F(P),\text{ pues } O_{p'}(G)\subseteq F.$$

Por el Teorema 0.29. $C_X(\overline{F})\subseteq\overline{F}$, ya que X es soluble. Luego: $[U,C_F(P)]\subseteq F$, pues F es normal en G y $[U,C_F(P)]\subseteq U$ porque $C_G(P)\supseteq C_F(P)$ normaliza a U. Tomando cocientes tenemos: $[\overline{U},C_F(P)]\subseteq\overline{U}\cap\overline{F}=1$. Pero entonces resulta que $\overline{U}\times P$ actúa en $\overline{F}$, y por el inciso anterior $[\overline{U},\overline{F}]=1$, es decir: $\overline{U}\subseteq C_X(\overline{F})\subseteq\overline{F}$. Esto implica que $\overline{U}=1$ porque $\overline{U}$ y $\overline{F}$ tienen órdenes que son primos entre sí. Entonces $U\subseteq O_{p'}(G)$. #

Teorema 2.5. (Huppert) [Gor 5.3.10] = [Ben 2.4] Sea A un p'-grupo que actúa en el p-grupo P con p impar. Si $[A,\Omega_1(P)]=1$ entonces $[A,P]=1$.

Demostración. Supongamos que el enunciado es cierto cuando A es un q-grupo, $q\neq p$. Entonces el teorema se sigue inmediatamente:

Sean A un p'-grupo, como en el teorema y $\{A_q\}$ sus q-subgrupos de Sylow; por hipótesis $[A,\Omega_1(P)]=1$, luego $[A_q,\Omega_1(P)]=1$ para cualquier q-Sylow A_q de A. Pero entonces $[A_q,P]=1$ por la suposición del párrafo anterior. Finalmente $[A,P]=1$, dado que A está generado por los A_q.

Supondremos de ahora en adelante que A es un q-grupo, $q\neq p$.
Haremos la prueba por inducción en $|P|$.

Caso Base: P es abeliano.

Por el Teorema 2.1., $P = C_P(A)[A,P]$. Por hipótesis, $\Omega_1([A,P]) \subseteq \Omega_1(P) \subseteq C_P(A)$. Supongamos $[A,P] \neq 1$.

Sea $1 \neq a = \varphi(b)b^{-1}$ $(=[\varphi,b])$, $\varphi \in A$, $b \in P$, un generador de $[A,P]$. Entonces, $1 \neq a^{|\varphi|/p} \in \Omega_1([A,P])$ y además $x := a^{|\varphi|/p} = \varphi(b^{|\varphi|/p})b^{-|\varphi|/p} = \varphi(y)y^{-1}$ (con $y = b^{|\varphi|/p}$). Así tenemos que $\varphi \in A$, $y \in P$, $1 \neq x = \varphi(y)y^{-1} \in \Omega_1([A,P]) \subseteq C_P(A)$. Luego $\varphi(y) = xy$; $\varphi^2(y) = \varphi(x)\varphi(y) = x\varphi(y) = x^2y$, ... , y de manera semejante $\varphi^r(y) = x^r y$. Pero tomando $r = |\varphi|$ resulta: $y = \varphi^r(y) = x^r y \Rightarrow x^r = 1 \Rightarrow x = 1$ (pues $(|\varphi|, p) = 1$). Contradicción. Luego $[A,P] = 1$. Con lo que termina el caso base.

Paso Inductivo:

Ciertamente, si Q es un subgrupo propio de P, A-invariante, tenemos $\Omega_1(Q) \subseteq \Omega_1(P)$; por hipótesis: $[A,\Omega_1(P)] = 1$, luego: $[A,\Omega_1(Q)] = 1$ y esto implica que $[A,Q] = 1$ por hipótesis de inducción. Luego A actúa trivialmente en todo subgrupo propio A-invariante de P.

Sea $C \, char \, P$ un subgrupo crítico de P (ver el Teorema 1.14. y la definición que sigue). Si $C \subsetneq P$, tenemos $[A,C] = 1$ por la observación anterior y entonces $[A,P] = 1$ por el Teorema 1.14.(iv) y en tal caso terminamos rápidamente. Supongamos entonces, en adelante, que $C = P$. Entonces, por el Teorema 1.14. :

(1) $cl(P) \leq 2$.
(2) $P/Z(P)$ es elementalmente abeliano.

En estas condiciones podemos aplicar el Teorema 0.34. y así, si $\varphi \in A$ y $x \in P$, tenemos: $(\varphi(x)x^{-1})^p = \varphi(x)^p x^{-p}$; por (2), $x^p \in Z(P)$ (pues en $P/Z(P)$ $\bar{x}^p = 1$). Si $Z(P) = P$, la afirmación ya se probó en el caso base, así que supondremos que $Z(P) \subsetneq P$.

Por la observación del principio $[A,Z(P)] = 1$, luego $(\varphi(x)x^{-1})^p = \varphi(x^p)x^{-p}$ $= x^p x^{-p} = 1$ y así $[\varphi,x] = \varphi(x)x^{-1} \in \Omega_1(P)$. Como todo $[A,P]$ es generado por elementos de esta forma, $[A,P] \subseteq \Omega_1(P)$ y, como A actúa trivialmente en $\Omega_1(P)$ (por hipótesis), resulta que A estabiliza a la serie subnormal $P \rhd \Omega_1(P) \rhd 1$ y por Teorema 0.19.: $[A,P] = 1$. #

Teorema 2.6. [Gor 5.3.13] Para primos impares p, un p-grupo P posee un subgrupo característico D de clase a lo más 2 y exponente p tal que todo p'-automorfismo no trivial de P induce un automorfismo no trivial de D.

Demostración. Sea C un subgrupo crítico de P, es decir: C es característico en P y
i) $cl(C) \leq 2$, $C/Z(C)$ es elementalmente abeliano.
ii) $[P,C] \subseteq Z(C)$.
iii) $C_P(C) = Z(C)$.
iv) Todo p'-automorfismo no trivial de P induce un automorfismo no trivial de C.
(¡Por el Teorema 1.14. existe!)

Sea $D = \Omega_1(C)$; entonces D tiene exponente p por (i) y por el Teorema 0.34.(i). Además $cl(D) \leq 2$, pues $[[D,D],D] \subseteq [[C,C],C] = 1$. Por otro lado D *char* P, ya que D *char* C *char* P. Más aún, de nuevo porque p es impar, todo p'-automorfismo no trivial de C induce un automorfismo no trivial de D (por el Teorema 2.5.). Pero todo p'-automorfismo no trivial de P induce un p'-automorfismo no trivial de C, y de esta forma concluimos. #

TEOREMAS DE ESTRUCTURA

Teorema 2.7. (Baer) [Ben II, B] Sea H un grupo de orden impar tal que $H/Z(H)$ es abeliano; entonces en el conjunto subyacente de H se puede definir una nueva operación "+" con las siguientes propiedades: (sea $H^+ := (H,+)$)

i) H^+ es un grupo abeliano.

ii) los elementos de H tienen el mismo orden en H^+.

iii) Cada automorfismo de H es también un automorfismo de H^+.

Demostración. Sea $\pi: H \to H/Z(H)$ la proyección natural. Si definimos $\sigma: H \to H$ como $\sigma(x) = x^2$, afirmamos que σ es biyectiva:

Si $x^2 = y^2$ para $x,y \in H$, entonces $\overline{x}^2 = \overline{y}^2$ ($\overline{x} := \pi(x)$; $\overline{y} := \pi(y)$). Como $H/Z(H)$ es abeliano, $\overline{x}^2 = \overline{y}^2$ implica $(\overline{x}\overline{y}^{-1})^2 = 1$, es decir, $\overline{x}\overline{y}^{-1} = 1$ (pues H y $H/Z(H)$ son de orden impar). Luego $\overline{x} = \overline{y}$ o bien $x = yz$ para alguna $z \in Z(H)$, pero entonces $y^2z^2 = x^2 = y^2$, es decir, $z^2 = 1$, y de nuevo, $z = 1$ (pues H es de orden impar). Se concluye entonces que $x = y$ con lo que queda probado que σ es biyectiva.

Concluimos entonces:

1) $x^2 = y^2$ si y sólo si $x = y$, $\forall x,y \in H$.
2) $x^{1/2} := \sigma^{-1}(x)$ está unívocamente definida $\forall x \in H$.
3) Todo subgrupo de H es cerrado bajo (la restricción de) σ y por tanto bajo σ^{-1}.
4) $[a,b] \in Z(H)$, $\forall a,b \in H$, es decir, $H' = [H,H] \subseteq Z(H)$
   (como $H/Z(H)$ es abeliano, $[a,b] = aba^{-1}b^{-1} \equiv 1 \bmod Z(H)$).
5) $[a,b]^{1/2} \in Z(H)$, $\forall a,b \in H$, (por 3 y 4).

Con estas observaciones definimos: $a + b := [b,a]^{1/2}ab$.

Entonces, claramente (para cualesquiera a y b en H):

6) $a + 1 = a = 1 + a$.
7) $a + a^{-1} = 1 = a^{-1} + a$.

8) $a+b=b+a$:

$$\begin{aligned}(a+b)^2 &= [b,a]abab \quad \text{(por 5)}\\ &= baab\\ &= ba[a,b]ba\\ &= (b+a)^2 \quad \text{(por 5)}\end{aligned}$$

Con esto concluimos que $a+b=b+a$, por (1).

También, para a, b y c en H:

9) $(a+b)+c=a+(b+c)$:

$$\begin{aligned}((a+b)+c)^2 &= ([b,a]^{1/2}ab+c)^2\\ &= ([c,[b,a]^{1/2}ab]^{1/2}[b,a]^{1/2}abc)^2\\ &= [c,[b,a]^{1/2}ab]\cdot[b,a]\cdot abcabc \qquad (5)\\ &= [c,ab]\cdot[b,a]\cdot abcabc \qquad (5)\\ &= cabc^{-1}b^{-1}a^{-1}[b,a]abcabc\\ &= c[b,a]abc^{-1}b^{-1}a^{-1}abcabc \qquad (4)\\ &= cbac^{-1}b^{-1}a^{-1}abcabc\\ &= cbaabc\end{aligned}$$

$$\begin{aligned}(a+(b+c))^2 &= (a+[c,b]^{1/2}bc)^2\\ &= ([[c,b]^{1/2}bc,a]^{1/2}a[c,b]^{1/2}bc)^2\\ &= [[c,b]^{1/2}bc,a]\cdot[c,b]\cdot abcabc \qquad (5)\\ &= [bc,a]\cdot[c,b]\cdot abcabc \qquad (5)\\ &= bcac^{-1}b^{-1}a^{-1}[c,b]abcabc\\ &= [c,b]bcac^{-1}b^{-1}a^{-1}abcabc \qquad (4)\\ &= cbac^{-1}b^{-1}a^{-1}abcabc\\ &= cbaabc\end{aligned}$$

Por (1) concluimos que '+' es asociativo.
Ahora, (6)-(9) nos dicen que H^+ es un grupo abeliano y con ello queda probado (i).

Como $a+b=ab$ cada vez que a y b conmutan ($[a,b]=1$, $1^{1/2}=1$) tenemos: $\underbrace{a+\ldots+a}_{r\text{ veces}}=\underbrace{a\cdot\ldots\cdot a}_{r\text{ veces}}$, es decir $r\cdot a=a^r$ y, en particular, tenemos (ii).

Finalmente, si $\varphi: H\to H$ es un automorfismo y si $x=a^{1/2}$, Dado que $\varphi(a)=\varphi(x^2)=\varphi(x)^2$, concluimos $\varphi(a)^{1/2}=\varphi(x)=\varphi(a^{1/2})$. Con ello en mente, resulta $\varphi(a+b)=\varphi([b,a]^{1/2}ab)=[\varphi(b),\varphi(a)]^{1/2}\varphi(a)\varphi(b)=\varphi(a)+\varphi(b)$. Y así terminamos. #

Lema 2.8. [Ben 2.5]=[Ben II, Satz] Sea A un p-subgrupo del grupo soluble G, $p \neq 2$. Si A contiene todos los elementos de orden p de su centralizador, entonces todos los p'-subgrupos A-invariantes de G están en $O_{p'}(G)$.

Demostración. Supongamos que el teorema es falso.

Entonces existe un p'-subgrupo K de G normalizado por A que no está contenido en $O_{p'}(G)$.

Sea $\overline{G} = G/O_{p'}(G)$. Si $g \in G$, $\overline{g}$ denotará la imagen de g bajo la proyección natural.

Dado que $O_q\left(G/O_{p'}(G)\right) = 1$, para cualquier primo q distinto de p, usando el Teorema 0.28. tenemos: $F(\overline{G}) = O_p(\overline{G})$.

Como K actúa en G y en $O_{p'}(G)$, luego actúa también en $\overline{G}$ y en $O_p(\overline{G})$. Si $\left[K, F(\overline{G})\right] = 1$ tendriamos $\left[\overline{K}, F(\overline{G})\right] = 1$, es decir, $\overline{K} \subseteq C_G(F(\overline{G}))$ y, por el Teorema 0.29., $\overline{K} \subseteq F(\overline{G})$; como $\overline{K}$ es un p'-grupo y $F(\overline{G}) = O_p(\overline{G})$ es un p-grupo, esto implica que $\overline{K} = 1$, es decir $K \subseteq O_{p'}(G)$; contrario a lo supuesto.

Luego K no centraliza a $F(\overline{G}) = O_p(\overline{G})$.

Sea H un subgrupo crítico de $O_p(\overline{G})$ (ver Teorema 1.14.), entonces:

1) $H/Z(H)$ es elementalmente abeliano.
2) Todo p'-automorfismo no trivial de $O_p(\overline{G})$ induce un automorfismo no trivial de H.
3) H *char* $O_p(\overline{G})$.

Entonces K actúa en H (por 3). Por otro lado, A actúa en G y en $O_{p'}(G)$ y, por tanto, en $\overline{G}$, $O_p(\overline{G})$ y H. Así, KA actúa en H. Además por (2), $[K, H] \neq 1$.

Sea H^* el grupo abeliano del Teorema 2.7. Gracias al Teorema 2.7. (iii), H^* es un KA-módulo.

Suponga que $\overline{g} \in C_H(A)$ y $|\overline{g}| = p$, entonces $[A, \overline{g}] = 1$ y esto implica que $[A, g] \subseteq O_{p'}(G)$ y además $g^p \in O_{p'}(G)$. Luego ${}^gA \subseteq AO_{p'}(G)$ (pues $aga^{-1}g^{-1} \in O_{p'}(G)$). Como A es un p-subgrupo de Sylow de $AO_{p'}(G)$, existe $d \in O_{p'}(G)$ tal que ${}^gA = {}^dA$; entonces ${}^{d^{-1}g}A = A$ y, en consecuencia, $\left[A, d^{-1}g\right] \subseteq A$. Por otro lado, $\overline{\left[A, d^{-1}g\right]} = \left[\overline{A}, \overline{d}^{-1}\overline{g}\right]$ $= \left[\overline{A}, \overline{g}\right] = 1$, es decir $\left[A, d^{-1}g\right] \subseteq O_{p'}(G)$, y así :

$$\left[A, d^{-1}g\right] \subseteq A \cap O_{p'}(G) = 1 \text{ (ya que } A \text{ es un } p\text{-grupo).}$$

También:

$$\left|\langle d^{-1}g\rangle\right|_p = \left|\frac{\langle d^{-1}g\rangle}{\langle d^{-1}g\rangle \cap O_{p'}(G)}\right|_p = \left|\overline{\langle d^{-1}g\rangle}\right|_p = |\langle \overline{g}\rangle| = p$$

Concluimos que cualquier p-subgrupo de Sylow de $\langle d^{-1}g\rangle$ centraliza a A y es isomorfo a Z_p; por hipótesis A contiene a cualquier p-subgrupo de Sylow de $\langle d^{-1}g\rangle$, luego $\overline{g} \in \overline{A}$. Como K es normalizado por A, tenemos $\left[\overline{K}, \overline{g}\right] \subseteq \left[\overline{K}, \overline{A}\right] \subseteq \overline{K}$. Por otro lado, ya que

$\overline{g} \in C_H(A) \subseteq H$, también sabemos que $[\overline{K}, \overline{g}] \subseteq [\overline{K}, H] \subseteq H$. Como $\overline{K}$ es un p'-grupo y H es un p-grupo, resulta que $[\overline{K}, \overline{g}] \subseteq \overline{K} \cap H = 1$. Así, sabemos que $\overline{g} \in C_H(K)$.

Hemos probado entonces que $\overline{g} \in C_H(A)$ y $|\overline{g}| = p$ implican que $\overline{g} \in C_H(K)$. Gracias al Teorema 2.7. tenemos:

(*) $\quad x \in C_{H^+}(A)$ y $|x| = p$ implican que $x \in C_{H^+}(K)$.

Sean $\mu: H^+ \to H^+$ la multiplicación por $|K|$ y $\tau: H^+ \to H^+$ la función definida por:

$$\tau(h) = \sum_{k \in K} {}^k h .$$

Como $(|K|, |H^+|) = 1$, μ es un automorfismo de H^+ (pues H^+ es abeliano), luego μ es un KA-automorfismo. Probemos que τ es un KA-endomorfismo y que $\sigma := \mu^{-1}\tau$ es (un KA-endomorfismo) idempotente:

4) $\tau(h_1 + h_2) = \sum_{k \in K} {}^k(h_1 + h_2) = \sum_{k \in K} {}^k h_1 + {}^k h_2 = \sum_{k \in K} {}^k h_1 + \sum_{k \in K} {}^k h_2 = \tau(h_1) + \tau(h_2)$.

En particular $\mu\tau = \tau\mu$ y $\mu^{-1}\tau = \tau\mu^{-1}$.

5) $\tau({}^x h) = \sum_{k \in K} {}^k({}^x h) = \sum_{k \in K} {}^{kx} h = \sum_{k \in K} {}^{x(x^{-1}kx)} h = {}^x\left(\sum_{k \in K} {}^{(x^{-1}kx)} h\right)$

$= {}^x\left(\sum_{x^{-1}kx \in K} {}^{(x^{-1}kx)} h\right) = {}^x(\tau(h)) = {}^x\tau(h)$, para cualquier x en KA.

6) $\sigma(\sigma(h)) = \mu^{-1}\tau(\mu^{-1}\tau(h)) = \mu^{-2}\tau^2(h) = \frac{1}{|K|^2} \sum_{k' \in K} \sum_{k \in K} {}^{k'k} h = \frac{1}{|K|^2} \cdot |K| \cdot \sum_{k \in K} {}^k h = \sigma(h)$.

Así, podemos descomponer a H^+ como $H^+ = \sigma H^+ \oplus (1-\sigma)H^+$.

Si $h \in C_{H^+}(K)$ tenemos $|K|h = \sum_{k \in K} {}^k h$, es decir, $\sigma(h) = h$; en particular, $h \in \sigma(H^+)$. Recíprocamente, si $h \in \sigma(H^+)$, entonces $h = \sigma(x)$ para alguna $x \in H^+$; luego $|K| \cdot {}^q(\sigma(x)) = \sum_{k \in K} {}^{qk} x = \sum_{qk \in K} {}^{qk} x = |K|\sigma(x)$, para cualquier $q \in K$. Así ${}^q h = h$, es decir $h \in C_{H^+}(K)$. Por lo tanto:

(**) $\qquad C_{H^+}(K) = \sigma(H^+)$

En particular $\sigma(H^+) \neq H^+$, pues $[K, H^+] = [K, H] \neq 1$, y en consecuencia $(1-\sigma)H^+ \neq 0$. Como A actúa en H^+ y σ es un KA-endomorfismo, tenemos que A actúa en $(1-\sigma)H^+$ (y en $\sigma(H^+)$). Como A y $(1-\sigma)H^+$ son ambos p-grupos, el centralizador de A

en $(1-\sigma)H'$ no puede ser trivial (por la ecuación de clase); asi, existe una $x \in C_{(1-\sigma)H'}(A)$ con $|x| = p$; por (*) y (**), $x \in \sigma(H')$ también y entonces $0 \neq x \in (1-\sigma)H' \cap \sigma(H') = 0$. Contradicción. #

Nota: Si A es un p-subgrupo elementalmente abeliano maximal del grupo G, es claro que A contiene a todo elemento de orden p de su centralizador. Así, el teorema anterior es directamente aplicable a tales subgrupos.

Lema 2.9. [Ben 2.9] Si un p-grupo P actúa no trivialmente en un q-grupo Q de rango ≤ 2, entonces $p \leq q$ o $q = 2$.

Demostración. Supondremos que $2 \neq q < p$ para llegar a una contradicción.

Por el Teorema 2.6. podemos asumir sin pérdida de generalidad que Q tiene exponente q. Ahora $|Z(Q)| < q^{r(Q)}$ o $Q = Z(Q)$ pues si $g \in Q - Z(Q)$, $Z(Q) \times \langle g \rangle$ es elementalmente abeliano y $|Z(Q) \times \langle g \rangle| \leq q^{r(Q)}$. Analizaremos ahora el orden de Q en dos casos:

Caso 1: Si $r(Q) = 1$, entonces $Q = Z(Q) \cong Z_q$ y $|Q| = q$.

Pues de otro modo $|Z(Q)| < q \Rightarrow |Z(Q)| = 1$, pero todo p-grupo tiene centro no trivial.

Caso 2: Si $r(Q) = 2$, tenemos que $|Q| = q^2$ ó q^3.

Como $Z(Q)$ es elementalmente abeliano, $|Z(Q)| \leq q^2$. Si $|Z(Q)| = q^2$, entonces $Q = Z(Q)$ ya que $Z(Q) \times \langle g \rangle$ es elementalmente abeliano para cada $g \in Q - Z(Q)$. Por otro lado, si $|Z(Q)| = q$, entonces podemos encontrar un subgrupo V tal que $Z(Q) \lhd V \lhd Q$ y $[V : Z(Q)] = q$ (por el Teorema 0.13.); V tiene que ser elementalmente abeliano y además maximal, por el supuesto $r(Q) = 2$.

Entonces $C_Q(V) = V$, pues $V\langle g \rangle$ es elementalmente abeliano de rango 3 para cualquier $g \in C_Q(V) - V$. Además, $Q/V = Q/C_Q(V)$ se inyecta en $Aut(V) \cong Aut(Z_q \times Z_q)$ pues Q actúa en V por conjugación; pero $|Aut(Z_q \times Z_q)| = (q^2-1)(q^2-q) = q(q-1)^2(q+1)$ y, como Q es un q-grupo, tenemos $|Q/V| \leq q$. Como $|V| = q^2$, tenemos $|Q| \leq q^3$.

En cualquiera de los dos casos resulta $|Q| \leq q^3$. Ahora veremos que, sin pérdida de generalidad, podemos suponer que $|Q| \leq q^2$ (reemplazando Q por $Q/Z(Q)$ si fuera necesario):

Si $|Q| = q^3$, entonces $|Z(Q)|$ debe ser igual a q. Como $Z(Q)$ es caracteristico, P actúa en $Z(Q)$, pero como $Aut(Z(Q)) \cong Aut(Z_q)$ y $|Aut(Z_q)| = q-1$ y $q < p$, resulta que P actúa trivialmente en $Z(Q)$. Afirmamos que P actúa no trivialmente en $Q/Z(Q)$. Si no, para toda $x \in Q$ y $\sigma \in P$ existiría una $z \in Z(Q)$ tal que $\sigma(x) = xz$ o bien $\sigma(x)x^{-1} \in Z(Q)$ que es equivalente a $[P,Q] \subseteq Z(Q) \lhd Q$. Tendríamos entonces $Z(Q) \lhd Q \lhd QP$ con $[P,Q] \subseteq Z(Q)$. Por el Teorema 2.1. $Q = Z(Q) \cdot C_Q(P)$, es decir, P actúa trivialmente en Q. Contradicción.

Finalmente, estamos suponiendo que P actúa no trivialmente en Q, $|Q| \leq q^2$, $2 \neq q < p$, pero entonces $Q \cong Z_q$ o $Q \cong Z_q \times Z_q$ implica que $p \| Aut(Z_q)|$ o $p \| Aut(Z_q \times Z_q)|$, es decir, $p|q-1$ o $p|q(q-1)^2(q+1)$. Así $p|q$ o $p|q-1$ o $p|q+1$, luego $p|q+1$ pues $q < p$, pero entonces $p = q+1$, lo que implica que p es par. Contradicción. #

Teorema 2.10. [Ben 2.10] Sean P y Q p- y q-subgrupos, respectivamente, no triviales de $GL(2,p)$, tales que P normaliza a Q. Suponga que $2 \neq p \neq q$. Si $[P,Q] \neq 1$, entonces $q = 2$; y si $q = 2$, entonces $r(Q) = 1$.

Demostración. Observamos en primer lugar que $q < p$, pues gracias al Lema 0.45., sabemos que p es el divisor primo de $|GL(2,p)|$ más grande, a menos que $p = 2$, que no es nuestro caso. Suponga que $R := [P,Q] \neq 1$; entonces $Q = R \cdot C_Q(P)$ por el Teorema 2.1. Así $[P,R] \neq 1$, pues de lo contrario $R \subseteq C_Q(P)$ y en consecuencia $Q = C_Q(P)$; pero entonces $[Q,P] = 1$, contrario a lo supuesto.

Observamos también que $R = [P,Q] \subseteq GL(2,p)' \subseteq SL(2,p)$. Entonces, por el Lema 0.47., si $q \neq 2$, R tiene que ser cíclico. Pero entonces $R \cong Z_{q^\alpha}$ y $|Aut(R)| = |Aut(Z_{q^\alpha})| = \varphi(q^\alpha) = q^\alpha - q^{\alpha-1} = q^{\alpha-1}(q-1)$ que no admite a $p > q$ como divisor. Esto contradice el hecho de que $[P,R] \neq 1$. Así, $q = 2$.

Demostraremos que $q = 2$ implica $r(Q) = 1$, en dos casos.

Caso I: $[P,Q] \neq 1$.

Todo lo que hemos dicho en los párrafos anteriores sigue vigente.

Por el Lema 0.48., R tiene un único elemento de orden 2 (y por lo tanto $r(R) = 1$), y así, todo subgrupo de orden 4 debe ser cíclico. Si R fuera abeliano, tendría entonces que ser cíclico. Pero $R \cong Z_{2^\alpha}$ implica $|Aut(R)| = 2^{\alpha-1}$ que, de nueva cuenta no admite a p como divisor y entonces P tendría que actuar trivialmente sobre R, lo cual contradice $[P,R] \neq 1$. Concluimos que R no es abeliano.

Así, R debe ser un 2-subgrupo de $SL(2,p)$, no abeliano, tal que todo subgrupo de orden 4 es cíclico. Por el Lema 1.12., tenemos que $|R| = 8$ (pues P actúa no trivialmente en R), pero entonces $R \cong Q_8$ (el único otro grupo no abeliano de orden 8 es D_4, el grupo diédrico, pero éste tiene más (5) elementos de orden 2). Entonces el Lema 0.43. nos dice que $|Aut(R)| = 8 \cdot 3$, es decir: $p = 3$.

Como P es de Sylow, sin pérdida de generalidad, podemos suponer que

$$P = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle.$$

Entonces, si $x=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C_Q(P)=C_Q\left(\left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle\right)$, tenemos que

$$\begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a & b \\ a+c & b+d \end{pmatrix}.$$

Esto es equivalente al sistema:

$$\begin{cases} a+b=a \\ c+d=a+c \\ b+d=d \end{cases} \quad \text{o bien,} \quad \begin{cases} b=0 \\ a=d \end{cases} \quad \text{es decir :} \quad x=\begin{pmatrix} a & 0 \\ c & a \end{pmatrix}.$$

Pero tal x tiene orden $|x|=p\cdot|a|$ (es fácil probar, por inducción, que $\begin{pmatrix} a & 0 \\ c & a \end{pmatrix}^r=\begin{pmatrix} a^r & 0 \\ ra^{r-1}c & a^r \end{pmatrix}$) a menos que $c=0$.

Como Q es un 2-grupo, tenemos $c=0$, $|a|=2^a$. Puesto que $p=3$, en $GL(2,p)$ sólo hay dos de tales matrices: la identidad y $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Así $C_Q(P)=\left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \subseteq R$, pues $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ es el único elemento de orden 2 de $SL(2,p)$.

Si ahora recordamos del inicio de la prueba que $Q=R\cdot C_Q(P)$, tenemos $Q=R$; pero ya sabemos que $r(R)=1$ así que $r(Q)=1$.

Caso II: $[P,Q]=1$.

Si $r(Q)\geq 2$, entonces, P centralizaría a algún subgrupo $U\subseteq Q$, con $U\cong Z_2\times Z_2$. Luego, si V es el espacio vectorial en el que $GL(2,3)$ actúa, P normalizaría a cada $C_V(u)$ para cualquier $u\in U^*$ ($U^*:=U-\{0\}$). En efecto, si $x\in P$ y $v\in C_V(u)$, tenemos que $xu=ux$ implica que $x(v)=x(u(v))=u(x(v))$, y así $x(v)\in C_V(u)$.

Pero entonces, P centralizaría a cada $C_V(u)$ para $u\in U^*$ pues, si $C_V(u)=\{0\}$ es obvio, y si $dim(C_V(u))=1$, entonces $C_V(u)\cong Z_p$ y $|Aut(C_V(u))|=p-1$, que no admite a p como divisor ($dim(C_V(u))=2$ implica $u=1$). Por el Lema 2.3. (aplicado al q-grupo U actuando en el p-grupo V), tenemos que $V=\langle C_V(u)|u\in U^*\rangle$. Entonces P centralizaría a todo V, lo que no puede ser, pues P no es trivial. #

Con estas herramientas, podemos ahora probar el siguiente Lema, de carácter técnico, que será necesario más adelante.

Del capítulo 0 (Definición 0.36), recordamos que si P es un p-grupo, definimos:

$$J(P)=\langle A\subseteq P|A \text{ es elementalmente abeliano y } r(A)=r(P)\rangle.$$

Recuerde también que $J(P)\ char\ P$, que $J(P)\subseteq U\subseteq P$ implica $J(P)=J(U)$, y que si G_p es un p-Sylow de un grupo G, entonces: $J(G_p)\lhd G$ si y sólo si $J(G_p)\subseteq O_p(G)$.

Teorema 2.11. (Thompson) [Ben 2.11] Sea X un grupo, con $|X:O_{p,q}(X)|=p$ y $2\neq p\neq q$. Sean $Z=\Omega_1(Z(O_p(X)))$ y $Y=X/C_X(Z)$. Suponga que $J(P)$ no es normal en X para algún p-subgrupo de Sylow P de X y que P_1 y P_2 son p-subgrupos de Sylow de Y distintos. Entonces $q=2$, $|Z:C_Z(\langle P_1,P_2\rangle)|=p^2$ y $\langle P_1,P_2\rangle$ contiene exactamente una involución.

Demostración. Tenemos que $|X|=p^aq^b$, pues $|O_{p,q}(X)|=|O_q(X/O_p(X))|\cdot|O_p(X)|$, y además $|X|=|O_q(X/O_p(X))|\cdot|O_p(X)|\cdot p$. También tenemos que $O_p(X)$ tiene índice p en cualquier p-subgrupo de Sylow de X. Además $O_p(X)\subseteq C_X(Z)$ por la definición de Z. Como Y tiene p-subgrupos de Sylow, resulta:

$$p\leq |Y|_p=|X/C_X(Z)|_p=\left|\frac{X}{O_p(X)}\Big/\frac{C_X(Z)}{O_p(X)}\right|_p$$

$$=|X/O_p(X)|_p\Big/|C_X(Z)/O_p(X)|_p=p\Big/|C_X(Z)/O_p(X)|_p$$

y esto implica que $|Y|_p=p$ y $\left|\frac{C_X(Z)}{O_p(X)}\right|_p=1$; es decir que $O_p(X)$ es un p-subgrupo de Sylow de $C_X(Z)$. Como Y tiene al menos 2 p-subgrupos de Sylow, Y no puede ser un p-grupo, así: $|Y|=pq^\alpha$ para algún entero $\alpha\neq 0$.

Sea $G=\langle P_1,P_2\rangle\subseteq Y$; entonces $G=QP_1$ con Q un q-subgrupo de Sylow de G, con $[Q,P_1]\neq 1$, pues de otro modo P_1 seria normal en G. Por el Corolario 1.2., $Q\lhd G$.

Afirmamos que debe existir un p-grupo elementalmente abeliano $A\subseteq X$ de rango $r(P)$, que no está contenido en $O_p(X)$, pues de otro modo: $J(P)\subseteq O_p(X)\subseteq P$ y esto implicaria que $J(P)=J(O_p(X))$; pero entonces $J(P)\ char\ O_p(X)\ char\ X$ y en particular $J(P)\lhd X$; contrario a lo supuesto. Si tomamos $A_0=A\cap O_p(X)$, como $O_p(X)$ tiene índice p en cualquier p-subgrupo de Sylow de X y $A\not\subseteq O_p(X)$, tenemos que $AO_p(X)$ es un p-subgrupo de Sylow de X y por lo tanto:

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

Además, dado que Z conmuta con todo $O_p(X)$, ZA_0 es elementalmente abeliano, y como A es elementalmente abeliano de rango máximo, resulta $|ZA_0|\leq|A|$.

Recordando que $Z \subseteq O_p(X)$, tenemos $Z \cap A = O_p(X) \cap Z \cap A_0 = Z \cap A_0$, luego:

$$|Z: Z \cap A| = |Z: Z \cap A_0| = \frac{|Z|}{|Z \cap A_0|} = \frac{|ZA_0|}{|A_0|} \leq \frac{|A|}{|A_0|} = p.$$

Por otro lado $C_Z(A) = A \cap Z = A_0 \cap Z$, pues si $x \in C_Z(A) - A$, $\langle A, x \rangle$ sería elementalmente abeliano, de rango mayor que A (contradiciendo su maximalidad).

Ahora bien, como $O_p(X)$ es el único p-subgrupo de Sylow de $C_X(Z)$ tenemos que

$$\frac{AC_X(Z)}{C_X(Z)} \cong \frac{A}{A \cap C_X(Z)} = \frac{A}{A \cap O_p(X)} = \frac{A}{A_0}.$$

Entonces $\left|\frac{AC_X(Z)}{C_X(Z)}\right| = p$, es decir, $\frac{AC_X(Z)}{C_X(Z)}$ es un p-subgrupo de Sylow de Y. Decimos que A *induce* un p-subgrupo de Sylow de Y en este sentido.

Pero cuanto hemos dicho sobre A vale para cualquiera de sus conjugados. Entonces todos los p-subgrupos de Sylow de Y son *inducidos* por algún conjugado de A. En efecto, $AO_p(X)$ es un p-Sylow de X y por tanto, todos los p-Sylows de X son de la forma ${}^x(AO_p(X)) = {}^xA \cdot O_p(X)$ para alguna x en X; y estos Sylows de X están en correspondencia biunívoca con los de Y. En particular, tenemos dos subgrupos A_1 y A_2, conjugados de A, tales que:

(1) $$P_1 = \frac{A_1 C_X(Z)}{C_X(Z)},\ P_2 = \frac{A_2 C_X(Z)}{C_X(Z)}.$$

Sabemos además que:

(2) $r(A_1) = r(A_2) = r(A) = r(P)$.
(3) $A_1, A_2 \not\subseteq O_p(X)$.
(4) $|Z: C_Z(A_1)| = [Z: Z \cap A_1] \leq p$ y $|Z: C_Z(A_2)| = [Z: Z \cap A_2] \leq p$

Pero entonces: $C_Z(P_1) = C_Z\left(\frac{A_1 C_X(Z)}{C_X(Z)}\right) = C_Z(A_1 C_X(Z)) = C_Z(A_1)$, y de manera semejante: $C_Z(P_2) = C_Z(A_2)$.

Luego:

$$|Z: C_Z(QP_1)| = |Z: C_Z(\langle P_1, P_2 \rangle)| = |Z: C_Z(P_1) \cap C_Z(P_2)| = \frac{|Z|}{|C_Z(P_1) \cap C_Z(P_2)|}$$

$$= \frac{|Z|}{|C_Z(P_1)|} \cdot \frac{|C_Z(P_1)|}{|C_Z(P_1) \cap C_Z(P_2)|} \leq p \frac{|C_Z(P_1)|}{|C_Z(P_1) \cap C_Z(P_2)|} = p \frac{|C_Z(P_1) \cdot C_Z(P_2)|}{|C_Z(P_2)|} \leq p \frac{|Z|}{|C_Z(P_2)|} \leq p^2.$$

Por otro lado, X actúa en Z, luego $X/C_X(Z)$ actúa fielmente en Z; entonces Q y P_1 actúan fielmente en Z, y en consecuencia Q y P_1 actúan en $Z/C_Z(QP_1)$. Afirmamos que Q y P_1 actúan fielmente en $Z/C_Z(QP_1)$:

Si Q no actúa fielmente en $Z/C_Z(QP_1)$, sea $\sigma \in Q$ con $\sigma \neq 1$, tal que σ actúa trivialmente en $Z/C_Z(QP_1)$. Entonces $\langle\sigma\rangle$ estabiliza a la serie subnormal: $Z \rhd C_Z(QP_1) \rhd 1$ y, por el Teorema 0.19., $\langle\sigma\rangle$ actúa trivialmente en Z. Esto contradice el hecho de que Q actúa fielmente en Z.

Si P_1 no actúa fielmente en $Z/C_Z(QP_1)$, como $P_1 \cong Z_p$, P_1 tendría que actuar trivialmente; luego también P_2 actúa trivialmente (por ser conjugado de P_1), pero entonces $Q \subseteq \langle P_1, P_2\rangle$ nos lleva a una contradicción.

Afirmamos que QP_1 actúa fielmente en $Z/C_Z(QP_1)$:

Si el núcleo de la acción contiene un q-grupo no trivial, éste tiene que estar contenido en el único q-subgrupo de Sylow de QP_1, a saber, Q. Esto que contradice el que Q actúa fielmente. Entonces el núcleo de la acción debe ser un p-subgrupo normal, y por tanto estar contenido en todos los p-Sylows de QP_1; esto obliga a que el núcleo de la acción sea trivial; es decir: QP_1 actúa fielmente en $Z/C_Z(QP_1)$.

Así tenemos que $|Z/C_Z(QP_1)| = p^2$, pues si $|Z/C_Z(QP_1)| = 1$ ó p, P_1 no podría inyectarse en los automorfismos de $Z/C_Z(QP_1)$. Ahora por el Teorema 2.10., $q = 2$. Por el Lema 0.45. y dado que $SL(2,p)$ es normal en $GL(2,p)$, resulta que todo p-Sylow de $GL(2,p)$ es también un p-Sylow de $SL(2,p)$; es decir P_1 y P_2, están contenidos (en realidad se inyectan) en $SL(Z/C_Z(QP_1))$ y por el Lema 0.48. $\langle P_1, P_2\rangle$ tiene exactamente una involución. #

3. El contraejemplo minimal

En este capítulo empezamos propiamente a demostrar el teorema de Burnside. La demostración quedará concluida en el capítulo 6.

Advertencia: Todos los resultados que se presentan a partir de este momento y hasta el final del capítulo 6 asumen que existe un contraejemplo minimal al teorema de Burnside, es decir que el teorema de Burnside es FALSO.

El objetivo principal de este capítulo es probar el Lema A que se enuncia al final y que será de gran utilidad en la demostración del teorema que nos ocupa.

Supondremos entonces a partir de aquí y hasta el capítulo 6 que G es un contraejemplo minimal al teorema de Burnside.

Luego todo subgrupo propio de G es soluble y G es simple (si ese no fuera el caso, G sería extensión de dos grupos solubles y, por lo tanto, sería soluble); además $|G| = p^{\alpha}q^{\beta}$ donde p y q son primos distintos y $\alpha, \beta \geq 1$, pues todo p-grupo es soluble (de hecho, podríamos tomar $\alpha, \beta \geq 2$ gracias al Teorema 1.1., pero no haremos uso de ello).

Si A es un subgrupo de G, para $r = p$ o $r = q$, definimos:

$$\mathcal{L}_r = \left\{ K \leq G \;\middle|\; \begin{array}{l} K = N_G(X) \text{ ó } K = C_G(X), \text{ donde } X \text{ es un} \\ r\text{-subgrupo no trivial de } G \end{array} \right\}$$

$$\mathcal{J}(A,r) = \{ H \leq G \mid H \text{ es un } r\text{-subgrupo } A\text{-invariante de } G \}$$

También definimos a $\mathcal{L}_r^*$ y $\mathcal{J}^*(A,r)$ como los conjuntos formados por los elementos maximales de $\mathcal{L}_r$ y $\mathcal{J}(A,r)$ respectivamente. Observamos que si $H \in \mathcal{L}_q$, entonces $O_q(H) \neq 1$ y $H \subsetneq G$. También, si $H \in \mathcal{L}_q^*$, entonces $H = N_G(O_q(H))$.

Llamaremos *central* a cualquier r-subgrupo (o r-elemento) no trivial que esté contenido en el centro de un r-subgrupo de Sylow de G.

Lema 3.1. [Ben 3.1] Si $G = XY$, con $X \neq G$ y Y subgrupos de G, entonces Y no normaliza a ningún subgrupo no trivial de X.

Demostración. Si Y normaliza a un subgrupo $N \neq 1$ de X, tenemos $1 \neq N \subseteq \bigcap_{y \in Y} X^y = \bigcap_{g \in G} X^g \lhd G$, pero $\bigcap_{g \in G} X^g \subseteq X \subsetneq G$, contradiciendo la simplicidad de G. #

Lema 3.2. [Ben 3.2] Ningún p-subgrupo de Sylow de G normaliza a ningún q-subgrupo no trivial (y viceversa).

Demostración. Esto se sigue de inmediato del Lema 3.1., ya que $G = PQ$ para cualesquiera $P \in Syl_p(G)$ y $Q \in Syl_q(G)$. Claramente la situación es simétrica para p y q. #

Lema 3.3. [Ben 3.3] Si z es un p-elemento central y $Q \in Syl_q(G)$, entonces $\langle Q, z\rangle = G$.

Demostración. Como z es un p-elemento central, $C_G(z)$ contiene un p-Sylow de G, luego $G = \langle Q, z\rangle C_G(z)$. Pero ahora $C_G(z)$ normaliza (de hecho centraliza) a $1 \neq \langle z\rangle \subseteq \langle Q, z\rangle$ lo que contradice al Lema 3.1., a menos que $G = \langle Q, z\rangle$. #

Lema 3.4. [Ben 3.4] Ningún p-subgrupo central normaliza a ningún q-subgrupo central.

Demostración. Suponga que Q es un q-subgrupo central normalizado por un p-subgrupo central; entonces $N_G(Q)$ contiene a un q-Sylow de G y a un p-elemento central. Por el Lema 3.3., tenemos: $1 \neq Q \lhd N_G(Q) = G$, en contradicción con la simplicidad de G. #

Lema 3.5. [Ben 3.5] Sea P un p-subgrupo de G con la propiedad de que, cada vez que $P \subseteq H \in \mathcal{L}_q$, todos los q-subgrupos P-invariantes de H están contenidos en $O_q(H)$.

(i) Si $P \subseteq H \in \mathcal{L}_q$, entonces $O_q(H) \in \mathcal{J}^*(P,q)$.

(ii) Si Q_1 y Q_2 son elementos distintos de $\mathcal{J}^*(P,q)$, entonces $Q_1 \cap Q_2 = 1$.

Demostración. Probemos (i):

Supongamos que $P \subseteq H \in \mathcal{L}_q$.

Claramente $H \subseteq N_G(O_q(H)) \in \mathcal{L}_q$ (recuerde que $H \in \mathcal{L}_q$, implica $O_q(H) \neq 1$). Como H es maximal tenemos: $H = N_G(O_q(H))$. También $O_q(H) \in \mathcal{J}(P,q)$, pues $O_q(H)$ *char* H. Si ahora $O_q(H) \subseteq K \in \mathcal{J}(P,q)$, tenemos que $N_K(O_q(H))$ es un q-subgrupo P-invariante. Dado que $N_K(O_q(H)) \subseteq N_G(O_q(H)) = H$, resulta que $N_K(O_q(H)) \subseteq O_q(H)$ (por hipótesis) y, por tanto, $N_K(O_q(H)) = O_q(H)$. Pero en un q-grupo, el único subgrupo que es igual a su propio normalizador es el total, luego: $K = O_q(H)$, y así $O_q(H)$ es maximal.

Supongamos ahora que (ii) es falso.

Escogemos $D = Q_1 \cap Q_2$ maximal, sujeto a las condiciones $D \neq 1$, $Q_1 \neq Q_2$ y $Q_1, Q_2 \in \mathcal{J}^*(P,q)$.

Afirmamos que $N_{Q_i}(D) \subseteq O_q(N_G(D))$ para $i = 1,2$. En efecto, como D y Q_i son P-invariantes, también lo es $N_{Q_i}(D) \subseteq N_G(D)$; pero $P \subseteq N_G(D) \in \mathcal{L}_q$, luego $N_{Q_i}(D) \subseteq O_q(N_G(D))$ por hipótesis.

$O_q(N_G(D))$ es, por supuesto, P-invariante, pues G y D lo son. Luego podemos tomar $Q_3 \in \mathcal{J}^*(P,q)$ tal que $O_q(N_G(D)) \subseteq Q_3$. Entonces $D \subsetneq N_{Q_i}(D) \subseteq Q_i \cap Q_3$, porque en

un q-grupo el único subgrupo que es su propio normalizador es el total. Así, por la maximalidad de D, $Q_1 = Q_3 = Q_2$. Contradicción. #

Lema 3.6. [Ben 3.6] Si Y es un p-subgrupo de G y $Y \subseteq H \subsetneq G$, entonces $H \cap O_q(C_G(Y)) \subseteq O_q(H)$.

Demostración. Como $H \subsetneq G$, H es soluble. Dado que Y es un p-grupo, por el Lema 2.4.(iii), tenemos $O_q(C_H(Y)) \subseteq O_q(H)$. Ahora bien: $H \cap O_q(C_G(Y)) \subseteq C_H(Y)$, pues $O_q(C_G(Y)) \subseteq C_G(Y)$. Pero $C_H(Y) \subseteq H$ normaliza a H y, por otro lado, $C_G(Y)$ (y por tanto $C_H(Y)$) normaliza a $O_q(C_G(Y))$; luego $H \cap O_q(C_G(Y)) \lhd C_H(Y)$. Así, $H \cap O_q(C_G(Y)) \subseteq O_q(C_H(Y)) \subseteq O_q(H)$. #

Lema 3.7. [Ben 3.7, Ben 3.8] Si Y es un p-subgrupo de G tal que $O_q(C_G(Y)) \neq 1$, entonces existe un p-subgrupo X de G que satisface:

(1) $O_q(C_G(X)) \neq 1$

(2) $|X| = p$

(3) Para todo $P \in Syl_p(C_G(X))$, si $P \subseteq H \subsetneq G$ entonces todo q-subgrupo P-invariante de H está contenido en $O_q(H)$.

Demostración. Notemos que $Y \neq 1$, pues G es simple.

Si $y \in Z(Y)^*$ con $|y| = p$, tenemos que $Y \subseteq C_G(y) \subsetneq G$ (si no, $\langle y \rangle \lhd G$). Por el Lema 3.6.: $C_G(y) \cap O_q(C_G(Y)) \subseteq O_q(C_G(y))$, pero $O_q(C_G(Y)) \subseteq C_G(Y) \subseteq C_G(y)$.

Luego $1 \neq O_q(C_G(Y)) \subseteq O_q(C_G(y))$. Ahora $X := \langle y \rangle$ es un p-subgrupo de G que satisface (1) y (2).

Supondremos de ahora en adelante que Y es un p-subgrupo de G que satisface (1) y (2), y demostraremos que existe otro p-subgrupo X que satisface (1)-(3).

Caso 1. $p \neq 2$.

Afirmamos que $X=Y$ funciona:

Claramente X está contenido en un p-subgrupo elementalmente abeliano maximal A de G. Entonces $A \subseteq C_G(X)$. Podemos escoger A (conjugando en $C_G(X)$), de tal forma que $X \subseteq A \subseteq P$, para cualquier $P \in Syl_p(C_G(X))$. Luego, si $P \subseteq H \subsetneq G$, tenemos que todo q-subgrupo P-invariante de H es también A-invariante y por el Lema 2.8. (y la nota que le sigue), está contenido en $O_q(H)$.

Caso 2. $p = 2$.

Veamos primero que existe un p-subgrupo X de G que satisface (1) y (2) y además:

$$|P| = \frac{|G|_2}{2} \qquad (\text{con } P \in Syl_p(C_G(X))).$$

Y no es central, pues de otro modo $C_G(Y)$ contendría a un p-Sylow de G y por el Lema 3.2., $O_q(C_G(Y)) = 1$, que es una contradicción.

Entonces G tiene al menos dos clases de conjugación de involuciones, si no, y (para $\langle y \rangle = Y$) sería conjugada a una involución central, y entonces Y mismo sería central.

Si $\overline{T}$ es un p-Sylow de G, por el Lema 1.13., existe una $\overline{U} \lhd \overline{T}$, con $\overline{U} \cong Z_p \times Z_p$ y $\overline{U}^g \subseteq C_G(Y)$ para alguna $g \in G$. Si definimos $U := \overline{U}^g$ y $T := \overline{T}^g$, tenemos $U \lhd T$, $T \in Syl_p(G)$, $U \cong Z_p \times Z_p = Z_2 \times Z_2$ y $U \subseteq C_G(Y)$. Como T actúa en U, $T/C_T(U)$ se inyecta en $Aut(U) \cong S_3$ y en consecuencia $|T : C_T(U)| \leq 2$. Así, $|G|_2 \leq 2|C_T(U)|$. Se sigue que $\frac{|G|_2}{2} \leq |C_G(U)|_2$.

Como $U \subseteq C_G(Y) \rhd O_q(C_G(Y))$, U actúa en $O_q(C_G(Y)) =: Q$ y por el Lema 2.3., $Q = \langle C_Q(u) \mid u \in U^* \rangle$. Entonces existe una $u \in U^*$, tal que $C_Q(u) \neq 1$. Por Lema 3.6., $Y \subseteq C_G(u) \subsetneq G$ implica que $1 \neq C_Q(u) = C_G(u) \cap O_q(C_G(Y)) \subseteq O_q(C_G(u))$. Si tomamos $X := \langle u \rangle$, tenemos: $\frac{|G|_2}{2} \leq |C_G(U)|_2 \leq |C_G(u)|_2 = |P|$ para $P \in Syl_p(C_G(X))$.

Pero P no puede ser un p-Sylow de G, pues entonces éste normalizaría a $O_q(C_G(X)) \neq 1$, contrario al Lema 3.2. Luego $|P| = \frac{|G|_2}{2}$.

Entonces, X satisface (1) y (2) y, para cualquier $P \in Syl_p(C_G(X))$, $|P| = \frac{|G|_2}{2}$.

Afirmamos que esta X satisface también (3).

Supongamos ahora que $P \in Syl_p(C_G(X))$, que tenemos un subgrupo H con $P \subseteq H \subsetneq G$ y que $H_0 \subseteq H$ es un q-subgrupo, P-invariante. Tenemos que probar que $H_0 \subseteq O_q(H)$.

Hay dos posibilidades:

Caso 2.1. $P \in Syl_p(H)$.

Entonces $H = \overline{Q}P$, con $H_0 \subseteq \overline{Q} \in Syl_q(H)$, luego:

$H_0 \subseteq \bigcap_{p \in P} \overline{Q}^p = \bigcap_{g \in H} \overline{Q}^g \lhd H$ y así: $H_0 \subseteq O_q(H)$.

Caso 2.2. $P \notin Syl_p(H)$.

Tenemos: $P \subsetneq T \in Syl_p(H)$, $T \in Syl_p(G)$ y $|T : P| = 2$.

Por el Lema 3.2., $O_q(H) = 1$. Además, por el Teorema 0.28., $F := F(H) = O_p(H)$.

Tenemos entonces dos subcasos:

Subcaso 2.2.1. $F \subseteq P$.

Entonces F actúa en H_0 y viceversa; así $[H_0, F] \subseteq H_0 \cap F = 1$, luego $H_0 \subseteq C_H(F) \subseteq F$ (por el Teorema 0.29.), y en consecuencia, $H_0 = 1$.

Subcaso 2.2.2. $F \not\subseteq P$.

FP es claramente un grupo, pues P normaliza a F. Como F es normal en H, está contenido en todos los p-Sylows de H, en particular en T. Entonces, por la maximalidad de P en T, resulta que $T = FP$. Así $TH_0 = FPH_0 =: K$ es un grupo, pues P normaliza a H_0 y ambos normalizan a F.

Observamos que H_0 es un q-Sylow de K, y en consecuencia, H_0 es un q-Sylow de $N_K(H_0)$. Ahora ya es claro que $H_0 = O_q(N_K(H_0))$. Por otro lado, $PH_0 \subseteq N_K(H_0)$ implica que $|K: N_K(H_0)| \leq |K: PH_0| = |TH_0: PH_0| \leq 2$ y en consecuencia $N_K(H_0) \lhd K$.

Así, $H_0 = O_q(N_K(H_0))$ *char* $N_K(H_0) \lhd K$, luego $H_0 \lhd K$ y por lo tanto $H_0 = 1$, gracias al Lema 3.2., porque K contiene a T que es un p-Sylow de G. #

Nota 3.8. El objetivo de los lemas 3.9 al 3.14 es probar que no existe ningún p-subgrupo X de G con la propiedad $O_q(C_G(X)) \neq 1$. Gracias al lema anterior, basta probar que no existe un p-subgrupo X de G que satisface:

(1) $O_q(C_G(X)) \neq 1$

(2) $|X| = p$

(3) Para todo $P \in Syl_p(C_G(X))$: Si $P \subseteq H \subsetneq G$ entonces todo q-subgrupo P-invariante de H está contenido en $O_q(H)$.

Así que:

Supondremos, a lo largo del texto que abarca los lemas 3.9 al 3.12 y el 3.14, que X es uno de tales p-subgrupos. Note que cualquier $P \in Syl_p(C_G(X))$ satisface los supuestos del Lema 3.5.

También, a lo largo de los mismos lemas **fijamos** Q:

$$Q := O_q(C_G(X)) \neq 1,$$

y **escogemos** P, H y x, como sigue.

$P \in Syl_p(C_G(X))$.

$C_G(X) \subseteq H$, H maximal en G.

$X = \langle x \rangle$.

Lema 3.9. [Ben 3.9]

(i) $O_q(H) \in \mathcal{J}^*(P,q)$ y $H = N_G(O_q(H))$.

(ii) Existe una $g \in G$, tal que $H^g \neq H$ y $P \subseteq H^g$.

(iii) Si g es como en (ii), $O_q(H^g) \in \mathcal{J}^*(P,q)$ y $O_q(H^g) \cap H = 1$.

(En particular, $O_q(H) \neq O_q(H^g)$).

Demostración. Recuerde que los supuestos de la Nota 3.8. están vigentes.

Observamos en primer lugar que $1 \neq Q = H \cap Q \subseteq O_q(H)$ (por el Lema 3.6.). Entonces, por la maximalidad de H y como $H \subseteq N_G(O_q(H))$, tenemos $H = N_G(O_q(H)) \in \mathcal{L}_p^*$. Ya que $P \subseteq H \in \mathcal{L}_p^*$, tenemos: $O_q(H) \in \mathcal{J}^*(P,q)$ por el Lema 3.5.. Así, queda probado (i).

Por el Lema 3.2., H no contiene un p-Sylow de G. Sea $H_p \in Syl_p(H)$, con $P \subseteq H_p$.

Como el normalizador de H_p en un p-Sylow T de G que contenga a H_p contiene propiamente a H_p, tenemos que $N_G(H_p) - H \neq \phi$. Sea $g \in N_G(H_p) - H$. Entonces $P \subseteq H_p = H_p^g \subseteq H^g$, además $H^g \neq H$ (pues si $H^g = H$, entonces $H \lhd \langle H, \langle g \rangle \rangle = G$, por la maximalidad de H). Es decir: (ii).

Puesto que también $O_q(H^g) \neq 1$ y H^g es a su vez maximal, resulta $H^g \subseteq N_G(O_q(H^g))$ y $H^g = N_G(O_q(H^g)) \in \mathcal{L}_p^*$. Luego, $O_q(H^g) \in \mathcal{J}^*(P,q)$ (otra vez por el Lema 3.5.).

Finalmente, dado que H y $O_q(H^g)$ son P-invariantes, $H \cap O_q(H^g)$ es un q-subgrupo P-invariante de H; por los supuestos de la Nota 3.8., $H \cap O_q(H^g) \subseteq O_q(H)$. Luego $H \cap O_q(H^g) = 1$, por el Lema 3.5.(ii). Entonces, (iii) también es verdadero. #

Lema 3.10. [Ben 3.10]

$|\Omega_1(Z(P))| = p^2$.

Si $P \subseteq T \in Syl_p(G)$, entonces $\Omega_1(Z(T)) \subseteq \Omega_1(Z(P))$.

Demostración. Asumimos, como ya se dijo, los supuestos de la Nota 3.8.

Sean $A := \Omega_1(Z(P))$, $g \in G$ como en el lema anterior, $Q_1 := O_q(H)$ y $Q_2 := O_q(H^g)$.

Afirmamos que, si $a \in A^*$ entonces $C_{Q_1}(a) = 1$ o $C_{Q_2}(a) = 1$.

Observamos que $P \subseteq C_G(a)$, y entonces $O_q(C_G(a)) \in \mathcal{J}(P,q)$. También $C_G(a) \in \mathcal{L}_p$. Como $\langle a \rangle$, Q_1 y Q_2 son P-invariantes, también lo son $C_{Q_1}(a)$ y $C_{Q_2}(a)$; por la Nota 3.8.(3) ambos están contenidos en $O_q(C_G(a))$. Es decir:

$$\langle C_{Q_1}(a), C_{Q_2}(a) \rangle \subseteq O_q(C_G(a)) \subseteq Q_3 \qquad \text{(con } Q_3 \in \mathcal{J}^*(P,q)\text{)}.$$

Por el Lema 3.5., $Q_1 \cap Q_3 = 1$ o $Q_2 \cap Q_3 = 1$ (ver también el Lema 3.9.). Luego, como se había afirmado:

(*) $\quad C_{Q_i}(a) = 1 \quad$ o $\quad C_{Q_i}(a) = 1.$

Como P es un p-grupo, $Z(P) \neq 1$ y, claramente, $|A| \geq p$. Entonces, por el Lema 2.3.,

$$Q_i = \langle C_{Q_i}(U) \| A:U| = p \rangle, \text{ para } i = 1,2.$$

Luego existen U_1 y U_2 tales que $C_{Q_1}(U_1) \neq 1$ y $C_{Q_2}(U_2) \neq 1$. Pero $U_1 \cap U_2 = 1$, pues si no, tomando $a \in (U_1 \cap U_2)^*$ resulta $1 \neq C_{Q_1}(U_1) \subseteq C_{Q_1}(a)$ y $1 \neq C_{Q_2}(U_2) \subseteq C_{Q_1}(a)$, que contradice (*).

Supongamos que $|A| > p$:

$$|A| = |U_1U_2| = \frac{|U_1||U_2|}{|U_1 \cap U_2|} = |U_1||U_2| \quad \text{y} \quad p = \frac{|A|}{|U_1|} = |U_2|.$$

De manera semejante, $|A| > p$ implica $|U_1| = p$, y en consecuencia $|A| = p^2$.

De modo que $|A| = p$ o $|A| = p^2$.

Observemos que X está contenido en un p-subgrupo elementalmente abeliano maximal $\hat{A}$ de G. Claramente $\hat{A} \subseteq C_G(X)$ y conjugando por un elemento de $C_G(X)$, podemos escoger $\hat{A}$ de forma que $\hat{A} \subseteq P$. Entonces $\hat{A}$ debe contener todos los elementos centrales de orden p de un cierto p-Sylow T de G (a saber, cualquiera que contenga a $\hat{A}$). Como $\hat{A} \subseteq P$, P también debe contener a todos los elementos centrales de orden p de T; más aún, si tomamos a T de tal forma que $\hat{A} \subseteq P \subseteq T$, entonces $A = \Omega_1(Z(P))$ también contiene a todos estos elementos centrales de orden p de T, i.e. $\Omega_1(Z(T)) \subseteq \Omega_1(Z(P))$.

Notemos que $X \subseteq A$.

Ahora bien, si $|A| = p$ entonces $A = X$ y, por la observación anterior, algún $y \in X^*$ es central, luego X mismo lo es (pues $X = \langle y \rangle$). Entonces $C_G(X)$ contendría a un p-Sylow de G, contradiciendo al Lema 3.2., pues $O_q(C_G(X)) \neq 1$ sería necesariamente normalizado por este p-Sylow de G.

Luego $|A| = p^2$. #

Lema 3.11. [Ben 3.11] $Q = O_q(H)$.

Demostración. Recuerde que los supuestos y la notación de la Nota 3.8. siguen vigentes.

Sean $A := \Omega_1(Z(P))$, $g \in G$ como en el Lema 3.9., $Q_1 := O_q(H)$ y $Q_2 := O_q(H^g)$.

Observamos ahora que, por el lema anterior, $|A^*| = p^2 - 1$. Así, si E es un subgrupo de A de orden p, entonces $|E^*| = p-1$, y como la intersección de dos subgrupos distintos de orden p es siempre trivial, resulta que A tiene exactamente $\frac{p^2-1}{p-1} = p+1$ subgrupos de orden p.

Sea T un p-Sylow de G que contenga a P, entonces $P \subsetneq T$ (por el Lema 3.2., ya que $O_q(C_G(X)) \neq 1$) y en consecuencia $P \subsetneq N_T(P)$ por el Lema 0.11. Luego $N_T(P) \not\subseteq C_G(x)$, pues P es un p-Sylow de $C_G(x)$. Si $k \in N_T(P) - C_G(x)$, entonces k normaliza a A (dado que A *char* $P \lhd N_T(P)$) pero no a X (como $|k| = p^a$, la ecuación de clase obligaría a que k centralizara a X). Así, si nos fijamos en la ecuación de clase con k actuando en los subgrupos de orden p de A, tenemos exactamente p conjugados de X en A por potencias de k, digamos: $X = X_1, X_2, \ldots, X_p$. El restante subgrupo Z de orden p de A es, por el Lema 3.10., necesariamente, un p-subgrupo central de A: $Z = \Omega_1(Z(T)) \subseteq \Omega_1(Z(P)) =: A$.

Sea $z \in Z^*$. Tenemos $A = \langle x, z \rangle$, con $z \in Z(T)$. Como $z \in A = \Omega_1(Z(P))$, resulta que $P \subseteq C_G(z)$ y entonces $C_{Q_i}(z)$ para $i = 1,2$, son q-subgrupos P-invariantes de $C_G(z)$. Por el supuesto (3) de la Nota 3.8., tenemos que $C_{Q_i}(z) \subseteq O_q(C_G(z)) = 1$, pues $C_G(z)$ contiene a T, un p-Sylow de G (ver Lema 3.2.).

Afirmamos que $N_T(P) - H \neq \phi$.

En efecto: supongamos que $N_T(P) \subseteq H$. Como A actúa en Q_2, por el Lema 2.3., tenemos que existe un subgrupo E de A de orden p, tal que $C_{Q_2}(E) \neq 1$. Pero $E \neq Z$, pues, del párrafo anterior, sabemos que $C_{Q_2}(Z) = 1$. Luego $E = X_t = X^t$, con $t \in N_T(P)$ (t es alguna potencia de k). Entonces:

$$1 \neq C_{Q_2}(X^t) \subseteq Q_2 \cap C_G(x^t) \subseteq Q_2 \cap C_G(x)^t \subseteq Q_2 \cap H^t = Q_2 \cap H \ .$$

Con esta contradicción al Lema 3.9., hemos demostrado que $N_T(P) - H \neq \phi$.

Sabemos que $Q \subseteq Q_1$, por los supuestos de la Nota 3.8., pues $Q \subseteq H$ es q-subgrupo P-invariante.

Supongamos que $Q \subsetneq Q_1$.

Como $Q_1 \lhd H \supseteq C_G(X)$, tenemos que $C_{Q_1}(X) = Q_1 \cap C_G(X) \lhd C_G(X)$ y así $C_{Q_1}(X) \subseteq Q$. Claramente $Q \subseteq C_{Q_1}(X)$. Entonces, como A actúa en Q_1, por el Lema 2.3., existe una j, entre 1 y p, tal que $C_{Q_1}(X_j) \subsetneq Q = C_{Q_1}(X)$ (de nuevo, sabemos que $C_{Q_1}(Z) = 1$). Luego $X_j = X^f$ para alguna $f \in N_T(P) - H$.

Tomamos ahora $g = f$, y como en la demostración del Lema 3.9.(ii) tenemos: $1 \neq C_{Q_1}(X^g) \subseteq C_G(X^g) \subseteq C_G(X)^g \subseteq H^g \neq H$ y $P = P^g \subseteq H^g$. Pero ya que X^g y Q_1 son P-invariantes (pues $P = P^g \in Syl_p(C_G(X^g))$), también lo es $C_{Q_1}(X^g)$. Por el supuesto de la

Nota 3.8., resulta que $1 \neq C_{Q_1}(X^g) \subseteq O_q(H^g)$ y en particular $O_q(H^g) \cap H \neq 1$, en contradicción con el Lema 3.9.(iii).

Luego, nuestro supuesto $Q \subsetneq Q_1$ debe ser falso, y en consecuencia $Q = Q_1$. #

Lema 3.12. [Ben 3.12] $C_H(Q)$ no tiene subgrupos de tipo (p,p).

Demostración. Nuevamente, manejamos los acuerdos de la Nota 3.8.

Por el Lema 3.11., $Q = O_q(H)$.

Supongamos que el lema es falso.

Afirmamos que podemos escoger una $E \subseteq C_H(Q)$, $E \cong Z_p \times Z_p$ con $X \subseteq E$:

Sea $\overline{P} \in Syl_p(C_H(Q))$, con $X \subseteq \overline{P}$.

Caso 1. $x \notin \Omega_1(Z(\overline{P}))$.

Como $X \subseteq \overline{P}$, tenemos que $[X, \Omega_1(Z(\overline{P}))] = 1$ y nos basta tomar una $y \in \Omega_1(Z(\overline{P}))$, $|y| = p$. El grupo $E = \langle x, y \rangle$ es, claramente, elementalmente abeliano.

Caso 2. $x \in \Omega_1(Z(\overline{P}))$.

Sea E' un p-subgrupo elementalmente abeliano de rango máximo de $C_H(Q)$. Por hipótesis $r(E') \geq 2$. Sin pérdida de generalidad (conjugando a E' por elementos de $C_H(Q)$ si fuera necesario), podemos escoger a E' de forma que $E' \subseteq \overline{P}$. Luego, $\Omega_1(Z(\overline{P})) \subseteq E'$ (pues de otro modo $\Omega_1(Z(\overline{P})) \cdot E'$ sería de rango mayor). Pero entonces $x \in \Omega_1(Z(\overline{P})) \subseteq E'$. Así, podemos extraer de E' un subgrupo E con $E \subseteq C_H(Q)$, $E \cong Z_p \times Z_p$ y $X \subseteq E$.

En cualquier caso tenemos: $X \subseteq E \subseteq C_G(X) \cap C_H(Q)$, $E \cong Z_p \times Z_p$.

Como $C_G(X)$ normaliza a $C_H(Q)$ y $P \in Syl_p(C_G(X))$, podemos ahora suponer además que $E \subseteq P$, conjugando a E con algún elemento de $C_G(X)$ de ser necesario. Si ahora tomamos $g \in G$ como en el Lema 3.9.(ii) y $Q_2 := O_q(H^g)$, resulta que E actúa en Q_2 y, por el Lema 2.3., $C_{Q_2}(e) \neq 1$ para alguna $e \in E^*$. Entonces, por el Lema 3.9.(iii), $C_G(e) \not\subseteq H$.

Como $e \in E \subseteq C_H(Q)$, tenemos $C_G(e) \supseteq Q$. Así, $Q \subseteq Q \cap C_G(e) \subseteq O_q(C_G(e))$, por Lema 3.6., pues $X \subseteq C_G(e)$. De manera semejante, dado que $\langle e \rangle \subseteq H \subsetneq G$, podemos aplicar de nuevo Lema 3.6. y obtenemos que $O_q(C_G(e)) \cap H \subseteq O_q(H) = Q$ (Lema 3.11.).

Entonces $N_G(Q) \subseteq H$ (Lema 3.9.(i)) implica que $Q \subseteq N_{O_q(C_G(e))}(Q) = O_q(C_G(e)) \cap N_G(Q) \subseteq O_q(C_G(e)) \cap H \subseteq Q$ y en consecuencia $N_{O_q(C_G(e))}(Q) = Q$. Por lo tanto $O_q(C_G(e))$ no puede contener propiamente a Q (pues en un q-grupo el único subgrupo que es igual a su propio normalizador es el total). Luego $O_q(C_G(e)) = Q$ y así $C_G(e)$ normaliza a Q, es decir $C_G(e) \subseteq N_G(Q) = H$. Contradicción. #

Nota: El siguiente lema vale en general, al margen de los supuestos de la sección. De hecho también vale si sustituimos "p" por "π_1" y "q" por "π_2", con π_1 y π_2 un par de conjuntos de números primos tal que $\pi_1 \cap \pi_2 = \phi$, y la demostración es esencialmente la misma, pero no haremos uso de ello.

Lema 3.13. [Piz 3.13] Sean M un grupo, p y q primos distintos, Y un p-subgrupo de M. Entonces $O_q(C_M(Y)) = O_q(N_M(Y))$.

Demostración. De $O_q(C_M(Y))\ char\ C_M(Y) \lhd N_M(Y)$, tenemos que $O_q(C_M(Y)) \lhd N_M(Y)$, y en consecuencia: $O_q(C_M(Y)) \subseteq O_q(N_M(Y))$.

Por otro lado, Y y $O_q(N_M(Y))$ son ambos normales en $N_M(Y)$; entonces $[O_q(N_M(Y)), Y] \subseteq O_q(N_M(Y)) \cap Y = 1$ (Y es un p-grupo). Luego $O_q(N_M(Y)) \subseteq C_M(Y)$. Pero $O_q(N_M(Y)) \lhd N_M(Y) \supseteq C_M(Y)$ implica que $O_q(N_M(Y)) \lhd C_M(Y)$ y así, tenemos $O_q(N_M(Y)) \subseteq O_q(C_M(Y))$. #

Lema 3.14. [Ben, Sección 3] No existe un p-subgrupo X de G tal que $O_q(C_G(X)) \neq 1$.

Demostración. Recuerde que se ha supuesto desde el Lema 3.9. hasta el actual, que tal p-subgrupo X existe y que incluso (S.P.G.) satisface los supuestos adicionales de la Nota 3.8.

Observamos que si $x \notin O_p(C_H(Q))$, entonces X centralizaría a algún p-elemento no trivial y de $O_p(C_H(Q))$, y en consecuencia $C_H(Q)$ contendría al subgrupo $\langle x, y \rangle$ de tipo (p,p), contrario al Lema 3.12..

Luego $X \subseteq O_p(C_H(Q)) \subseteq O_p(H)$ por el Lema 2.4.(iii). Pero entonces $X = \Omega_1(Z(O_p(C_H(Q))))$ (otra vez por el Lema 3.12.).

Si $y \in C_H(Q)$ con $|y| = p$ y $y \notin X$, entonces y actúa en $X\ char\ C_H(Q)$, y actúa trivialmente pues $p \nmid |Aut(X)| = p-1$. Esto contradice al Lema 3.12. Entonces X es el único subgrupo de orden p de $C_H(Q)$. Pero $C_G(Q) \subseteq N_G(Q) = H$. Luego $C_G(Q) = C_H(Q)$ y X es también el único subgrupo de orden p de $C_G(Q)$.

Como $X\ char\ C_G(Q) \lhd N_G(Q)$, tenemos que $1 \neq X \subseteq O_p(N_G(Q))$, y, por tanto, $O_p(N_G(Q)) \neq 1$. Por el Lema 3.13., $O_p(C_G(Q)) \neq 1$.

Así, podemos intercambiar p y q si es necesario, y suponer que $p < q$.

Como $Q = O_q(H)\ char\ H$, tenemos que $C_H(Q)\ char\ H$ y $X = \Omega_1(Z(O_p(C_H(Q))))$ $char\ H$. Si $S \in Syl_q(H)$, S actúa en X, trivialmente, pues $q \nmid |Aut(X)| = p-1$, ya que escogimos $q > p$. Luego $X \subseteq C_G(S)$ y X es el único subgrupo de orden p en $C_G(S) \subseteq C_G(Q) = C_H(Q)$.

Entonces $X\ char\ C_G(S)$, y además, otra vez por el Lema 3.12., $X = \Omega_1(Z(O_p(C_G(S)))) = \Omega_1(Z(O_p(N_G(S))))$ (recuerde del Lema 3.13. que

$O_p(C_G(S)) = O_p(N_G(S)))$. Así, X *char* $N_G(S)$ y entonces $N_G(S) \subseteq N_G(X) \supseteq H$. Luego $N_G(X) = H$ por la maximalidad de H. Además, $N_G(S) \subseteq H$, pero entonces $S \in Syl_q(G)$ necesariamente (como siempre, si $K \in Syl_q(G)$ con $S \subsetneq K$, entonces $S \subsetneq N_K(S) \subseteq N_G(S)$, pero $N_K(S) \cap H = S$). Así, S normaliza a $X \neq 1$, contrario al Lema 3.2. #

Lema A. [Ben, Lemma 1] Si $R \in \mathcal{L}_r$, entonces el subgrupo de Fitting $F(R)$ es un r-grupo. En particular, $Z(F(R))$ contiene al centro de algún r-subgrupo de Sylow de G.

Demostración. Supongamos, para fijar notación, que $r = p$.

Por el Teorema 0.28., $F(R) = O_p(R) \times O_q(R)$. Si $R \in \mathcal{L}_p$ entonces $R = C_G(X)$ o $R = N_G(X)$, para algún p-subgrupo X de G. Entonces, por el lema anterior (y por el Lema 3.13.) $O_q(R) = O_q(N_G(X)) = O_q(C_G(X)) = 1$ y por lo tanto $F(R) = O_p(R)$ es un p-grupo.

Solo resta probar que $Z(F(R))$ contiene al centro de un r-Sylow de G.

Sea $R \in \mathcal{L}_r$; entonces $R = N_G(X)$ o $R = C_G(X)$ para algún r-subgrupo X de G no trivial. Como $X \trianglelefteq R$, $X \subseteq O_r(R)$. Sea P un r-Sylow de G, tal que $X \subseteq O_r(R) = F(R) \subseteq P$. Entonces $Z(P) \subseteq C_G(X) \subseteq R$ (en cualquiera de los dos casos). Luego: $[Z(P), F(R)] \subseteq [Z(P), P] = 1$, y así $Z(P) \subseteq C_R(F(R)) \subseteq F(R)$.

Por lo tanto $Z(P) \subseteq Z(F(R))$. #

4. Subgrupos q-locales maximales para $q < p$

Como se dijo al inicio del capítulo anterior, el objetivo de los capítulos 3 al 6 es probar el teorema de Burnside. Para ello hemos supuesto que el teorema de Burnside es falso. En el capítulo 6 esta suposición nos llevará a una contradicción. De modo que:

Advertencia: Todos los resultados de este capítulo suponen la existencia de un contraejemplo minimal al teorema de Burnside y no deben ser usados fuera de este contexto.

Suponemos, como en el capítulo anterior, que G es tal contraejemplo. Las observaciones y la notación del inicio del capítulo 3 siguen siendo válidas. Podremos usar tanto los lemas 3.1 al 3.7 como el Lema A, que no hacen supuestos adicionales sobre G.

Nota 4.1. En este capítulo supondremos que:

$d = max\{r_p(H) \mid H \in \mathcal{L}_q\} \geq 2$, $q < p$, $H \in \mathcal{L}_q$, $r_p(H) = d$, $A \subseteq H$ es un p-subgrupo elementalmente abeliano de orden p^d y definimos: $Q := O_q(H)$. Recuerde, que gracias al Lema A, $O_q(H) = F(H)$.

Repetidamente, a lo largo del texto, consideraremos la situación descrita en (*):

$$(*) \qquad \begin{cases} 1 \neq B \subseteq A \\ M = C_G(B) \\ V = \text{un } q\text{-subgrupo de } C_Q(B) \text{ elementalmente abeliano no trivial} \end{cases}$$

Al final de este capítulo recogeremos en el Lema B las implicaciones más importantes de estas premisas.

Lema 4.2. [Ben 4.1] Si $A \subseteq \overline{H} \in \mathcal{L}_q$, entonces todos los q-subgrupos A-invariantes de $\overline{H}$ están en $O_q(\overline{H})$.

Demostración. Como A es un p-subgrupo elementalmente abeliano maximal de $\overline{H}$, y como $q < p$ implica que $p \neq 2$, podemos aplicar el Lema 2.8. (ver también la nota que le sigue). #

Lema 4.3. [Ben 4.2] Si $A \subseteq \overline{H} \in \mathcal{L}_q$ y $\overline{H} \cap Q \neq 1$, entonces $\overline{H} \subseteq H$.

Demostración. Suponga las hipótesis del enunciado y que $H \neq \overline{H} \in \mathcal{L}_q^*$. Entonces $Q \cap \overline{H}$ es un q-subgrupo A-invariante de $\overline{H}$; por lo tanto, $Q \cap \overline{H} \subseteq O_q(\overline{H})$ (ver el Lema 4.2.). Como A satisface los supuestos del Lema 3.5. (gracias al Lema 4.2.), tenemos: $Q = O_q(H) \in \mathcal{J}^*(A,q)$ y $O_q(\overline{H}) \in \mathcal{J}^*(A,q)$. Además, $Q \cap O_q(\overline{H}) = 1$ (recuerde que H maximal y $O_q(H) \neq 1$ implican $H = N_G(O_q(H))$, en particular $O_q(H) \neq O_q(\overline{H})$), pero entonces $Q \cap \overline{H} \subseteq Q \cap O_q(\overline{H}) = 1$, contrario a lo supuesto. #

Lema 4.4. [Ben 4.3] Suponga (*). Entonces $O_p(M) = F(M) \not\subseteq H$. Si $|A:B| = p$, entonces V tiene un subgrupo U de indice q tal que $r_p(C_G(U)) \geq d$.

Demostración. Sea $P = O_p(M)$. Como $M \in \mathcal{L}_p$, tenemos, gracias al Lema A, que $P = F(M)$.

Si $[V,P] = 1$, tenemos que $V \subseteq C_M(P) \subseteq P$ (de nuevo por el Teorema 0.29.) y entonces (como V es un q-grupo) $V = 1$, contrario a (*). Concluimos que $[V,P] \neq 1$.

Si ahora $P \subseteq H$, entonces P actúa en $Q\,char\,H$ y (trivialmente) en $B \subseteq Z(M)$ ($M := C_G(B) \supseteq P$); luego P actúa en $C_Q(B)$, y viceversa, pues $P\,char\,M = C_G(B) \supseteq C_Q(B)$. Entonces $1 \neq [V,P] \subseteq [C_Q(B),P] \subseteq C_Q(B) \cap P = 1$.

Concluimos que $P \not\subseteq H$.

De $[V,P] \neq 1$, tenemos $C_P(V) \neq P$ y así (como V actúa en P, y por el Lema 2.3.) existe una U, con $|V:U| = q$, tal que $C_P(U) \not\subseteq C_P(V)$. Como V actúa en P y en U, tenemos que actúa también en $C_P(U)$, y además $[V,C_P(U)] \neq 1$, pues de otro modo $C_P(U) \subseteq C_P(V)$. Por el Teorema 2.5., $[V,\Omega_1(C_P(U))] \neq 1$, y así, existe un elemento $a \in C_P(U)$, de orden p, que no es centralizado por V. En particular, $a \notin B$ (recuerde que $V \subseteq C_Q(B)$). Como $a \in P \subseteq M = C_G(B)$, $B\langle a \rangle$ es elementalmente abeliano, de rango $r(B)+1 = r(A) = d$ (por hipótesis $|A:B| = p$). Luego $B\langle a \rangle \subseteq C_G(U)$ y $r_p(C_G(U)) \geq d$. #

Lema 4.5. [Ben 4.4] $C_H(A)$ no tiene subgrupos de tipo (q, q).

Demostración. Supongamos que existe una $V \subseteq C_H(A)$, con $V \cong Z_q \times Z_q$. Por el Lema 4.2., $V \subseteq O_q(H) = Q$. Entonces, si $x \in V^*$, tenemos $A \subseteq C_G(x) \in \mathcal{L}_q$, y $1 \neq x \in C_G(x) \cap Q$, y por el Lema 4.3., tenemos: $C_G(x) \subseteq H$.

Sea $P = O_p(C_G(A))$. Como $V \subseteq C_H(A) \subseteq C_G(A)$, V actúa en P, $|V| = q^2$ y, por el Lema 2.3., $P = \langle C_P(x) | x \in V^* \rangle$. Pero entonces, $P = \langle C_P(x) | x \in V^* \rangle \subseteq \langle C_G(x) | x \in V^* \rangle \subseteq H$.

Si en el Lema 4.4. tomamos $B=A$, tenemos: $P = O_p(M) = F(M)$, $M = C_G(B)$, $B \neq 1$ (pues $A \neq 1$) y $1 \neq V \subseteq C_Q(B)$, es decir, los supuestos del Lema 4.4.; usando éste, concluimos $P \not\subseteq H$. Esto es una contradicción con la última expresión del párrafo anterior. #

Lema 4.6. [Ben 4.6] Suponga (*), con $|A:B| = p$. Entonces $|V| \leq q^2$.

Demostración. Si ese no es el caso, por el Lema 4.4., existe una U con $|V:U| = q$ (y en particular $r(U) \geq 2$) tal que $r_p(C_G(U)) \geq d$. Si $\overline{A} \subseteq C_G(U)$, con $r(\overline{A}) = d$, y $\overline{H}$ es tal que $C_G(U) \subseteq \overline{H} \in \mathcal{L}_q^*$, tenemos $U \subseteq C_{\overline{H}}(\overline{A})$. Pero entonces $C_{\overline{H}}(\overline{A})$ contiene un $U_0 \subseteq U$, de tipo (q, q), contrario al Lema 4.5. #

Lema 4.7. [Ben 4.5] Si $C_H(A)$ contiene un subgrupo Q_0 de orden q, Q_0 es único. Existen subgrupos $\overline{H}$ y $\overline{A}$ que satisfacen las mismas propiedades que H y A respectivamente, y además $C_{\overline{H}}(\overline{A})$ contiene un subgrupo Q_0 de orden q.

Demostración. Si tal Q_0 existe, como Q_0 es A-invariante, el Lema 4.2. nos dice que $Q_0 \subseteq Q = O_q(H)$. Entonces su unicidad se sigue del Lema 4.5. y del Lema 0.41.

Supongamos que $C_H(A)$ es un p-grupo.

Sea $V \subseteq Q$ un q-subgrupo A-invariante no trivial minimal (como Q mismo es A-invariante, tal V existe). Entonces V es elementalmente abeliano, pues $\Omega_1(Z(V)) \neq 1$ es característico en V, y por lo tanto A-invariante. Por la minimalidad de V, tenemos que $V = \Omega_1(Z(V))$.

Ahora $q < p$ implica que $|V| \geq q^2$, pues si no, $p \mid q - 1 = |Aut(Z_q)|$ implica que $[A, V] = 1$ y entonces $V \subseteq C_H(A)$ y $C_H(A)$ no sería un p-grupo.

Así, por el Lema 2.3., $V = \langle C_V(B) \,\|\, A:B| = p \rangle$. Pero como cada $C_V(B)$ es A-invariante, tenemos que, por la minimalidad de V, $V = C_V(B)$, para alguna $B \subseteq A$, con $|A:B| = p$. Además $B \neq 1$, pues $r(A) = d \geq 2$ implica que $r(B) = d - 1 \geq 1$. También $1 \neq V = C_V(B) \subseteq C_Q(B) \subseteq C_G(B) = M$. Ahora podemos aplicar el Lema 4.4., para concluir que V tiene un subgrupo U, de índice q, (en particular $U \neq 1$), tal que $C_G(U)$ contiene un p-subgrupo elementalmente abeliano $\overline{A}$ de rango $r(\overline{A}) = d$ (máximo).

Si ahora $\overline{H}$ es tal que $C_G(U) \subseteq \overline{H} \in \mathcal{L}_q^*$, podemos reemplazar A por $\overline{A}$ y H por $\overline{H}$ ($1 \neq U \subseteq C_G(\overline{A}) \cap \overline{H} = C_{\overline{H}}(\overline{A})$, U es un q-grupo). #

Nota 4.8. De aquí en adelante, supondremos que $C_H(A)$ contiene un (único) subgrupo Q_0 de orden q. Entonces Q_0 es A-invariante y, por el Lema 4.2., $Q_0 \subseteq Q$.

Lema 4.9. [Ben 4.7] Q_0 es el único subgrupo no trivial elementalmente abeliano A-invariante de Q. En particular $Q_0 = \Omega_1(Z(Q))$.

Demostración. Suponga que existe un contraejemplo V. Afirmamos que existe otro contraejemplo $\overline{V}$ que satisface $Q_0 \subsetneq \overline{V}$:

Caso I. $Q_0 \subseteq Z(Q)$.

Tomamos $\overline{V} = \langle Q_0, V \rangle \neq Q_0$. Entonces $\overline{V}$ es elementalmente abeliano, A-invariante y $Q_0 \subsetneq \overline{V}$.

Caso II. $Q_0 \not\subseteq Z(Q)$.

Tómese $\overline{V} = \langle Q_0, \Omega_1(Z(Q)) \rangle \neq Q_0$ (note que $Q_0 \cap \Omega_1(Z(Q)) = 1$). Entonces $Q_0 \subsetneq \overline{V}$, y como $\Omega_1(Z(Q))$ *char* Q es A-invariante, $\overline{V}$ también lo es. Claramente $\overline{V}$ es elementalmente abeliano.

Así, como se afirmó, existe otro contraejemplo $\overline{V}$ con $Q_0 \subsetneq \overline{V}$.

Sea V un contraejemplo minimal al Lema, que respete la condición $Q_0 \subseteq V$.

Entonces, como $C_V(A) \subseteq C_H(A)$, Q_0 es el único subgrupo de $C_H(A)$ de orden q y $C_V(A)$ es elementalmente abeliano, tenemos $C_V(A) = Q_0$.

(1) Afirmamos que $|V| \geq q^3$:

Si $|V| \leq q^2$, entonces $|V| = q^2$. Como A actúa en $V/C_V(A) = V/Q_0$ y $|V/Q_0| = q$, A tendría que actuar trivialmente en $V/Q_0 \cong Z_q$, pues $|Aut(Z_q)| = q-1 < q < p$. Entonces A estabilizaría la serie $V \rhd Q_0 \rhd 1$. Por el Teorema 0.19., A actúa trivialmente en V, contrario a $C_V(A) = Q_0$.

Tenemos $V = \langle C_V(B) \mid |A:B| = p \rangle$ (por el Lema 2.3.), pero entonces $V = C_V(B)$, para alguna B, con $|A:B| = p$, por la minimalidad de V (pues $C_V(B)$ es A-invariante y $Q_0 = C_V(A) \subseteq C_V(B)$).

De nuevo $B \neq 1$, ya que $r(A) = d \geq 2$ y $|A:B| = p$. Así $1 \neq V \subseteq C_Q(B)$ y, del Lema 4.6., concluimos que $|V| \leq q^2$. Esto contradice (1). #

Lema 4.10. [Ben 4.8] Tenemos $H = N_G(Q_0) = C_G(Q_0)$. Cualquier subgrupo $Q_1 \subseteq G$ de orden q que satisfaga $r_p(C_G(Q_1)) \geq d$ es conjugado a Q_0 y es central.

Demostración. Del lema anterior, tenemos $Q_0 = \Omega_1(Z(Q))$ *char* $Q \lhd H$. Luego $H \subseteq N_G(Q_0)$, y por la maximalidad de H, tenemos: $H = N_G(Q_0)$. Además, por el Lema A, existe un $G_q \in Syl_q(G)$, con $Z(G_q) \subseteq Z(F(H)) = Z(Q)$. Entonces $1 \neq \Omega_1(Z(G_q)) \subseteq \Omega_1(Z(Q)) = Q_0$. Luego: $Q_0 = \Omega_1(Z(G_q))$, pues $|Q_0| = q$.

Claramente Q_0 es central.

Sea ahora $Q_1 \subseteq G$, con $|Q_1| = q$ y $r_p(C_G(Q_1)) \geq d$. Sean $\overline{A} \subseteq C_G(Q_1)$ un subgrupo elementalmente abeliano, con $r(\overline{A}) = d$ y $\overline{H}$ tal que $C_G(Q_1) \subseteq \overline{H} \in \mathcal{F}_q$. Tomemos $\overline{Q} := O_q(\overline{H}) = F(\overline{H})$. Entonces Q_1 es un subgrupo de orden q de $C_G(Q_1) = C_{\overline{H}}(Q_1)$ y por el Lema 4.7., Q_1 es único. De nuevo, como Q_1 es $\overline{A}$-invariante, tenemos $Q_1 \subseteq \overline{Q}$ (ver el Lema

4.2.). Así, $Q_1 = \Omega_1(Z(\overline{Q}))$ (por el Lema 4.9.). Entonces, igual que antes, $Q_1 = \Omega_1(Z(G_q'))$, para alguna $G_q' \in Syl_q(G)$. Luego $G_q' = G_q^g$, para alguna $g \in G$. En consecuencia:

$$Q_0^g = \Omega_1(Z(G_q^g)) = \Omega_1(Z(G_q')) = Q_1.$$

Ahora bien: sabemos que H normaliza a Q_0. Como $|Aut(Q_0)| = |Aut(Z_q)| = q-1$ y $q-1 < q < p$, resulta que ningún elemento de H puede inducir un automorfismo de Q_0 no trivial, luego $H = N_G(Q_0) = C_G(Q_0)$. #

Lema 4.11. [Ben 4.9] $q = 2$.

Demostración. A actúa en Q. Luego, por el Lema 2.3., tenemos $Q = \langle C_Q(B) \mid |A:B| = p \rangle$.

Recuerde que $C_Q(A) \neq Q$: si $C_Q(A) = Q$, tendríamos $[Q, A] = 1$, y por el Teorema 0.29., resulta $A \subseteq C_H(Q) \subseteq Q = F(H)$, lo cual implica que $A = 1$.

Como $C_Q(A) \neq Q$, existe una $B \subseteq A$, con $|A:B| = p$, tal que $C_Q(B)$ no es centralizado por A, es decir: $C_Q(B) \not\subseteq C_Q(A)$ (en particular $C_Q(B) \neq 1$). Por el Lema 4.6., $r(C_Q(B)) \leq 2$.

Tenemos entonces que un p-grupo A actúa no trivialmente en un q-grupo $C_Q(B)$, de rango a lo más 2. Como también sabemos que $q < p$, podemos aplicar el Lema 2.9., para concluir que $q = 2$. #

Lema 4.12. [Ben 4.10] Suponga (•), con $|A:B| \leq p^2$ y $C_Q(B) \not\subseteq C_Q(A)$. Entonces (i) o (ii) (pero no ambas) es verdadera:

(i) $C_Q(B)$ es un grupo cuaternio de orden 8.

(ii) $C_Q(B)$ tiene más de una involución, $|A:B| = p^2$ y $A \not\subseteq \Omega_1(Z(O_p(C_G(B))))$.

En el caso (ii), si z es la involución de Q_0 y $t \neq z$ es otra involución en $C_Q(B)$, entonces z es conjugada a alguna $s \in \{t, tz\}$ y $z \notin F(C_G(s))$.

Demostración. Sabemos que $Q_0 \subseteq Q$ (Nota 4.8.). Sabemos también que A actúa en $C_Q(B)$ (pues Q *char* $H \supseteq A$, $B \subseteq A$ y A es abeliano). Por otro lado $[A, C_Q(B)] \neq 1$ (de otro modo $C_Q(B) \subseteq C_Q(A)$, contrario a las hipótesis). Ahora, $\Omega_1(Z(C_Q(B)))$ es no trivial y elementalmente abeliano, está contenido en Q y es A-invariante (pues A actúa en $C_Q(B)$ y $\Omega_1(Z(C_Q(B)))$ *char* $C_Q(B)$). Luego, por el Lema 4.9., $Q_0 = \Omega_1(Z(C_Q(B)))$. En particular Q_0 *char* $C_Q(B)$.

Supongamos que $C_Q(B)$ no tiene más que una involución.

Entonces, $C_Q(B)$ no tiene 4-grupos.

Afirmamos que $C_Q(B)$ no es abeliano:

Si $C_Q(B)$ es abeliano tendría que ser cíclico, pues sabemos que $C_Q(B)$ tiene un único subgrupo de orden 2: Q_0. Entonces $|Aut(C_Q(B))| = |Aut(Z_{2^a})| = 2^a - 2^{a-1} = 2^{a-1}$, y A tendría que actuar trivialmente en $C_Q(B)$, contrario a lo que sabemos.

Ahora podemos aplicar el Lema 1.12. y tenemos $|C_Q(B)| = 8$. Luego $C_Q(B) \cong Q_8$, pues el único otro grupo no abeliano de orden 8 es D_4, y éste tiene más (5) involuciones.

Así, si $C_Q(B)$ tiene una sola involución, $C_Q(B) \cong Q_8$, es decir satisface (i).

Supongamos para el resto de la demostración que $C_Q(B)$ tiene más de una involución. Tenemos que probar (ii).

Sea z la involución de Q_0 y sea $t \neq z$ una involución de $C_Q(B)$.

Sea $Y = \Omega_1(Z(O_p(M)))$, con $M = C_G(B)$. Por el Lema A, tenemos $O_p(M) = F(M) \neq 1$ (M es soluble) y, en particular, $Y \neq 1$.

Sea $W := [Y, Q_0]$.

Como $Q_0 \subseteq C_Q(A) \subseteq C_Q(B) \subseteq M$ y Y *char* M, tenemos $W \subseteq Y$.

Afirmamos que $W \subseteq \{w \in Y | w^t = w^{-1}\}$.

Si $w = yzy^{-1}z$, con $y \in Y$, es un generador de W, tenemos $w^t = zyzy^{-1} = (yzy^{-1}z)^{-1} = w^{-1}$. Como $W \subseteq Y \subseteq Z(O_p(M))$ es abeliano, tenemos $w^t = w^{-1}$, también en el caso de que w sea un producto de generadores. Esto prueba la afirmación previa.

En particular $C_W(z) = C_W(Q_0) = 1$.

Notemos que $C_Q(B)$ actúa en $W = [Y, Q_0]$ (pues $C_Q(B)$ actúa en Q_0 *char* $C_Q(B)$ y $C_Q(B)$ actúa en Y *char* $M \supseteq C_Q(B)$), y que A actúa en W (pues A actúa en Q_0 (trivialmente) y en Y *char* $M \supseteq A$).

Afirmamos que $C_Q(B)$ actúa fielmente en W.

Supongamos que $C_Q(B)$ no actúa fielmente en W. Entonces $K := C_{C_Q(B)}(W) \neq 1$.

Como A actúa en W y en $C_Q(B)$, A actúa en K. Como $K \neq 1$, $\Omega_1(Z(K)) \neq 1$. Además, $K \subseteq C_Q(B) \subseteq Q$. Luego, $Q_0 = \Omega_1(Z(K)) \subseteq K \subseteq C_G(W)$ (aplicando el Lema 4.9., pues $\Omega_1(Z(K))$ *char* K es A-invariante). Entonces $[Q_0, W] = 1$ y $W \subseteq C_Y(Q_0)$.

Como Q_0 actúa en Y *char* M, por el Teorema 2.1., tenemos: $Y = C_Y(Q_0)[Y, Q_0] = C_Y(Q_0)W = C_Y(Q_0)$. Entonces $[Q_0, Y] = 1$.

Por el Lema A, $Z(O_p(M)) = Z(F(M))$ contiene elementos centrales, y por lo tanto $Y = \Omega_1(Z(O_p(M)))$ también. Luego Q_0 centraliza a algún p-subgrupo (de Y) central. Pero Q_0 mismo es central (por el Lema 4.10.). Esto contradice el Lema 3.4.

Concluimos entonces que, como se había afirmado, $C_Q(B)$ actúa fielmente en W.

Afirmamos a continuación que $A \not\subseteq C_G(W)$.

Supongamos que $A \subseteq C_G(W)$. Entonces $[A,W]=1$, luego:

$[C_Q(B),W,A] \subseteq [W,A]=1$ (pues $C_Q(B)$ actúa en W), también $[W,A,C_Q(B)]$ $=[1,C_Q(B)]=1$, y entonces, por el Lema de los tres subgrupos, resulta $[A,C_Q(B),W]=1$. Si recordamos que $[A,C_Q(B)] \neq 1$ y que $C_Q(B)$ actúa fielmente en W, tenemos: $1 \neq [A,C_Q(B)] \subseteq C_{C_Q(B)}(W)=1$.

Esta contradicción prueba que, como se había dicho, $A \not\subseteq C_G(W)$. En particular, $A \not\subseteq Y = \Omega_1(Z(O_p(C_G(B))))$, pues $Y \subseteq C_G(W)$.

Claramente $AC_Q(B)$ actúa en W, es decir, tenemos un homomorfismo $\varphi: AC_Q(B) \to Aut(W) = GL(W)$. La imagen de φ es un grupo de orden $p^\alpha q^\beta$ con $\alpha \neq 0 \neq \beta$, pues $A \not\subseteq C_G(W)$ y $C_Q(B)$ actúa fielmente en W.

Afirmamos que $Ker(\varphi) = C_A(W)$.

Claramente $C_A(W) \subseteq Ker(\varphi)$. Como $C_Q(B)$ actúa fielmente en W, tenemos que $C_Q(B) \cong \varphi(C_Q(B))$ y, en consecuencia, $Ker(\varphi) \cap C_Q(B) = 1$.

Si $ac \in Ker(\varphi)$, con $a \in A$ y $c \in C_Q(B)$, tenemos $acwc^{-1}a^{-1} = w$, para toda $w \in W$. Entonces $cwc^{-1} = a^{-1}wa$ para toda $w \in W$; pero c induce un 2-automorfismo de W y a induce un p-automorfismo de W. Se sigue que $cwc^{-1} = a^{-1}wa = w$, para toda $w \in W$. Luego $c \in C_{C_Q(B)}(W)$ y $a \in C_A(W)$, entonces $c=1$ y $ac \in C_A(W)$. En consecuencia $Ker(\varphi) = C_A(W)$, como se había afirmado.

Entonces $\varphi(A)$ y $\varphi(C_Q(B))$ son (respectivamente) p- y q- subgrupos no triviales de $GL(W)$. Veamos que, además, $\varphi(A)$ normaliza a $\varphi(C_Q(B))$:

Tenemos $C_Q(B)C_A(W) \lhd AC_Q(B)$ (A normaliza a $C_Q(B)$ y $C_A(W)$ es normal en $AC_Q(B)$ por ser el núcleo de un homomorfismo). Entonces $\varphi(C_Q(B)C_A(W)) = \varphi(C_Q(B))$, y en consecuencia, $\varphi(C_Q(B)) \lhd \varphi(AC_Q(B))$. En particular, $\varphi(A)$ normaliza a $\varphi(C_Q(B))$.

Observamos que $r(W) > 1$, pues de lo contrario, $W \cong Z_p$ o $W \cong 1$; en cualquier caso A tendría que actuar trivialmente en W, contrario a lo que sabemos.

También, $r(W) \neq 2$, pues de lo contrario, gracias a los resultados del párrafo anterior, podríamos aplicar el Teorema 2.10. para concluir que $r(C_Q(B)) = 1$ (recuerde que $C_Q(B) \cong \varphi(C_Q(B))$). Sin embargo, $\langle z \rangle = Q_0\ char\ C_Q(B)$ implica que t actúa en Q_0, y entonces $[t,Q_0]=1$ ($Aut(Z_2)=1$). Luego $\langle t,z \rangle \leq C_Q(B)$ es elementalmente abeliano, de rango 2, y entonces $r(C_Q(B)) \geq 2$, contrario al resultado previo.

Concluimos que $r(W) \geq 3$.

Ahora $\langle t, z \rangle$ actúa en W y (como ya se dijo) $C_W(z) = C_W(Q_0) = 1$. Luego, por el Lema 2.3., tenemos que $W = C_W(t) + C_W(tz)$. Entonces, una de dos: $r(C_W(t)) \geq 2$ o $r(C_W(tz)) \geq 2$. Sea $s \in \{t, tz\}$ tal que $r(C_W(s)) \geq 2$.

Observamos 3 cosas:

(1) $B, C_W(s) \subseteq C_G(s)$.
(2) $[B, C_W(s)] = 1$ (pues $C_W(s) \subseteq M = C_G(B)$).

Dado que $[Q_0, B] = 1$ y $C_W(Q_0) = 1$, es decir, que todos los elementos de B conmutan con Q_0 y todos los elementos no triviales de W no conmutan con Q_0, tenemos:

(3) $B \cap C_W(s) = 1$.

Entonces, $d \geq r_p(C_G(s)) \geq r(B) + r(C_W(s)) \geq d - 2 + 2 = d$. Luego $r_p(C_G(s)) = d$ y $r(B) = d - 2$; es decir $|A : B| = p^2$.

Por el Lema 4.10., s y z son conjugadas.

Finalmente, sólo resta probar que $z \notin F(C_G(s))$.

Sabemos que $D := B + C_W(s) \subseteq C_G(s) \cap Y$ es elementalmente abeliano, de rango $r(D) = d$ y $|D : B| = p^2$. Además, z no conmuta con D (pues $C_W(z) = 1$).

Supongamos que $z = s^g \in F(C_G(s))$, con $g \in G$. Entonces, $z^g, s, z \in F(C_G(z)) = Q$.

Definimos:

$$\overline{A} := D^g = B^g + C_{W^g}(s^g) \subseteq C_G(z) \cap Y^g$$
$$\overline{B} := B^g$$
$$\overline{M} := C_G(\overline{B}) = M^g$$
$$\overline{Y} := \Omega_1(Z(O_p(\overline{M}))) = Y^g$$

Observamos que $\overline{A} \subseteq \overline{Y} \subseteq \Omega_1(Z(O_p(C_G(\overline{B}))))$. Si podemos aplicar la parte del lema que ya tenemos probada, sobre $\overline{A}$, $\overline{B}$, $\overline{M}$ y $\overline{Y}$ en lugar de A, B, M y Y, podríamos concluir que $\overline{A} \not\subseteq \Omega_1(Z(O_p(C_G(\overline{B}))))$, lo cual nos conduce a la contradicción que necesitamos. Esto es justo lo que nos proponemos hacer. Más concretamente, vamos a probar que $\overline{A}$, $\overline{B}$, $\overline{M}$ y $\overline{Y}$ satisfacen los supuestos del lema, es decir:

(A) $r(\overline{A}) = d$:
$r(\overline{A}) = r(D) = d$.

(B) $\overline{A} \subseteq H$:
$D \subseteq C_G(S)$ implica que $\overline{A} = D^g \subseteq C_G(s^g) = C_G(z) = H$.

(C) $1 \neq \overline{B} \subseteq \overline{A}$:

$\overline{B} = B^s$, B es no trivial y $B \subseteq D$ implica que $\overline{B} \subseteq \overline{A}$.

(D) $\overline{M} := C_G(\overline{B})$:
Por definición.

(E) $1 \neq C_Q(\overline{B})$:
Como s conmuta con B, $z = s^x$ conmuta con $\overline{B} = B^x$. Luego $1 \neq z \in C_Q(\overline{B})$.

(F) $C_H(\overline{A})$ tiene un subgrupo de orden q:
Como s conmuta con D, z conmuta con $\overline{A}$. Entonces $z \in C_H(\overline{A})$.

(G) $|\overline{A}:\overline{B}| \leq p^2$:
$|\overline{A}:\overline{B}| = |D:B| = p^2$.

(H) $C_Q(\overline{B}) \not\subseteq C_Q(\overline{A})$:
Como z no conmuta con D, z^x no conmuta con $\overline{A}$. Como z conmuta con B, z^x conmuta con $\overline{B}$. Recordamos que $z^x \in Q = F(C_G(z))$ (pues hemos supuesto $z \in F(C_G(s))$). Luego $z^x \in C_Q(\overline{B}) - C_Q(\overline{A})$. En particular $C_Q(\overline{B}) \not\subseteq C_Q(\overline{A})$.

(I) $C_Q(\overline{B})$ no es un grupo cuaternio:
Un grupo cuaternio tiene sólo una involución. Entonces $z, z^x \in C_Q(\overline{B})$ y $z = s^x \neq z^x$ implican que $C_Q(\overline{B}) \not\cong Q_8$.

Observamos que las condiciones (A) y (B) son condiciones generales de este capítulo; (C)-(E) corresponden a los supuestos (•); (F) es el supuesto de la Nota 4.8.; (G) y (H) son premisas explícitas de este lema. Finalmente se verifica (I) para asegurarnos de poder aplicar el resultado (ii) del lema. #

Lema 4.13. [Ben 4.11]

(i) $p = 3$.

(ii) $C_Q(A) = Q_0$.

(iii) Si $B \subseteq A$, con $|A:B| = p$ y $C_Q(B) \neq Q_0$, entonces $|C_Q(B)| = 8$.

Demostración. Si $C_Q(A) = Q$, entonces $A \subseteq C_H(Q) \subseteq Q$ (pues $Q = F(H)$), lo que implica que $A = 1$. Concluimos que $C_Q(A) \neq Q$. Por el Lema 2.3., A tiene un subgrupo B de índice p, tal que $C_Q(B) \not\subseteq C_Q(A)$. Por el Lema 4.12., $C_Q(B) \cong Q_8$, para esta B. Luego $1 \neq Q_0 \subseteq C_Q(A) \subsetneq C_Q(B) \cong Q_8$. Observamos que $C_Q(A) \lhd C_Q(B)$, pues todo subgrupo de Q_8 es normal. Entonces:

$$C_Q(B)/C_Q(A) \cong Z_2 \quad \text{o} \quad C_Q(B)/C_Q(A) \cong Z_2 \times Z_2.$$

En el primer caso, A actuaría trivialmente en $C_Q(B)/C_Q(A)$, estabilizando a la serie subnormal $C_Q(B) \rhd C_Q(A) \rhd 1$. En tal caso, por el Teorema 0.19., $[A, C_Q(B)] = 1$, que sabemos es falso, puesto que $C_Q(B) \not\subseteq C_Q(A)$.

Entonces $C_Q(B)/C_Q(A) \cong Z_2 \times Z_2$, $|C_Q(A)| = 2$, y así $C_Q(A) = Q_0$. También A actúa no trivialmente en $C_Q(B)/C_Q(A)$, y, como $|Aut(Z_2 \times Z_2)| = |S_3| = 6$, resulta que $p = 3$.

Si ahora B es cualquier subgrupo de A de índice p, $C_Q(B) \neq Q_0$ implica que $C_Q(B) \not\subseteq C_Q(A)$ y aplicando de nuevo el Lema 4.12., tenemos (iii). #

Lema 4.14. [Ben 4.12] Q/Q_0 es elementalmente abeliano.

Demostración. De hecho probaremos que Q_0 es el subgrupo de Frattini de Q. Sea $\Phi := \Phi(Q)$, el subgrupo de Frattini de Q. Si N es un subgrupo maximal de Q, entonces tiene índice 2, y por lo tanto es normal en Q. Luego, $N \cap Z(Q) \neq 1$ (por el Lema 0.11.), y esto implica que $\Omega_1(N \cap Z(Q)) \neq 1$. Entonces $N \cap \Omega_1(Z(Q)) \neq 1$, pero $\Omega_1(Z(Q)) = Q_0$ (por el Lema 4.9.). Así $N \cap Q_0 \neq 1$. Recordando que $|Q_0| = 2$, tenemos $Q_0 \subseteq N$. Entonces Q_0 está contenido en cualquier subgrupo maximal, y por lo tanto $Q_0 \subseteq \Phi$.

Suponga que $Q_0 \subsetneq \Phi$. Entonces, por el Teorema 0.13., podemos refinar la serie normal $Q \rhd \Phi \rhd Q_0 \rhd 1$, y encontrar un subgrupo $U \lhd Q$, de orden 4, con $Q_0 \subseteq U \subseteq \Phi$. Ahora $Q/C_Q(U)$ se inyecta en $Aut(U)$ (Q actúa en U). Entonces, tenemos dos posibilidades:

$$|Aut(U)| = \begin{cases} 2 \text{ si } U \cong Z_4 \\ 6 \text{ si } U \cong Z_2 \times Z_2 \end{cases}$$

En cualquier caso, $|Q : C_Q(U)| \leq 2$, y o bien $C_Q(U) = Q$, o bien $C_Q(U)$ es maximal. De nuevo en cualquier caso $\Phi \subseteq C_Q(U)$, es decir, $U \subseteq Z(\Phi)$. Así tenemos $Q_0 \subsetneq U \subseteq Z(\Phi) \subseteq \Phi$. Como $\Omega_1(Z(\Phi))$ es un q-subgrupo elementalmente abeliano de Q, claramente A-invariante, por el Lema 4.9., $Q_0 = \Omega_1(Z(\Phi))$. Luego $Z(\Phi)$ es cíclico y $|Aut(Z(\Phi))| = |Aut(Z_{2^\alpha})| = 2^\alpha - 2^{\alpha-1} = 2^{\alpha-1}$. A tendría entonces que actuar trivialmente en $Z(\Phi) \supsetneq Q_0$, esto contradice $C_Q(A) = Q_0$.

Finalmente, $Q/Q_0 = Q/\Phi(Q)$ es elementalmente abeliano, por el Teorema 0.38. #

Lema 4.15. [Ben 4.13] $Q/Q_0 =: \overline{Q}$ es producto directo de $n \geq 2$ subgrupos A-invariantes de orden 4: $\overline{Q}_1, \ldots, \overline{Q}_n$.

Demostración. Como A actúa en $\overline{Q}$, sabemos (por el Lema 2.3.) que $\overline{Q} = \langle C_{\overline{Q}}(B) \mid |A : B| = p \rangle$. Además, por el Lema 2.2., para cada $B \subseteq A$:

$$C_{\overline{Q}}(B) = \frac{C_Q(B)Q_0}{Q_0} = \frac{C_Q(B)}{Q_0}.$$

Luego, si $C_{\overline{Q}}(B) \neq 1$, entonces $C_Q(B) \neq Q_0$. Por el Lema 4.13., $|C_Q(B)| = 8$, y en consecuencia, $|C_{\overline{Q}}(B)| = 4$. Claramente $C_{\overline{Q}}(B)$ es A-invariante (pues B y $\overline{Q}$ lo son).

Observemos también que (si $C_Q(B) \neq 1$) $C_Q(B)^* := C_Q(B) - \{1\}$ es una órbita bajo la acción de A: claramente A actúa en $C_Q(B)^*$ (con acción de conjuntos) y $|C_Q(B)^*| = 3$; como $|A| = 3^a$, tenemos que $C_Q(B)^*$ es una órbita o $C_Q(B)^* \subseteq C_Q(A)$. Esto último no ocurre pues, por el Lema 2.2. y el Lema 4.13.,

$$C_Q(A) = \frac{C_Q(A)Q_0}{Q_0} = \frac{Q_0}{Q_0} = 1.$$

Tomemos ahora algunos subgrupos $B_1, \ldots, B_n \subseteq A$, con $|A:B_i| = p = 3$, para $i = 1,2,\ldots,n$, tales que $\overline{Q}_1, \ldots, \overline{Q}_n$ (definidos por $\overline{Q}_i := C_Q(B_i)$ para $i = 1,2,\ldots,n$) formen un producto directo (interno) maximal $\overline{Q}_1 \times \ldots \times \overline{Q}_n \subseteq \overline{Q}$.

Suponga, para llegar a una contradicción, que $\overline{Q}_1 \times \ldots \times \overline{Q}_n \subsetneq \overline{Q}$.

Por el Lema 2.3., existe un subgrupo $B \subseteq A$, con $|A:B| = p$ y $C_Q(B) \not\subseteq \overline{Q}_1 \times \ldots \times \overline{Q}_n$. Como $C_Q(B)^*$ es una órbita bajo la acción de A, y $\overline{Q}_1 \times \ldots \times \overline{Q}_n$ es A-invariante (y por lo tanto unión de órbitas), tenemos que $C_Q(B)^* \subseteq \overline{Q}_1 \times \ldots \times \overline{Q}_n$ o $C_Q(B)^* \cap \overline{Q}_1 \times \ldots \times \overline{Q}_n = \phi$. Como $C_Q(B) \not\subseteq \overline{Q}_1 \times \ldots \times \overline{Q}_n$, se sigue que $C_Q(B) \cap \overline{Q}_1 \times \ldots \times \overline{Q}_n = 1$. Ahora $C_Q(B) \times \overline{Q}_1 \times \ldots \times \overline{Q}_n$ es un producto directo más grande que $\overline{Q}_1 \times \ldots \times \overline{Q}_n$. Contradicción.

Concluimos que $\overline{Q} = \overline{Q}_1 \times \ldots \times \overline{Q}_n$, como se afirmaba.

Si ahora $n = 1$, tenemos $\overline{Q} = \overline{Q}_1 = C_Q(B_1)$. Esto implica, por el Teorema 0.29., que $B_1 \subseteq C_A(\overline{Q}) = 1$. Luego $B_1 = 1$ y $|A| = p$, contrario a $r(A) = d \geq 2$. #

Lema 4.16. [Ben 4.14] Sea $t \in Q - Q_0$ un conjugado a la involución $z \in Q_0$, con $z \notin F(C_G(t))$. Sea $C := H \cap F(C_G(t)) = C_{F(C_G(t))}(z)$. Entonces $C \cap Q = \langle t \rangle$, $|C| \geq 2^n$ (con n como en el lema anterior), y $C_{O_{3'}(H)}(t) \subseteq Q$.

Demostración. Sea $Q' := F(C_G(t)) \trianglelefteq Q$, $z \notin Q'$. Como $H = C_G(z)$, tenemos $z \in C_G(t)$, luego z actúa en Q' y (trivialmente) en $\langle t \rangle$. Entonces z actúa en $\overline{Q}' := Q'/\langle t \rangle$, que es elementalmente abeliano por el Lema 4.14. Así $[z,\overline{Q}'] \subseteq \overline{Q}'$ y z actúa en $[z,\overline{Q}']$ por inversión. Como $\overline{Q}'$ es elementalmente abeliano, z actúa trivialmente en $[z,\overline{Q}']$ (pues todo elemento es su propio inverso).

Ahora, sea $T \in End(\overline{Q}')$ la transformación Z_2-lineal definida por $T(q) = zqz^{-1}q = (T_z + I)(q)$, donde $T_z(q) := zqz^{-1}$ es la transformación lineal inducida por z. Luego $Ker(T) = C_{\overline{Q}'}(z)$ y $Im(T) = [z,\overline{Q}']$. Como $[z,\overline{Q}'] \subseteq C_{\overline{Q}'}(z)$ (pues z actúa

trivialmente en $[z,\overline{Q}']$), tenemos $dim(Im(T)) \le dim(Ker(T))$. Además, $2n = dim(\overline{Q}') = dim(Im(T)) + dim(Ker(T))$. Así, $dim(Ker(T)) \ge 2n/2 = n$, es decir, $|C_{Q'}(z)| \ge 2^n$.

Sea $\pi: Q' \to \overline{Q}'$ la proyección natural.

Observemos que $\pi^{-1}(C_{\overline{Q}'}(z)) \subseteq N_{Q'}(\langle t,z\rangle)$.

Si $x \in \pi^{-1}(C_{\overline{Q}'}(z))$, entonces $xzx^{-1} \equiv z \bmod t$, es decir, $xzx^{-1} = z$ o $xzx^{-1} = zt$. En particular, $xzx^{-1} \in \langle t,z\rangle$. Además $x \in \pi^{-1}(C_{\overline{Q}'}(z))$ implica que $x \in Q' \subseteq C_G(t)$; por lo tanto, $xtx^{-1} = t \in \langle t,z\rangle$.

Concluimos que $x \in N_{Q'}(\langle t,z\rangle)$.

Así, $N_{Q'}(\langle t,z\rangle) \ge 2^{n+1}$.

Además $C = H \cap Q' = C_{Q'}(z) = C_{Q'}(\langle t,z\rangle)$ (pues $Q' \subseteq C_G(t)$). Luego:

$C = C_{Q'}(\langle t,z\rangle) \subseteq N_{Q'}(\langle t,z\rangle)$ y entonces $\dfrac{N_{Q'}(\langle t,z\rangle)}{C_{Q'}(\langle t,z\rangle)}$ se inyecta en $Aut(\langle z,t\rangle) \cong S_3$. Luego $|N_{Q'}(\langle t,z\rangle) : C_{Q'}(\langle t,z\rangle)| \le 2$, y por lo tanto, $|C| = |C_{Q'}(\langle t,z\rangle)| \ge 2^n$.

Sea $V = C \cap Q = H \cap Q' \cap Q = Q' \cap Q \lhd H' \cap Q = C_Q(t)$ (con $H' := C_G(t)$). Luego $t \in V \lhd C_Q(t)$ y $C_Q(t) \subseteq N_Q(V)$.

También tenemos que $C_Q(t) = C_Q(\langle t,z\rangle)$ (pues $Q \subseteq H = C_G(z)$) y como Q/Q_0 es elementalmente abeliano, tenemos $\langle t,z\rangle/Q_0 \lhd Q/Q_0$, y ello implica que $\langle t,z\rangle \lhd Q$. Entonces $Q/C_Q(\langle t,z\rangle)$ se inyecta en $Aut(\langle t,z\rangle) \cong S_3$. Así, $|Q : C_Q(t)| = |Q : C_Q(\langle t,z\rangle)| \le 2$, y, consecuentemente, $|Q : N_Q(V)| \le 2$.

Pero $V \not\lhd Q$, pues de otro modo $V \cap Z(Q) \ne 1$ (ver el Lema 0.11.) implica que $V \cap \Omega_1(Z(Q)) \ne 1$; luego $z \in V = Q \cap Q' \subseteq Q' = F(C_G(t))$. Contrario a las hipótesis.

Concluimos que $|Q : N_Q(V)| = 2$.

Además $VQ_0/Q_0 \lhd Q/Q_0$ implica que $VQ_0 \lhd Q$. Entonces, si $g \in Q - N_Q(V)$, $V^g Q_0 = (VQ_0)^g = VQ_0$. Luego $\langle V, V^g\rangle = VV^g = VQ_0$. Por lo tanto $|V \cap V^g| = \dfrac{|V||V^g|}{|VQ_0|} = \dfrac{|V|}{2}$.

Si $|V| > 2$, tendríamos que $V \cap V^g \ne 1$, pero $V \cap V^g \lhd Q$ y $z \in V \cap V^g \subseteq V \subseteq Q'$, contrario a las hipótesis.

Concluimos que $|V| = 2$ y, entonces, $\langle t\rangle = V = C \cap Q$.

Recuerde que $O_{2,p}(H)$ se define por $O_{2,p}(H)/O_2(H) = O_p(H/O_2(H))$.

Sea P un p-Sylow de $C_{O_{2,p}(H)}(t)$. Entonces $P \subseteq O_{2,p}(H) \cap C_G(t) = O_{2,p}(H) \cap H'$ ($H' := C_G(t)$) y $C = H \cap Q'$. Como H actúa en $O_{2,p}(H)$ *char* H, $C_G(t)$ actúa en $Q' = F(C_G(t))$ y $Q = O_2(H)$ es un q-Sylow normal de $O_{2,p}(H)$, tenemos:

$$[P,C] \subseteq [O_{2,p}(H) \cap C_G(t) : H \cap Q'] \subseteq O_{2,p}(H) \cap Q' = Q \cap Q' = V = \langle t \rangle$$

Pero P actúa en $C = H \cap Q'$, pues P actúa en H ($P \subseteq H$) y en Q' *char* $H' \supseteq P$. Luego, por el Teorema 2.1., tenemos $C = C_C(P)[P,C]$. Como P actúa trivialmente en $\langle t \rangle$, tenemos $[P,C] \subseteq \langle t \rangle \subseteq C_C(P)$. Entonces $C = C_C(P)$, y por lo tanto $[P,C] = 1$. Recordando que $C = C_{Q'}(z)$, acabamos de probar que $[P, C_{Q'}(z)] = 1$.

Ahora, P conmuta con Q_0 *char* $H \supseteq P$ ($Aut(Q_0) = 1$), es decir, Q_0 y P forman un producto directo (interno) $PQ_0 = P \times Q_0$. Además este producto actúa en Q', pues $P \times Q_0 \subseteq C_G(t) \triangleright Q'$. Entonces, gracias al último resultado del párrafo anterior, podemos aplicar el Lema 2.4.(ii) ($Q_0 = \langle z \rangle$ en lugar de P, P en lugar de Q y Q' en lugar de B) para concluir que $[P,Q'] = 1$. Como $P \subseteq H' \cap C_G(Q')$ y $Q' = F(H')$, tenemos $P \subseteq Q'$ (Teorema 0.29.). Esto implica que $P = 1$. Concluimos que $C_{O_{2,p}(H)}(t) \subseteq Q$. #

El siguiente lema vale en general, al margen de los supuestos del capítulo.

Lema 4.17. [Suz II, 4.4.20] Suponga que $p \neq 2$, A y P son p-grupos, A actúa P y P no es cíclico. Entonces existe un subgrupo $U \lhd P$, A-invariante con $U \cong Z_p \times Z_p$.

Demostración. Dividimos el problema en 3 casos:

Caso 1. P es elementalmente abeliano.

Como A actúa en P, por la ecuación de clase, A centraliza a algún subgrupo no trivial de P, es decir, $C_P(A) \neq 1$. Si $|C_P(A)| > p$, ya acabamos. Si no, A actúa en $P/C_P(A)$ y centraliza a algún subgrupo $\overline{U}$, de orden p. Entonces U (la imagen inversa de $\overline{U}$ bajo la proyección natural) es el subgrupo que buscamos.

Caso 2. P es abeliano.

En este caso $\Omega_1(P)$ es elementalmente abeliano y de rango máximo en P. En particular, $\Omega_1(P)$ no es cíclico. Por el Caso 1, existe un subgrupo $U \subseteq \Omega_1(P)$, A-invariante y $U \cong Z_p \times Z_p$. Claramente $U \lhd P$, pues P es abeliano.

Caso 3. P no es abeliano.

A actúa en $Z(P) \neq 1$ y centraliza a algún subgrupo de orden p: $P_0 \subseteq Z(P)$. Entonces $P_0 \lhd P$ y P_0 es A-invariante. Además P/P_0 no es cíclico (pues P sería abeliano). Luego, como A actúa en P/P_0, por hipótesis de inducción, existe una $\overline{U}_1 \lhd P/P_0$, $\overline{U}_1$ es A-invariante y $\overline{U}_1 \cong Z_p \times Z_p$. Entonces, la imagen inversa de $\overline{U}_1$ bajo la proyección natural satisface: $U_1 \lhd P$, U_1 es A-invariante, $|U_1| = p^3$ y U_1 no es cíclico (pues $\overline{U}_1 \cong Z_p \times Z_p$). Dividimos ahora en dos subcasos:

Subcaso 3.1. U_1 tiene exponente p.

Tenemos que $P \rtimes A$ actúa en U_1, y centraliza algún subgrupo U_0 de orden p. También $P \rtimes A$ actúa en U_1/U_0 y centraliza a algún subgrupo $\overline{U}$ de orden p. Entonces U (la imagen inversa de $\overline{U}$) es el grupo que buscamos.

Subcaso 3.2. U_1 no tiene exponente p.

En este caso, U_1 tiene, necesariamente, un elemento x, de orden p^2. Puesto que U_1 no es cíclico, existe una $y \in U_1 - \langle x \rangle$ de orden p (Lema 0.41.). Como $|U_1 : \langle x \rangle| = p$, $\langle x \rangle \lhd U_1$. Entonces $\langle y \rangle$ actúa en $\langle x \rangle$, luego $U_1 = \langle x, y \rangle \cong Z_{p^2} \rtimes Z_p$. Claramente $\langle y \rangle$ actúa trivialmente en $\langle x^p \rangle$. Luego $\langle y, x^p \rangle$ es elementalmente abeliano y $\langle y, x^p \rangle \subseteq \Omega_1(U_1)$.

Si existiera una $z \in U_1 - \langle y, x^p \rangle$ de orden p, entonces z actuaría en $\langle y, x^p \rangle$ (éste último es normal pues tiene índice p en U_1), y en consecuencia, $U_1 \cong (Z_p \times Z_p) \rtimes Z_p$. Por el Corolario 0.35., U_1 tendría exponente p, contrario a lo supuesto.

Concluimos que $\Omega_1(U_1) = \langle y, x^p \rangle$ *char* U_1. Luego, $U := \langle y, x^p \rangle$ es el subgrupo que buscamos. #

Lema 4.18. [Ben 4.15] Suponga que $d \geq 3$. Sea P un p-Sylow de $O_{2,p}(H)$. Entonces P es un grupo no abeliano de orden p^3 $(= 3^3)$.

Demostración. Sean $B_1, B_2, \ldots, B_m$ todos los subgrupos de A de índice p tales que $Q_0 \subseteq C_Q(B_i)$ y $Q_i := C_Q(B_i)$ para $1 \leq i \leq m$. También, para $1 \leq i \leq m$, sean $\overline{Q_i} := Q_i/Q_0$. Por el Lema 2.3., $Q = \langle Q_i \mid 1 \leq i \leq m \rangle$. Por el Lema 4.12., cada Q_i es isomorfo al grupo cuaternio de orden 8 y entonces $\overline{Q_i} \cong Z_2 \times Z_2$, para toda i. Observamos que $Q_i = Q_j$ implica que $B_i = B_j$, pues de otro modo, por el Lema 4.13., $Q_i \subseteq C_Q(\langle B_i, B_j \rangle) = C_Q(A) = Q_0$ que es una contradicción. En consecuencia $Q_i = Q_j$ si y sólo si $B_i = B_j$ si y sólo si $i = j$. Note que si n es como en el Lema 4.15., $n \leq m$.

Igual que antes, sea z la única involución de Q_0.

Sin pérdida de generalidad, por el Lema 0.16., podemos escoger a P de forma que sea A-invariante.

Afirmamos que Q_iQ_j, para $i \neq j$, contiene (al menos) una involución t, conjugada a z, tal que $z \notin F(C_G(t))$ y que ningún elemento no trivial de P centraliza a Q_iQ_j (es decir: $C_P(Q_iQ_j) = 1$).

Claramente Q_iQ_j es un grupo (como Q/Q_0 es elementalmente abeliano, todo subgrupo de Q que contenga a Q_0 es normal en Q). Sea $B = C_A(Q_iQ_j)$. Entonces $Q_iQ_j \subseteq C_Q(B)$ y $B_i \cap B_j \subseteq B$. Como $B_i \neq B_j$, tenemos:

$$|A| = |B_i B_j| = \frac{|B_i||B_j|}{|B_i \cap B_j|},$$

y como $|A: B_i| = |A: B_j| = p$, resulta que:

$$|B_i \cap B_j| = \frac{|B_i||B_j|}{|A|} = \frac{|B_i|}{p}.$$

Luego $|A: B_i \cap B_j| = p^2$, como $B_i \cap B_j \subseteq B$ tenemos $|A: B| \leq p^2$.

Como cada Q_k, para $1 \leq k \leq m$, es isomorfo al grupo cuaternio con 8 elementos, $Q_i Q_j$ no puede ser abeliano.

Observamos también que B_i actúa en $Q_k = C_Q(B_k)$, para toda k (pues $B_i, B_k \subseteq A$, que es abeliano, y Q *char* $H \supseteq B_i$). Además B_i no puede actuar trivialmente en Q_j, pues, en ese caso, $Q_j \subseteq C_Q(B_i) = Q_i$, en contradicción con $i \neq j$. Concluimos que B_i actúa no trivialmente en $Q_i Q_j$. En particular, $Q_i Q_j$ tiene automorfismos no triviales de orden impar.

Si $Q_i Q_j$ no tiene más que una sola involución (la involución z), entonces no tiene 4-grupos. En tal caso, el Lema 1.12. afirma que $|Q_i Q_j| = 8$, lo que implica $Q_i Q_j = Q_i = Q_j$, una contradicción.

Concluimos que $Q_i Q_j$ tiene una involución $t' \neq z$.

Como $C_Q(A) = Q_0 \subsetneq Q_i Q_j \subseteq C_Q(B)$, tenemos que $C_Q(B) \subsetneq C_Q(A)$. Entonces el Lema 4.12. nos dice que existe otra involución $t \neq z$ en $Q_i Q_j$, conjugada a z, y tal que $z \notin F(C_Q(t))$.

Para una tal t, el Lema 4.16. afirma que $C_P(t) \subseteq C_{O_{2,p}(H)}(t) \subseteq Q$. En particular $C_P(t) = 1$. Concluimos que ningún elemento no trivial de P puede centralizar a dos Q_k's, es decir: para $i \neq j$, $C_P(Q_i Q_j) = 1$.

Con esto hemos probado la afirmación anterior.

Mostraremos a continuación que P no es cíclico.

Recuerde que $Q = F(H) = O_q(H)$. Sean $\pi: H \to H/Q$ la proyección natural y $\overline{H} := \pi(H)$. Recuerde que $O_{2,p}(H) = \pi^{-1}(O_p(\overline{H})) = \pi^{-1}(O_p(H/Q))$. Observamos que $\overline{P} := \pi(P) \cong P$, pues:

$$\overline{P} = \frac{PQ}{Q} \cong \frac{P}{P \cap Q} = \frac{P}{1} \cong P.$$

Basta probar, entonces, que $\overline{P}$ no es cíclico.

De acuerdo con las definiciones que tenemos, $\overline{P} = O_p(\overline{H})$. También $\overline{P} = F(\overline{H})$ por el Teorema 0.28., pues $O_q(H/O_q(H)) = 1$. Por el Teorema 0.29., $C_{\overline{H}}(\overline{P}) \subseteq \overline{P}$.

Supongamos, para llegar a una contradicción, que $\overline{P}$ **es cíclico. Entonces** $C_{\overline{H}}(\overline{P}) = \overline{P}$. **Además,** $\overline{H}/C_{\overline{H}}(\overline{P})$ **se inyecta en** $Aut(\overline{P})$. **Como** $|Aut(\overline{P})| = p^{a-1}(p-1) = 2 \cdot 3^{a-1}$, **tenemos que** $|\overline{H}:C_{\overline{H}}(\overline{P})|_2 \leq 2$. **Si** P' **es un** p-**Sylow de** $\overline{H}/C_{\overline{H}}(\overline{P})$, **entonces debe ser normal pues tiene índice a lo más 2. Luego** $P' \subseteq O_p(\overline{H}/C_{\overline{H}}(\overline{P})) = O_p(\overline{H}/\overline{P}) = O_p(\overline{H}/O_p(\overline{H})) = 1$. **Se sigue que** $|\overline{H}:\overline{P}| = |\overline{H}:C_{\overline{H}}(\overline{P})| \leq 2$. **Entonces** $\overline{P}$ **es un** p-**Sylow de** $\overline{H}$.

Como $|H| = |\overline{H}||Q|$, **tenemos** $|H|_p = |\overline{H}|_p$, **y en consecuencia,** $P \cong \overline{P}$ **es un** p-**Sylow de** H. **Así** $A^g \subseteq P$ **para alguna** $g \in H$. **Luego** $1 = r_p(P) \geq r_p(A) = d \geq 3$. **Contradicción.**

Concluimos que P **no puede ser cíclico.**

Recordando que hemos escogido a P **de tal forma que sea** A-**invariante, ahora podemos aplicar el Lema 4.17., para concluir que existe un subgrupo normal** U **de** P, **que es** A-**invariante y de tipo** (p, p).

Afirmamos que podemos suponer, sin pérdida de generalidad, que $U \subseteq A$:
Tenemos que $r(U) = 2$. **También** $A/C_A(U)$ **se inyecta en** $Aut(U)$. **Como** $|Aut(U)| = p(p+1)(p-1)^2$, **resulta que** $|A:C_A(U)| \leq p$. **Luego** $r(C_A(U)) \geq d-1$. **Si** $U \subsetneq A$, **entonces** $r(U \cdot C_A(U)) > d-1$, **lo que implica que** $r(U \cdot C_A(U)) = d$. **Claramente** $U \cdot C_A(U)$ **es elementalmente abeliano y** P **es** $U \cdot C_A(U)$-**invariante. Luego, podemos reemplazar** A **por** $U \cdot C_A(U)$, **en caso de ser necesario, y suponer en adelante que** $U \subseteq A$. **Entonces:**

Supondremos en adelante, que existe un subgrupo $U \subseteq P \cap A$, **de tipo** (p, p) **y normalizado por** P **y por** A.

Recuerde que $\overline{Q_k} := Q_k/Q_o \cong Z_2 \times Z_2$, **para** $1 \leq k \leq m$. **Claramente** $U \subseteq A$ **actúa en cada** $Q_k := C_Q(B_k)$ **y por lo tanto, también en cada** $\overline{Q_k}$.

Sean $U_k := C_U(\overline{Q_k})$ **para** $1 \leq k \leq m$.

Observamos que $U_k \neq 1$. **Si no,** $U \cong U/U_k$ **se inyecta en** $Aut(\overline{Q_k}) \cong S_3$, **lo que es imposible pues** U **tiene orden 4.**

Afirmamos ahora que $\overline{Q_k} = C_{\overline{Q}}(U_k)$:

Claramente $\overline{Q_k} \subseteq C_{\overline{Q}}(U_k)$. **Supongamos que** $\overline{Q_k} \subsetneq C_{\overline{Q}}(U_k)$. **Entonces, como** $C_{\overline{Q}}(U_k)$ **es** A-**invariante, por el Lema 2.3., existe una** $B \subseteq A$, **con** $|A:B| = p$ **y tal que** $1 \neq C_{C_{\overline{Q}}(U_k)}(B) \subsetneq \overline{Q_k}$. **Teniendo en mente que** $Q_0 \subsetneq C_Q(B)$ **si y sólo si** $C_{\overline{Q}}(B) \neq 1$ **(Lema 2.2.), obtenemos de lo anterior que** $B = B_j$, **para alguna** j **con** $1 \leq j \leq m$. **Como** $C_{\overline{Q}}(U_k)$ **es**

A-invariante y $C_Q(B_j)^*$ es una órbita de $\overline{Q}$ según la acción de A (ver la prueba del Lema 4.15.), tenemos:

$$1 \neq C_{C_Q(U_k)}(B_j) = C_Q(U_k) \cap C_Q(B_j) = C_Q(B_j).$$

Luego, por el Lema 2.2., $\overline{Q}_j = C_Q(B_j) \subseteq C_Q(U_k)$ y $\overline{Q}_j = C_Q(B_j) \trianglelefteq \overline{Q}_k$; esto último implica que $j \neq k$. Entonces $\overline{Q}_j \overline{Q}_k \subseteq C_Q(U_k)$. También, U_k actúa trivialmente en Q_0 ($Aut(Q_0) = 1$). Luego U_k estabiliza a la serie subnormal: $Q_j Q_k \rhd Q_0 \rhd 1$, y por el Teorema 0.19., U_k centraliza a $Q_j Q_k$. Recordando, de la primera afirmación de esta demostración, que ningún elemento no trivial de P puede centralizar a dos Q_k's y que $U_k \subseteq P$, concluimos que $U_k = 1$, contrario a lo que sabemos.

Gracias a la contradicción anterior, concluimos que el supuesto $\overline{Q}_k \subsetneq C_Q(U_k)$, es falso.

Entonces $\overline{Q}_k = C_Q(U_k)$, como se había afirmado.

Ahora, por el Lema 2.2.:

$$\frac{Q_k}{Q_0} = \overline{Q}_k = C_Q(U_k) = \frac{C_Q(U_k)}{Q_0}.$$

Luego, $Q_k = C_Q(U_k)$ y, por el Teorema 0.19., $U_k = C_U(\overline{Q}_k) = C_U(Q_k)$.

Entonces $C_P(U)$ normaliza a cada $Q_k = C_Q(U_k)$ ($C_P(U)$ actúa en $U_k \subseteq U$ (trivialmente) y también actúa en Q).

Afirmamos también que $U_k \neq U$.

Si $U_k = U$, entonces $Q_k = C_Q(U)$. Si U_j es otro de estos subgrupos, $U_j \subseteq U = U_k$. Luego $Q_k = C_Q(U_k) \subseteq C_Q(U_j) = Q_j$. Entonces todos los Q_k's son iguales (pues $|Q_k| = 8$, para toda k). Luego $n \leq m = 1$ en contradicción con el Lema 4.15.

Si observamos ahora que $U/U_k \neq 1$ se inyecta en $Aut(\overline{Q}_k) \cong S_3$ y que $U \subseteq C_P(U)$, podemos afirmar también que $C_P(U)$ normaliza a cada $\overline{Q}_k = C_Q(U_k)$ y actúa no trivialmente en cada $\overline{Q}_k$. En particular, $C_P(U)$ actúa no trivialmente en cada Q_k.

Veamos ahora que $|C_P(U)| = p^2 = 3^2$:

Sea $X := C_P(U)$. Entonces $X/C_X(Q_k)$se inyecta en $Aut(Q_k)$, para toda k. Como sabemos que $X = C_P(U)$ actúa no trivialmente en cada Q_k, y que $|Aut(Q_k)| = 24$ (Lema 0.43.), tenemos $|X:C_X(Q_k)| = 3$, para toda k.

Si $Q_i \neq Q_j$ entonces $C_X(Q_i) \cap C_X(Q_j) = C_X(Q_i Q_j) \subseteq C_P(Q_i Q_j) = 1$. También, como

$C_X(Q_i)$ y $C_X(Q_j)$ son ambos maximales en X, y no triviales (pues $1 \neq U_k \subseteq C_X(Q_k)$ para toda k), concluimos que $C_X(Q_i)C_X(Q_j) = X$. Entonces:

$$3 = \frac{|X|}{|C_X(Q_i)|} = \frac{|C_X(Q_i)C_X(Q_j)|}{|C_X(Q_i)|} = \frac{1}{|C_X(Q_i)|} \cdot \frac{|C_X(Q_i)||C_X(Q_j)|}{|C_X(Q_i) \cap C_X(Q_j)|} = |C_X(Q_j)| = |C_X(Q_i)|.$$

Concluimos que $|C_P(U)| = |X| = p^2 = 3^2$.

Ahora $P/C_P(U)$ se inyecta en $Aut(U) \cong GL(2,p)$. Como $|Aut(U)| = p(p+1)(p-1)^2$, concluimos que $|P:C_P(U)| \leq p = 3$. Luego $p^2 \leq |P| \leq p^3$.

Si $[A, P] = 1$, entonces, en el cociente $\overline{H} = H/Q$, tenemos $\overline{A} \cong A$, $\overline{P} \cong P$ y $[\overline{A}, \overline{P}] = 1$. También $\overline{A} \subseteq C_{\overline{H}}(\overline{P}) \subseteq \overline{P} = F(\overline{H})$. Luego $r(\overline{A}) = r(A) = d \geq 3$, implica que $|A| \geq p^3$. Como $|\overline{P}| = |P| \leq p^3$, resulta que $|\overline{P}| = |\overline{A}| = p^3$. En consecuencia $P \cong \overline{P} = \overline{A}$ es abeliano y $|C_P(U)| = |P| \neq p^2$. Contradicción.

Concluimos entonces $[A,P] \neq 1$.

Luego $|P| = p^3$ (si no, $P = U$ y $[A,P] = 1$).
Finalmente, P no es abeliano, pues si lo fuera, $C_P(U) = P$ que no tiene orden p^2. #

Lema 4.19. [Ben 4.16] $d = 2$.

Demostración. Suponga $d \geq 3$. Sean $B_1, \ldots, B_n$, como en la prueba del Lema 4.15. y $Q_i := C_Q(B_i)$ para $1 \leq i \leq n$. Sea t como en la prueba de el Lema 4.18., es decir: t es una involución conjugada a z, $t \in Q_iQ_j$ y $z \notin F(C_G(t))$. Sea $C = H \cap F(C_G(t))$ (igual que en el Lema 4.16.). Sea $\overline{H} = H/O_{2,p}(H) = H/PQ$, con $P \in Syl_p(O_{2,p}(H))$. Tomemos $B := C_A(t)$.

Entonces $B \neq 1$:
Tenemos $C_A(Q_iQ_j) \subseteq C_A(t) =: B$. Igual que antes (primera afirmación de la prueba del Lema 4.18.), $|A:C_A(Q_iQ_j)| \leq p^2$. Como $r(A) = d \geq 3$, tenemos $1 \neq C_A(Q_iQ_j) \subseteq B$.

Si $B \subseteq O_{2,p}(H)$, resulta que $B = C_A(t) \cap O_{2,p}(H) \subseteq C_{O_{2,p}(H)}(t) \subseteq Q$ (Lema 4.16.). Esto implicaría que $B = 1$, contrario a lo que sabemos.
Concluimos que $B \not\subseteq O_{2,p}(H)$.

Veamos que H actúa en QP/QP', donde $P' = [P, P]$ es el grupo derivado de P:
$Q \lhd O_{2,p}(H)$ y $Q \in Syl_q(O_{2,p}(H))$ implican que Q *char* $O_{2,p}(H)$.

Si $\pi: O_{2,p}(H) \to O_{2,p}(H)/Q$ es la proyección natural, entonces $\pi(O_{2,p}(H)) = \pi(P) \cong P$ y $\pi([P,P]) = [\pi(P), \pi(P)]$. Luego, $\pi(QP') = \pi(P') = \pi(P)'$ *char* $\pi(P) = \pi(O_{2,p}(H))$. Así, puesto que Q *char* $O_{2,p}(H)$, tenemos: QP' *char* QP. Entonces QP' *char* QP *char* H, y así, H actúa en QP/QP'.

Ahora, $P/Z(P)$ no puede ser cíclico, pues si lo fuera, $P = \langle Z(P), x \rangle$ (tomando a x de forma que $\langle \overline{x} \rangle = P/Z(P)$) sería abeliano, contrario al Lema 4.18. Entonces $Z(P) \neq 1$ (P es un p-grupo) implica que $|Z(P)| = p$ y $P/Z(P) \cong Z_p \times Z_p$. Como $P/Z(P)$ es abeliano y P no lo es, tenemos $1 \neq P' \subseteq Z(P)$. Entonces $P' = Z(P)$. Luego $P/P' \cong Z_p \times Z_p$. También,

$$\frac{QP}{QP'} = \frac{(QP')P}{QP'} \cong \frac{P}{P \cap QP'} = \frac{P}{P'}, \text{ y por lo tanto: } \frac{QP}{QP'} \cong Z_p \times Z_p.$$

Afirmamos que $O_{2,p}(H) = C_H\left(\frac{QP}{QP'}\right)$.

Notemos que $O_{2,p}(H) = QP$ y $P \cong \overline{P} := \frac{QP}{Q} = O_p(H/Q) = F(H/Q)$ (pues $Q = O_q(H)$ y $O_q(H/O_q(H)) = 1$). También $\overline{(P')} := \frac{QP'}{Q} = \frac{Q[P,P]}{Q} = [\overline{P}, \overline{P}] = (\overline{P})'$ y $P' \cong \overline{P}' = \overline{Z(P)} \subseteq Z(\overline{P})$.

Observamos que $x \in C_H\left(\frac{QP}{QP'}\right)$ si y sólo si $x \in H$ y $[x, QP] \subseteq QP'$.

Como $[QP, QP] \subseteq QP'$ (pues $QP/QP' \cong Z_p \times Z_p$ es abeliano), tenemos:

$$QP \subseteq C_H\left(\frac{QP}{QP'}\right).$$

Si $w \in C_H\left(\frac{QP}{QP'}\right)$ es un q-elemento, entonces $[w, QP] \subseteq QP'$; tomando el cociente por Q, resulta $[\overline{w}, \overline{P}] \subseteq \overline{P}'$. Si $1 \neq x = [a,b]$, con $a, b \in \overline{P}$, entonces $\overline{P}' = \langle x \rangle$ (ya que $\overline{P}' \cong Z_p$). También, si $c \in \overline{P}$, tenemos $\overline{w} c \overline{w}^{-1} c^{-1} = x_1$, para alguna $x_1 \in \overline{P}'$. Luego, $\overline{w} c \overline{w}^{-1} = x_1 c$. Entonces $\overline{w} x \overline{w}^{-1} = \overline{w}[a,b]\overline{w}^{-1} = [\overline{w} a \overline{w}^{-1}, \overline{w} b \overline{w}^{-1}] = [x_1 a, x_2 b]$, para algunas $x_1, x_2 \in \overline{P}'$. Como $x_1, x_2 \in \overline{P}' = Z(\overline{P})$, resulta $\overline{w} x \overline{w}^{-1} = [x_1 a, x_2 b] = [a,b] = x$. Así, $\overline{w}$ actúa trivialmente en $\overline{P}'$. Como $[\overline{w}, \overline{P}] \subseteq \overline{P}'$, tenemos que $\overline{w}$ estabiliza a la serie $\overline{P} \rhd \overline{P}' \rhd 1$.

Luego $\overline{w}$ actúa trivialmente en $\overline{P}$ (Teorema 0.19., aplicado al q-grupo $\langle\overline{w}\rangle$). Entonces $\overline{w} \in C_{H/Q}(\overline{P}) \subseteq \overline{P} = F(H/Q)$, y esto implica que $\overline{w} = 1$. En consecuencia, $w \in Q$.

Ahora $C_H(QP/QP')/Q$ es un p-subgrupo de H/Q, y es normal pues $C_H(QP/QP') \lhd H$ (puesto que $C_H(QP/QP')$ es el núcleo de un homomorfismo). Entonces $C_H(QP/QP')/Q \subseteq O_p(H/Q) = \overline{P} = QP/Q$. Y así $C_H(QP/QP') \subseteq QP$.

Concluimos que $C_H(QP/QP') = QP$, como se había afirmado.

Entonces $\overline{H} := H/O_{2',p}(H)$ actúa fielmente en $QP/QP' \cong Z_p \times Z_p$. Como $B \not\subseteq O_{2',p}(H)$, tenemos que $\overline{B} := \left(B \cdot O_{2',p}(H)\right)/O_{2',p}(H)$ no es trivial.

Del Lema 4.16., tenemos: $C \cap QP = C \cap O_{2',p}(H) \subseteq C_{O_{2',p}(H)}(t) \subseteq Q$; por lo tanto, $C \cap QP = C \cap Q$. Luego: $\overline{C} := (C \cdot QP)/QP \cong C/(C \cap QP) = C/(C \cap Q) = C/\langle t \rangle$ y $|\overline{C}| = |C|/2 \geq 2^{n-1}$.

Como t es conjugada a z, digamos $t = z^g$ $(g \in G)$, resulta que $C/\langle t \rangle = C/\langle z^g \rangle \subseteq F(C_G(t))/\langle z^g \rangle = F(C_G(z^g))/\langle z^g \rangle \cong F(C_G(z))/\langle z \rangle$ es elementalmente abeliano.

Como $B = C_A(t)$ centraliza a t, B actúa en $C_G(t)$, en $F(C_G(t))$ y en $C = H \cap F(C_G(t))$ $(B \subseteq H)$. Luego, $\overline{B}$ normaliza a $\overline{C}$. Por el Teorema 2.10., tenemos $r(\overline{C}) = 1$. Luego $\overline{C} \cong Z_2$ y $|C| = 4$. Como $|C| \geq 2^n$ y $n \geq 2$, resulta $n = 2$. Entonces $Q = Q_i Q_j$ y, como al inicio de la prueba, tenemos $C_A(Q) = C_A(Q_i Q_j) \neq 1$. Por otro lado, como $Q = F(H)$ y por el Teorema 0.29., $C_A(Q) \subseteq C_H(Q) \subseteq Q$; luego $C_A(Q) = 1$. Contradicción. #

Lema B. [Ben, Lemma 2] Sea $d = max\{r_p(H) | H \in \mathcal{F}_q\}$. Suponga $d \geq 2$ y $q < p$. Entonces $d = 2$, y se cumple lo siguiente:

(i) $q = 2$ y $p = 3$.

(ii) Cualquier involución t que satisface $r_p(C_G(t)) \geq 2$, es central.

(iii) Ningún 4-subgrupo U de G satisface $r_p(C_G(U)) \geq 2$.

Demostración. Los Lemas de este capítulo han usado las hipótesis de éste, es decir: $d = max\{r_p(H) | H \in \mathcal{F}_q\}$, $d \geq 2$ y $q < p$. Los Lemas 4.9 al 4.19, asumen además el supuesto de la Nota 4.8, pero este supuesto adicional es consecuencia de los anteriores (Lema 4.7.). Entonces podemos usar libremente los resultados de todo el capítulo.

Luego:

$d = 2$ se obtiene del Lema 4.19.

$q = 2$ se sigue del Lema 4.11.

$p = 3$ es consecuencia del Lema 4.13.

(ii) se obtiene del Lema 4.10., ahora que sabemos que $d = 2$ y $q = 2$.

Probemos (iii):

Sean U un 4-subgrupo de G, con $r_p(C_G(U)) \geq 2$ y $A \subseteq C_G(U)$, con $A \cong Z_p \times Z_p$. Sea H un subgrupo de G tal que $C_G(U) \subseteq H \in \mathcal{L}_q^*$. Entonces $C_H(A) \supseteq U \cong Z_q \times Z_q$, contrario al Lema 4.5. #

5. Subgrupos p-locales, para $p \neq 2$

Seguimos bajo el supuesto de que existe un contraejemplo minimal al teorema de Burnside.

Recuerde que, para un p-grupo P, definimos:

$$J(P) := \langle E \subseteq P \mid E \text{ es elementalmente abeliano y } r(E) = r(P) \rangle.$$

El objetivo de este capítulo es probar el lema C:

Lema C. [Ben, Lemma 3] Sean $p \neq 2$, $H \in \mathcal{F}_p$ y $H_p \in Syl_p(H)$. Suponga que $J(H_p)$ no es normal en H. Entonces $q = 2$. Si además H contiene una involución central, existe otra $\overline{H} \in \mathcal{F}_p$, con $|H|_p \leq |\overline{H}|_p$ y $|F(\overline{H})| > |F(H)|$, que también contiene una involución central.

Esquema de la demostración.

La demostración se hará, a lo largo de todo el capítulo, de la siguiente manera: en los Supuestos 5.1. asumimos las hipótesis del Lema C y con ello, en el Lema 5.3., probamos que $q = 2$. A continuación, en los Supuestos 5.4., se asume que el Lema C es falso; ello nos permite concluir, después de varios pasos, los Lemas 5.9. y 5.10., que se contradicen mutuamente. En consecuencia el Lema C debe ser verdadero. #

Supuestos 5.1. Supondremos, a lo largo de todo este capítulo, las hipótesis del Lema C; es decir, supondremos que $p \neq 2$, $H \in \mathcal{F}_p$, $H_p \in Syl_p(H)$ y que $J(H_p) \not\subseteq O_p(H)$. Fijamos además un poco de notación:

$$Q \in Syl_q(O_{p,q}(H)),$$
$$P_0 \in Syl_p(N_H(Q)),$$
$$P = O_p(H) = F(H),$$
$$Z = \Omega_1(Z(P)).$$

Las siguientes observaciones son consecuencia de los supuestos anteriores y se usarán libremente a lo largo de este capítulo:

Observaciones 5.2.

(1) Como $O_q(H/O_p(H)) = O_{p,q}(H)/O_p(H)$, $O_{p,q}(H) = PQ \cong P \rtimes Q$.

(2) $J(H_p) \lhd H$ si y sólo si $J(H_p) \subseteq O_p(H)$ (ver la definición 0.36 y la nota que le sigue).

(3) Como hemos supuesto que $J(H_p) \not\lhd H$, tenemos $J(H_p) \not\subseteq O_p(H)$.

(4) $|H/O_{p,q}(H)|_p \neq 1$, pues, si no, $P \in Syl_p(H)$ y entonces $P = O_p(H) \lhd H$, luego $J(H_p) \subseteq H_p = P = O_p(H)$, contrario a (3).

Tenemos:

$$H/PQ = H/O_{p,q}(H) \cong (H/O_p(H))/(O_{p,q}(H)/O_p(H)) = (H/O_p(H))/O_q(H/O_p(H)).$$

Entonces, $O_q(H/PQ) \cong O_q((H/P)/O_q(H/P)) = 1$ y $H/PQ \neq 1$ es soluble. Luego,

(5) $O_p(H/PQ) = F(H/PQ) \neq 1$.

También, por el argumento de Frattini, $H = O_{p,q}(H)N_H(Q) = PQN_H(Q) = PN_H(Q)$ $= P(P_0Q') = (PP_0)Q'$ para alguna $Q' \in Syl_q(N_H(Q))$. Entonces:

(6) $PP_0 \in Syl_p(H)$.

Finalmente :

(7) $\overline{Q} := PQ/P = F(H/P) = O_q(H/P) \cong Q$.

Lema 5.3. [Ben 5.1] $q = 2$.

Demostración. Suponga que $q \neq 2$.

Afirmamos que H/PQ tiene p-Sylows cíclicos:

Caso 1. $p < q$.

Sea $d = max\{r_q(M) \mid M \in \mathcal{L}_p\}$. Entonces por el Lema B, $d = 1$ (si no, $p = 2$). Luego $r(Q) \leq r_q(H) \leq d = 1$. Así, gracias al Lema 0.41., Q es cíclico y también lo es $\overline{Q} = F(H/P) \lhd H/P$, pues $\overline{Q} \cong Q$. Como H/P es soluble, por el Teorema 0.29., $C_{H/P}(\overline{Q}) \subseteq \overline{Q}$. Luego $C_{H/P}(\overline{Q}) = Z(\overline{Q}) = \overline{Q}$. Entonces:

$\frac{H}{PQ} \cong \frac{H/P}{\overline{Q}} = \frac{H/P}{C_{H/P}(\overline{Q})}$ se inyecta en $Aut(\overline{Q})$, que es cíclico, pues $\overline{Q}$ lo es y $q \neq 2$.

Concluimos, en particular, que los p-Sylows de H/PQ son cíclicos.

Caso 2. $q < p$.

Sea $d = max\{r_p(M) \mid M \in \mathcal{L}_q\}$. Entonces, de nuevo por el Lema B, $d = 1$ (si no, $q = 2$). Entonces $r(P_0) \leq r_p(N_H(Q)) \leq r_p(N_G(Q)) \leq d = 1$. Luego P_0 es cíclico. Sabemos

que $H = PQN_H(Q)$; como $P_0 \in Syl_p(N_H(Q))$ es cíclico, y como los Sylows de un grupo siempre caen en Sylows del cociente, también son cíclicos los p-Sylows de $\frac{N_H(Q)}{PQ \cap N_H(Q)} \cong \frac{PQ \cdot N_H(Q)}{PQ} = \frac{H}{PQ}$.

En cualquier caso, como se había afirmado, los p-Sylows de H/PQ son cíclicos.

Afirmamos a continuación que H/PQ tiene un único subgrupo X/PQ de orden p:

Sea P_1 un subgrupo de orden p de H/PQ. Entonces $P_1 \subseteq S_p \in Syl_p(H/PQ)$. Como $O_p(H/PQ) \lhd H/PQ$, $O_p(H/PQ) \subseteq S_p$. Dado que S_p es cíclico, $O_p(H/PQ) \neq 1$ y $|P_1| = p$, tenemos $P_1 \subseteq O_p(H/PQ)$; pero $O_p(H/PQ)$ es cíclico y por lo tanto tiene un único subgrupo de orden p. Claramente P_1 tiene la forma X/PQ.

Observe que $|X:PQ| = p$.

Veamos ahora que $J(H_p) \subseteq X$.

Si $A_p \subseteq H_p$ es un subgrupo elementalmente abeliano, de rango $r(H_p)$; entonces $\frac{A_p \cdot PQ}{PQ} \subseteq S_p \in Syl_p(H/PQ)$ y, como S_p es cíclico, $\left|\frac{A_p \cdot PQ}{PQ}\right| \leq p$ (pues $\frac{A_p \cdot PQ}{PQ}$ debe ser, también, elementalmente abeliano). Luego $\frac{A_p \cdot PQ}{PQ} \subseteq \frac{X}{PQ}$, y ello implica que $A_p \subseteq X$. Concluimos que $J(H_p) \subseteq X$.

Veamos que $O_p(X) = O_p(H) = P$.

Como $X/PQ \, char \, H/PQ$ y $PQ \, char \, H$, tenemos $X \, char \, H$. Entonces, de $O_p(X) \, char \, X \, char \, H$ obtenemos $O_p(X) \lhd H$ y, en consecuencia, $O_p(X) \subseteq O_p(H)$. Por otro lado, $O_p(H) = P \lhd X$ implica que $O_p(H) \subseteq O_p(X)$. Concluimos que $O_p(X) = O_p(H)$.

Observe que, como $O_p(X) = O_p(H) = P$ y $PQ \lhd X$, tenemos $PQ/P \lhd X/P$, luego $PQ/P \subseteq O_q(X/P)$. Por otro lado $X \lhd H$ implica que $O_q(X/P) \, char \, X/P \lhd H/P$; así, $O_q(X/P) \subseteq O_q(H/P) = PQ/P$. Entonces $O_q(X/P) = PQ/P$ y concluimos que $O_{p,q}(X) = O_{p,q}(H)$.

Asimismo $Z := \Omega_1(Z(P)) = \Omega_1(Z(O_p(X)))$. $J(H_p) \subseteq X$ implica que $J(H_p) \subseteq S_p$ para algún $S_p \in Syl_p(X)$. Entonces $J(S_p) = J(H_p) \not\subseteq P = O_p(X)$. Concluimos que $J(S_p) \not\lhd X$, para todo $S_p \in Syl_p(X)$.

Si $C_X(Z) = P$, entonces $Y := X/C_X(Z) = X/P = X/O_p(X)$, y $O_p(Y) = 1$. Luego Y tendría al menos dos p-subgrupos de Sylow. Entonces, por el Teorema 2.11., $q = 2$, contrario a lo supuesto. Concluimos que $C_X(Z) \neq P$.

Afirmamos ahora que $C_X(Z)$ contiene algún q-elemento no trivial a.

Tenemos $P \subseteq C_X(\Omega_1(Z(P))) = C_X(Z) \neq P$. Como $Z = \Omega_1(Z(O_p(X)))$ *char* X, tenemos $C_X(Z)$ *char* X. Si $C_X(Z)$ fuera un p-grupo, entonces sería un p-subgrupo normal de X. Luego $C_X(Z) \subseteq O_p(X) = P$, que es una contradicción.

Sean $a \in C_X(Z)$ un q-elemento no trivial y M tal que $C_G(a) \subseteq M \in \mathcal{L}_q^*$.

Mostremos que Z contiene un p-subgrupo central de G:

Por el Lema A, $Z(P) = Z(F(H)) \supseteq Z(G_p)$ para alguna $G_p \in Syl_p(G)$. Entonces $Z = \Omega_1(Z(P)) \supseteq \Omega_1(Z(G_p)) \neq 1$. En particular, Z contiene un p-subgrupo central de G. Ahora, si $M_q \in Syl_q(M)$ entonces $M_q \notin Syl_q(G)$, pues de otro modo, $Z \subseteq C_G(a) \subseteq M$ y, por el Lema 3.3., $M \supseteq \langle M_q, Z \rangle = G$, contrario a $M \in \mathcal{L}_q^*$.

Afirmamos que $J(M_q) \not\trianglelefteq M$, para $M_q \in Syl_q(M)$.

Si $J(M_q) \trianglelefteq M$, entonces, para una $G_q \in Syl_q(G)$ con $M_q \subseteq G_q$, tenemos (gracias al párrafo anterior) $M_q \subsetneq G_q$. Luego $M_q \subsetneq N_{G_q}(M_q) =: \hat{M}_q$ (pues en todo q-grupo, sólo el total es su propio normalizador). Entonces $J(M_q)$ *char* $M_q \trianglelefteq \hat{M}_q$ implica (por la maximalidad de M) que $M = N_G(J(M_q)) \supseteq \hat{M}_q \supsetneq M_q \in Syl_q(M)$. Esto es claramente imposible.

Recapitulando:

A partir de H con las propiedades:

(1) $H \in \mathcal{L}_p$.
(2) $J(H_p) \not\trianglelefteq H$ para toda $H_p \in Syl_p(H)$.

Hemos construido M con las propiedades:

(1) $M \in \mathcal{L}_q^*$.
(2) $J(M_q) \not\trianglelefteq M$ para toda $M_q \in Syl_q(M)$.
(3) M contiene un p-subgrupo central.

Como habíamos supuesto que $q \neq 2$, la situación es simétrica para p y q. Entonces podemos aplicar el mismo proceso a la M para construir H' con las propiedades:

(1) $H' \in \mathcal{L}_p^*$.

(2) $J(H_p') \not\trianglelefteq H'$ para toda $H_p' \in Syl_p(H')$, .

(3) H' contiene un q-subgrupo central.

Sin pérdida de generalidad, supondremos que H contiene un q-subgrupo central y que $q < p$. (Intercambie p y q en caso de ser necesario y tome, según convenga, H' o M en lugar de H.)

Sea $d = max\{r_p(K) \mid K \in \mathcal{L}_q\}$; entonces, por el Lema B, $d = 1$ (si no, $q = 2$). Luego, si a es el q-elemento cuya existencia garantizamos antes, $r(Z) \le r_p(C_G(a)) \le d = 1$. Como $Z = \Omega_1(Z(P))$ es elementalmente abeliano, tenemos que $|Z| = p$. Nuevamente, como vimos antes, Z contiene un p-subgrupo central, y así Z mismo es central. Pero $H \subseteq N_G(Z)$ contiene un q-subgrupo central, que necesariamente normaliza a Z. Esto contradice el Lema 3.4.

Concluimos que $q = 2$. #

Supuestos 5.4. Para el resto del capítulo supondremos que el Lema C es falso, es decir, además de las hipótesis del Lema C (Supuestos 5.1.), asumimos que la conclusión del Lema C es falsa. Entonces:

Supondremos para el resto del capítulo que:

$J(H_p)$ no es normal en H, H contiene una involución central y que no existe una $\overline{H} \in \mathcal{L}_p$, con $|H|_p \le |\overline{H}|_p$ y $|F(\overline{H})| > |F(H)|$, que contenga una involución central.

Lema 5.5. [Ben 5.2] $r(Z) \ge 2$ y $C_H(Z) = P$.

Demostración. Sabemos, por el Lema A, que $Z = \Omega_1(Z(F(H)))$ contiene un subgrupo central. Si $r(Z) = 1$, entonces $|Z| = p$ y Z mismo es central. De acuerdo con los Supuestos 5.4., H contiene una involución central, que necesariamente normaliza a Z *char* H, contrario al Lema 3.4.

Entonces $r(Z) \ge 2$.

Claramente, $P \subseteq C_H(Z)$.

Si $C_H(Z)$ es un p-subgrupo, como $C_H(Z) \trianglelefteq H$ (Z *char* H), tenemos $C_H(Z) \subseteq P$ y concluimos que $C_H(Z) = P$.

Supongamos que $C_H(Z) \ne P$. Entonces existe una involución $t \in H$ que centraliza a Z. Como Z contiene elementos centrales, t no puede ser central (ver el Lema 3.4.).

También, $2 \le r(Z) \le r_p(C_G(t))$. Como $C_G(t) \in \mathcal{L}_q$, resulta que $2 \le r_p(C_G(t)) \le d = max\{r_p(K) \mid K \in \mathcal{L}_q\}$ y, por el Lema B, t es central, contrario al párrafo anterior. #

Lema 5.6. [Ben 5.3] Si $V \subseteq H$ es un 4-grupo centralizado por un elemento $a \in H$ de orden p, entonces V contiene un elemento central.

Demostración. Suponga que para toda $x \in V^*$, x no es central. Entonces $r_p(C_G(x)) = 1$, por el Lema B (ii). Por otro lado, V actúa en $\langle a \rangle Z$ y por el Lema 2.3.: $\langle a \rangle Z = \langle C_{\langle a \rangle Z}(x) \mid x \in V^* \rangle$. Pero $1 \leq r_p(C_{\langle a \rangle Z}(x)) \leq r_p(C_G(x)) = 1$. Por el Lema 0.41., $C_{\langle a \rangle Z}(x)$ es cíclico. Si $\langle a \rangle \subsetneq C_{\langle a \rangle Z}(x)$, entonces $a^n z \in C_{\langle a \rangle Z}(x)$ para algunas $z \in Z - \langle a \rangle$ y $n \geq 0$. Entonces $z \in C_{\langle a \rangle Z}(x)$. Luego $\langle a \rangle \neq \langle z \rangle$ son dos subgrupos de orden p de $C_{\langle a \rangle Z}(x)$. Esto es imposible pues $C_{\langle a \rangle Z}(x)$ es cíclico. Concluimos que $C_{\langle a \rangle Z}(x) = \langle a \rangle$ para toda $x \in V^*$. Como $\langle a \rangle Z$ es generado por tales centralizadores, concluimos que $\langle a \rangle Z = \langle a \rangle$. Esto es contrario al Lema 5.5. #

Lema 5.7. [Ben 5.4] H no tiene subgrupos elementalmente abelianos de orden 2^4.

Demostración. Suponga que V es uno de tales subgrupos de orden 2^4. Entonces V actúa en Z y, por el Lema 2.3., $Z = \langle C_Z(V_i) \mid |V:V_i| = 2 \rangle$.

Si $r_p(C_Z(V_i)) \geq 2$ para alguna i, tomamos un 4-subgrupo U de V_i, que satisface $C_Z(V_i) \subseteq C_Z(U)$. Entonces $r_p(C_G(U)) \geq r_p(C_Z(U)) \geq r_p(C_Z(V_i)) \geq 2$ contrario al Lema B.

Si en cambio $r_p(C_Z(V_i)) = 1$ para toda i, podemos tomar, en vista de que $r(Z) \geq 2$, dos subgrupos V_1 y V_2 de V de índice 2 tales que $r_p(C_Z(V_1) + C_Z(V_2)) \geq 2$. Sea $U = V_1 \cap V_2$. Entonces $|U| = \frac{|V_1||V_2|}{|V_1 V_2|} = \frac{2^3 \cdot 2^3}{2^4} = 4$ y $C_Z(V_1) + C_Z(V_2) \subseteq C_Z(U)$. Luego:

$$r_p(C_G(U)) \geq r_p(C_Z(U)) \geq r_p(C_Z(V_1) + C_Z(V_2)) \geq 2.$$

De nuevo contrario al Lema B. #

Lema 5.8. [Ben 5.5] $\overline{P_0} := P_0/(P \cap P_0)$ es cíclico.

Demostración. Supongamos que $\overline{P_0}$ no es cíclico. Por el Lema 0.41., tenemos $r(\overline{P_0}) \geq 2$. Sea $U = \Omega_1(Z(Q))$. Como P_0 actúa en Q, también actúa en U. Por el Lema 5.7., $|U| \leq 8 = 2^3$. Entonces (ver el Lema 0.45.) $|Aut(U)| = 1$ o $2 \cdot 3$ o $8 \cdot 7 \cdot 3$. En cualquier caso $|P_0 : C_{P_0}(U)| \leq p$. También:

$$|PP_0 : PC_{P_0}(U)| = \left|\frac{PP_0}{PC_{P_0}(U)}\right| = \left|\frac{PC_{P_0}(U)P_0}{PC_{P_0}(U)}\right| = \left|\frac{P_0}{PC_{P_0}(U) \cap P_0}\right| \leq \left|\frac{P_0}{C_{P_0}(U)}\right| \leq p.$$

Recordamos, de las observaciones del principio del capítulo, que PP_0 es un p-Sylow de H. Dividiremos el resto de la prueba en dos casos:

Caso 1. U contiene una involución central.

Sea $\overline{H} := N_G(PC_{P_0}(U))$. Como U normaliza a P y a $C_{P_0}(U)$, tenemos $U \subseteq \overline{H}$. Luego $\overline{H}$ tiene una involución central. Además $|PP_0 : PC_{P_0}(U)| \leq p$ implica que $PP_0 \subseteq N_G(PC_{P_0}(U))$. En consecuencia $|\overline{H}|_p \geq |H|_p$. Por otro lado tenemos que $PC_{P_0}(U) \subseteq O_p(\overline{H})$. Es claro que $P \subseteq PC_{P_0}(U)$.

Si $P = PC_{P_0}(U)$ tendríamos:

$$\overline{P_0} := \frac{P_0}{P \cap P_0} = \frac{P_0}{PC_{P_0}(U) \cap P_0}.$$

Entonces $|\overline{P_0}| = |P_0 : PC_{P_0}(U) \cap P_0| \leq |P_0 : C_{P_0}(U)| \leq p$, y $\overline{P_0}$ tendría que ser cíclico.

Concluimos que $P \subsetneq PC_{P_0}(U) \subseteq O_p(\overline{H}) \subseteq F(\overline{H})$.
Pero entonces $|F(\overline{H})| > |F(H)|$, que es contrario a los Supuestos 5.4.

Caso 2. U no posee involuciones centrales.

Como $|P_0 : C_{P_0}(U)| \leq p$ y $r(P_0) \neq 1$, tenemos que $C_{P_0}(U) \neq 1$. Entonces U es centralizado por un elemento de $C_{P_0}(U) \subseteq H$ de orden p; así que, por el Lema 5.6., $|U| = 2$. Luego $Aut(U) = 1$. Dado que P_0 actúa en U, P_0 debe centralizar a U y así $P_0 \subseteq C_G(U)$. Como U no es central tenemos, por el Lema B, que $r_p(C_G(U)) = 1$. Entonces $2 \leq r(P_0) \leq r_p(C_G(U)) = 1$ nos da la contradicción buscada. #

Lema 5.9. [Ben 5.6] H/PQ tiene un único subgrupo X/PQ de orden p. Además:

(i) Ninguna involución central normaliza a un p-Sylow de X.

(ii) Q contiene una involución central.

Demostración. De las Observaciones 5.2., recordamos que $H = PN_H(Q)$ y $PP_0 \in Syl_p(H)$. Entonces un p-Sylow de H/PQ es:

$$\frac{PP_0 \cdot PQ}{PQ} = \frac{P_0 \cdot PQ}{PQ} \cong \frac{P_0}{P_0 \cap PQ} = \frac{P_0}{P_0 \cap P} = \overline{P_0}, \text{ que es cíclico.}$$

Recordamos (nuevamente, de las Observaciones 5.2.) que $O_p(H/PQ) \neq 1$. Por ser un p-subgrupo normal, $O_p(H/PQ)$ está contenido en todos los p-Sylows de H/PQ; como éstos son cíclicos, $O_p(H/PQ)$ también lo es. Se sigue que todo subgrupo de orden p de H/PQ debe estar contenido en $O_p(H/PQ)$ y este último (por ser cíclico) tiene sólo un subgrupo de ese orden. Denotaremos tal subgrupo por X/PQ.

Mostremos (i): Suponga que una involución central $t \in G$ normaliza a un $X_p \in Syl_p(X)$.

Sea $\overline{H} := N_G(X_p)$. Entonces $\overline{H} \in \mathcal{F}_p$ y $\overline{H}$ tiene una involución central. Claramente $X \lhd H$ y $X = X_pQ$. Luego, por el argumento de Frattini, $H = XN_H(X_p) = QN_H(X_p)$. Así $|H|_p = |N_H(X_p)|_p \leq |N_G(X_p)|_p$ y $|H|_p \leq |\overline{H}|_p$. Además $F(H) = P \subsetneq X_p \subseteq O_p(\overline{H}) \subseteq F(\overline{H})$. Concluimos que $|F(H)| < |F(\overline{H})|$, contrario a los Supuestos 5.4.

Mostremos (ii): Suponga que Q no tiene involuciones centrales.

Luego tampoco las tiene PQ (conjugue por elementos de PQ; observe que $Q \in Syl_q(PQ)$). Si $t \in H$ es una involución central (Supuestos 5.4.), $t \notin PQ$. Entonces, si $\bar{t}$ denota la clase de t en H módulo P, $\bar{t} \in O_2(H/O_p(H)) = QP/P =: \overline{Q}$. Luego, por el Teorema 1.7., $\bar{t}$ invierte (normaliza) un subgrupo de H/P de orden p, digamos $\overline{X}_p$. Entonces t normaliza a X_p (la imagen inversa de $\overline{X}_p$ según la proyección natural). Por otro lado, $X_pQ = X_pPQ$ y

$$\frac{X_pPQ}{PQ} = \frac{X_pQ}{PQ} = \frac{X}{PQ} \quad \text{(pues } \frac{X_pQ}{PQ} \text{ tiene orden } p\text{)}.$$

Concluimos que $X_pQ = X$, es decir, X_p es un p-Sylow de X normalizado por t. Esto es contrario a (i). #

Lema 5.10. [Ben 5.7] Q contiene exactamente una involución y ésta no es central.

Demostración. Sea $P_1 = P_0 \cap X$. Veamos que $P_1 \in Syl_p(N_X(Q))$. Claramente $P_1 \subseteq N_X(Q)$. Sean $S_p \in Syl_p(N_X(Q))$ y $\hat{S}_p \in Syl_p(N_H(Q))$ tales que $P_1 \subseteq S_p \subseteq \hat{S}_p$. En este caso $\hat{S}_p \cap X = S_p$. Como P_0 y $\hat{S}_p$ son conjugados en $N_H(Q)$, entonces para alguna $g \in N_H(Q)$ y recordando que X *char* H, tenemos: $S_p^g = (\hat{S}_p \cap X)^g = \hat{S}_p^g \cap X^g = \hat{S}_p^g \cap X = P_0 \cap X = P_1$. Concluimos que $P_1 = S_p$ es un p-Sylow de $N_X(Q)$.

Por el argumento de Frattini, como $PQ \lhd X$, tenemos $X = PN_X(Q) = PP_1Q$. Concluimos que $PP_1 \in Syl_p(X)$. En particular $P_1 \neq 1$ y $P_1 \not\subseteq P$, pues $|X : PQ| = p$.

Ahora, por el Lema 5.9.(i), $C_Q(P_1) \subseteq N_Q(PP_1)$ no contiene involuciones centrales. Luego, por el Lema 5.6., $C_Q(P_1)$ no contiene 4-grupos.

Si $P_1^g = P_1$ para toda $g \in Q$, entonces Q normaliza a P_1 y $\overline{Q}$ normaliza a $\overline{P_1}$ (donde $\overline{Q}$ y $\overline{P_1}$ son las imágenes de Q y P_1, bajo la proyección $H \to H/P$). Luego, dado que también $\overline{Q} = O_q(H/P) \lhd H/P$, tenemos $[\overline{Q}, \overline{P_1}] \subseteq \overline{Q} \cap \overline{P_1} = 1$ y por lo tanto $P_1 \subseteq P$, contrario a lo que sabemos.

Sea $P_2 := P_1^g \neq P_1$ con $g \in Q$.

Los siguientes argumentos van encaminadas a usar el Teorema 2.11.

Claramente, $P \subseteq O_p(X)$ y, como también $O_p(X)$ *char* X *char* H, tenemos $O_p(X) \lhd H$ y $O_p(X) \subseteq O_p(H) =: P$. Concluimos que $O_p(X) = O_p(H) = P$.

También es claro que $\overline{Q} = QP/P = O_q(X/P)$, pues $\overline{Q} \in Syl_q(X/P)$ y $\overline{Q} \lhd H/P$. Entonces $O_{p,q}(X) = PQ$ y $|X : O_{p,q}(X)| = p$.

Afirmamos que $J(X_p) \not\lhd X$ para cada $X_p \in Syl_p(X)$:

Note que si $J(X_p) \lhd X$ para algún $X_p \in Syl_p(X)$, necesariamente eso sucede para todo p-Sylow de X.

Sean $X_p \in Syl_p(X)$ tal que $J(X_p) \lhd X$ y H_p tal que $X_p \subseteq H_p \in Syl_p(H)$. Si $A \subseteq H_p$ es cualquier p-subgrupo elementalmente abeliano de rango máximo; entonces $\overline{A} := \frac{A \cdot PQ}{PQ} \cong \frac{A}{A \cap PQ}$ es también elementalmente abeliano. Como $\overline{A} \subseteq H/PQ$, tenemos, por el Lema 5.9., que $\overline{A} \subseteq X/PQ$. Como $|X|_p = p \cdot |P|$, tenemos que $X_p \not\subseteq PQ$. Luego $\overline{X_p} := (X_p \cdot PQ)/PQ \neq 1$ y, así, $\overline{X_p} = X/PQ$. Entonces $\overline{A} \subseteq \overline{X_p}$ implica que $A \subseteq X_p PQ \cap H_p$; como $P \lhd X$, tenemos que P está contenido en todos los Sylows de X, en particular, $X_p P = X_p$. Luego, $A \subseteq X_p Q \cap H_p = X_p$ y en consecuencia $J(H_p) \subseteq X_p \subseteq H_p$. Por las Observaciones 5.2.(2), tenemos: $J(H_p) = J(X_p) \lhd X$. Luego $J(H_p) = J(X_p) \subseteq O_p(X) = O_p(H)$, que es una contradicción con las Observaciones 5.2.(3).

Ahora, $\overline{P_1} := \frac{P_1 P}{P}$ y $\overline{P_2} := \frac{P_2 P}{P}$ son p-Sylows distintos de X/P, pues si fueran iguales, tendríamos $P_1 P = P_2 P$. Luego, puesto que P_1 y P_2 son p-Sylows de $N_X(Q)$, tenemos $P_1 = P_1 P \cap N_X(Q) = P_2 P \cap N_X(Q) = P_2$. Esto es una contradicción.

También $C_X(Z) = P$, pues $C_H(Z) = P$ (Lema 5.5.).

Usando el Teorema 2.11., concluimos que $\langle \overline{P_1}, \overline{P_2} \rangle$ contiene exactamente una involución y que $|Z : C_Z(\langle \overline{P_1}, \overline{P_2} \rangle)| = p^2$.

Afirmamos ahora que $\langle P_1, P_2\rangle$ tiene una sola involución.

Como $|X: PQ| = p$, tenemos que Q es un q-Sylow de $N_X(Q)$. Además $Q \lhd N_X(Q)$. Luego, Q es el único q-Sylow de $N_X(Q)$. Entonces $\langle P_1, P_2\rangle \cap Q := Q'$ es un q-Sylow de $\langle P_1, P_2\rangle$, claramente normal. Luego $\langle P_1, P_2\rangle = P_1 Q'$ con $Q' \lhd \langle P_1, P_2\rangle$ y $Q' \subseteq Q$, pues P_1 es un p-Sylow de $\langle P_1, P_2\rangle$. Entonces $Q' \cong \frac{Q'}{P \cap Q'} \cong \frac{Q'P}{P} =: \overline{Q}' \subseteq \langle \overline{P}_1, \overline{P}_2\rangle$. Concluimos que $\overline{Q}'$ y $Q' \cong \overline{Q}'$ tienen a lo más una involución (ver párrafo anterior). Como $\langle P_1, P_2\rangle$ tiene al menos dos p-Sylows, Q' no puede ser trivial y, así, Q' tiene exactamente una involución. En consecuencia, $\langle P_1, P_2\rangle$ debe tener exactamente una involución, pues todo 2-elemento de $\langle P_1, P_2\rangle$ debe estar contenido en $Q' \lhd \langle P_1, P_2\rangle$.

Sea t la única involución de $\langle P_1, P_2\rangle$.

Dado que $P = C_X(Z)$, $\langle \overline{P}_1, \overline{P}_2\rangle$ actúa fielmente en Z. Sea $\bar{t}$ la imagen de t bajo la proyección natural, al tomar cociente por P. Tenemos que $|Z: C_Z(\langle \overline{P}_1, \overline{P}_2\rangle)| = p^2$ implica $|Z: C_Z(\bar{t})| \leq p^2$. Recordando nuevamente que $P = C_X(Z)$, tenemos que $\bar{t}$ actúa en Z de idéntica manera que t. Entonces $|Z: C_Z(t)| \leq p^2$.

Ahora bien, $t \in C_Q(P_1)$, pues $t \in Q' \subseteq Q$, y como t es la única involución de $\langle P_1, P_2\rangle$, tenemos $\langle t\rangle$ *char* $\langle P_1, P_2\rangle$; luego P_1 actúa en $\langle t\rangle$, trivialmente pues $Aut(\langle t\rangle) = 1$. Además t es la única involución de $C_Q(P_1)$, pues, por el tercer párrafo de esta demostración, $C_Q(P_1)$ no tiene 4-grupos (ver Lema 0.41.). También por el tercer párrafo de esta demostración, t no puede ser central.

Afirmamos que todo q-subgrupo P_1-invariante no trivial R de Q contiene a t.

Como R es P_1-invariante, si R normaliza a P_1, tenemos $[R, P_1] \subseteq R \cap P_1 = 1$. Luego $R \subseteq C_Q(P_1)$ o RP_1 tiene un p-Sylow $P_3 \neq P_1$. En el primer caso, como R es no trivial, debe contener a la única involución de $C_Q(P_1)$: t. En el segundo caso, igual que antes, $\langle P_3, P_1\rangle \subseteq P_1 R$ debe contener una única involución; ya que $R \lhd P_1 R$, ésta debe estar contenida en R. Entonces, también igual que antes, esta involución debe estar contenida en $C_Q(P_1)$, pero $C_Q(P_1)$ tiene una sola involución: t.

Sea $W := [t, Z]$.

Afirmamos que $W = \{w \in Z \mid w^t = w^{-1}\}$.

Sea $W_0 = \{w \in Z \mid w^t = w^{-1}\}$. Si $tzt z^{-1}$ es un generador de W, tenemos $t(tzt z^{-1})t = zt z^{-1} t = (tzt z^{-1})^{-1}$, luego $w^t = w^{-1}$. Como W es abeliano, lo mismo pasa para el resto de los elementos de W y entonces $W \subseteq W_0$. Por el Teorema 2.1., $Z = C_Z(t)[t, Z]$; entonces, como t actúa en W por inversión y como W no es un 2-grupo, tenemos $C_Z(t) \cap [t, Z] = 1$. Luego $Z = C_Z(t) \times [t, Z] = C_Z(t) \times W$. Si ahora $z \in Z$, entonces $z = cw$

para algunas $c \in C_Z(t)$ y $w \in [t,Z] = W$. Si $z' = z^{-1}$, tenemos $cw^{-1} = (cw)' = w^{-1}c^{-1} = c^{-1}w^{-1}$. Esto implica que $c^{-1} = c = 1$ y $z = w$. Entonces $W_0 \subseteq W$. Concluimos que, como se había afirmado, $W = W_0$.

Observe que $W \neq 1$, pues en caso contrario, $Z = C_Z(t)$ y $t \in C_H(Z) = P$. Además, $Z = C_Z(t) \times W$ implica que $|W| = |Z : C_Z(t)| \leq p^2$.

Veamos ahora que $C_Q(t)$ actúa fielmente en W:

Observamos que P_1 actúa en $\langle t \rangle$, en Q y en P. Luego P_1 actúa también en $Z := \Omega_1(Z(P))$, en $W := [t,Z]$, en $C_Q(t)$ y también en $C_{C_Q(t)}(W)$. Si $C_{C_Q(t)}(W) \neq 1$, entonces $t \in C_{C_Q(t)}(W)$, pero t no centraliza a W.

Suponga en adelante que el Lema que nos ocupa es falso.

Como hemos probado que $t \in Q$ es una involución no central, Q debe contener alguna otra involución.

Afirmamos que $C_Q(t)$ contiene un 4-grupo U.

Como Q es P_1-invariante, también lo es $\Omega_1(Z(Q))$; luego $t \in \Omega_1(Z(Q))$. Si u es cualquier involución de Q distinta de t, tenemos que $U = \langle u,t \rangle \subseteq C_Q(t)$ es el 4-grupo deseado.

Observemos también que $[P_1, C_Q(t)] \neq 1$:

Si $[P_1, C_Q(t)] = 1$, entonces $[P_1, U] = 1$. Por el Lema 5.6., U contiene una involución central: τ. Luego τ actúa en P_1 (trivialmente) y en P *char* H. Entonces τ actúa en $PP_1 \in Syl_p(X)$, contrario al Lema 5.9. (i).

Veamos ahora que $[P_1, W] \neq 1$:

Suponga que $[P_1, W] = 1$. Por Teorema 2.1., $W = C_W(t)[t,W]$ y, como sabemos que t actúa por inversión en W, tenemos $C_W(t) = 1$ y $[C_Q(t), W] \supseteq [t,W] = W$. Puesto que $C_Q(t)$ actúa en W, resulta $W = [C_Q(t), W]$. Entonces $[P_1, W, C_Q(t)] = [[P_1, W], C_Q(t)] = 1$ y también $[W, C_Q(t), P_1] = [W, P_1] = 1$. Por el teorema de los tres subgrupos, $[C_Q(t), P_1, W] = 1$. Luego $[C_Q(t), P_1] \subseteq C_{C_Q(t)}(W) = 1$. La igualdad $[C_Q(t), P_1] = 1$ contradice el párrafo anterior.

Ahora bien, sabemos que $|W| \leq p^2$ y que, claramente, P_1 actúa en W. Si $|W| \leq p$, entonces P_1 actuaría trivialmente en W, contrario a lo que sabemos. Concluimos que $|W| = p^2$.

Así pues, $C_Q(t)P_1 \cong C_Q(t) \rtimes P_1$ actúa en W y el homomorfismo respectivo $\varphi : C_Q(t)P_1 \to Aut(W) = GL(W) \cong GL(2,p)$ es tal que $\varphi(C_Q(t)) \cong C_Q(t) \neq 1$, $\varphi(P_1) \neq 1$ y

$\varphi(P_1)$ normaliza a $\varphi(C_Q(t))$. Como $q = 2$, por el Teorema 2.10., tenemos $r(C_Q(t)) = 1$. Esto es contrario a que $C_Q(t)$ contiene 4-grupos.

Con esta contradicción terminamos la prueba. #

6. La contradicción

Teorema 6.1. (-$p^\alpha q^\beta$ de Burnside) Todo grupo G de orden $|G| = p^\alpha q^\beta$, con p y q números primos es soluble.

Demostración. Supongamos que el teorema es falso. Sea G un contraejemplo minimal. Entonces, como se dijo al inicio del capítulo 4, $p \neq q$ y G debe ser simple.

Caso I. $q = 2$ (es decir, alguno de los dos primos es 2).

Según el Teorema 1.7. toda involución invierte a algún p-elemento (pues, como G es simple, $O_2(G) = 1$). Sea t una involución central y $a \neq 1$ un p-elemento que es invertido por t. Entonces $t \in H := N_G(\langle a \rangle) \in \mathcal{F}_p$. Concluimos que existe $H \in \mathcal{F}_p$ que contiene involuciones centrales.

Escoja $H \in \mathcal{F}_p$ con las siguientes condiciones:

1) H tiene involuciones centrales.
2) $|H|_p$ es máximo entre los que satisfacen (1).
3) $|F(H)|$ es máximo de entre los que satisfacen (1) y (2).

Por el Lema C, $J(H_p) \lhd H$ para cualquier $H_p \in Syl_p(H)$.

Suponga que H_p no es un p-Sylow de G. Sea $G_p \supsetneq H_p$ un p-Sylow de G; entonces, como G_p es un p-grupo, tenemos $H_p \subsetneq N_{G_p}(H_p)$. Ahora $J(H_p)\, char\, H_p \lhd N_{G_p}(H_p)$ implica que $J(H_p) \lhd N_{G_p}(H_p) \supsetneq H_p$. Luego $H \subsetneq N_G(J(H_p)) \in \mathcal{F}_p$ y $N_G(J(H_p))$ también contiene involuciones centrales. Además $|N_G(J(H_p))|_p \geq |N_{G_p}(J(H_p))| > |H_p| = |H|_p$, en contradicción con la maximalidad de H.

Concluimos que $H_p = G_p$ es un p-Sylow de G.

Ahora H contiene a un p-Sylow de G y a una involución central, por el Lema 3.3., $H = G$. Luego $1 \neq J(H_p) \lhd G$ contradiciendo la simplicidad de G.

Caso II. $p \neq 2 \neq q$

Escogemos notación de tal forma que $|G|_p > |G|_q$.

Si $H \in \mathcal{F}_p$ y $H_p \in Syl_p(H)$, por el Lema C y como $q \neq 2$, tenemos $J(H_p) \lhd H$. Entonces, si $H \in \mathcal{F}_p^*$, $H = N_G(J(H_p))$.

Afirmamos que $H \in \mathcal{F}_p^*$ implica $Syl_p(H) \subseteq Syl_p(G)$.

Supongamos que la afirmación es falsa. Sean $H_p \in Syl_p(H) - Syl_p(G)$ y G_p un p-Sylow de G tal que $H_p \subsetneq G_p$. Entonces $\hat{H}_p := N_{G_p}(H_p) \supsetneq H_p$. Luego $J(H_p)\ char\ H_p \lhd \hat{H}_p$ implica $\hat{H}_p \subseteq N_G(J(H_p)) = H$, contrario a que $H_p \subsetneq \hat{H}_p$ es un p-Sylow de H.

Entonces $H \in \mathcal{F}_p^*$ implica que $H = N_G(J(G_p))$, para algún $G_p \in Syl_p(G)$. En particular $|H|_p = |G|_p$. Además, todos los elementos de $\mathcal{F}_p^*$ son conjugados entre sí (con elementos de G). Como G es simple, $|\mathcal{F}_p^*| > 1$.

Escogemos $M_1, M_2 \in \mathcal{F}_p^*$ con $M_1 \neq M_2$ tal que $|M_1 \cap M_2|_p$ es maximal. Sea $P \in Syl_p(M_1 \cap M_2)$ (note que $|P| = |M_1 \cap M_2|_p$). Ahora bien, P no puede ser un p-Sylow de G (ni de M_1 o M_2) pues, si lo fuera, tendríamos $M_1 = N_G(J(P)) = M_2$, contrario a lo supuesto. Entonces P está contenido propiamente en dos p-Sylows S_p^1 y S_p^2 de M_1 y M_2 respectivamente. Así, $|P| < |N_{S_p^i}(P)| \leq |N_{M_i}(P)|_p$ para $i = 1,2$.

Suponga que $P \neq 1$. Sea H_i tal que $N_G(P) \subseteq H \in \mathcal{F}_p^*$. Entonces, para $i = 1,2$, tenemos $|P| < |N_{M_i}(P)|_p = |M_i \cap N_G(P)|_p \leq |M_i \cap H|_p$. Por la maximalidad de $|P|$, resulta que $M_1 = H = M_2$, contrario a lo supuesto.

Concluimos que $P = 1$.
Entonces $|M_1 M_2| \geq |M_1|_p |M_2|_p = |G|_p^2 > |G|$, pues $|G|_p > |G|_q$.
Contradicción. #

Bibliografía

[Alp] Alperin, J. y Lyons, R.
"On Conjugacy Classes of p-Elements"
J. of Algebra **19**, 536-537 (1971)

[Asc] Aschbacher, Michael
Finite Group Theory
Cambridge Studies in Advanced Mathematics 10 (1986)

[Ben] Bender, Helmut.
"A Group Theoretic Proof of Burnside's p^aq^b-Theorem"
Math. Z. **126**, 327-338 (1972)

[Ben II] Bender, Helmut.
"Über den größten p'-Normalteiler in p-auflösbaren Gruppen"
Arch. der Math. **18**, 15-16 (1967)

[Bur] Burnside, W.
"On Groups of Order $p^\alpha q^\beta$"
Proc. London Math. Soc. (2) **2**, 432-437 (1904)

[Bur II] Burnside, W.
Theory of Groups of Finite Order
Dover Publications Inc. (1955)
(Versión original: Cambridge Univ. Press, 2ª edición: 1911)

[Fei] Feit, W. y Thompson, J. G.
"Solvability of Groups of Odd Order"
Pacific J. Math. **13**, 775-1029 (1963)

[Gla] Glauberman, G.
"A Characteristic Subgroup of a p-Stable Group"
Canad. J. Math. **20**, 1101-1135 (1968)

[Gol] Goldschmidt, David.
"A Group Theoretic Proof of the p^aq^b Theorem for Odd Primes"
Math. Z. **113**, 373-375 (1970)

[Gor] Gorenstein, Daniel.
Finite Groups
New York: Harper and Row (1968).

[Hal] Hall, Marshall Jr.
Teoria de los Grupos Finitos
Ed. Trillas (1979)
(Versión Original en Inglés: 1967)

[Mat] Matsuyama, Hiroshi.
"Solvability of Groups of Order $2^a p^b$"
Osaka J. Math **10**, 375-378 (1973)

[Piz] Pizaña-López, Miguel-Angel
"Sobre el Teorema $p^a q^\beta$ de Burnside"
Tesis de Licenciatura UNAM (1996)

[Rot] Rotman, Joseph J.
An Introduction to the Theory of Groups
Wm. C. Brown Publishers, Dubuque, Iowa, (1988)

[Tho] Thompson, J. G.
"Non-Solvable finite Groups all of Whose local subgroups are solvable"
Bull. Amer. Math. Soc. **74**, 383-437 (1968)

[Suz] Suzuki, Michio.
Group Theory. Vols. I y II
Berlin-Heidelberg-New York, Springer Verlag (1982)
(Versión original en japonés: 1977)